ABSTRACT

Title of Dissertation: THE DEGREE OF MODULAR PARAMETRIZATIONS OF $\mathbb{Q}$-CURVES

Mark D. Morgan, Doctor of Philosophy, 1999

Dissertation directed by: Professor Lawrence C. Washington
Department of Mathematics

An elliptic curve E is modular if there is a non-constant morphism from $J_1(N)$, the Jacobian of the modular curve $X_1(N)$, to the elliptic curve E. An elliptic curve defined over a number field which is isogenous to each of its Galois conjugates is called a $\mathbb{Q}$-curve. It is conjectured that the set of $\mathbb{Q}$-curves is precisely the set of modular elliptic curves [15]. Suppose that there exists a map ϕ from $X_1(N)$ to E which is given by

$$\phi(\tau) = \int_{\tau_0}^{\tau} h(z)dz$$

where τ_0 is a fixed point in the upper half plane and h is a cusp form of weight 2 and level N. The map ϕ is called a strong Weil parametrization. In this work, we will be focusing on computing the degree of this covering map when E is a $\mathbb{Q}$-curve without complex multiplication where E is defined over a quadratic field.

The first step is to develop an algorithm for computing the degree. This is done by modifying an algorithm of Cremona which computes the degree of modular parametrization of an elliptic curve defined over $\mathbb{Q}$ [4]. This algorithm can be effectively implemented when ϕ is a map from $X_0(N)$ rather than $X_1(N)$. A number of computational tools are developed using modular symbol techniques which are used in developing the algorithm.

The map ϕ will factor through an abelian variety A_f where f is an eigenform which is given by a construction of Shimura [19]. If A_f is a two-dimensional abelian variety, we show that the set of strong Weil parametrizations which factor through A_f is in one-to-one correspondence to $\mathbb{P}^1(\mathbb{Z})$. For each point $(u:v) \in \mathbb{P}^1(\mathbb{Z})$, we have a parametrization $\phi(u,v)$ to some $\mathbb{Q}$-curve. Also, the degrees of the maps $\phi(u,v)$ are given by the values of a positive definite binary quadratic form in the variables u and v. We show how this quadratic form can be determined algebraically up to a constant multiple.

Not all $\mathbb{Q}$-curves are isogenous to a quotient of a two-dimensional abelian variety. Given a modular $\mathbb{Q}$-curve, one would like to determine the dimension of the smallest abelian variety A_f which contains E as a simple factor up to isogeny. Assuming E is modular, we give conditions which guarantee that E is a simple factor of an abelian variety A_f with dimension either 2, 4, or 8.

THE DEGREE OF MODULAR

PARAMETRIZATIONS OF $\mathbb{Q}$-CURVES

by

Mark D. Morgan

Dissertation submitted to the Faculty of the Graduate School of the
University of Maryland at College Park in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
1999

Advisory Committee:

Professor Lawrence C. Washington, Chairman/Advisor
Professor Kevin R. Coombes
Professor Stephen S. Kudla
Professor Jonathan M. Rosenberg
Professor Willam I. Gasarch

DEDICATION

To my wife, Melissa, and my parents, Douglas and Beverly.

ACKNOWLEDGEMENTS

I would like to extend my deepest gratitude to my advisor, Lawrence Washington, for his assistance and encouragement during my graduate school career.

I would like to thank my parents, Douglas and Beverly Morgan, for all of their support throughout my life. I am so proud to be their son.

To my wife, Melissa Varney, I am so grateful for your love and devotion. Thank you for being the love of my life and for helping me achieve my goals.

I want to express my thanks to God for giving me the ability and discipline to complete my degree. I have been so richly blessed by Him.

TABLE OF CONTENTS

Chapter 0

Introduction

An elliptic curve E defined over a number field is called *modular* if there is a non-constant morphism from $J_1(N)$, the Jacobian of the modular curve $X_1(N)$, to E. In his proof of Fermat's Last Theorem, A. Wiles has shown that all semi-stable elliptic curves defined over $\mathbb{Q}$ are modular [22]. Since then, others have extended this to a larger class of elliptic curves defined over $\mathbb{Q}$. The next step in understanding modularity is to determine which elliptic curves over number fields are modular. An elliptic curve defined over a number field which is isogenous to each of its Galois conjugates is called a $\mathbb{Q}$-curve. It is conjectured that $\mathbb{Q}$-curves are precisely the set of elliptic curves which are modular [15]. Suppose there exists a map ϕ from $X_1(N)$ to E given analytically by

$$\phi(\tau) = \int_{\tau_0}^{\tau} h(z)dz$$

where τ_0 is a fixed point in the upper half plane and h is a cusp form of weight 2 and level N for $\Gamma_1(N)$. In this case, E is said to have a strong Weil parametrization. Every modular elliptic curve is obtained by such a map followed by an isogeny. Both $X_1(N)$ and E are Riemann surfaces, and ϕ is a branched covering of E. The Hurwitz formula does not give any information about the degree of

ϕ since the genus of E is one. Throughout the work, we will assume that E is a modular $\mathbb{Q}$-curve defined over $\mathbb{Q}(\sqrt{t})$ without complex multiplication. We will discuss several aspects concerning the degree of modular parametrizations of $\mathbb{Q}$-curves defined over quadratic fields. First, we develop an effective algorithm to compute the degree. This requires a great deal of computational work as well as the development of the theoretical background to verify that the algorithm works. Secondly, we compute the degree of modular parametrization in a number of examples. Finally, several number theoretic properties of the degree are proved which relate the degree to certain quadratic extensions of $\mathbb{Q}$.

Let us restrict to the case when E has a modular parametrization ϕ from $X_0(N)$ for some N. J. Cremona has developed modular symbol algorithms which compute a basis for the homology of $X_0(N)$, compute Fourier coefficients of cusp forms, and numerically approximate the periods of cusp forms [5]. We have written computer programs using the GP-PARI package which perform the algorithms described by Cremona. We have had to be mindful of both running time and storage space in order to make the programs effective. We have also made improvements to Cremona's algorithm for approximating periods of cusp forms. In Chapter 1, these algorithms using modular symbols are described which provide the computational basis for conducting a large part of the research.

Cremona has developed an algorithm for computing the degree of a strong Weil parametrization of an elliptic curve over $\mathbb{Q}$. However, for a $\mathbb{Q}$-curve defined over a quadratic extension, Cremona's formula cannot be used without solving two problems. First, one must find the cusp form h such that the periods of h are equal to the periods of E up to a constant multiple. Let $\{\omega_1, \omega_2\}$ be a basis for the period lattice of h. Then for any $\gamma \in \Gamma_0(N)$, $\int_0^{\gamma(0)} h(z)dz = n_1(\gamma)\omega_1 + n_2(\gamma)\omega_2$

for some integers $n_1(\gamma)$ and $n_2(\gamma)$. The second problem is finding these values of n_i for any $\gamma \in \Gamma_0(N)$ in a systematic way that does not involve approximating a basis for the period lattice. The choice of basis for the period lattice of h does not affect the degree calculation. Hence, the goal is to find a convenient basis $\{\omega_1, \omega_2\}$ such that it is possible to calculate the values of n_1 and n_2. In Chapter 2, we develop an algorithm which overcomes each of these problems and gives an effective method for computing the degree. The algorithm is particularly nice since one does not have to compute a large number of Fourier coefficients of cusp forms, which is time-consuming. However, if a large number of Fourier coefficients of h are known, then this algorithm provides a way to calculate a numerical approximation to a basis for the period lattice by computing the periods of h over two particular paths.

Also in chapter 2, we discuss the decomposition of abelian varieties into the product of elliptic curves up to isogeny. For any eigenform f, Shimura has constructed an abelian variety A_f which is a factor of $J_1(N)$ [19]. If K is the extension of $\mathbb{Q}$ obtained by adjoining the coefficients of f, then $[K : Q] = \dim_{\mathbb{Q}} A_f$. Let f be a cusp form such that $K = \mathbb{Q}(\sqrt{r})$, and let f' be the Galois conjugate of f. Suppose $f' = f \otimes \chi$ where χ is a quadratic character associated to the field $L = \mathbb{Q}(\sqrt{t})$. Let $End(A_f) \otimes \mathbb{Q}$ denote the set of all endomorphisms of A_f which are defined over $\overline{\mathbb{Q}}$. Then $End(A_f) \otimes \mathbb{Q}$ is isomorphic to a quaternion algebra. If the quaternion algebra is isomorphic to $M_2(\mathbb{Q})$, then A_f can be split into the product of two elliptic curves defined over $\mathbb{Q}(\sqrt{t})$. Otherwise, the abelian variety cannot be decomposed. Let e be an endomorphism of A_f corresponding to a rank one matrix in $M_2(\mathbb{Q})$. Then A_f is isogenous to $A_f/eA_f \times A_f/e^\sigma A_f$, which is the product of an elliptic curve and its Galois conjugate. Using the endomorphism e, a function h in the span of f and f' can be found such that $eh = 0$. The periods of h form a lattice which is the same as the lattice of E up to a constant multiple. This construction is illustrated in a paper by Roberts and Washington [17].

Different choices for an endomorphism e may produce different choices for h. In Chapter 3, we discuss the different choices for h and how these choices are related to each other. Let

$$H = \{h = af + bf' \,|a, b \in \mathbb{C} \text{ and the periods of } h \text{ form a lattice in } \mathbb{C}\}.$$

Identify two elements in H if they differ by a constant multiple. In Chapter 3, we show that H can be parameterized by $\mathbb{P}^1(\mathbb{Z})$. Each (u, v) pair in $\mathbb{P}^1(\mathbb{Z})$ gives a different map from $X_1(N)$ to some elliptic curve E. In addition, the map ϕ can be factored as follows:

$$\begin{array}{ccccc} X_1(N) & \xrightarrow{\psi_1} & A_f & \xrightarrow{\psi_2} & E \\ \tau & \mapsto & (\int_{\tau_0}^{\tau} f(z)dz, \int_{\tau_0}^{\tau} f'(z)dz) & \mapsto & \int_{\tau_0}^{\tau} h(z)dz. \end{array}$$

The image of ψ_1 is an algebraic curve and is independent of the choice of splitting of A_f. Let deg $\psi_1 = d$. Then using the algorithm for calculating the degree of ϕ, we obtain for a (u, v) pair:

$$\deg\, \phi(u, v) = d\, \frac{g(u, v)}{k(u, v)},$$

where $g(u, v)$ is a positive definite binary quadratic form and $k(u, v)$ is called the dependency constant. This form is well-defined modulo equivalence of binary quadratic forms of a fixed discriminant. The choice of a correspondence between $\mathbb{P}^1(\mathbb{Z})$ and H fixes a choice for g in its equivalence class. The quadratic form depends only on the two quadratic fields K and L and not on the level N. Given the two fields K and L and a correspondence between H and $\mathbb{P}^1(\mathbb{Z})$, We have found an algebraic way to determine the form g which appears in the degree. This technique is illustrated in Chapter 3. For each choice of (u, v) pair, the image of ϕ gives a different elliptic curve which are all isogenous and many are isomorphic. The constant $k(u, v)$ provides information about which curves are isomorphic. This work also shows that there are different strong Weil parametrizations of the same $\mathbb{Q}$-curve. This does not occur in the case of elliptic curves over $\mathbb{Q}$.

Based on my experimental computations, the integer d appears to be related to the intersection numbers of the abelian variety A_f, as described in papers by X. Wang [20] and H. Hida [11]. Experimental results also suggest that the integer d is closely related to the congruence primes for the cusp form f. This would extend a result of K. Ribet which states that the primes that divide the degree of a strong Weil parametrization of an elliptic curve over $\mathbb{Q}$ are exactly the congruence primes [23].

Not all $\mathbb{Q}$-curves over quadratic fields have modular parametrizations from $X_0(N)$. In order to obtain information about the degree of modular parametrizations of a $\mathbb{Q}$-curve, one must find an abelian variety A_f such that E is isogenous to A_f/eA_f for some endomorphism $e \in End(A_f)$. E. Pyle gives an example of a $\mathbb{Q}$-curve E defined over $\mathbb{Q}(\sqrt{-3})$ which is 2 isogenous to its Galois conjugate [14]. However, the isogeny cannot be defined over $\mathbb{Q}(\sqrt{-3})$ for any twist of E. If this curve is modular, the desired A_f is a four-dimensional abelian variety which is a factor of $J_1(N)$ and not $J_0(N)$. In addition, the coefficients of f will lie in $\mathbb{Q}(\sqrt{2}, \sqrt{-2})$. In general, if all of the Galois conjugates of f are quadratic twists of f, then we have shown that $End(A_f) \otimes \mathbb{Q}$ is isomorphic to the tensor product of two quaternion algebras. If $End(A_f) \otimes \mathbb{Q}$ is isomorphic to $M_4(\mathbb{Q})$, then by choosing a rank three matrix in $M_4(\mathbb{Q})$, one can obtain $e \in End(A_f)$ such that A_f/eA_f is an elliptic curve. From this endomorphism, the proper linear combination of f and its conjugates can be found which gives the map ϕ. In Chapter 4, we extend the results from Chapter 3, in order to obtain that the degree of modular parametrization is

$$d\,\frac{g(u,v,w,z)}{k(u,v,w,z)}$$

where g is quadratic form in 4 variables. Given information concerning the coefficients of f and the quadratic characters, one should be able to uniquely determine the quadratic form g in an analogous method to the one described in Chapter 3. Computational evidence of this is given in Chapter 4.

Given an arbitrary modular $\mathbb{Q}$-curve E, another goal is to determine the dimension of the smallest A_f such that E is a quotient of A_f. If the isogeny between E and its conjugate can be defined over $\mathbb{Q}(\sqrt{t})$ then A_f can be chosen to have dimension two. However, if it cannot be defined over $\mathbb{Q}(\sqrt{t})$ for any twist of E, then dim $A_f \geq 4$. In Chapter 4, a list of conditions is given which determine if there is an abelian variety A_f of dimension 4 or 8 which contains E as a simple factor. This problem is investigated using tools from Galois cohomology and the embedding problem of fields.

Chapter 1

Computational Tools

Let $\Gamma = SL_2(\mathbb{Z})$ and let G be a subgroup of Γ with finite index. We are primarily interested in the cases when $G = \Gamma_1(N)$ and $G = \Gamma_0(N)$. Let $\mathcal{H}^*$ denote union of the upper half plane with $\mathbb{Q}$ and the point ∞. Then G acts on $\mathcal{H}^*$ by linear fractional transformations. Let $X_G = G \backslash \mathcal{H}^*$ be the quotient space. Let $S_2(G)$ denote the set of weight 2 cusp forms for G. If $G = \Gamma_0(N)$, then we simply write $S_2(N)$.

1.1 Modular Symbols and Cusp Forms

In order to perform calculations on elements of $S_2(G)$, we will be using the elements of $H_1(X_G, \mathbb{Z})$, the first homology group of the curve X_G. Suppose that the genus of X_G is g. Then $H_1(X_G, \mathbb{Z})$ is a free abelian group on $2g$ generators. Let α and β be any two points in $\mathcal{H}^*$ such that $\beta = M(\alpha)$ for some $M \in G$. Then define the modular symbol $\{\alpha, \beta\}$ to be a path in $\mathcal{H}^*$ starting at α and ending at β. By projecting onto X_G, $\{\alpha, \beta\}$ becomes a closed path and gives a well-defined class in $H_1(X_G, \mathbb{Z})$. In addition, any element of $H_1(X_G, \mathbb{Z})$ can be expressed as a modular symbol. If $\gamma = \{\alpha, \beta\}$, then given an $f \in S_2(G)$, we define a period of

f by

$$\langle \gamma, f \rangle = \int_\gamma 2\pi i f(z) dz.$$

Thus, given the modular symbol $\{\alpha, \beta\}$, we have defined a $\mathbb{C}$-linear functional.

We can extend the definition of modular symbols from elements of $H_1(X_G, \mathbb{Z})$ to elements of $H_1(X_G, \mathbb{R})$. Now suppose that $\alpha, \beta \in \mathcal{H}^*$ are arbitrary points. Then we can interpret the symbol $\{\alpha, \beta\}$ as the $\mathbb{C}$-linear functional

$$f \mapsto \langle \{\alpha, \beta\}, f \rangle = \int_\alpha^\beta 2\pi i f(z) dz.$$

The $\mathbb{R}$-vector space $H_1(X_G, \mathbb{R}) \cong H_1(X_G, \mathbb{Z}) \otimes \mathbb{R}$ gives all of the $\mathbb{C}$-linear functionals on $S_2(G)$. Let $\{\gamma_1, \gamma_2, \ldots, \gamma_{2g}\}$ be a $\mathbb{Z}$-basis for $H_1(X_G, \mathbb{Z})$. Given $\gamma \in H_1(X_G, \mathbb{R})$, then γ can be written uniquely as a a sum of elements in $H_1(X_G, \mathbb{Z})$ with real coefficients as follows: $\gamma = \sum_{j=1}^{2g} a_j \gamma_j$. We obtain a $\mathbb{C}$-linear functional

$$f \mapsto \langle \gamma, f \rangle = \sum_{j=1}^{2g} a_j \langle \gamma_j, f \rangle.$$

Hence, we define the modular symbol $\{\alpha, \beta\}$ to be the element in $H_1(X_G, \mathbb{R})$ which is equal to the linear functional given by $f \mapsto \langle \{\alpha, \beta\}, f \rangle$.

We have an $\mathbb{R}$-bilinear pairing defined as follows:

$$\begin{aligned} S_2(G) \times H_1(X_G, \mathbb{R}) &\to \mathbb{C} \\ (f, \gamma) &\mapsto \langle \gamma, f \rangle. \end{aligned}$$

By regarding $S_2(G)$ as a real vector space, we have a duality between the space of cusp forms and the homology of the modular curve X_G. Using this duality is the driving force behind the algorithms presented. It allows us to work with elements of $H_1(X_G, \mathbb{Q})$ rather than the cusp forms themselves. Since the elements of $H_1(X_G, \mathbb{Q})$ will be given algebraically, this will make the computation better suited for computer implementation.

1.2 Modular Symbol and M-symbol Properties

The following Lemma lists basic properties satisfied by the modular symbols. The proofs are given in [5].

Lemma 1. *Let α, β, and $\gamma \in \mathcal{H}^*$ and let $M \in G$. Then the following are true:*

1. $\{\alpha, \alpha\} = 0$
2. $\{\alpha, \beta\} + \{\beta, \alpha\} = 0$
3. $\{\alpha, \beta\} + \{\beta, \gamma\} + \{\gamma, \alpha\} = 0$
4. $\{M\alpha, M\beta\} = \{\alpha, \beta\}$
5. $\{\alpha, M\alpha\} = \{\beta, M\beta\}$
6. $\{\alpha, M\alpha\} \in H_1(X_G, \mathbb{Z})$.

For computational purposes, we will restrict our attention to $G = \Gamma_0(N)$ for the remainder of the chapter. Rather than working with modular symbols directly, we will define the M-symbols which are an effective tool for performing computations on the homology of $X_0(N)$.

An M-symbol (for $G = \Gamma_0(N)$) is simply a point in $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$. Two matrices $\begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix} \in SL_2(\mathbb{Z})$ for $i = 1, 2$ are in the same right coset with respect to $\Gamma_0(N)$ if and only if $(c_1 : d_1) = (c_2 : d_2)$ in $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$. Therefore, we have a correspondence

$$\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z}) \leftrightarrow [\Gamma : \Gamma_0(N)] \leftrightarrow \{\{M(0), M(\infty)\} \,|M \in [\Gamma : \Gamma_0(N)]\}$$

which is given by

$$(c:d) \leftrightarrow M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \leftrightarrow \{M(0), M(\infty)\} = \{b/d, a/c\}$$

where a and b are chosen so that $ad - bc = 1$.

We need to be able to convert from modular symbols to M-symbols and vice versa. The conversion from an M-symbol to a modular symbol is given by

$$(c:d) \mapsto \{b/d, a/c\}$$

where a and b are chosen so that $ad - bc = 1$. To convert from modular symbols to M-symbols, we will not necessarily get an M-symbol, but instead a sum of M-symbols. This is because every modular symbol is a rational sum of symbols of the form $\{M(0), M(\infty)\}$ for some $M \in \Gamma_0(N)$. The conversion is done using continued fractions. Write $\{\alpha, \beta\}$ as $\{0, \beta\} - \{0, \alpha\}$. Thus we only need to show how to convert a modular symbol of the form $\{0, \beta\}$. Let

$$\frac{p_{-2}}{q_{-2}} = \frac{0}{1}, \frac{p_{-1}}{q_{-1}} = \frac{1}{0}, \frac{p_0}{q_0}, \frac{p_1}{q_1}, \frac{p_2}{q_2}, \ldots \frac{p_k}{q_k} = \beta$$

denote the continued fraction convergents of β. Then

$$M_j = \begin{pmatrix} (-1)^{j-1}p_j & p_{j-1} \\ (-1)^{j-1}q_j & q_{j-1} \end{pmatrix}$$

is in Γ. Thus

$$\{0, \beta\} = \sum_{j=-1}^{k} \{\frac{p_{j-1}}{q_{j-1}}, \frac{p_j}{q_j}\} = \sum_{j=-1}^{k} \{M_j(0), M_j(\infty)\} = \sum_{j=-1}^{k} ((-1)^{j-1}q_j : q_{j-1}).$$

1.3 Computing Homology of Modular Curves

Using modular symbols and M-symbols, we will determine how to compute the degree of modular parametrization and other quantities of interest. These algorithms are useful for calculating the homology of modular curves, computing Fourier coefficients of cusp forms, approximating periods of cusp forms, and computing the degree of modular parametrization. In the following, the techniques for performing various computations are outlined. For a more in depth treatment, one should refer to Manin [13] and Cremona [5].

The following is a basic outline of the steps for computing a basis for the homology of the modular curve $X_0(N)$.

Steps for Computing Homology of $X_0(N)$:

1. Make a list of all inequivalent M-symbols for the level N.

2. Given $(c : d)$, one needs to determine the class to which it belongs. Construct a look up table which can be used throughout the algorithm.

3. Factor out the two-term relations

$$(c : d) + (-d : c) = 0.$$

4. Factor out the three-term relations

$$(c : d) + (c + d : -c) + (d : -c - d) = 0.$$

5. Gather a list of remaining generators.

6. Let $[x]$ denote the class of the cusp x. Determine the kernel of the boundary map

$$\delta((c : d)) = [a/c] - [b/d]$$

from the remaining generators. The values a and d are chosen such that $ad - bc = 1$.

7. The kernel gives a $\mathbb{Q}$-basis for $H_1(X_0(N), \mathbb{Q})$.

The space $H_1(X_0(N), \mathbb{Q})$ can be split into the direct sum of two spaces each of dimension g. For $z \in \mathcal{H}^*$, let $z^* = -\overline{z}$. Then this action on $\mathcal{H}^*$ induces an action on $H_1(X_0(N), \mathbb{Q})$. The matrix for the action of $(*)$ has eigenvalues $+1$ and -1 each with multiplicity g. So let $H^+(X_0(N), \mathbb{Q})$ denote the $+1$ eigenspace of the action, and let $H^-(X_0(N), \mathbb{Q})$ denote the -1 eigenspace of the action. Then $H_1(X_0(N), \mathbb{Q}) \cong H^+(X_0(N), \mathbb{Q}) \oplus H^-(X_0(N), \mathbb{Q})$. Working in the smaller space is helpful for computing Fourier coefficients of cusp forms. However, we will not go into detail concerning this since the general degree calculation for $\mathbb{Q}$-curves over quadratic fields will not permit us to use this decomposition. The algorithm as discussed later requires that we work in the full homology space.

1.4 Hecke Operators

For each prime p not dividing N, we can define the action of the Hecke operator T_p on the modular symbol $\{\alpha, \beta\}$.

$$T_p : \{\alpha, \beta\} \to \{p\alpha, p\beta\} + \sum_{r=0}^{p-1} \{\frac{\alpha + r}{p}, \frac{\beta + r}{p}\}.$$

This action is defined so that it is compatible with the action of the Hecke operator T_p which acts on the space of cusp forms. That is,

$$\langle T_p\{\alpha, \beta\}, f\rangle = \langle \{\alpha, \beta\}, T_p f\rangle.$$

In order to perform the computations that follow, it is necessary to compute the action of T_p on $H_1(X_0(N), \mathbb{Q})$. First, apply the Hecke operator to each basis element of $H_1(X_0(N), \mathbb{Q})$. Each basis element is represented as a sum of M-symbols. In order to apply the Hecke operator to an M-symbol, the M-symbol can be converted to a modular symbol. The Hecke action can be applied to obtain a sum of modular symbols. Then each modular symbol can be expressed as a sum of M-symbols. Performing the conversions every time is a very time consuming calculation. Cremona outlines another way to apply the Hecke operator directly to the M-symbols without doing the conversions between the different symbols. This method uses Heilbronn matrices and provides a considerable computational improvement when computing the Hecke action on the homology of the modular curve. The algorithm is clearly given in Cremona's text [5]. After T_p has been applied to each basis element, the matrix T_p with respect to our basis for $H_1(X_0(N), \mathbb{Q})$ can be constructed.

If $f = \sum_{n=1}^{\infty} a_n q^n$ is an eigenform in $S_2(N)$, then $T_p f = a_p f$ for all primes p which do not divide N. There is a corresponding two-dimensional subspace of $H_1(X_0(N), \mathbb{C})$ which are eigenvectors for all T_p. If all of the coefficients of f lie in $\mathbb{Q}$, then the two-dimensional subspace can be found by computing the action of T_p on $H_1(X_0(N), \mathbb{Q})$ for a few primes p, where $p \nmid N$. Suppose $f = \sum_{j=1}^{\infty} a_n q^n \in S_2(N)$ is an eigenform and the corresponding eigenspace in homology is spanned by $V = \langle v_1, v_2 \rangle$. Suppose $g = \sum_{j=1}^{\infty} b_n q^n \in S_2(N)$ is a different eigenform and its corresponding eigenspace in homology is spanned by $U = \langle u_1, u_2 \rangle$. Let p be a prime not dividing N such that $a_p \neq b_p$ and let $u \in U$. Then

$$\langle u, T_p f \rangle = \langle u, a_p f \rangle = a_p \langle u, f \rangle$$

which is also equal to

$$\langle T_p u, f \rangle = \langle b_p u, f \rangle = b_p \langle u, f \rangle.$$

Since $a_p \neq b_p$, we must have that $\langle u, f \rangle = 0$. Suppose that $v_1, v_2, \ldots, v_{2g}$ form a basis of $H_1(X_0(N), \mathbb{Q})$ such that each v_i is an eigenvector for all the Hecke operators. For simplicity, assume that f has coefficients lying in $\mathbb{Q}$. If f corresponds to $\langle v_1, v_2\rangle$, then for any $\gamma \in H_1(X_0(N), \mathbb{Z})$

$$\gamma = \sum_{j=1}^{2g} c_i v_i$$

for some $c_i \in \mathbb{Z}$. Hence,

$$\langle \gamma, f\rangle = c_1\langle v_1, f\rangle + c_2\langle v_2, f\rangle.$$

Given any $\gamma \in H_1(X_0(N), \mathbb{Z})$, it is crucial to know how to determine the value of the coefficients c_i in the above equation. We will be fairly explicit in this part of the computation because it is a key operation in the remaining algorithms. The vector $\gamma \in H_1(X_0(N), \mathbb{Z})$ is represented by a column vector with $2g$ integer entries. Suppose we want to find the projection of γ onto the eigenspace v_1. Then it is necessary to find a dual basis to $\{v_1, v_2, \ldots, v_{2g}\}$. We will represent the dual basis as $\{w_1, w_2, \ldots, w_{2g}\} \subset \mathbb{Q}^{2g}$, such that

$$v_i \cdot w_j = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j. \end{cases}$$

Since $\{v_1, v_2\}$ generate a common eigenspace for all the Hecke operators T_p, then we can determine the span of $\{w_1, w_2\}$ by computing the common eigenspaces for the action of T_p^t. Suppose that this space is spanned by $\{w_1', w_2'\}$. Then one can can determine the linear combination of w_1' and w_2' which will give the correct values of the dot products above. The vectors w_1 and w_2 are elements of $\mathbb{Q}^{2g}$.

Suppose that $f = \sum_{j=1}^{\infty} a_n q^n$ is an eigenform with coefficients in $\mathbb{Q}$. We now outline the steps for determining the vectors $\{v_1, v_2\} \in \mathbb{Z}^{2g}$ and $\{w_1, w_2\} \in \mathbb{Q}^{2g}$ which correspond to f. In the following, V and W are subspaces of $H_1(X_0(N), \mathbb{Q})$. Both V and W are represented as $2g \times k$ matrices where k is the dimension of the subspace. The columns of the matrices V and W span the spaces V and W respectively.

1. Set $V := W :=$ $2g \times 2g$ identity matrix. The i-th column represents γ_i, the i-th basis element of $H_1(X_0(N), \mathbb{Q})$. Let p be the smallest prime that does not divide N.

2. Compute the matrix of T_p with respect to the basis given by the columns of V.

3. Set $V := (a_p$ eigenspace of $T_p) \cap V$.

4. Set $W := (a_p$ eigenspace of $T_p^t) \cap W$.

5. If the dimension of $V > 2$, set $p =$ next largest prime that does not divide N. Return to Step 2.

6. Let d be the smallest integer such that d times the i-th column of V represents an element of $H_1(X_0(N), \mathbb{Z})$. Set $V := d \cdot V$.

7. Let V^t denote the matrix obtained by placing the i-th basis element in each column of V in the i-th row for each i. Set $M := (W * V^t)^{-1}$.

8. Set $W := M * W$.

9. The columns of V are v_1 and v_2. The rows of W are w_1 and w_2.

1.5 Approximating Periods of Cusp Forms

In order to conduct several numerical experiments, it is important to have a method for approximating periods of cusp forms. In order to have an accurate computation, one needs to compute a large number of Fourier coefficients.

Cremona explains an effective method for computing the p-th coefficient of an eigenform f for p a prime not dividing N. His method relies on using the one dimensional eigenspace in $H^+(X_0(N), \mathbb{Z})$ which corresponds to the cusp form f. Then a large number of Fourier coefficients can be computed in an effective manner [5].

Cremona has proved the following two theorems in [5] which are helpful for approximating the periods. Let $f \in S_2(N)$ be fixed. Suppose $M \in \Gamma_0(N)$ and $\alpha \in \mathbb{Q}$. Then define $\omega(M) = \langle\{\alpha, M(\alpha)\}, f\rangle$. Note that $\omega(M)$ is independent of the choice of α.

Theorem 1. *Let* $f \in S_2(N)$ *and let* $M = \begin{pmatrix} a & b \\ cN & d \end{pmatrix} \in \Gamma_0(N)$ *with* $c > 0$. *Then*

$$\begin{aligned}\omega(M) &= \langle\{\alpha, M\alpha\}, f\rangle \\ &= \sum_{n=1}^{\infty} \frac{a_n}{n} e^{-2\pi n/cN}(e^{2\pi ina/cN} - e^{-2\pi ind/cN}).\end{aligned}$$

Let W denote the Fricke involution on $S_2(N)$. This action comes from the transformation $z \mapsto -\frac{1}{Nz}$. This acts on both $S_2(N)$ and $H_1(X_0(N), \mathbb{Q})$. Also, the common eigenspaces for the action of the Hecke operators are also eigenspaces for the action of W.

Theorem 2. *Let* $M = \begin{pmatrix} a & b \\ cN & d \end{pmatrix} \in \Gamma_0(N)$ *with* $d > 0$. *Let* $f \in S_2(N)$ *and suppose* $W(f) = \epsilon f$ *where* $\epsilon = \pm 1$. *Then*

$$\begin{aligned}\omega(M) &= \langle\{\alpha, M\alpha\}, f\rangle \\ &= \sum_{n=1}^{\infty} \frac{a_n}{n}((\epsilon - 1)e^{-2\pi n/\sqrt{N}} + e^{-2\pi n/d\sqrt{N}}(e^{2\pi ib/d} - \epsilon e^{2\pi ic/d}).\end{aligned}$$

It is ideal to be able to compute good approximations with as few Fourier coefficients as possible. Computing the p-th coefficient of an eigenform has a running time on the order of $O(p)$. If the series converges more quickly, then fewer coefficients are needed. In the first theorem, the convergence depends on the size of cN and in the second, it depends on the size of $d\sqrt{N}$. In most cases, the second of the two theorems will converge more rapidly. In order to improve the convergence, we investigate ways to write the period as a sum of periods which converge at a faster rate. This is done by reducing the c value in the first theorem and the d value in the second theorem.

Let $\gamma = \begin{pmatrix} a & b \\ cN & d \end{pmatrix} \in \Gamma_0(N)$. Let $c(\gamma)$ denote the value of c in the matrix γ. Similarly, let $d(\gamma)$ denote d. In order to compute $\omega(\gamma)$, the goal is to change the path $\{0, \gamma(0)\}$ into a sum of paths of the form $\{0, \gamma_i(0)\}$ for some $\gamma_i \in \Gamma_0(N)$ such that $|c(\gamma_i)| < |c(\gamma)|$ or $|d(\gamma_i)| < |d(\gamma)|$. Let $\tau \in \Gamma_0(N)$ and let $\tau(0) = \alpha$. Then using modular symbol properties, we obtain

$$\begin{aligned} \{0, \gamma(0)\} &= \{\alpha, \gamma(\alpha)\} \\ &= \{\alpha, 0\} + \{0, \gamma(\tau(0))\} \\ &= \{0, \gamma\tau(0)\} - \{0, \tau(0)\}. \end{aligned}$$

On the other hand,

$$\begin{aligned} \{0, \gamma(0)\} &= \{\tau(0), \tau(\gamma(0))\} \\ &= \{\tau(0), 0\} + \{0, \tau\gamma(0)\} \\ &= \{0, \tau\gamma(0)\} - \{0, \tau(0)\}. \end{aligned}$$

Hence we would like to find a matrix τ such that $|c(\tau)| < |c(\gamma)|$ and either $|c(\gamma\tau)| < |c(\gamma)|$ or $|c(\tau\gamma)| < |c(\gamma)|$. Then the process can be iterated so that the c values can be made as small as possible. In order to decrease the d value, we simply replace the c in these conditions with a d.

First we will concentrate on reducing the value of c. Let

$$\gamma = \begin{pmatrix} a_0 & b_0 \\ c_0 N & d_0 \end{pmatrix} \qquad \text{and} \qquad \tau = \begin{pmatrix} a_1 & b_1 \\ c_1 N & d_1 \end{pmatrix}.$$

Then $c(\gamma\tau) = a_1 c_0 + c_1 d_0$. Hence, our goal is to find a matrix τ that simultaneously minimizes $a_1 c_0 + c_1 d_0$ and c_1. Since $(c_0, d_0) = 1$, we can find values of a_1 and c_1 such that $a_1 c_0 + c_1 d_0 = 1$. Choose $c_1 \equiv d_0^{-1} \pmod{c_0}$ with $0 < c_1 < c_0$. Then $a_1 = (1 - c_1 d_0)/c_0$. In order to insure that $\tau \in \Gamma_0(N)$, we must have $\det \tau = 1$. Hence, we need to solve for the variables b_1 and d_1 in the equation, $a_1 d_1 - b_1 c_1 N = 1$. However, there is no guarantee that $(a_1, N) = 1$. If $(a_1, N) > 1$, we may choose $c_1' = c_1 - c_0$ and $a_1' = a_1 + d_0$. Notice that $a_1' c_0 + c_1' d_0 = 1$ and $0 > c_1' > c_0$. Hence, we can also test $a_1' = a_1 + d_0$ to determine if $(a_1', N) = 1$. If the greatest common divisor is greater than 1, we will have to do some more work. Suppose that N is a power of a prime. Then at least one of a_1 or a_1' will have to be relatively prime to N since d_0 is relatively prime to N. Therefore, we are guaranteed a solution for the matrix τ. Thus by iterating this process, our original path can be written as a sum of paths of the form $\{0, \gamma_i(0)\}$ with $c(\gamma_i) = 1$.

If both a and a' have a common factor with N, we can attempt a similar calculation with $\tau\gamma$ rather than $\gamma\tau$. This time we would like find a matrix τ which minimizes c_1 and $a_0 c_1 + c_0 d_1$. Since $(a_0, c_0) = 1$, we can choose $c_1 \equiv a_0^{-1} \pmod{c_0}$ with $0 < c_1 < c_0$. Then set $d_1 = (1 - a_0 c_1)/c_0$, provided that $(d_1, N) = 1$. Then we can find solutions for a_1 and b_1 to $a_1 d_1 - b_1 c_1 N = 1$. If $(d_1, N) > 1$, then we make adjustments as before, by setting $d_1' = d_1 + a_0$ and $c_1' = c_1 - c_0$. If $(d_1', N) = 1$, we can once again solve for τ. If $(d_1', N) > 1$ at this stage, then there is no matrix τ such that $|c(\gamma\tau)| = 1$ or $|c(\tau\gamma)| = 1$. If this occurs, other methods can be used to reduce the c values. If all the c values cannot be reduced to 1, in most cases it will be better to use the second theorem in order to approximate the period. We now give the algorithm for computing an approximation to the period using this method. In the algorithm, computing $\omega(M)$ is done by using Theorem 1. We assume that $c(M) > 0$, since $\omega(M) = \omega(-M)$.

Function = Approximate period (Using Theorem 1)

Input = $M := \gamma \in \Gamma_0(N)$

Output = Return period and CMax

Period := 0; sign := 1; done := 0

IF ($c(M) = 1$) Period := Compute $\omega(M)$ by formula

WHILE (done = 0)

$c_1 := (d_0^{-1}) \pmod{c_0}$

$a_1 := (1 - c_1 d_0)/c_0$

IF ($(a_1, N) > 1$)

$c_1 := c_1 - c_0; a_1 := a_1 + d_0$

IF ($(a_1, N) = 1$)

Construct τ by finding a solution for b_1 and d_1 in $a_1 d_1 - b_1 c_1 N = 1$

$A := M\tau$

Period := Period + sign $\cdot \omega(A)$

$M := \tau$; sign := sign $\cdot - 1$

ELSE

$c_1 := (a_0^{-1}) \pmod{c_0}$

$d_1 := (1 - c_1 a_0)/c_0$

IF ($(d_1, N) > 1$)

$c_1 := c_1 - c_0; d_1 := d_1 + a_0$

IF $((d_1, N) = 1)$

Construct τ by finding a solution for a_1 and b_1 in $a_1 d_1 - b_1 c_1 N = 1$

$A := \tau M$

Period := Period + sign $\cdot \omega(A)$

$M := \tau$; sign := sign $\cdot - 1$

ELSE

Period := Period + sign $\cdot \omega(M)$

done := 1; CMax := c(M)

Now we will discuss how to use the second theorem in order to approximate the period of a cusp form. This will be done by reducing the d-value of our matrices. We will assume that $d_0 > 0$. Note that $d(\gamma\tau) = c_0 b_1 N + d_0 d_1$ and $d(\tau\gamma) = b_0 c_1 N + d_0 d_1$. Working with $\gamma\tau$ we see that we need

$$-d_0 < c_0 b_1 N + d_0 d_1 < d_0$$
$$-d_0(d_1 + 1) < c_0 b_1 N < -d_0(d_1 - 1)$$
$$\frac{-d_0(d_1 + 1)}{c_0 N} < b_1 < \frac{-d_0(d_1 - 1)}{c_0 N}.$$

if $c_0 > 0$. If $c_0 < 0$, simply reverse the inequality signs. On the other hand, we could work with the matrix $\tau\gamma$. Then we would need

$$-d_0 < b_0 c_1 N + d_0 d_1 < d_0$$
$$-d_0(d_1 + 1) < b_0 c_1 N < -d_0(d_1 - 1)$$
$$\frac{-d_0(d_1 + 1)}{b_0 N} < c_1 < \frac{-d_0(d_1 - 1)}{b_0 N}.$$

if $b_0 > 0$. If $b_0 < 0$, reverse the direction of the inequality signs.

Using these inequalities, we search for either an integer b_1 which satisfies the first equation or an integer c_1 which satisfies the second equation with d_1 as small as possible and $(d_1, b_1c_1N) = 1$. This leads to the following recursive algorithm for computing an approximation to the period.

Function = Approximate period (Using Theorem 2)

Input = $M := \gamma \in \Gamma_0(N)$, DMax := 1, Period := 0

Output = Return Updated period and modify DMax

Reduce d value(M)

IF (two matrices M_1 and M_2 were returned in this function)

Period := Period + Approximate Period(M_1, DMax, Period)

Period := Period - Approximate Period(M_2, DMax, Period)

ELSE

Period := Period + Compute Period by the formula

IF DMax < $d(M_1)$

DMax := $d(M_1)$

RETURN Period

Function = Reduce d value

Input = Enter a matrix in $\Gamma_0(N)$.

Output = Either 1 or 2 matrices M_1 and M_2 with smaller d values

Initialize $d_1 := 1$.

IF $(c_0 > 0)$ $(*)$

$bot := \lceil \frac{-d_0(d_1+1)}{c_0N} \rceil$; $top := \lfloor \frac{-d_0(d_1-1)}{c_0N} \rfloor$

ELSE

$top := \lfloor \frac{-d_0(d_1+1)}{c_0N} \rfloor$; $bot := \lceil \frac{-d_0(d_1+1)}{c_0N} \rceil$

IF (top<bot)

IF $(b_0 > 0)$ $(**)$

$bot := \lceil \frac{-d_0(d_1+1)}{b_0 N} \rceil$; $top := \lfloor \frac{-d_0(d_1-1)}{b_0 N} \rfloor$

ELSE

$top := \lfloor \frac{-d_0(d_1+1)}{b_0 N} \rfloor$; $bot := \lceil \frac{-d_0(d_1+1)}{b_0 N} \rceil$

IF (top<bot)

WHILE $((d_1, N) > 1)$ $d_1 := d_1 + 1$ $(***)$

IF $(d_1 > d_0)$ RETURN M

ELSE Go back to line $(*)$

ELSE

FOR($c_1 =$ bot to top)

IF $((c_1, d_1) = 1)$

Find τ by solving for a_1 and b_1 in $a_1 d_1 - b_1 c_1 N = 1$

Compute $\gamma\tau$; RETURN $M_1 = \tau\gamma$ and $M_2 = \tau$

Go back to line (***)

FOR($b_1 =$ bot to top)

IF $((b_1, d_1) = 1)$

Find τ by solving for a_1 and c_1 in $a_1 d_1 - b_1 c_1 N = 1$

Compute $\gamma\tau$; RETURN $M_1 = \gamma\tau$ and $M_2 = \tau$

Go back to line $(**)$

1.6 Examples of $\mathbb{Q}$-curves

A $\mathbb{Q}$-curve is an elliptic curve defined over a number field which is isogenous to each of its Galois conjugates. Throughout the discussion, we will be focusing on $\mathbb{Q}$-curves which are defined over a quadratic field and are without complex multiplication. Roberts has given a list of $\mathbb{Q}$-curves defined over a quadratic field which are either 2-isogenous or 3-isogenous to their Galois conjugates [16]. These lists are used to produce a number of examples.

Theorem 3. *Suppose $K = \mathbb{Q}(\sqrt{t})$ and E/K is a $\mathbb{Q}$-curve which is 2-isogenous to its Galois conjugate. Then E has an equation of the form*

$$y^2 = x^3 - 12Dx^2 + 18(1 - mt\sqrt{t})D^2x$$

where $D \in K^\times$ and $m \in \mathbb{Q}^\times$. The isogeny is defined over K if and only if the norm of D is $-2a^2$ for some $a \in K^\times$.

Theorem 4. *Suppose $K = \mathbb{Q}(\sqrt{t})$ and E/K is a $\mathbb{Q}$-curve which is 3-isogenous to its Galois conjugate. Then E has an equation of the form*

$$y^2 = x^3 - \frac{15m^2\sqrt{t} - 6m}{\sqrt{t}}D^2x - \frac{22m^3t - 14m^2\sqrt{t} + m}{t}D^3$$

where $D \in K^\times$ and $m \in \mathbb{Q}^\times$. The isogeny is defined over K if and only if the norm of D is $-3a^2$ for some $a \in K^\times$.

Chapter 2

Computing the Degree of Modular Parametrization

2.1 Elliptic Curves over $\mathbb{Q}$

After building a number of computational tools, the next step is to use these tools to calculate the degree of modular parametrization. Cremona has developed an algorithm which computes the degree of modular parametrization of an elliptic curve over $\mathbb{Q}$. However, the formula developed by Cremona is no longer usable when trying to compute the degree for $\mathbb{Q}$-curves over quadratic fields. In order to understand how to conduct the computation in the latter case, it is necessary to understand Cremona's method of calculation for elliptic curves over $\mathbb{Q}$.

Suppose there exists a map ϕ from $X_0(N)$ to the elliptic curve E given by

$$\phi(\tau) = \int_{\tau_0}^{\tau} f(z)dz$$

where τ_0 is a fixed point in the upper half plane and f is a weight two cusp form of level N. In this case, the elliptic curve E is said to have a strong Weil parametrization. Every modular parametrization of an elliptic curve is obtained by a strong Weil map followed by an isogeny. We will use the notation that

$\phi(\tau) = \langle\{\tau, \tau_0\}, f\rangle$ but omit the scaling factor of $2\pi i$ when we write down our integrals. This will not cause a problem since we will be looking at cusp forms which are defined up to a constant multiple. Suppose ω_1 and ω_2 form a basis for the period lattice of f. Then for any $\gamma \in \Gamma_0(N)$,

$$\omega(\gamma) = \int_0^{\gamma(0)} f(z)dz = n_1(\gamma)\omega_1 + n_2(\gamma)\omega_2$$

where n_i is an integer valued function of γ for $i = 1, 2$. In fact, n_i defines a homomorphism from $\Gamma_0(N)$ to $\mathbb{Z}$.

Define the Petersson norm of a cusp form f for $\Gamma_0(N)$ by

$$\|f\|^2 = \int_X f(\tau)^2 dudv$$

where $\tau = u + iv$, and X is a fundamental domain for the action of $\Gamma_0(N)$. The following is a result of D. Zagier used by Cremona to develop his algorithm. The proof is given in [23].

Theorem 5. *Let ϕ be a strong Weil parametrization of the elliptic curve E as given above. Then*

$$4\pi^2\|f\|^2 = \textit{deg } (\phi) \ \textit{Vol } E.$$

Let

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \qquad \text{and} \qquad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Then S and T generate $SL_2(\mathbb{Z})$. Let Ω be a complete list of right coset representatives for $\Gamma_0(N)$ in $SL_2(\mathbb{Z})$ chosen such that if $\gamma \in \Omega$, then $\gamma TS \in \Omega$. This is possible since all of the conjugates of TS are not in $\Gamma_0(N)$. The matrix TS has order 3 in $PSL_2(\mathbb{Z})$. Choosing a set of coset representatives specifies a non-standard but useful fundamental domain for the action of G. For more information on this formulation see [4]. The matrix T acts on the right cosets. If $\gamma \in \Omega$, then set

$$\gamma T = t(\gamma)\tau(\gamma)$$

where $t : \Omega \to \Gamma_0(N)$ is a function and $\tau : \Omega \to \Omega$ is a permutation of the coset representatives. The function t shows how the various edges of the fundamental domain match up with each other. The permutation τ breaks the set Ω into a number of orbits, which are in one-to-one correspondence with the distinct cusps of $X_0(N)$. The length of an orbit is equal to the width of the corresponding cusp. By choosing a base point in each orbit, it is possible to place a partial ordering on Ω. Define $\gamma < \gamma'$ if

- γ and γ' are in the same orbit with base point γ_1, and
- $\gamma = \tau^j(\gamma_1), \gamma' = \tau^k(\gamma_1)$ with $0 < j, k < |\text{orbit}|$ implies that $j < k$.

Cremona uses the following theorem along with Zagier's theorem to determine a useful formula for calculating the degree [4].

Theorem 6. *Let ϕ be a strong Weil parametrization of the elliptic curve E as given previously. Then*

$$||f||^2 = \frac{1}{8\pi^2} \sum_{\gamma < \gamma'} Im(\omega(t(\gamma))\overline{\omega(t(\gamma'))})$$

where the sum means the following. The sum is taken over all γ and γ' such that γ and γ' are in the same orbit. Then one sums over all of the orbits of Ω.

Theorem 7. *Let ϕ be a strong Weil parametrization of the elliptic curve E as given previously. Let $\{\omega_1, \omega_2\}$ be a basis for the period lattice of h. If $Im\ (\frac{\omega_2}{\omega_1}) > 0$,* *then*

$$deg\ (\phi) = \frac{1}{2} \sum_{\gamma < \gamma'} det \begin{pmatrix} n_1(t(\gamma)) & n_1(t(\gamma')) \\ n_2(t(\gamma)) & n_2(t(\gamma')) \end{pmatrix}$$

where the sum is the same as in the previous theorem.

Cremona proves this formula for the degree of a modular parametrization from X_G where G is a congruence subgroup of $SL_2(\mathbb{Z})$. When the index of G grows too large, the algorithm will become ineffective. For computational purposes, we will restrict our attention to $G = \Gamma_0(N)$ for the remainder of this chapter as well as the next.

If Im $(\frac{\omega_2}{\omega_1}) < 0$, then one can simply reverse the order of ω_1 and ω_2 to use the formula. Suppose that Λ is a lattice with a basis ω_1 and ω_2. Then

$$\text{Vol } \Lambda = |\text{Im}(\overline{\omega_1}\omega_2)|.$$

If ω and ω' are in Λ such that $\omega = n_1(\omega)\omega_1 + n_2(\omega)\omega_2$ and $\omega' = n_1(\omega')\omega_1 + n_2(\omega')\omega_2$ then up to sign

$$\text{Im}(\overline{\omega}\omega') = \text{Vol } \Lambda \cdot \begin{vmatrix} n_1(\omega) & n_1(\omega') \\ n_2(\omega) & n_2(\omega') \end{vmatrix}.$$

A direct calculation shows that exact equality is obtained if $\text{Im}(\frac{\omega_2}{\omega_1}) > 0$.

Suppose there are two elliptic curves which have strong Weil parametrizations from $X_0(N)$. When comparing the degree calculation in these two cases, it is important to note that the summation is taken over the exact same orbits of Ω and the values of the function t do not change. The only difference in the calculation is the values of n_i which depend on the function f in the parametrization. Cremona's algorithm demonstrates how one can determine the values of n_i for a particular basis of the period lattice when the elliptic curve is defined over $\mathbb{Q}$. Cremona gives a detailed account of each of these steps in the computation for an elliptic curve over $\mathbb{Q}$ with conductor 11 [4].

2.2 Splitting Abelian Varieties

In order to compute the degree of modular parametrization of a $\mathbb{Q}$-curve defined over a quadratic field, it is necessary to have some information about the cusp form f appearing in the strong Weil parametrization. In order to determine this cusp form, it is necessary to discuss certain abelian varieties and how they can be decomposed into the products of $\mathbb{Q}$-curves. Let $f = \sum a_n q^n$ be a weight 2 eigenform for $\Gamma_1(N)$. Set $L = \mathbb{Q}(a_1, a_2, a_3, \dots)$. By a construction of G. Shimura in [19], an abelian variety A_f is obtained such that $\dim A_f = [L : \mathbb{Q}]$. Let $f_1 = f, f_2, f_3, \dots, f_n$ denote all of the Galois conjugates of f. Then analytically A_f is isomorphic to

$$\mathbb{C}^n / \left\{ \left(\int_\gamma f_1, \int_\gamma f_2, \dots, \int_\gamma f_n\right) \mid \gamma \in H_1(X_1(N), \mathbb{Z}) \right\}.$$

Let f be an eigenform with $L = \mathbb{Q}(\sqrt{r})$. Let f' denote the Galois conjugate of f. Hence, A_f is a two-dimensional abelian variety which is simple over $\mathbb{Q}$. The cases of interest are when A_f is isogenous to a product of two elliptic curves over $\overline{\mathbb{Q}}$.

The endomorphisms of A_f provide information about the decomposition of the abelian variety into its simple components. Let $End_{\mathbb{Q}}(A_f)$ denote the endomorphisms of A_f which are defined over $\mathbb{Q}$, and let $End(A_f)$ denote all of the endomorphisms of A_f which are defined over $\overline{\mathbb{Q}}$. Suppose there is a prime p such that $a_p = \sqrt{r}$. Then the Hecke operator T_p induces an endomorphism of A_f

which is defined over $\mathbb{Q}$. Also, $End_{\mathbb{Q}}(A_f) \otimes \mathbb{Q} \cong \mathbb{Q}(\sqrt{r})$. Suppose that $f' = f \otimes \chi$ where χ is a quadratic character associated to the field $K = \mathbb{Q}(\sqrt{t'})$. The form f is said to have an extra twist. If f is a normalized eigenform with an extra twist, then each Fourier coefficient of f is either an integer or the square root of an integer. It should be noted that all $\mathbb{Q}$-curves over quadratic fields which have modular parametrizations from $X_0(N)$ are obtained by decomposing an abelian variety A_f where f is an eigenform with an extra twist. The presence of this extra twist gives rise to an endomorphism η which is not defined over $\mathbb{Q}$ but is defined over a quadratic extension of $\mathbb{Q}$. The full endomorphism algebra of A_f is larger than in the general case because f has an extra twist. Set $t =$ disc (K). The endomorphism η acts on the space of cusp forms by mapping

$$f(z) \mapsto \sum_{k=1}^{|t|-1} \chi(k) f\left(z + \frac{k}{t}\right) = g(\chi) \sum_{k=1}^{|t|-1} \chi(k) f(z)$$

where $g(\chi)$ denotes the Gauss sum. This maps the space of cusp forms for $\Gamma_0(N)$ into itself and the span of f and f' into itself. In addition, η satisfies the following properties.

1. $\eta^2 = g(\chi)^2 = t$
2. $T_p \eta = \chi(p) \eta T_p$ for all $p \nmid N$ where p is a prime
3. $\eta f = g(\chi) f'$ and $\eta f' = g(\chi) f$
4. $\eta^\sigma = -\eta$ where σ is the non-trivial automorphism of $\mathbb{Q}(\sqrt{t})$.

These properties of η are proved in [17]. In the case when $t' \equiv 1 \pmod 4$, $t = t'$, then $\eta^2 = t$, and when $t' \equiv 2, 3 \pmod 4$, $t = 4t'$. Also, $End(A_f) \otimes \mathbb{Q}$ is generated by $1, T_p, \eta$, and $T_p\eta$. Hence, $End(A_f) \otimes \mathbb{Q}$ is isomorphic to the quaternion algebra $\left(\frac{r,t}{\mathbb{Q}}\right)$. Suppose the quaternion algebra is a division algebra, and A_f is isogenous to $E_1 \times E_2$ where E_1 and E_2 are non-CM elliptic curves. Since $End(E_1 \times E_2)$ clearly has zero divisors, we get a contradiction. Hence, A_f cannot be split into the product of two elliptic curves.

If the quaternion algebra is isomorphic to $M_2(\mathbb{Q})$, then A_f can be split. Let $\psi : End(A_f) \otimes \mathbb{Q} \to M_2(\mathbb{Q})$ be an isomorphism. Let $e \in End_{\mathbb{Q}}(A_f) \otimes \mathbb{Q}$ such that $\psi(e)$ is a rank one matrix. Then eA_f is a one-dimensional subvariety of A_f, and A_f/eA_f is a one-dimensional abelian variety. Washington and Roberts have shown that A_f is isogenous to the product of the two elliptic curves, $E_1 = A_f/eA_f$ and $E_2 = A_f/e^{\sigma}A_f$ [17]. In addition, they have shown that there exists a unique cusp form h, up to a constant multiple, in the span of f and f' such that $eh = 0$ and the period lattice of h is homothetic to the period lattice of E_1. Hence, a modular parametrization of E_1 is given by $\phi(\tau) = \int_0^{\tau} h(z)dz$. Suppose that $e = a + bT_p + c\eta + dT_p\eta$. Then a straight-forward calculation using the properties of T_p and η shows that h can be given by

$$h = \sqrt{t}f - \frac{a + b\sqrt{r}}{c + d\sqrt{r}}f'.$$

The function h is unique up to a constant multiple. Each endomorphism which corresponds to a rank one matrix produces a strong Weil parametrization of some $\mathbb{Q}$-curve. In the following chapter, we will discuss how these different parametrizations are related.

2.3 Implementing the Algorithm

Given a modular parametrization ϕ of a $\mathbb{Q}$-curve, the next step is to compute the degree of the map ϕ. Theorem 6 and Theorem 7 remain true in the case of elliptic curves over number fields. However, they are not usable in their present form. When working with elliptic curves over $\mathbb{Q}$, Cremona's modular symbol algorithms gave an explicit way to calculate the values of the functions n_1 and n_2 for a particular basis of the period lattice. Since Cremona's work deals with elliptic curves defined over $\mathbb{Q}$, the eigenforms used in the strong Weil parametrization have coefficients lying in $\mathbb{Q}$. Hence, the abelian variety A_f is one-dimensional. The two-dimensional subspace of $H_1(X_0(N), \mathbb{Q})$ which corresponds to the eigenform f can be found using integer arithmetic as described in Chapter 1. In addition, Cremona uses the fact that f is an eigenform and simplifies the computation by working in the two subspaces $H^+(N) = H^+(X_0(N), \mathbb{Q})$ and $H^-(N) = H^-(X_0(N), \mathbb{Q})$. However, when ϕ is a modular parametrization of a $\mathbb{Q}$-curve defined over a quadratic field, Cremona's methods do not describe how to find the two-dimensional subspace in $H_1(X_0(N), \mathbb{Q})$ which corresponds to the cusp form h in the modular parametrization. Also, h is not an eigenform, and we cannot benefit from using the decomposition of the homology into $H^+(N)$ and $H^-(N)$ since h does not always have real coefficients. In the following, we will discuss how to overcome this difficulty so that the values of n_1 and n_2 can be obtained with exact integer arithmetic. The rest of the algorithm for computing the degree remains unchanged.

Rather than working with the cusp forms directly, we will instead do computations of $H_1(X_0(N), \mathbb{Q})$ in order to determine the values of n_1 and n_2. In Chapter 1, we described how the Hecke operator T_p acted on the modular symbols. Since η acts on the space of cusp forms, it must also act on the homology.

Let $\gamma = \{\alpha, \beta\}$, and let f be a cusp form. Then

$$\begin{aligned}
\langle \gamma, \eta f \rangle &= \left\langle \gamma, \sum_{j=1}^{|t|-1} \chi(j) f \middle| \begin{pmatrix} 1 & j/t \\ 0 & 1 \end{pmatrix} \right\rangle \\
&= \sum_{j=1}^{|t|-1} \left\langle \chi(j)\gamma, f \middle| \begin{pmatrix} 1 & j/t \\ 0 & 1 \end{pmatrix} \right\rangle \\
&= \sum_{j=1}^{|t|-1} \left\langle \chi(j) \begin{pmatrix} 1 & j/t \\ 0 & 1 \end{pmatrix} \gamma, f \right\rangle \\
&= \left\langle \sum_{j=1}^{|t|-1} \chi(j) \left\{ \alpha + \frac{j}{t}, \beta + \frac{j}{t} \right\}, f \right\rangle.
\end{aligned}$$

Since the pairing $\langle \gamma, f \rangle$ is non-degenerate, we can define the action of η on modular symbols by

$$\eta(\{\alpha, \beta\}) = \sum_{j=1}^{|t|-1} \chi(j) \left\{ \alpha + \frac{j}{t}, \beta + \frac{j}{t} \right\}.$$

Since the $\mathbb{Q}$-algebra $End(A_f) \otimes \mathbb{Q}$ is generated $\{1, T_p, \eta, T_p\eta\}$, any endomorphism $e \in End_{\mathbb{Q}}(A_f) \otimes \mathbb{Q}$ acts on the space of cusp forms and $H_1(X_0(N), \mathbb{Q})$ such that

$$\langle \gamma, eh \rangle = \langle e\gamma, h \rangle.$$

Let $\gamma_1, \gamma_2, \ldots, \gamma_{2g}$ be a basis for $H_1(X_0(N), \mathbb{Q})$. The goal is to isolate the four-dimensional eigenspace in homology which corresponds to the span of f and f'. Suppose that $T_p^2 = r$ and $\eta^2 = t$. By computing the action of the Hecke operator T_p on the basis, one can determine the r eigenspace of T_p^2. This will be at least a four-dimensional space. If it is larger than four-dimensional, then the action of T_q for another prime q must be calculated. Finding the a_q^2 eigenspace of T_q^2 and intersecting it with the the previous space may reduce the dimension. By continuing this process, a distinct four-dimensional subspace of $H_1(X_0(N), \mathbb{Q})$

can be found which corresponds to the span of f and f'. This can be accomplished after a finite number of steps. Let V be the subspace of $H_1(X_0(N), \mathbb{Q})$ spanned by $\{v_1, v_2, v_3, v_4\} \subset \mathbb{Z}^{2g}$. Let W be spanned by the dual basis $\{w_1, w_2, w_3, w_4\} \subset \mathbb{Q}^{2g}$ such that

$$v_i \cdot w_j = \begin{cases} 1 & \text{if } i = j \\ \\ 0 & \text{if } i \neq j \end{cases}$$

and $v \cdot w_j = 0$ if v is not in V. A basis for the space W can be found by isolating the four-dimensional eigenspace which corresponds to the transpose of the Hecke operator matrices. Then the desired basis of W, $\{w_1, w_2, w_3, w_4\}$, can be found which gives the correct dot products. Each v_i is a vector of integers which represents an integral sum of M-symbols. Each w_i is a vector of rational numbers. Let $\gamma \in H_1(X_0(N), \mathbb{Z})$. The path γ is viewed as an integer vector of length $2g$ which represents an integral linear combination of the basis for $H_1(X_0(N), \mathbb{Q})$. Then

$$\langle \gamma, h \rangle = \langle \sum_{j=1}^{4} (w_j \cdot \gamma) v_j, h \rangle.$$

Recall that h was chosen so that $eh = 0$. So if $\gamma \in eV$, then

$$\langle \gamma, h \rangle = \langle e\gamma', h \rangle = \langle \gamma', eh \rangle = 0.$$

Since e corresponds to a rank one matrix, eV must be a two-dimensional subspace of V. Suppose V/eV is generated by z_1 and z_2. Define linear functions α and β from $\mathbb{Q}^4$ to $\mathbb{Q}$ such that

$$av_1 + bv_2 + cv_3 + dv_4 \equiv \alpha(a, b, c, d) z_1 + \beta(a, b, c, d) z_2 \pmod{eV}.$$

Then

$$\begin{aligned} \langle \gamma, h \rangle = & \langle \alpha(w_1 \cdot \gamma, w_2 \cdot \gamma, w_3 \cdot \gamma, w_4 \cdot \gamma) z_1, h \rangle \\ & + \langle \beta(w_1 \cdot \gamma, w_2 \cdot \gamma, w_3 \cdot \gamma, w_4 \cdot \gamma) z_2, h \rangle. \end{aligned}$$

Extend the function α to $\tilde{\alpha} : (\mathbb{Q}^{2g})^4 \to \mathbb{Q}^{2g}$ as follows. The i-th component of the result is obtained by applying α on the 4-tuple formed by the i-th components of each vector in $\mathbb{Q}^{2g}$. Extend β to $\tilde{\beta}$ in the same way. Then

$$\langle \gamma, h \rangle = \gamma \cdot \tilde{\alpha}(w_1, w_2, w_3, w_4)\, \langle z_1, h \rangle + \gamma \cdot \tilde{\beta}(w_1, w_2, w_3, w_4)\, \langle z_2, h \rangle.$$

Both $\tilde{\alpha}(w_1, w_2, w_3, w_4)$ and $\tilde{\beta}(w_1, w_2, w_3, w_4)$ are vectors of rational numbers. Let k_1 and k_2 be rational numbers such that

$$A = \tilde{\alpha}(w_1, w_2, w_3, w_4)/k_1 \text{ and}$$
$$B = \tilde{\beta}(w_1, w_2, w_3, w_4)/k_2$$

are vectors of integers. Then

$$\langle \gamma, h \rangle = (\gamma \cdot A)\, k_1 \langle z_1, h \rangle + (\gamma \cdot B)\, k_2 \langle z_2, h \rangle.$$

Since A and B are vectors of integers, the value of the period is an integral linear combination of two complex numbers, $\omega_1 = k_1\langle z_1, h \rangle$ and $\omega_2 = k_2 \langle z_2, h \rangle$.

In order to show that we have indeed found a basis for the period lattice of h, it is necessary to show that both ω_1 and ω_2 are periods of h. These two quantities are periods if and only if there exist vectors of integers u_1 and u_2 such that

$$\begin{array}{ll} u_1 \cdot A = 1 & u_1 \cdot B = 0 \\ u_2 \cdot A = 0 & u_2 \cdot B = 1. \end{array}$$

If γ_i is the path represented by the vector u_i, then $\langle \gamma_i, h \rangle = (u_i \cdot A)\omega_1 + (u_i \cdot B)\omega_2$ for $i = 1$ and 2. Therefore, $\langle \gamma_1, h \rangle = \omega_1$ and $\langle \gamma_2, h \rangle = \omega_2$. Let M_1 be the matrix formed by letting the two rows be u_1 and u_2. Let M_2 be the matrix formed by letting the two columns be A and B. Then the equations above are satisfied if and only if there exists a solution for M_1 in integers to the equation $M_1 M_2 = I$.

A solution in integers for M_1 exists if and only if the matrix M_2 can be row reduced with integer operations to

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \\ \vdots & \vdots \end{pmatrix}.$$

This row reduction can occur if and only if the two vectors A and B are independent modulo p for all primes p. Hence, it might be the case that ω_1 and ω_2 are not periods.

If the two columns are dependent modulo p, then a modification needs to be made to determine a basis for the period lattice of h. Let M be a $m \times 2$ matrix. Define $\Phi(M)$ to be the greatest common divisor of all determinants of the 2×2 submatrices of M. Suppose $\Phi(M) = m$. Let a and b be the greatest common divisors of all of the entries of A and B respectively. Set $m' = m/(ab)$, $A' = A/a$, and $B' = B/b$. If $m' = 1$, then

$$\langle \gamma, h \rangle = (\gamma \cdot A')(ak_1\langle z_1, h\rangle) + (\gamma \cdot B')(bk_2\langle z_2, h\rangle).$$

Hence, $a\omega_1$ and $b\omega_2$ are a basis for the period lattice of h. Also, $n_1(\gamma) = \gamma \cdot A'$ and $n_2(\gamma) = \gamma \cdot B'$. Now suppose $m' > 1$ and that $A' \equiv kB' \pmod{m'}$ for some k. Then set D' equal to the vector $(A' - kB')/m'$. Then

$$\begin{aligned}\langle \gamma, h \rangle &= \gamma \cdot A'(ak_1\langle z_1, h\rangle) - \gamma \cdot kB'(ak_1\langle z_1, h\rangle) \\ &\quad + \gamma \cdot B'(bk_2\langle z_2, h\rangle) + \gamma \cdot kB'(ak_1\langle z_1, h\rangle) \\ &= \gamma \cdot D'(m'ak_1\langle z_1, h\rangle) + \gamma \cdot B'(kak_1\langle z_1, h\rangle + bk_2\langle z_2, h\rangle).\end{aligned}$$

So the period is written as an integral linear combination of two complex numbers which are different from the original pair.

This procedure can be summarized in matrix notation. Let

$$P_1 = \begin{pmatrix} 1/a & 0 \\ 0 & 1/b \end{pmatrix} \text{ and } P_2 = \begin{pmatrix} 1/m' & 0 \\ k/m' & 1 \end{pmatrix}.$$

Then $M_2 P_1 = [A' \;\; B']$, and $[A' \;\; B']P_2 = [D' \;\; B']$. The transformation from the matrix $M_2 = [A \;\; B]$ to $[D' \;\; B']$ can be obtained by right multiplying M_2 by $P_1 P_2$. Also det $(P_1 P_2) = 1/(abm') = 1/m$. Hence $\Phi([D' \;\; B']) = 1$ and so D' and B' are independent modulo p for all primes p. This guarantees that a basis has been found for the period lattice of h. Therefore $n_1(\gamma) = \gamma \cdot D'$ and $n_2(\gamma) = \gamma \cdot B'$. This transformation process will be referred to as *removing the dependency relation*. This will be discussed in more detail in the following chapter.

The algorithm for computing the values of the functions n_i requires only integer arithmetic. It does not rely on computing a numerical approximation to the period lattice of the function h. It is also important to note that one does not have to compute a large number of Fourier coefficients in order to conduct the calculation. In most cases, a few Fourier coefficients are sufficient provided that it is known that the eigenforms f and f' have an extra twist. If a large number of Fourier coefficients are known, then the algorithm provides a simple way to find an approximation for a basis of the period lattice of h. Let δ_1 and δ_2 be any two closed paths on $X_0(N)$ such that $n_1(\delta_1)n_2(\delta_2) - n_1(\delta_2)n_2(\delta_1) \neq 0$. Then

$$\begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = \begin{pmatrix} n_1(\delta_1) & n_2(\delta_1) \\ n_1(\delta_2) & n_2(\delta_2) \end{pmatrix}^{-1} \begin{pmatrix} \langle \delta_1, h \rangle \\ \langle \delta_2, h \rangle \end{pmatrix}.$$

The values of $\langle \delta_i, h \rangle$ can be approximated for $i = 1, 2$ using Theorems 1 and 2. This will give $\{\omega_1, \omega_2\}$ as an approximation to the basis of the period lattice of h. Note that the algorithm presented here for computing the values of n_1 and n_2 did not depend on the fact that f was an eigenform for $\Gamma_0(N)$. Hence, theoretically it could be used to calculate the degree of a modular parametrization from $X_1(N)$ to the $\mathbb{Q}$-curve E where f is an eigenform for $\Gamma_1(N)$ with an extra twist. However, the algorithms presented by Cremona for computing a basis for $H_1(X_1(N), \mathbb{Q})$ become computationally not feasible for $N \geq 200$. This computational problem is discussed by Cremona in [3].

2.4 Algorithm Outline

We will now give a concise outline of the steps to compute the degree of modular parametrization. We will assume that we know that there is a cusp form f of weight two at level N which has an extra twist and that the abelian variety A_f can be split into the product of two elliptic curves. Suppose that p is the smallest prime such that the p-th coefficient of f is not in $\mathbb{Q}$. Let $e = a + bT_p + c\eta + dT_p\eta$ be an endomorphism of A_f such that e corresponds to a rank one matrix. The following steps determine the values of $n_1(\gamma_i)$ and $n_2(\gamma_i)$ for γ_i a basis element of $H_1(X_0(N), \mathbb{Q})$. Once again, V and W are subspaces of $H_1(X_0(N), \mathbb{Q})$ and are represented as $2g \times k$ matrices where k is the dimension of the subspace. The columns of the matrices V and W span the spaces V and W respectively.

1. Compute a basis for $H_1(X_0(N), \mathbb{Q})$. Set $V := W := 2g \times 2g$ identity matrix. The i-th column represents γ_i, the i-th basis element of $H_1(X_0(N), \mathbb{Q})$. Let p be the smallest prime that does not divide N.

2. Compute the matrix of T_p with respect to V.

3. Set $V := (a_p^2$ eigenspace of $T_p) \cap V$.

4. Set $W := (a_p^2$ eigenspace of $T_p^t) \cap W$.

5. If the dimension of $V > 4$, set $p =$ next largest prime that does not divide N. Return to Step 2.

6. Let V^t denote the matrix obtained by placing the i-th basis element in each column of V in the i-th row for each i. Set $M := (W \cdot V^t)^{-1}$.

7. Set $W := M \cdot W$.

8. Compute the action of T_p on V where p is the smallest prime such that the p-th coefficient of f is not in $\mathbb{Q}$.

9. Compute the action of η on V.

10. Compute $T_p\eta$ on V.

11. Set $eV =$ two-dimensional subspace formed by $a + bT_p + c\eta + dT_p\eta$ acting on V. The space eV is represented by a 2×4 matrix called S where the rows span eV. Each row represents a linear combination of v_1, v_2, v_3 and v_4.

12. If the 2×2 submatrix R formed by the first 2 columns of S is invertible, set $S = R^{-1}S$. If it is not invertible, let R be any 2×2 submatrix of S such that R is invertible. Then set $S := R^{-1}(S)$. Step 13 will have to be modified by adjusting the subscripts and indices in this case.

13. Let w_i denote the i-th row of W. Then set

$$A := -S[1,3] \cdot w_1 - S[2,3] \cdot w_2 + w_3$$
$$B := -S[1,4] \cdot w_1 - S[2,4] \cdot w_2 + w_4$$

14. Let d_1 and d_2 be the smallest integers such that the vectors d_1A and d_2B are vectors of integers. Set $A := d_1A$ and $B := d_2B$.

15. $a' :=$ greatest common divisor of entries of A; $b' :=$ greatest common divisor of entries of B; $A := A/a'$; $B := B/b'$.

16. Set $m := \Phi([A \;\; B])$.

17. If $m > 1$, solve for k in $A \equiv kB \pmod{m}$.

18. If $m > 1$, $A := (A - kB)/m$.

Given γ_i which is the i-th basis element of $H_1(X_0(N), \mathbb{Q})$, we have

$$\langle \gamma_i, h \rangle = A[i]\omega_1 + B[i]\omega_2$$

where $\{\omega_1, \omega_2\}$ is a basis of the period lattice of h.

We list the steps needed to compute the degree of modular parametrization.

1. Make a list called EC of inequivalent points in $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$ which are invariant under the action of TS. Set deg $:= 0$.

2. Choose an M-symbol α from EC which has not been handled yet.

3. Apply T to α.

4. IF ($T(\alpha)$ is in the list EC) $\alpha := \tau(\alpha)$ and go back to step 3 if not at the end of the orbit; ELSE continue

5. Compute $t(\alpha) \in \Gamma_0(N)$.

6. Write the path $\{0, t(\alpha)(0)\}$ as a sum of basis elements of $H_1(X_0(N), \mathbb{Z})$. This will be represented by a vector $v \in Z^{2g}$.

7. Compute $n_1(t(\alpha)) := v \cdot A$ and $n_2(t(\alpha)) := v \cdot B$ and store values.

8. Set $\alpha := \tau(\alpha)$. Go to step 3 until the end of orbit is reached.

9. Update Sum by adding in the values 2×2 determinants of the stored n_1 and n_2 values.

10. Clear the n_1 and n_2 values. Go back to step 2 and repeat these steps until all orbits have been handled.

11. RETURN $|\mathrm{deg}|/2$.

2.5 An Example

In the following, we will give an example of the computational results for computing the values of the functions n_i where E is $\mathbb{Q}$-curve with a modular parametrization from $X_0(81)$. There is a cusp form f at level 81 for $\Gamma_0(N)$ such that $f' = f \otimes \chi$ where χ is a quadratic character associated to $\mathbb{Q}(\sqrt{-3})$. The first few coefficients of f are

$$\begin{aligned} f &= q + \sqrt{3}q^2 + q^4 - \sqrt{3}q^5 + 2q^7 - \sqrt{3}q^8 + \cdots \\ f' &= q - \sqrt{3}q^2 + q^4 + \sqrt{3}q^5 + 2q^7 + \sqrt{3}q^8 + \cdots \end{aligned}$$

Let $\{\gamma_1, \gamma_2, \ldots, \gamma_8\}$ be a basis for $H_1(X_0(81), \mathbb{Q})$. Let the symbol (a) denote the M-symbol $(a:1)$. Then the basis can be chosen as follows:

$$\begin{aligned} \gamma_1 &= (39) - (21) & \gamma_2 &= (42) - (15) \\ \gamma_3 &= (48) - (21) & \gamma_4 &= (51) - (15) \\ \gamma_5 &= (66) - (21) & \gamma_6 &= (69) - (15) \\ \gamma_7 &= (75) - (21) & \gamma_8 &= (78) - (15). \end{aligned}$$

Computing the 3 eigenspace of T_2^2 and the 3 eigenspace of $(T_2^t)^2$ gives

$$V = \begin{pmatrix} v_1 \\ v_2 \\ v_3 \\ v_4 \end{pmatrix} = \begin{pmatrix} -1 & 1 & -1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 1 \end{pmatrix} \quad \text{and}$$

$$W = \begin{pmatrix} -1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 1 & 0 & 0 \\ 2 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ -1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

By adjusting the basis of W so that it is a dual basis to V gives

$$\begin{pmatrix} w_1 \\ w_2 \\ w_3 \\ w_4 \end{pmatrix} = \begin{pmatrix} -2/3 & 0 & 0 & 1/3 & 1/3 & 0 & 0 & 1/3 \\ 0 & -1/3 & -2/3 & -1/3 & -1/3 & 1/3 & -1/3 & -1/3 \\ 2/3 & 2/3 & 1/3 & 1/3 & 1/3 & 1/3 & 2/3 & 1/3 \\ -1/3 & 0 & 0 & -1/3 & -1/3 & 0 & 0 & 2/3 \end{pmatrix}.$$

Let $e = 6 + 3T_2 - T_2\eta$. Then $e^2 = 12e$. So e corresponds to a rank one matrix. The action of T_2 and η on the space V can be computed. This gives $eV = \langle v_1 - v_4, v_2 + v_3 \rangle$. Therefore, V/eV can be generated by v_1 and v_2 subject to the relations $v_4 \equiv v_1 \pmod{eV}$ and $v_3 \equiv -v_2 \pmod{eV}$. Then $\alpha(a,b,c,d) = a + d$ and $\beta(a,b,c,d) = b - c$. Thus

$$\alpha(w_1, w_2, w_3, w_4) = [-1, 0, 0, 0, 0, 0, 0, 1] \text{ and}$$
$$\beta(w_1, w_2, w_3, w_4) = -1/3[2, 3, 3, 2, 2, 0, 3, 2].$$

Thus $A = [-1, 0, 0, 0, 0, 0, 0, 1]$ and $B = [2, 3, 3, 2, 2, 0, 3, 2]$, which are independent modulo p for all primes p. Therefore, if $\gamma \in H_1(X_0(81), \mathbb{Q})$, $n_1(\gamma) = \gamma \cdot A$ and $n_2(\gamma) = \gamma \cdot B$. Using the degree calculation algorithm, the degree of modular parametrization of E is 6.

Chapter 3

Properties of the Degree of Parametrization

In Chapter 2, we presented an algorithm for computing the degree of modular parametrization for a particular class of $\mathbb{Q}$-curves defined over a quadratic field. For computational purposes, we concentrated on $\mathbb{Q}$-curves with a modular parametrization from $X_0(N)$. We will consider f to be an eigenform for $\Gamma_0(N)$ with an extra twist with coefficients lying in $L = \mathbb{Q}(\sqrt{r})$. Hence, $f' = f \otimes \chi$ where f' is the Galois conjugate of f and $\chi(n) = (\frac{t}{n})$. Therefore,

$$\begin{aligned} \phi : X_0(N) &\to E \\ \tau &\mapsto \int_{\tau_o}^{\tau} h(z)dz \end{aligned}$$

where h is a particular cusp form in the span of f and f'. In the following chapter, we will present several results concerning modular parametrizations from $X_0(N)$. Each argument also applies to modular parametrizations from $X_1(N)$ under the above assumptions concerning the cusp form f.

3.1 Characterizing the Strong Weil Parametrizations

Let ψ be an isomorphism between $End(A_f)\otimes\mathbb{Q}$ and $M_2(\mathbb{Q})$. In the previous chapter, we proved that every endomorphism e of A_f such that $\psi(e)$ is a rank one matrix will give rise to an elliptic curve A_f/eA_f with a strong Weil parametrization. The following theorem characterizes all of the strong Weil parametrizations from $X_1(N)$ to $\mathbb{Q}$-curves defined over quadratic fields.

Theorem 8. *Let*

$$H = \{h = af + bf' \,|a, b \in \mathbb{C}, \textit{ the periods of } h \textit{ form a lattice in } \mathbb{C}\}/\{constants\}.$$

Then H is in one-to-one correspondence with $\mathbb{P}^1(\mathbb{Z})$. The correspondence is given in the proof of the theorem.

Proof. Let $h \in H$. There is an $e \in End(A_f)$ such that $eh = 0$. Then $\psi(e)$ is a rank one matrix. Let $[u, v]^t$ be the kernel of $\psi(e)$. Therefore, we obtain a point $(u : v) \in \mathbb{P}^1(\mathbb{Z})$.

Let $(u : v) \in \mathbb{P}^1(\mathbb{Z})$ and

$$M = \begin{pmatrix} -v & u \\ 0 & 0 \end{pmatrix}.$$

We obtain h by choosing the unique element of H which is annihilated by e.

Now, we need to show that the composition is the identity. Start with $(u : v) \in \mathbb{P}^1(\mathbb{Z})$ and obtain $h \in H$. Suppose that e' is any endomorphism of A_f which annihilates h. Let $e = \psi^{-1}(M)$ and $M' = \psi(e)$. Then $M' = AM$ for some invertible matrix A. Thus, $e' = ae$ for some invertible element of $End(A_f) \otimes \mathbb{Q}$.

Since the kernel of M' equals the kernel of M, we obtain the point $(u : v) \in \mathbb{P}^1(\mathbb{Z})$ regardless of the choice of endomorphism. $\square$

This theorem describes all of the strong Weil parametrizations from $X_1(N)$ to the elliptic curves A_f/eA_f for all $e \in End(A_f)$. Suppose that $h_0 \in H$ corresponds to the point $(u_0 : v_0) \in \mathbb{P}^1(\mathbb{Z})$. This means that $e_0 h_0 = 0$ where

$$e_0 = \psi^{-1}\left(\begin{pmatrix} -v_0 & u_0 \\ 0 & 0 \end{pmatrix}\right) h_0 = 0.$$

Suppose that $e = \alpha + \beta T_p + \gamma\eta + \delta T_p \eta \in End(A_f)$. Define $\overline{e} = \alpha - \beta T_p - \gamma\eta - \delta T_p\eta$. Then $\psi(\overline{e})$ is the adjoint of $\psi(e)$. Also, $(e_0\overline{e})eh_0 = 0$. Let

$$\psi(e) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Then

$$\psi(e_0\overline{e}) = \begin{pmatrix} -dv_0 - cu_0 & bv_0 + au_0 \\ 0 & 0 \end{pmatrix}.$$

Therefore, the cusp form eh_0 corresponds to the point $(au_0 + bv_0 : cu_0 + dv_0) \in \mathbb{P}^1(\mathbb{Z})$.

3.2 N=81 Example Revisited

Let us continue with the example from the previous chapter concerning modular parametrizations of $\mathbb{Q}$-curves from $X_0(81)$. This time the goal is to compute the degrees of all the modular parametrizations from $X_0(81)$ to $\mathbb{Q}$-curves over quadratic fields. In this case, $End(A_f) \otimes \mathbb{Q} \cong \left(\frac{3,-3}{\mathbb{Q}}\right)$. We can choose an isomorphism between this quaternion algebra and $M_2(\mathbb{Q})$ as follows:

$$T_2 = \begin{pmatrix} 0 & 1 \\ 3 & 0 \end{pmatrix} \qquad \text{and} \qquad \eta = \begin{pmatrix} 0 & 1 \\ -3 & 0 \end{pmatrix}.$$

Then we have the correspondence

$$\begin{pmatrix} v & -u \\ 0 & 0 \end{pmatrix} \leftrightarrow \frac{1}{2}v - \frac{1}{2}uT_2 - \frac{1}{2}u\eta - \frac{1}{6}vT_2\eta$$

By clearing the denominators, this gives an endomorphism of A_f

$$e = 3v - 3uT_2 - 3u\eta - vT_2\eta.$$

Isolate the four-dimensional subspace V of $H_1(X_0(N), \mathbb{Q})$ that corresponds to the span of f and f'. This can be done by calculating the matrix T_2 with respect to a basis of $H_1(X_0(N), \mathbb{Q})$, and calculating the 3 eigenspace of T_2^2. Let v_1, v_2, v_3, and v_4 be a basis for V. Each v_i is represented as a sum of M-symbols. So we can apply both T_2 and η to them. Hence, we can obtain the 4×4 matrices for the actions of T_2 and η with respect to the basis $\{v_1, v_2, v_3, v_4\}$. Now, we can compute a basis for the two-dimensional space eV. Thus, eV is spanned by the rows of

$$\begin{pmatrix} 6u + 6v & -3u + v & -12u - 2v & 12u \\ 0 & 6u + 6v & -12u & 0 \end{pmatrix}.$$

Suppose $(u : v) \neq (1 : -1)$, then the 2×2 submatrix of eV formed by the first two columns, is invertible. Multiplying by the inverse of this submatrix shows that V/eV can be generated by v_3 and v_4, and v_1 and v_2 are given in terms of these generators. Continuing the algorithm as before, we obtain the matrix of the values of $n_1(\gamma_i)$ and $n_2(\gamma_i)$ for $\gamma_1, \gamma_2, \ldots, \gamma_{2g}$.

$$M = [A \;\; B] = \begin{pmatrix} -12u^2+4v^2 & 3u-v \\ 6uv+6v^2 & 0 \\ -9u^2-6uv+3v^2 & 0 \\ 6u^2+6uv+4v^2 & -3u-v \\ 6u^2+6uv+4v^2 & -3u-v \\ 9u^2+12uv+3v^2 & 0 \\ 6uv+6v^2 & 0 \\ 6u^2+6uv+4v^2 & 2v \end{pmatrix}.$$

By computing the polynomial greatest common divisor of all of the 2×2 determinants, we see that $3(u+v)|\Phi(M)$. We will remove the dependencies $u+v$ and 3 one at a time. First, $A \equiv -2uB \pmod{u+v}$. So set $D = (A+2uB)/(u+v)$. Then the result has $D \equiv 2B \pmod 3$. So change D to $(D-2B)/3$. This gives us

$$M' = [D \;\; B] = \begin{pmatrix} -4u+2v & 3u-v \\ 2v & 0 \\ -3u+v & 0 \\ 2u+2v & -3u-v \\ 2u+2v & -3u-v \\ 3u+v & 0 \\ 2v & 0 \\ 2u & 2v \end{pmatrix}.$$

If u and v are relatively prime, these two columns could only be dependent modulo 3. In addition, if $v \equiv 0 \pmod 3$, then the two columns will be dependent modulo 3. In that case this dependency must be removed to obtain the correct matrix. Assuming that these two columns are independent modulo 3, the degree calculation algorithm determines that the degree of modular parametrization of the elliptic curve A_f/eA_f is $6(3u^2+v^2)$. Now suppose that the two columns are dependent modulo 3. Then each of the 2×2 determinants in the degree formula are too large by a factor of 3. Therefore, the degree in these cases is given by $2(3u^2+v^2)$.

3.3 Preliminary Results Concerning the Degree of Parametrization

Let

$$\phi(u,v)(\tau) = \int_{\tau_0}^{\tau} h(u,v)(z)dz$$

be a strong Weil parametrization of a $\mathbb{Q}$-curve for each (u,v) pair such that u and v are relatively prime. For any $h \in H$, let L_h denote the period lattice of h. Let $\gamma_1, \gamma_2, \ldots, \gamma_{2g}$ be a $\mathbb{Z}$-basis for $H_1(X_0(N), \mathbb{Z})$. When looking at the set H, all of the cusp forms are well-defined up to a constant multiple. This is not always a convenient point of view. In order to remove this ambiguity, we give the following lemma.

Lemma 2. *Let $h_0 \in H$ correspond to the point $(u_0 : v_0) \in \mathbb{P}^1(\mathbb{Z})$ where u_0 and v_0 are relatively prime. Set*

$$H' = \{eh_0 \mid e \in End(A_f) \otimes \mathbb{Q}\}.$$

Define the map τ as follows:

$$\begin{aligned} \tau : H' \to & \quad \mathbb{Q}^2 \\ eh_0 \mapsto & \ (au_0 + bv_0, cu_0 + dv_0) \end{aligned}$$

where

$$\psi(e) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Then τ is a well-defined isomorphism of $\mathbb{Q}$-vector spaces.

Proof. Let

$$\psi(e_0) = \begin{pmatrix} -v_0 & u_0 \\ 0 & 0 \end{pmatrix}.$$

Suppose that e_1 and e_2 are distinct elements of $End(A_f) \otimes \mathbb{Q}$ such that $e_1 h_0 = e_2 h_0$. Then $(e_1 - e_2)h_0 = 0$. Since $e_0 h_0 = 0$, we see that $e_1 - e_2 = \gamma e_0$ for some $\gamma \in End(A_f) \otimes \mathbb{Q}$. Then

$$\psi(e_1 - e_2) \begin{pmatrix} u_0 \\ v_0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

Therefore,

$$\psi(e_1) \begin{pmatrix} u_0 \\ v_0 \end{pmatrix} = \psi(e_2) \begin{pmatrix} u_0 \\ v_0 \end{pmatrix},$$

which implies that $\tau(e_1 h_0) = \tau(e_2 h_0)$. Let $(u, v) \in \mathbb{Q}^2$. Then there is an $M \in M_2(\mathbb{Q})$ such that

$$M \begin{pmatrix} u_0 \\ v_0 \end{pmatrix} = \begin{pmatrix} u \\ v \end{pmatrix}.$$

Set $e = \psi^{-1}(M)$. Then $\tau(eh_0) = (u, v)$, which proves that τ is surjective. Suppose that $\tau(e_1 h_0) = \tau(e_2 h_0)$. Then, we clearly have

$$\psi(e_1 - e_2) \begin{pmatrix} u_0 \\ v_0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

Therefore, $\psi(e_1 - e_2)$ is either a rank one or two matrix. If it is rank 0, then $e_1 = e_2$. If it is rank 1, then $\psi(e_1 - e_2) = A\psi(e_0)$, where A is an invertible matrix. Thus, $(e_1 - e_2)h_0 = 0$, which implies that τ is injective. $\square$

Theorem 9. *Let h_0 be a cusp form in H' and suppose $\{\nu_1, \nu_2\}$ forms a basis for the period lattice of h_0. Let e be an endomorphism of A_f which is an invertible element of $End(A_f) \otimes \mathbb{Q}$. Suppose eh_0 corresponds to the point $(u, v) \in \mathbb{Q}^2$ as in the previous lemma. Then there exists a $2g \times 2$ matrix $Q(u, v)$ with entries which are integral linear combinations of u and v such that*

$$Q(u,v)\begin{pmatrix}\nu_1\\ \nu_2\end{pmatrix} = \left(\int_{\gamma_i} h(z)dz\right).$$

Proof. Let $h_0 \in H$ correspond to the point $(u_0 : v_0) \in \mathbb{P}^1(\mathbb{Z})$ with u_0 and v_0 relatively prime. Let

$$\psi(e) = \begin{pmatrix} a & b\\ c & d\end{pmatrix}.$$

Suppose eh_0 corresponds to the point

$$(u, v) = (au_0 + bv_0, cu_0 + dv_0) \in \mathbb{Q}^2$$

as in Lemma 2. Since $e \in End(A_f)$, we have that $(u, v) \in \mathbb{Z}^2$. Also,

$$\int_{\gamma_i} eh_0(z)dz = \int_{e\gamma_i} h_0(z)dz,$$

implies that $L_{eh_0} \subset L_{h_0}$. Hence, there exists a matrix $Q(e)$ with integer entries, such that

$$Q(e)\begin{pmatrix}\nu_1\\ \nu_2\end{pmatrix} = \left(\int_{\gamma_i} eh_0(z)dz\right).$$

Since we have the one-to-one correspondence in Lemma 2, we see that e uniquely determines $(u,v) \in \mathbb{Z}^2$. Therefore, Q depends only on the pair (u,v). Thus we can write the well-defined equation

$$Q(u,v)\begin{pmatrix}\nu_1\\ \nu_2\end{pmatrix} = \left(\int_{\gamma_i} eh_0(z)dz\right)$$

where (u,v) corresponds to eh_0. The entries in $Q(u,v)$ are of the form $a_iu + b_iv$ for some integers a_i and b_i since Q is clearly linear in e, and e is linear in u and v. $\square$

The map $\phi(u,v)$ factors through the abelian variety A_f as follows:

$$\begin{array}{ccccc} X_0(N) & \xrightarrow{\psi_1} & A_f & \xrightarrow{\psi_2} & E \\ \tau & \mapsto & \left(\int_{\tau_0}^{\tau} f(z)dz, \int_{\tau_0}^{\tau} f'(z)dz\right) & \mapsto & \int_{\tau_0}^{\tau} h(u,v)(z)dz. \end{array}$$

The image of the map ψ_1 is an algebraic curve in A_f. Let $d =$ deg ψ_1. The following theorem gives a general result concerning the form of the degree of the map $\phi(u,v)$. When $\phi(u,v)$ is regarded instead as a map from $X_1(N)$ to E, we will set $d =$ deg $(X_1(N) \to A_f)$.

Theorem 10. *Let $\phi(u,v)$ be the modular parametrization of a $\mathbb{Q}$-curve defined over a quadratic field as given above. Then*

$$deg\ \phi(u,v) = d\,\frac{g(u,v)}{k(u,v)}$$

where $g(u,v)$ is a binary quadratic form over $\mathbb{Z}$ and $k(u,v)$ is an integer called the dependency constant.

Proof. Let $h \in H$ correspond to the point $(u:v)$. Then let $Q(u,v)$, ν_1, ν_2 be given as in Theorem 9. Set $k(u,v) = \Phi(Q(u,v))$. If $k(u,v) = 1$, then Theorem

7 implies that the degree is simply the finite sum of certain 2×2 determinants. Since each entry in Q is an integral linear combination of u and v, each 2×2 determinant must be a binary quadratic form with integer coefficients. Hence deg $\phi(u,v) = \tilde{g}(u,v)$, which is a binary quadratic form. If $k(u,v) \neq 1$, then deg $\phi(u,v) = \frac{\tilde{g}(u,v)}{k(u,v)}$. Let $d =$ deg ψ_1 which is independent of the choice of u and v. By pulling out this constant, we get deg $\phi(u,v) = d\,\frac{g(u,v)}{k(u,v)}$ where g is a binary quadratic form and k is the dependency constant. $\square$

It is important to note that the form g depends on a choice of isomorphism between $M_2(\mathbb{Q})$ and $End(A_f) \otimes \mathbb{Q}$. By choosing a different isomorphism, the variables u and v change by a $SL_2(\mathbb{Z})$ transformation. Therefore, the form g can be described by a well-defined equivalence class of binary quadratic forms of a fixed discriminant. In the previous example, we know that the form $g = c(3u^2 + v^2)$ where $c|6$. This implies (deg $\psi_1)|6$, but we do not know the precise value of deg ψ_1.

Suppose that E is an elliptic curve over $\mathbb{Q}$ without complex multiplication which has a strong Weil parametrization by $\phi(\tau) = \langle\{0,\tau\}, f\rangle$. Then f has Fourier coefficients lying in $\mathbb{Q}$. So in this case, we trivially have $A_f \cong E$. Suppose that ϕ' is any modular parametrization of E. Since E does not have complex multiplication ϕ' must factor as $[u] \cdot \phi$ where $[u]$ denotes multiplication by u on E. Suppose that deg $\phi = c$. Then deg $\phi' = cu^2$. Hence, one can view the degree in this case as a trivial quadratic form in one variable. In comparison, when A_f has dimension two, we obtain that the degrees of modular parametrization are given by the values of a quadratic form in two variables. In chapter 4, we will extend these ideas to other cases. In addition, when A_f has dimension one, the value of the dependency constant is always 1, since the only way to decompose

A_f is to take E exactly isomorphic to A_f.

3.4 Computational Results

We have calculated the degrees of modular parametrization from $X_0(N)$ for a number of $\mathbb{Q}$-curves. In the following table, we list values of N where there exists a cusp form in $S_2(N)$ with an extra twist such that the abelian variety A_f is isogenous to the product of two elliptic curves. The field $L = \mathbb{Q}(\sqrt{r})$ represents the coefficient field of the eigenforms f and f'. The field $K = \mathbb{Q}(\sqrt{t'})$ is the field associated to the character χ. Also the elliptic curve is defined over K. Let $t = \text{disc}\ (K)$. Cremona [2] lists the 9 such examples where $N \leq 300$ and L is an imaginary quadratic field. We expand this list by adding more examples, including 2 examples where L is a real quadratic field. For each entry in the table on the following page, we list $c(g'(u,v))$ where c is a constant and g' is a quadratic form with content 1. The discriminant of g' is listed as Δ. We know that the form g will be a multiple of g', and the integer d divides c. We do not know precisely which of the factors of c belong to d and which belong to g'. In the table, we simply list the product $dg(u,v)$ as $c(g'(u,v))$.

From the computations, a number of striking results are observed. First, the quadratic form g appear to be dependent only on the values of r and t, and not on the level N. In addition, all of the listed quadratic forms are positive definite. The discriminants of these quadratic forms also appears to be closely related to r and t. The remainder of this chapter will be devoted to proving and expanding these observations.

N	r	t	$dg(u,v)$	Δ
63	3	-3	$4(3u^2+v^2)$	-12
81	3	-3	$6(3u^2+v^2)$	-12
117	3	-3	$8(3u^2+v^2)$	-12
189	3	-3	$12(3u^2+v^2)$	-12
243	3	-3	$18(3u^2+v^2)$	-12
98	2	-7	$8(2u^2+uv+v^2)$	-7
196	2	-7	$84(2u^2+uv+v^2)$	-7
160	8	-4	$8(8u^2+4uv+v^2)$	-16
189	7	-3	$252(7u^2+4uv+v^2)$	-12
363	3	-11	$60(5u^2+3uv+v^2)$	-11
363	5	-11	$264(3u^2+uv+v^2)$	-11
387	12	-3	$40(12u^2+v^2)$	-48
169	3	13	$4(6u^2+3uv+2v^2)$	-39
841	5	29	$812(35u^2+20uv+7v^2)$	-580

3.5 Action on $\mathbb{P}^1(\mathbb{Z})$

Let $h \in H$ and let e be an endomorphism such that $eh = 0$. Then if γ is any endomorphism which is not a zero divisor, then $e\overline{\gamma}$ annihilates γh. Hence, the endomorphism γ defines a map on H by sending $h \mapsto \gamma h$. This will induce a map on $\mathbb{P}^1(\mathbb{Z})$.

To understand how this map works, we will introduce a matrix $\beta_e \in M_2(\mathbb{Q})$. Let $e_0, e \in End(A_f) \otimes \mathbb{Q}$ such that e is invertible and

$$\psi(e_0) = \begin{pmatrix} v & -u \\ 0 & 0 \end{pmatrix} \text{ and } \psi(e) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Then

$$\psi(e_0 e) = \begin{pmatrix} av - cu & bv - du \\ 0 & 0 \end{pmatrix}.$$

We can see that $\psi(e_0 e)$ could have been obtained by the transformation

$$u \mapsto du - bv \text{ and } v \mapsto av - cu.$$

We define the matrix β_e using this transformation law. Thus

$$\beta_e = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

which is the adjoint of the matrix $\psi(e)$. Therefore, we have shown that $\beta_e = \psi(\overline{e})$

Since the matrix β_e is designed to act on u, v pairs, the action naturally descends to give an action on $\mathbb{P}^1(\mathbb{Z})$. Hence, this gives an action on the space H. We denote the action of β_e on $(u : v)$ by $\beta_e(u, v)$. If c is any non-zero constant, then note that the two matrices β_e and β_{ce} give the same maps on $\mathbb{P}^1(\mathbb{Z})$.

These actions are useful because they provide information about the relations between the different modular parametrizations. In addition, the action β clearly satisfy the following three properties:

- $\beta_e + \beta_{e'} = \beta_{e+e'}$
- $\beta_e \beta_{e'} = \beta_{e'e}$
- $\beta_{\overline{e}} = \alpha \beta_e^{-1}$ where $\alpha = e\overline{e}$.

3.6 Understanding the Dependency Constant

Let $h_0 \in H$ and let $\gamma_1, \gamma_2, \dots, \gamma_{2g}$ be a $\mathbb{Z}$-basis for $H_1(X_1(N), \mathbb{Z})$. Theorem 9 implies that there is a matrix $Q(u, v)$ which is linear in u and v and complex numbers ν_1 and ν_2 independent of u and v such that

$$Q(u,v) \begin{pmatrix} \nu_1 \\ \\ \nu_2 \end{pmatrix} = \left(\int_{\gamma_i} eh_0(z)dz \right)$$

where eh_0 corresponds to the point $(u : v) \in \mathbb{P}^1(\mathbb{Z})$. However, the values in the i-th row of the matrix $Q(u, v)$ may not be the actual values of $n_1(\gamma_i)$ and $n_2(\gamma_i)$ since ν_1 and ν_2 will not be a basis for eh_0 for all e. Recall $k(u, v)$ was defined to be $\Phi(Q(u, v))$. If $k(u, v) = 1$, then the values of $Q(u, v)$ correspond to the values of n_1 and n_2. If $k(u, v) > 1$, the dependency relation must be removed in order to get the correct values of n_1 and n_2. The process of removing the dependency relation was discussed in Chapter 2. Let E_h denote the elliptic curve which is the image of the modular parametrization given by $\phi(\tau) = \langle \{\tau_0, \tau\}, h \rangle$.

Theorem 11. *L_{eh_0} is a sublattice of L_{h_0} with index equal to $k(u, v)$. Thus, there is an isogeny from E_{h_0} to E_{eh_0} of degree $k(u, v)$.*

Proof. Suppose eh_0 corresponds to the point $(u : v) \in \mathbb{P}^1(\mathbb{Z})$. Let $m = k(u, v)$. Let A and B denote the first and second columns of $Q(u, v)$. Let a and b denote the greatest common divisors of all the entries of A and B respectively. Set $A' = A/a$ and $B' = B/b$ and $m' = m/(ab)$. If $m' > 1$, $A' \equiv kB' \pmod{m'}$ for some $k \in \mathbb{Z}$. Then change A' to $(A' - kB')/m'$. If $m' = 1$, set $k = 1$. Then

$$Q(u, v) = \begin{pmatrix} A' & B' \end{pmatrix} \begin{pmatrix} 1/(am') & 0 \\ k/(bm') & 1/b \end{pmatrix}^{-1}.$$

Thus

$$\begin{pmatrix} A' & B' \end{pmatrix} \begin{pmatrix} am' & 0 \\ -ak & b \end{pmatrix} \begin{pmatrix} \nu_1 \\ \nu_2 \end{pmatrix} = \begin{pmatrix} \int_{\gamma_i} eh_0 \end{pmatrix}$$

$$\begin{pmatrix} A' & B' \end{pmatrix} \begin{pmatrix} am'\nu_1 \\ -ak\nu_1 + b\nu_2 \end{pmatrix} = \begin{pmatrix} \int_{\gamma_i} eh_0 \end{pmatrix}$$

Therefore, a basis for L_{eh_0} is given by $\omega_1 = am'\nu_1$ and $\omega_2 = -ak\nu_1 + b\nu_2$. Thus the index of L_{eh_0} in L_{h_0} is $abm' = m = k(u, v)$. $\square$

3.7 Determining the Quadratic Form

Let $\phi(\tau) = \langle \{\tau, \tau_0\}, h\rangle$ for some $h \in H$. Suppose that $e \in End(A_f)$. Then define $\phi^e(\tau) = \langle \{\tau, \tau_0\}, eh\rangle$. Let E^e be the elliptic curve which is the image of ϕ^e.

Theorem 12.

1. *deg* $\phi =$ *deg* ϕ^{T_p}.

2. *Suppose* $\eta^2 = t$ *where* $|t|$ *is a prime. Then one of the following is true:*

   (a) *deg* $\phi =$ *deg* ϕ^η *and* E *and* E^η *are not isomorphic.*

(b) $deg\ \phi = |t|\ deg\ \phi^{\eta}$ and $E \cong E^{\eta}$.

(c) $|t|\ deg\ \phi = \ deg\ \phi^{\eta}$ and $E \cong E^{\eta}$.

Proof. (1) Let $h = mf + nf'$. Then $T_p(h) = \sqrt{r}(mf - nf')$. Suppose $e = a + bT_p + c\eta + dT_p\eta$ is an endomorphism such that $eh = 0$. Let σ be the non-trivial Galois automorphism of $\mathbb{Q}(\sqrt{t})$. Then $e^{\sigma} = a + bT_p - c\eta - dT_p\eta$. We can choose $m = \sqrt{t}$ and $n = -\frac{a+b\sqrt{r}}{c+d\sqrt{r}}$ so that $e^{\sigma}(mf - nf') = 0$. Thus $e^{\sigma}(T_p(h)) = 0$. This means that the action of T_p on H corresponds to the action of the Galois automorphism σ. Hence, E^{T_p} can be naturally identified with E^{σ}. Since $A_f \to A_f/eA_f$ is an algebraic map, applying a Galois action to the map will not change the degree.

(2) Let $h = mf + nf'$. Then $\eta(h) = \sqrt{t}(nf + mf')$. Note that $h \otimes \chi = m(f \otimes \chi) + n(f' \otimes \chi) = (mf' + nf)$. Thus $\eta(h) = \sqrt{t}(h \otimes \chi)$. To determine how the two degrees are related, we use Zagier's result in Theorem 5 which says

$$\text{deg } (\phi) = 4\pi^2 \frac{||h||^2}{\text{Vol } E}.$$

Following the arguments in Zagier [23] and Edixhoven [7], our goal is to determine how the degree changes when h switches to $\eta(h)$ by observing how the Petersson norms and the volume of the period lattices differ. Suppose $h(z) = \sum_{n=1}^{\infty} a_n q^n$ is a cusp form for $\Gamma_0(N)$. Rankin's formula gives

$$||h||^2 = \frac{1}{48\pi}[SL_2(\mathbb{Z}) : \Gamma_0(N)] Res_{s=2} \sum_{n=1}^{\infty} \frac{|a_n|^2}{n^s}.$$

Therefore, $||h \otimes \chi||^2 = ||h||^2$. If h is a cusp form for $\Gamma_1(N)$, then we obtain the same result since

$$||h||^2 = C \cdot Res_{s=2} \sum_{n=1}^{\infty} \frac{|a_n|^2}{n^s}$$

where C is a constant depending on the volume of the fundamental domain of $X_1(N)$. Also,

$$h \otimes \chi(z) = \frac{g(\chi)}{t} \sum_{k=0}^{t-1} \chi(-k) h(z + \frac{k}{t})$$

where $g(\chi)$ denotes the Gauss sum. Let Λ be the period lattice of h, and let Λ' be the period lattice for $\eta(h)$. Then one can easily see from the above formula for $h \otimes \chi$ that

$$g(\chi)\Lambda \subset \Lambda' \subset g(\chi)^{-1}\Lambda,$$

and

$$t\Lambda \subset g(\chi)\Lambda' \subset \Lambda.$$

Let $v_1 =$ Vol Λ and $v_2 =$ Vol Λ'. Then by taking the volumes from the inclusions above, we obtain $tv_2 = k_1 v_1$ and $t^2 v_1 = k_2 t v_2$ for some positive integers k_1 and k_2. This yields $k_1 k_2 = t^2$. Since t is prime, this yields three possibilities. If $k_1 = k_2 = t$, then $v_1 = v_2$. Since the volume and Petersson norm do not change, deg $\phi =$ deg ϕ^η. Since $[\Lambda : g(\chi)\Lambda'] = t$, the lattices Λ and Λ' are not isomorphic and so E and E^η are not isomorphic. In the other two cases, either $v_1 = tv_2$ or $tv_1 = v_2$. Since the volumes change by a factor of t, the degrees must change be that same factor of t. Also Λ' and Λ are homothetic. Therefore, $E \cong E^\eta$.

$\square$

Suppose that M is the action on $\mathbb{P}^1(\mathbb{Z})$ corresponding to either T_p, η, or $T_p\eta$. Then the above theorem shows that

$$\text{deg } \phi(u,v) = c \text{ deg } \phi(M(u,v)) \text{ and}$$
$$d\frac{g(u,v)}{k(u,v)} = cd\frac{g(M(u,v))}{k(M(u,v))}$$

where c is an integer or the reciprocal of an integer. Then

$$g(M(u,v)) = \frac{k(M(u,v))}{c\ k(u,v)} g(u,v) = \alpha_M g(u,v)$$

where α_M is some constant depending on the action M. In order to determine the form $g(u,v)$, the next step is to determine the set of binary quadratic forms which satisfy the relation $g(M(u,v)) = \alpha_M g(u,v)$ where $M = \beta_{T_p}, \beta_\eta$, and $\beta_{T_p\eta}$.

Let the triple (a,b,c) denote the binary quadratic form $au^2+buv+v^2$. The set of binary quadratic forms with rational coefficients is isomorphic to the $\mathbb{Q}-$vector space $\mathbb{Q}^3$. Our interest for the moment is in binary quadratic forms up to a scalar multiple. Hence, the triple (a,b,c) can be interpreted as a line through the origin in $\mathbb{Z}^3$.

Lemma 3. *Let $M \in M_2(\mathbb{Z})$ be a non-scalar matrix such that $M^2 = \mu I$ with $\mu \neq 0$. Let $w = (u,v)$. Suppose $g(Mw) = \epsilon g(w)$. Then $\epsilon = \pm\mu$. Also, the space of binary quadratic forms such that*

$$g(Mw) = -\mu g(w)$$

is one-dimensional. The space of binary quadratic forms such that

$$g(Mw) = \mu g(w)$$

is two-dimensional.

Proof. Let $g = (s_1, s_2, s_3)$. Suppose $g(M(u,v)) = \epsilon g(u,v)$. Since $M^2 = \mu I$ and

M is not a scalar, M has the form $\begin{pmatrix} a & b \\ c & -a \end{pmatrix}$ where $a^2 + bc = \mu$. Then

$$\begin{aligned} g(M(u,v)) &= g(au + bv, cu - av) \\ &= u^2(s_1(a^2) + s_2(ac) + s_3(c^2)) \\ &+ uv(s_1(2ab) + s_2(bc - a^2) + s_3(-2ac)) \\ &+ v^2(s_1(b^2) + s_2(-ab) + s_3(a^2)) \\ &= \epsilon(s_1u^2 + s_2uv + s_3v^2) \end{aligned}$$

for all (u,v). Using the last equality, the coefficients of the u^2 terms, the uv terms, and the v^2 terms must be equal. This yields the following matrix equation.

$$\begin{pmatrix} a^2 & ac & c^2 \\ 2ab & bc - a^2 & -2ac \\ b^2 & -ab & a^2 \end{pmatrix} \begin{pmatrix} s_1 \\ s_2 \\ s_3 \end{pmatrix} = \epsilon \begin{pmatrix} s_1 \\ s_2 \\ s_3 \end{pmatrix}.$$

Hence ϵ must be an eigenvalue and the form g must be an eigenvector. A direct computation shows that $-\mu = -a^2 - bc$ is an eigenvalue with multiplicity one. The associated eigenvector is $(-c, 2a, b)$. Also $\mu = a^2 + bc$ is an eigenvalue with multiplicity two. Its eigenspace is spanned by $(c, 0, b)$ and $(a, b, 0)$. $\square$

Lemma 4. *Let $M_i \in M_2(\mathbb{Z})$ such that $M_i^2 = \mu_i I$ and $\mu_i \neq 0$ for $i = 1, 2$ and $M_1M_2 = -M_2M_1$. Let $w = (u,v)$. Suppose that $g(M_iw) = \epsilon_i g(w)$ for $i = 1$ and 2, and $g((M_1M_2)w) = \epsilon_3 g(w)$ for some ϵ_1, ϵ_2, and ϵ_3. Then $\epsilon_1 = \pm\mu_1$, $\epsilon_2 = \pm\mu_2$, and $\epsilon_3 = \pm\mu_1\mu_2$. The forms g that satisfy the above properties are contained in three one-dimensional subspaces of binary quadratic forms over $\mathbb{Q}$. In addition, the discriminants of each of these three sets of quadratic forms are $\mu_1 z_1^2, \mu_2 z_2^2$, and $-\mu_1\mu_2 z_3^2$ for some integers z_1, z_2, z_3.*

Proof. Note that the algebra generated by all sums and products of M_1 and M_2 over $\mathbb{Q}$ is a quaternion algebra, and it generates all of $M_2(\mathbb{Q})$. Set $r = \mu_1$. Then we can choose M_1 to have rational canonical form:

$$M_1 = \begin{pmatrix} 0 & 1 \\ r & 0 \end{pmatrix}.$$

There exists $a, b \in \mathbb{Q}$ such that $\mu_2 = a^2 - rb^2$. Then the condition on M_2 force

$$M_2 = \begin{pmatrix} a & b \\ -rb & -a \end{pmatrix}.$$

Since $g(M_1 w) = \epsilon_1 g(w)$, the previous lemma states that g must be in $L_1 = \langle(-r, 0, 1)\rangle$ or $P_1 = \langle(r, 0, 1), (0, 1, 0)\rangle$. Now the same lemma can be applied to M_2. Hence g is in $L_2 = \langle(rb, 2a, b)\rangle$ or $P_2 = \langle(-r, 0, 1), (a, b, 0)\rangle$. Finally, apply the lemma to M_1M_2 to see that g is in $L_3 = \langle(ra, 2rb, a)\rangle$ or $P_3 = \langle(-r, 0, 1), (rb, a, 0)\rangle$. Therefore, $g \in (L_1 \cup P_1) \cap (L_2 \cup P_2) \cap (L_3 \cup P_3)$. After careful examination of these spaces, one can see that this intersection is precisely $L_1 \cup L_2 \cup L_3$. Therefore, we get three one-dimensional spaces. By computing the discriminants of each, we get the above result. $\square$

Theorem 13. *The binary quadratic form $g(u, v)$ is positive definite.*

Proof. The result of the degree calculation algorithm is always positive because of the absolute value sign. Without taking the absolute value, the degree may be positive or negative, depending on the ordering of the two basis elements of the lattice. In order to show that $g(u, v)$ is positive definite, it is necessary and sufficient to show that the result of the degree calculation without taking the absolute value has the same sign for all (u, v). In Theorem 7, we require that the basis for the period lattice $\{\omega_1, \omega_2\}$ be chosen so that Im $\frac{\omega_2}{\omega_1} > 0$. Suppose

$h_0 \in H$ corresponds to a point $(u_0 : v_0)$. For any other $h \in H$, there exists an $e \in End(A_f)$ such that $h = eh_0$ up to a constant multiple. So assume that h is scaled so that $h = eh_0$. Let $\{\nu_1, \nu_2\}$ be the basis for the lattice L_{h_0} obtained by using the degree calculation algorithm. Lemma 11 implies that L_h is a sublattice of L_{h_0}. In addition, the proof of that lemma shows that the basis for the lattice L_h obtained by the degree calculation algorithm is $\{\omega_1, \omega_2\}$ where $\omega_1 = am'\nu_1$ and $\omega_2 = -ak\nu_1 + b\nu_2$ for some positive integers a, b, k, and m'. Then

$$\begin{aligned}
\mathrm{Im}\ (\frac{\omega_2}{\omega_1}) &= \mathrm{Im}\ (\frac{-ak\nu_1 + b\nu_2}{am'\nu_1}) \\
&= \mathrm{Im}\ (-\frac{k}{m'} + \frac{b}{am'}\frac{\nu_2}{\nu_1}) \\
&= \frac{b}{am'}\mathrm{Im}\ (\frac{\nu_2}{\nu_1}).
\end{aligned}$$

Since b, a, and m' are positive, the sign of Im $\frac{\nu_2}{\nu_1}$ is the same as the sign of Im $\frac{\omega_2}{\omega_1}$. Therefore, the result of the degree calculation algorithm will have the same sign for all values of $(u : v)$. Since the degree is positive, the quadratic form must be positive definite. $\square$

Theorem 14. *The quadratic form $g(u, v)$ is uniquely determined up to a constant multiple by choosing an isomorphism between $\left(\frac{r,t}{\mathbb{Q}}\right)$ and $M_2(\mathbb{Q})$. In other words, the class of the quadratic form is uniquely determined up to a constant multiple by the unique imaginary quadratic field in the list $\mathbb{Q}(\sqrt{r}), \mathbb{Q}(\sqrt{t})$, and $\mathbb{Q}(\sqrt{-rt})$.*

Proof. Lemma 4 shows that g could be one of three quadratic forms up to a scalar multiple. A result of Ribet shows that at least one of the 2 fields $\mathbb{Q}(\sqrt{r})$ or $\mathbb{Q}(\sqrt{t})$ is a real quadratic field [15]. Therefore, exactly one of the three quadratic fields will be imaginary. Since $T_p^2 = rz_1^2$, $\eta^2 = tz_2^2$, and $(T_p\eta)^2 = -rtz_3^2$ for some integers z_1, z_2, and z_3, exactly one of these endomorphisms has a negative square.

Therefore, Lemma 4 implies that exactly one of the three quadratic forms must be positive definite. $\square$

3.8 Examples of $\mathbb{Q}$-curves

For each $h \in H$, we obtain a strong Weil parametrization of some $\mathbb{Q}$-curve. By Theorem 11, we know that all of the resulting $\mathbb{Q}$-curves are isogenous. However, we do not know how many of them are isomorphic. In this section, we will present some examples which illustrate the different elliptic curves obtained from $X_0(N)$ and their relationship to the quadratic form and the dependency constant. Numerical evidence also shows that the following conjecture holds.

Conjecture 1. *Let $h_i \in H$ correspond to $(u_i : v_i) \in \mathbb{P}^1(\mathbb{Z})$ for $i = 1, 2$. Let ℓ be the square-free part of $k(u_1, v_1) \cdot k(u_2, v_2)$. Then E_{h_1} and E_{h_2} are ℓ-isogenous.*

If the conjecture holds, then the the number non-isomorphic elliptic curves of the form A_f/eA_f, is reduced to the number of non-square values of $k(u, v)$ where u and v are relatively prime.

Consider the case where $N = 98$ and $f \in S_2(98)$ is a newform with an extra twist. Then

$$f = q + q^2 + \sqrt{2}q^3 + q^4 - 2\sqrt{2}q^5 + \sqrt{2}q^6 + q^8 + \cdots$$
$$f' = q + q^2 - \sqrt{2}q^3 + q^4 + 2\sqrt{2}q^5 - \sqrt{2}q^6 + q^8 + \cdots$$

where $f' = f \otimes \chi$ and $\chi(n) = (\frac{-7}{n})$. We will see that there are exactly 4 non-isomorphic $\mathbb{Q}$-curves which have a modular parametrization from $X_0(98)$. Define the isomorphism ψ between $End(A_f) \otimes \mathbb{Q}$ and $M_2(\mathbb{Q})$ by

$$\psi(T_3) = \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix} \qquad \psi(\eta) = \begin{pmatrix} 1 & 2 \\ -4 & -1 \end{pmatrix}.$$

Then the endomorphism $e = (7v) - (7u)T_3 - (4u+v)\eta - (u+2v)T_3\eta$ corresponds to a rank one matrix. Using this isomorphism we obtain for all u and v relatively prime that

$$\deg\ \phi(u,v) = \frac{8(2u^2+uv+v^2)}{k(u,v)},$$

where

$$k(u,v) = \begin{cases} 2, & \text{if } v \equiv 0 \pmod 2 \text{ and } v \not\equiv -4u \pmod 7, \\ 7, & \text{if } v \not\equiv 0 \pmod 2 \text{ and } v \equiv -4u \pmod 7, \\ 14, & \text{if } v \equiv 0 \pmod 2 \text{ and } v \equiv -4u \pmod 7, \\ 1, & \text{otherwise.} \end{cases}$$

In the following table, we will list some values of $(u:v) \in \mathbb{P}^1(\mathbb{Z})$ in a meaningful manner. In the first column, we will list some values where $k(u,v) = 1$. In the second column, we apply β_{T_2} to the first column. The third column is obtained by applying β_η to the first column. Finally, we apply $\beta_{T_2\eta}$ to the first column to obtain the fourth column.

$(u:v)$	$\beta_{T_3}(u:v)$	$\beta_\eta(u:v)$	$\beta_{T_3\eta}(u:v)$
$(0:1)$	$(1:0)$	$(-2:1)$	$(-1:4)$
$(1:1)$	$(1:2)$	$(-3:5)$	$(-5:6)$
$(2:1)$	$(1:4)$	$(-4:9)$	$(-9:8)$
$(2:3)$	$(3:4)$	$(-8:11)$	$(-11:16)$

Note that the $k(u,v)$ values for entries are 1, 2, 7, 14 for the first, second, third, and fourth columns respectively. By computing $g(u,v)$ for each entry on the same row, we see that $g(u,v)$ increases by a factor of 2, 7, and 14 from the first column to the second, third and fourth columns respectively. Hence, all of the $(u:v)$ values on the same row give modular parametrizations with the same degree by Theorem 12. By Theorem 11, we also see that an elliptic curve given by an entry in the first column is 7-isogenous to the corresponding elliptic curve in the third column. Hence, we have isogenies from an elliptic curve in the first column to each curve in the other columns with degree 2, 7, and 14. Therefore, there are at least 4 elliptic curves of the form A_f/eA_f. Also, Theorem 11 implies that all of entries within a column produce isomorphic $\mathbb{Q}$-curves. Therefore, all the elliptic curves produced by entries of a column are isomorphic, and so there are exactly 4 elliptic curves of the form A_f/eA_f.

By computing an approximation to the period lattice for each entry on a row, we can determine an approximation for the j-invariant. We see that

$$j_1 \approx 1722.3416\ldots - 151.4187\ldots i$$
$$j_2 \approx 1722.3416\ldots + 151.4187\ldots i$$
$$j_3 \approx -1316.1242\ldots - 5447.2714\ldots i$$
$$j_4 \approx -1316.1242\ldots + 5447.2714\ldots i$$

where j_i corresponds to the i-th column. Suppose A_f/eA_f corresponds to the elliptic curve in the first column. We know that it is 2-isogenous to its Galois conjugate. Therefore, it is one of the curves on the list in Theorem 3. In order to find the curve on the list, we need to find the correct value of m. Also $A_f/e\eta A_f$ is 2-isogenous to its Galois conjugate. We know that $A_f/e\eta A_f$ and its conjugate must correspond to substituting $m = \pm 13/343$. Roberts has shown that this elliptic curve is modular and that it has a modular parametrization from $X_0(98)$ [16]. By performing a search for the correct $\mathbb{Q}$-curve that corresponds to A_f/eA_f and its conjugate, we strongly suspect that we should substitute $m = \pm 181/49$ into the equation in Theorem 3. If true, this could probably be verified using the methods of [17].

Not all examples of modular parametrizations of $\mathbb{Q}$-curves from $X_0(N)$ give rise to 4 elliptic curves. In our previous example with $N = 81$, we find that there are only three possible values of $k(u,v)$ with u and v relatively prime. Those are $1, 3$ and 9. Once again there are at most 4 elliptic curves of the form A_f/eA_f. However, computing numerical approximations for j-invariants suggest that E_h and $E_{T_2\eta h}$ are isomorphic, and E_{T_2h} and $E_{\eta h}$ are isomorphic. This would imply that there are only 2 non-isomorphic curves of the form A_f/eA_f which agrees with the conjecture. Also the curves E_h and E_{T_2h} are 3-isogenous, since E_{T_2h} can be identified with the Galois conjugate of E_h. Also E_h is 9-isogenous to $E_{T_2\eta h}$. Since these curves are believed to be isomorphic, the isogeny should be the multiplication by 3 map.

3.9 Further Questions

In the previous sections, we have discussed the roles of the quadratic form $g(u,v)$ and the dependency constant $k(u,v)$ in the degree. Now we turn our attention to the integer d. Recall that d is the degree of the map ψ_1 from $X_1(N)$ to A_f. First, consider the case where E is a non-CM elliptic curve over $\mathbb{Q}$ which has a strong Weil parametrization ϕ. The degree of ϕ is simply the integer d. Let ϕ' be any modular parametrization of E. Then ϕ' factors through ϕ. Thus deg $\phi' = du^2$ for some integer u. Hence, we can see that the degree in this case is given by a trivial quadratic form in one variable. So we see that our result concerning the degree of a strong Weil parametrization extends this idea.

Let f be an eigenform for $\Gamma_1(N)$, and let S denote the span of f and its Galois conjugates. Let T be the orthogonal complement of S with respect to the

Petersson inner product. Then $S \oplus T$ is the set of cusp forms for $\Gamma_1(N)$. We say that a prime $p \in \mathbb{Z}$ is a congruence prime for f if and only if there is an eigenform $g \in T$ such that $f \equiv g \pmod{\mathcal{P}}$ where $\mathcal{P}$ is a prime ideal of $\mathcal{O}$ lying above p where $\mathcal{O}$ is the ring of integers in the field obtained by adjoining the coefficients of f and g. In [23], there is the result that if $\phi(\tau) = \langle\{\tau_0, \tau\}, f\rangle$ is a strong Weil parametrization of an elliptic curve E defined over $\mathbb{Q}$, then the congruence primes for f are precisely the primes which divide the degree of ϕ.

As an extension of this result, we have the following conjecture.

Conjecture 2. *Let $\psi_1 : X_1(N) \to A_f$ be the map given by*

$$\tau \mapsto (\langle\{\tau_0, \tau\}, f\rangle, \langle\{\tau_0, \tau\}, f'\rangle).$$

Let $d = deg\ \psi_1$. Let K be the field of definition for E. If $p|d$, then p is a congruence prime for f. If p is a congruence prime for f, then either $p|d$ or $p|disc(K)$.

In support of this conjecture, we have some numerical evidence. In the case where $N = 63$, $S_2(63)$ has dimension 5. A result of Doi and Ohta is useful for determining if certain values are congruence primes. Suppose that $p \nmid N$ and $f = \sum a_n q^n$ and $g = \sum b_n q^n$ are two eigenforms for $\Gamma_0(N)$. Let $\mathcal{P}$ be a prime ideal lying above p If $a_q \equiv b_q \pmod{\mathcal{P}}$ for all $q \leq 2g(X_0(N)) - 1$, then $a_n \equiv b_n \pmod{\mathcal{P}}$ for all n [6]. Let f be one of the two eigenforms in $S_2(63)$ such that which has coefficients lying in $\mathbb{Q}(\sqrt{3})$ with an extra twist. We can use the result of Doi and Ohto to show that 2 is a congruence prime for f. In fact, by examining the 5 eigenforms, we can verify that 2 is the only congruence prime. In the degree calculation, we know that the product $dg(u, v) = 4(3u^2 + v^2)$. Hence, $d|4$.

Now let us examine the case where $N = 81$. $S_2(81)$ has dimension 4. Let

$$f = q + \sqrt{3}q^2 + q^4 - \sqrt{3}q^5 + 2q^7 - \sqrt{3}q^8 + \cdots$$

Calculation shows that the only possible congruence prime is 3. Doi and Ohta's result cannot be used since $3|81$. By computing the first 200 coefficients of f and another eigenform, we can verify that 3 appears to be a congruence prime. Using the degree calculation algorithm, we know that $d|6$. If the conjecture is true, then $d = 3$ and $g(u, v) = 2(3u^2 + v^2)$, which is reasonable.

Consider the modular parametrizations from $X_0(169)$. The space of cusp forms for $\Gamma_0(N)$ is eight-dimensional and can be decomposed by $\langle f, f' \rangle \oplus T$ where T is a six-dimensional space, and $f' = f \otimes \chi$. Let g be any one of the 6 eigenforms in T. Then let L be the extension of $\mathbb{Q}$ obtained by adjoining the coefficients of f and g. Then $[L : \mathbb{Q}] = 6$. Let $\mathcal{O}_L$ denote the ring of integers in L. If $f = \sum a_n q^n$ and $g = \sum b_n q^n$, then $a_p \equiv b_p \pmod{\mathcal{P}}$ for the first 25 primes p where $\mathcal{P}$ is a prime lying above 13. In addition, 13 is the only possible congruence prime. In this example, $\operatorname{disc}(K) = 13$. By computing the degree of modular parametrization we see that

$$\deg \phi(u, v) = 4\,\frac{6u^2 + 3uv + 2v^2}{k(u, v)}.$$

The integer d must divide the greatest common divisor over all of the possible degrees. Hence, $d|4$. However, when $(u : v) = (1 : 1)$, then $\deg \phi(1, 1) = 11$. Therefore, $d = 1$, and $X_0(169)$ injects into A_f, which supports the conjecture.

Not only does the integer d appear to be related to the congruence primes, it also seems to be closely related to the intersection numbers of the abelian variety A_f. X. Wang calculates the intersection numbers e_1 and e_2 of several principally polarized two-dimensional abelian varieties A_f [20]. In these cases, $e_1 = e_2$.

There are three examples of Wang's which were isogenous to the product of two $\mathbb{Q}$-curves. For $N = 63$, Wang calculates $e_1 = e_2 = 2$ and the degree calculation algorithm shows that $d|4$. For $N = 117$, we have $e_1 = e_2 = 4$ and $d|8$. For $N = 189$ and $L = \mathbb{Q}(\sqrt{3})$, we have $e_1 = e_2 = 6$ and $d|12$. This data suggests a strong correlation between the intersection numbers and the value of d in the degree. It still remains to make this relationship precise.

Chapter 4

Modular Parametrizations and Higher Dimensional Abelian Varieties

Not all $\mathbb{Q}$-curves defined over quadratic fields are isomorphic to A_f/eA_f where A_f is some two-dimensional abelian variety and f is an eigenform with an extra twist, even though all $\mathbb{Q}$-curves over quadratic fields with a parametrization from $X_0(N)$ are obtained in this way. Let E be a $\mathbb{Q}$-curve defined over a $\mathbb{Q}(\sqrt{t})$, and let E^σ denote its Galois conjugate. We start by investigating abelian varieties with large endomorphism algebras which have E as a simple factor. Assuming that E is modular, our goal is to determine the dimension of the smallest A_f, where f is an eigenform, such that E is a simple factor of A_f.

4.1 Abelian Varieties of GL_2-type

An abelian variety A defined over $\mathbb{Q}$ is of GL_2-type if $End_{\mathbb{Q}}(A) \otimes \mathbb{Q}$ is a number field of degree equal to the dimension of A. If f is an eigenform for $\Gamma_1(N)$, then the abelian variety A_f is of GL_2-type. A result of Ribet [15] and extended by Pyle [14] states that for any $\mathbb{Q}$-curve E , there exists an abelian variety of GL_2-type with E as a simple factor. In this section, we will attempt to determine the dimension of the smallest abelian variety of GL_2-type which contains E as a simple factor. Then assuming that E is modular, this gives information concerning the dimension of A_f with A_f/eA_f isogenous to E for some $e \in End(A_f)$. The following is a result of Ribet which determines which $\mathbb{Q}$-curves defined over quadratic fields are factors of a two-dimensional abelian variety of GL_2-type. [15]

Theorem 15. *Let E be a non-CM $\mathbb{Q}$-curve defined over $K = \mathbb{Q}(\sqrt{t})$. Suppose E and its Galois conjugate E^σ are r-isogenous and that the isogeny between the two curves is defined over K. Then there exists a two-dimensional abelian variety A of GL_2-type with E as a simple factor of A and $End_{\mathbb{Q}}(A) \otimes \mathbb{Q} = \mathbb{Q}(\sqrt{r})$ or $\mathbb{Q}(\sqrt{-r})$.*

Let E be a $\mathbb{Q}$-curve defined over $K = \mathbb{Q}(\sqrt{t})$ which is either 2 or 3 isogenous to its Galois conjugate. Using Roberts' results we can determine if there is a twist of E such that the isogeny is defined over K. Let $(a, b)_p$ denote the Hilbert symbol. That is $(a, b)_p = 1$ if and only if $a = x^2 - by^2$ has a solution for x and y in $\mathbb{Q}_p$. Otherwise, $(a, b)_p = -1$. Let $(a, b) = 1$ if and only if $a = x^2 - by^2$ has a solution for x and y in $\mathbb{Q}$. Otherwise, $(a, b) = -1$. Using these Hilbert symbols, we can rewrite the condition in Theorems 3 and 4 which determines if the isogeny can be defined over the field K. The isogeny can be defined over K if and only if either $(-r, t) = 1$ or $(r, t) = 1$, where $r = 2$ in Theorem 3 and $r = 3$ in Theorem 4.

Suppose that for all twists of E and E^σ, the isogeny between these two curves is not defined over K. Let L denote the field of definition for the isogeny between E and E^σ. In the case when the isogeny is either degree 2 or 3, $L = \mathbb{Q}(\sqrt{t}, \sqrt{-rA})$ where where r is either 2 or 3 respectively and $A = x^2 - ty^2$ for some $x, y \in \mathbb{Q}$.

The field L is not unique. It depends on the value of A which is the norm of D in Theorems 3 and 4. In general, we will assume that L is this extension.

Let $G_{\mathbb{Q}} = \text{Gal}\,(\overline{\mathbb{Q}}/\mathbb{Q})$. For each $\sigma \in G_{\mathbb{Q}}$, we define a collection of isogenies

$$\{\mu_\sigma : E^\sigma \to E\},$$

such that $\mu_\sigma = \mu_\gamma$ if and only if $E^\sigma = E^\gamma$. Suppose that $\tau \in G_{\mathbb{Q}}$, then τ acts on an isogeny μ_σ by

$$\mu_\sigma^\tau : E^{\tau\sigma} \to E^\tau$$

where $E^{\tau\sigma}$ means $(E^\sigma)^\tau$.

We will be working with abelian varieties defined up to isogeny. So we are working in the category whose objects are abelian varieties, say A_1 and A_2, with morphisms $Hom(A_1, A_2) \otimes \mathbb{Q}$. So we can formally invert any isogeny. Then we are able to define a function from $G_{\mathbb{Q}} \times G_{\mathbb{Q}}$ to $End(E)$ as follows:

$$c(\sigma, \tau) = \mu_\sigma \circ \mu_\tau^\sigma \circ \mu_{\sigma\tau}^{-1}.$$

$c(\sigma, \tau)$ is an element of $End(E)$. Since E does not have complex multiplication, $c(\sigma, \tau) \in \mathbb{Q}^\times$. Also, c is a locally constant two-cocycle on $G_{\mathbb{Q}}$. Changing the system of isogenies above will change c by a coboundary. Therefore, for each $\mathbb{Q}$-curve E,we obtain a well-defined element $[c] \in H^2(G_{\mathbb{Q}}, \mathbb{Q}^\times)$, where the action of $G_{\mathbb{Q}}$ on $\mathbb{Q}^\times$ is trivial.

A result of Tate (see [18]) says that the cohomology group $H^2(G_{\mathbb{Q}}, \overline{\mathbb{Q}}^\times) = 1$. Thus, our cocycle $[c]$ becomes trivial in $H^2(G_{\mathbb{Q}}, \overline{\mathbb{Q}}^\times)$. That is, there exists a locally constant function $\beta : G_{\mathbb{Q}} \to \overline{\mathbb{Q}}^\times$ such that

$$c(\sigma, \tau) = \frac{\beta(\sigma)\beta(\tau)}{\beta(\sigma\tau)} \text{ for all } \sigma, \tau \in G_{\mathbb{Q}}.$$

Let B be the extension of $\mathbb{Q}$ obtained by adjoining the values of $\beta(\sigma)$ for all $\sigma \in G_{\mathbb{Q}}$. The main result of Pyle's thesis states that there exists an abelian variety of GL_2-type which contains E as a simple factor and $End_{\mathbb{Q}}(A) \otimes \mathbb{Q} \cong B$ [14]. Assuming that E is modular, we see that $A \cong A_f$ for some eigenform f for $\Gamma_1(N)$ with coefficient field equal to B. Given a $\mathbb{Q}$-curve E, our task is to determine the smallest possible abelian variety of GL_2-type containing E as a simple factor and the corresponding field B.

Let Gal $(K/\mathbb{Q}) = \{1, \sigma\}$. Since E is defined over K, we only need two isogenies in our system.

$$\mu_1 = id : E \to E,$$
$$\mu := \mu_\sigma : E^\sigma \to E.$$

Let Gal $(L/\mathbb{Q}) = \{1, \sigma, \tau, \sigma\tau\}$, where τ fixes the field K.

Lemma 5. *We have the following properties:*

- $\mu\mu^\sigma = a$
- $\mu^\tau = -\mu$
- $\mu^{\sigma\tau} = \mu^{\tau\sigma} = -\mu^\sigma$

where $|a| = deg\ \mu$. *Using these relations we obtain the values of the cocycle* $c \in H^2(G_{\mathbb{Q}}, \mathbb{Q}^\times)$ *in the following table.*

$c(g,h)$	1	σ	τ	$\sigma\tau$
1	1	1	1	1
σ	1	a	1	a
τ	1	-1	1	-1
$\sigma\tau$	1	$-a$	1	$-a$

Proof. The first statement is true by definition. The isogeny μ^τ is a map from $E^{\tau\sigma}$ to E^τ. Since E is defined over K and τ fixes K, μ^τ is an isogeny from E^σ to E. Since E and E^σ do not have complex multiplication, $k_1\mu^\tau = k_2\mu$ for some $k_1, k_2 \in \mathbb{Z}$. We have that

$$k_1\mu^{\sigma\tau} = (k_1\mu^\tau)^\sigma = (k_2\mu)^\sigma = k_2\mu^\sigma.$$

Also,

$$\begin{aligned} k_1^2\mu^\sigma &= k_1(k_1\mu^{\sigma\tau})^\tau \\ &= k_1(k_2\mu^\sigma)^\tau \\ &= k_2(k_1\mu^{\tau\sigma}) \\ &= k_2^2\mu^\sigma. \end{aligned}$$

Therefore $k_2 = \pm k_1$. If $\mu^\tau = \mu$, μ is defined over K. Therefore $\mu^\tau = -\mu$. The fourth statement follows directly from the third. For any $g, h \in H^2(G_{\mathbb{Q}}, \mathbb{Q}^\times)$, we can now calculate the value of the cocycle $c(g,h) = \mu_g \circ \mu_h^g \circ \mu_{gh}^{-1}$ using the above properties. This completes the values in the table. □

Since $c(\sigma,\tau) \neq c(\tau,\sigma)$, the cocycle $[c] \in H^2(\text{Gal }(L/\mathbb{Q}), \overline{\mathbb{Q}}^\times)$ is not trivial. In order to trivialize the cocycle, we need to find an extension F of L which is non-abelian over $\mathbb{Q}$ such that $[c] = 1$ in $H^2(\text{Gal }(F/\mathbb{Q}), \overline{\mathbb{Q}}^\times)$. Thus, the extensions of σ and τ from L to F must not commute.

Our goal is to determine the set of biquadratic fields L which can be embedded into a non-abelian extension F over $\mathbb{Q}$ of degree 8 or 16 such that the cocycle $[c]$ becomes trivial when extend to the Galois group of $F/\mathbb{Q}$. First, we list all non-abelian groups of order 8 or 16.

$$\begin{aligned} D_4 &= \{x, y \,|\, x^4 = y^2 = 1, y^{-1}xy = x^{-1}\} \\ Q_8 &= \{x, y \,|\, x^4 = y^4 = 1, y^{-1}xy = x^{-1}, x^2 = y^2\} \end{aligned}$$

$$
\begin{aligned}
D_8 &= \{x, y \mid x^8 = y^2 = 1, y^{-1}xy = x^{-1}\} \\
Q_{16} &= \{x, y \mid x^8 = y^4 = 1, y^{-1}xy = x^{-1}, y^2 = x^4\} \\
SD_8 &= \{x, y \mid x^8 = y^2 = 1, y^{-1}xy = x^3\} \\
M_{16} &= \{x, y \mid x^8 = y^2 = 1, y^{-1}xy = x^5\} \\
Q \curlywedge C &= \{x, y \mid x^4 = y^4 = 1, y^{-1}xy = x^{-1}\} \\
DC &= \{x, y, z \mid x^2 = y^2 = z^4 = 1, y^{-1}xy = xz^2, [x, z] = [y, z] = 1\} \\
D \curlywedge C &= \{x, y, z \mid x^4 = y^2 = z^2 = 1, y^{-1}xy = xz, [x, z] = [y, z] = 1\}
\end{aligned}
$$

Theorem 16. *Suppose that $K = \mathbb{Q}(\sqrt{t})$ and $L = \mathbb{Q}(\sqrt{t}, \sqrt{-rA})$ where A is a norm from K. Suppose that for some value of A, L can be embedded into an extension F such that either*

1. *Gal $(F/\mathbb{Q}) = D_4$ and Gal$(F/K) = \mathbb{Z}/4\mathbb{Z}$,*

2. *Gal $(F/\mathbb{Q}) = Q_8$, or*

3. *Gal $(F/\mathbb{Q}) = DC$.*

There exists a four-dimensional abelian variety $\mathcal{A}$ of GL_2-type such that the $\mathbb{Q}$-curve E is a simple factor of $\mathcal{A}$ and $End_{\mathbb{Q}}(\mathcal{A}) \otimes \mathbb{Q} \cong \mathbb{Q}(\sqrt{r}, \sqrt{-r})$.

Proof. Suppose $L \subset F$ such that Gal $(F/\mathbb{Q}) = D_4$ and Gal $(F/K) = \mathbb{Z}/4\mathbb{Z}$. Then $\tau \in$ Gal $(L/\mathbb{Q})$ fixes K. Hence, the extension of τ to an automorphism of F forces τ to have order 4. We can also extend $\sigma \in$ Gal $(L/\mathbb{Q})$ to an automorphism $\sigma \in$ Gal $(F/\mathbb{Q})$ such that σ has order 2. Now σ and τ no longer commute. In order to show that the cocycle $[c]$ is trivial, we need find $\beta : G_{\mathbb{Q}} \to \overline{\mathbb{Q}}$ such that

$$c(g, h) = \frac{\beta(g)\beta(h)}{\beta(gh)}$$

for all $g, h \in G_{\mathbb{Q}}$. We can define β as follows:

g	1	τ	τ^2	τ^3	σ	$\tau\sigma$	$\tau^2\sigma$	$\tau^3\sigma$
$\beta(g)$	1	$\sqrt{-1}$	-1	$-\sqrt{-1}$	$\sqrt{a}$	$-\sqrt{-a}$	$-\sqrt{a}$	$\sqrt{-a}$

Now suppose that Gal $(F/\mathbb{Q}) = Q_8$. Then extend τ and σ so that $\tau^4 = \sigma^4 = 1$ and let -1 represent the automorphism $\tau^2 = \sigma^2$. Then it is possible to define β in the following manner.

g	1	-1	τ	$-\tau$	σ	$-\sigma$	$\tau\sigma$	$-\tau\sigma$
$\beta(g)$	1	-1	$\sqrt{-1}$	$-\sqrt{-1}$	$\sqrt{-a}$	$-\sqrt{-a}$	$\sqrt{a}$	$-\sqrt{a}$

Suppose that Gal $(F/\mathbb{Q}) = DC$. We extend τ and σ such that $\tau^2 = \sigma^2 = 1$, $[\tau, \sigma] = \gamma^2$, where γ is the third generator of DC with order 4, and $[\sigma, \gamma] = [\tau, \gamma] = 1$. Then define β as follows.

g	1	τ	γ	γ^2	γ^3	$\tau\gamma$	$\tau\gamma^2$	$\tau\gamma^3$
$\beta(g)$	1	-1	$\sqrt{-1}$	1	$-\sqrt{-1}$	$-\sqrt{-1}$	-1	$\sqrt{-1}$

g	σ	$\sigma\gamma$	$\sigma\gamma^2$	$\sigma\gamma^3$	$\tau\sigma$	$\tau\sigma\gamma$	$\tau\sigma\gamma^2$	$\tau\sigma\gamma^3$
$\beta(g)$	$\sqrt{a}$	$\sqrt{-a}$	$-\sqrt{a}$	$-\sqrt{-a}$	$\sqrt{a}$	$\sqrt{-a}$	$-\sqrt{a}$	$-\sqrt{-a}$

In each of these cases we see that the field obtained by adjoining the values of $\beta(g)$ for all automorphisms g is $B = \mathbb{Q}(\sqrt{a}, \sqrt{-a})$. Since $a = r$ or $a = -r$, where r is the degree of the isogeny from E to its Galois conjugate, we have $B = \mathbb{Q}(\sqrt{r}, \sqrt{-r})$. Note that B cannot be a smaller field in each of the cases regardless of how the function β is defined. Therefore, there exists a four-dimensional abelian variety $\mathcal{A}$ of GL_2-type such that $End(\mathcal{A}) \otimes \mathbb{Q} = B$. $\square$

Given $L = \mathbb{Q}(\sqrt{t}, \sqrt{-rA})$ where A is a norm from $\mathbb{Q}(\sqrt{t})$, we would like to have conditions which determine if L can be embedded into either a field with Galois group D_4, Q_8, or DC. Later, we will also be interested in embedding L into an extension with Galois group isomorphic to M_{16}. The following result determines the answer to the embedding problem by imposing conditions on the Hilbert symbols. The proofs of the following theorem are given in [8], [9], [10], and [12].

Theorem 17. *The field $L = \mathbb{Q}(\sqrt{a}, \sqrt{b})$ can be embedded into a field F with Galois group*

- *D_4 with $F/\mathbb{Q}(\sqrt{b})$ cyclic if and only if $(a, -b) = 1$.*
- *Q_8 if and only if $(a, b)_p(ab, -1)_p = 1$ for all primes p.*
- *DC if and only if there exists c independent of a, b modulo $(\mathbb{Q}^\times)^2$ such that $(a, b)_p(c, -1)_p = 1$ for all primes p.*
- *M_{16} with $F/\mathbb{Q}(\sqrt{a})$ non-cyclic if and only if there exists $x \in \mathbb{Q}^\times$ such that $(b, -1)_p = (b, 2a)_p(x, -1)_p = 1$ for all primes p.*

We can apply the theorem to determine which biquadratic extensions of the form $L = \mathbb{Q}(\sqrt{t}, \sqrt{-rA})$ can be embedded into a D_4 extension which trivializes the cocycle. First suppose that $[L : \mathbb{Q}] = 4$ for all values of A. This implies that $(t, r) = (t, -r) = -1$. Also note that $(A, t) = 1$. In the following table we calculate $(a, -b)_p$ where a is the value in the rows and b is the value in the columns.

Value of $(a, -b)_p$

	t	$-rA$	$-rtA$
t	——————-	$(t, r)_p$	$(t, -r)_p$
$-rA$	$(t, -r)_p(-rA, -1)_p$	———	$(t, -r)_p$
$-rtA$	$(t, -r)_p(-rA, -1)_p$	$(t, r)_p$	———

Thus we can successfully trivialize the cocycle as in the proof of Theorem 16 when there is an A, which is a norm from $\mathbb{Q}(\sqrt{t})$, such that $(t,-r)_p(-rA,-1)_p = 1$ for all primes p.

Suppose L can be embedded into F with Gal $(F/L) \cong D_4$. Using the table, we see that if either $F/\mathbb{Q}(\sqrt{-rA})$ or $F/\mathbb{Q}(\sqrt{-rtA})$ is cyclic, then either $(t,r) = 1$ or $(t,-r) = 1$ respectively. Hence, there exists an A such that $L = \mathbb{Q}(\sqrt{t}, \sqrt{-rA})$ and $[L : \mathbb{Q}] = 2$. Since $[L : \mathbb{Q}] = 4$, we are only interested in the case when $F/\mathbb{Q}(\sqrt{t})$ is cyclic.

Now, we could ask if we could use the other 6 groups of order 16 to trivialize the cocycle. If L can be embedded into any of the groups, $D_8, Q_{16}, SD_8, Q \curlywedge C$, or $D \curlywedge C$, then L could have been embedded into D_4. Hence, it is not necessary to look at these groups. In order to trivialize the cocycle using the group M_{16}, the field B that we obtain is an extension of degree greater than 4.

Theorem 18. *Suppose that $K = \mathbb{Q}(\sqrt{t})$ and $L = \mathbb{Q}(\sqrt{t}, \sqrt{-rA})$ where A is a norm from K. If for some value of A, L can be embedded into an extension F such that Gal $(F/\mathbb{Q}) \cong M_{16}$ and $F/\mathbb{Q}(\sqrt{-rA})$ is not cyclic, then there exists an eight-dimensional abelian variety $\mathcal{A}$ of GL_2-type such that $End(\mathcal{A}) \otimes \mathbb{Q} \cong \mathbb{Q}(\sqrt{r}, \zeta)$, where ζ is a primitive eighth root of unity.*

Proof. $Gal(L/\mathbb{Q}) = \{1, \tau, \sigma, \tau\sigma\}$. The automorphism τ fixes K, and the automorphism σ fixes $\mathbb{Q}(\sqrt{-rA})$. Under the assumption that $F/\mathbb{Q}(\sqrt{-rA})$ is non-cyclic, we have that τ extends to an automorphism of F with order 8 and σ extends to an automorphism of order 2 and $\tau\sigma = \sigma\tau^5$. In order to trivialize the cocycle c, we clearly have $\beta(1) = 1$. For any integer j, we have

$$1 = c(\tau, \tau^j) = \frac{\beta(\tau)\beta(\tau^j)}{\beta(\tau^{j+1})}$$

implies that $\beta(\tau^j) = \beta(\tau)^j$. Hence $\beta(\tau)$ is an eighth root of unity. Also,

$$a = c(\sigma, \sigma) = \frac{\beta(\sigma)^2}{\beta(\sigma^2)} = \beta(\sigma)^2.$$

So we can choose, $\beta(\sigma) = \sqrt{a}$. Recall a is either r or $-r$. In addition,

$$1 = c(\sigma, \tau^j) = \frac{\beta(\sigma)\beta(\tau)^j}{\beta(\sigma\tau^j)}.$$

Thus, $\beta(\sigma\tau^j) = \beta(\sigma)\beta(\tau)^j$ Also,

$$\begin{aligned} -1 = c(\tau, \sigma) &= \frac{\beta(\tau)\beta(\sigma)}{\beta(\tau\sigma)} \\ &= \frac{\beta(\tau)\beta(\sigma)}{\beta(\sigma\tau^5)} \\ &= \frac{\beta(\tau)}{\beta(\tau)^5} \\ &= \frac{1}{\beta(\tau)^4}. \end{aligned}$$

Therefore, $\beta(\tau)$ must be a primitive eighth root of unity. Set $\beta(\tau) = \zeta$. We can define β as follows.

g	1	τ	τ^2	τ^3	τ^4	τ^5	τ^6	τ^7
$\beta(g)$	1	ζ	ζ^2	ζ^3	ζ^4	ζ^5	ζ^6	ζ^7

g	σ	$\sigma\tau$	$\sigma\tau^2$	$\sigma\tau^3$	$\sigma\tau^4$	$\sigma\tau^5$	$\sigma\tau^6$	$\sigma\tau^7$
$\beta(g)$	$\sqrt{a}$	$\sqrt{a}\zeta$	$\sqrt{a}\zeta^2$	$\sqrt{a}\zeta^3$	$\sqrt{a}\zeta^4$	$\sqrt{a}\zeta^5$	$\sqrt{a}\zeta^6$	$\sqrt{a}\zeta^7$

Therefore, there exists an eight-dimensional abelian variety $\mathcal{A}$ such that

$$End(\mathcal{A}) \otimes \mathbb{Q} \cong \mathbb{Q}(\sqrt{r}, \zeta).$$

□

Let E be a non-CM $\mathbb{Q}$-curve defined over $\mathbb{Q}(\sqrt{-3})$ which is 2-isogenous to its Galois conjugate. Then E is given by a curve from Theorem 3. For example, we could let E be given by

$$E : y^2 = x^3 + 2Dx^2 + \frac{1+\sqrt{-3}}{2}D^2x$$

where $D \in \mathbb{Q}(\sqrt{-3})^\times$. In this case, the isogeny from E to its Galois conjugate is defined over $L = \mathbb{Q}(\sqrt{-3}, \sqrt{-2A})$ where A is the norm of D. Since $(-2,-3) = (2,-3) = -1$, the field L is a biquadratic extension of $\mathbb{Q}$ for all possible D. By choosing $D = 1$, we see that $L = \mathbb{Q}(\sqrt{-3}, \sqrt{-2})$. Since the Hilbert symbol $(-2, 3) = 1$, L can be embedded into a field F such that Gal $(F/\mathbb{Q}) = D_4$ and Gal $(F/\mathbb{Q}(\sqrt{-3}))$ is cyclic. Therefore, we can apply the above theorem.

Let E be a non-CM $\mathbb{Q}$-curve defined over $\mathbb{Q}(\sqrt{5})$ which is 3-isogenous to its Galois conjugate. Then E is given by a curve in Theorem 4. The isogeny between E and its Galois conjugate is defined over $L = \mathbb{Q}(\sqrt{5}, \sqrt{-3A})$ where A is a norm from $\mathbb{Q}(\sqrt{5})$. Since $(5,3) = (5,-3) = -1$, $[L : \mathbb{Q}] = 4$ for all choices of A.

Our next goal is to show that L cannot be embedded into an extension with Galois group D_4 or Q_8. We do this using the following series of Lemmas.

Lemma 6. *Let p be an odd prime. Let $K/\mathbb{Q}_p$ be a finite extension and suppose that L/K is a totally ramified extension with $G = Gal(L/K)$ equal to a 2-group. Then G is cyclic.*

Proof. If there is a unique subgroup of G which has index 2, then we are done (see page 128 of [1]). Suppose that there exists $H_1 \neq H_2$ which are subgroups of G with index 2. Then $H_1 \cap H_2$ is normal, has index 4, and $G/(H_1 \cap H_2)$ is not cyclic. Let F be the fixed field of of $H_1 \cap H_2$. F is a totally, tamely ramified extension of K with Galois group isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. This type of extension is obtained by adjoining $\sqrt[4]{\pi}$ for some $\pi \in K$ (see Lemma 14.5 in [21]). If $\sqrt{-1} \in K$, then F/K is cyclic which is a contradiction. If $\sqrt{-1} \notin K$, then F/K is not Galois which is a contradiction. Therefore, there must be a unique subgroup of G of order 2 which completes the proof. $\square$

Lemma 7. *Let p be an odd prime and let $L/\mathbb{Q}_p$ be a finite extension with $G = Gal(L/\mathbb{Q}_p)$ equal to a 2-group. Let I be the inertia group of G. Then we have an exact sequence*

$$1 \to I \to G \to G/I \to 1$$

with I and G/I both cyclic.

Proof. The inertia group is cyclic using Lemma 6. The quotient G/I is the Galois group of an unramified extension, therefore cyclic (see Lemma 14.4 in [21]). $\square$

Theorem 19. *Let p be a prime with $p \equiv 1 \pmod{2^n}$. Let $L/\mathbb{Q}_p$ be a finite extension with $G = Gal(L/\mathbb{Q}_p)$ equal to a 2-group. Let I be the inertia group of G. If G is non-abelian, then $|I| \geq 2^{n+1}$.*

Proof. Let K be the fixed field of I. Then L/K is a totally, tamely ramified extension. Assume that $|I| \leq 2^n$. Let $m = |I|$. Then, $L = K(\sqrt[m]{\pi})$ where $\pi = p \cdot u$ and u is a unit in $\mathcal{O}_K$. Since the m-th roots of unity are contained in $\mathbb{Q}_p$, $\mathbb{Q}_p(\sqrt[m]{p})/\mathbb{Q}_p$ is abelian. Since u is a unit and p is odd, $\mathbb{Q}_p(\sqrt[m]{u})/\mathbb{Q}_p$ is unramified, therefore abelian. Also, $K/\mathbb{Q}_p$ is unramified, therefore abelian. Thus L is an abelian extension over $\mathbb{Q}_p$ which is a contradiction. Therefore, $|I| \geq 2^{n+1}$. $\square$

We will now use this theorem to show that $L = \mathbb{Q}(\sqrt{5}, \sqrt{-3A})$ cannot be embedded into an extension of $\mathbb{Q}$ with degree 8 in order to trivialize the cocycle c. Suppose that F is an extension of L such that $[F : \mathbb{Q}] = 8$ and the image of c in $H^2(\text{Gal }(F/\mathbb{Q}), \overline{\mathbb{Q}}^\times)$ is trivial. Choose a prime in the ring of integers of F which lies above 5. Let F_5 denote the completion of F at this prime. Then, we have the containment of local fields $\mathbb{Q}_5 \subset L_5 \subset F_5$. By ramification considerations, we have that $[L_5 : \mathbb{Q}_5] = 4$ and $[F_5 : L_5] \leq 2$, since Gal $(L_5/\mathbb{Q}_5) \cong$ Gal $(L/\mathbb{Q})$. The cocycle c defines an element in $H^2(\text{Gal}\,(\overline{L_5}/\mathbb{Q}_5), \overline{\mathbb{Q}}^\times)$ which cannot be trivialized by an abelian extension. Hence $F_5/\mathbb{Q}_5$ must be non-abelian and so $[F_5 : \mathbb{Q}_5] = 8$. The previous theorem implies that the inertia group of Gal $(F_5/\mathbb{Q}_5)$ has order 8, which gives a contradiction. Therefore, L cannot be embedded into a non-abelian Galois extension over $\mathbb{Q}$ with degree 8. In order to trivialize the cocycle, we will have to embed L into an extension which has degree at least 16 over $\mathbb{Q}$.

Theorem 19 also shows that by choosing p congruent to 1 modulo a high power of 2, certain biquadratic fields containing $\mathbb{Q}(\sqrt{p})$ will have to be embedded into arbitrarily large extensions in order to trivialize the cocycle.

Now we want to eliminate the group DC. The Hilbert symbol $(5, -3A)_p = -1$ if and only if $p = 3$ or $p = 5$. For any x, $(x, -1)_5 = 1$ since $(5, -1) = 1$. Therefore, there is no value of x such that $(5, -3A)_p(x, -1)_p = 1$ for all primes p. Hence, by Theorem 17, $\mathbb{Q}(\sqrt{5}, \sqrt{-3A})$ cannot be embedded into an extension with Galois group isomorphic to DC.

Now choose $A = 1$. Using Hilbert symbol calculations, we see that

$$(5, -6)_p = (-5, -6)_p(-1, -6)_p = (-5, 6)_p(-5, -1)_p(-1 - 6)_p = (-1, 30)_p.$$

Since $(5, -1)_p = (5, -6)_p(-1, 30)_p = 1$ for all p, we may use Theorem 17 to determine that $L = \mathbb{Q}(\sqrt{5}, \sqrt{-3})$ can be embedded into an extension F with Gal $(F/\mathbb{Q}) \cong M_{16}$ and $F/\mathbb{Q}(\sqrt{-3})$ is non-cyclic. Thus, we can apply Theorem 18 to determine that there an an eight-dimensional abelian variety $\mathcal{A}$ of GL_2-type which contains E as a simple factor. It still remains to determine if E can be realized as a simple factor of some abelian variety of GL_2-type with dimension smaller than 8. We could possibly embed L into an extension with degree greater than 16 in such a way so that the cocycle becomes trivial. Is is possible that the field obtained by adjoining the values of $\beta(g)$ has degree smaller than 8? If so, this method of obtaining an abelian variety of GL_2-type is not minimal.

4.2 Extending Results Concerning the Degree of Modular Parametrization

In Section 1, we developed a list of $\mathbb{Q}$-curves which are factors of four-dimensional abelian varieties of GL_2-type. Let E be a $\mathbb{Q}$-curve defined over K such that the r-isogeny between E and its Galois conjugate is defined over L. Assume L is a biquadratic extension of $\mathbb{Q}$ for all twists of E. In this section, we will assume that E is a modular elliptic curve. In other words, there is an eigenform f for $\Gamma_1(N)$ such that A_f contains E as a simple factor. Throughout, we will assume that dim $A_f = 4$ and $End_{\mathbb{Q}}(A_f) \otimes \mathbb{Q} = \mathbb{Q}(\sqrt{r}, \sqrt{-r})$, so that E fits into the framework from Section 1. Hence, the coefficient field of f is $B = \mathbb{Q}(\sqrt{r}, \sqrt{-r})$. Let $f_0 = f$, and let f_1, f_2, and f_3 denote the Galois conjugates of f. In Chapter 3, we restricted our attention to eigenforms with an extra twist. This produced abelian varieties with large endomorphism algebras. Hence, it seems natural to do the same in this case. So suppose that

$$f_i = f \otimes \chi_i$$

where χ_i is a quadratic character associated to the field $K_i = \mathbb{Q}(\sqrt{t_i'})$. Let $t_i = \text{disc } (K_i)$.

We already know that $End_{\mathbb{Q}}(A_f) \otimes \mathbb{Q} = B = \mathbb{Q}(\sqrt{r}, \sqrt{-r})$, since the endomorphisms defined over $\mathbb{Q}$ are determined by the Hecke operators. Choose primes p and q such that $a_p = \sqrt{r_1}$ and $a_q = \sqrt{r_2}$, $\mathbb{Q}(\sqrt{r_1}, \sqrt{r_2}) = B$, and $|r_1|$ and $|r_2|$ minimal. Then $End_{\mathbb{Q}}(A_f) \otimes \mathbb{Q} = \langle 1, T_p, T_q, T_pT_q \rangle$. All of these endomorphisms commute. The n-th coefficients of the eigenforms f_0, f_1, f_2, f_3 are summarized in the table below.

n	f_0	f_1	f_2	f_3
p	$\sqrt{r_1}$	$-\sqrt{r_1}$	$\sqrt{r_1}$	$-\sqrt{r_1}$
q	$\sqrt{r_2}$	$\sqrt{r_2}$	$-\sqrt{r_2}$	$-\sqrt{r_2}$

The above table shows that $\chi_1(p) = -1$ and $\chi_1(q) = 1$. Also $\chi_2(p) = 1$ and $\chi_2(q) = -1$. The presence of an additional twist produces other endomorphisms of A_f which are not defined over $\mathbb{Q}$. We have η_i which corresponds to the character χ_i for $i = 1, 2$. In addition, $\eta_1^2 = t_1$ and $\eta_2^2 = t_2$, and $\eta_1\eta_2 = \eta_2\eta_1$. We can derive the commuting properties of the Hecke operators with the η endomorphisms.

$$\begin{aligned} T_p\eta_1 &= \chi_1(p)\eta_1 T_p = -\eta_1 T_p, \\ T_q\eta_1 &= \chi_1(q)\eta_1 T_q = \eta_1 T_q, \\ T_p\eta_2 &= \chi_2(p)\eta_2 T_p = \eta_2 T_p, \\ T_q\eta_2 &= \chi_2(q)\eta_2 T_q = -\eta_2 T_q. \end{aligned}$$

Lemma 8. *$End(A_f) \otimes \mathbb{Q}$ is generated as a $\mathbb{Q}$-algebra by*

$$\langle T_p, T_q, \eta_1, \eta_2 \rangle$$

and

$$End(A_f) \otimes \mathbb{Q} \cong \left(\frac{r_1, t_1}{\mathbb{Q}}\right) \otimes \left(\frac{r_2, t_2}{\mathbb{Q}}\right)$$

Proof. Let $\mathcal{E} = \langle T_p, T_q, \eta_1, \eta_2 \rangle$. Clearly $\mathcal{E} \subset End(A_f) \otimes \mathbb{Q}$. Let B be the biquadratic field obtained by adjoining the coefficients of f. Since the $[B : \mathbb{Q}] = 4$, a result of Ribet (see [15]) implies that the dimension of the algebra $End(A_f) \otimes \mathbb{Q}$ over $\mathbb{Q}$ is 16. Since we know all of the commuting properties of T_p, T_q, η_1, and η_2, we have 16 possible generators of $\mathcal{E}$. Let $e_1, e_2, \ldots, e_3$ denote the 16 elements of $\mathcal{E}$ formed by products T_p, T_q, η_1, and η_2. Suppose that $\sum_{i=1}^{16} a_i e_i = 0$ for some values of a_i where some $a_i \neq 0$. Let e be any of the e_i. Then

$$e(\sum a_i e_i)e = e^2(\sum s(i) a_i e_i)$$

where $s(i) = -1$ if e and e_i anti-commute and $s(i) = 1$ otherwise. So $s(i) = -1$ for exactly four entries if $e \neq 1$. Since $e^2 \in \mathbb{Q}$ and $End(A_f) \otimes \mathbb{Q}$ has no torsion, we obtain 16 equations of the form:

$$\sum s(i) a_i e_i = 0.$$

Writing out these equations, we obtain a matrix equation $M(e_i) = 0$. Also $\det(M) = c(a_1 a_2 \cdots a_{16})$ for some nonzero constant c. Then clearly $a_1 = a_2 = \cdots = a_{16} = 0$. Therefore, $\mathcal{E} = End(A_f) \otimes \mathbb{Q}$. Let $Q_1 = \left(\frac{r_1, t_1}{\mathbb{Q}}\right)$ and $Q_2 = \left(\frac{r_2, t_2}{\mathbb{Q}}\right)$. The above argument also shows that $\mathcal{E}$ is isomorphic to $Q_1 \otimes Q_2$. Therefore, we can define the following map.

$$\psi : Q_1 \otimes Q_2 \to End(A_f)$$
$$\sum_i a_i \otimes b_i \mapsto \sum_i a_i b_i.$$

The map ψ is clearly a well-defined homomorphism and is bilinear. It is an isomorphism since Q_1 and Q_2 generate $End(A_f) \otimes \mathbb{Q}$ and both algebras have the same dimension. $\square$

Let $Br(\mathbb{Q})$ denote the Brauer group of $\mathbb{Q}$. Assume that the $\mathbb{Q}$-curve E is a simple factor of a four-dimensional abelian variety A_f, for some eigenform f. Then the class of $End(A_f) \otimes \mathbb{Q}$ and the class of $End(E) \otimes \mathbb{Q}$ are the same in $Br(\mathbb{Q})$ (see [14]). Since E does not have complex multiplication, each of these classes is trivial in the Brauer group. Therefore, we are interested in the case where $End(A_f) \otimes \mathbb{Q}$ is isomorphic to $M_4(\mathbb{Q})$.

Theorem 20. *$End(A_f) \otimes \mathbb{Q} \cong M_4(\mathbb{Q})$ if and only if $(r_1, t_1)_p = (r_2, t_2)_p$ for all primes p including $p = \infty$. This occurs if and only if there exists a solution for the variables $a_1, a_2, a_3, b_1, b_2, b_3$ in $\mathbb{Q}$ in the system of equations*

$$r_1 a_1^2 + t_1 a_2^2 - r_1 t_1 a_3^2 = r_2$$
$$r_1 b_1^2 + t_1 b_2^2 - r_1 t_1 b_3^2 = t_2$$
$$r_1 a_1 b_1 + t_1 a_2 b_2 - r_1 t_1 a_3 b_3 = 0.$$

Proof. Let $Q_1 = \left(\frac{r_1, t_1}{\mathbb{Q}}\right)$ and $Q_2 = \left(\frac{r_2, t_2}{\mathbb{Q}}\right)$. Then both Q_1 and Q_2 have order 2 in $Br(\mathbb{Q})$. Thus $Q_1 \otimes Q_2 \cong M_4(\mathbb{Q})$ if and only if $[Q_1][Q_2] = 1$ in $Br(\mathbb{Q})$. Therefore $Q_1 \otimes Q_2$ is a matrix algebra if and only if $Q_1 \cong Q_2$. Using Hilbert symbols, we determine that $Q_1 \cong Q_2$ if and only if $(r_1, t_1)_p = (r_2, t_2)_p$ for all primes p. We can embed Q_1 in $M_4(\mathbb{Q})$ by the left regular representation. This determines matrices T_p and η_1.

$$T_p = \begin{pmatrix} 0 & r_1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & r_1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \qquad \eta_1 = \begin{pmatrix} 0 & 0 & t_1 & 0 \\ 0 & 0 & 0 & t_1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

Using the commuting properties, we can attempt to determine the matrices corresponding to T_q and η_2. A solution for these matrices can be found if and only if a solution can be found in the above system of equations. If a solution exists, then we can express the isomorphism with the following matrices.

$$T_q = \begin{pmatrix} 0 & r_1 a_1 & t_1 a_2 & -r_1 t_1 a_3 \\ a_1 & 0 & -t_1 a_3 & t_1 a_2 \\ a_2 & r_1 a_3 & 0 & -r_1 a_1 \\ a_3 & a_2 & a_1 & 0 \end{pmatrix} \qquad \eta_2 = \begin{pmatrix} 0 & r_1 b_1 & t_1 b_2 & -r_1 t_1 b_3 \\ b_1 & 0 & -t_1 b_3 & t_1 b_2 \\ b_2 & r_1 b_3 & 0 & -r_1 b_1 \\ b_3 & b_2 & b_1 & 0 \end{pmatrix}$$

□

Now we are ready to extend the results from Chapter 3. Since B is not a totally real field, the modular parametrization of our $\mathbb{Q}$-curve E will not come from $X_0(N)$. Cremona's Theorem 6, which gives a formula for computing the degree of a strong Weil parametrization remains true. In addition, the algorithm developed in Chapter 2 can also be extended to work in this case where $\dim A_f = 4$. However, it is computationally not feasible to perform the calculations in this case because the index $[SL_2(\mathbb{Z}) : \Gamma_1(N)]$ grows much too quickly as N increases. Cremona's Theorem and the algorithm developed in Chapter 2 can be used to determine properties of the degree of a strong Weil parametrization.

Let $H =$

$$\{h = af_0 + bf_1 + cf_2 + df_3 \mid$$
$$a, b, c, d \in \mathbb{C}, \text{ the periods of } h \text{ form a lattice in } \mathbb{C}\}/\{\text{constants}\}.$$

Let $M \in M_4(\mathbb{Q})$ with $\ker(M) = [u, v, w, z]^t$. Let $e \in End(A_f) \otimes \mathbb{Q}$ such that e corresponds to M under the isomorphism. Then eA_f is a three-dimensional abelian variety. Therefore, $E = A_f/eA_f$ is a $\mathbb{Q}$-curve defined over L. The endomorphism e acts on $\langle f_0, f_1, f_2, f_3 \rangle$. There is a unique (up to constant multiple) $h \in H$ such that $eh = 0$, and the periods of h correspond to the periods of E up to a constant multiple. In addition, we can extend Theorem 8 to determine that H is in one-to-one correspondence with $\mathbb{P}^3(\mathbb{Z})$. Hence, we have a set of modular parametrizations of $\mathbb{Q}$-curves given by

$$\phi(u, v, w, z)(\tau) = \int_{\tau_0}^{\tau} h(u, v, w, z)(t)dt.$$

Theorem 21. *Let $\phi(u, v, w, z)$ be the modular parametrization as above. Then*

$$deg\ \phi(u, v, w, z) = d\,\frac{g(u, v, w, z)}{k(u, v, w, z)}$$

where g is a quadratic form, k is the dependency constant, and d is the degree of the map from $X_1(N)$ into A_f.

Proof. The proof follows clearly by extending the proofs of Theorems 9 and 10 from 2 variables to 4 variables. $\square$

In addition, the quadratic form once again depends on the choice of the isomorphism between $End(A_f) \otimes \mathbb{Q}$ and the matrix ring. We can define the action β_e on $\mathbb{P}^3(\mathbb{Z})$ for any invertible element $e \in End(A_f) \otimes \mathbb{Q}$. If $e \in End(A_f) \otimes \mathbb{Q}$, then set $e = a + b$ where $a \in \mathbb{Q}$ and b is an endomorphism which has no constant term. Define $\overline{e} = a - b$. So $e\overline{e} \in \mathbb{Q}$. The proofs of Theorems 11 and 12 did not depend on the fact that H was parameterized by $\mathbb{P}^1(\mathbb{Z})$. We could use these same arguments, but simply replace the pair (u, v) by the 4-tuple (u, v, w, z). We combine these facts to give the following result.

Theorem 22. *Let $h \in H$ and let $e \in End(A_f) \otimes \mathbb{Q}$ be invertible. Then h corresponds to a point $(u : v : w : z) \in \mathbb{P}^3(\mathbb{Z})$. Let $\phi(\tau) = \langle \{\tau_0, \tau\}, h \rangle$.*

1. *There exists an isogeny from E to E_{eh} with degree equal to*

$$\frac{k(\beta_{\overline{e}}(u, v, w, z))}{k(u, v, w, z)}.$$

2. *$deg\ \phi = deg\ \phi^{T_p} = deg\ \phi^{T_q}$.*

3. *Suppose $|t_i|$ is prime. Then the quantity*

$$\frac{deg\ \phi}{deg\ \phi^{\eta_i}}$$

   is an either 1, t_i, or $1/t_i$.

4. *The quadratic form $g(u, v, w, z)$ is positive definite.*

4.3 Computations of Quadratic Forms

By using the last theorem from the previous section, we can try to use the same technique as in Chapter 3 to isolate the quadratic form g. That is, we would like to find the set of positive definite quadratic forms g such that

$$g(M(u,v,w,z)) = \alpha_M g(u,v,w,z)$$

where $M = \beta_{T_p}, \beta_{T_q}, \beta_{\eta_1}, \beta_{\eta_2}$. Here we present some computational results which suggest that the quadratic form g is uniquely determined, as it is when A_f is two-dimensional.

Let E by the $\mathbb{Q}$-curve

$$y^2 = x^3 + 2Dx^2 + \frac{1+\sqrt{-3}}{2}D^2x$$

discussed earlier in this chapter. Assume that $E \cong A_f/eA_f$ for some eigenform f for $\Gamma_1(N)$ and $e \in End(A_f)$. Then the coefficients field of f is $B = \mathbb{Q}(\sqrt{2}, \sqrt{-2})$. We further assume that f is an eigenform with an extra twist. The isogeny between E and its Galois conjugate is defined over $L = \mathbb{Q}(\sqrt{-3}, \sqrt{-2A})$ where A is the norm of D. Then we know that T_p^2 and T_q^2 are integers equivalent to either 2, -2, or -1 in $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$. In addition, η_1^2 and η_2^2 are integers which are equivalent to either -3, $-2A$, or $6A$ in $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$. For simplicity of exposition, we will assume that $r_1, r_2 \in \{2, -2, -1\}$. Since 1 is a norm from $\mathbb{Q}(\sqrt{-3})$, we will set $A = 1$. Then, we will assume that $t_1', t_2' \in \{-3, -2, 6\}$. Then $t_1, t_2 \in \{-3, -8, 24\}$. By using Theorem 20, we see that there could only be three possibilities up to permutation of the two quaternion algebras.

Case 1

$$r_1 = -2 \qquad\qquad r_2 = -1$$

$$t_1 = -3 \qquad\qquad t_2 = -8$$

$$a_1 = 0 \quad a_2 = 1/3 \quad a_3 = 1/3 \quad b_1 = 2 \quad b_2 = 0 \quad b_3 = 0$$

Case 2

$$r_1 = 2 \qquad\qquad r_2 = -1$$

$$t_1 = -3 \qquad\qquad t_2 = -24$$

$$a_1 = 1 \quad a_2 = 1 \quad a_3 = 0 \quad b_1 = 0 \quad b_2 = 0 \quad b_3 = 2$$

Case 3

$$r_1 = -2 \qquad\qquad r_2 = 2$$

$$t_1 = 24 \qquad\qquad t_2 = -8$$

$$a_1 = 1 \quad a_2 = 1/3 \quad a_3 = 1/6 \quad b_1 = 4 \quad b_2 = 1 \quad b_3 = 0$$

In each of the above cases, we can use the isomorphism between $End(A_f) \otimes \mathbb{Q}$ and $M_4(\mathbb{Q})$ to determine the potential quadratic forms $g(u, v, w, z)$ which would appear in the degree of modular parametrization of E.

In the first case, we can determine up to a constant multiple that there are exactly 10 quadratic forms that satisfy $g(M(u, v, w, z)) = \alpha_M g(u, v, w, z)$ for the matrices $M = \beta_{T_p}, \beta_{T_q}, \beta_{\eta_1}, \beta_{\eta_2}$. The form g is represented below by a vector of length ten with the coefficients of the terms as the entries. We list the coefficients in the following order:

$$[u^2, v^2, w^2, z^2, uv, uw, uz, vw, vz, wz].$$

The ten possibilities are listed below.

$g_1 = [1, -2, -3, 6, -4, 0, 0, 0, 0, -12]$ $\quad g_2 = [0, 0, 0, 0, 0, -1, -2, 2, -2, 0]$

$g_3 = [-1, 2, 3, -6, -2, 0, 0, 0, 0, -6]$ $\quad g_4 = [0, 0, 0, 0, 0, -1, 1, -1, -2, 0]$

$g_5 = [1, -2, 3, -6, 2, 0, 0, 0, 0, -6]$ $\quad g_6 = [-1, 2, -3, 6, 4, 0, 0, 0, 0, -12]$

$g_7 = [0, 0, 0, 0, 0, 1, 0, 0, -2, 0]$ $\quad g_8 = [1, 2, -3, -6, 0, 0, 0, 0, 0, 0]$

$g_9 = [0, 0, 0, 0, 0, 0, 1, 1, 0, 0]$ $\quad g_{10} = [1, 2, 3, 6, 0, 0, 0, 0, 0, 0]$

By setting two of the four variables equal to zero, we get a binary quadratic form. Since the entire form must be positive definite, each of these 6 binary quadratic forms must be positive definite. Among the ten choices, there is only one form which satisfies this property. That is $g_{10}(u, v, w, z) = u^2+2v^2+3w^2+6z^2$. The six discriminants of the binary quadratic forms are all congruent to either $-2, -3$, or -6 in $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$. This suggests that these discriminants are closely related to the values of t_1 and t_2.

In the second case, we obtain similar results. First, we find 10 quadratic forms only one of which is positive definite. In this case, $g(u, v, w, z) = (u^2 - 4uz + 6z^2) + (2v^2 - 4vw + 3w^2)$. In this case the 6 discriminant of the binary quadratic forms are $-2, -3$ in $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$.

In the third case, the same phenomenon occurs. We obtain the quadratic form $g(u, v, w, z) = (u^2 + 12uz + 48z^2) + (2v^2 - 12vw + 24w^2)$. The six discriminants are $-2, -3$, or -6 in $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$.

BIBLIOGRAPHY

[1] R. Carmichael. *Introduction to the Theory of Groups of Finite Order*. Ginn and Company, 1937.

[2] J.E. Cremona. Abelian varieties with extra twist, cusp forms, and elliptic curves over imaginary quadratic fields. *J. London Math. Soc.*, 45:404–416, 1992.

[3] J.E. Cremona. Modular symbols for $\Gamma_1(N)$ and elliptic curves with everywhere good reduction. *Proc. Camb. Phil. Soc.*, 111:199–218, 1992.

[4] J.E. Cremona. Computing the degree of the modular parametrization of a modular elliptic curve. *Math. Comp.*, 64:1235–1250, 1995.

[5] J.E. Cremona. *Algorithms for Modular Elliptic Curves*. Cambridge University Press, 1997.

[6] K. Doi and M. Ohta. On some congruences between cusp forms on $\Gamma_0(N)$. *Modular Functions of One Variable, V, Lecture Notes in Mathematics*, 601:91–105, 1977.

[7] B. Edixhoven. On the Manin constants of modular elliptic curves. In *Arithmetic Algebraic Geometry*, volume 89 of *Progress in Mathematics*, pages 25–39. Birkhäuser, 1991.

[8] A. Frohlich. Orthogonal representations as Galois groups, Stiefel- Whitney classes and Hasse-Witt invariants. *J. Reine Angew. Math.*, 360:84–123, 1985.

[9] H. Grundman and T. Smith. Automatic realizability of galois groups of order 16. *Proc. of Amer. Math. Soc.*, 124:2631–2640, 1996.

[10] H. Grundman, T. Smith, and J. Swallow. Groups of order 16 as Galois groups. *Expo. Math.*, 13:289–319, 1995.

[11] H. Hida. Congruences of cusp forms and special values of their zeta functions. *Invent. Math.*, 63:225–261, 1981.

[12] I. Kiming. Explicit classifications of some 2-extensions of a field of characteristic different from 2. *Canad. J. Math.*, 42:825–855, 1990.

[13] J. Manin. Parabolic points and zeta functions on modular curves. *Math. USSR-Izv.*, 6:19–64, 1972.

[14] E. Pyle. *Abelian Varieties over* $\mathbb{Q}$ *with Large Endomorphism Algebras and Their Simple Components over* $\overline{\mathbb{Q}}$. PhD thesis, University of California, Berkeley, 1995.

[15] K. Ribet. Abelian varieties over $\mathbb{Q}$ and modular forms. In *Algebra and Topology 1992 (Taejŏn)*, pages 53–79. Korea Adv. Inst. Sci. Tech., Taejŏn, 1992.

[16] B. Roberts. $\mathbb{Q}$-*curves over Quadratic Fields.* PhD thesis, University of Maryland, College Park, 1995.

[17] B. Roberts and L. Washington. The modularity of some $\mathbb{Q}$-curves. *Comp. Math.*, 111:35–49, 1998.

[18] J-P. Serre. Modular forms of weight one and Galois representations. In *Algebraic Number Fields (L-functions and Galois Properties)*, pages 193–268. Academic Press, 1977. prepared in collaboration with C.J. Bushnell.

[19] G. Shimura. *Introduction to the Arithmetic Theory of Automorphic Functions.* Princeton Univ. Press, 1971.

[20] X. Wang. 2-dimensional simple factors of $J_0(n)$. *Manuscripta Math.*, 87:179–197, 1995.

[21] L. Washington. *Introduction to Cyclotomic Fields.* Springer-Verlag, 1997.

[22] A. Wiles. Modular elliptic curves and Fermat's Last Theorem. *Ann. Math.*, 141:443–551, 1995.

[23] D. Zagier. Modular parametrizations of elliptic curves. *Canad. Math. Bull.*, 28:372 – 384, 1985.