©Copyright 2014

Alyson Deines

Shimura Degrees for Elliptic Curves over Number Fields

Alyson Deines

A dissertation submitted in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

University of Washington

2014

Reading Committee:

William Stein, Chair

Ralph Greenberg

Max Lieblich

Anna Karlin

Program Authorized to Offer Degree:

Mathematics

University of Washington

Abstract

Shimura Degrees for
Elliptic Curves over Number Fields

Alyson Deines

Chair of the Supervisory Committee:

Thesis Advisor William Stein

Mathematics

A crowning achievement of Number theory in the 20th century is a theorem of Wiles which states that for an elliptic curve E over $\mathbb{Q}$ of conductor N, there is a non-constant map from the modular curve $X_0(N)$ to E. For some curve isogenous to E, the degree of this map will be minimal; this is the modular degree. Generalizing to number fields, we no longer always have a modular curve. In the totally real number field case, the modular curve is replaced with a variety of dimension the same as the number field. It is only in the special case of $\mathbb{Q}$ that this variety happens to be a curve. The Jacquet-Langlands correspondence allows us to parameterize elliptic curves by Shimura curves. In this case we have several different Shimura curve parameterizations for a given isogeny class. I generalize to totally real number fields some of the results of Ribet and Takahashi over $\mathbb{Q}$. I further discuss finding the curve in the isogeny class parameterized by a given Shimura curve and how this relates to pairs of isogenous curves with the same discriminant. Finally, I use my algorithm to compute new data about degrees. Then I compare it with D-new modular degrees and D-new congruence primes. This data indicates that there is a strong relationship between Shimura degrees and new modular degrees and congruence primes. These connections with D-new degrees lead me to the conjecture that they are the same.

TABLE OF CONTENTS

Page

Glossary iii

Chapter 1: Introduction 1
- 1.1 Motivation 1
- 1.2 Classical Case 4
- 1.3 Modular Degree 5
- 1.4 Shimura Degree 6

Chapter 2: Preliminaries 9
- 2.1 Quaternion Algebras 10
- 2.2 Shimura Curves 14
- 2.3 Hilbert and Quaternionic Modular Forms 16
- 2.4 Néron Models and Character groups 19
- 2.5 Comparing Curves 21
- 2.6 Dual Graphs 22
- 2.7 Dual Graphs of Shimura Curves 25

Chapter 3: Shimura Degrees 30
- 3.1 Shimura Degrees over $\mathbb{Q}$ 30
- 3.2 Shimura Degree for Abelian Varieties Over Totally Real Number Fields 35
- 3.3 Finding Optimal Quotient 38

Chapter 4: Computing Shimura Degrees 42
- 4.1 Brandt and Hecke Modules $X(\mathfrak{D}, \mathfrak{M})$ 42
- 4.2 Computing $\mathcal{X}_{\mathfrak{p}}(J)$ 43
- 4.3 Computing $\mathcal{L}_{\mathfrak{p}}(f)$ 48
- 4.4 Computing $\delta^{\mathfrak{D}}(\mathfrak{M})$ and Optimal Quotients 49

Chapter 5: Data and Conjectures 53
5.1 D-new invariants 53

Chapter 6: Discriminant Twins 61
6.1 p-adic Uniformization of Elliptic Curves and Isogenies 62
6.2 Semistable Isogenous Curves 65
6.3 Number Fields 76
6.4 Semistable Non-Isogenous Discriminant Twins 78

Bibliography 80

Appendix A: Code 84
A.1 Shimura Degrees 84
A.2 Discriminant Twins 91

GLOSSARY

F: a totally real number field of degree d with real embeddings $\tau_1, \tau_2, \ldots, \tau_d$.

$\mathbb{Z}_F$: the ring of integers of F.

$\mathfrak{D}$: a square free ideal of $\mathbb{Z}_F$.

$\mathfrak{M}$: an ideal of $\mathbb{Z}_F$.

$\mathfrak{N}$: the ideal $\mathfrak{D}\mathfrak{M}$ of $\mathbb{Z}_F$.

E: an elliptic curve over F.

$\mathcal{H}$: the upper half complex plain.

$\Gamma_0(\mathfrak{N})$: the congruence subgroup of $\mathrm{SL}_2(\mathbb{Z}_F)$ with lower left hand entries in the ideal $\mathfrak{N}$.

$X_0(N)$: the modular curve $\Gamma_0(N) \setminus \mathcal{H} \cup$ cusps.

$J_0(N)$: the Jacobian of $X_0(N)$.

π: a modular parameterization $\pi : X_0(N) \to E$.

M_E: the degree of the modular parameterization.

B: an indefinite quaternion algebra over F split at τ_1, ramified at $\tau_2, \ldots, \tau_d$ of discriminant.

$\mathcal{O}_B(\mathfrak{M})$: a level $\mathfrak{M}$ Eichler order of B.

H: a definite quaternion algebra over F.

$\mathrm{CL}(\mathcal{O})$: the right ideal classes of the quaternion order $\mathcal{O}$.

$\Gamma_0(\mathcal{O}_B(\mathfrak{M}))$: The norm 1 invertible elements of $\mathcal{O}_B(\mathfrak{M})$ viewed as embedded in $\mathrm{SL}_2(\mathbb{R})$ via the embedding τ_1.

$X_0^{\mathfrak{D}}(\mathfrak{M})$: the Shimura curve associated to $\mathcal{O}_B(\mathfrak{M})$.

π: a Shimura curve parameterization $\pi : X_0^{\mathfrak{D}}(\mathfrak{M}) \to E$.

$\delta^{\mathfrak{D}}(\mathfrak{M})$: the degree of the Shimura curve parameterization $\pi : X_0^{\mathfrak{D}}(\mathfrak{M}) \to E$.

$M_2(N)$: the space of classical weight 2 level N modular forms.

$S_2(N)$: the space of classical weight 2 level N cuspforms.

$M_{\bar{2}}(\mathfrak{N})$: the space of parallel weight 2 level N Hilbert modular forms.

$S_{\bar{2}}(\mathfrak{N})$: the space of parallel weight 2 level N Hilbert cuspforms.

$M_2^{\mathfrak{D}}(\mathfrak{M})$: the space of weight 2 level $\mathcal{O}_B(\mathfrak{M})$ quaternionic modular forms.

$S_2^{\mathfrak{D}}(\mathfrak{M})$: the space of classical weight 2 level $\mathcal{O}_B(\mathfrak{M})$ quaternionic cuspforms.

f: a newform in $S_{\bar{2}}(\mathfrak{N})$ (or $S_2(N)$) with Fourier coefficients $a_{\mathfrak{n}}(f)$.

$\mathcal{X}_{\mathfrak{p}}(A)$: the character group at $\mathfrak{p}$ of an abelian variety A.

$\Phi_{\mathfrak{p}}(A)$: the component group at $\mathfrak{p}$ of an abelian variety A.

$u_{A,\mathfrak{p}}$: the monodromy pairing on $\mathcal{X}_{\mathfrak{p}}(A)$.

$\bar{c}_{\mathfrak{p}}(A)$: the order of $\Phi_{\mathfrak{p}}(A)$.

π_*: the map $\pi_* : \Phi_{\mathfrak{p}}(J) \to \Phi_{\mathfrak{p}}(E)$.

$i_{\mathfrak{p}}$: the order of the image of π_*.

$j_{\mathfrak{p}}$: the order of the cokernel of π_*.

$\mathcal{L}_{\mathfrak{p}}(f)$: the f-isotypical subgroup of $\mathcal{X}_{\mathfrak{p}}(J)$ corresponding to f.

$h_{\mathfrak{p}}$: the integer $u_{J,\mathfrak{p}}(g_{\mathfrak{p}}, g_{\mathfrak{p}})$ where $g_{\mathfrak{p}}$ is a generator of $\mathcal{L}_{\mathfrak{p}}(f)$.

ACKNOWLEDGMENTS

I am very grateful to my thesis adviser, William Stein, for patiently guiding my intellectual development in innumerable ways, introducing me to amazing mathematics, and providing support while writing this dissertation. I would also like to thank John Voight for his enthusiastic answers to my many questions and Ben Lundell for our long discussions. Surviving the process of writing this dissertation was only made possible by Tim Schartz and Aimee Schellentrager. Finally, I would like to give my sincerest gratitude to my parents, Ruth and Alan Deines, for their love and encouragement.

Chapter 1

INTRODUCTION

In the introduction, we first provide some background motivation for the study of modular degrees. In particular, we discuss how Modular degrees, the precursor to Shimura degrees, were first studied in relation to the Gauss class number problem. Next we describe the modular parameterization of elliptic curves and and give a definition modular degrees. In this we also discuss more recent results. In the late 1990's Ribet and Takahashi [41] use the parameterization of elliptic curves by Shimura curves to define and work with Shimura degrees, a direct generalization of modular degrees. We discuss this work on Shimura degrees and briefly mention some of the interesting problems that arise when studying them and how they can be generalized.

1.1 Motivation

In 1801 Gauss published the following conjecture in Disquisitiones Arithmetica [14]:

Conjecture 1.1.1. *Let $h(D)$ be the class number of $\mathbb{Q}(\sqrt{D})$ for discriminant $D < 0$, then*

$$h(D) \to \infty \text{ as } D \to -\infty.$$

This conjecture stood until Hecke, Deuring, and Heilbronn proved this 133 years later in 1934. Their solution showed the limit, but did not effectively solve the problem. Namely, their solution does not give an algorithm for producing all discriminants D with a given given class number $h(D)$.

Work in effectively solving the Gauss class number problem was coming along at a slower rate. Even the class number one problem, listing all D such that $h(D) = 1$, had not been completely solved. That same year, 1934, Heilbron and Linfoot attacked the class number

one problem gave a list of nine $D < 0$'s with $h(D) = 1$ and showed there are at most ten $D < 0$.

Finding an effective solution lead to he (more difficult) modern version of Gauss' Class Number Problem as stated by Goldfeld [16]:

Conjecture 1.1.2. *There exists an effective algorithm for determining all negative discriminants D with a given class number $h(D)$.*

In 1952, Heegner gave an incomplete proof of the class number one case and in 1966, 1967, Baker and Stark respectively proved it:

Theorem 1.1.3. *The only discriminants $D < 0$ such that $h(D) = 1$ are*

$$D = -3, -4, -7, -8, -11, -19, -43, -67, \text{ and } -163.$$

The class number two problem came along much more quickly. In 1971 Baker and Stark independently proved the analogous this result.

Theorem 1.1.4. *There are exactly 18 imaginary quadratic fields with class number 2.*

The race was on to find all D such that $h(D) = 3$. This case would be prove to be more challenging and require new techniques. Is solving the $h(D) = 3$ case, modular elliptic curve L functions and many elliptic curve invariants come into play. For the first time, people were interested in computing modular degrees of elliptic curves parameterized by modular curves.

In 1985, combining work of Goldfeld and Gross-Zagier [16] using L-functions of modular elliptic curves led to a key part of the solution:

Theorem 1.1.5 (Goldfeld-Gross-Zagier)**.** *If there exists a modular elliptic curve E over $\mathbb{Q}$ whose associated base change Hasse-Weil L-Function $L_{E/\mathbb{Q}(\sqrt{D})}(s)$ has a zero of order greater than or equal to 4 at $s = 1$, then for every $\epsilon > 0$, there exists an effective compatible constant $c_\epsilon(E) > 0$, depending only on ϵ and E such that:*

$$h(D) > c_\epsilon(E) \cdot (\log |D|)^{1-\epsilon}.$$

To use this theorem, you need a modular elliptic curve of rank 3 or larger. You also must explicitly compute the constant $c_\epsilon(E)$ and among other things, compute the modular degree

of E. Until this point there was no systematic algorithm for computing modular degree. Modular degree could only be computed in very special cases. For a modular elliptic curve E parameterized by $X = \Gamma \setminus \mathcal{H} \cup \text{cusps}$, the degree of the map $\pi : X \to E$ could be computed if the elliptic curve was isomorphic to some modular curve $X' = \Gamma' \setminus \mathcal{H} \cup \text{cusps}$ for some Γ' between Γ and its normalizer. In this case $\deg(\pi) = [\Gamma' : \Gamma]$.

In 1984 Osterlé computed the constant $c_\epsilon(E)$ for the rank 3 curve $E : -139y^2 = x^3 + 4x^2 - 48x + 80$ of conductor $N = 37 \cdot (139)^2$. This gave

$$h(D) > \frac{1}{7000} (\log |D|) \prod_{p|D, p \neq D} \left(1 - \frac{[2\sqrt{p}]}{p+1}\right).$$

However, the constant $\frac{1}{7000}$ is too small and so this bound was not tight enough.

Additionally, ordered by conductor, this wasn't the smallest rank 3 curve. Brumer and Kramer found this smallest rank 3 curve

$$y^2 + y = x^3 - 7x + 6$$

with $N = 5077$. In 1984, Zagier created the algorithm which first computed its modular degree, also 1984.

Osterlé then noticed that this gives a better bound, good enough to finish $h(D) = 3$ case, but only if the elliptic curve was modular. In particular, it gave the bound:

$$h(D) > \frac{1}{55} (\log |D|) \prod_{p|D, p \neq D} \left(1 - \frac{[2\sqrt{p}]}{p+1}\right).$$

Fortunately, about this same time Mestre, Oesterle, and Serre proved this curve is modular. The bound given using this curve combined with other work to give a complete list of D such that $h(D) = 3$. It also lead to Zagier's [58] interest in a computing modular degrees and it lead to an observation by Ribet [58]: the modular degree divides the congruence number.

1.2 Classical Case

Let E be an elliptic curve over the rationals. Define

$$\Gamma_0(N) = \left\{ \gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{GL}_2(\mathbb{Z}) : c \equiv 0 \pmod{N} \right\}.$$

Then $\gamma \in \Gamma_0(N)$ acts on $\mathcal{H}$, the complex upper half plan, as a linear transformation:

$$\gamma z = \frac{az+b}{cz+d}.$$

The modular curve $X_0(N)$ is defined as the compactification of $\Gamma_0(N) \setminus \mathcal{H} \cup$ cusps. By work of Wiles [52]and others we know there exists a surjective morphism

$$\pi : X_0(N) \to E.$$

Many interesting results come from studying the degree of this map. Let f be a weight 2 level $\Gamma_0(N)$ newform. Assume that the Fourier coefficients, $a_n(f)$, of f are integers. Then associated to f is an isogeny class of elliptic curves defined over $\mathbb{Q}$ of level N. There is one particular curve in the isogeny class, say E, so that the map from the Jacobian of the modular curve $J_0(N) \to E$ has connected kernel. We call this curve the optimal quotient or the strong Weil curve. The degree of this map is called the modular degree. As the terminology suggests, the optimal quotient E can be written as a quotient of $J_0(N)$. More specifically, there is an action of Hecke operators on $J_0(N)$. Let $\mathbb{T}$ be the Hecke algebra that acts on $J_0(N)$. Let I_f be the kernel of the homomorphism $\mathbb{T} \to \mathbb{Z}[\cdots, a_n(f), \cdots]$ that sends T_n to $a_n(f)$. Then we can write E as the quotient $J_0(N)/I_f J_0(N)$.

Modular degrees have been of interest for over 30. Zagier was first interested in computing modular degrees because they were used in finding a bound for effective solutions Gauss's class number problem [58]. In [58] Zagier also discusses a result of Ribet; the modular degree divides the congruence number.s, i.e., the largest number for which there is a congruence between f and eigenforms orthogonal to f in $S_2(N)$. More recently, Agashe, Ribet, and Stein give in [1] a more precise statement regarding the relationship between modular degree and congruence numbers. In particular, for semistable elliptic curves the modular degree

and congruence numbers are equal. In [9] Stein and Conrad show how modular degree is a key component in computing component groups of abelian varieties at a prime p.

Work on computing the modular degree has been well explored. The first algorithms for computing it date back to Zagier's work in the early 1980's [58]. Watkins [56] discusses the history and the many methods used to compute modular degrees. He also discusses the running time and drawbacks of these methods. More importantly, Watkins [56] creates an algorithm using special values of a symmetric square L-function. This allows him to compute the modular degree of a rank 5 curve, which was not possible with the earlier methods.

Modular elliptic curves can be parameterized by other modular curves as well. The modular parameterization $X_1(N) \to E$ has also been studied. One of the more interesting aspects of this parameterization is the optimal quotient. In [47] Stein and Watkins prove Steven's conjecture; they prove that the optimal quotient of $X_1(N) \to E$ is the curve in the isogeny class with minimal Faltings height. This is an intrinsic way to characterize the optimal quotient. For elliptic curves parameterized by $X_0(N)$, there is no intrinsic characterization.

Interestingly, for the modular parameterization $X_1(N) \to E$, Agashe, Ribet, and Stein show that the modular degree does not divide the congruence number of $f \in S_2(\Gamma_1(N))$.

Via the Jacquet-Langlands correspondence, we can also associate to an isogeny class various quaternionic modular forms. Using a similar construction, we can parameterize a particular element E in the isogeny class by the Jacobian of a Shimura curve. Many of the interesting properties of modular degree then generalize to this case. We will be interested in this generalization, in particular to modular abelian varieties defined over totally real number fields associated to Hilbert modular forms. The relationship between Shimura degrees as congruence numbers will also be of interest.

1.3 Modular Degree

As before, let E be an elliptic curve over $\mathbb{Q}$ of conductor N and $X_0(N) = \Gamma_0(N) \setminus \mathcal{H} \cup \text{cusps}$ be the modular curve parameterizing E. By work due to Wiles and Taylor [57], [52], there is a surjective morphism $\pi : X_0(N) \to E$. This is called the modular parameterization.

Definition 1.3.1. Choose π to be of minimal degree. Then the degree m_E of the map π is called the *modular degree* of E.

To restate this definition more formally, we need the concept of optimal quotient. Let $J_0(N)$ be the Jacobian of the modular curve $X_0(N)$.

Definition 1.3.2. An *optimal quotient* of $J_0(N)$ is an abelian variety A and a surjective morphism $\pi : J \to A$ whose kernel is connected.

While all elliptic curves of conductor N in an isogeny class are parameterized by $J_0(N)$, only one will be an optimal quotient. All other morphisms $X_0(N) \to E'$ to elliptic curves E' factor through the optimal quotient.

For example, if $N = 42$, then there is one isogeny class and it contains six curves. All these curves are parameterized by $X_0(42)$. The curve $E : y^2 + xy + y = x^3 + x^2 - 4x + 5$, which has LMFDB label 42.a5 [31], is the optimal quotient of $X_0(42)$.

If E is an optimal quotient of $J_0(N)$, then the dual map $\pi^\vee : E \hookrightarrow J_0(N)$ is injective. This allows us to give an alternative definition of the modular degree. Let $\theta_E = \pi \circ \pi^\vee$. The following equivalent definition for modular degree was first given by Stein [46] and is as follows:

Definition 1.3.3. If E is an optimal quotient of $J_0(N)$, the *modular degree* of E as a quotient of $J_0(N)$ is the integer $m_E = \sqrt{\deg(\theta_E))}$.

1.4 Shimura Degree

Shimura curves are a natural generalization of modular curves. They are formed by the action of a discrete subgroup of $M_2(\mathbb{R})$ on $\mathcal{H}$. Instead being a moduli space parameterizing elliptic curves with some level structure, they are moduli spaces parameterizing abelian varieties with level structure. Further, in an analogous fashion, they have associated modular forms, quaternionic modular forms. Quaternionic modular forms give a similar parameterization of modular elliptic curves and abelian varieties.

More generally define the optimal quotient of a parameterization to be the abelian variety

in the isogeny class so that the map $J \to A$ has connected kernel. Then let E be an elliptic curve over $\mathbb{Q}$ that is an optimal quotient of the Jacobian of a Shimura curve J. The dual map is injective and so the composition of the map $\pi : J \to E$ and $\pi^\vee : E \to J$, $\pi \circ \pi^\vee \in \mathrm{End}(E)$ is multiplication by an integer. We will call this integer $\delta(J)$ the Shimura degree of E by J. Since in general E can be parameterized by many different Shimura curves, E will have many different Shimura degrees associated to it.

Elaborating on work of Takahashi [51], [50] and Ribet [41], I examine how to generalize Takahashi's work on computing the Shimura degrees of an elliptic curves over $\mathbb{Q}$ to abelian varieties and totally real number fields. The Shimura degrees are a direct generalization of the modular degree. Takahashi outlines an algorithm for computing Shimura degrees, i.e., degrees of parameterization of an elliptic curve over $\mathbb{Q}$ by the associated Shimura curves. This algorithm is based on the ability to compute with the character group of the Jacobian of the Shimura curve.

From Ribet [40] and Buzzard [6] we know of correspondences between these character groups and appropriate Hecke modules. Computing these Hecke modules has been made explicit by several people including Pizer [37], Kohel [27], and Voight [26].

If the discriminant of the curve is unique in the isogeny class, Takahashi's algorithm also finds the curve which is the optimal quotient in the isogeny class. I examine the uniqueness of discriminants in an isogeny class of semistable and show that discriminant twins only occur for conductors $11, 17, 19$, and 37. Using this result I am able to find the optimal quotient in every case. Examining discriminant twins over number fields, the same proofs hold but do not give the same results. Over number fields it is unknown if there are finitely many semistable isogenous discriminant twin pairs.

Finally, I compute tables of Shimura degrees, D-new modular degrees, and D-new congruence numbers. These tables allow me to make conjectures analogous to the theorems of Agashe, Ribet, and Stein [1]. In particular, the data suggests that for semistable elliptic curves the D-new modular degree, the D-new congruence number, and the Shimura degree $\delta^D(M)$ are all the same.

All code created and used for writing this paper is included in the appendix. Even though proofs and algorithms are given in the paper, code is precise and often clears up confusion. It can also be used to generate more examples.

Chapter 2

PRELIMINARIES

In this chapter I will introduce the necessary notation and the preliminary results needed to describe Shimura degrees and work with them. All results in this section are well known to the experts. In Section 2, I describe quaternion algebras over number fields and Eichler orders in these quaternion algebras. This gives the basic structure need to define Shimura curves and quaternionic modular forms. The following Sections 2.1 and 2.2 I define Shimura curves and Hilbert and quaternionic modular forms.

Section 2.3 gives all the background on Néron models necessary to define character groups, the monodromy pairing on character groups, and component groups. In the following Section 2.4, I use the parameterization of modular abelian varieties by Shimura curves to write maps between the character groups and component groups of the Jacobian of the Shimura curve and the parameterized modular abelian variety which are compatible with the respective monodromy pairings. This allows us to define the degree of this parameterization in terms of maps on character groups.

Studying the dual graphs of Shimura curves in Section 2.5 allows us to compare the component groups of Shimura curves of different levels. Using the dual graph construction also allows us to write the character groups of Shimura curves in terms of right ideal classes of definite quaternion algebras. Due to an algorithm for computing right ideal classes of quaternion algebras by Kirschmer and Voight [26], we can explicitly compute the character groups of Shimura curves. This in turn allows us to compute the degree of the map from the Shimura curve to the optimal abelian variety.

2.1 Quaternion Algebras

Quaternion algebras are the basic structure we will need to define Shimura curves, quaternionic modular forms, and also to implement our computations. We will use quaternion algebras to explicitly describe character groups of Jacobians of Shimura curves and the Hecke action on these objects. For further reference on quaternion algebras, see Vignéras [54].

Definition 2.1.1. A *quaternion algebra* B over a field F is a central simple algebra of dimension 4.

If the characteristic of F is not equal to 2, a more concrete way to view B is as an F-algebra generated by elements i and j, with

$$i^2 = a, \quad j^2 = b, \quad \text{, and} \quad ji = -ij$$

for some $a, b \in F^\times$. We denote such quaternion algebra B by $B = \left(\frac{a,b}{F}\right)$.

Two well known examples of quaternion algebras are the Hamiltonian quaternions, $\mathbb{H} = \left(\frac{-1,-1}{\mathbb{R}}\right)$ and the 2×2 matrices over $\mathbb{R}, \left(\frac{1,1}{\mathbb{R}}\right) \cong M_2(\mathbb{R})$. The isomorphism between $\left(\frac{1,1}{\mathbb{R}}\right) \cong M_2(\mathbb{R})$ is given by

$$i \mapsto \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \text{ and } j \mapsto \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

We can even view the Hamiltonians as a subalgebra of $M_2(\mathbb{C})$ via

$$i \mapsto \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} \text{ and } j \mapsto \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}.$$

In general, if K is an algebraic extension containing the square roots of both b and a, α, β respectively, if $i^2 = a$ and $j^2 = b$we can view B as a subgroup of $M_2(K)$ via the map

$$i \mapsto \begin{bmatrix} \alpha & 0 \\ 0 & -\alpha \end{bmatrix} \text{ and } j \mapsto \begin{bmatrix} 0 & \beta \\ -\beta & 0 \end{bmatrix}.$$

Elements of the quaternion algebra $B = \left(\frac{a,b}{F}\right)$, $i^2 = a, j^2 = b, ij = k$, can be written as $\alpha = x + yi + wj + zk$ for $x, y, w, z \in B$. The conjugation map $\overline{\alpha} = x - yi - wj - zk$

defines a standard involution on B. Notice that $\alpha\overline{\alpha} = x^2 - ay^2 - bw^2 + abz^2 \in F$ and $\alpha + \overline{\alpha} = 2x \in F$.

Definition 2.1.2. The *reduced norm* of B is $\mathrm{nrd}(\alpha) = \alpha\overline{\alpha}$ and the *reduced trace* of B is $\mathrm{trd}(\alpha) = \alpha + \overline{\alpha}$.

Via the embedding of a quaternion algebra into a matrix ring, the reduced trace map is the trace of the matrix and the reduced norm is the determinant of the matrix. The reduced norm $\mathrm{nrd} : B \to F$ is a quadratic form on B with associated bilinear form $T(x, y) : B \times B \to F$ given by

$$T(x, y) = (x + y)\overline{(x + y)} - x\bar{x} - y\bar{y} = x\bar{y} + y\bar{x} = \mathrm{trd}(x\bar{y}).$$

Now we restrict to number fields. Let F be a totally real number field of degree d with real places $\tau_1, ..., \tau_d$ and let K be any field containing F. By tensoring we construct a quaternion algebra over K, $B_K = B \otimes_F K$.

Definition 2.1.3. We say K *splits* B if $B_K \cong M_2(K)$.

In particular, we will be interested in the case where $K = F_\nu$ where ν is a non-complex place of F. As with number fields, we can look at splitting locally to examine ramification properties.

Let ν be a non-complex place of F and let F_ν be the completion of F at ν. Let $B_\nu = B \otimes_F F_\nu$. Then B_ν is either $M_2(F_\nu)$ or the unique division ring of dimension 4 over F_ν.

Definition 2.1.4. If F_ν splits B, i.e., $B_\nu \cong M_2(F_\nu)$, we say that B is *unramified* or *split* at ν. Otherwise we say that B is *ramified* at ν.

Quaternion algebras are ramified at only finitely many places. Further, they are only ramified at an even number of places. As B is a quaternion algebra over a number field F with ring of integers $\mathbb{Z}_F$, we can define the following invariant associated to B.

Definition 2.1.5. The *discriminant* of B, $\mathrm{disc}(B)$, is the ideal in $\mathbb{Z}_F$ that is the product of the finite ramified places of B.

In particular, if B is a quaternion algebra over $\mathbb{Q}$ that is split at ∞, then $D = \mathrm{disc}(B)$ is divisible by an even number of primes. If $B/\mathbb{Q}$ is ramified at ∞, then D is divisible by an

odd number of primes.

Definition 2.1.6. Fix an isomorphism $B \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathrm{M}_2(\mathbb{R})^r \times \mathbb{H}^{d-r}$. If $r = 0$, B is said to be *definite* (or sometimes totally definite). If $r \geq 1$, B is said to be *indefinite*.

If B is quaternion algebra over $\mathbb{Q}$ and is split at infinity, B is indefinite. If B is ramified at infinity, it is definite.

Assume $B = \left(\frac{a,b}{F}\right)$ is an indefinite quaternion algebra split at a real place ν of F, then $B_v = B \otimes \mathbb{R} \cong M_2(\mathbb{R})$. Via this isomorphism, we can view elements of B as 2 by 2 real matrices. Specifically, if $\nu(a) > 0$ and we pick an embedding of $\sqrt{a} \in \mathbb{R}$ so that $(\sqrt{a})^2 = a$,

$$x + iy + zj + tk \mapsto \begin{pmatrix} x + y\sqrt{a} & z + t\sqrt{a} \\ b(z - t\sqrt{a}) & x - y\sqrt{a} \end{pmatrix} \in \mathrm{M}_2(F(\sqrt{a})) \subset \mathrm{M}_2(\mathbb{R})$$

The elements of $B^\times$ with positive reduced norm (or determinant) act on $\mathcal{H}$ as linear fractional transformations. Notice that we have such action for every real embedding of F at which B splits. We use this action to create Shimura curves as a generalization of modular curves. As modular curves come from an action of a discrete subgroup of $\mathrm{SL}_2(\mathbb{R})$ so must Shimura curves. Thus we need subring of B which gives us appropriate discrete subgroups. These groups will be analogous to the ring of integers of a number field.

Definition 2.1.7. A $\mathbb{Z}_F$-*lattice* of B is a finitely generated $\mathbb{Z}_F$-submodule $\mathbb{Z}$ such that $F \otimes \mathcal{O} = B$. If $\mathcal{O}_B$ is a $\mathbb{Z}_F$-lattice of B and a subring of B then we say $\mathcal{O}_B$ is an *order* of B. A *maximal order* is an order that is not contained in any other order of B.

It is important to note that while maximal orders are a generalization of the ring of integers of a number field, in general maximal orders of quaternion algebras fail to be unique. For example, if $B \cong M_2(\mathbb{Q})$, then there are many maximal orders of B, all of which are conjugate to $M_2(\mathbb{Z})$. Maximal orders of quaternion algebras are the structure we will use to build our generalization of $\mathrm{SL}_2(\mathbb{Z})$. Suborders of maximal orders will give us our level structure.

Definition 2.1.8. An *Eichler order* $\mathcal{O}$ is an order that can be written as the intersection of two (not necessarily distinct) maximal orders. The *level* of $\mathcal{O}$ is the index
$M = [\mathcal{O}_B : \mathcal{O}]$, where $\mathcal{O}_B$ is a maximal order containing $\mathcal{O}$.

For example, a maximal order is trivially an Eichler order of level one.

We will frequently denote by $\mathcal{O}_B = \mathcal{O}_B(1)$ a maximal order of B and by $\mathcal{O}_B(\mathfrak{M})$ an Eichler order of level $\mathfrak{M}$ contained in $\mathcal{O}_B$. Again take the quaternion algebra $B \cong M_2(\mathbb{Q})$ of discriminant 1 is split at ∞. We've seen that $\mathcal{O}_B = \mathrm{M}_2(\mathbb{Z})$ is a maximal order of B. Then

$$\mathcal{O}_B(N) = \left\{ \begin{pmatrix} a & b \\ cN & d \end{pmatrix} : a, b, c, d \in \mathbb{Z} \right\}$$

is an Eichler order of level N. If we take all the norm one units of $\mathcal{O}_B(N)$, then $\mathcal{O}_B(N)^{\times,1} = \Gamma_0(N)$.

We can also examine quaternion orders locally. Let $\mathcal{O}$ be an order of B. Then for a non-complex place ν of F, we write $\mathcal{O}_\nu = \mathcal{O} \otimes \mathbb{Z}_{F_\nu}$ as a suborder of B_ν. Locally, B_ν is either split, $\mathrm{M}_2(F_\nu)$, or ramifies and is the unique division algebra over F_ν. In either case, we can completely classify what happens local when $\mathcal{O}$ is globally a maximal order or Eichler order.

If B_ν is ramified, everything works out quite nicely. In this case, B_ν has a single maximal order $\mathcal{O}_\nu$, which consists of all integral elements of B_ν. Thus if $\mathcal{O}$ was a maximal order $\mathcal{O}_\nu$ is as well. Further, every Eichler order $\mathcal{O}$ of B is locally maximal.

The more interesting case is when B_ν splits, so $B_\nu \cong \mathrm{M}_2(F_\nu)$. In this case all maximal orders of B are locally conjugate to $\mathrm{M}_2(\mathbb{Z}_{F_\nu})$. Further, we can classify all Eichler orders. Let π be a uniformizer of F_ν. Then locally, all Eichler orders of level $\pi^n \mid \mathfrak{N}$ are conjugate to the order

$$\mathcal{O}_B(\pi^n) = \left\{ \begin{bmatrix} a & b \\ \pi^n c & d \end{bmatrix} : a, b, c, d \in \mathbb{Z}_{F_\nu} \right\}.$$

We can construct a graph which has maximal orders of $\mathrm{M}_2(F_\nu)$ as vertices. Two vertices are connected by a single edge if and only if their intersection is an Eichler order of level π. This graph, Δ, is called the *Bruhat-Tits tree* of $\mathrm{PGL}_2(F_\nu)$. We will see this again later when we are using Mumford-Kurihara uniformization to describe the dual graphs of Shimura curves.

It will be useful to examine quaternion algebra structures at all non-archimedian places at the same time. Let

$$\hat{\mathbb{Z}} = \prod_{\mathfrak{p}}' \mathbb{Z}_{F_{\mathfrak{p}}}$$

be the restricted direct product. We denote by $\hat{}$, tensoring over $\mathbb{Z}$ with $\hat{\mathbb{Z}}$ In particular we will use $\hat{B} = B \otimes \hat{Z}$ and $\hat{\mathcal{O}}_B(\mathfrak{M}) = \mathcal{O}_B(\mathfrak{M}) \otimes \hat{Z}$. Notice that the double coset space

$$B^\times \setminus \hat{B}^\times / \hat{\mathcal{O}}_B(\mathfrak{M})^\times$$

is isomorphic to the set of right ideal classes of $\hat{\mathcal{O}}_B(\mathfrak{M})$. This correspondence will later allow us to compute character groups of Shimura curves.

To generalize the level structure, we use Eichler orders of indefinite quaternion algebras. For example, let B be a quaternion algebra over $\mathbb{Q}$ isomorphic to $M_2(\mathbb{Q})$. When we take the set of norm one units of $\mathcal{O}_B(N)$, as we have seen, this is exactly $\Gamma_0(N)$.

In general, let B be a quaternion algebra over a number field F of discriminant $\mathfrak{D}$ and let $\mathcal{O}_B$ be a maximal order of B. Take $\mathfrak{M}$ coprime to $\mathfrak{D}$ and let $\mathcal{O}_B(\mathfrak{M})$ be an Eichler order of level $\mathfrak{M}$. Then we can define a group that generalize the modular group $\mathrm{SL}_2(\mathbb{Z})$ and level structure.

Definition 2.1.9. Take B and $\mathcal{O}_B(\mathfrak{M})$ as above. Then

$$\Gamma_0^{\mathfrak{D}}(\mathfrak{M}) = \{x \in \mathcal{O}_B(\mathfrak{M})^\times : \mathrm{nrd}(x) = 1\}.$$

Now we have everything we need to define Shimura curves over number fields.

2.2 Shimura Curves

As before, let F be a totally real number field of degree d with embeddings $\tau_1, ..., \tau_d$ and take B to be a quaternion algebra over F split at τ_1 and ramified at $\tau_2, ..., \tau_d$. Then we can fix an isomorphism $B \otimes \mathbb{R} \cong M_2(\mathbb{R})$. Using this isomorphism, we have the usual action of elements of $B^\times$ with positive reduced norm on $\mathcal{H}$. Take $\mathfrak{M}$ to be an ideal of the ring of integers $\mathbb{Z}_F$ of F and let $\mathcal{O}$ be an Eichler order in B of level $\mathfrak{M}$. Then we can define the

Shimura curve over $\mathbb{C}$

$$X_0^{\mathfrak{D}}(\mathfrak{M})(\mathbb{C}) = B^\times \setminus \hat{B}^\times \times \mathcal{H}/\hat{\mathcal{O}}^\times.$$

Shimura proved that the curve $X_0^{\mathfrak{D}}(\mathfrak{M})$ has a canonical model over defined over F. We will write this model as $X_0^{\mathfrak{D}}(\mathfrak{M})$ and the points over $\mathbb{C}$ as $X_0^{\mathfrak{D}}(\mathfrak{M})(\mathbb{C})$.

Theorem 2.2.1 (Shimura [44])**.** *The Shimura curve $X_0^{\mathfrak{D}}(\mathfrak{M})$ is defined over F. It is the model for the quotient*

$$X_0^{\mathfrak{D}}(\mathfrak{M}) = \overline{\Gamma_0^{\mathfrak{D}}(\mathfrak{M}) \setminus \mathcal{H}}.$$

The bar indicates compactification. In general, $\Gamma_0^{\mathfrak{D}}(\mathfrak{M}) \setminus \mathcal{H}$ is already compact. The only case where $\Gamma_0^{\mathfrak{D}}(M) \setminus \mathcal{H}$ is not compact is the modular curve case, i.e., B is defined over $\mathbb{Q}$ with discriminant 1 and $\Gamma_0^1(M) = \Gamma_0(M)$ [43].

Analogously to the case of modular curves, we can define Hecke operators on these Shimura curves. To describe this action, given $g \in \hat{B}^\times$ and a pair of compact open subgroups $\mathcal{O}$ and $\mathcal{O}'$ of $\hat{B}^\times$ such that $g^{-1}\mathcal{O}g \subset \mathcal{O}'$. Multiplication on the right induces a natural map on on the Shimura curves over $\mathbb{C}$: $X_{\mathcal{O}}(\mathbb{C}) \to X_{\mathcal{O}'}(\mathbb{C})$. This map descents to a finite flat morphism on the models: $X_{\mathcal{O}} \to X_{\mathcal{O}'}$. From these maps, we can use double coset operators to define Hecke operators on $X_{\mathcal{O}}$. To see this, recall that we can write $[HgH] = \amalg_i (g_i H)$. Then given a complex point $x = [g, h] \in X_{\mathcal{O}}(\mathbb{C}) = B^\times \setminus \hat{B}^\times \times \mathcal{H}/\hat{\mathcal{O}}^\times$, the double coset operator acts on x as

$$[HgH](x) = \sum_i [xg_i, h] \in \mathrm{Div}(X_{\mathcal{O}}(\mathbb{C})).$$

Further, the Hecke operators have a natural left action on the Jacobian $J_{\mathcal{O}}$ of $X_{\mathcal{O}}$. Thus the Hecke algebra

$$\mathbb{T}_{\mathcal{O}} = \mathrm{End}_{\mathbb{Z}[\hat{B}^\times]}\left(\mathbb{Z}[\hat{B}^\times]\right) = \mathbb{Z}[\hat{\mathcal{O}}^\times \setminus \hat{B}^\times/\hat{\mathcal{O}}^\times]$$

can be viewed as a subring of the endomorphism ring of $J_{\mathcal{O}}$, $\mathbb{T}_{\mathcal{O}} \subset \mathrm{End}(J_{\mathcal{O}})$.

Shimura varieties can be defined more generally by allowing B to be unramified at more real places, or allowing more generic orders and thus different types of level structure, but here we are only interested in Shimura curves as defined above.

2.3 Hilbert and Quaternionic Modular Forms

Much of what has been done readily generalizes to abelian varieties over number fields. Let F be a totally real number field. Then we can let $J = J_0^{\mathfrak{D}}(\mathfrak{M})$ be the Jacobian of a Shimura curve over F, where $\mathfrak{N} = \mathfrak{D}\mathfrak{M}$ is a square-free ideal of $\mathbb{Z}_F$. Let A be a modular abelian variety over F with purely toric reduction that is an optimal quotient of J.

When we look more generally at modular abelian varieties over totally real number fields, they are no longer connected with classical modular forms, but are now (conjecturally) associated to Hilbert modular forms. Excitingly, modularity appears to have recently been proven in the case of real quadratic number fields [13].

Let F be a totally real number field of degree d with real embeddings $\tau_1, ..., \tau_d$. Let $\mathfrak{N}$ be an ideal of $\mathbb{Z}_F$. Let

$$\Gamma_0(\mathfrak{N}) = \{\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z}_F, c \in \mathfrak{N}, \det(\gamma) = 1\}.$$

Take $z = (z_1, ..., z_d) \in \mathcal{H}^d$. Then $\gamma \in \Gamma_0(\mathfrak{N})$ acts on $\mathcal{H}^d$ by the following linear fractional transformations $\gamma z = (\gamma_1 z_1, ..., \gamma_d z_1)$ where $\gamma_i = \begin{pmatrix} \tau_i(a) & \tau_i(b) \\ \tau_i(c) & \tau_i(d) \end{pmatrix}$.

Definition 2.3.1. Then Hilbert modular forms of weight $\bar{k} = (k_1, ..., k_d)$ and level $\mathfrak{N}$ are maps

$$f : \mathcal{H}^d \to \mathbb{C}$$

such that

$$f(\gamma z) = \prod_{i=1}^{d} (c_i z_i + d_i)^{k_i} f(z)$$

for all $\gamma \in \Gamma_0(\mathfrak{N})$.

Note that for $d > 1$, $\Gamma_0(\mathfrak{N})$ acts on $\mathcal{H}^d$ via each embedding and thus we have a Riemann form, $\Gamma_0(\mathfrak{N}) \setminus \mathcal{H}^d$ which is a Shimura variety due to Shimura [43]. As this is no longer a curve, we cannot construct a modular parameterization to an abelian variety. This is one of the reasons the Shimura degree is so interesting. It is definable in this more general situation where the modular degree does not necessarily exist. We can define quaternionic

modular forms over number fields and use the Eichler-Shimura-Jacquet-Langlands relation to construct the Shimura curve parameterization.

As Shimura curves are a direct generalization of modular curves, it would be nice if their Jacobians parameterized abelian varieties in a way analogous to modular curves. The Jacquet-Langlands theorem allows us to create this parameterization. Modular abelian varieties over totally real number fields have parameterizations by Jacobians of Shimura curves.

To use Jacobians of Shimura curves to parameterize elliptic curves, we need maps

$$f : \mathcal{H} \to \mathbb{C}$$

that behave like modular forms with respect to Shimura curves instead of modular curves or Hilbert modular varieties. Specifically, we need quaternionic modular forms.

Let B be an indefinite quaternion algebra of discriminant $\mathfrak{D}$ defined over a totally real number field F, ramified at $\tau_2, \cdots, \tau_d$, and split at τ_1. Let $\mathcal{O}_B(\mathfrak{M})$ be an Eichler order of level $\mathfrak{M}$ contained in B. Recall That $\Gamma_0^{\mathfrak{D}}(\mathfrak{M})$ is the set of norm 1 units in $\mathcal{O}_B^{\mathfrak{D}}(\mathfrak{M})$.

Definition 2.3.2. A *quaternionic modular form* of weight k on $\Gamma_0^{\mathfrak{D}}(\mathfrak{M})$ is a holomorphic function f on $\mathcal{H}$ such that

$$f(\gamma\tau) = (c\gamma + d)^k f(\tau) \text{ for all } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0^{\mathfrak{D}}(\mathfrak{M}).$$

The space of such forms is denoted by $\mathcal{M}_k^{\mathfrak{D}}(\mathfrak{M})$, and cusp forms by $\mathcal{S}_k^{\mathfrak{D}}(\mathfrak{M})$.

Quaternionic modular forms can be defined more generally. Specifically, they can be defined when B is split at more real places. When $B = M_2(F)$, then they are Hilbert modular forms.

As we are examining quaternionic modular forms for B split at only one real place, the Shimura curves only have cusps when they are actually modular curves over $\mathbb{Q}$. Thus in most cases the space of cusps forms is vacuously the entire space, i.e., $\mathcal{M}_k^{\mathfrak{D}}(\mathfrak{M}) = \mathcal{S}_k^{\mathfrak{D}}(\mathfrak{M})$. Further, the lack of cusps also indicates the lack of q-expansion.

The Jacquet-Langlands theorem gives us a correspondence between quaternionic modular forms and Hilbert modular forms. This is the correspondence that allows us to parameterize elliptic curves associated to Hilbert modular forms by Shimura curves.

Let $\mathfrak{M}, \mathfrak{D}$ be square-free ideals of F such that $\mathfrak{D}\mathfrak{M} = \mathfrak{N}$.

Theorem 2.3.3 (Jacquet-Langlands)**.** *There is an injective map of Hecke modules*

$$\mathcal{S}_2^{\mathfrak{D}}(\mathfrak{M}) \hookrightarrow \mathcal{S}_{\bar{2}}(\mathfrak{N})$$

whose image consists of those cusp forms that are new at all primes $\mathfrak{p}|\mathfrak{D}$*. In general,*

$$\mathcal{S}_2^{\mathfrak{D}}(\mathfrak{M}) \cong \mathcal{S}_{\bar{2}}(\mathfrak{N})^{\mathfrak{D}-new}.$$

Using this result, Zhang achieves exactly what we want for a special case. Take F, B, $\mathfrak{D}, \mathfrak{M}$, and $\mathfrak{N}$ as above. Let $f \in S_{\bar{2}}(\mathfrak{N})$ and define $\mathbb{Z}_f = \mathbb{Z}[a_n(f) : n \nmid \mathfrak{N}]$, which is an order in a number field.

Define the Shimura curve $X = X_0^{\mathfrak{D}}(\mathfrak{M})$, formed as usual from an Eichler of level $\mathfrak{M}$, in an indefinite quaternion algebra of discriminant $\mathfrak{D}$.

Theorem 2.3.4 (Zhang [59])**.** *If E is a modular elliptic over F of conductor $\mathfrak{N}$ and $\mathfrak{N}$ is square-free or the degree of F is odd, then E can be parameterized by the Shimura curve X.*

This works more generally for modular abelian varieties of GL_2 type, i.e., abelian varieties A such that $\mathrm{End}(A) \oplus \mathbb{Q}$ contains a totally real field of degree equal to the dimension of A.

To summarize what we know for elliptic curves over F, let $\mathcal{E}$ be an isogeny class of elliptic curves of conductor $\mathfrak{N}$. Let $J_0^{\mathfrak{D}}(\mathfrak{M})$ be the Jacobian of $X_0^{\mathfrak{D}}(\mathfrak{M})$ where $\mathfrak{D}\mathfrak{M} = \mathfrak{N}$. There exists a homomorphism

$$\pi : J_0^{\mathfrak{D}}(\mathfrak{M}) \to E$$

for some $E \in \mathcal{E}$, an optimal quotient of $J_0^{\mathfrak{D}}(\mathfrak{M})$. When E is parameterized by a modular curve, it is sometimes called the *strong Weil curve* instead of optimal quotient.

2.4 Néron Models and Character groups

In this section, we study Shimura curves and elliptic curves over number fields at their primes of bad reduction. This allows a definition of Shimura degree which yields a formula in terms of local invariants. Elliptic curves have bad reduction at exactly the primes dividing their conductors and Shimura curves $X_0^{\mathfrak{D}}(\mathfrak{M})$ have bad reduction exactly at the primes dividing $\mathfrak{D}\mathfrak{M}$. Specifically, we will study elliptic curves with multiplicative reduction as we have good tools for this case: Néron models and character groups. Since we will want the generality later, we will define these objects generally now.

Let R be a discrete valuation ring with field of fractions K. Let $\mathfrak{p}$ be the maximal ideal of R and $k = R/\mathfrak{p}$ be the residue field. Let A be an abelian variety over K. The case we will be interested in is when $K = F_{\mathfrak{p}}$ for a finite place $\mathfrak{p}$ and A is an elliptic curve or the Jacobian of Shimura curve.

Definition 2.4.1. The *Néron model*, $\mathcal{A}$, of A is a smooth commutative group scheme $\mathcal{A}$ over R such that A is its generic fiber and

$$\mathrm{Hom}_R(S, \mathcal{A}) \to \mathrm{Hom}_K(S_K, A)$$

is bijective for all smooth schemes S over R.

Néron models are unique up to isomorphism. Think of them as a "best possible" group scheme $\mathcal{A}$ over R such that after a base change from R to K are isomorphic to the original curve A/K. As we will be interested in the case where A is the Jacobian of a curve C, the Néron model of C can be constructed in terms of the minimal proper regular model $\mathcal{C}$ of A. As $\mathcal{C} \to R$ might not be smooth, let $\mathcal{C}'$ be the smooth locus of $\mathcal{C} \to R$ obtained by removing from each closed fiber $\mathcal{C}_k = \sum n_i C_i$ over all irreducible components with multiplicity $n_i \geq 2$, all singular points on each C_i, and all points where two C_i intersect each other. Then the group structure of A extends to a group structure on $\mathcal{C}'$ and $\mathcal{C}'$ equipped with this group structure is the Néron model.

The special fiber $\mathcal{A}_{\mathfrak{p}}$ of $\mathcal{A}$ is a group scheme that is not necessarily connected. To compute Shimura degrees, we will be interested in two groups associated with $\mathcal{A}_{\mathfrak{p}}$ and how they relate

to each other, the component group $\Phi_{\mathfrak{p}}(A)$ and the character group $\mathcal{X}_{\mathfrak{p}}(A)$. Let $\mathcal{A}_{\mathfrak{p}}^0$ be the connected component of $\mathcal{A}_{\mathfrak{p}}$ containing the identity. The following short exact sequence defines the component group $\Phi_{\mathfrak{p}}(A)$ as a finite group scheme:

$$0 \to \mathcal{A}_{\mathfrak{p}}^0 \to \mathcal{A}_{\mathfrak{p}} \to \Phi_{\mathfrak{p}}(A) \to 0.$$

Definition 2.4.2. The *component group* of an abelian variety A at k is the finite group scheme $\Phi_{\mathfrak{p}}(A) = \mathcal{A}_{\mathfrak{p}}/\mathcal{A}_{\mathfrak{p}}^0$.

We will be interested in the order of the component group $\Phi_{\mathfrak{p}}(A)$ over the algebraic closure $\bar{k}$ as this arises in the formula for Shimura degree. Further, if we just look at the $\mathbb{F}_{\mathfrak{p}}$ points of $\Phi_{\mathfrak{p}}(A)$, then the order of this group $\#\Phi_{\mathfrak{p}}(A)(k)$ is the Tamagawa number, which is a constant of great interests. For example, Tamagawa numbers are used in the conjectural Birch and Swinnerton-Dyer formula.

To define the the character group requires a bit more work. If K is a perfect extension field of k, by Chevalley's structure theorem [8], since $\mathcal{A}_{\mathfrak{p}}^0$ is connected, it has a largest connected normal affine subgroup $\mathcal{C}$ and there is a unique short exact sequence

$$0 \to \mathcal{C} \to \mathcal{A}_{\mathfrak{p}}^0 \to \mathcal{B} \to 0$$

such that $\mathcal{B} = \mathcal{A}_{\mathfrak{p}}^0/\mathcal{C}$ is an abelian variety.

Further, we have a unique short exact sequence for $\mathcal{C}$

$$0 \to \mathcal{T}_{\mathfrak{p}}(A) \to \mathcal{C} \to \mathcal{U} \to 0$$

where $\mathcal{T}_{\mathfrak{p}}(A)$ is a torus and $\mathcal{U}$ is unipotent. We call $\mathcal{T}_{\mathfrak{p}}(A)$ the *toral* part of A at k, or just the torus of A.

We can now define the character group. Let $\bar{k}$ be the algebraic closure of k.

Definition 2.4.3. The *character group* of an abelian variety A at $\mathfrak{p}$ is

$$\mathcal{X}_{\mathfrak{p}}(A) = \mathrm{Hom}_{\bar{k}}(\mathcal{T}_{\bar{k}}(A), \mathbb{G}_{m,\bar{k}}).$$

It is contraviantly associated to A.

So when we have a map $\pi : J \to A$ between abelian varieties, we have an induced map on the component groups $\pi : \mathcal{X}_{\mathfrak{p}}(A) \to \mathcal{X}_{\mathfrak{p}}(J)$.

It is worth mentioning that $\mathcal{T}_{\bar{k}}(A) \cong \mathbb{G}^a_{m,\bar{k}}$ for some $a \leq \dim(A)$. Further $\mathcal{X}_{\mathfrak{p}}(A)$ is a free $\mathbb{Z}$-module of rank a. Thus we will be working with free $\mathbb{Z}$-modules and many computations are reduced to linear algebra.

Definition 2.4.4. An abelian variety A has *purely toric reduction* if $\mathcal{A}^0_{\mathfrak{p}}$ is a torus. If $\mathcal{A}^0_{\mathfrak{p}}$ has vanishing unipotent part (is a semi-abelian variety) then A has *semi-stable reduction.*

If A is semistable, the monodromy paring gives a relationship between $\Phi_{\mathfrak{p}}(A)$ and $\mathcal{X}_{\mathfrak{p}}(A)$. Assume A has semistable reduction at k, then Grothendieck [19] gives us a *monodromy pairing*

$$u_{A,\mathfrak{p}} : \mathcal{X}_{\mathfrak{p}}(A) \times \mathcal{X}_{\mathfrak{p}}(A^\vee) \to \mathbb{Z}$$

and a short exact sequence

$$0 \to \mathcal{X}_{\mathfrak{p}}(A^\vee) \xrightarrow{\alpha} \mathrm{Hom}(\mathcal{X}_{\mathfrak{p}}(A), \mathbb{Z}) \to \Phi_{\mathfrak{p}}(A) \to 0$$

in that α is obtained from $u_{A,\mathfrak{p}}$ by the $(\alpha(x))(y) = u_{A,\mathfrak{p}}(x, y)$.

We will now use this short exact sequence to relate the Shimura curve to the appropriate elliptic curve.

2.5 Comparing Curves

Let J be a Jacobian of a curve defined over F. In particular we will take J to be the Jacobian of a modular curve or Shimura curve. Let E be an elliptic curve that is an optimal quotient of J. Since E and J are self-dual, we can rewrite the monodromy paring:

$$u_{J,\mathfrak{p}} : \mathcal{X}_{\mathfrak{p}}(J) \times \mathcal{X}_{\mathfrak{p}}(J) \to \mathbb{Z}$$

$$u_{E,\mathfrak{p}} : \mathcal{X}_{\mathfrak{p}}(E) \times \mathcal{X}_{\mathfrak{p}}(E) \to \mathbb{Z}$$

and the short exact sequence:

$$0 \to \mathcal{X}_{\mathfrak{p}}(J) \xrightarrow{\alpha_J} \mathrm{Hom}(\mathcal{X}_{\mathfrak{p}}(J), \mathbb{Z}) \to \Phi_{\mathfrak{p}}(J) \to 0$$

$$0 \to \mathcal{X}_{\mathfrak{p}}(E) \xrightarrow{\alpha_E} \mathrm{Hom}(\mathcal{X}_{\mathfrak{p}}(E), \mathbb{Z}) \to \Phi_{\mathfrak{p}}(E) \to 0$$

Further, as E is an optimal quotient of J, the contravariance of the character groups gives $\pi^* : \mathcal{X}_{\mathfrak{p}}(E) \to \mathcal{X}_{\mathfrak{p}}(J)$ and induces the following diagram:

$$\begin{tikzcd}
0 \arrow[r] & \mathcal{X}_{\mathfrak{p}}(J) \arrow[r] \arrow[d, "\pi_*"] & \mathrm{Hom}(\mathcal{X}_{\mathfrak{p}}(J), \mathbb{Z}) \arrow[r] \arrow[d] & \Phi_{\mathfrak{p}}(J) \arrow[r] \arrow[d, "\pi_*"] & 0 \\
0 \arrow[r] & \mathcal{X}_{\mathfrak{p}}(E) \arrow[r] & \mathrm{Hom}(\mathcal{X}_{\mathfrak{p}}(E), \mathbb{Z}) \arrow[r] & \Phi_{\mathfrak{p}}(E) \arrow[r] & 0
\end{tikzcd}$$

This allows us to define the following invariants:

Definition 2.5.1. Let $\pi_* : \Phi_{\mathfrak{p}}(J) \to \Phi_{\mathfrak{p}}(E)$, then

$$\bar{c}_{\mathfrak{p}} = \#\Phi_{\mathfrak{p}}(E) \quad i_{\mathfrak{p}} = \#\mathrm{image}(\pi_*) \quad j_{\mathfrak{p}} = \#\mathrm{coker}(\pi_*)$$

Further, we have the following relationship between the monodromy pairings. Let $x \in \mathcal{X}_{\mathfrak{p}}(E)$. Then

$$\delta \cdot u_{E,\mathfrak{p}}(x, x) = u_{E,\mathfrak{p}}(x, \pi_*(\pi^*(x))) = u_{J,\mathfrak{p}}(\pi^* x, \pi^* x).$$

We will come back to these relations once we have ways to compute $\mathcal{X}_{\mathfrak{p}}(J)$ and u_J.

2.6 Dual Graphs

Now we switch gears to discuss dual graphs of Jacobians of curves. Our goal here is to compute character groups of Jacobians of Shimura curves and to compute Hecke operators on them as well. To do this we first describe algebraic cycles and then come full circle to see how we can represent them as Bruhat-Tits trees. Dual graphs of Shimura curves will allow us to write the character groups in terms of right ideal classes of definite quaternion algebras and in turn, compare different levels. For Shimura curves, we need the more general case where the curve is admissible. First we follow Ribet's introduction to dual graphs and the Picard-Lefschetz formula. We then use work of Carayol [7] to explicitly describe the supersingular points and irreducible components of a Shimura curve at a prime dividing the level. Using Cerednick uniformization [5] we are able to similarly parameterize the dual

graph of a Shimura curve at a prime the discriminant. Combining this information we can write a short exact sequence comparing character groups of Shimura curves. This is a direct generalization of Ribet's short exact sequence in [40] as found in work by Rajaei [38] and Jarvis [22], [23].

As in the previous section let $\mathfrak{p}$ be a prime and let K be a $\mathfrak{p}$-adic field of characteristic 0. Let R be the ring of integers of K and let k be the residue field of characteristic $\mathfrak{p}$. Let C be a curve over K. Eventually, we will take C to be our Shimura curve. Let $\mathcal{J}$ be the Néron model of the Jacobian of C and $\mathcal{J}_{\mathfrak{p}}$ the special fiber. Take $\mathcal{C}$ to be the regular model of C over R. If the greatest common divisors of the irreducible components of $\mathcal{C}_{\mathfrak{p}}$ is one, then due to Raynaud, see appendix of [32], the Jacobian of $\mathcal{C}_{\mathfrak{p}}$ is isomorphic to $\mathcal{J}_{\mathfrak{p}}$.

If the all the singular points of $\mathcal{C}_{\mathfrak{p}}$ are ordinary double points, then $\mathcal{J}_{\mathfrak{p}}$ is an extension of an abelian variety A by a torus $\mathcal{T}_{\mathfrak{p}}$. Writing $\mathcal{C}_{\mathfrak{p}}$ as the disjoint union of non-singular curves D_j, the normalization map $\cup D_j \to \mathcal{C}_{\mathfrak{p}}$ induces a surjection

$$\mathcal{J}_{\mathfrak{p}} \to \prod_i \mathrm{Pic}^0 D_j = A$$

where the kernel is the torus T.

We will study an alternate way to express this. We will use the *dual graph* $\mathcal{G}$ attached to $\mathcal{C}_{\mathfrak{p}}$. This is the unoriented graph with vertices, $\mathcal{V}(\mathcal{G})$, the set of irreducible components of $\mathcal{C}_{\mathfrak{p}}$, and edges, $\mathcal{E}(\mathcal{G})$, the set of singular points of $\mathcal{C}_{\mathfrak{p}}$. The edge corresponding to a singular point $e \in \mathcal{E}$ connects the two vertices corresponding to the two components of $\mathcal{C}_{\mathfrak{p}}$ which meet at e.

Proposition 2.6.1. *There is a canonical isomorphism from the torus to the first cohomology group*

$$\mathcal{T}_{\mathfrak{p}} \cong H^1(\mathcal{G}, \mathbb{Z}) \otimes \mathbb{G}_m$$

and equivalently there is a canonical isomorphism from the character group of $\mathcal{T}_{\mathfrak{p}}$ to the first homology group

$$\mathcal{X}(\mathcal{T}_{\mathfrak{p}}) \cong H_1(\mathcal{G}, \mathbb{Z}).$$

For proof, see Grothendieck, SGA7 section 12.3.7 [19].

As our goal is to compute $\mathcal{X}$, we would like to identify $\mathcal{X}$ with a subgroup of $\mathbb{Z}[\mathcal{E}(\mathcal{G})]$. Let $\mathbb{Z}[\mathcal{V}(\mathcal{G})]^0$ be the group of degree-0 formal linear combinations of elements of $\mathbb{Z}[\mathcal{V}(\mathcal{G})]$.

Proposition 2.6.2. *The group $\mathcal{X}$ corresponds with the kernel of the homomorphism defined by*

$$\alpha : \mathbb{Z}[\mathcal{E}(\mathcal{G})] \to \mathbb{Z}[\mathcal{V}(\mathcal{G})]^0$$

given by $\alpha(e) = j_1(e) - j_2(e)$.

One problem so far, is that we would like to examine curves that are not necessarily regular. Instead we examine admissible curves $\mathcal{C}$ in the sense of Jordan-Livné, which relaxes the condition that $\mathcal{C}$ be regular.

Definition 2.6.3. We say a curve C over R is *admissible* if

1. C is proper and flat over R, and has a smooth generic fiber.
2. The special fiber $\mathcal{C}_k$ is reduced. The normalization of each of its irreducible components is isomorphic to $\mathbb{P}^1_k$ and $\mathcal{C}_k$ has only k-rational, ordinary double points as singularities.
3. The completion of the local ring of C at any one of its singular points e is isomorphic to an R-algebra $R[[X,Y]]/(XY - \pi^{n(e)-1})$ for some uniquely determined integer $n(e) > 1$.

This is the case we will need for the Shimura curves that parameterize elliptic curves.

Again, let $\mathcal{G}$ be the dual graph of $\mathcal{C}_k$ as defined above. For each $e \in \mathcal{E}$, let $n(e)$ be the integer such that the regular minimal model for C can be obtained from $\mathcal{C}_k$ by replacing each singular point e by a chain of $n(e) - 1$ copies of $\mathbb{P}^1$.

We can construct a graph $\tilde{\mathcal{G}}$ on this blow up of $\mathcal{C}_k$. Contracting the $\mathbb{P}^1$'s gives a surjective map

$$\tilde{\mathcal{E}} \to \mathcal{E}.$$

In the other direction, we have the map

$$\tau : \mathbb{Z}[\mathcal{E}] \to \mathbb{Z}[\tilde{\mathcal{E}}]$$

which takes e to the sum of its preimage in $\tilde{\mathcal{E}}$. This map is then an injection, with torsion free cokernel.

We can also examine maps between the vertices. As $\mathcal{V}(\mathcal{G}) \subset \mathcal{V}(\tilde{\mathcal{G}})$, we have an injection

$$\mathbb{Z}[\mathcal{V}(\mathcal{G})] \hookrightarrow \mathbb{Z}[\mathcal{V}(\tilde{\mathcal{G}})].$$

Moreover, we can restrict to the degree 0 divisors and again get an injection

$$\iota : \mathbb{Z}[\mathcal{V}(\mathcal{G})]^0 \hookrightarrow \mathbb{Z}[\mathcal{V}(\tilde{\mathcal{G}})]^0.$$

Thus following Ribet's exposition [40] we have the following theorem of Raynaud

Theorem 2.6.4 ([40])**.** *There is a canonical short exact sequence*

$$\begin{tikzcd}
0 \arrow[r] & \mathcal{X} \arrow[r] \arrow[d, equal] & \mathbb{Z}[\mathcal{E}(\mathcal{G})] \arrow[r, "\alpha"] \arrow[d, "\tau"] & \mathbb{Z}[\mathcal{V}(\mathcal{G})]^0 \arrow[r] \arrow[d, "\iota"] & 0 \\
0 \arrow[r] & \mathcal{X} \arrow[r] & \mathbb{Z}[\mathcal{E}(\tilde{\mathcal{G}})] \arrow[r] & \mathbb{Z}[\mathcal{V}(\tilde{\mathcal{G}})]^0 \arrow[r] & 0
\end{tikzcd}$$

where ker$(d_*) \cong \mathcal{X}$*.*

Via this construction, Ribet [40]proves the following theorem.

Theorem 2.6.5 (Ribet [40])**.** *There is a natural homomorphism* $\Theta : \mathbb{Z}[\mathcal{V}(\mathcal{G})]^0 \to \Phi$ *whose cokernel is a quotient of the group Hom*$(\mathbb{Z}[\mathcal{E}], \mathbb{Z})/\mathbb{Z}[\mathcal{E}] \cong \oplus_{e \in \mathcal{E}}(\mathbb{Z}/n(e)\mathbb{Z})$*.*

2.7 Dual Graphs of Shimura Curves

Now that we have a parameterization of the character group for admissible curves, we use Mumford-Kurihara uniformization [30] to show that our curves are indeed admissible. Then we use work of Carayol [7] and Jarvis [22] to describe the supersingular points and geometrically irreducible components when $\mathfrak{p}$ divides the level. With a bit more work and Cerednick uniformization [5], we will be able to write the component group of the Shimura curve in the case when $\mathfrak{p}$ divides the discriminant in terms of another Shimura curve where $\mathfrak{p}$ divides the level.

First we discuss the Mumford-Kurihara uniformization. For more background, see [5]. Recall that F is a totally real number field. Let $\mathfrak{p}$ be a finite prime of F over p. Let $K = F_{\mathfrak{p}}$ and $\mathbb{C}_{\mathfrak{p}}$ the completion of a fixed algebraic closure of K. Then take $\hat{\Omega} = \hat{\Omega}_K$ to be the $\mathfrak{p}$-adic upper

half plane over K. Viewing $\hat{\Omega}$ as a formal scheme over $\mathbb{Z}_{F_\mathfrak{p}}$, $\hat{\Omega}$ is flat and locally of finite type over $\mathbb{Z}_{F_\mathfrak{p}}$. Further, $\hat{\Omega}$ is regular and irreducible and supports an action of $\mathrm{GL}_2(F_\mathfrak{p})$. Let Ω be the generic fiber. Then Ω is a rigid analytic space with $\mathbb{C}_\mathfrak{p}$ points $\Omega(\mathbb{C}_\mathfrak{p}) = \mathbb{C}_\mathfrak{p} - F_\mathfrak{p}$. It also supports an action of $\mathrm{GL}_2(F_\mathfrak{p})$.

The special fiber of $\hat{\Omega}$ is reduced an geometrically connected. Further, the dual graph of $\hat{\Omega}_\mathfrak{p}$ is the Bruhat-Tits tree Δ of $\mathrm{SL}_2(F_\mathfrak{p})$. The following theorem will give us the dual graphs of Shimura curves relative to Δ.

Theorem 2.7.1 (Mumford-Kurihara [30]). *If $\Gamma \subset PGL_2(F_\mathfrak{p})$ is any discrete, cocompact subgroup, then the associated scheme $\Omega_\Gamma = \Gamma \setminus \hat{\Omega}$ is an admissible curve over $\mathbb{Z}_{F_\mathfrak{p}}$. Its dual graph is isomorphic to $\Gamma \setminus \Delta$, minus any loops.*

2.7.1 When $\mathfrak{p}$ divides the level.

Now we would like to explicitly compute the character groups of our Shimura curves. We will do this in two parts, when $\mathfrak{p}$ divides the level of the Eichler order and when $\mathfrak{p}$ the discriminant of the quaternion algebra. Then we will relate these two cases together which will allow us to compute the character group when $\mathfrak{p}$ divides the discriminant and further, it will allow us to compare the degrees of parameterization between two different Shimura curves.

When $\mathfrak{p}$ divides the level of the quaternion algebra, due to work of Morita and Carayol [7], the Shimura curve has good reduction and there exists a unique, smooth, proper model over $\mathbb{Z}_{F,(\mathfrak{p})}$. We can explicitly write down the set of super singular points of the Shimura curve. In this case, let B be an indefinite quaternion algebra over F of discriminant $\mathfrak{D}$, split at τ_1, and ramified at $\tau_2, \cdots, \tau_d$, and let $\mathcal{O} = \mathcal{O}_B(\mathfrak{p}\mathfrak{M})$ be an Eichler order of B of level $\mathfrak{p}\mathfrak{M}$. As before, we denote by $X = X_0^{\mathfrak{D}}(\mathfrak{p}\mathfrak{M})$ our Shimura curve. Let $X' = X_0^{\mathfrak{D}}(\mathfrak{M})$.

Next, let H be the definite quaternion algebra ramified at $\tau_1, \cdots, \tau_n$ with discriminant $\mathfrak{p}\mathfrak{D}$ and let $\mathcal{O}_H(\mathfrak{M})$ be an Eichler order of H of level $\mathfrak{M}$.

Theorem 2.7.2 (Carayol [7], Jarvis [22]). *Let $X_\mathfrak{p}^{ss}$ denote the set of super singular points*

of $X_{\mathfrak{p}}$. Then

$$X_{\mathfrak{p}}^{ss} \cong H^{\times} \setminus \hat{H}^{\times}/\mathcal{O}_H(\mathfrak{M}).$$

Further, the irreducible components of $X_{\mathfrak{p}}$ consist of two copies of the irreducible curve $X'_{\mathfrak{p}}$ intersecting transversally at the supersingular points via the Frobenius morphism at $\mathfrak{p}$.

Thus via the dual graph, the character group of the Jacobian of X is isomorphic to the degree zero sums on the free $\mathbb{Z}$-module on the set of super singular points of X. Further, we know this set of super singular points corresponds to right ideal classes of $\mathcal{O}_H(\mathfrak{M})$ [7]. In particular, we have the following relationship between $\mathcal{X}_{\mathfrak{p}}$, the character group of the Jacobian of $X_{\mathfrak{p}}$, and the dual graph of $X_{\mathfrak{p}}$.

Corollary 2.7.3. *For $\mathfrak{p} \mid \mathfrak{M}$, the character group $\mathcal{X}_{\mathfrak{p}} \cong \mathbb{Z}[\mathcal{E}(\mathcal{G})]^0$*

Proof. This follows from Raynaud's short exact sequence and Carayol's description of the supersinglar points and irreducible components. □

Note that $H^{\times} \setminus \hat{H}^{\times}/\mathcal{O}_H(\mathfrak{M})$ is in bijection with the right ideal class of $\mathcal{O}_H(\mathfrak{M})$. As we can now write the character group $\mathcal{X}_{\mathfrak{p}}$ in terms of degree zero divisors on $H^{\times} \setminus \hat{H}^{\times}/\mathcal{O}_H(\mathfrak{M})$, we have

$$\mathcal{X}_{\mathfrak{p}} \cong \mathbb{Z}[\mathrm{Cl}(\mathcal{O}_H(\mathfrak{M}))]^0,$$

i.e., $\mathcal{X}_{\mathfrak{p}}$ is isomorphic to the formal sums of degree zero on right ideal classes of the Eichler order $\mathcal{O}_H(\mathfrak{M})$.

By functorality of character groups, the Hecke operators on the Shimura curve induce Hecke operators on the character groups. We will see in future Section 4 that these Hecke operators are fully compatible via the right ideal class correspondence.

2.7.2 When p divides the Discriminant

The case where $p \mid D$ is significantly different. For this we need p-adic uniformization. Recall that $\hat{\Omega}$ is the $\mathfrak{p}$-adic upper half plane over $F_{\mathfrak{p}}$. Let $F_{\mathfrak{p}}^{unr}$ be the maximal unramified extension

of $F_{\mathfrak{p}}$, and let $\mathcal{O}_{F_{\mathfrak{p}}}^{unr}$ be its ring of integers. Then take $\hat{\Omega}^{unr}$ to be

$$\hat{\Omega}^{unr} = \hat{\Omega} \times_{\mathrm{Spf}(\mathcal{O}_{F_{\mathfrak{p}}})} \mathrm{Spf}(\mathcal{O}_{F_{\mathfrak{p}}^{unr}}).$$

Next, let B be the indefinite quaternion algebra split at τ_1, ramified at $\tau_2, \cdots, \tau_d$, with discriminant $\mathfrak{p}\mathfrak{D}$. Let $\mathcal{O}$ be an Eichler order in B of level $\mathfrak{M}$. Denote by $X_0^{\mathfrak{p}\mathfrak{D}}(\mathfrak{M})$ the associated Shimura curve. We again use an auxiliary definite quaternion algebra. Let H be the definite quaternion algebra ramified at $\tau_1, \cdots, \tau_d$ with discriminant $\mathfrak{D}$. Let $\mathcal{O}_H(\mathfrak{M})$ be an Eichler order in H of level $\mathfrak{M}$ and $\mathcal{O}_H(\mathfrak{M}\mathfrak{p})$ be an Eichler order of H of level $\mathfrak{M}\mathfrak{p}$.

Theorem 2.7.4 (Cerednik-Drinfeld [5])**.** *There is a canonical integral model of the Shimura curve $X_0^{\mathfrak{p}\mathfrak{D}}(\mathfrak{M})$ over $\mathbb{Z}_{F_{\mathfrak{p}}}$, again denoted by $X = X_0^{\mathfrak{p}\mathfrak{D}}(\mathfrak{M})/\mathbb{Z}_{F_{\mathfrak{p}}}$. Further, there is a canonical isomorphism of $\mathbb{Z}_{F_{\mathfrak{p}}}$-formal schemes*

$$X/\mathbb{Z}_{F_{\mathfrak{p}}} \cong GL_2(F_{\mathfrak{p}}) \setminus \hat{\Omega}^{unr} \times H^{\times} \setminus \hat{H}^{\times}/\mathcal{O}_H. \tag{2.7.1}$$

With this $\mathfrak{p}$-adic uniformization, we can explicitly write the edges and vertices of the dual graph of $X_{\mathfrak{p}}$.

Corollary 2.7.5. *Let $\mathcal{G}$ be the dual graph of $X_{\mathfrak{p}}$. Then*

$$\mathcal{V}(\mathcal{G}) \cong H^{\times} \setminus \hat{H}^{\times}/\mathcal{O}_H(\mathfrak{M}) \times \mathbb{Z}/2\mathbb{Z}$$

$$\mathcal{E}(\mathcal{G}) \cong H^{\times} \setminus \hat{H}^{\times}/\mathcal{O}_H(\mathfrak{p}\mathfrak{M}).$$

We can also explicitly write the maps

$$\alpha, \beta : \mathcal{E}(\mathcal{G}) \to \mathcal{V}(\mathcal{G}) \tag{2.7.2}$$

in terms of the above right ideal class parameterization. The map α is just the inclusion of $\mathcal{O}_H(\mathfrak{p}\mathfrak{M})$ into $\mathcal{O}_H(\mathfrak{M})$. Let $\pi_{\mathfrak{p}}$ a uniformizing element. The map β is obtained by considering the Eichler order $\mathcal{O}_{H,g}(\mathfrak{M}) = g^{-1}\mathcal{O}_H(\mathfrak{M})g$ conjugate to $\mathcal{O}_H(\mathfrak{M})$ by an element $g \in \hat{H}^{\times}$ where g is the diagonal matrix

$$\begin{pmatrix} 0 & 1 \\ \pi_{\mathfrak{p}} & 0 \end{pmatrix}$$

and is the identity everywhere else. We can then identify

$$H^\times \setminus \hat{H}^\times / \mathcal{O}_H(\mathfrak{M}) \to H^\times \setminus \hat{H}^\times / \mathcal{O}_{H,g}(\mathfrak{M})$$

via multiplication by g^{-1} on $\hat{H}^\times$. From this we see that β maps the ideal class $[I]$ in $H^\times \setminus \hat{H}^\times / \mathcal{O}_H(\mathfrak{p}\mathfrak{M})$ to the class of $[g^{-1}I]$ in $H^\times \setminus \hat{H}^\times / \mathcal{O}_{H,g}(\mathfrak{M})$.

Further, we can now write the character group $\mathcal{X}_\mathfrak{p}$ explicitly in terms of right ideal classes of Eichler orders using dual graphs 2.6. While this is enough to compute $\mathcal{X}_\mathfrak{p}$, it will be useful to relate this character group to the character groups of other Shimura curves as in [40].

Let B now be the indefinite quaternion algebra of discriminant $\mathfrak{D}\mathfrak{p}\mathfrak{q}$ with Eichler order $\mathcal{O}_B(\mathfrak{M})$ of level $\mathfrak{M}$. Let H be the definite quaternion algebra of discriminant $\mathfrak{D}\mathfrak{q}$ with Eichler orders $\mathcal{O}_H(\mathfrak{M})$ and $\mathcal{O}_H(\mathfrak{M}\mathfrak{p})$ of levels $\mathfrak{M}$ and $\mathfrak{M}\mathfrak{p}$ respectively. Next, let B' be the indefinite quaternion algebra $\mathfrak{D}$ and with Eichler orders $\mathcal{O}_{B'}(\mathfrak{M}\mathfrak{q})$ and $\mathcal{O}_{B'}(\mathfrak{M}\mathfrak{p}\mathfrak{q})$ with levels $\mathfrak{M}$ and $\mathfrak{M}\mathfrak{p}$ respectively. We now notice that H is the auxiliary quaternion algebra for both cases, where $\mathfrak{p} \mid \mathfrak{D}$ and where $\mathfrak{q} \mid \mathfrak{M}$. The edge of vertices of the graph of$\mathcal{X}_\mathfrak{p}(J_0^{\mathfrak{D}\mathfrak{p}\mathfrak{q}}(\mathfrak{M}))$ correspond to the character groups of $\mathcal{X}_\mathfrak{q}(J_0^{\mathfrak{D}}(\mathfrak{M}\mathfrak{p}\mathfrak{q}))$ and $\mathcal{X}_\mathfrak{q}(J_0^{\mathfrak{D}}(\mathfrak{M}\mathfrak{q}))$ respectively.

Note that by functorality of character groups, we have an induced action of Hecke algebras in $\mathrm{End}(J)$ on $\mathcal{X}_\mathfrak{p}(J)$ where J is the Jacobian of a Shimura curve.

Proposition 2.7.6. *With the given notation, we have the following short exact sequence of Hecke modules*

$$0 \to \mathcal{X}_\mathfrak{p}(J_0^{\mathfrak{D}\mathfrak{p}\mathfrak{q}}(\mathfrak{M})) \to \mathcal{X}_\mathfrak{q}(J_0^{\mathfrak{D}}(\mathfrak{M}\mathfrak{p}\mathfrak{q})) \to \mathcal{X}_\mathfrak{q}(J_0^{\mathfrak{D}}(\mathfrak{M}\mathfrak{q})) \times \mathcal{X}_\mathfrak{q}(J_0^{\mathfrak{D}}(\mathfrak{M}\mathfrak{q})) \to 0.$$

Chapter 3

SHIMURA DEGREES

Here we will see that the formula for Shimura degrees can be defined more generally for modular abelian varieties over number fields. Further, due to the generalization of Ribet's short exact sequence comparing levels, we can generalize much of the work of Takahashi comparing different Shimura degrees. We start by recapping Shimura degrees for elliptic curves over $\mathbb{Q}$, with proofs left for the more general Section 3.1. In Section 3.1 we will define Shimura degrees for modular abelian varieties over totally real number fields and extend results of Takahashi and Ribet [41] to this case.

3.1 Shimura Degrees over $\mathbb{Q}$

For this section, let B be an indefinite quaternion algebra over $\mathbb{Q}$ with discriminant D. Let $\mathcal{O}$ be an Eichler order in B of level M. Then we have the Shimura curve $X_0^D(M)$ with Jacobian $J_0^D(M)$. Assume $E/\mathbb{Q}$ is an elliptic curve with square-free conductor $N = DM$ and further, is an optimal quotient of $J_0^D(M)$. Recall that this implies that the map $\pi : J_0^D(M) \to E$ has a connected kernel, which in turn means the dual map is injective:

$$\pi^\vee : E \to J_0^D(M)$$

and $\pi \circ \pi^\vee \in \mathrm{End}(E)$ is multiplication by an integer $\delta^D(M)$.

Definition 3.1.1. The square root of this integer, $\delta^D(M)$, is called the *Shimura Degree* of E with respect to $J_0^D(M)$.

Depending on how N factors, it is possible for an isogeny class to have many different Shimura degrees. For example, if $N = p$, then there is only one option, $D = 1$, $M = p$,

the modular degree. If $N = pq$, then there are two options $D = pq$, $M = 1$ and $D = 1$, $M = pq$.

By examining the Shimura degree in terms of character and component groups, we get a formula for the Shimura degree. Let E be an optimal quotient of J. Let $f \in \mathcal{S}_2(N)$ be the newform associated to the isogeny class of E. Take $\mathbb{T}$ to be the Hecke algebra over $\mathbb{Z}$ of endomorphisms of $\mathcal{S}_2(N)$ and let p be a prime exactly dividing N. Recall from before:

Let $\pi_* : \Phi_p(J) \to \Phi_p(E)$

$$\bar{c}_p = \#\Phi_p(E) \quad i_p = \#\text{image}(\pi_*) \quad j_p = \#\text{coker}(\pi_*).$$

Following directly from this definition $j_p = \frac{\bar{c}_p}{i_p}$.

We need one further invariant to compute the Shimura degree. Recall that $\mathcal{X}_p(J)$ has an action of the Hecke module $\mathbb{T}$ functorially induced from the action of $\mathbb{T}$ on J. Using $f \in S_2(N)$ associated the isogeny class of E, we can define the following one dimensional subspace of $\mathcal{X}_p(J)$:

Definition 3.1.2. Define the f-isotypical component $\mathcal{L}_p(f) \subset \mathcal{X}_p(J)$ as

$$\mathcal{L}_p(f) = \{x \in \mathcal{X}_p(J) : T_n x = a_n(f)x \text{ for all } n \text{ coprime to } N\}.$$

To view this more concretely, view J as its decomposition, up to isogeny, of simple abelian varieties defined over $\mathbb{Q}$. Then the optimal quotient E occurs uniquely as a factor of J. The other factors correspond to other $g \in \mathcal{S}_2(N)$, $g \neq f$. We are using the Hecke operators to cut out the subspace $\mathcal{L}_p(f)$ that corresponds to E.

Recall the monodromy paring $u_{J,p} : \mathcal{X}_p(J) \times \mathcal{X}_p(J) \to \mathbb{Z}$. Let g_p be a generator of $\mathcal{L}_p(f)$. The final invariant we need is:

Definition 3.1.3.

$$h_p = u_{J,p}(g_p, g_p).$$

Takahashi states and proves the following for elliptic curves over $\mathbb{Q}$.

Theorem 3.1.4 (Takahashi [50]). *i_p divides h_p, j_p divides δ_M^D and*

$$\delta_M^D = \frac{h_p}{i_p} j_p. \tag{3.1.1}$$

Notice that the above equation does not depend on which $p \mid N$. To find δ_M^D, we only have to find h_p, i_p, and j_p for one prime p exactly dividing N.

To show this, Takahashi proves the following results. The results follow exactly from the proofs of Ribet and Takahashi found in [41] and [51].

Lemma 3.1.5. *The order of the cokernel of $\pi_* : \Phi_p(J) \to \Phi_p(E)$ is equal to the index of $\pi^* \mathcal{X}_p(E)$ in $\mathcal{L}_p(f)$,*

$$j_p = [\mathcal{L}_p(f) : \pi^* \mathcal{X}_p(E)].$$

Recalling that $\mathcal{X}_p(E)$ is one-dimensional and using the result above, we pick a generator x_p so that $\pi^*(x_p) = j_p g_p$. Using the short exact sequence

$$0 \to \mathcal{X}_p(E) \to \mathrm{Hom}(\mathcal{X}_p(E), \mathbb{Z}) \to \Phi_p(E) \to 0$$

and the monodromy paring $u_{E,p}$, $\bar{c}_p = u_{E,p}(x_p, x_p)$.

Further, since $\pi_* \circ \pi^*$ is multiplication by an integer δ on $\mathcal{X}_p(E)$,

$$\delta u_{E,p}(x, x) = u_{E,p}(x, \pi_*(\pi^*(x))) = u_{J,p}(\pi^*(x), \pi^*(x))$$

for all $x \in \mathcal{X}_p(E)$. Taking $x = x_p$, $\delta \bar{c}_p = j_p^2 h_p$, or $\delta = \frac{h_p}{\bar{c}_p} j_p^2$. Since $j_p = \bar{c}_p / i_p$, we have $\delta = \frac{h_p}{i_p} j_p$.

For elliptic curves, $\bar{c}_p = \mathrm{ord}_p(\Delta)$, where Δ is the minimal discriminant of E. The problem is that we don't know before starting which curve E in the isogeny class is the optimal quotient. Asymptotically, the optimal quotients of the different parameterizations will be the same since asymptotically 100% of curves have trivial isogeny class. However, the optimal quotient E' of $X_0^D(M)$ need not be the same optimal quotient E of $X_0(N)$. For example, if $N = 38$, E the curve with LMFDB label 38.b2 [31], is an optimal quotient of $X_0(38)$. Setting $D = 38$ and $M = 1$ gives $\bar{c}_2 = 1$ and $\bar{c}_{19} = 5$ and E' is 38.b1, i.e., the curve 38.b1 is the optimal quotient of the Shimura curve $X_0^{38}(1)$.

Due to Voight and Willis [55] we can non-provably approximate the j-invariant of the curve that is the optimal quotient of the parameterization. They accomplish this by computing with a Taylor series expansion of the quaternionic modular form. From this we can compute all $\bar{c}_p$. This will be discussed in greater detail in Section 3.3.

Next, we must compute the other invariants found in Equation 3.1.4, namely h_p, i_p, and j_p. Using work of Kirschmer and Voight [26] we can compute $\mathcal{X}_p(J)$, complete with Hecke action and monodromy pairing. Thus we can compute h_p by computing kernels of the Hecke action $T_n - a_n(f)$ for $n \nmid N$ until we have a subspace of dimension one. This subspace is generated by g_p. By computing the monodromy pairing on g_p, we have h_p. The next theorem allows us to compute i_p.

Lemma 3.1.6. *The order of the image of $\Phi_p(J) \to \Phi_p(E)$, i_p, generates the ideal $I_p = \{u_J(g_p, y) | y \in \mathcal{X}_p(J)\}$.*

We can now compute i_p by computing $u_{J,p}(h_p, y)$ for all y in a basis of $\mathcal{X}_p(J)$. The work of Voight and Willis was not available when Takahashi was first studying Shimura degrees. The following conjecture of Takahashi offers a way to compute δ_M^D in the cases where $D > 1$. If $D = 1$, δ_M^1 is the modular degree. We have other means of computing the modular degree.

Conjecture 3.1.7. *For $p|D$ we have $j_p = 1$, i.e., the map $\Phi_p(J) \to \Phi_p(E)$ is surjective.*

This was originally stated as a direct corollary of Proposition 4.4 of Bertollini and Darmon [3]. Bertollini and Darmon studied and compared the short exact sequences created by the p-adic uniformization of the Jacobian of the Shimura curve and the elliptic curve. We give an outline of their construction so we can discuss the gap and the motivation for the conjecture.

In particular, by combining the p-adic uniformization of the Shimura curve we saw above in Equation 2.7.4 and the theory of Mumford curve Jacobians [3],[35], we have a rigid analytic uniformization of the Jacobian of the Shimura curve, J, that we can compare to the Tate curve parameterization of E. Let Λ_J be the lattice of p-adic periods of J, Λ_E be the lattice associated with the Tate curve of E, and let $\mathbb{C}_p$ be the completion of the algebraic closure of

$\mathbb{Q}_p$. Then we have the following short exact sequences with injective vertical arrows.

$$\begin{tikzcd}
0 \arrow[r] & \Lambda_E \arrow[r] \arrow[d] & \mathbb{C}_p^\times \arrow[r] \arrow[d] & E(\mathbb{C}_p) \arrow[r] \arrow[d, "\pi_*"] & 0 \\
0 \arrow[r] & \Lambda_J \arrow[r] & \mathrm{Hom}(\Lambda_J, \mathbb{C}_p^\times) \arrow[r] & J(\mathbb{C}_p) \arrow[r] & 0
\end{tikzcd}$$

Let Λ_f be the submodule of Λ_J defined as

$$\Lambda_f = \{x \in \Lambda_J : T_n x = a_n(f)x \text{ for all } n \text{ coprime to } N\}.$$

Note that $\Lambda_J \cong \mathcal{X}_p(J)$, $\Lambda_E \cong \mathcal{X}_p(E)$ and $\Lambda_f \cong \mathcal{L}_p(f)$ with the associated monodromy pairings equal to the composition of an inner product with ord_p. With this notation, the following is Proposition 4.4 of Bertollini and Darmon [3] .

Conjecture 3.1.8. *The kernel $\Lambda_E = q^{\mathbb{Z}}$ of $\mathbb{C}_p^\times \to E(\mathbb{C}_p)$ is canonically equal to the module Λ_f, and the above Diagram 3.1 is Hecke-equivariant and commutes up to sign.*

In particular, even though $\Lambda_E \hookrightarrow \Lambda_f$, there could be a nontrivial cokernel. More explicitly, both Λ_E and Λ_f are dimension 1 free $\mathbb{Z}$ modules. The generator $x \in \Lambda_E$ only maps to a constant times the generator $g \in \Lambda_f$, $x \mapsto cg$ for some integer $c \in \mathbb{Z}$. More can be said about this constant c, in particular due to work of Papikian and Rabinoff [36], c divides the order of the roots of unity in $\mathbb{Q}_p$. For more background and discussion see Papikian and Rabinoff [36]. Note that everything involved in this generalizes to the totally real number field case, complete with the same gap and conclusions.

Assuming Takahashi's Conjecture 3.1, if we can compute h_p and i_p for $p \mid DM$ we can compute modular degree. First compute $\delta^D(M)$ for primes $p \mid D$, via $\delta^D(M) = \frac{h_p}{i_p}$. Then for primes $p \mid M$, use $j_p = \delta^D(M)\frac{i_p}{h_p}$ and use this to compute $\bar{c}_p$. This gives you the modular degree and all $\bar{c}_p$, so using the Cremona tables or LMFDB we can also potentially find the optimal quotient. In Section 5.1 we show that for semistable elliptic curves over $\mathbb{Q}$, if we compute the $\bar{c}_p$ for all $p \mid DM$, it is enough information to find the optimal quotient.

3.2 Shimura Degree for Abelian Varieties Over Totally Real Number Fields

In [53], Ullmo generalizes Takahashi's main result in [51] to modular abelian varieties over $\mathbb{Q}$. Let $N = dpqm$ be square-free, where p, q are primes and d has an even number of prime factors. Let $J = J_0^d(pqm)$ and $J' = J_0^{dpq}(m)$. Let A, A' be optimal quotients of J and J' respectively. Let $\delta, j_p, j_q, \bar{c}_p, \bar{c}_q$ and let $\delta', j'_p, j'_q, \bar{c}'_p, \bar{c}'_q$ be the respective invariants. Takahashi's main result in [51] is as follows:

Theorem 3.2.1. *We have*

$$\frac{\delta}{\delta'} = \frac{\bar{c}_q \bar{c}'_p}{i_p^2 j_q'^2}.$$

Note that this equation is symmetric with respect to p and q, i.e., switching them yields the same result.

Following the work of Ullmo [53] and the exposition of Papikian [35], we can work through much of what Takahashi managed but for modular abelian varieties over totally real number fields.

For the following section, let F be a totally real number field, let $\mathfrak{N}$ be a square-free ideal of F and $J = J_0^{\mathfrak{D}}(\mathfrak{M})$ where $\mathfrak{D}\mathfrak{M} = \mathfrak{N}$. Left $f \in \mathcal{S}_{\bar{2}}(\mathfrak{N})$ be a Hilbert modular cuspform. Let A be a modular abelian variety associated to f. Assume A is an optimal quotient of J, that is to say, the map $\pi : J \to A$ is a surjective morphism with a connected kernel. As before, the dual map $\pi^\vee : A^\vee \to J$ is injective. Let $\theta_f = \pi \circ \pi^\vee$ and we define the Shimura degree to be:

Definition 3.2.2. The *Shimura degree* of A is $\delta^{\mathfrak{D}}(\mathfrak{M}) = \sqrt{\deg(\ker(\theta_f))}$

Let $\mathfrak{p}$ be a prime dividing $\mathfrak{N}$. As before, we have the following diagram:

$$\begin{tikzcd}
0 \arrow[r] & \mathcal{X}_{\mathfrak{p}}(J) \arrow[r] \arrow[d, "\pi_*"] & \mathrm{Hom}(\mathcal{X}_{\mathfrak{p}}(J), \mathbb{Z}) \arrow[r] \arrow[d] & \Phi_{\mathfrak{p}}(J) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \mathcal{X}_{\mathfrak{p}}(A^\vee) \arrow[r] & \mathrm{Hom}(\mathcal{X}_{\mathfrak{p}}(A), \mathbb{Z}) \arrow[r] & \Phi_{\mathfrak{p}}(A) \arrow[r] & 0
\end{tikzcd}$$

and the following invariants for $\mathfrak{p}|\mathfrak{N}$:

Definition 3.2.3. Let $\pi_* : \Phi_{\mathfrak{p}}(J) \to \Phi_{\mathfrak{p}}(A^\vee)$

$$\bar{c}_{\mathfrak{p}} = \#\Phi_{\mathfrak{p}}(A) \quad i_{\mathfrak{p}} = \#\text{image}(\pi_*) \quad j_{\mathfrak{p}} = \#\text{coker}(\pi_*)$$

As before $j_{\mathfrak{p}} = \frac{\bar{c}_{\mathfrak{p}}}{i_{\mathfrak{p}}}$.

This is where we part ways from the original definitions. Pick a Hilbert modular newform $f \in \mathcal{S}_{\bar{2}}(\mathfrak{N})$. Let $\mathbb{Z}_f = \mathbb{Z}[a_{\mathfrak{n}}(f) : \mathfrak{n} \nmid N]$, where $a_{\mathfrak{n}}(f)$ are the coefficients of f. Then $\mathbb{Z}_f$ is again the ring of integers for some number field. If A is an abelian variety associated to f, $\dim(A) = [\mathbb{Z}_f : \mathbb{Z}]$. If A is not an elliptic curve, $[\mathbb{Z}_f : \mathbb{Z}] > 1$ and A is also associated to all conjugates of f, f^σ for $\sigma \in \text{Aut}(\mathbb{Z}_f)$. Thus $\pi^*(\mathcal{X}_{\mathfrak{p}}(A))$ has dimension greater than 1. Further, if A is purely toric, it has dimension equal to the dimension of A. We now have

$$\pi^*\mathcal{X}_{\mathfrak{p}}(A^\vee) \subset \oplus_\sigma \mathcal{L}_{\mathfrak{p}}(f^\sigma),$$

where the direct sum is over all the conjugates of f.

Another way to view $\mathcal{L}_{\mathfrak{p}}(A) = \oplus\mathcal{L}_{\mathfrak{p}}(f^\sigma)$ is as the saturation of $\pi^*\mathcal{X}_{\mathfrak{p}}(A^\vee)$ inside $\mathcal{X}_{\mathfrak{p}}(J)$. By saturation, we mean tensoring with $\mathbb{Q}$ and taking the intersection with the larger module. Saturating allows us to define $\mathcal{L}_{\mathfrak{p}}(A)$ in another way.

Definition 3.2.4. The saturation of $\pi^*(\mathcal{X}_{\mathfrak{p}}(A^\vee))$ in $\mathcal{X}_{\mathfrak{p}}(J)$ is

$$\mathcal{L}_{\mathfrak{p}}(A) = \left(\pi^*\mathcal{X}_{\mathfrak{p}}(A^\vee) \otimes \mathbb{Q}\right) \cap \mathcal{X}_{\mathfrak{p}}(J).$$

Thus $\mathcal{X}_{\mathfrak{p}}(J)/\mathcal{L}_{\mathfrak{p}}(A)$ is torsion-free. Notice that $\mathcal{L}_{\mathfrak{p}}(A)$ is the generalization of the f-isotypical component $\mathcal{L}_{\mathfrak{p}}(f)$. Further $\pi^*\mathcal{X}_{\mathfrak{p}}(A^\vee) \subset \mathcal{L}_{\mathfrak{p}}(A)$.

To create a generalization of $h_{\mathfrak{p}}$ that works in this setting where $\mathcal{L}_{\mathfrak{p}}(A)$ has dimension greater than one and to generalize Lemma 1, we consider the exterior algebras $\wedge^a\mathcal{X}_{\mathfrak{p}}(A)$ where $a = \text{rank}_{\mathbb{Z}}(\mathcal{X}_{\mathfrak{p}}(A))$. Then $\wedge^a\mathcal{X}_{\mathfrak{p}}(A)$ and $\wedge^a\mathcal{X}_{\mathfrak{p}}(A^\vee)$ are rank one $\mathbb{Z}$-modules. Let $y_{\mathfrak{p}}$ and $z_{\mathfrak{p}}$ be generators of $\wedge^a\mathcal{X}_{\mathfrak{p}}(A)$ and $\wedge^a\mathcal{X}_{\mathfrak{p}}(A^\vee)$ respectively. Consider the pairing induced on $\wedge^a\mathcal{X}_{\mathfrak{p}}(A) \times \wedge^a\mathcal{X}_{\mathfrak{p}}(A^\vee)$ by the monodromy paring $u_{A,\mathfrak{p}}$, denoted by the same symbol, then by Papikian [35]

$$\bar{c}_{\mathfrak{p}} = |u_{A,\mathfrak{p}}(y_{\mathfrak{p}}, z_{\mathfrak{p}})|.$$

Now let $x_{\mathfrak{p}}$ be a generator of $\wedge^a \mathcal{L}_{\mathfrak{p}}(A)$, analogous to the generator of $\mathcal{L}_{\mathfrak{p}}(f)$. Then we can define

$$h_{\mathfrak{p}} = u_{J,\mathfrak{p}}(x_{\mathfrak{p}}, x_{\mathfrak{p}}).$$

As an analogue of Lemma 1, we have Proposition 2.12 of [35]

Theorem 3.2.5.

$$j_{\mathfrak{p}} = [\mathcal{L}_{\mathfrak{p}}(A) : \pi^* \mathcal{X}_{\mathfrak{p}}(A)]$$

Proof. From the surjectivity of $\mathcal{X}_{\mathfrak{p}}(J) \to \mathcal{X}_{\mathfrak{p}}(A)$, when we apply the snake lemma to the two short exact sequences above, we see that $\operatorname{coker}(\operatorname{Hom}(\mathcal{X}_{\mathfrak{p}}(J), \mathbb{Z}) \to \operatorname{Hom}(\mathcal{X}_{\mathfrak{p}}(A), \mathbb{Z})) \cong \operatorname{coker}(\phi_{\mathfrak{p}}(J) \to \phi_{\mathfrak{p}}(A))$. The order of the torsion subgroup of $\operatorname{coker}(\pi^* : \mathcal{X}_{\mathfrak{p}}(A) \to \mathcal{X}_{\mathfrak{p}}(J))$ is the order of $\operatorname{coker}(\operatorname{Hom}(\mathcal{X}_{\mathfrak{p}}(J), \mathbb{Z}) \to \operatorname{Hom}(\mathcal{X}_{\mathfrak{p}}(A), \mathbb{Z})$. By definition of $\mathcal{L}_{\mathfrak{p}}(f)$, $\mathcal{X}_{\mathfrak{p}}(J)/\mathcal{L}_{\mathfrak{p}}(f)$ is torsion-free. Winding back through, $[\mathcal{L}_{\mathfrak{p}}(f) : \pi^* \mathcal{X}_{\mathfrak{p}}(A)] = \#\operatorname{coker}(\phi_{\mathfrak{p}}(J) \to \phi_{\mathfrak{p}}(A))$. $\square$

Finally, applying Proposition 2.10 of [35]

Theorem 3.2.6.

$$\delta^{\mathfrak{D}}(\mathfrak{M}) \bar{c}_{\mathfrak{p}} = j_{\mathfrak{p}}^2 h_{\mathfrak{p}}.$$

Which after rearranging is the generalized version of the Shimura degree Equation 3.1.4.

Let $\mathfrak{N} = \mathfrak{D}\mathfrak{p}\mathfrak{q}\mathfrak{M}$ be a product of primes such that the number of primes dividing $\mathfrak{D}$ is congruent to $d-1$ mod 2, i.e., so that we can form indefinite quaternion algebras ramified at $\tau_2, \cdots, \tau_d$ and split at τ_1 of discriminant $\mathfrak{D}$ and discriminant $\mathfrak{D}\mathfrak{p}\mathfrak{q}$. Let $J = J_0^{\mathfrak{D}}(\mathfrak{p}\mathfrak{q}\mathfrak{M})$ and $J' = J_0^{\mathfrak{D}\mathfrak{p}\mathfrak{q}}(\mathfrak{M})$. Additionally, define $J'' = J_0^{\mathfrak{D}}(\mathfrak{q}\mathfrak{M})$. Let A, A' be optimal quotients of J and J' respectively. By Faltings, A and A' are isogenous. Let $\delta, j_{\mathfrak{p}}, j_{\mathfrak{q}}, \bar{c}_{\mathfrak{p}}, \bar{c}_{\mathfrak{q}}$ and let $\delta', j'_{\mathfrak{p}}, j'_{\mathfrak{q}}, \bar{c}'_{\mathfrak{p}}, \bar{c}'_{\mathfrak{q}}$ be the respective invariants.

As in [51], Ullmo applies the canonical exact sequence

$$0 \to \mathcal{X}_{\mathfrak{p}}(J') \xrightarrow{\iota} \mathcal{X}_{\mathfrak{q}}(J) \to \mathcal{X}_{\mathfrak{q}}(J'') \times \mathcal{X}_{\mathfrak{q}}(J'') \to 0$$

The following is Theorem 1.1 of [53] generalized to modular abelian varieties over totally real number fields.

Theorem 3.2.7. *The Shimura degrees δ and δ' are related by*

$$\delta' = \frac{\delta}{\bar{c}'_{\mathfrak{p}}\bar{c}_{\mathfrak{q}}} i_{\mathfrak{q}}^2 j_{\mathfrak{p}}'^2.$$

Proof. As the map $\iota : \mathcal{X}_{\mathfrak{p}}(J') \hookrightarrow \mathcal{X}_{\mathfrak{q}}(J)$ is compatible with the action of Hecke operators $T_{\mathfrak{n}}$ for all $\mathfrak{n}$ coprime to $\mathfrak{N}$, by definition of $\mathcal{L}_{\mathfrak{p}}(A') \subset \mathcal{X}_{\mathfrak{p}}(J')$ and $\mathcal{L}_{\mathfrak{q}}(A) \subset \mathcal{X}_{\mathfrak{q}}(J)$, we have $\iota\left(\mathcal{L}_{\mathfrak{p}}(A')\right) \subset \mathcal{L}_{\mathfrak{q}}(A)$. Further, as $\mathcal{L}_{\mathfrak{p}}(A')$ is saturated and ι is injective we must have $\iota\left(\mathcal{L}_{\mathfrak{p}}(A')\right) = \mathcal{L}_{\mathfrak{q}}(A)$ and thus $h_{\mathfrak{q}} = h'_{\mathfrak{p}}$. Writing down the formula for the modular degree in both cases and using this relation yields the result. □

3.3 Finding Optimal Quotient

There are two drastically different ways to find optimal quotients of Shimura curves, neither of which are provably correct. A recent result of Voight and Willis [55] allows us to approximate Taylor series expansions of the quaternionic modular form. This in turn allows us to approximate the periods, and thus the j-invariant of the optimal quotient. In the cases where we have Cremona type tables [10] of modular elliptic curves, if we compute the j-invariant to high enough precision, we can determine which curve in the isogeny class is corresponds to. If we do not have Cremona type tables, then we can conjecturally construct the optimal quotient.

Alternatively, Takahashi has conjectured that for elliptic curves over $\mathbb{Q}$, when $p|D$, the map from the component group of the Jacobian of the Shimura curve to the component group of the elliptic curve, should be surjective:

$$\Phi_p(J) \twoheadrightarrow \Phi_p(E).$$

We can write the Shimura degree for p in terms of only two invariants: $\delta = \frac{h_p}{i_p}$. Then we work backwards to compute all the $\bar{c}_q$ for all $q \mid N$. We show that having $\bar{c}_q$ for all $q \mid N$ is enough to find all elliptic curve optimal quotients over $\mathbb{Q}$.

3.3.1 Finding Optimal Quotients Numerically

Via work of Voight and Willis [55], we conjecturally compute the j-invariant of the optimal quotient of the Shimura curve by computing the Taylor series expansion of the associated quaternionic modular form. As we can then compute the order of the component groups at each prime dividing the level, we can compute the Shimura degree.

Classical modular forms admit a Fourier expansion, also called a q-expansion. Let f be a weight k classical modular form. Then at the cusp ∞, where $q = e^{2\pi i z}$ we can write

$$f(z) = \sum_{n=0}^{\infty} a_n q^n.$$

Zagier computed the complex periods of the optimal quotient directly using the Fourier series expansion of the modular form [58]. From here, he was able to compute the j-invariant of the optimal quotient of the modular parameterization.

Unfortunately, as we generalize the idea of modular forms on modular groups to modular forms on quaternion algebras, we no longer have cusps, thus we no longer have q-expansions. A q-expansion is just a power series expansion at ∞, so instead we can take a power series expansion in the neighborhood of some point $p \in \mathcal{H}$. In actuality, we work on the unit disc $\mathcal{D}$ instead of $\mathcal{H}$ via the map

$$w : \mathcal{H} \to \mathcal{D}$$

$$z \mapsto w(z) = \frac{z - p}{z - \bar{p}}$$

which sends p to 0. Let f be a weight k quaternionic modular form of level Γ, where Γ is a Fuchsian group with compact fundamental domain $D \subset \mathcal{D}$. Then we can write f in a power series expansion form

$$f(z) = (1 - w)^k \sum_{n=0}^{\infty} b_n w^n,$$

which converges in $\mathcal{D}$ with $|w| < 1$. Using work of Voight and Willis we can compute enough b_n; so we can approximate f to high enough precision to allow us to work with f computationally. In particular, they compute the following approximation

$$f \approx f_N = (1 - w)^k \sum_{n=0}^{N} b_n w^n.$$

In our case f is a weight 2 quaternionic modular form of level Γ where Γ is the norm 1units of an appropriate Eichler order so that $X = \Gamma \setminus \mathcal{H}$ is a Shimura curve. We will use f to compute the period matrix of the elliptic curve parameterized by X. In computing $D(p)$, we compute the side pairings of Γ. Using the side pairings and the vertices they map to each other, $v_1 \mapsto v_2 \mapsto v_3$, we compute approximations to the periods

$$\omega_1 = \int_{v_2}^{v_3} f(z)\frac{dw}{(1-w)^2} \approx \sum_{n=0}^{N} \frac{b_n}{n+1} w^{n+1} \mid_{v_2}^{v_3}$$

and

$$\omega_2 = \int_{v_1}^{v_2} f(z)\frac{dw}{(1-w)^2} \approx \sum_{n=0}^{N} \frac{b_n}{n+1} w^{n+1} \mid_{v_1}^{v_2} .$$

From the periods, we compute the j-invariant $j(\omega_1/\omega_2)$ as an algebraic number in F. With the algebraic j-invariant, we can recognize the elliptic curve that is the optimal quotient of $\mathrm{Jac}(X)$ in various ways. We can use the Eisenstein series to recognize the curve, we could twist by a curve with the given j invariant, or, as we in general already have the isogeny class of curves we are interested in, we can just check which curve has the given j-invariant and thus is optimal.

3.3.2 Discriminant Twins

As we have seen [41], Ribet and Takahashi give a formula for computing the degree of parameterization of an elliptic curve $E/\mathbb{Q}$ by a Shimura curve. Further, I generalize this to the totally real number field case. If we assume the map from $\Phi_p(J) \to \Phi_p(E)$ is surjective for primes p dividing the discriminant of the quaternion algebra, we can compute the order of the component groups of the elliptic curve that is the optimal quotient of the Jacobian of the Shimura curve. However, at the start we do not know which curve in the isogeny class is the optimal quotient. As the order of the component groups is the valuation of the discriminant, we know both the discriminant and the conductor of the optimal quotient, but not the optimal quotient itself. This raises the question, when are the conductor and discriminant enough to determine an elliptic curve?

Takahashi [51] gives a table of degrees of parameterization of elliptic curves by Shimura curves for isogeny classes of elliptic curves and their optimal quotients with conductor $N = p \cdot q$, where p and q are distinct primes, and is N up to 94. In this table he is always able to find a unique curve with conductor N and corresponding discriminant. This leads one to ask if this process always works. The answer is yes. This process in fact works if N is squarefree and non-prime. If N is prime, this fails exactly four times. Looking at the first few semistable elliptic curve isogeny classes yields the following examples of isogenous curves with the same discriminant and conductor. Using LMFDB labels [31], the first examples are:

Δ-twins	N	Δ
$11a.1, 11a.3$	11	-11
$17a.1, 17a.4$	17	17
$19a.1, 19a.3$	19	-19
$37a.1, 37b.1, 37b.3$	37	37

However, if we look further, we do not find any more failures. In fact, these are all semistable, isogenous, discriminant twins.

Theorem 3.3.1 (D.-Lundell)**.** *Over $\mathbb{Q}$, there are only finitely many semistable, isogenous discriminant twins. Using LMFDB [31] labels, they are* $11a.1, 11a.3$*,* $17a.1, 17a.4$*,* $19a.1, 19a.3$*, and* $37b.1, 37b.3$*.*

Over $\mathbb{Q}$, as we are only interested in the curves that can be parameterized by Shimura curves, the conductor cannot be a prime. Thus for all semistable elliptic curves, we can find the optimal quotient of the Shimura curve parameterization by computing the order of the component group at each prime, $\bar{c}_p$, and looking up which curve in the isogeny class this corresponds to.

Chapter 4

COMPUTING SHIMURA DEGREES

To compute Shimura degrees, we compute Hecke modules to allow for our character group computations. Further, in general we must also compute the order of the component groups and this involves computing Taylor series expansions of quaternionic modular forms. The previous section highlighted work by Takahashi on how to compute $\delta^{\mathfrak{D}}(\mathfrak{M})$ once the invariants $h_{\mathfrak{p}}$ and $i_{\mathfrak{p}}$ are known for one prime $\mathfrak{p}|\mathfrak{D}\mathfrak{M}$. To compute $h_{\mathfrak{p}}$ and $i_{\mathfrak{p}}$ we use isomorphisms between character groups and Hecke modules on quaternion ideals, which is what this section will focus on. In particular, this section focuses on using Hecke modules and maps between Hecke modules to compute character groups $\mathcal{X}_p(J_0^D(M))$ and using Hecke operators $T_{\mathfrak{p}}$ on these Hecke modules to compute the subspaces $\mathcal{L}_{\mathfrak{p}}(E)$ corresponding to the elliptic curve.

To illustrate the algorithm, we will also be working through the example $N = 42$. Further, we can provably compute the Shimura degrees and optimal quotients without previously computing the order of the component groups or assuming the map from $\Phi_p(J) \to \Phi_p(E)$ is surjective for $p \mid D$, where D is the discriminant of the quaternion algebra.

4.1 Brandt and Hecke Modules $X(\mathfrak{D}, \mathfrak{M})$

For more motivation and exposition see Kohel [27]. Let H be a definite quaternion algebra over F with discriminant $\mathfrak{D}$. Let $\mathcal{O} = \mathcal{O}_H(\mathfrak{M})$ be an Eichler order in H of level $\mathfrak{M}$. Take $\mathrm{Cl}(\mathcal{O})$ to be the set of right ideal classes of $\mathcal{O}$.

Definition 4.1.1. The *Brandt module* is the formal divisor group

$$\mathrm{Br}(\mathfrak{D}, \mathfrak{M}) = \mathbb{Z}[\mathrm{Cl}(\mathcal{O})].$$

The *Hecke module*

$$X(\mathfrak{D}, \mathfrak{M}) = \mathbb{Z}[\mathrm{Cl}(\mathcal{O})]^0$$

is the set of formal degree zero elements of $\mathrm{Br}(\mathfrak{D}, \mathfrak{M})$.

The Hecke module $X(\mathfrak{D}, \mathfrak{M})$ comes equipped with an action of Hecke operators $T_{\mathfrak{n}}$ and an inner product $\langle , \rangle$ satisfying $\langle [I], T_{\mathfrak{n}}([J]) \rangle = \langle T_{\mathfrak{n}}([I]), [J] \rangle$. Lastly, since $X(\mathfrak{D}, \mathfrak{M}) \subset \mathrm{Br}(\mathfrak{D}, \mathfrak{M})$ is the orthogonal complement to the Eisenstein subspace, a subspace of dimension 1, $\dim(X(\mathfrak{D}, \mathfrak{M})) + 1 = \dim(\mathrm{Br}(\mathfrak{D}, \mathfrak{M}))$.

We can compute both the Hecke operators and the inner product. The inner product is given by the following formula:

$$\langle [I], [J] \rangle = \omega_{[I]} \delta_{[I],[J]}/2$$

where $\delta_{[I],[J]} = 1$ if $[I] = [J]$ and 0 otherwise, and $\omega_{[I]} = \#\mathcal{O}_L(I)^\times / \mathbb{Z}_F^\times$ where $\mathcal{O}_L(I) = \{x \in B : xI \subset I\}$ is the left order of I.

We compute the Hecke operators similarly. Let n be the order of $\mathrm{Cl}(\mathcal{O})$ and let $[I_1], \cdots, [I_n]$ be some indexing of $\mathrm{Cl}(\mathcal{O})$. Take $\mathfrak{p}$ to be a prime not dividing $\mathfrak{N} = \mathfrak{D}\mathfrak{M}$. Then the Hecke operator $T_{\mathfrak{p}}$ is an $n \times n$ integer matrix with (i, j)th entry

$$T_{\mathfrak{p},(i,j)} = \# \left\{ x \in I_i I_j^{-1} : \mathrm{nrm}(x I_i I_j^{-1}) = \mathfrak{p} \right\}.$$

Following work of Kirschmer and Voight [26], $\mathrm{Cl}(\mathcal{O})$ is compatible in Magma [4] and from this both the inner product and Hecke operators are implementable. Over $\mathbb{Q}$ this is already fully implemented, using the

```
BrandtModule
```

construction. For number fields, we can define right ideal classes of quaternion algebras and directly compute the monodromy pairing and Hecke operators.

4.2 Computing $\mathcal{X}_{\mathfrak{p}}(J)$

Here we rely on the identifications of character groups of Shimura curves with right ideal classes of quaternion algebras, which is summarized in the following two theorems:

Theorem 4.2.1. *Let H be a definite quaternion algebra of discriminant $\mathfrak{D}\mathfrak{p}$, and let $X(\mathfrak{D}\mathfrak{p}, \mathfrak{M})$ be the Hecke module for an Eichler order $\mathcal{O}_H(\mathfrak{M}) \subset H$ of level $\mathfrak{M}$. Let B be an indefinite quaternion algebra of discriminant $\mathfrak{D}$. Then there exists a canonical isomorphism*

$$X(\mathfrak{D}\mathfrak{p}, \mathfrak{M}) \cong \mathcal{X}_{\mathfrak{p}}(J_0^{\mathfrak{D}}(\mathfrak{M}\mathfrak{p})).$$

This isomorphism is compatible with Hecke operators $T_{\mathfrak{n}}$, $(\mathfrak{D}\mathfrak{p}\mathfrak{M}, \mathfrak{n}) = 1$, and is an isometry with respect to the respective inner products.

Proof. This follows directly from Corollary 2.7.1 and the definition of Hecke modules. □

If $\mathfrak{p} \mid \mathfrak{M}$, then we have an isomorphism that allows us to compute $\mathcal{X}_{\mathfrak{p}}(J_0^{\mathfrak{D}}(\mathfrak{M}))$. The case were $\mathfrak{p}|\mathfrak{D}$ is a bit more complicated. In this case we compute $\mathcal{X}_{\mathfrak{p}}(J_0^{\mathfrak{D}}(\mathfrak{M}))$ as the kernel of other Hecke modules using Corollary 2.7.2 that gives us the following corollary.

Corollary 4.2.2. *Let B be an indefinite quaternion algebra over F, split at τ_1, ramified at $\tau_2, \cdots, \tau_d$, of discriminant $\mathfrak{D}\mathfrak{p}$ where $\mathfrak{p}$ is a prime coprime to D. Then there exists a canonical exact sequence*

$$0 \to \mathcal{X}_{\mathfrak{p}}(J^{\mathfrak{D}\mathfrak{p}}(\mathfrak{M})) \to X(\mathfrak{D}, \mathfrak{M}\mathfrak{p}) \to X(\mathfrak{D}, \mathfrak{M}) \times X(\mathfrak{D}, \mathfrak{M}) \to 0$$

where the homomorphisms are compatible with the Hecke operators $T_{\mathfrak{n}}$ for all $\mathfrak{n}$ relatively prime to $\mathfrak{D}\mathfrak{M}\mathfrak{p}$. With respect to the monodromy pairings on $\mathcal{X}_{\mathfrak{p}}(J^{\mathfrak{D}\mathfrak{p}}(\mathfrak{M}))$ and $X(\mathfrak{D}, \mathfrak{M}\mathfrak{p})$, the map $\mathcal{X}_{\mathfrak{p}}(J^{\mathfrak{D}\mathfrak{p}}(\mathfrak{M})) \to X(\mathfrak{D}, \mathfrak{M}\mathfrak{p})$ is an isometry with its image.

In particular, we can write $\mathcal{X}_p(J^B(M)) \cong \ker\left(X(D'q, Mp) \to X(D'q, M) \times X(D'q, M)\right)$.

From the previous section, computing $h_{\mathfrak{p}}$ and $i_{\mathfrak{p}}$ where $\mathfrak{p} \mid \mathfrak{D}\mathfrak{M}$ reduces to computing $\mathcal{X}_{\mathfrak{p}}(J^{\mathfrak{D}}(\mathfrak{M}))$ in terms of a Hecke module or Hecke module subspace, along with the action of $T_{\mathfrak{n}}$ and an inner product.

We already noticed that to compute $\mathcal{X}_{\mathfrak{p}}(J^{\mathfrak{D}}(\mathfrak{M}))$, we have two cases. First $\mathfrak{p} \mid \mathfrak{M}$ and the second where $\mathfrak{p} \mid \mathfrak{D}$.

If $\mathfrak{p} \mid \mathfrak{M}$, again, we use Theorem 4.2 with $\mathfrak{M} = \mathfrak{m}\mathfrak{p}$. So we have the canonical isomorphism

$$X(\mathfrak{D}\mathfrak{p}, \mathfrak{m}) \cong \mathcal{X}_{\mathfrak{p}}(J_0^{\mathfrak{D}}(\mathfrak{m}\mathfrak{p})).$$

For Magma **??** code to compute the Hecke module see **??** and **??** or the Git repository `https://github.com/adeines/ShimuraDegrees`.

For an interesting example, pick N divisible by three primes. The smallest such example is $N = 30 = 2 \cdot 3 \cdot 5$ and all Hecke modules in this case have been computed by Kohel in [27]. The second smallest example is $N = 42 = 2 \cdot 3 \cdot 7$. There are four different Shimura curve parameterizations, $X_0^{21}(2), X_0^{14}(3), X_0^6(7)$, and the modular curve $X_0(42)$. For p dividing the level we have

$$\mathcal{X}_2(J_0^{21}(2)) \cong \mathcal{X}(J_0^{14}(3)) \cong \mathcal{X}_7(J_0^6(7)) \cong X(42,1).$$

Computing $X(42,1)$, we see that is a one dimensional Hecke module. Thus $\mathcal{L}_{\mathfrak{p}}(f) = X(42,1)$ and in all cases $h_p = i_p$.

If $p|D$, we must use Corollary 4.2. With $D = p_1p_2$ and $M = p_3$, then there are six possibilities:

$$\begin{array}{lcccccccc}
(1) & 0 & \to \mathcal{X}_7(J_0^{21}(2)) & \to & X(3,14) & \to & X(3,2)\times X(3,2) & \to & 0 \\
(2) & 0 & \to \mathcal{X}_3(J_0^{21}(2)) & \to & X(7,6) & \to & X(7,2)\times X(7,2) & \to & 0 \\
(3) & 0 & \to \mathcal{X}_7(J_0^{14}(3)) & \to & X(2,21) & \to & X(2,3)\times X(2,3) & \to & 0 \\
(4) & 0 & \to \mathcal{X}_2(J_0^{14}(3)) & \to & X(7,6) & \to & X(7,3)\times X(7,3) & \to & 0 \\
(5) & 0 & \to \mathcal{X}_2(J_0^{6}(7)) & \to & X(3,14) & \to & X(3,7)\times X(3,7) & \to & 0 \\
(6) & 0 & \to \mathcal{X}_3(J_0^{6}(7)) & \to & X(2,21) & \to & X(2,7)\times X(2,7) & \to & 0
\end{array}$$

Computing the dimensions of the Hecke modules, we can compute the dimensions of the character groups. The dimension of the character group $\mathcal{X}_p(Dp, M)$ will be the dimension of $X(D, Mp)$ minus two times the dimension of $X(D, M)$.

$\mathcal{X}_p^{Dp}(M)$	rank	$X(D,Mp)$	rank	$X(D,M)$	rank
$\mathcal{X}_7(J_0^{21}(2))$	3	$X(3,14)$	3	$X(3,2)$	0
$\mathcal{X}_3(J_0^{21}(2))$	3	$X(7,6)$	5	$X(7,2)$	1
$\mathcal{X}_7(J_0^{14}(3))$	3	$X(2,21)$	3	$X(2,3)$	0
$\mathcal{X}_2(J_0^{14}(3))$	3	$X(7,6)$	5	$X(7,3)$	1
$\mathcal{X}_2(J_0^{6}(7))$	1	$X(3,14)$	3	$X(3,7)$	1
$\mathcal{X}_3(J_0^{6}(7))$	1	$X(2,21)$	3	$X(2,7)$	1

Since $X(2,3)$ and $X(3,2)$ have dimension 0, $\mathcal{X}_7(J_0^{21}(2)) \cong X(3,14)$, a dimension 3 Hecke module, and $\mathcal{X}_7(J_0^{14}(3)) \cong X(2,21)$, another dimension 3 Hecke module.

Next, we examine the sequences where the character group is not isomorphic to the Hecke module. We start with the short exact sequence (5). In this we see $X(3,7)$ has basis $\{(1,-1)\}$ and $X(3,14)$ has basis $\{(1,0,0,-1),(0,1,0,-1),(0,0,1,-1)\}$.

There are two basic methods to compute the kernel of the map

$$\gamma : X(D,Mp) \to X(D,M) \times X(D,M).$$

The first method is illustrated by Kohel [27] and only works when the kernel has dimension 1, and thus corresponds to Λ_f. As the Hecke module homomorphism must be compatible with the action of the Hecke operators T_n for $n \nmid DMp$, you compute the kernels of the Hecke operators at p $T(p)+1$ or $T(p)-1$ until you have a subspace of $X(D,Mp)$ with the correct dimension $\dim(X(D,Mp)) - 2\cdot\dim(X(D,M))$. The kernel of γ is the kernel of some $T(p)+1$ or $T(p)-1$ because $X(D,Mp)$ has bad reduction at p and $X(D,M)$ does not, thus $T(p)$ will have eigenvalues ± 1 on $X(Dq,mp)$ and not necessarily on $X(Dq,m)$.

The map

$$X(3,14) \to X(3,7) \times X(3,7)$$

must be compatible under the action of Hecke operators. Let f be the modular form associated to the isogeny class of elliptic curves of conductor 42. Then f has q-expansion

$$q + q^2 - q^3 + q^4 - 2q^5 - q^6 - q^7 + q^8 + q^9 - 2q^{10} - 4q^{11} + O(q^12)$$

and as the coefficient of q^3 is -1, we compute the kernel of $T_3 - (-1)$. The kernel of $T_3 + 1$ has dimension 1 and basis $\{(1, -1, 0)\}$ Thus the kernel of $T(3) + 1$ in $X(3, 14)$ is generated by the element $1 \cdot (1, 0, 0, -1) - 1 \cdot (0, 1, 0, -1) = (1, -1, 0, 0)$.

For the short exact sequence (6), we repeat the process and find the kernel of $T_3 + 1$ on $X(2, 21)$ gives us the subspace generated by $(1, 1, -1, -1)$.

For the dimension 3 character groups not isomorphic to the middle Hecke module, $\mathcal{X}_2(J_0^{14}(3))$ and $\mathcal{X}_3(J_0^{21}(2)$, we must compute them as kernels. We do this by explicitly writing the maps α and β defined on character graphs in Equation 2.7.2 as maps on write ideal classes of quaternion orders.

Recall our notation. Let H be a definite quaternion algebra of discriminant $\mathfrak{D}$. Let $\mathcal{O}_H(\mathfrak{M}\mathfrak{p})$ and $\mathcal{O}_H(\mathfrak{M})$ be quaternion orders of H of levels $\mathfrak{M}\mathfrak{p}$ and $\mathfrak{M}$ respectively such that $\mathcal{O}_H(\mathfrak{M}\mathfrak{p}) \subset \mathcal{O}_H(\mathfrak{M})$. Let π be a uniformizer for $F_\mathfrak{p}$ and $g \in \hat{H}^\times$ be $\begin{pmatrix} 1 & 0 \\ 0 & \pi \end{pmatrix}$ at $\mathfrak{p}$ and 1 everywhere else. Further, take $\mathcal{O}_{H,g}(\mathfrak{M})$ to be the Eichler order of level $\mathfrak{M}\mathfrak{p}$ conjugate to $\mathcal{O}_H(\mathfrak{M})$ by the adelic element g.

Recall that α is just the inclusion map from

$$\alpha :: \mathrm{Cl}(\mathcal{O}_H(\mathfrak{M}\mathfrak{p})) \to \mathrm{Cl}(\mathcal{O}_H(\mathfrak{M}))$$

where

$$\alpha : [I] \mapsto [I\mathcal{O}_H(\mathfrak{M})].$$

The map

$$\beta : \mathrm{Cl}(\mathcal{O}_H(\mathfrak{M}\mathfrak{p}) \to \mathrm{Cl}(\mathcal{O}_{H,g}(\mathfrak{M}))$$

is defined similarly

$$\beta : [I] \mapsto [g^{-1}I\mathcal{O}_{H,g}(\mathfrak{M})].$$

The Magma code for computing these kernels can be found at line 33 in A.1.1 and line 50 in A.1.3.

The Hecke module $X(7,3)$ is a rank 5 $\mathbb{Z}$-module with basis

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

Computing the kernel of the map

$$(\alpha,\beta) : X(7,6) \to X(7,3) \times X(7,3)$$

we find it is given by the basis

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

Similarly, the kernel of

$$(\alpha,\beta) : X(7,6) \to X(7,2) \times X(7,2)$$

is given by the basis

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

Now that we can compute a basis for all of our character groups, we need to compute the subspace of the character group corresponding to the optimal elliptic curve.

4.3 Computing $\mathcal{L}_{\mathfrak{p}}(f)$

As before, define the f-isotypical component to be

$$\mathcal{L}_{\mathfrak{p}}(f) = \{x \in \mathcal{X}_{\mathfrak{p}}(J) : T_{\mathfrak{n}}(x) = a_{\mathfrak{n}}(f)x \text{ for all } \mathfrak{n} \text{ coprime to } \mathfrak{N}\}.$$

Since we know the isogeny class of E, we can compute $a_{\mathfrak{n}}(f)$. By systematically computing the kernels of $T_{\mathfrak{p}} - a_{\mathfrak{p}}$ on $\mathcal{X}_{\mathfrak{p}}(f)$ for $\mathfrak{p}$ not dividing $\mathfrak{N}$, we can cut down until we have a dimension 1 subspace, which will be $\mathcal{L}_{\mathfrak{p}}(f)$. Then $g_{\mathfrak{p}}$ is the single basis element for this subspace. Further, since we're are actually working with subspace of Brandt modules, $\mathcal{L}_{\mathfrak{p}}(f)$ inherits the monodromy pairing. So we also now compute $h_{\mathfrak{p}}^{\mathfrak{D}}(\mathfrak{M}) = u_{J,\mathfrak{p}}(g_{\mathfrak{p}}, g_{\mathfrak{p}})$ and $i_{\mathfrak{p}} = \mathrm{LCM}\{u_{J,\mathfrak{p}}(g_{\mathfrak{p}}, y) : y \in \mathrm{Basis}(\mathcal{X}_{\mathfrak{p}}^{\mathfrak{D}}(\mathfrak{M}))\}$. Magma code for computing the f-isotypical subspace is on line 65 of A.1.1.

Recall that our goal is to compute

$$\delta^{\mathfrak{D}}(\mathfrak{M}) = \frac{h_{\mathfrak{p}} j_{\mathfrak{p}}}{i_{\mathfrak{p}}} = \frac{h_{\mathfrak{p}} \bar{c}_{\mathfrak{p}}}{i_{\mathfrak{p}}^2}$$

where $\mathfrak{p} \mid \mathfrak{N}$ and to also compute the elliptic curve parameterized by $X_0^{\mathfrak{D}}(\mathfrak{M})$. This is why we are interested in the invariants $h_{\mathfrak{p}}, i_{\mathfrak{p}}, j_{\mathfrak{p}}$, and $\bar{c}_{\mathfrak{p}}$.

Using the bases for $\mathcal{X}_p(J_0^D(M))$ computed above, we can compute $\mathcal{L}_{\mathfrak{p}}(f)$. In all cases it was enough to compute the kernel of $T_{11} - a_{11}(f) = T_{11} + 4$.

$\mathcal{X}_p^{Dp}(M)$	Basis	g_p	h_p	i_p
$\mathcal{X}_7(J_0^{21}(2))$	$\{(1,0,0,-1),(0,1,0,-1),(0,0,1,-1)\}$	$(1,-1,0,0)$	2	1
$\mathcal{X}_3(J_0^{21}(2))$	$\{(1,-1,0,0,0,0),(0,0,1,-1,0,0),(0,0,0,0,1,-1)\}$	$(0,0,1,-1,1,-1)$	4	2
$\mathcal{X}_2(J_0^{21}(2))$	$\{(1,-1)\}$	$(1,-1)$	4	4
$\mathcal{X}_7(J_0^{14}(3))$	$\{(1,0,0,-1),(0,1,0,-1),(0,0,1,-1)\}$	$(1,1,-1,-1)$	8	4
$\mathcal{X}_2(J_0^{14}(3))$	$\{(1,1,0,0,-1,-1),(0,0,1,0,0,-1),(0,0,0,1,-1,0)\}$	$(0,0,1,-1,1,-1)$	4	2
$\mathcal{X}_3(J_0^{14}(3))$	$\{(1,-1)\}$	$(1,-1)$	4	4
$\mathcal{X}_2(J_0^{6}(7))$	$\{(1,-1,0,0)\}$	$(1,-1,0,0)$	2	2
$\mathcal{X}_3(J_0^{6}(7))$	$\{(1,1,-1,-1)\}$	$(1,1,-1,-1)$	8	8
$\mathcal{X}_7(J_0^{6}(7))$	$\{(1,-1)\}$	$(1,-1)$	4	4

As we can compute $\mathcal{L}_{\mathfrak{p}}(f)$, allowing us to compute the Shimura degree for elliptic curves, we can do more work to compute the Shimura degree of modular abelian varieties. In particular, we need to compute $\mathcal{L}_{\mathfrak{p}}(f^{\sigma})$ for each conjugate of f. Computing the generator of the wedge product $\mathcal{L}_{\mathfrak{p}}(A)$ then comes down to computing a determinant.

4.4 Computing $\delta^{\mathfrak{D}}(\mathfrak{M})$ and Optimal Quotients

As discussed before, there are two methods for determining the Shimura degree. One in which we approximate the j-value of the optimal quotient and another in which we make the assumption that the map $\phi_{\mathfrak{p}}(J) \to \phi_{\mathfrak{p}}(E)$ is surjective.

Frequently, by computing the order of the component groups for the full isogeny class, we can provably compute both the Shimura degree and the optimal quotient. Here is a list of all curves in the isogeny class $42.a$ with the order of their component groups at given primes.

LMFDB Label	$\bar{c}_2$	$\bar{c}_3$	$\bar{c}_7$
$42.a1$	4	4	2
$42.a2$	8	2	1
$42.a3$	2	8	4
$42.a4$	1	4	8
$42.a5$	2	2	1
$42.a6$	1	16	2

In particular, the following relationships must be satisfied.

$\delta^D(M) = \frac{h_p \bar{c}_p}{i_p^2}$	$p = 2$	$p = 3$	$p = 4$
$\delta^{21}(2)$	$\frac{\bar{c}_2}{4}$	$\bar{c}_3$	$2\bar{c}_7$
$\delta^{14}(3)$	$\bar{c}_2$	$\frac{\bar{c}_3}{4}$	$\frac{\bar{c}_7}{2}$
$\delta^{6}(7)$	$\frac{\bar{c}_2}{2}$	$\frac{\bar{c}_3}{8}$	$\frac{\bar{c}_7}{4}$

Combining all the conditions forces the following degrees

$$\delta^{21}(2) = 2, \text{ with optimal quotient } 42.a2$$

$$\delta^{14}(3) = 2, \text{ with optimal quotient } 42.a3$$

$$\delta^{6}(7) = 1, \text{ with optimal quotient } 42.a3.$$

Notice that in all cases, this implies that for $p \mid D$, we have $j_p = 1$ and $i_p = \bar{c}_p$. Thus $\phi_p(J) \to \phi_p(E)$ is surjective.

In general, if we assume that $\phi_{\mathfrak{p}}(J) \to \phi_{\mathfrak{p}}(E)$ is surjective, and that at least one prime $\mathfrak{p}$ divides $\mathfrak{D}$, then we can compute the Shimura degrees.

In this case, we do not know what the $\bar{c}_p$'s are, but we are assuming that when $\mathfrak{p} \mid \mathfrak{D}$ that $\bar{c}_{\mathfrak{p}} = i_{\mathfrak{p}}$. Thus we can compute $\delta^{\mathfrak{D}}(\mathfrak{M})$ for one prime, and then work backwards and compute

$\bar{c}_{\mathfrak{q}} = \delta^{\mathfrak{D}}(\mathfrak{M}) i_{\mathfrak{q}}^2 / h_{\mathfrak{q}}$ for all other primes $\mathfrak{q} \mid \mathfrak{D}\mathfrak{M}$. Once we have computed all $\bar{c}_{\mathfrak{q}}$, we can use the LMFDB to find the curve in the isogeny class with the given discriminant

$$\Delta(E) = \prod_{\mathfrak{q} \mid \mathfrak{D}\mathfrak{M}} \mathfrak{q}^{\bar{c}_{\mathfrak{q}}}.$$

Due to Theorem 3.3.2, for elliptic curves over $\mathbb{Q}$ this method will always give the optimal quotient.

For abelian varieties, not knowing the $\bar{c}_{\mathfrak{p}}$'s is an even larger issue. As we do not have tables of modular abelian varieties with already computed component groups, this is the point where we cannot push this algorithm forward.

Problem 4.4.1. To compute Shimura degrees of modular abelian varieties, we need to know the order of their component groups. Is there an algorithm to compute component groups of modular abelian varieties?

4.4.1 Example over $\mathbb{Q}(\sqrt{5})$

Let J be a Jacobian of a curve X. A useful fact that we will commonly exploit is that the degree of the parameterization

$$J \to E$$

is one if and only if the dimension of J is one, i.e., if the genus of X is one. For modular curves, this can similarly be stated $m_E = 1$ if and only if the dimension of $S_2(N)^{\text{new}}$ is one.

We can apply this to the first isogeny class of elliptic curves over $F = \mathbb{Q}(\sqrt{5})$. Let $a = \frac{1+\sqrt{5}}{2}$. Then the curve $E : y^2 + xy + ay = x^3 + (-a-1)\,x^2$ has co conductor $N = (-5a+3)$ of norm 31. Let B-indefinite quaternion algebra over F with discriminant N. The Shimura curve$X_0^N(1)$ is a genus one curve, so the Shimura degree is trivially 1. However, there are 6 curves in the isogeny class. Using the tables of Bober, et al. [24] these curves have the following discriminant of the form $u \cdot (5a-3)^{\bar{c}_{\mathfrak{p}}}$ where u is a unit and $\mathfrak{p} = (5a-3)\mathbb{Z}_F$.

curve	$a1$	$a2$	$a3$	$a4$	$a5$	$a6$
$\bar{c}_{\mathfrak{p}}$	1	2	1	4	8	2

None of the discriminants are equal. If they share $\bar{c}_p$ then they still differ by a unit. However, this does give credence to the Voight and Willis method which uses the j-invariant to find the optimal quotient. Additionally, over $\mathbb{Q}(\sqrt{5})$ we have not proved any theorems on the finiteness of semistable isogenous discriminant twins.

Voight and Willis use their method of power series expansion to compute the j-invariant of the optimal quotient E:

$$j(E) = (-a)(-51a + 37)^3(-39a + 25)^3(5a - 3)^{-8}.$$

Examining all curves in the isogeny class, we find only one curve with corresponding j invariant:

$$a5 : y^2 + xy + ay = x^3 - (a + 1)x^2 - (30a + 45)x - (111a + 117).$$

As a double check, I also computed the Shimura degree using Hecke modules and found the same optimal quotient, without any assumptions such as Conjecture 3.1.

Chapter 5

DATA AND CONJECTURES

In this chapter I present the data gathered. Using Jacquet-Langlands, Shimura degrees should be connected with D-new subspaces of Hilbert and classical modular forms. In the computations I also explore this connection. It leads to interesting data and several conjectures.

5.1 D-new invariants

In [1], Agashe, Ribet, and Stein formulate the following relationship between congruence primes and modular degrees. Let E be an elliptic curve over $\mathbb{Q}$ with modular degree m_E and congruence number r_E. Let N_E be the conductor of E.

Theorem 5.1.1 (Agashe, Ribet, Stein)**.** *The modular degree m_E divides the congruence number r_E. Further, if $ord_p(N_E) \leq 1$ then $ord_p(m_E) = ord_p(r_E)$.*

In examining modular degree and congruence numbers, we have been studying these invariants on the entire modular curve and on the entire space of modular forms. However, the Jacquet-Langlands correspondence gives a precise relationship between the quaternionic modular forms and new subspace of classical modular forms. We can use this to formulate a conjecture similar to Theorem 5.1 for Shimura degrees.

First, recall the following definition. Let M and N be positive integers so that $M \mid N$. Let $D = N/M$. Then for $f(\tau) \in S_2(M)$ and $t \mid D$, $f(t\tau) \in S_2(N)$. Thus we have maps

$$S_2(M) \to S_2(N)$$

for each $t \mid D$. Combining these maps gives

$$\phi_M : \oplus_{(t|D)} S_2(M) \to S_2(N).$$

Definition 5.1.2. The image of ϕ_M is called the *D-old subspace* $S_2(N)^{D-\text{old}}$. The orthogonal complement of $S_2(N)^{D-\text{old}}$ in $S_2(N)$ with respect to the Petersson inner product $(\cdot,\cdot)$ is called the *D-new subspace* $S_2(N)^{D-\text{new}}$.

Recall that the Jacquet-Langlands correspondence says:

Theorem 5.1.3 (Jacquet-Langlands)**.** *There is a non-canonical map of Hecke modules*

$$\mathcal{S}_2^D(M) \cong \mathcal{S}_2(N)^{D-new}.$$

Further, we can restrict the Jacobian of the modular curve $X_0(N)$ to D-new subvarieties, $J_0(N)^{D-\text{new}}$. It then follows from Faltings' isogeny theorem that $J_0(N)^{D-\text{new}}$ is isogenous to the Shimura curve Jacobian $J_0^D(M)$. We can now define D-new analogues of congruence numbers and modular degrees.

Definition 5.1.4. The **D-new congruence number** $r_E^{D-\text{new}}$ is the integer that satisfies the following equivalent conditions:

1. r is the largest integer such that there exists $g \in L$ with $f \equiv g \pmod{r}$.
2. $\{(f,h) | h \in S\} = r^{-1}(f,f)\mathbb{Z}$.
3. r is the exponent of the finite group $S/(\mathbb{Z}f + L)$.

Similarly, we can define $m_E^{D-\text{new}}$ the D-new modular degree by restricting to the D-new part of the modular Jacobian $J_0(M)$.

Definition 5.1.5. The **D-new modular degree** is the degree of the map from

$$J_0^{D-\text{new}}(N) \to E$$

where E the an optimal quotient of $J_0^{D-\text{new}}(N)$.

These definitions lead us to the following questions: Does $m_E^{D-\text{new}}$ divide $r_E^{D-\text{new}}$? Does δ_M^D divide $r_E^{D-\text{new}}$? Is there a relationship between δ_M^D and $m_E^{D-\text{new}}$?

Computationally, $m_E^{D-\text{new}}$ is nice as it is a fast modular symbol computation. This contrasts with computing Brandt modules and Hecke operators, which can be quite slow. Further, our data in Table 5.1 gives the following proposition.

Proposition 5.1.6. *For semistable elliptic curves of conductor $N = DM$ with $N < 100$ and $N \neq 66, 91$, the invariants m_E^{D-new},r_E^{D-new},δ_M^D are all equal:*

$$\delta_M^D = m_E^{D-new} = r_E^{D-new}.$$

Despite 100 being relatively small, this does give good evidence for the following conjectures. Especially since with elliptic curves it is common to find counter examples at smaller conductors.

Conjecture 5.1.7. *For elliptic curves with square-free conductor N, the D-new degree equals the D-new congruence number.*

Conjecture 5.1.8. *For elliptic curves with square-free conductor $N = DM$, the D-new degree equals Shimura degree δ_M^D.*

In the following table, I have computed all Shimura degrees, associated new degrees, and new congruence numbers for elliptic curves with conductor less than 100, squarefree, and non-prime. The code can be found in the appendix, with the Shimura degree code A.1.1 and the D-new code A.1.2. The curve in the isogeny class 91b has a * indicating that I was only able to compute the Shimura degrees assuming Takahashi's Conjecture 3.1. I have to assume Conjecture 3.1, as in 66b there are curves with discriminants $-1 \cdot 7 \cdot 13$ and $-1 \cdot 7^3 \cdot 13^3$. Here the relations $\delta_1^{91} = \frac{h_p \bar{c}_p}{i_p}$ for $p = 7$ and $p = 13$ only give the information that $\bar{c}_7 = \bar{c}_{13}$. As there are two curves in the isogeny class satisfying this relationship, we cannot find the optimal quotient without more information or assuming Conjecture 3.1. Assuming Conjecture 3.1 says that Shimura degree here is both 4 instead of 12.

This situation occurs for several other isogeny classes as well, namely 39a, 55a, 65a, and 66b. However, in each of these cases, the Shimura degree is either 1 or $n > 1$. As none of the appropriate Shimura curves has genus 1, then the degree must be > 1. In all of the data, Takahashi's Conjecture 3.1 holds.

Isogeny Class	D	M	LMFDB Label	$\delta^D(M)$	$\delta^{D-\text{new}}(DM)$	r_E
$14a$	1	14	$a6$	1	–	–
$14a$	14	1	$a3$	1	1	1
$15a$	1	15	$a5$	1	–	–
$15a$	15	1	$a5$	1	1	1
$21a$	1	21	$a5$	1	–	–
$21a$	21	1	$a2$	1	1	1
$26a$	1	26	$a2$	2	–	–
$26a$	26	1	$a2$	2	2	2
$26b$	1	26	$b2$	2	–	–
$26b$	26	1	$b1$	2	2	2
$30a$	1	30	$a8$	2	–	–
$30a$	15	2	$a6$	2	2	2
$30a$	6	5	$a1$	1	1	1
$30a$	10	3	$a7$	1	1	1
$33a$	1	33	$a2$	3	–	–
$33a$	33	1	$a2$	1	1	1
$34a$	1	34	$a4$	2	–	–
$34a$	34	1	$a2$	1	1	1
$35a$	1	35	$a3$	2	–	–
$35a$	35	1	$a3$	2	2	2
$38a$	1	38	$a3$	6	–	–
$38a$	38	1	$a3$	2	2	2
$38b$	1	38	$b2$	2	–	–
$38b$	38	1	$b1$	2	2	2
$39a$	1	39	$a3$	2	–	–
$39a$	39	1	$a3$	2	2	2

Isogeny Class	D	M	LMFDB Label	$\delta^D(M)$	$\delta^{D-\text{new}}(DM)$	r_E
$42a$	1	42	$a5$	4	–	–
$42a$	21	2	$a4$	2	2	2
$42a$	14	3	$a3$	2	2	2
$42a$	6	2	$a3$	1	1	1
$46a$	1	46	$a2$	5	–	–
$46a$	46	1	$a1$	1	1	1
$51a$	1	51	$a2$	2	–	–
$51a$	51	1	$a1$	2	2	2
$55a$	1	55	$a3$	2	–	–
$55a$	55	1	$a3$	2	2	2
$57a$	1	57	$a1$	4	–	–
$57a$	57	1	$a1$	2	2	2
$57b$	1	57	$b2$	12	–	–
$57b$	57	1	$b1$	6	6	6
$57c$	1	57	$c2$	3	–	–
$57c$	57	1	$c2$	3	3	3
$58a$	1	58	$a1$	4	–	–
$58a$	58	1	$a1$	2	2	2
$58b$	1	58	$b2$	4	–	–
$58b$	58	1	$b1$	2	2	2
$62a$	1	62	$a4$	2	–	–
$62a$	62	1	$a2$	2	2	2
$65a$	1	65	$a1$	2	–	–
$65a$	65	1	$a1$	2	2	2

Isogeny Class	D	M	LMFDB Label	$\delta^D(M)$	$\delta^{D-\text{new}}(DM)$	r_E
$66a$	1	66	$a3$	4	–	–
$66a$	6	11	$a1$	2	2	2
$66a$	22	3	$a3$	2	2	2
$66a$	33	2	$a1$	4	4	4
$66b$	1	66	$b4$	4	–	–
$66b$	6	11	$b2^*$	2^*	2	2
$66b$	22	3	$b2^*$	2^*	2	2
$66b$	33	2	$b4$	4	4	4
$66c$	1	66	$c3$	20	–	–
$66c$	6	11	$c1$	2	2	2
$66c$	22	3	$c3$	2	2	2
$66c$	33	2	$c3$	4	4	4
$69a$	1	69	$a2$	2	–	–
$69a$	69	1	$a1$	2	2	2
$70a$	1	70	$a4$	4	–	–
$70a$	10	7	$a3$	1	1	1
$70a$	14	5	$a3$	2	2	2
$70a$	35	2	$a4$	2	2	2
$77a$	1	77	$a1$	4	–	–
$77a$	77	1	$a1$	2	2	2
$77b$	1	77	$b2$	20	–	–
$77b$	77	1	$b2$	10	10	10
$77c$	1	77	$c2$	6	–	–
$77c$	77	1	$c1$	2	2	2

Isogeny Class	D	M	LMFDB Label	$\delta^D(M)$	$\delta^{D-\text{new}}(DM)$	r_E
$78a$	1	78	$a4$	40	–	–
$78a$	6	13	$a3$	1	1	1
$78a$	26	3	$a3$	5	5	5
$78a$	39	2	$a4$	8	8	8
$82a$	1	82	$a2$	4	–	–
$82a$	82	1	$a2$	2	2	2
$84a$	1	84	$a2$	6	–	–
$84a$	21	4	–	?	2	2
$84b$	1	84	$b4$	6	–	–
$84b$	21	4	–	?	6	6
$85a$	1	85	$a1$	4	–	–
$85a$	85	1	$a1$	2	2	2
$90a$	1	90	$a4$	8	–	–
$90a$	10	1	$a2$	4	4	4
$90b$	1	90	$b3$	8	–	–
$90b$	10	1	$b4$	4	4	4
$90c$	1	90	$c8$	16	–	–
$90c$	10	1	–	?	4	4
$91a$	1	91	$a1$	4	–	–
$91a$	91	1	$a1$	4	4	4
$91b$	1	91	$b2$	4	–	–
$91b$	91	1	$b2^*$	4^*	4	4
$94a$	1	94	$a2$	2	–	–
$94a$	94	1	$a1$	2	2	2

The following table is for elliptic curves over $\mathbb{Q}(\sqrt{5})$. For each isogeny class up to conjugation, I have computed the congruence number r_E, Shimura degree when it is 1, and the optimal quotient when the Shimura degree is 1. As Hecke operators have not been implemented for

number fields, I cannot compute Shimura degrees in the cases where the Hecke module has rank greater than one. It is interesting to note that I was able to provably compute the optimal quotient in every case where I know the Shimura degree.

Isogeny Class	N	gen	D	M	LMFDB Label	$\delta^D(M)$	r_E
a	$31b$	$5a-2$	$5a-2$	1	$a5$	1	1
a	$36b$	6	2	3	$a3$	1	1
a	$36b$	6	3	2	$a4$	1	1
a	$41b$	$a+6$	$a+6$	1	$a2$	1	1
a	$45a$	$-6a+3$	3	$-2a+1$	$a5$	1	1
a	$45a$	$-6a+3$	$-2a+1$	3	$a4$	1	1
a	$49a$	7	7	1	$a2$	1	1
a	$55a$	$-a+8$	$-2a+1$	$-3a+2$	$a5$	1	1
a	$55a$	$-a+8$	$-3a+2$	$-2a+1$	$a5$	1	1
a	$71b$	$a+8$	$a+8$	1	$a4$	1	1
a	$76a$	$-8a+3$	2	$-4a+1$	?	?	2
a	$76a$	$-8a+3$	$-4a+1$	2	?	?	2
b	$76a$	$-8a+3$	2	$-4a+1$	?	?	2
b	$76a$	$-8a+3$	$-4a+1$	2	?	?	2
a	$79a$	$-8a+3$	$-8a+3$	1	$a4$	1	1
a	$89b$	$a+9$	$a+9$	1	$a3$	1	1
a	$95b$	$-2a+11$	$-2a+1$	$-4a+3$	$a6$	1	1
a	$95b$	$-2a+11$	$-4a+3$	$-2a+1$	$a1$	1	1
a	$99a$	$-9a+3$	3	$-3a+1$	$a1$	1	1
a	$99a$	$-9a+3$	$-3a+1$	3	$a4$	1	1

Chapter 6

DISCRIMINANT TWINS

In this section I discuss the proof of the following theorem stated earlier Theorem 3.3.2 and other results pertaining to discriminant twins. This section is joint work with Ben Lundell.

Theorem 6.0.9. *Over $\mathbb{Q}$, there are only finitely many semistable, isogenous discriminant twins. Using LMFDB labels [31], they are* $11a.1, 11a.3$, $17a.1, 17a.4$, $19a.1, 19a.3$, *and* $37b.1, 37b.3$.

The conductor and discriminant of an elliptic curve are two invariants that measure the bad reduction of the curve. The conductor of an elliptic curve E over $\mathbb{Q}$ is an integer N that measures the ramification in the extensions $\mathbb{Q}(E[p^\infty])/\mathbb{Q}$. The discriminant is an integer Δ which counts the number of irreducible components of $E(\mathbb{F}_p)$. We can view the conductor as an algebraic measure of the bad reduction and the discriminant as a geometric measure. When two elliptic curves have the same discriminant and conductor, we say they are discriminant twins.

If we do not restrict to the semistable or isogenous case, there are infinitely many discriminant twins. Via twisting curves of conductor 37, we show there are infinitely many isogenous and non-isogenous discriminant twins. Since we are twisting, this gives us a family of non-semistable discriminant twins. However, even though data suggests there are infinitely many semistable, non-isogenous discriminant twins, we do not yet know how to show this. Further, as Ribet and Takahashi can be generalized to elliptic curves over totally real number fields, we can ask about discriminant twins in this case as well. Unfortunately, due to an abundance of units, our results fail to directly generalize to this case.

6.1 p-adic Uniformization of Elliptic Curves and Isogenies

Let K be a field and E an elliptic curve over K. Then we can write E as

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

$a_1, a_2, a_3, a_4, a_6 \in K$, with the usual invariants:

$$\begin{aligned} b_2 &= a_1^2 + 4a_2 & b_4 &= 2a_4 + a_1a_3 \\ b_6 &= a_3^2 + 4a_4 & b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \\ c_4 &= b^2 - 24b_4 & c_6 &= -b_2^3 + 36b_2b_4 - 216b_6 \\ \Delta &= -b_2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 & j &= c_4^3/\Delta \\ &= (c_4^3 - c_6^2)/1728 \end{aligned}$$

As the discriminant depends on the choice of model, it is useful to work with a fixed model. Over $\mathbb{Q}$ we can find a curve E' isomorphic to E so that E' has the minimal discriminant. We define the discriminant of E' to be the minimal discriminant. By the Laska-Kraus algorithm, we known the minimal discriminant of E over $\mathbb{Q}$ is unique and compatible [28].

As we will frequently be changing models and examining what happens under isomorphism, it is useful to have the following notation. Let E, E' be isomorphic elliptic curves defined over a field K. If $\tau : E \to E'$ is an isomorphism of elliptic curves E and E', with E given by $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ and E' by $y'^2 + a_1'x'y' + a_3'y' = x'^3 + a_2'x'^2 + a_4'x' + a_6'$, then we denote $\tau = [u, r, s, t]$ and

$$\begin{aligned} x &= u^2x' + r \\ y &= u^3y' + su^2x' + t \\ \Delta &= u^{12}\Delta' \end{aligned}$$

Notice that τ changes the discriminant by 12th powers of u.

If all of $u, r, s, t \in K$, then we say τ is defined over K and thus E and E' are isomorphic over K, or just isomorphic. In general, τ need not be defined over K. The isomorphism τ could instead be defined over some extension of K. When this happens E and E' have the same j-invariants, $j = j'$, and we say E and E' are twists. In particular, we will be interested in

quadratic twists of elliptic curves over $\mathbb{Q}$. The quadratic twist of E by d and given in short Weierstrass form, denoted by E^d, is

$$dy^2 = x^3 + Ax + B.$$

This isomorphism is defined over $\mathbb{Q}(\sqrt{d})$. When N and d are coprime, wee see that it changes the discriminant by 6th powers of D where D is the discriminant of $\mathbb{Q}(\sqrt{d})$. Similarly, it changes the conductor from N to ND^2 [10].

Let $E/\mathbb{Q}$ be a minimal model with discriminant Δ. Then for each prime p dividing Δ, we can examine $\tilde{E}$, the reduction of $E \pmod p$. The primes p that divide the minimal discriminant Δ are exactly the primes where E is not smooth mod p, i.e., the primes of bad reduction. Further, the primes dividing Δ can give a model with bad reduction in two different ways. Either $\tilde{E}$ can have a singularity and one tangent line, in which case we say $\tilde{E}$ has additive reduction, or $\tilde{E}$ can have a singularity and two tangent lines. If the slopes are defined over the residue field, we say $\tilde{E}$ has split multiplicative reduction. Otherwise, if the slopes are defined over some extension of the residue field, we say $\tilde{E}$ has non-split multiplicative reduction.

The conductor N of an elliptic curve E is can be written explicitly as

$$N = \prod_{p|D} p^{f_p}$$

where $f_p = 1$ if E has a node at p and $f_p = 2 + \delta$ if E has a cusp at p, $\delta \in \mathbb{Z}_+$. If $p \neq 2, 3$, $\delta = 0$. The conductor and minimal discriminant are both compatible via Tate's algorithm [45]. An elliptic curve E is semistable if it has only multiplicative reduction, i.e., if N is square-free. Note that the conductor is an isomorphism class invariant; in fact, it does not depend on the choice of model. Further, the conductor is actually an isogeny class invariant, and does not depend on the choice of curve in the isogeny class.

If K is a field of characteristic zero then we can write E in short Weierstrass form

$$y^2 = x^3 + Ax + B, \qquad A, B \in K.$$

In particular, the isogeny defined by the composition $\tau = [1, -b_2/12, 0, 0] \circ [1, 0, -a_1/2, -a_3/2]$ sends E to this form. Note that for both isogenies in the composition of τ, we have $u = 1$

and so the discriminant does not change. Thus if $E/\mathbb{Q}$ has a minimal discriminant, so does the short Weierstrass form.

Let K be an algebraically closed field of characteristic zero. If E and E' are isogenous elliptic curves defined over K, then there is a non-constant map that sends identities to identities: $\mathcal{O} \mapsto \mathcal{O}'$. Let $\mu : E \to E'$ be an isogeny, then we can write μ as a rational map. In particular, if $(x, y) \in E$, $\mu(x, y) = \left(f_\mu(x), \frac{1}{\gamma_\mu} y \frac{df_\mu(x)}{dx}\right)$, with $f_\mu \in K(x)$. If we know the kernel of the isogeny, we can write down f_μ explicitly. Let C be a finite, non-trivial subgroup of $E(K)$ and write E in short Weierstrass form $y^2 = x^3 + Ax + B$. If $Q \in E(K)$, denote the coordinates of Q by $(x(Q), y(Q))$. Following González's reformulation of Vélu's formulas [17], we can write the isogenous curve explicitly in terms of C. Let $\mu_C : E \to E_C$ denote the isogeny given by $\mu_C(x, y) = \left(f_C(x), y \frac{df_C(x)}{dx}\right)$ with

$$f_C(x) = x + \sum_{Q \in C \setminus \{\mathcal{O}\}} \left(\frac{t(Q)}{x - x(Q)} + \frac{u(Q)}{(x - x(Q))^2} \right),$$

where $t(Q) = 3x(Q)^2$ and $u(Q) = 2(x(Q)^3 + Ax(Q) + B)$. Then taking $A_C = A - 5t$, $t = \sum_{Q \in C \setminus \{\mathcal{O}\}} t(Q)$ and $B_C = B - 7w$ with $w = \sum_{Q \in C \setminus \{\mathcal{O}\}} (u(Q) + x(Q)t(Q))$, we can write E_C as $y^2 = x^3 + A_C x + B_C$.

6.1.1 Infinitely Many Discriminant Twin Pairs

Proposition 6.1.1. *There exists infinitely many pairs of isogenous discriminant twins and infinitely many pairs of non-isogenous discriminant twins over $\mathbb{Q}$.*

Proof. As twisting preserves isogenies, that is, E and E' are isogenous if and only if the twists E^d and E'^d are isogenous, we can prove both the isogenous and non-isogenous cases at the same time. We begin by examining the curves of conductor 37, as there are three curves in two isogeny classes with the same conductor and discriminant, giving us our initial curves to twist. These curves are: $37a.1$, $37b.1$, and $37b.3$ and all have discriminant 37. Let $p \neq 37$, $p \equiv 1 \pmod 4$ so that the discriminant of $\mathbb{Q}(\sqrt{p})$. Then the quadratic twists of $37a.1$, $37b.1$, and $37b.3$ by p all have conductor $37p^2$ and discriminant $37p^6$. Moreover, twisting commutes with isogenies [10], so the twists of $37a.1$ and $37b.1$ remain non-isogenous,

while the twists of $37b.1$ and $37b.3$ remain isogenous. Thus twisting $37a.1$ and $37b.2$ gives a family of non-isogenous discriminant twins, and twisting $37b.1$ and $37b.3$ gives a family of isogenous discriminant twins. $\square$

However, with the exception of the original curves, all curves in either family will have additive reduction at the prime p. So while this gives infinitely many discriminant twin pairs, it does nothing to address whether there are infinitely many semistable, non-isogenous discriminant twins. Further, we do not even know if infinitely many j-invariants occur among the discriminant twins.

Question 6.1.2. Do infinitely many j-invariants occur among all discriminant twin pairs?

6.2 Semistable Isogenous Curves

For semistable curves, we can use the Tate curve parameterization over $\mathbb{Q}_p$ to examine how discriminants change under isogeny. For background and proofs see Chapter V, Sections 3-6 of [45]. Let K be a number field, fix a prime $\mathfrak{p}$ ideal in the ring of integers $\mathbb{Z}_K$, and k the residue field of $\mathfrak{p}$. Take $K_\mathfrak{p}$ to be the completion of K at $\mathfrak{p}$ and $\nu_\mathfrak{p} = \nu$ be the valuation map.

If E has multiplicative reduction, then there exists a unique parameter $q \in \mathbb{Z}_{K_\mathfrak{p}}$ with $\nu(q) \geq 1$ such that $E(\overline{K}_\mathfrak{p}) \cong \overline{K}_\mathfrak{p}^\times / q^\mathbb{Z}$.

Let $\gamma(E) = -c_4/c_6 \in K_\mathfrak{p}^\times / K_\mathfrak{p}^{\times 2}$. If $\sqrt{\gamma(E)} \in K$, then E has split multiplicative reduction at $\mathfrak{p}$ we can say even more: $E(K_\mathfrak{p}) \cong K_\mathfrak{p}^\times / q^\mathbb{Z}$. If E has non-split multiplicative reduction at $\mathfrak{p}$ then for the extension $L_\mathfrak{p} = K_\mathfrak{p}(\sqrt{\gamma(E)})$ of $K_\mathfrak{p}$: $E(L_\mathfrak{p}) \cong L_\mathfrak{p}^\times / q^\mathbb{Z}$.

Further, we can also write the discriminant and j-invariant of E in terms of its Tate parameter q: $\Delta(E) = q \prod_{n \geq 1} (1 - q^n)^{24}$ so that $\nu(\Delta(E)) = \nu(q)$, and $j(E) = \frac{1}{q} + \sum_{n \geq 0} c_n q^n$, where the c_n can be explicitly described, so that $\nu(j) = -\nu(q)$.

We now use Tate curves to study how discriminants change under isogeny. Let E and E' be two semistable ℓ-isogenous curves over K where $\ell \in \mathbb{Z}$ is a prime. Pick a prime p such that E has split multiplicative reduction at $\mathfrak{p}$. As E and E' are isogenous, E' has split

multiplicative reduction at $\mathfrak{p}$ as well. Let E have parameter q and E' have parameter q'. The ℓ-isogeny and its dual can be written explicitly:

$$\begin{array}{ccc} K_{\mathfrak{p}}^{\times}/q^{\mathbb{Z}} \to K_{\mathfrak{p}}^{\times}/(q')^{\mathbb{Z}} & \text{and} & K_{\mathfrak{p}}^{\times}/(q')^{\mathbb{Z}} \to K_{\mathfrak{p}}^{\times}/q^{\mathbb{Z}} \\ u \mapsto u^n & & v \mapsto v^m \end{array}$$

for some integers n, m such that $q^n = (q')^m$ and $nm = \ell$. Since ℓ is prime, pick $n = 1$ and $m = \ell$ and $q = (q')^{\ell}$. Thus we can write precisely how the discriminant changes, $\nu(\Delta) = \ell\nu(\Delta')$.

If E has non-split multiplicative reduction, E' does as well. Then $E(L) \cong L_{\mathfrak{p}}^{\times}/q^{\mathbb{Z}}$, $E'(L) \cong L_{\mathfrak{p}}^{\times}/q'^{\mathbb{Z}}$, and the same argument applies. Thus, if an isogeny class has only two curves, then the isogeny between the curves must be prime degree and so we get the following corollary:

Corollary 6.2.1. *Isogeny classes of size two with at least one prime of multiplicative reduction cannot have discriminant twins.*

Now let's examine isogeny classes with three non-isomorphic curves, E, E', E'', where there is a degree ℓ isogeny from $E \to E'$ and another ℓ isogeny from $E' \to E''$. Again we are assuming split multiplicative reduction at $\mathfrak{p}$. Then we get the same Tate parameterization as before, q, q', q'' respectively and get the following sequence:

$$K_{\mathfrak{p}}^{\times}/q^{\mathbb{Z}} \to K_{\mathfrak{p}}^{\times}/(q')^{\mathbb{Z}} \to K_{\mathfrak{p}}^{\times}/(q'')^{\mathbb{Z}}.$$

If we start as before with $q = (q')^{\ell}$, then there are two cases for the second isogeny:

1. $q' = (q'')^{\ell}$ and then $\nu(\Delta) = \ell\nu(\Delta') = \ell^2\nu(\Delta'')$.
2. $q'' = (q')^{\ell}$, but this implies that $q'' = q$. As E and E' are non-isomorphic, over K they have distinct j-invariants, thus they also do over $K_{\mathfrak{p}}$ and so $q'' \neq q$ and this case cannot occur.

Now instead assume $q' = q^{\ell}$. If $q'' = (q')^{\ell}$ we are in the analogous case to the first and $\nu(\Delta'') = \ell\nu(\Delta') = \ell^2\nu(\Delta)$. If instead $q' = (q'')^{\ell}$ we have $(q'')^{\ell} = q^{\ell}$. If $K_{\mathfrak{p}}$ does not contain ℓ-th roots of unity, this implies that $q'' = q$ and again this cannot occur. If however, $K_{\mathfrak{p}}$

does contain the ℓ-th roots of unity, this does and can occur. Over $\mathbb{Q}_p$ this is the case where $p \equiv 1 \pmod{\ell}$. Analyzing the discriminants, $\nu(\Delta) = \nu(\Delta'')$ and $\nu(\Delta') = \ell\nu(\Delta) = \ell\nu(\Delta'')$. In this case we say that E and E'' are ℓ-discriminant twins.

Using the same notation as before we summarize this in the following table.

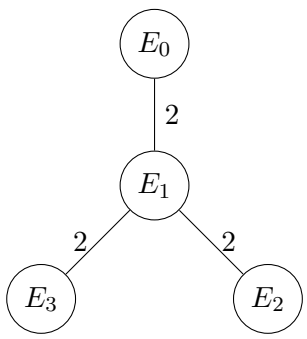
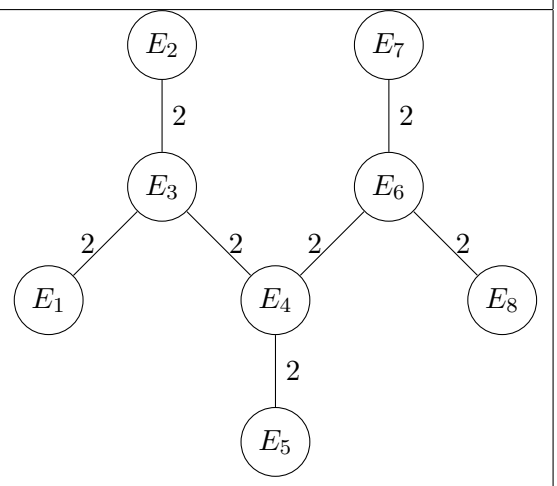
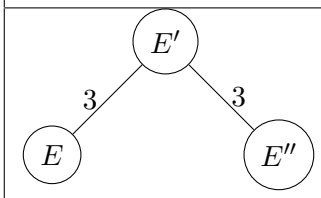
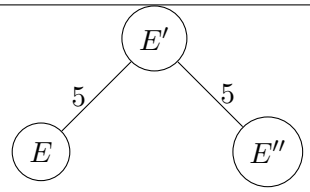
Tate parameter $= q$	q'	q''	Behavior
q	q^ℓ	$(q^\ell)^\ell$	not discriminant twins
q	q^ℓ	$(q^\ell)^{1/\ell}$	different ℓth root of unity, ℓ-discriminant twins
q	$q^{1/\ell}$	$(q^{1/\ell})^\ell = q$	$E = E''$
q	$q^{1/\ell}$	$(q^{1/\ell})^{1/\ell}$	not discriminant twins

(6.2.1)

Corollary 6.2.2. *If E' is a semistable elliptic curve with two ℓ-isogenies, then $\nu_p(\Delta(E')) \equiv 0 \pmod{\ell}$ for all $p \mid \Delta(E')$.*

Proof. Following the above table of all possible q-parameters for the Tate curves, in the first two rows, q' is already an ℓth power. The third case, cannot occur. In the fourth case, as $\nu(q'') \geq 1$, $q' = q^{1/\ell}$must be an ℓth power so that the ℓth root is in $K_\mathfrak{p}$. As E' is semistable, we do this for all primes dividing $\Delta(E')$. Thus $\Delta(E')$ is an ℓ-th power. $\square$

The goal of this section is to show that there are only finitely many semistable, isogenous, discriminant twin pairs of elliptic curves over $\mathbb{Q}$. However, locally, we see that ℓ-discriminant twins occur frequently, but only when the two curves have prime squared power isogenies. Using results of Mazur [33] and Kenku [25], we cut down on possible isogeny degrees as follows: The only prime power isogeny degrees that occur for semistable elliptic curve isogenies are $\ell = 2^2, 2^3, 3^2$, or 5^2 and have the following prime degree isogeny graphs:

Isogeny Graph for 2^2	Isogeny Graph for 2^3
	
Isogeny Graph for 3^2	Isogeny Graph for 5^2
	

Kubert's [29] parameterizations of curves with rational torsion allows us to explicitly compute the isogenous curves. We can examine the discriminants of these curves to study how the discriminants change under isogeny. In the next sections, we go through each case, $2^2, 3^2, 5^2$ and find all possible semistable, isogenous, discriminant twin pairs of each isogeny degree. To set notation, let E, E', E'' be isogenous elliptic curves with isogenies of degree ℓ between $E \to E'$ and $E' \to E''$ and a degree ℓ^2 isogeny between $E \to E''$ so we have the following sequence:

$$E \to E' \to E''.$$

When $\ell = 3$ or 5 we need the following lemma.

Lemma 6.2.3. *If $K = \mathbb{Q}$ and $\ell = 3$ or 5, E and E' have rational ℓ torsion and E'' does not.*

Proof. For any two ℓ-isogenous curves, $E \to E'$, the kernel is either $\mathbb{Z}/\ell\mathbb{Z}$, rational torsion in E or μ_ℓ, a Galois invariant subgroup. Thus one of E or E' must have rational ℓ-torsion.

By Mazur's Theorem [33] the torsion subgroup of an elliptic curve over $\mathbb{Q}$ is only divisible by ℓ^2 if $\ell = 2$. Thus for $\ell \geq 3$ and ℓ-isogenous elliptic curves

$$E \to E' \to E'',$$

either E and E' both have ℓ-rational torsion, E' and E'' both have ℓ-rational torsion, or E and E'' have ℓ-rational torsion. As E' has two ℓ isogenies $E' \to E''$ and $E' \to E$, the dual of $E \to E'$, and $\ell \geq 3$, then the kernel of one of the isogenies is $\mathbb{Z}/\ell\mathbb{Z}$. Thus E' has ℓ-rational torsion. By switching E and E'' if necessary, we get the first statement.

□

Now we can start the case by case work for $\ell = 2, 3, 5$. All code for the computations in the proofs is found in the appendix, 5-isogenies A.2.1, 3-isogenies A.2.2, 2-isogenies A.2.3, and can also be found on Github `https://github.com/adeines/DiscriminantTwins`. All three cases follow a similar pattern of proof. First, we use the parameterization of curves with given torsion as found in Kubert [29]. We use this parameterization to make statements about the reduction type of the model at given primes. Next, we use the parameterization to find all the torsion points. Once we have the torsion points, we write the curves in a form which allows us to use Vélu's formulas to find the other curves in the isogeny class and write their discriminants in terms of the initial parameters. Finally, we are able to again use Tate curves to find the only cases in which discriminant twins with semistable reduction can occur.

Theorem 6.2.4. *There are no* 5*-isogenous discriminant twins outside the pair* $11a.2$ *and* $11a.3$.

Proof. As above, let E, E', E'' be elliptic curves over $\mathbb{Q}$ such that there are $\ell = 5$ isogenies $E \to E'$ and $E' \to E''$, so we have the following sequence:

$$E \to E' \to E''$$

and we can assume both E and E' both have rational 5-torsion (and that E'' does not.) Kubert gives a parameterization for curves with rational 5-torsion. Using this parameterization, we

can assume E has the form

$$y^2 + (1-t)xy - ty = x^3 - tx^2$$

for some t and a rational point $(0,0)$ of order 5. Then the discriminant is

$$\Delta(E) = \Delta = t^5(t^2 - 11t - 1).$$

As we want $\Delta(E) \in \mathbb{Z}$, we must have $t \in \mathbb{Z}$. Note that this $\Delta(E)$ is already minimal at $p \mid t$. To see this, pick any prime p dividing t. Since $c_4(E) = t^4 - 12t^3 + 14t^2 + 12t + 1$ is not divisible by p, Kraus' algorithm tells us that the discriminant is already minimal at p.

Using Sage we can compute all the points in $E(\mathbb{Q})[5]$ in terms of t. They are $\mathcal{O}$ = the point at infinity, $(0,0)$, $(t,0)$, $(0,t)$, and (t,t^2). Since we know all the points in $E(\mathbb{Q})[5]$ it is possible to use Véul's formula to explicitly compute E'. We start by rewriting E in the form $y^2 = x^3 + A(t)x + B(t)$ via $\tau = [1, -\frac{1}{12}t^2 + \frac{1}{2}t - \frac{1}{12}, \frac{1}{2}t - \frac{1}{2}, -\frac{1}{24}t^3 + \frac{7}{24}t^2 + \frac{5}{24}t + \frac{1}{24}]$ to get

$$y^2 = x^3 + \left(-\frac{1}{48}t^4 + \frac{1}{4}t^3 - \frac{7}{24}t^2 - \frac{1}{4}t - \frac{1}{48}\right)x + \frac{1}{864}t^6 - \frac{1}{48}t^5 + \frac{25}{288}t^4 + \frac{25}{288}t^2 + \frac{1}{48}t + \frac{1}{864}.$$

Using τ, and the 5-torsion on the original model we can compute all of $E(\mathbb{Q})[5]$ and then use Vélu's formula to compute E' in terms of the parameter t to get

$$y^2 = x^3 + \left(-\frac{1}{48}t^4 - \frac{19}{4}t^3 - \frac{247}{24}t^2 + \frac{19}{4}t - \frac{1}{48}\right)x + \frac{1}{864}t^6 - \frac{29}{48}t^5 - \frac{3335}{288}t^4 - \frac{3335}{288}t^2 + \frac{29}{48}t + \frac{1}{864}.$$

For the Sage code, see the appendix. Doing so we find

$$\Delta(E') = \Delta' = t(t^2 - 11t - 1)^5.$$

Again since $c_4(E')$ is not divisible by p, $\Delta(E')$ is also minimal at p.

Examining the parameterization of E by t, we can reduce mod p to get:

$$y^2 + xy = x^3.$$

Using Tate's algorithm, as $p \nmid c_4$, E has multiplicative reduction. As $T^2 - a_1T - a_2 \equiv T(T-1) \pmod{p}$, both tangents are in $\mathbb{F}_p$ and E has split multiplicative reduction at p. Thus E' and

E'' also have split multiplicative reduction at p and we get the following sequence of Tate curve parameterizations:

$$\mathbb{Q}_p^\times/q^{\mathbb{Z}} \to \mathbb{Q}_p^\times/(q^{1/5})^{\mathbb{Z}} \to \mathbb{Q}_p^\times/(q'')^{\mathbb{Z}}.$$

What are the possibilities for q''? If $q'' = (q^{1/5})^5 = q$, then $q = q''$ and $E = E''$ over $\mathbb{Q}_p$. Since we assumed that E and E'' are isogenous and not isomorphic, this cannot occur. Thus we must have $q'' = q^{1/25}$ and $25v_p(\Delta'') = v_p(\Delta)$.

Thus 5-discriminant twins can only occur if t is a unit. Over $\mathbb{Q}$, if $t = \pm 1$, then E is the elliptic curve with LMFDB label $11a.3$ and discriminant 11, E' is $11a.2$ with discriminant 11^5 and E'' is $11a.1$ with discriminant 11 [31].

□

Theorem 6.2.5. *There are no* 3*-discriminant twins outside the two pairs* $19a_2, 19a_3$ *and* $37b_2, 37b_3$.

Proof. This proof follows similarly to the $\ell = 5$ case. The main difference is that the elliptic curves E with rational 3-torsion are parameterized by two variables and so a bit more work goes into this at the end. If E has rational 3-torsion, we can write E as:

$$y^2 + a_1xy + a_3y = x^3$$

with a point of order three at $(0, 0)$. Its discriminant is $\Delta = \Delta(E) = -a_3^3(-a_1^3 + 27a_3)$. By using Tate's algorithm, we see that Δ is reduced at all $p \mid \Delta$ unless $p \mid a_1$ and $p \mid a_3^3$. If $p \mid a_1$ and $p \mid a_3^3$, $\mathrm{ord}_p(\Delta) = 9\mathrm{ord}_p(a_3) + 3\max\{\mathrm{ord}_p(a_1) + \mathrm{ord}_p(a_3/3)\} \geq 12$. In this case $p^{12} \mid \Delta$ and thus we can take an isomorphism $[u, r, s, t] = [p, 0, 0, 0]$ that changes the model of E to the form $y^2 + a_1p^{-1}xy + a_3p^{-3}y = x^3$. So assume a_1 and a_3 are reduced. Then, E only has additive reduction if $p \mid a_1$ and $p \mid a_3$.

To see this, assume that if $p \mid a_1$, then $p^3 \nmid a_3$ and if $p^3 \mid a_3$, then $p \nmid a_1$. There are three cases to check: $p \mid a_3$ and $p \nmid a_1$, $p \mid a_3$ and $p \mid a_3$, and $p \nmid a_1a_3$ but $p \mid -a_1^2 + 27a_3$. In the first and third cases, $p \mid \Delta$, but $b_2 = a_1^2$ is not divisible by p, so E has multiplicative reduction. In the second case, $p \mid \Delta$ and $p \mid b_2 = a_1^2$. Running Tate's algorithm we see $p^2 \mid a_6 = 0$, $p^3 \mid b_8 = 0$

and we get to the point where we check if $p^3 \mid b_6 = a_3^2$. If $p \mid\mid a_3$, then the answer is no, and E has additive reduction at p. Otherwise $p^2 \mid\mid a_3$ and we do a bit more work but get to step 8 of [45] and see that in this case E has additive reduction as well. As we are working with semistable curves, we can now assume $(a_1, a_3) = 1$.

Again we use Sage to find all torsion points of E. We then write E in the form

$$y^2 = x^3 + A(a_1, a_3)x + B(a_1, a_3),$$

and push the points onto this form As before, we proceed to use Vélu's formulas to find the curve $E' = E/E(\mathbb{Q})[3]$. Then $\Delta' = \Delta(E') = -a_3(-a_1^3 + 27a_3)^3$. Making again the assumption that E' has rational 3-torsion, equivalently, E' is isogenous to E'' with E'' and E non-isomorphic, Δ' must be a cube. The only case where E and E'' can be discriminant twins is if

$$\mathbb{Q}_p^\times/q^{\mathbb{Z}} \to \mathbb{Q}_p^\times/(q^3)^{\mathbb{Z}} \to \mathbb{Q}_p^\times/(\xi q)^{\mathbb{Z}}$$

where ξ is a 3rd root of unity in $\mathbb{Q}_p$.

As with $\ell = 5$, we study primes p dividing a_3. Take p a prime dividing a_3 and let $n = v_p(a_3)$. As $a_3^3 \mid \Delta$, $v_p(\Delta) = 3n$. However, Δ' is a cube and $(a_3, -a_1^3 + 27a_3) = 1$, thus $v_p(a_3) = 3m$. To have E and E' be discriminant twins, $3v_p(\Delta) = v_p(\Delta')$, but $3v_p(\Delta) = 3v_p(a_3^3) = 9v_p(a_3)$ and $v_p(\Delta') = v_p(a_3)$ so $3v_p(\Delta) \neq v_p(\Delta')$. Thus if $p \mid a_3$, we cannot have discriminant twins and to have discriminant twins we must have $a_3 = \pm 1$.

Again assume E and E'' are discriminant twins. Then $a_3 = \pm 1$ and E' has 3-torsion so we can write E' as

$$y^2 + a_1'xy + a_3'y = x^3$$

with a point of order three at $(0, 0)$. Its discriminant is $\Delta' = -a_3'^3(-a_1'^3 + 27a_3') = -a_3(-a_1^3 + 27a_3)^3$. Further, $\Delta'' = \Delta(E'') = -a_3'(-a_1'^3 + 27a_3')^3$. As Δ' is a cube and $v_p(\Delta') = 3v_p(\Delta'')$, $-a_1'^3 + 27a_3' = \pm 1$ and $a_3' = -a_1^3 + 27a_3$. The only integers $(a_1, a_3), (a_1', a_3')$ satisfying these relations are $(-4, -1), (-10, -37)$ corresponding to $37b.3$ and $37b.2$, $(-3, -1), (-1, 0)$ (which give singular curves) and $(-2, -1), (-8, -19)$ corresponding to $19a.3$ and $19a.2$. Thus we get the only 3-isogenous discriminant twins are $37b.3, 37b.1$ and $19a.3, 19a.1$. $\square$

Finally, we examine $\ell = 2$. If E has two torsion, then we can write E in the form

$$y^2 = x(x-s)(x-r) = x^3 - (r+s)x^2 + rsx$$

for $r, s \in \mathbb{Q}$. Via the isomorphism $x \mapsto u^{-2}x$, $y \mapsto u^{-3}y$, we can take $r, s \in \mathbb{Z}$. Then $\Delta = 16r^2s^2(r-s)^2 \in \mathbb{Z}$. As before, we must first address the issue that this might not give a minimal model.

Lemma 6.2.6. *For $p = 2$ and $p \mid \Delta$, if $p \mid r$ and $p \mid s$, then either the curve is not minimal or it has additive reduction.*

Proof. If $p \mid 2$, then $\tilde{E}$ can be written as $y^2 = x^3$ and $\mathrm{ord}_p(\Delta) = 4\mathrm{ord}_p(2) + 2\mathrm{ord}_p(r) + 2\mathrm{ord}_p(s)$. If either $p^2 \mid s$ or $p^2 \mid r$ then via the isomorphism $[p, 0, 0, 0]$ we can reduce the model. So without loss of generality, assume $p \mid\mid s$ and $p \mid\mid r$. Then we fly through Tate's algorithm: as $2 \mid b_2 = -4(r+s)$, $p^2 \mid a_6 = 0$, $p^3 \mid b_8 = -(rs)^2$, and $p^3 \mid b_6 = 0$, we find ourselves at step 6 as given in [45]. Studying how the polynomial $T^3 + a_2/2T^2 + a_4/4T + a_6/8 = T^3 - (r+s)/2T^2 + (rs)/4T$ factors mod 2, we see that as $2 | r+s$ and $4 \mid\mid rs$, the polynomial either has three distinct roots (if $2 \mid\mid r+s$) or one simple root and a double root (if $4 \mid r+s$). In either case, Tate's algorithm tells us that E has additive reduction.

□

Thus we can assume $p = 2$ only divides one of r, s, or $r - s$. Without loss of generality, assume $2 \mid r$. Note that under the isomorphism $[1, s, 0, 0]$, the model of E changes to $y^2 = x^3 - (s + (s-r))x^2 + s(s-r)x$ and the torsion is parameterized by the points s and $s - r$ instead of s and r. So we really can assume $2 \mid r$ without any loss of generality. Then we have the following lemma.

Lemma 6.2.7. *Assume $2 \mid r$ and $2 \nmid s$. If $2^4 \mid\mid r$ then E has good reduction, if $2^n \mid r$ for $n > 4$, E has multiplicative reduction, and if $2^n \mid r$ for $n < 4$, E has additive reduction.*

Proof. As $2 \mid r$ and $2 \nmid s$, $\mathrm{ord}_2(\Delta) = 4 + 2\mathrm{ord}_2(r)$. Then $\tilde{E}$ is $y^2 = x^3 - sx^2$ which has a singular point at $(0, 0)$. As $2 \mid b_2 = -4(r+s)$ and $4 \mid a_6 = 0$, we get to step 4 of Tate's algorithm. For our curve, $b_8 = -(rs)^2$ so $\mathrm{ord}_2(b_8) = 2\mathrm{ord}_2(r)$. Thus if $\mathrm{ord}_2(r) = 1$, E has

additive reduction. To continue, assume $\mathrm{ord}_2(r) > 1$, so that $2^3 \mid b_8$. Then $b_6 = 0$ so $2^8 \mid b_6$ and we are in step 6. Here we must change coordinates so that

$$2 \mid a_1 \text{ and } a_2, 4 \mid a_3 \text{ and } a_4, \text{ and} 8 \mid a_6.$$

Note that in our current state: $y^2 = x^3 - (r+s)x^2 + rsx$, $2 \nmid a_2 = -(r+s)$. However, the substitution $y' = y + x$ gives a new model which does satisfy these conditions and which we will proceed to use for the remainder of the algorithm:

$$y^2 + 2xy = x^3 - (r+s+1)x^2 + rsx.$$

Next, we factor the polynomial

$$P(T) = T^3 + a_2/2T^2 + a_4/4T + a_6/8 = T^3 - (r+s+1)/2T^2 + rs/4T$$

in $\mathbb{F}_2$. If $\mathrm{ord}_2(r) = 2$ we have two choices:

$$P(T) \equiv T(T^2 + rs/4) \pmod 2 \text{ and } P(T) \equiv T(T^2 + T + rs/4) \pmod 2$$

both of which indicate additive reduction. If $\mathrm{ord}_2(r) > 2$, we again have two choices:

$$P(T) \equiv T^3 \pmod 2 \text{ and } P(T) \equiv T^2(T+1) \pmod 2.$$

In the latter case, with a simple and a double root, E has additive reduction. Assume $P(T) \equiv T^3 \pmod 2$. To reiterate, this means that $\mathrm{ord}_2(r) > 2$ and $\mathrm{ord}_2(s+1) \geq 2$. We are now at step 8 in Tate's algorithm. As the polynomial $Y^2 + a_3/4Y - a_6/16 = Y^2$ has a double root mod 2, we move on to step 9 and check if $2^4 \mid a_4$. Here $a_4 = rs$ and $\mathrm{ord}_2(s) = 0$. If $\mathrm{ord}_2(r) = 3$, then E has additive reduction. If $\mathrm{ord}_2(r) \geq 4$, we move on to the final step, step 11. If $\mathrm{ord}_2(r) \geq 4$, we try again with the curve

$$y^2 + xy = x^3 - (r+s+1)/4x^2 + rs/16x.$$

The discriminant of this new model is $1/256(r-s)^2r^2s^2$. Thus if $\mathrm{ord}_2(r) = 4$, $2 \nmid 1/256(r-s)^2r^2s^2$. If $\mathrm{ord}_2(r) > 4$, $\tilde{E}$ is $y^2 + xy = x^3 - x$ or $y^2 + xy = x^3$. Either way, $(0,0)$ is a singular point. However, $b_2 = 1 - (r+s+1) \equiv 1 \pmod 2$ as $2 \nmid s$. Thus E has split multiplicative reduction at 2.

$\square$

Now, let p be any prime not equal to 2. As before, without loss of generality, let $p \mid r$. Notice that then $p \mid r$ if and only if $p \mid s + r$.

Lemma 6.2.8. *If $p \mid r$ and $(r, s) = 1$, then E has multiplicative reduction. Otherwise, E has additive reduction or is not minimal.*

Proof. Start with $p \mid r$. As $\Delta = 16r^2s^2(r-s)^2$, $p \mid \Delta$. Over $\mathbb{F}_p$, $\tilde{E}$ has the form $y^2 = x^3 - sx^2$ and thus has a singular point at $(0, 0)$. Next we examine the valuation of $b_2 = a_1^2 + 4a_2 = -4(r + s)$. If $\mathrm{ord}_p(b_2) = 0$, then E has split multiplicative reduction reduction and we are done.

Notice that $\mathrm{ord}_p(b_2) = 0$ if and only if $p \nmid s$. Thus if $(r, s) = 1$, E has multiplicative reduction.

Continue by assuming $\mathrm{ord}_p(b_2) > 0$, so $p \mid s$ (and thus $p \mid r + s$.) Then as $p^2 \mid a_6 = 0$, $p^2 \mid b_8 = -a_4^2 = -(rs)^2$, and $p^3 \mid b_6 = 0$, we are in step 6. Since $p \mid a_1, a_2$, $p^2 \mid a_3, a_4$ and $p^3 \mid a_6$, we examine $P(T) = T^3 - (r + s)/2T^2 + rs/4T \pmod p$. There are several cases: If $P(T) \equiv T^3+T^2+T \equiv T(T^2+T+1) \pmod p$, then $\mathrm{ord}_p(r) = \mathrm{ord}_p(s) = \mathrm{ord}_p(s+r) = 1$ and E has additive reduction. If $P(T) \equiv T^3+T^2 \equiv T^2(T+1) \pmod p$, then only one of $\mathrm{ord}_p(r) > 1$ or $\mathrm{ord}_p(s) > 1$ occurs and E still has additive reduction. If $P(T) \equiv T^3 + T \equiv T(T^2 + 1) \pmod p$, then $\mathrm{ord}_p(r) = \mathrm{ord}_p(s) = 1$ and $\mathrm{ord}_p(r + s) > 1$, but still, E has additive reduction. Finally, if $P(T) \equiv T^3 \pmod p$, then $\mathrm{ord}_p(r) \geq 2$ and $\mathrm{ord}_p(s) \geq 2$ and we move on to step 9. As $a_3 = a_6 = 0$ and $p^4 \mid rs$, the curve E was not in reduced form. $\square$

Now we repeat the process used for $p = 3$ and $p = 5$; we find the minimal discriminants of the isogenous curves using Vélu's formulas. Again, the Sage code is in the appendix. These are

$$\begin{aligned}
\Delta_0 &= 2^{-8}s^2r^2(r-s)^2 \\
\Delta_1 &= 2^{-4}sr(r-s)^4 \\
\Delta_2 &= 2^{-4}sr^4(-r+s) \\
\Delta_3 &= 2^{-4}s^4r(r-s)
\end{aligned}$$

where E_1, E_2, and E_3 are all 4-isogenous and factor through $E = E_0$. There are three cases to

check, $\Delta_1 = \Delta_2, \Delta_1 = \Delta_3$, and $\Delta_2 = \Delta_3$. Checking these yields the following relation:

$$r^3 = (2^4)^3(s-r)^3.$$

As r and $s-r$ are coprime integers, $s-r=1$ and the only solution is $s=17, r=16$. This solution gives us the discriminant twin pair $17a_3, 17a_4$.

Thus the only case we have left to cover is the isogeny class of 8 curves, all connected by 2-isogenies. In particular, the last case is if E and E' are 16-isogenous curves. Let $E \to A \to B \to C \to E'$ be the chain of 2-isogenies. Then we can write the discriminants of A and B in terms of C. Without loss of generality, let $t = r - s$, then we can write

$$\begin{aligned} \Delta_A &= -2^{-4}s^2r^8t^2 \\ \Delta_B &= 2^{-8}s^4r^4t^4 \\ \Delta_C &= 2^{-4}s^8r^2t^2 \end{aligned}$$

As $E \to A$ is a 2-isogeny, for each $p \mid \Delta_A$, the power to twice $p \mid \Delta_E$ must change by a multiple of 2 and similarly with $B \to E'$. Thus the only way $\Delta_E = \Delta_{E'}$ is if $\Delta_E = \Delta_B = \Delta_{E'}$, which we've already shown only happens for $17a.1$ and $17a.4$ and this isogeny class only has four curves.

6.3 Number Fields

With a bit of care, the above proofs hold for number fields as well, but we unfortunately cannot draw the same conclusions. For example, when $\ell = 5$, we see that in the parameterization, t must be a unit for a discriminant twin to occur. As the only units over $\mathbb{Q}$, are ± 1, we find our bad case and move on. Over totally real number fields we have infinite unit groups and thus we cannot draw the same conclusions. It is however, interesting to note that over $\mathbb{Q}(\sqrt{d})$, for $d = 2, 3, 5, 7, 13$ examining this parameterization for $t = u^n$ with u a generator of the unit group and $-50 \leq n \leq 50$, $n \neq 0$, does not yield any discriminant twin examples. As expected, we do get an isogeny class of at least three 5-isogenous curves exactly when $5 \mid n$, so it is not due to isogeny class structure. This leads to the following question.

Question 6.3.1. Does the 5-torsion parameterization yield infinitely many discriminant twin pairs over number fields with infinite unit group?

Further, if we examine instances of discriminant twins from the tables over $\mathbb{Q}(\sqrt{5})$ as in Bober et al. [24], we find that out of all curves up to and including norm conductor 1831, there are 1414 isogeny classes and 146 pairs of discriminant twins, 79 of which have additive reduction and 67 with multiplicative. Most interestingly, up to conjugation, we only get three new semistable isogenous discriminant twin pairs. Here is the complete list of semistable discriminant twin pairs from these tables.

Norm Conductor	Conductor	Discriminant	Curves	Isogeny Degree
$121a$	11	-11	$a1, a3$	25
$199a$	$3a+13$	$-16a-3$	$a1, a3$	9
$199b$	$-3a+16$	$16a-19$	$a1, a3$	9
$289a$	17	17	$a1, a3$	4
$361a$	19	-19	$a1, a3$	9
$369a$	$-3a+21$	$-69a+114$	$b1, b3$	4
$369b$	$3a+18$	$69a+45$	$b1, b3$	4
$1009a$	$-29a+8$	$-45a+82$	$b1, b3$	4
$1009b$	$-29a+21$	$45a+37$	$b1, b3$	4
$1369a$	37	37	$a1, a3$	9

Notice that the curves with norm conductor $121a, 289a, 361a, 1369a$ all come from curves over $\mathbb{Q}$. Further, none come from larger isogeny class structures, i.e., isogeny classes larger than those found over $\mathbb{Q}$.

Question 6.3.2. Are there infinitely many semistable isogenous discriminant twin pairs over $\mathbb{Q}(\sqrt{5})$?

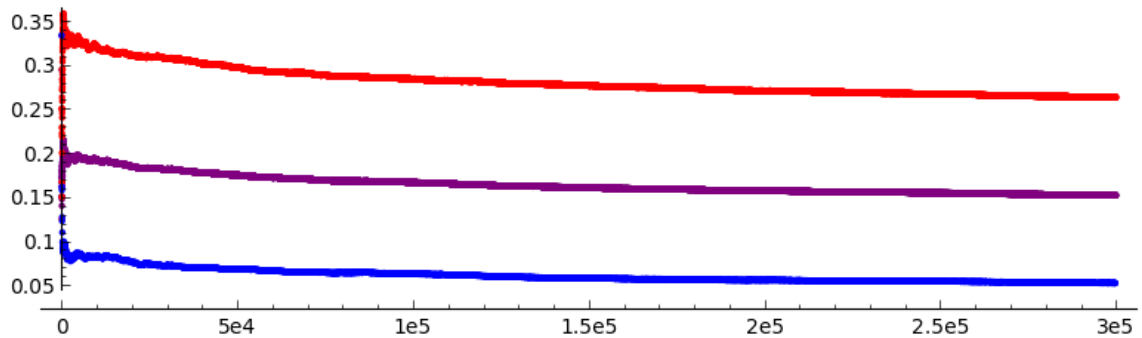
Question 6.3.3. What about over number fields in general? Or just restricting to totally real or totally imaginary number fields?

Question 6.3.4. Can we get more semistable isogenous discriminant twin pairs from number fields that allow larger isogeny classes?

$$\kappa(X) = \frac{\#\{N \leq X : \exists \text{ discriminant twins of conductor } N\}}{\#\{N \leq X : \exists E \text{ of conductor } N\}}$$

κ_{ad} non square free (top) - red, κ All Curves (middle) - purple,

κ_{ss} square free (bottom) - blue



6.4 Semistable Non-Isogenous Discriminant Twins

The data seems to support that there are in fact infinitely many semistable, non-isogenous discriminant twin pairs over $\mathbb{Q}$. We have computed all such pairs for all curves up to conductor 299998 in the Cremona Database [10]. More precisely, for small values of X, we can easily compute the following functions:

$$\kappa(X) = \frac{\#\{N \leq X : \exists \text{ discriminant twins of conductor } N\}}{\#\{N \leq X : \exists E \text{ of conductor } N\}}$$

and similarly for semistable N, κ_{ss} and N with additive reduction, κ_{ad}. In Figure 6.4 κ, κ_{ss}, and κ_{ad} have been computed for all curves in the Cremona Database up to conductor 299998.

The final values:

$\kappa(299998)$	$\kappa_{ss}(299998)$	$\kappa_{ad}(299998)$
0.15189	0.26314	0.05223

Further, we have a computation method that seems to generate large numbers of such discriminant twin pairs. This method is inspired by work of Howe and Joshi [20]. By examining non-torsion, integral, points on the family of curves of the form $y^2 = x^3 - 1728\Delta$,

for Δ square free, we can find curves with conductor $N = \Delta$. If $P = (x, y)$ is an integral point on $y^2 = x^3 - 1728\Delta$, then (x, y) correspond to the c_4, c_6 pair of a curve with discriminant Δ, and as Δ is square free, the curve has conductor $N = \Delta$. Thus if we could make a statement about some subfamily always having two non-torsion, integral points, we would be able to show there are infinitely many non-isogenous, semistable, discriminant twins.

Conjecture 6.4.1. *There are infinitely many semistable non-isogenous discriminant twin pairs.*

With the data from the Graph 6.4 we can also ask the following questions.

Question 6.4.2. Do discriminant twin pairs occur with positive density?

Question 6.4.3. Do semistable non-isogenous discriminant twin pairs occur with positive density?

BIBLIOGRAPHY

[1] Amod Agashe, Kenneth A. Ribet, and William A. Stein. The modular degree, congruence primes, and multiplicity one. In *Number theory, analysis and geometry*, pages 19–49. Springer, New York, 2012.

[2] M. Bertolini and H. Darmon. A rigid analytic Gross-Zagier formula and arithmetic applications. *Ann. of Math. (2)*, 146(1):111–147, 1997. With an appendix by Bas Edixhoven.

[3] M. Bertolini and H. Darmon. p-adic periods, p-adic L-functions, and the p-adic uniformization of Shimura curves. *Duke Math. J.*, 98(2):305–334, 1999.

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

[5] J.-F. Boutot and H. Carayol. Uniformisation p-adique des courbes de Shimura: les théorèmes de Čerednik et de Drinfel′d. *Astérisque*, (196-197):7, 45–158 (1992), 1991. Courbes modulaires et courbes de Shimura (Orsay, 1987/1988).

[6] K. Buzzard. Integral models of certain Shimura curves. *Duke Math. J.*, 87(3):591–612, 1997.

[7] Henri Carayol. Sur la mauvaise réduction des courbes de Shimura. *Compositio Math.*, 59(2):151–230, 1986.

[8] C. Chevalley. Une démonstration d'un théorème sur les groupes algébriques. *J. Math. Pures Appl. (9)*, 39:307–317, 1960.

[9] B. Conrad and W. Stein. Component groups of purely toric quotients. *Math. Res. Lett.*, 8(5-6):745–766, 2001.

[10] J. E. Cremona. *Algorithms for modular elliptic curves.* Cambridge University Press, Cambridge, second edition, 1997.

[11] P. Deligne and M. Rapoport. Les schémas de modules de courbes elliptiques. pages 143–316. Lecture Notes in Math., Vol. 349, 1973.

[12] G. Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.*, 73(3):349–366, 1983.

[13] N. Freitas, B. V. Le Hung, and S. Siksek. Elliptic Curves over Real Quadratic Fields are Modular. *ArXiv e-prints*, October 2013.

[14] C. F. Gauss. *Disquisitiones arithmeticae*, 1801.

[15] Lothar Gerritzen and Marius van der Put. *Schottky groups and Mumford curves*, volume 817 of *Lecture Notes in Mathematics*. Springer, Berlin, 1980.

[16] D. Goldfeld. The conjectures of Birch and Swinnerton-Dyer and the class numbers of quadratic fields. pages 219–227. Astérisque No. 41–42, 1977.

[17] J. González. On the division polynomials of elliptic curves. *Rev. R. Acad. Cienc. Exactas Fís. Nat. (Esp.)*, 94(3):377–381, 2000. Contributions to the algorithmic study of problems of arithmetic moduli (Spanish).

[18] B. Gross and D. Zagier. Points de Heegner et dérivées de fonctions *L. C. R. Acad. Sci. Paris Sér. I Math.*, 297(2):85–87, 1983.

[19] A. Grothendieck.

[20] S. Howe and K. Joshi. Elliptic curves of almost-prime conductor. *ArXiv e-prints*, January 2012.

[21] H. Jacquet and R. P. Langlands. *Automorphic forms on* GL(2). Lecture Notes in Mathematics, Vol. 114. Springer-Verlag, Berlin, 1970.

[22] Frazer Jarvis. Mazur's principle for totally real fields of odd degree. *Compositio Math.*, 116(1):39–79, 1999.

[23] Frazer Jarvis. Correspondences on Shimura curves and Mazur's principle at p. *Pacific J. Math.*, 213(2):267–280, 2004.

[24] Ariah Klages-Mundt Benjamin LeVeque R. Andrew Ohana Ashwath Rabindranath Paul Sharaba Jonathan Bober, Alyson Deines and William Stein. A database of elliptic curves over $\mathbb{Q}(\sqrt{5})$: a first report. *ANTS X*, 2012.

[25] M. A. Kenku. On the number of $\mathbf{Q}$-isomorphism classes of elliptic curves in each $\mathbf{Q}$-isogeny class. *J. Number Theory*, 15(2):199–202, 1982.

[26] M. Kirschmer and J. Voight. Algorithmic enumeration of ideal classes for quaternion orders. *SIAM J. Comput.*, 39(5):1714–1747, 2010.

[27] D. Kohel. Hecke module structure of quaternions. 30:177–195, 2001.

[28] Alain Kraus. Quelques remarques à propos des invariants c_4, c_6 et Δ d'une courbe elliptique. *Acta Arith.*, 54(1):75–80, 1989.

[29] Daniel Sion Kubert. Universal bounds on the torsion of elliptic curves. *Compositio Math.*, 38(1):121–128, 1979.

[30] Akira Kurihara. On some examples of equations defining Shimura curves and the Mumford uniformization. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.*, 25(3):277–300, 1979.

[31] The LMFDB Collaboration. The l-functions and modular forms database. `http://www.lmfdb.org`, 2013. [Online; accessed 16 September 2013].

[32] B. Mazur. Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.*, (47):33–186 (1978), 1977.

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

[34] A. P. Ogg. Elliptic curves and wild ramification. *Amer. J. Math.*, 89:1–21, 1967.

[35] M. Papikian. On component groups of Jacobians of Drinfeld modular curves. *Ann. Inst. Fourier (Grenoble)*, 54(7):2163–2199 (2005), 2004.

[36] M. Papikian and J. Rabinoff. Optimal quotients of Jacobians with toric reduction and component groups. *ArXiv e-prints*, December 2012.

[37] A. Pizer. An algorithm for computing modular forms on $\Gamma_0(N)$. *J. Algebra*, 64(2):340–390, 1980.

[38] Ali Rajaei. On the levels of mod l Hilbert modular forms. *J. Reine Angew. Math.*, 537:33–65, 2001.

[39] K. Ribet. Letter about component groups of elliptic curves, 2001. arXiv:math.AG/0105124v1.

[40] K. A. Ribet. On modular representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ arising from modular forms. *Invent. Math.*, 100(2):431–476, 1990.

[41] Kenneth A. Ribet and Shuzo Takahashi. Parametrizations of elliptic curves by Shimura curves and by classical modular curves. *Proc. Nat. Acad. Sci. U.S.A.*, 94(21):11110–11114, 1997. Elliptic curves and modular forms (Washington, DC, 1996).

[42] Takeshi Saito. Conductor, discriminant, and the Noether formula of arithmetic surfaces. *Duke Math. J.*, 57(1):151–173, 1988.

[43] Goro Shimura. Construction of class fields and zeta functions of algebraic curves. *Ann. of Math. (2)*, 85:58–159, 1967.

[44] Goro Shimura. *Introduction to the arithmetic theory of automorphic functions*. Publications of the Mathematical Society of Japan, No. 11. Iwanami Shoten, Publishers, Tokyo; Princeton University Press, Princeton, N.J., 1971. Kanô Memorial Lectures, No. 1.

[45] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[46] W. Stein. Explicit approaches to modular abelian varieties. *PhD thesis, University of California, Berkeley*, 2000.

[47] William Stein and Mark Watkins. Modular parametrizations of Neumann-Setzer elliptic curves. *Int. Math. Res. Not.*, (27):1395–1405, 2004.

[48] W. A. Stein et al. *Sage Mathematics Software (Version 6.2.beta1)*. The Sage Development Team, 2014. `http://www.sagemath.org`.

[49] Lucien Szpiro. Small points and torsion points. In *The Lefschetz centennial conference, Part I (Mexico City, 1984)*, volume 58 of *Contemp. Math.*, pages 251–260. Amer. Math. Soc., Providence, RI, 1986.

[50] S. Takahashi. Degrees of parametrizations of elliptic curves by shimura curves and by classical modular curves. *PhD thesis, University of California, Berkeley*, 1998.

[51] S. Takahashi. Degrees of parametrizations of elliptic curves by Shimura curves. *J. Number Theory*, 90(1):74–88, 2001.

[52] R. Taylor and A. Wiles. Ring-theoretic properties of certain Hecke algebras. *Ann. of Math. (2)*, 141(3):553–572, 1995.

[53] E. Ullmo. Sur la constante de Hida des courbes modulaires et des courbes de Shimura. *J. Théor. Nombres Bordeaux*, 13(1):325–337, 2001. 21st Journées Arithmétiques (Rome, 2001).

[54] Marie-France Vignéras. *Arithmétique des algèbres de quaternions*, volume 800 of *Lecture Notes in Mathematics*. Springer, Berlin, 1980.

[55] John Voight and John Willis. Computing power series expansions of modular forms. In Gebhard BâĹŽâĹĆckle and Gabor Wiese, editors, *Computations with Modular Forms*, volume 6 of *Contributions in Mathematical and Computational Sciences*, pages 331–361. Springer International Publishing, 2014.

[56] M. Watkins. Computing the modular degree of an elliptic curve. *Experiment. Math.*, 11(4):487–502 (2003), 2002.

[57] A. Wiles. Modular elliptic curves and Fermat's last theorem. *Ann. of Math. (2)*, 141(3):443–551, 1995.

[58] D. Zagier. Modular parametrizations of elliptic curves. *Canad. Math. Bull.*, 28(3):372–384, 1985.

[59] S. Zhang. Heights of Heegner points on Shimura curves. *Ann. of Math. (2)*, 153(1):27–147, 2001.

Appendix A

CODE

A.1 Shimura Degrees

All of the Shimura Degree code is in Magma [4]. It requires Magma V2.20-6. Specifically, the Shimura degree code for elliptic curves over $\mathbb{Q}$ A.1.1 requires Magma V2.20-6. The number field code A.1.3 also works on older versions such as Magma V2.18-6. The D-new code A.1.2 is in Sage [48]. It works with Sage 6.0 or higher. It should work with much older versions of Sage as well, but I have not tested this.

A.1.1 $\mathbb{Q}$ Shimura Degrees

```
function pConjugate(O,Ip)
    Opp, phi, mpp := pMatrixRing(O, Ip);
    p:=Generator(Ip);
    alphapp := Opp![[0,1],[mpp(p),0]];
    I := rideal<O | [alphappphi,p]>;
    Oc := LeftOrder(I);
    return Oc;
end function;

function RightIdealClass(I,RIC)
    /*
    Given a quaternion ideal over an order O
    this returns the ideal class of O that
    contains I
    */
    O:=RightOrder(I);
    RIC:=RightIdealClasses(O);
```

```
    for RI in RIC do
        if IsIsomorphic(RI,I) then
            return RI,Index(RIC,RI);
        end if;
    end for;
end function;

function Alpha(I,O,RIC)
    /*
    This is the map beta:CL(Om) -->CL(O)
    */
    I := rideal<O | [bas:bas in Basis(I)]>;
    return RightIdealClass(I,RIC);
end function;

function AlphaBetaKernel(D,M,p)
    ZZ:=Integers();
    Zp:=ideal<ZZ|p>;
    Q:=QuaternionAlgebra(D);
    QM:=MaximalOrder(Q);
    OM:=Order(QM,M);
    OMg:=pConjugate(OM,Zp);
    OMp:= OM meet OMg;
    Opp, phi, mpp := pMatrixRing(OM, Zp);
    p:=Generator(Zp);
    alphapp := Opp![[0,1],[mpp(p),0]];
    alphainv:=alphapp^(-1);
    B:=BrandtModule(OMp: ComputeGrams:=false);
    Mat:=[];
    BLI:=B`LeftIdeals;
    BRI:=[Conjugate(BI):BI in BLI];
    for RI in BRI do
        AI,ai:= Alpha(RI,OM,BRI);
        J:=rideal<OMg|[alphainvphi*b: b in Basis(RI)]>;
        BI,bi:= RightIdealClass(J,BRI);
        v:=[0:i in [1..#BRI]];
```

```
        w:=[0:i in [1..#BRI]];
        v[ai] := 1;
        w[bi]:= 1;
        Append(~Mat,v cat w);
    end for;
    ABMat:=Matrix(Mat);
    ABBas:=Basis(Kernel(ABMat));
    BBas:=[B!Eltseq(ab): ab in ABBas];
    return BBas,B,CuspidalSubspace(B);
end function;

function CurveKernel(E,XBig,N)
    f:=ModularForm(E);
    NewBas:=XBig;
    coefs:=[[i,Coefficient(f,i)]: i in PrimesUpTo(35)| N mod i ne 0];
    HeckeOps:=[HeckeOperator(XBig,c[1])-c[2]: c in coefs];
    for T in HeckeOps do
        try
            Ker:=Kernel(T);
            KerBas:=[XBig!Eltseq(ker): ker in Basis(Ker)];
            if #KerBas eq 1 then
                return KerBas[1];
            end if;
        catch e
            print "In Try";
        end try;
    end for;
    return "Increase Hecke Operator Bound!";
end function;
```

A.1.2 D-new code

```
def D_new_degree(J,D,E):

    Jnew = J
    for p in D.factor():
```

```
        Jpnew = sum([jnew for jnew in J.new_subvariety(p[0]).decomposition()
            if jnew != E])
        if Jpnew == 0:
            Jnew = Jnew.zero_subvariety()
            break
        Jnew  = Jpnew.intersection(Jnew)[1]
    return Jnew.dimension(), sqrt(Jnew.intersection(E)[0].order())

def NewDegs(N):
    J = J0(N)
    if J.dimension() > 0:
        print "Conductor", N
        Jnew = J.new_subvariety()
        Dc = [E for E in Jnew.decomposition() if E.dimension() == 1]
        Dlist = N.divisors()
        for E in Dc:
            print E.label()
            for D in Dlist:
                dd, dnew = D_new_degree(J,D,E)
                print "    ","D = ", D,"Dim=", dd, "Dnew = ", dnew
            Jnot = sum([jj for jj in J.decomposition() if jj != E])
            if Jnot == 0:
                print "    ", "Modular Degree", 1
            else:
                print "    ", "Modular Degree", sqrt(Jnot.intersection(E)
                    [0].order())
    return None

def D_new_modsym(J, D):
    Sym = J.modular_symbols(sign=1)
    for p in D.factor():
        Sym = Sym.intersection(Sym.new_submodule(p[0]))
    return Sym

def D_new_congruence(J,D,E):
    S = D_new_modsym(J, D)
```

```
    Eperp = E.modular_symbols(sign=1).complement()
    I = Eperp.intersection(S)
    return I.congruence_number(E.modular_symbols(sign=1))

def NewCongs(N):
    J = J0(N)
    if J.dimension() > 0:
        print "Conductor", N
        Jnew = J.new_subvariety()
        Dc = [E for E in Jnew.decomposition() if E.dimension() == 1]
        Dlist = N.divisors()
        for E in Dc:
            print E.label()
            for D in Dlist:
                cong = D_new_congruence(J,D,E)
                print "    ","D = ", D, "Dcong = ", cong
    return None
```

A.1.3 $\mathbb{Q}(\sqrt{5})$ *code*

```
function pConjugate(O,Ip)
    /*
    This is the number field version.
    Given an Eichler order O of a quaternion algebra,
    this returns an adelically conjugate Eichler order
    with the same level.
    */
    Opp, phi, mpp := pMatrixRing(O, Ip);
    p:=UniformizingElement(Ip);
    alphapp := Opp![[0,1],[mpp(p),0]];
    I := rideal<O | [alphappphi,p]>;
    Oc := LeftOrder(I);
    return Oc,alphapp,phi;
end function;

function RightIdealClass(I,RIC)
    /*
```

```
    Given a quaternion ideal over an order O
    this returns the ideal class of O that
    contains I
    */
    O:=RightOrder(I);
    for RI in RIC do
        try
            if IsIsomorphic(RI,I) then
                return RI,Index(RIC,RI);
            end if;
        catch e
            print "In catch handler";
            //error "Error calling procedure with parameter: ", e`Object;
        end try;
    end for;
end function;

function Alpha(I,O,RIC)
    /*
    Input:
        I - an ideal of Om
        O - the order we are mapping to
        RIC - the right ideal classes of O

    This is the map alpha:CL(Om) -->CL(O)
    It sends the ideal I to an ideal class of
    the order O.
    */
    I := rideal<O | Generators(I)>;
    return RightIdealClass(I,RIC);
end function;

function AlphaBetaKernel(F,D,M,Ip)
    /*
    Input:
        F - number field
```

```
        D,M,p - ideals in F.
    Number Field AlphaBetaKernel
    Let H be a definite quaternion algebra of discriminant D.
    This finds the kernel in X(H,O(Mp)) of the maps
    alpha,beta:X(H,O(Mp)) --> X(H,O(M))
    which can be used to compute character groups.
    */
    R:=RealPlaces(F);
    if D eq 1 then
        Q:=QuaternionAlgebra(R);
    else
        Q:=QuaternionAlgebra(D,R);
    end if;
    QM:=MaximalOrder(Q);
    //The first Eichler Order
    //Level M
    OM:=Order(QM,M);

    //Construct p-conjugate order
    //keep the map to use with the beta map
    OMg,alphapp,phi:=pConjugate(OM,Ip);

    //order p-conjugate to OM
    //intersection of OM and OMg
    //an Eichler order of level Mp
    OMp:= OM meet OMg;
    alphainv:=alphapp^(-1);
    print "Norm O", Norm(Discriminant(OM));
    print "Norm Op", Norm(Discriminant(OMp));


    Mat:=[];
    RIM:=RightIdealClasses(OM);
    RIMg:=RightIdealClasses(OMg);
    RIp:=RightIdealClasses(OMp);
    print "Middle Space:", #RIp-1;
```

```
    print "Right Space:", #RIM-1, #RIMg-1, #RIM+#RIMg-2;
    for RI in RIp do
        //alpha is easy!
        AI,ai:= Alpha(RI,OM,RIM);
        //print "alpha is done";
        //beta is hard.
        J:=rideal<OMg|[alphainvphi*b: b in Generators(RI)]>;
        //print "J computed okay?", RightOrder(J) eq OMg;

        BI,bi:= RightIdealClass(J,RIMg);
        v:=[0:i in [1..#RIp]];
        w:=[0:i in [1..#RIp]];
        v[ai] := 1;
        w[bi]:= 1;
        Append(~Mat,v cat w);
    end for;
    ABMat:=Matrix(Mat);
    ABBas:=Basis(Kernel(ABMat));
    AutoNums := [ #Units(LeftOrder(I)) : I in RIp ];
    print AutoNums;
    return ABBas;
    //return "done";

end function;
```

A.2 Discriminant Twins

All of the Discriminant Twins code is in Sage [48]. It works with Sage 6.0 or higher. It should work with much older versions of Sage as well, but I have not tested this.

A.2.1 5-isogenies

```
R.<t>=QQ[]
Q = R.fraction_field()
E = EllipticCurve([(1-t),-t,-t,0,0])
print "Original Discriminant"
```

```
print E.discriminant().factor()

def Point(E,xcoord,ycoord):
    P = E.defining_polynomial()
    if P(x = xcoord,y = ycoord,z=1) == 0:
        pass
    else:
        print P(x = xcoord,y = ycoord,z=1)
        raise ValueError, "Point must lie on curve"
    return [xcoord,ycoord]

def add_points(E,P,Q):
    """
    INPUT: curve and two points
    OUTPUT: lambda and nu from silverman
    """
    x1,y1 = P
    x2,y2 = Q
    a1 = E.a1()
    a2 = E.a2()
    a3 = E.a3()
    a4 = E.a4()
    a6 = E.a6()
    if x1 != x2:
        lam = (y2-y1)/(x2-x1)
        nu = (y1*x2-y2*x1)/(x2-x1)
    if x1 == x2:
        lam = (3*x1^2+2*a2*x1+a4-a1*y1)/(2*y1+a1*x1+a3)
        nu = (-x1^3+a4*x1+2*a6-a3*y1)/(2*y1+a1*x1+a3)
    x3 = lam^2+a1*lam-a2-x1-x2
    y3 = -(lam+a1)*x3-nu-a3
    return Point(E,x3,y3)

def neg_point(E,P):
    """
    INPUT: a curve and a point
```

```
    """
    x0,y0 = P
    x1 = x0
    y1 = -y0-E.a1()*x0-E.a3()
    return Point(E,x1,y1)
P1 = Point(E,0,0)
#P2 = point at infinity
P3 = Point(E,t,0)
P4 = Point(E,0,t)
P5 = Point(E,t,t^2)

u = 1
r = -(E.a1()^2+4*E.a2())/12
s = -E.a1()/2
tt = -(E.a3()+r*E.a1())/2

EAB = E.change_weierstrass_model([u,r,s,tt])

def Pnew(Enew,P):
    x0,y0 = P
    xnew = x0-r
    ynew = y0-s*x0+s*r-tt
    return Point(Enew,xnew,ynew)

def t_tilde(EABform,Q):
    x0,y0 = Q
    A = EABform.a4()
    return 3*x0^2+A
def u_tilde(EABform,Q):
    x0,y0 = Q
    A = EABform.a4()
    B = EABform.a6()
    return 2*(x0^3+A*x0+B)

A = EAB.a4()
B = EAB.a6()
```

```
t_total = 0
w_total = 0
C = [Pn1,Pn3,Pn4,Pn5]
for Q in C:
    t_total = t_total + t_tilde(EAB,Q)
    w_total = w_total + (u_tilde(EAB,Q)+Q[0]*t_tilde(EAB,Q))
AC = A - 5*t_total
BC = B - 7*w_total
EC = EllipticCurve([0,0,0,AC,BC])
print "5-isogenous Discriminant"
print EC.discriminant().factor()
```

A.2.2 3-isogenies

```
R.<A1,A3>=QQ[]
Q = R.fraction_field()
E = EllipticCurve([A1,0,A3,0,0]);
print "Original Discriminant,"
print E.discriminant().factor()

def Point(E,xcoord,ycoord):
    P = E.defining_polynomial()
    if P(x = xcoord,y = ycoord,z=1) == 0:
        pass
    else:
        print P(x = xcoord,y = ycoord,z=1)
        raise ValueError, "Point must lie on curve"
    return [xcoord,ycoord]

def add_points(E,P,Q):
    """
    INPUT: curve and two points
    OUTPUT: lambda and nu from silverman
    """
    x1,y1 = P
    x2,y2 = Q
    a1 = E.a1()
```

```
    a2 = E.a2()
    a3 = E.a3()
    a4 = E.a4()
    a6 = E.a6()
    if x1 != x2:
        lam = (y2-y1)/(x2-x1)
        nu = (y1*x2-y2*x1)/(x2-x1)
    if x1 == x2:
        lam = (3*x1^2+2*a2*x1+a4-a1*y1)/(2*y1+a1*x1+a3)
        nu = (-x1^3+a4*x1+2*a6-a3*y1)/(2*y1+a1*x1+a3)
    x3 = lam^2+a1*lam-a2-x1-x2
    y3 = -(lam+a1)*x3-nu-a3
    return Point(E,x3,y3)

def neg_point(E,P):
    """
    INPUT: a curve and a point
    """
    x0,y0 = P
    x1 = x0
    y1 = -y0-E.a1()*x0-E.a3()
    return Point(E,x1,y1)

P1 = Point(E,0,0)
P2 = add_points(E,P1,P1)

u = 1
r = -(E.a1()^2+4*E.a2())/12
s = -E.a1()/2
t = -(E.a3()+r*E.a1())/2

EAB = E.change_weierstrass_model([u,r,s,t])

def Pnew(Enew,P):
    x0,y0 = P
    xnew = x0-r
```

```
    ynew = y0-s*x0+s*r-t
    return Point(Enew,xnew,ynew)

Pn1 = Pnew(EAB,P1)
Pn2 = Pnew(EAB,P2)

def t_tilde(EABform,Q):
    x0,y0 = Q
    A = EABform.a4()
    return 3*x0^2+A
def u_tilde(EABform,Q):
    x0,y0 = Q
    A = EABform.a4()
    B = EABform.a6()
    return 2*(x0^3+A*x0+B)

A = EAB.a4()
B = EAB.a6()
t_total = 0
w_total = 0
C = [Pn1,Pn2]
for Q in C:
    t_total = t_total + t_tilde(EAB,Q)
    w_total = w_total + (u_tilde(EAB,Q)+Q[0]*t_tilde(EAB,Q))
AC = A - 5*t_total
BC = B - 7*w_total

EC = EllipticCurve([0,0,0,AC,BC])

r = A1^2/12
s = A1/2
t = -9*A3/2

EC1 = EC.change_weierstrass_model([1,r,s,t])
print "3-isogenous discriminant"
print EC1.discriminant().factor()
```

A.2.3 2-isogenies

```
R.<r,s,u>=QQ[]
Q = R.fraction_field()
E = EllipticCurve([0,-(r+s),0,r*s,0])

def Point(E,xcoord,ycoord):
    P = E.defining_polynomial()
    if P(x = xcoord,y = ycoord,z=1) == 0:
        pass
    else:
        print P(x = xcoord,y = ycoord,z=1)
        raise ValueError, "Point must lie on curve"
    return [xcoord,ycoord]

def add_points(E,P,Q):
    """
    INPUT: curve and two points
    OUTPUT: lambda and nu from silverman
    """
    x1,y1 = P
    x2,y2 = Q
    a1 = E.a1()
    a2 = E.a2()
    a3 = E.a3()
    a4 = E.a4()
    a6 = E.a6()
    if x1 != x2:
        lam = (y2-y1)/(x2-x1)
        nu = (y1*x2-y2*x1)/(x2-x1)
    if x1 == x2:
        lam = (3*x1^2+2*a2*x1+a4-a1*y1)/(2*y1+a1*x1+a3)
        nu = (-x1^3+a4*x1+2*a6-a3*y1)/(2*y1+a1*x1+a3)
    x3 = lam^2+a1*lam-a2-x1-x2
    y3 = -(lam+a1)*x3-nu-a3
    return Point(E,x3,y3)

```

```
def neg_point(E,P):
    """
    INPUT: a curve and a point
    """
    x0,y0 = P
    x1 = x0
    y1 = -y0-E.a1()*x0-E.a3()
    return Point(E,x1,y1)

P1 = Point(E,0,0)
P2 = Point(E,s,0)
P3 = Point(E,r,0)

uu = 1
rr = -(E.a1()^2+4*E.a2())/12
ss = -E.a1()/2
tt = -(E.a3()+rr*E.a1())/2

EAB = E.change_weierstrass_model([uu,rr,ss,tt])

def Pnew(Enew,P):
    x0,y0 = P
    xnew = x0-rr
    ynew = y0-ss*x0+ss*rr-tt
    return Point(Enew,xnew,ynew)

Pn1 = Pnew(EAB,P1)
Pn2 = Pnew(EAB,P2)
Pn3 = Pnew(EAB,P3)

def t_tilde(EABform,Q):
    x0,y0 = Q
    A = EABform.a4()
    return 3*x0^2+A
def u_tilde(EABform,Q):
    x0,y0 = Q
```

```
    A = EABform.a4()
    B = EABform.a6()
    return 2*(x0^3+A*x0+B)

A = EAB.a4()
B = EAB.a6()
t_total = 0
w_total = 0
C1 = [Pn1]
for Q in C1:
    t_total = t_total + t_tilde(EAB,Q)
    w_total = w_total + (u_tilde(EAB,Q)+Q[0]*t_tilde(EAB,Q))
AC1 = A - 5*t_total
BC1 = B - 7*w_total
EC1 = EllipticCurve([0,0,0,AC1,BC1])

t_total = 0
w_total = 0
C2 = [Pn2]
for Q in C2:
    t_total = t_total + t_tilde(EAB,Q)
    w_total = w_total + (u_tilde(EAB,Q)+Q[0]*t_tilde(EAB,Q))
AC2 = A - 5*t_total
BC2 = B - 7*w_total
EC2 = EllipticCurve([0,0,0,AC2,BC2])

t_total = 0
w_total = 0
C3 = [Pn3]
for Q in C3:
    t_total = t_total + t_tilde(EAB,Q)
    w_total = w_total + (u_tilde(EAB,Q)+Q[0]*t_tilde(EAB,Q))
AC3 = A - 5*t_total
BC3 = B - 7*w_total
EC3 = EllipticCurve([0,0,0,AC3,BC3])

```

```
print "Discriminants"
print 'D0', E.discriminant().factor()
print 'D1', EC1.discriminant().factor()
print 'D2', EC2.discriminant().factor()
print 'D3', EC3.discriminant().factor()
```