Arithmetic of Totally Split Modular Jacobians and Enumeration of Isogeny Classes of Prime Level Simple Modular Abelian Varieties

Kevin Lui

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

Doctor of Philosophy

University of Washington

2019

Reading Committee:

William Stein, Chair

Ralph Greenberg

Bianca Viray

Program Authorized to Offer Degree:
Mathematics

University of Washington

Abstract

Arithmetic of Totally Split Modular Jacobians and Enumeration of Isogeny Classes of Prime Level Simple Modular Abelian Varieties

Kevin Lui

Chair of the Supervisory Committee:
Professor William Stein
Mathematics

In this thesis, we aim to give algorithms for computing two key invariants of the modular Jacobians $J_0(N)$.

We first give methods for computing the rational torsion order of rank-0 Jacobians $J_0(N)$ that are isogenous to a product of elliptic curves. We call these the rank-0 totally split Jacobians. The rational torsion is an important invariant of the Generalized BSD conjecture so being able to compute the rational torsion order will provide evidence towards this conjecture. We will provably enumerate the set of totally split $J_0(N)$, give an algorithm for computing the rational torsion subgroup, and later give techniques for computing the rational torsion order for rank-0 totally split Jacobians $J_0(N)$.

Next we will give an algorithm for computing the rational odd-isogeny class of a simple abelian subvariety A of $J_0(N)$ for prime N, under mild conditions. This is done by showing every $G_{\mathbb{Q}}$-submodule of $A(\overline{\mathbb{Q}})_{\text{odd}}$ is a Hecke module and then attacking the non-Eisenstein and Eisenstein isogenies separately.

TABLE OF CONTENTS

LIST OF TABLES

Table Number Page

ACKNOWLEDGMENTS

I would like to first and foremost my advisor William Stein for helping me through this thesis. I have learned so much by working with him. This thesis would not be possible without him.

Next I would like to thank my officemates in Padelford C-8D for making every day of graduate school a fun experience.

Lastly, I would like to thank my family for their love and support.

DEDICATION

to my mom and dad

PREFACE

I've have written this thesis with some accessibility in mind. In particular, my goal was to write a thesis assessable to myself as a second graduate student. I will assume the reader has taken a graduate level algebra sequence and have had some exposure to complex abelian varieties and modular forms. For learning about complex abelian varieties, I recommend the article of Rosen in [CS86], and for learning modular forms, I recommend the combination of the books by Stein [Ste07] and, Diamond and Shurman [DS05].

After reading the introduction, an interested expert can skip to Chapters 4 and 5, and back-reference as needed.

Chapter 3 has been largely taken from the source code of Sage [Sag19] and a forthcoming paper by Hao Chen, myself, and William Stein. For the most part, the algorithms were created and implemented into Sage and Magma by William Stein. This chapter is included in this thesis so I am not relying on currently unpublished work.

The code used to generate the data of this thesis was done in Sage [Sag19] will be available here `kevinlui.org/thesis`.

Chapter 1
INTRODUCTION

Let $X_0(N)$ be the modular curve whose non-cuspidal points parameterize complex elliptic curve with some additional N-torsion data. Let $J_0(N) = \mathrm{Jac}(X_0(N))$ be the Jacobian variety of $X_0(N)$. The study of $J_0(N)$ has yielded many deep results in arithmetic geometry. Two notable examples are:

- Mazur [Maz77] bounds the possible group structures for the rational torsion subgroup of an elliptic curve over $\mathbb{Q}$ by understanding the rational torsion subgroup of $J_0(N)$.

- The Modularity Theorem for elliptic curves over $\mathbb{Q}$ states that for every elliptic curve E, there is a surjective map $J_0(N) \to E$, where N is the conductor of E. As a step towards proving Fermat's Last Theorem, Taylor and Wiles [Wil95][TW95] prove the Modularity Theorem for semistable stable elliptic curves. The full Modularity Theorem was later established following the completion of [BCDT01].

The goal of this thesis is to study the computational aspects of $J_0(N)$. The most interesting work will be presented in Chapter 4 and Chapter 5. But before arriving at these chapters, we will lay down some theoretical and algorithmic preliminaries in Chapter 2 and Chapter 3.

1.1 Rational torsion points

As part of his landmark paper bounding the possible group structures for the rational torsion subgroup of an elliptic curve. As a key step, Mazur proves the Ogg Conjecture:

Theorem 1.1.1 ([Maz77, Thm. 1])**.** *Let N be prime and C_N be the cuspidal subgroup of $J_0(N)$. Then*

$$J_0(N)(\mathbb{Q})_{\mathrm{tor}} = C_N(\mathbb{Q}).$$

A natural generalization is to allow N to be composite. This is the Generalized Ogg Conjecture.

Conjecture 1.1.2 (Generalized Ogg Conjecture)**.** *Let C_N be the cuspidal subgroup of $J_0(N)$. Then*

$$J_0(N)(\mathbb{Q})_{\text{tor}} = C_N(\mathbb{Q}).$$

There been some progress towards this conjecture, particularly, away from 2 and 3.

1. When N is prime, $J_0(N)(\mathbb{Q})_{\text{tor}} = C(N)(\mathbb{Q})$. [Maz77, Thm. 1]

2. When $p \geq 5$ is a prime and r a positive integer,

   $$J_0(p^r)(\mathbb{Q})[q^\infty] = C(p^r)(\mathbb{Q})[q^\infty]$$

   for any prime $q \nmid 6p$. If $r = 2$, the result holds for any prime $q \nmid 2p$. [Lin97, Thm. 4]

3. When N is a positive squarefree integer,

   $$J_0(N)(\mathbb{Q})[q^\infty] = C(N)(\mathbb{Q})[q^\infty]$$

   for $q \nmid 6$. [Oht14, Thm. 3.6.2]

4. When $p > 3$,

   $$J_0(3p)(\mathbb{Q})[3^\infty] = C(3p)(\mathbb{Q})[3^\infty]$$

   unless $p \equiv 1 \pmod 9$ and $3^{\frac{p-1}{3}} \equiv 1 \pmod 9$. [Yoo16]

5. When N is any positive integer,

   $$J_0(N)(\mathbb{Q})[q^\infty] = 0$$

   for $q \nmid 6N\pi(N)$, where $\pi(N) = \prod_{p|N}(p^2 - 1)$. [Ren18, Thm. 1.2]

The original motivation of the rational torsion subgroup project is to compute the rational torsion subgroup for $J_0(N)$ for as many N's as possible. The first $J_0(N)$ for which Sage (Version 8.7) cannot compute is $J_0(30)$ which happens to be a product of 3 elliptic curves. The author and his advisor were able to compute the rational torsion subgroup using the fact that $J_0(30)$ is totally split, the fact that rational torsion subgroups of elliptic curves can be computed, and Galois cohomology.

The goal of this project is to see how far we can push these techniques. In particular, we are able to provably enumerate the set of totally split $J_0(N)$ (Theorem 4.1.4). There are 71 nontrivial N's for which $J_0(N)$ is totally split. Of these 71 abelian varieties, there are 46 N's for which $J_0(N)$ has algebraic rank 0. We will be able to verify the Generalized Ogg Conjecture for all but 9 abelian varieties. For those 9 abelian varieties, we are able to bound the discrepancy $[J_0(N)(\mathbb{Q})_{\text{tor}} : C_N(\mathbb{Q})]$ by a power of 2.

1.2 Rational isogeny class

By Faltings' isogeny theorem, the rational isogeny class of any abelian variety is finite. We would now like to be able to enumerate the rational isogeny class of any modular abelian variety (Defintion 2.1.1) within our computational framework (Chapter 3). In particular, if A is a modular abelian variety, we wish to give a set of finite $G_{\mathbb{Q}}$-subgroups of $A(\overline{\mathbb{Q}})$, $\{M_1, \ldots, M_r\}$ such that $\{A/M_1, \ldots, A/M_r\}$ is a set of pairwise non-isomorphic abelian varieties.

The goal of enumerating the rational isogeny class of any modular abelian variety seems hopelessly difficult. We will need to take on a few hypothesis. In particular, when A is a simple abelian subvariety of $J_0(N)$ with integrally closed Hecke algebra $\mathbb{T}_A \subseteq \operatorname{End}(A)$, Frank Calegari had an idea to bound the images of isogenies supported only on the non-Eisenstein primes of odd-residue characteristic by the class group of $\mathbb{T}_A$. So we will take on these hypothesis and attempt to enumerate the odd-degree isogeny class of A when $\mathbb{T}_A$ is integrally closed. From our computational experiments, when $\mathbb{T}_A$ is integrally closed, the class group is often trivial so, in these cases, it remains the enumerate the Eisenstein isogenies. We then adapt the work of Krzysztof Klosin and Mihran Papikian to enumerate the isogenies supported on the Eisenstein primes of odd-residue characteristic.

Chapter 2

THEORETICAL PRELIMINARIES

In this chapter, we will review some theoretical preliminaries needed for future chapters.

2.1 Modular Abelian Varieties

In Chapter 5, we will discuss enumerating the isogeny class of simple abelian subvarieties of $J_0(N)$. This leads us to define a class of abelian variety containing the subquotients of $J_0(N)$.

Definition 2.1.1. Let A be an abelian variety over $\mathbb{Q}$. Then A is *modular* if there exists some N and a finite degree morphism $\varphi : A \to J_1(N)$.

Note that modularity is closed under isogenies, subvarieties, and products.

The natural quotient of $X_1(N) \to X_0(N)$ induces a finite degree map $J_0(N) \to J_1(N)$. The kernel of this map, Σ_N, is finite and is the Shimura subgroup of $J_0(N)$. Therefore, all abelian varieties isogenous to a simple subvariety of $J_0(N)$ are modular.

2.2 Old subvariety and degeneracy maps

The goal of this section is to prove Corollary 2.2.5 which gives a direct sum decomposition of certain abelian subvarieties of $J_0(N)$. This will be particularly useful for computing the rational torsion order of $J_0(N)$ as rational torsion order is multiplicative on direct sums.

2.2.1 Degeneracy Maps

Let $L \mid N$, $LM = N$, and $t_1, \ldots, t_r$ be the divisors of M in increasing order. Then, for each t_i, there are degeneracy maps relating the modular curves, forms, and Jacobians of level L and N. For ease of exposition, we will present the $\Gamma_0(N)$ case. The same arguments generalize easily to $\Gamma_1(N)$.

We give the more algebraic construction. Recall that the non-cuspidal points of $X_0(N)$ correspond to elliptic curves with some N-torsion data. The degeneracy map to $X_0(L)$ will forget some of this data. More precisely, on the non-cuspidal points

$$\begin{aligned} \delta_t : Y_0(N) &\to Y_0(L) \\ [E, G_N] &\mapsto [E/G_t, G'_L], \end{aligned} \tag{2.2.1}$$

where G_N is a cyclic subgroup of E of order N, G_t is the unique cyclic subgroup of G_N of order t, and $G'_L \subseteq G_N/G_t$ is the unique subgroup of order L. By [Har77, Ghap. 1, Prop. 6.8], δ_t extends uniquely to a map (which we give the same name). By Pic and Alb functoriality, this induces the maps $\delta_t^* : J_0(L) \to J_0(N)$, $\delta_{t*} : J_0(N) \to J_0(L)$, respectively.

2.2.2 Optimal Elliptic Curves

Let E be an elliptic curve of conductor N. By the Modularity Theorem for elliptic curves [BCDT01]. There exists a surjection $\varphi : J_0(N) \twoheadrightarrow E$. In general, $\ker \varphi$ is not connected. There does $\varphi' : J_0(N) \twoheadrightarrow E'$ with E' isogenous to E so that $\ker \varphi'$ is connected. By multiplicity one, this E' is unique in its isogeny class. This leads to the definition of optimal quotients.

Definition 2.2.1. Let J be the Jacobian of a curve. Then an abelian variety A is an *optimal quotient* of J, if there exists a surjective morphism $J \twoheadrightarrow A$ with connected kernel. Equivalently, A is an optimal quotient of J is it is the quotient of J by an abelian subvariety.

If A is an optimal quotient of J, then $A^\vee$ can be embedded as a subvariety of J. This particularly useful in the case where J is totally split because both elliptic curves and Jacobians are self-dual.

Proposition 2.2.2. *Let A be an abelian variety and J a modular Jacobian. Then A is an optimal quotient of J if and only if there exists an injection of $A^\vee$ into J.*

Suppose A is self-dual. Then A is an optimal quotient of J if and only if it is an abelian subvariety of J.

Proof. Suppose A is an optimal quotient of J. Then by dualizing the sequence of abelian varieties [LB92, Proposition 2.4.2]

$$0 \to C \to J \to A \to 0 \qquad 0 \to A^\vee \to J^\vee \to C^\vee \to 0,$$

there is an injection of $A^\vee \hookrightarrow J^\vee$.

Conversely, if $A^\vee$ injects into J. Then by the Poincarè Reducibility Theorem, the quotient of J by $A^\vee$ is again an abelian variety C. Then by dualizing the sequence of abelian varieties

$$0 \to A^\vee \to J \to C \to 0 \qquad 0 \to C^\vee \to J^\vee \to A \to 0,$$

there is a surjection of $J^\vee \cong J \twoheadrightarrow A$ with connected kernel $C^\vee$. □

In particular, if f is a newform of level N, then there is an optimal quotient A_f of $J_0(N)$ attached to f. By dualizing, we obtain an abelian subvariety $A_f^\vee \subseteq J_0(N)$. We call this the *optimal abelian subvariety* attached to f.

Definition 2.2.3. Let f be a newform of level N and A_f be the optimal quotient of $J_0(N)$ attached to f. We call $A_f^\vee \subseteq J_0(N)$, the *optimal abelian subvariety* attached to f.

Using the machinery of modular symbols, Cremona has created large databases of elliptic curves and their invariants, including the $J_0(N)$-optimal curve in each isogeny class. In this database, the curves are labeled NXT, where N is the conductor, X is the isogeny class within that conductor, and T is the isomorphism class with that isogeny class. When $T = 1$, then that curve is the $J_0(N)$-optimal curve with its isogeny class. For example, the curve $15a1$ is the $J_0(N)$-optimal curve within the isogeny class $15a$.

We will soon also be interested in $J_1(N)$-optimal elliptic curves. Though the $J_0(N)$-optimal and $J_1(N)$-optimal curves often agree, this is not always the case. We can use Algorithm 3.5.3 to determine the Weierstrass equation of the $J_1(N)$-optimal curve. Alternatively, we can use Stevens Conjecture [Ste89, Conjecture II] which states that within an isogeny class, the $J_1(N)$-optimal curve is the curve of minimal Faltings height. This conjecture is still open but some progress has been made. Stein and Watkins [SW04, §3] have proved Stevens conjecture for isogeny classes of prime conductor. Vatsal [Vat05, Thm. 1.11] has proved Stevens conjectures for isogeny classes containing an elliptic curve E such that for some prime $\ell \geq 7$, $E[\ell]$ is reducible and E is ordinary at ℓ.

2.2.3 Old subvariety

Let L be a proper divisor of N and $t_1, \ldots, t_r$ be divisors of N/L in any order. For each divisor t_i, the degeneracy maps give a finite-degree morphism $\delta^*_{t_i} : J_0(L) \to J_0(N)$. We now gather all the degeneracy maps coming from $J_0(N)$ to define

$$\Phi^N_L = \prod_{i=1}^{r} \delta^*_{t_i} : J_0(L)^r \to J_0(N).$$

The *old subvariety* of $J_0(N)$ is $\sum_{L|N} \operatorname{Im} \Phi^N_L$ and the *N/L-old subvariety* is $\operatorname{Im} \Phi^N_L$.

There is a strong relationship between $\ker \Phi^N_L$ and

$$(\Sigma_L)^r_0 = \{(x_1, \ldots, x_r) \in \Sigma^r_L : \sum x_i = 0\}.$$

Because degeneracy maps agree on the Shimura subgroup [LO91, Theorem 4], $(\Sigma_L)^r_0 \subseteq \ker \Phi^N_L$. The reverse equality was established by Ribet when M a prime coprime to L and was generalized by Ling to:

Theorem 2.2.4 ([Rib90, Prop. 1][Lin95, Thm. 3])**.** *Let L and M be relatively prime integers with M squarefree. Let*

$$\Phi^N_L = \prod_{i=1}^{r} d^*_{t_i} : J_0(L)^r \to J_0(LM)$$

be as defined above. Then

1. *If L is odd or M is prime, then $(\Sigma_L)^r_0 = \ker \Phi^N_L$.*

2. *If L is even and M is not a prime, then $[\ker \Phi^N_L : (\Sigma_L)^r_0]$ is a power of 2.*

However, when $\ker \Phi^N_L = (\Sigma_L)^r_0$, there is an useful direct sum decomposition of $\operatorname{Im} \Phi^N_L$, especially when $J_0(L)$ is an elliptic curve.

Corollary 2.2.5. *Suppose that* $\ker \Phi_L^N = (\Sigma_L)_0^r$ *and* $E = J_0(L)$ *is an elliptic curve. Then there is a* $\mathbb{Q}$*-isomorphism*

$$\operatorname{Im} \Phi_L^N \cong E \times F^{r-1},$$

where F *is the* $J_1(L)$*-optimal curve in the isogeny class of* E*.*

Proof. This follows from Proposition 2.2.6 and Proposition 2.2.2. □

This decomposition is particularly useful because the $J_0(L)$-optimal curves are identified in Cremona's table and the $J_1(L)$-optimal curves can be identified using Steven's conjecture. For example, using this decomposition, $J_0(22) = J_0(22)_{\text{old}} \cong E \times F$, where E is the $J_0(11)$-optimal curve and F is the $J_1(11)$-optimal curve (in this case, $E = J_0(11)$ and $F = J_1(11)$). So computing the BSD invariants of $J_0(22)$ amounts to computing the BSD invariants of the elliptic curves E and F.

Proposition 2.2.6. *Suppose* $\ker \Phi_L^N = (\Sigma_L)_0^r$*. Then there is a* $\mathbb{Q}$*-isomorphism*

$$\operatorname{Im} \Phi_L^N \cong J_0(L) \times \operatorname{Im}(J_0(L) \to J_1(L))^{r-1}.$$

Proof. Let e be the exponent of Σ_L. For $i = 1, \ldots, r-1$, let m_i be integers so that $m_i \equiv 1 \pmod{e}$. Define $D_i : J_0(L) \to J_0(N)$ by

$$D_i = \begin{cases} \delta_i^* & \text{if } i = 1 \\ \delta_i^* - m_i \delta_{i-1}^* & \text{if } 2 \leq i \leq r. \end{cases}$$

We first show $\operatorname{Im} \Phi_L^N = \bigoplus_{i=1}^r \operatorname{Im} D_i$.

Define $\Phi_L^N = \prod_{i=1}^r D_i : J_0(L)^r \to J_0(N)$. We have that $\Phi_L^N = \Phi_L^N \circ T$, where

$$\begin{aligned} T : J_0(L)^r &\to J_0(L)^r \\ (x_1, x_2, \ldots, x_r) &\mapsto (x_1 - m_2 x_2, x_2 - m_3 x_3, \ldots, x_{r-1} - m_r x_r, x_r). \end{aligned}$$

The matrix associated to T is consisted of 1's along the diagonal and m_i's along the super-diagonal. The determinant is 1 so

$$\sum_{i=1}^r \operatorname{Im} D_i = \operatorname{Im} \Phi_L^N.$$

The goal is to now show that this sum is direct. Let $y_1, \ldots, y_r \in J_0(L)$. Suppose

$$\Phi_L^N(y_1, \ldots, y_r) = D_1(y_1) + \cdots + D_r(y_r) = 0. \tag{2.2.2}$$

Then that $T(y_1, \ldots, y_r) \in \ker \Phi_L^N = (\Sigma_L)_0^r$. This immediately implies that $y_r \in \Sigma_L$ and then, by repeated back-substitution, $y_i \in \Sigma_L$ for $i = 1, \ldots, r$. Since $m_i \equiv 1 \pmod{e}$,

$$T(y_1, \ldots, y_r) = (y_1 - y_2, y_2 - y_3, \ldots, y_{n-1} - y_n, y_n).$$

Since $T(y_1, \ldots, y_r) \in (\Sigma_L)_0^r$,

$$(y_1 - y_2) + (y_2 - y_3) + \cdots + (y_{n-1} - y_n) + y_n = 0.$$

This implies that $y_1 = 0$ so $D_1(y_1) = 0$. Moreover, for $i = 2, \ldots, r$,

$$D_i(y_i) = \delta_{i-1}^*(-y_i) + \delta_i^*(y_i) = \Phi_L^N(0, \ldots, 0, -y_i, y_i, 0, \ldots, 0) = 0,$$

where the last equality follows from the fact $(0, \ldots, 0, -y_i, y_i, 0, \ldots, 0) \in (\Sigma_L)_0^r$. Therefore, the terms in (2.2.2) are trivial so $\sum \operatorname{Im} D_i$ is direct.

It remains to show $D_1(J_0(L)) \cong J_0(L)$ and $D_i(J_0(L)) \cong \operatorname{Im}(J_0(L) \to J_1(L))$ for $i \geq 2$. Notice that $D_1(x) = \Phi_L^N(x, 0, \ldots, 0)$ and $D_i(x) = \Phi_L^N(\ldots, -m_i x, x, \ldots)$. Since $\ker \Phi_L^N = (\Sigma_L)_0^r$, $\ker D_1 = 0$ and $\ker D_i = \Sigma_L$ for $i \geq 2$, as desired. □

2.3 Subvarieties of $J_0(N)$

In this section, we will prove that every simple abelian subvariety of $J_0(N)$ is the image of degeneracy map and discuss some interesting questions arising from this. This fact will be extensively used in the decomposition algorithms of Chapter 3

Proposition 2.3.1. *Let A be a simple abelian subvariety of $J_0(N)$. There exists a divisor L of N and a newform f of level L such that $A_f \sim A$. Let $\delta_1^*, \ldots, \delta_r^*$ be the full collection of degeneracy maps from $J_0(L)$ to $J_0(N)$. Then there exists integers $n_1, \ldots, n_r$ such that $S := \sum n_i \delta_i^*|_{A_f^\vee} : A_f^\vee \to A$ is an isogeny from $A_f^\vee$ to A. Note that S is defined over $\mathbb{Q}$.*

Proof. Let $V_f = \sum_{i=1}^r \delta_i(A_f^\vee)$ and $\Phi : (A_f^\vee)^r \to V_f$ be defined by $\Phi(x_1, \dots, x_r) = \delta_1^*(x_1) + \cdots + \delta_r^*(x_r)$. Let K_f be the Fourier coefficient field of f. Since A is an abelian subvariety of V_f, there exists $M \in \operatorname{End}(V) \otimes \mathbb{Q} \cong M_{r\times r}(\operatorname{End}(A_f^\vee) \otimes \mathbb{Q}) = M_{r\times r}(K_f)$ such that $\operatorname{Im} M = A$. Let $i : A_f^\vee \to (A_f^\vee)^r$ be the inclusion map into the first coordinate. Then there exists $U \in \operatorname{Aut}((A_f^\vee)^r) = \mathrm{GL}_r(K_f)$ such that,

$$\begin{tikzcd} A_f^\vee \arrow[r, "i"] & (A_f^\vee)^r \arrow[r, dotted, "U"] & (A_f^\vee)^r \arrow[r, "D"] & V_f \arrow[r, "M"] & A, \end{tikzcd}$$

the map $T := M \circ \Phi \circ U \circ i : A_f^\vee \to A \in \operatorname{Hom}_0(A_f, A)$ is nonzero. Since degeneracy maps are K_f-linear, there exists coefficients $a_1, \dots, a_r \in K_f$ such that $T = \sum a_i \delta_i^*$. Now there exists $b \in \mathbb{Z}^*$ such that $T' := bT \in \operatorname{Hom}(A_f^\vee, A)$ is nonzero and hence an isogeny. As complex tori, $A_f \cong \mathbb{C}^n/\Lambda_{A_f^\vee}$ and $A \cong \mathbb{C}^n/\Lambda_A$. Since $T'(\Lambda_{A_f^\vee}) \subset \Lambda_A$, $T' = \sum q_i \delta_i^*$ for $q_i \in \mathbb{Q}$. Finally, there exists $w \in \mathbb{Z}^*$ such that $S := wT' = \sum n_i \delta_i^*$ with $n_i \in \mathbb{Z}$. □

2.4 Connectedness of Hecke Algebra

Mazur [Maz77, Prop. 10.6] proves that the Hecke Algebra $\mathbb{T}$ for $J_0(N)$ with N prime is connected. This was done by showing any direct product decomposition of $J_0(N)$ with N prime contradicts the irreducibility of the θ-divisor. This was surprising to the author as 2.2.5 gives a direct sum decomposition of $J_0(22)$. In this section, we dissect Mazur's proof and give a mild generalization. Moreover, we will explain why Mazur's argument fails in the composite case.

In this section, let V_A be the sum of all abelian subvarieties of $J_0(N)$ isogenous to A. Let $V_f = V_{A_f}$.

2.4.1 General results for semistable Jacobians

We will begin with some fairly general results. So assume J is a semistable Jacobian defined over $\mathbb{Q}$ that is possibly not $J_0(N)$. By [Rib75, Corollary 1.4], isogenies, endomorphisms, and abelian subvarieties (a priori defined over $\overline{\mathbb{Q}}$) are defined over $\mathbb{Q}$. In this section, we use this fact freely and will make no reference to the field of definition.

Theorem 2.4.1. *Any Jacobian J taken with its principal polarization cannot be decomposed into a nontrivial direct sum of principally polarized abelian varieties.*

Proof. Any such decomposition will give a decomposition of the Θ-divisor attached to J which contradicts the irreducibility of the Θ-divisor [Kem73, §4(a)]. □

Lemma 2.4.2. *Suppose J decomposes nontrivially as the direct sum of abelian subvarieties $A \oplus B$. Then A must share an isogenous factor with B.*

Proof. We proceed via contradiction. Suppose A and B share no isogenous factors. Let $\lambda : J \to \hat{J}$ be the principal polarization induced by its Θ-divisor. Since A shares no isogenous factors with B, $\lambda(A) = \hat{A}$ so $\lambda|_A$ is a polarization of A. Similarly, $\lambda|_B$ is a polarization of B. This now contradicts Theorem 2.4.1. □

Lemma 2.4.3. *Let R be a ring acting faithfully on J. Let $S = \{A_1, \dots, A_k\}$ be a set of representatives of the isogeny class of subvarieties of J. Suppose that for all $A \in S$, and every idempotent $r \in R$, either $rV_A = 0$ or $rV_A = V_A$. Then* $\operatorname{Spec} R$ *is connected.*

Proof. Recall that $\operatorname{Spec} R$ is connected if and only if R contains an idempotent r different from 0 or 1. We proceed via by contradiction. Let $r \in R$ be an idempotent different from 0 or 1. Then $K = rK \oplus (1-r)K$ is a decomposition of K into subvarieties. Moreover, this decomposition is nontrivial because R acts faithfully.

Let $S_1 = \{A \in S : rV_A = V_A\}$ and $S_2 = \{A \in S : (1-r)V_A = V_A\}$. Observe that r and $1-r$ kill every element of S_2 and S_1, respectively, so $S = S_1 \sqcup S_2$. We can rewrite the previous decomposition as

$$J = rJ \oplus (1-r)J = \left(\sum_{A \in S_1} V_A \right) \oplus \left(\sum_{A \in S_2} V_A \right).$$

The big summands share no isogenous factors which contradicts Lemma 2.4.2. □

2.4.2 Application to $J_0(N)$

The goal now is to apply Lemma 2.4.3 to the case of semistable J and subrings of the Hecke algebra $\mathbb{T}$. Recall that the action of the Hecke algebra on J is faithful.

Proposition 2.4.4. *Suppose that $J = J_{\mathrm{new}}$. Then* $\operatorname{Spec} \mathbb{T}$ *is connected.*

Proof. When all subvarieties are new, they appear with multiplicity 1 so the conditions of Lemma 2.4.3 are automatic. □

Proposition 2.4.5. *Suppose* $\mathbb{T}'$ *is the anemic Hecke algebra for J. Then* $\operatorname{Spec} \mathbb{T}'$ *is connected.*

Proof. By Lemma 2.4.3, it suffices to show that for any newform f, and $r \in \mathbb{T}'$, $rV_{A_f} = V_{A_f}$ or $rV_{A_f} = 0$. Fix a newform f of level L and $r \in \mathbb{T}'$. Let s be the number of divisors of N/L. We now abuse notation by overloading T_ℓ and r as operators on $A_f^\vee$, $(A_f^\vee)^s$, and J. Following the notation of 2.2.3, let $\Phi_f = (\Phi_L^N)|_{(A_f^\vee)^s} : (A_f^v ee)^s \to J_0(N)$.

In the Formulaire section of [Rib91b], for $\ell \nmid N$, $T_\ell \circ \phi = \phi \circ T_\ell$ when N is prime. However, this is also true with N squarefree since T_ℓ commutes with the pushforward and pullback of any degeneracy map δ_d^* with $d \mid N$. So for any prime $\ell \nmid N$,

$$T_\ell(\Phi_f(x_1, \ldots, x_s)) = \Phi_f(T_\ell(x_1), \ldots, T_\ell(x_s)).$$

It follows that

$$r(\Phi_f(x_1, \ldots, x_s)) = \Phi_f(rx_1, \ldots, rx_s).$$

Therefore,

$$rV_f = r(\Phi_f(A_f^\vee)) = \Phi_f(rA_f^\vee, \ldots, rA_f^\vee)$$

but $A_f^\vee$ is simple so either $rA_f^\vee = A_f^\vee$ or $rA_f^\vee = 0$. Therefore, by Lemma 2.4.3, $\operatorname{Spec} \mathbb{T}'$ is connected. □

Example 2.4.6. When N is prime, the argument Mazur [Maz77, Prop. 10.6] gives is essentially the same as Proposition 2.4.4. We see that this fails for $J = J_0(22)$ since $J = d_1(J_0(11)) + d_2(J_0(11))$ so the factors appear with multiplicity greater than 1. So one of the key difference is the multiplicities in which the simple factors appear.

Using Sage, we can show that the Hecke algebra of $J_0(22)$ is isomorphic to $\mathbb{Z}[i]$ and is thus connected. On the other hand, by 2.2.5, $J_0(22)$ is the direct product of elliptic curves so the endomorphism ring is not connected.

Chapter 3

ALGORITHMS FOR MODULAR ABELIAN VARIETIES

In this chapter, we will review algorithms on modular abelian varieties. For the most part, the goal is to reduce the computation problems to linear algebra on modular symbol spaces.

3.1 Defining Data

We begin by giving an explicit description of modular abelian varieties that is suitable for linear algebraic computations. We represent modular abelian varieties explicitly as follows. Let A be a modular abelian variety and $\varphi : A \to J$ a finite degree morphism. Let B be the image of A in J. By dualizing, there is an isogeny B to A with kernel G such that $A \cong B/G$.

$$\begin{tikzcd}
0 \arrow[r] & G \arrow[r] & B \arrow[r] \arrow[dr] & A \arrow[r] \arrow[d, "\varphi"] & 0 \\
 & & & J &
\end{tikzcd}$$

So we can represent any modular abelian variety J by giving $G \subseteq B \subseteq J$ all defined over $\mathbb{Q}$.

- We will represent J by giving a modular symbol basis for $H_1(J, \mathbb{Z})$ and $H_1(J, \mathbb{Q}) = H_1(J, \mathbb{Z}) \otimes \mathbb{Q}$ (Section 3.2).

- We will represent B as an abelian subvariety of J as follows. The inclusion of $B \subseteq J$ induces an inclusion of rational homology $V = H_1(B, \mathbb{Q})$ into $H_1(J, \mathbb{Q})$ and B is determined by this inclusion. Therefore, we specify B by a basis in reduced echelon form for the subspace V. Of course, not every subspace of $H_1(J, \mathbb{Q})$ corresponds to an abelian subvariety. In Algorithm 3.5, we give a method for determining exactly when a subspace of $H_1(J, \mathbb{Q})$ corresponds to the rational homology of an abelian subvariety.

- We will represent G as a finite subgroup of B as follows. Let $\Lambda = V \cap H_1(J, \mathbb{Z})$. Then the torsion subgroup of B is given by $B(\mathbb{C})_{\mathrm{tor}} = V/\Lambda$. Therefore, we represent G as specifying a Hermite normal form basis for the lattice L with $\Lambda \subseteq L \subseteq V$.

Therefore, we can represent any modular abelian variety A with the triplet (L, V, J), denoted $A \sim (L, V, J)$, with the properties $J = J_1(N)$ for some N, $V \subseteq H_1(J, \mathbb{Q})$, L a lattice containing $V \cap H_1(J, \mathbb{Z})$. Since the $\mathbb{Q}$-span of L is V, V can be recovered from L so A can also be specified by (L, J), denote $A \sim (L, J)$.

In this Chapter, it'll be convenient to allow other Jacobian besides $J_1(N)$. If H is congruence subgroup with $\Gamma_1(N) \subseteq H \subseteq \Gamma_0(N)$, we will denote $\mathrm{Jac}(X_H(N))$ by $J_H(N)$. For the purposes of this thesis, we usually take $J_H(N)$ to mean $J_0(N)$ or $J_1(N)$.

3.2 Modular Symbols

The computational tools presented in this chapter will be built on top of the theory of modular symbols. As mentioned in Section 3.1, modular symbols give a finite presentation of $H_1(J, \mathbb{Z})$. For instance, a $\mathbb{Z}$-basis for $H_1(J_0(15), \mathbb{Z})$ is given by the set of Manin symbols $\{(1, 8), (1, 9)\}$. For this thesis, we will not need to delve into the underlying theory of modular symbols and we will take it as a blackbox. We instead refer the reader to [Ste07, §3, §8, §9].

Similarly, the Hecke operators [Ste07, §8.3], the degeneracy maps [Ste07, §8.6], and the star involution [Ste07, §8.5] can all be defined via modular symbols and thus induce maps on modular Jacobians.

3.3 Finite Subgroups

The goal of this section is to establish some background for computing with finite subgroups of modular abelian varieties. We begin by explaining how we will present the data of a finite subgroup. We then go over some basic arithmetic performed on finite subgroup. Lastly, we will discuss computing the cuspidal and Shimura subgroup which will be used extensively in the upcoming chapters.

3.3.1 Defining Data

Let $A = (V, L, J)$ be a modular abelian variety. A finite subgroup G of A can be specified by giving a defining lattice $\mathcal{L}$ such that $\mathcal{L}/L = G$.

Given 2 finite subgroups $G_1 = (\mathcal{L}_1, A)$ and $G_2 = (\mathcal{L}_2, A)$, a map $\varphi : G_1 \to G_2$ can be given as a map on the defining lattices.

3.3.2 Intersection of Finite Subgroups

Let $G = (\mathcal{L}_1, A)$ and $H = (\mathcal{L}_2, A)$ be finite subgroups of an modular abelian variety $A = (L, V, J)$. Let $\mathcal{L}_1' = \mathcal{L}_1 + L$ and $\mathcal{L}_2' = \mathcal{L}_2 + L$. Then the intersection $G \cap H$ is the group $(\mathcal{L}, A)$, where $\mathcal{L} = \mathcal{L}_1 \cap \mathcal{L}_2 \cap V$.

3.3.3 Sums of Finite Subgroups

Let $G = (\mathcal{L}_1, A)$ and $H = (\mathcal{L}_2, A)$ be finite subgroups of $A = (L, V, J)$. The sum is given by $G + H = (\mathcal{L}_1 + \mathcal{L}_2 + L, A)$.

3.3.4 Quotients of Finite Subgroups

Let $G = (\mathcal{L}_1, A)$ and $H = (\mathcal{L}_2, A)$ be finite subgroups of $A = (L, V, J)$ with $H \subseteq G$ so $\mathcal{L}_2 \subseteq \mathcal{L}_1$. The quotient is given by $G/H = (\mathcal{L}_1/\mathcal{L}_2, A/H)$, where the computation of A/H is given in Section 3.4.4.

3.3.5 Cuspidal subgroup and rational cuspidal subgroup

In this section, we will review the computation of the cuspidal and rational cuspidal subgroups.

The cusps of $X_H(N)$ are the equivalence classes of $\mathcal{P}^1(\mathbb{Q})$ under $\Gamma_H(N)$. We will denote the elements by $[x/y]_{\Gamma_H(N)}$. The *cuspidal subgroup* C_N of $J_H(N)$ is the subgroup of degree-0 divisors $(\alpha) - (\beta)$ where α, β are cusps on J. More generally, if $A = (L, V, J)$ is a modular abelian variety that is the quotient of B by L. Then the cuspidal subgroup of A is defined to be $(C_N \cap B)/L$, where C_N is the cuspidal subgroup of $J_H(N)$.

The computational of C_N is given in [Ste00, §3.8] and we will now discuss the computation of the rational cuspidal subgroup. The Galois structure of the cuspidal subgroup is well-understood [Ste82, §1.3]. The points of the cuspidal subgroup are $\mathbb{Q}(\mu_N)$-rational under the following Galois action. There is an abstract group homomorphism $\mathrm{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q}) \cong \mathbb{Z}/N\mathbb{Z})^*$, let

$$\sigma_d \in \mathrm{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q}) : \mu_N \mapsto \mu_N^d$$

then

$$\sigma_d([x/y]_{\Gamma_1}) = [x/d'y]_{\Gamma_1},$$

where $dd' \equiv 1 \mod N$. This explicit description of the Galois action allows to us compute $C_N(\mathbb{Q}) = C_N^{\mathrm{Gal}(\mathbb{Q}(\mu)/\mathbb{Q})}$.

3.3.6 Shimura subgroup

In this section, we will explain how to compute the Shimura subgroup of $J_0(N)$. The *Shimura subgroup*, Σ_N, is the kernel of the natural map $J_0(N) \to J_1(N)$. This will be useful in Chapter 4, where Moreover, the Shimura subgroup is a Galois subgroup of $J_0(N)(\mathbb{Q})_{\mathrm{tor}}$. This fact will be used in Chapter 5 where we enumerate the rational isogeny classes.

Let Σ_N be the Shimura subgroup of $J_0(N)$ so Σ_N is the kernel of the natural map $J_0(N) \to J_1(N)$. To compute Σ_N, we will use a theorem by Ribet. We will choose some odd prime p coprime to N, by [Rib90, Prop. 1], $\Sigma_N = \ker(d_1 - d_p)$, where $\delta_1^*, \delta_p^* : J_0(N) \to J_0(pN)$ are the degeneracy maps corresponding to $1, p$. The computation of the kernel is given in 3.4.2.

3.4 Morphisms

The goal of this section is to establish some background for computing with morphisms between modular abelian varieties.

3.4.1 Defining Data

Let $A = (L, V, J)$ and $B = (L', V', J')$ be modular abelian varieties and $\varphi : A \to B$ a map of abelian varieties. Then φ induces a map on rational homology and is also completely determined by the map on rational homology. So we will defined $\varphi : A \to B$ by giving $\varphi_V : V \to V'$. For brevity, we will use φ to denote the maps on defining lattices, rational homology, and abelian varieties.

3.4.2 Kernel

Let $\varphi : A \to B$ be a morphism between modular abelian varieties $A = (L, V, J)$ and $B = (L', V', J')$. Let $V_K = \ker \varphi_V$ and $L_K = L \cap V_K$. Then the kernel K of φ is the extension of the abelian variety $K^0 = (L_K, V_K, J)$ by the finite component group $\varphi^{-1}(L')/L$.

3.4.3 Image

Let $\varphi : A \to B$ be a morphism between modular abelian varieties $A = (L, V, J)$ and $B = (L', V', J')$. The image of φ in B is the abelian subvariety $\varphi(A) = (L'', \varphi(V), J')$, where $L'' = \varphi(V) \cap L'$.

3.4.4 Quotienting by finite subgroup

Let $A = (L, V, J)$ be a modular abelian variety with a finite subgroup $G = \mathcal{L}, A)$. There is an isogeny $\varphi_G : A \to A' = (L + \mathcal{L}, V, J)$ with kernel exactly G given by the identity map on rational homology.

3.5 Decomposition and Verification of Abelian Subvarieties

3.5.1 Decomposition of $J_H(N)$

The decomposition of $J_H(N)$ is equivalent to the decomposition of the cuspidal modular symbol space of $\Gamma_H(N)$. This is discussed in [Ste07, §9].

3.5.2 Simple abelian subvarieties

In Proposition 2.3.1, we showed that every simple abelian subvariety of $J_H(N)$ is a integral linear combination of degeneracy maps. We know show that to explicit construct that map.

Algorithm 3.5.1 (Simple abelian subvarieties as image of degeneracies)**.** Given a simple abelian subvariety A of $J = J_H(N)$, this algorithm returns a newform f of level L, and an isogeny $\varphi : A_f^\vee \to A$, where $A_f^\vee \subseteq J_H(L)$ is the optimal subvariety attached to f.

1. [Decompose J] Decompose J as $J = \sum_f V_f$ 3.5.1, where the sum runs over newforms f of level dividing N and V_f is the sum of all abelian subvarieties of $J_H(N)$ isogenous to A_f.
2. [Determine newform] Find the newform f of level L so that $A \subseteq V_f$.
3. [Basis under degeneracy] Let $\{b_1, \ldots, b_r\}$ be a $\mathbb{Z}$-basis for the defining lattice of $A_f^\vee$ and $\{\delta_1, \ldots, \delta_s\}$ be the set of degeneracy maps $\delta_j : J_H(L) \to J_H(N)$.
4. [Solve system] Let x be any nonzero element of the defining lattice of $A_f^\vee$. Find $c_{ij} \in \mathbb{Q}$ such that $x = \sum c_{ij} d_j(b_i)$.
5. [Clear denominators] Let i', j' be such that $c_{i'j'} \neq 0$. Let $(n_1, \ldots, n_s) \in \mathbb{Z}^s$ be the vector obtained by clearing denominators from $(c_{i'1}, \ldots, c_{i's})$.
6. [Output] The desired isogeny is now given by $\varphi = \sum_{j=1}^s n_j \delta_j|_{A_f^\vee}$.

Let B be an abelian subvariety of J. The defining data of B is given by (L, V, J), where $V = H_1(B, \mathbb{Q})$ and $L = H_1(B, \mathbb{Z})$. Since $L = V \cap H_1(J, \mathbb{Z})$, the abelian subvariety B is completely determined by the subspace $V \subseteq H_1(J, \mathbb{Q})$, denoted $B \sim (V, J)$. As mentioned in Section 3.1, not every subspace V of $H_1(J, \mathbb{Q})$ corresponds to an abelian subvariety. The following algorithm will determine when V does correspond to an abelian subvariety. When V does correspond to an abelian subvariety B, we will also give a decomposition of B into simple abelian subvarieties.

Algorithm 3.5.2 (Decomposing and Verifying Abelian Subvarieties)**.** Let $J = J_H(N)$ and V be a subspace of $H_1(J, \mathbb{Q})$. If V corresponds to a subvariety B of J, then this algorithm will return a decomposition into simple abelian subvarieties $X_i = (V_i, J)$ of B, otherwise, this algorithm will return ‘not a subvariety’.

1. [Decompose J] Decompose J as $J = \sum_f X_f$ 3.5.1, where $X_f = (W_f, J)$ is the sum of all abelian subvarieties of J isogenous to A_f, where A_f is the optimal quotient attached to f.

2. [Intersect with V] Set $V_f = V \cap W_f$. We have that V corresponds to an abelian subvariety if and only if each V_f corresponds to an abelian subvariety. So we will explain the rest of our algorithm for just a single V_f with f a newform of level L.

3. [Build up to V_f] If V_f does correspond to an abelian subvariety B_f, then B_f must decompose as a product of simple abelian varieties isogenous to A_f. Using Proposition 2.3.1, V_f corresponds to an abelian subvariety if and only if $V_f = \sum V_i$, where each V_i is the image of an integral linear combination of $\delta_j : A_f^\vee \to J_0(N)$.

   (a) [Initiate] Set $S_0 = 0$ and $i = 0$.

   (b) [Add a V_i] Pick some $x \in V_f \setminus S_i$. Use Algorithm 3.5.1 to determine if there exists V_i such that $x \in V_i$, where V_i is the image of an integral linear combination of $\delta_j : A_f^\vee \to J_0(N)$. If not, then V_f does not correspond to an abelian subvariety and we are done.

   (c) [Done?] Set $S_{i+1} = S_i + V_i$. If $S_{i+1} = V_f$, we are done and we output $X_i = (V_i, J)$. Otherwise, increment i and return to the last step.

By applying the previous algorithm to 1-dimension abelian subvarieties, we can recover the Weierstrass equation.

Algorithm 3.5.3 (Weierstrass equation of 1-dimension abelian subvariety)**.** Given an elliptic curve subvariety E of $J_0(N)$. This algorithm returns the Weierstrass equation for E.

1. [Isogeny from optimal subvariety] Use Algorithm 3.5.1 to find a newform f of level L and an isogeny $\varphi : A_f^\vee \to E$.

2. [Weierstrass of optimal subvariety] The Cremona tables contain the Weierstrass equations for optimal subvarieties of $J_0(L)$ so in particular, for A_f.

3. [Kernel] Compute the kernel M of φ and use the complex exponential map to identify M as a set of points, M' on the Weierstrass equation for $A_f^\vee$.

4. [Velu's formulas] Output the Weierstrass equation of $A_f^\vee/M'$ using Vela's formulas.

3.6 Homomorphism spaces

Let A, B be simple modular abelian varieties. In this section, we give algorithms for computing with homomorphism spaces between A, B. This algorithms will be crucial for determining when A and B are isomorphic.

We begin by giving an algorithm for computing a $\mathbb{Z}$-basis for $\mathrm{Hom}(A, B)$. By applying this algorithm to the case when $A = B$, we obtain an algorithm for computing a $\mathbb{Z}$-basis for $\mathrm{End}(A)$. Of course, $\mathrm{End}(A)$ also has the structure of a ring that is isomorphic to an order in a number field. So we will also give an algorithm for determining an order $\mathcal{O}$ isomorphic to $\mathrm{End}(A)$, as well as maps to and from $\mathcal{O}$.

3.6.1 Extending by $\mathbb{Q}$

Let A, B be simple modular abelian varieties both of dimension d. If A is not isogenous B, then $\mathrm{Hom}(A, B) = 0$ and we are done. If A is isogenous to B, then $\mathrm{Hom}(A, B) \otimes \mathbb{Q} \cong \mathrm{End}(A) \otimes \mathbb{Q} \cong K_f$, where K_f is the Hecke eigenvalue field of a newform f associated to the simple modular abelian variety A ([Shi94, Prop 7.14]). The goal of this section is to prove Proposition 3.6.1 which allows us to recover $\mathrm{Hom}(A, B)$ from $\mathrm{Hom}(A, B) \otimes \mathbb{Q}$.

After choosing a basis for $\Lambda_1 = H_1(A, \mathbb{Z})$ and $H_1(B, \mathbb{Z})$,

$$\mathrm{Hom}(\Lambda_1, \Lambda_2) \cong (\mathbb{Z}^{(2d)})^2.$$

Proposition 3.6.1. *Let A, B be simple abelian varieties over $\mathbb{Q}$, let $\Lambda_1 = H_1(A, \mathbb{Z})$, and let $\Lambda_2 = H_1(B, \mathbb{Z})$. Embed $\mathrm{Hom}(A, B)$ into $\mathrm{Hom}(\Lambda_1, \Lambda_2)$ by the action on homology. Then*

$$\mathrm{Hom}(A, B) = (\mathrm{Hom}(A, B) \otimes \mathbb{Q}) \cap \mathrm{Hom}(\Lambda_1, \Lambda_2)$$

where the intersection takes place in $\mathrm{Hom}(A, B) \otimes \mathbb{Q}$.

We first prove a lemma that will be used in the proof of Proposition 3.6.1.

Lemma 3.6.2. *If $x \in \mathbb{C}$ is fixed by every element of $\mathrm{Aut}(\mathbb{C}/\mathbb{Q})$, then $x \in \mathbb{Q}$.*

Proof. Suppose x is transcendental, then there is a field automorphism $\sigma : \overline{\mathbb{Q}}(x) \to \overline{\mathbb{Q}}(x)$ given by $x \mapsto x + 1$. This automorphism extends to an automorphism of $\mathbb{C}$ that does not fix x. Therefore, x must be algebraic and by standard Galois theory, $x \in \mathbb{Q}$. □

Proof of Proposition 3.6.1. An element of $\mathrm{Hom}(A, B)$ is certainly an element of $\mathrm{Hom}(A, B) \otimes \mathbb{Q}$. Moreover, an element of $\mathrm{Hom}(A, B) \subseteq \mathrm{Hom}_{\mathbb{C}}(A, B)$ is a complex linear map from $\mathrm{Tan}(A_{\mathbb{C}}) \to \mathrm{Tan}(B_{\mathbb{C}})$ that sends Λ_1 to Λ_2 so it must be in $\mathrm{Hom}(\Lambda_1, \Lambda_2)$. This establishes the forward inclusion.

Conversely, suppose $\varphi \in (\mathrm{Hom}(A, B) \otimes \mathbb{Q}) \cap \mathrm{Hom}(\Lambda_1, \Lambda_2)$. Then there exists a positive integer n such that $n\varphi n\,\mathrm{Hom}(A, B)$. Hence, $n\varphi \in \mathrm{Hom}(A, B) \subseteq \mathrm{Hom}_{\mathbb{C}}(A, B)$ is a complex linear map from $\mathrm{Tan}(A_{\mathbb{C}})$ to $\mathrm{Tan}(B_{\mathbb{C}})$. Hence, $\varphi = (1/n)n\varphi$ is also a complex linear map from $\mathrm{Tan}(A_{\mathbb{C}})$ to $\mathrm{Tan}(B_{\mathbb{C}})$. By assumption, φ also maps Λ_1 to Λ_2 so $\varphi \in \mathrm{Hom}_{\mathbb{C}}(A, B)$. It remains to show that φ is defined over $\mathbb{Q}$. Let $\sigma \in \mathrm{Gal}(\mathbb{C}/\mathbb{Q})$. Since $[n]\varphi \in \mathrm{Hom}(A, B)$, $\sigma([n]\varphi) - [n]\varphi = 0$. By rearranging, $[n](\sigma\varphi - \varphi) = 0$. The image of $\sigma\varphi - \varphi$ is either infinite or 0 and the kernel of $[n]$ is finite so we must have $\sigma\varphi = \varphi$. By Lemma 3.6.2, $\varphi \in \mathrm{Hom}(A, B)$. □

3.6.2 Endomorphisms

Algorithm 3.6.3 (Endomorphism Algebra as Field)**.** Given a simple abelian variety A over $\mathbb{Q}$, this algorithm computes a number field F and an isomorphism from $\mathrm{End}(A) \otimes \mathbb{Q}$ to F. In light of Proposition 3.6.1, this also yields the endomorphism ring of A.

1. [Isogeny to $A_f^\vee$] Use Algorithm 3.5.1 to compute an optimal subvariety $A_f^\vee$ and an isogeny $\varphi : A \to A_f^\vee$. This isogeny induces an isomorphism $\mathrm{End}(A) \otimes \mathbb{Q}$ to $\mathrm{End}(A_f) \otimes \mathbb{Q}$.

2. [Random endomorphism] Compute a $\mathbb{Z}$-basis B for the Hecke algebra, $\mathbb{T}'$, of $A_f^\vee$. We then generated a random element, T, of $\mathrm{End}(A_f)$ by taking a random rational linear combination of the elements of B.

3. [Is random element primitive?] Let g be the minimal polynomial of T. If $\dim A = \deg g$, then g will be a primitive generator for $\mathrm{End}(A) \otimes \mathbb{Q}$ as a field and we proceed to the next step. Otherwise, return to the last step.

4. [Output] Let F be a number field generated a root, α, of g. Let $\Psi : \mathrm{End}(A) \otimes \mathbb{Q} \to F$ be the unique map sending T to α. We then precompose Ψ with the isomorphism $\mathrm{End}(A) \otimes \mathbb{Q} \to \mathrm{End}(A_f) \otimes \mathbb{Q}$ to obtain the desired isomorphism.

3.6.3 Homomorphism space

Let A, B be isogenous simple abelian varieties. The goal of this section is to compute $\mathrm{Hom}(A, B)$.

Algorithm 3.6.4 (Compute $\mathrm{Hom}(A, B)$)**.** Given simple modular abelian varieties A, B, this algorithm computes $\mathrm{Hom}(A, B)$.

1. [Isogenous?] Use Algorithm 3.7.1 to determine if A is isogenous to B. If not, then $\mathrm{Hom}(A, B)$ is trivial and we are done. If so, let $\varphi : A \to B$ be an isogeny.

2. [Compute $\mathrm{End}(A)$] Use Algorithm 3.6.3 to compute the endomorphism ring of A.

3. [Image of $\mathrm{End}(A)$] Compute the image, H, of $\mathrm{End}(A)$

4. [Saturate] Compute the saturation of H in $\mathrm{Hom}(L_1, L_2)$, where L_1, L_2 are the defining lattices of A, B.

3.7 Isogeny and isomorphism testing

In this section, we give an algorithm for determining when a pair of simple modular abelian varieties are isogenous or isomorphic.

Algorithm 3.7.1 (Isogeny testing)**.** Given simple modular abelian varieties A, B, this algorithm determine if A, B are isogenous. If so, this algorithm will also return an isogeny between A, B.

1. [Find newforms] Use Algorithm 3.5.1 to find newforms f, g and isogenies $\varphi_f : A_f^\vee \to A$ and $\varphi_g : A_g^\vee \to B$.

2. [Isogenous?] If $f = g$, then A is isogenous to B by $\varphi_g \circ \varphi_f^\vee : A \to B$. Otherwise, A is not isogenous to B.

Algorithm 3.7.2 (Isomorphism testing)**.** Given simple modular abelian varieties A, B, this algorithm determine if A, B are isomorphic. If so, this algorithm will also return an isomorphism between A, B.

1. [Isogenous?] Use Algorithm 3.7.1 to determine if A is isogenous to B. If not, then A and B are not isomorphic and we are done. If so, let $\varphi : A \to B$ be an isogeny.

2. [Square degree?] The composition $\varphi^\vee \circ \varphi : B \to B$ is the multiplication by d map where d is the degree of φ. If d is not square, return 'not isomorphic'.

3. [Endomorphism algebra] Use Algorithm 3.6.3 to find a number field K, an order $\mathcal{O} \subseteq K$, and an isomorphism $\tau : \mathrm{End}(A) \to \mathcal{O}$.

4. [Homomorphism space] Use Algorithm 3.6.4 to compute $\mathrm{Hom}(A, B)$.

5. [Image under φ] Compute the image H_f of $\mathrm{Hom}(A, B)$ in $\mathrm{End}(A)$ by composing with f.

6. [Norm equation] Find solutions $x_1, \ldots, x_r$, up to units in $\mathcal{O}$, to the norm equation $\mathrm{Norm}_{\mathcal{O}}(x) = \pm\sqrt{d}$. If there are no solutions, return 'not isomorphic'.

7. [Isomorphic?] For each solution x_i, determine if $x_i \in H_f$, if so, $x_i \circ f^{-1}$ is an isomorphism from $A \to B$. If $x_i \notin H_f$ for all x_i, then return 'not isomorphic'.

Chapter 4

TOTALLY SPLIT JACOBIANS

A Jacobian is said to be *totally split* if it is $\mathbb{Q}$-isogenous to a product of elliptic curves. As mentioned in the introduction, the first N for which Sage fails to compute the rational torsion subgroup is $J_0(30)$ which happens to be a product of 3 elliptic curves. The author and his adviser were able to compute the rational torsion subgroup using the fact that $J_0(30)$ is totally split, the fact that rational torsion subgroups of elliptic curves can be computed, and Galois cohomology. The goal of this chapter is to see how far we can push these techniques. In particular, we will show that there are finitely many totally split $J_0(N)$, give a general (but totally impractical) method for computing the rational torsion subgroup, and present some more practical techniques for computing the rational torsion subgroup.

4.1 Provably enumerating the set of totally split $J_0(N)$

The modular Jacobian $J_0(N)$ is totally split if and only if all newforms of level dividing N have rational Hecke coefficients. We expect this to be rare. In fact, there are only finitely many totally split $J_0(N)$. Ralph Greenberg quickly gave an argument on the way to a University of Washington Number Theory Seminar lunch proving the set of totally split $J_0(N)$ is finite but his argument did not give an effective method of enumeration. Moreover, at Sage Days 87, Alyson Dienes suggested proving this using asymptotic bounds.

Proposition 4.1.1. *The set of totally split $J_0(N)$ is finite.*

Proof. If $J_0(N)$ is a product of elliptic curves then the dimension is exactly equal to the number of elliptic factors.

- By [Mar05, Thm. 6], the dimension is bounded below by $\frac{1}{12}N + O(\sqrt{N} \log\log N)$.

- By [BS96, Cor. 2], the number of elliptic curve factors of $J_0(N)$ is bounded above by $O(N^{1/2+\epsilon})$ for any $\epsilon > 0$.

Asymptotically, the lower bound will surpass the upper bound so there are finitely many totally split $J_0(N)$. □

Neither of their arguments gave an effective method of enumeration. The goal of this section is to provably enumerate the set of $J_0(N)$ that are totally split. There are 71 of totally split $J_0(N)$ that are nontrivial (see Table 6).

We have that $J_0(N)$ is totally split if and only if its dimension is equal to the number of (modular) elliptic curves of conductor N. If N is less than the upper limit of conductors in the Cremona Database, then the hard work has been done and determining whether $J_0(N)$ is totally split is a quick computation since there is a closed-form formula for $\dim J_0(N)$.

Call a positive integer N *good*, if $J_0(N)$ is totally split and *bad* otherwise. The simple factors of $J_0(N)$ are isogenous to simple factors of $J_0(MN)$ for any positive integer M. Therefore, if N is bad, then so is any multiple of N.

In Lemma 4.1.2, we will enumerate all good primes. We can now do a search on the divisibility tree of the positive integers supported on the good primes. Moreover, we can prune a branch whenever we encounter a bad integer during our search. Theorem 4.1.4 asserts that all branches are eventually pruned so this search yields all good integers.

Lemma 4.1.2. *The only possible primes p where $J_0(p)$ is totally split are*

$$2, 3, 5, 7, 11, 13, 17, 19, 37.$$

Proof. Let $J = J_0(p)$ be a totally split Jacobian of prime level. If $\dim J = 0$, then J is clearly totally split so assume $\dim J > 0$. Then $J \cong \prod_f E_f$ with E_f's elliptic curves of conductor p. Let n denote the order of the rational cuspidal subgroup of J which is, as mentioned above, known to be the numerator of $(p-1)/12$. By Emerton's proof of Stein's refined Eisenstein conjecture [Eme03, Theorem B], if l divides n, then l divides the order of $E_f(\mathbb{Q})$ for some elliptic factor of J. But elliptic curves of prime conductor do not have much rational torsion.

In particular, Miyawaki [Miy73] enumerates all curves of prime power conductor with odd-order rational torsion. The largest prime conductor here being 37. This implies that if $p > 37$, then $\#C(\mathbb{Q})$ must be a power of 2 so $p = 2^a 3^b + 1$ for some $a \geq 0$ and $b \in \{0, 1\}$. We now show $a \leq 2$.

If $a > 2$, then $C(\mathbb{Q})$ has an order 2 element which implies some E_i has a rational 2-torsion point. As a result of Setzer [Set75, Theorem 2], $p = 17$ or $p = u^2 + 64$ for some integer u. We split into 2 cases to show that p is never $u^2 + 64$.

Suppose $b = 0$. Then p is a Fermat prime and thus a Fermat number. Outside of 3 and 5, the recursive formula for Fermat numbers and an induction argument shows that the last digit of Fermat numbers is always 7. But the only possible last digits of $u^2 + 64$ are $0, 3, 4, 5, 8, 9$.

Suppose $b = 1$. Then $2^a \cdot 3 = u^2 + 63$. This implies 3 divides u so 9 divides u^2. But now the right-hand side is divisible by 9 while the left is not.

In conclusion, we know that if $J_0(p)$ is a totally split Jacobian, then $p \leq 37$. A computer search then determines which primes less than or equal to 37 are totally split. □

The following procedure is a breath-first search.

Algorithm 4.1.3 (Enumerating Good Integers)**.** Let S be the set of primes found in Lemma 4.1.2. This procedure will halt (see Theorem 4.1.4) and return the list of good integers.

1. [Initialize] Set $i = 1$ and $M_1 = S$. Here M_i will represent the set of all good integers with i prime factors, counting multiplicity.

2. [Find prime multiples of M_i are that good] Set

$$M_{i+1} = \{pN : p \in S, N \in M_i, pN \text{ good}\}.$$

   If M_{i+1} is non-empty, increment i and repeat this step.

3. [Return] Return $\bigcup_i M_i$.

Theorem 4.1.4. *There are 71 integers N for which $J_0(N)$ is a totally split Jacobian of positive dimension. They are given in Table 6.*

Proof. We run Algorithm 4.1.3 and it terminates after find 71 integers N for which $J_0(N)$ is totally split (luckily before reaching the end of the Cremona database). This proves the finiteness of totally split $J_0(N)$ without using Proposition 4.1.1 but with the added benefit of provably enumerating the totally split $J_0(N)$. □

4.2 Enumerating rational torsion is algorithmic

In this section, we give a completely impractical algorithm to compute the rational torsion subgroup of a totally split Jacobian $J_0(N)$ just to show it is algorithmic.

Proposition 4.2.1. *Suppose A is a totally split abelian subvariety of $J = J_0(N)$ Then we can compute the following data:*

1. *A number field containing $\mathbb{Q}(A[n])$ for positive integer n.*

2. *Let n be a positive integer and L be a number field containing $\mathbb{Q}(A[n])$. The action of $\mathrm{Gal}(L/\mathbb{Q})$ on $A[n]$.*

3. *The K-rational torsion points of $A(K)_{\mathrm{tor}}$.*

In particular, we can compute the rational torsion subgroup of any totally split Jacobian.

Proof. Recall that the abelian subvarieties are represented by giving a submodule of the integral homology 3.1. Suppose A is 1-dimensional subvariety of J. Then by 3.5.3, we can compute an elliptic curve E_A given in Weierstrass defining equation and an isomorphism $\Phi_A : A_{\mathrm{tor}} \to (E_A)_{\mathrm{tor}}$.

We will proceed by induction on the dimension, d, of A. We first consider the case $d = 1$.

1. Let n be a positive integer. Then using division polynomials, we can compute a number field L containing $\mathbb{Q}(A[n])$.

2. Let n be a positive integer and L be a number field containing $\mathbb{Q}(A[n])$. The Galois action on the points of $E_A[n]$ is given by applying the Galois action to each coordinate. Using Φ_A and the action of $\mathrm{Gal}(L/\mathbb{Q})$ on E_A, we can explicit determine the action of $\mathrm{Gal}(L/\mathbb{Q})$ on $A[n]$.

3. Let K be a number field. Using reduction mod p, there exists an integer m, such that that $A(K)_{\mathrm{tor}} \subseteq A[m]$. Using (1), we can define a number field L that contains $\mathbb{Q}(A[m])$. Then using (2), we can compute
$$A(K)_{\mathrm{tor}} = A[m]^{\mathrm{Gal}(L/K)}.$$

Now assume we can compute (1)-(3) for any totally split abelian subvariety of dimension less than k.

Let A be of dimension $k+1$ and write $A = B + C$, where B is of dimension k and C is of dimension 1. We have the exact sequence
$$0 \to B \cap C \to B \times C \to A,$$
where we identify $B \cap C$ as a subgroup of $B \times C$ via the anti-diagonal embedding. So $A = (B \times C)/(B \cap C)$. Let r be the exponent of $B \cap C$.

1. For any integer n, $A[n] \subseteq B[nr] + C[nr]$. So a number field containing $\mathbb{Q}(A[n])$ is the compositum of the number fields containing $\mathbb{Q}(B[nr])$ and $\mathbb{Q}(C[nr])$ which can be computed by the inductive hypothesis.

2. The Galois action can be determined on $A[n]$ by viewing $A[n]$ as a subgroup of $(B[nr] \times C[nr])/(B \cap C)$.

3. Using reduction mod p, there exists an integer m such that $A(K)_{\mathrm{tor}} \subseteq A[m]$. Using (1), we can find a number field L that contains $\mathbb{Q}(A[m])$. Then we use (2), to compute
$$A(K)_{\mathrm{tor}} = A[m]^{\mathrm{Gal}(L/K)}.$$

□

4.3 Strategies for computing the rational torsion subgroup

The Generalized Ogg Conjecture is equivalent to the assertion that $[J_0(N)(\mathbb{Q})_{\text{tor}} : C_N(\mathbb{Q})] = 1$. In this section, we give strategies for bounding this index when $J_0(N)$ is a rank-0 totally split Jacobian. We are able to compute generators for $C_N(\mathbb{Q})$ in our presentation (3.3.5) and the group order. Therefore, when $[J_0(N)(\mathbb{Q}) : C_N(\mathbb{Q})] = 1$, we are able to compute generators for $J_0(N)(\mathbb{Q})_{\text{tor}}$ in our presentation.

Using these strategies, we are able to able to verify the Generalized Ogg Conjecture for all but 9 rank-0 $J_0(N)$. In these 9 cases, we are able to bound the index $[J_0(N)(\mathbb{Q})_{\text{tor}} : C_N(\mathbb{Q})]$ by a power of 2 (Table 6).

4.3.1 Upper bound

In this subsection, we give two techniques for giving an upper bound for $J_0(N)(\mathbb{Q})_{\text{tor}}$. The first technique uses reduction modulo p, Eicher-Shimura, and the Hecke polynomial to obtain a bound on the order. The second technique gives an ideal, I^*, similar to Mazur's Eisenstein ideal, so that $J_0(N)(\mathbb{Q})_{\text{tor}} \subseteq J_0(N)[I]$. We will be primarily using the second technique for our computations but we give the first technique to motivate the second and we will be using the first technique

Reduction modulo primes

Let A be a modular abelian variety and K be a number field. A common technique for bounding $A(K)_{\text{tor}}$ is to reduce modulo completely split primes p of K of good reduction for A. In particular, by [Kat81, Appendix], if $\mathcal{A}$ is the Neron model for A and p a prime completely split of K of good reduction for A, then

$$A(K)_{\text{tor}} \hookrightarrow \mathcal{A}_{/p}(\mathbb{F}_p)$$

so $\#A(K)_{\text{tor}} \mid \#\mathcal{A}_{/p}(\mathbb{F}_p)$.

The expression $\#\mathcal{A}_{\mathfrak{p}}(\mathbb{F}_p)$ is an isogeny invariant and multiplicative on direct products. So it suffices to describe how to compute $\mathcal{A}_{/p}(\mathbb{F}_p)$ when $A \subseteq J_0(N)$ is a simple abelian subvariety of the new subvariety of $J_0(N)$ (for $A \subseteq J_1(N)$, see [AS05, §3.5]). Let F_p be the absolute Frobenius at p. By the Eicher-Shimura relations, $T_p = F_p + p/F_p \in \operatorname{End}(\mathcal{A}_{/p})$. Then

$$\begin{aligned}
\#\mathcal{A}_{/p}(\mathbb{F}_p) &= \deg(1 - F_p) \\
&= |\det(1 - F_p)| \\
&= \operatorname{charpoly}(F_p)(1) \\
&= \operatorname{charpoly}(T_p)(p+1).
\end{aligned} \tag{4.3.1}$$

The last term is the characteristic polynomial of the matrix associated to the Hecke operator T_p which can be computed using Section 3.2.

We now return to the case of $K = \mathbb{Q}$ and will apply the more general number field case in Chapter 5. So in the case where $K = \mathbb{Q}$ and $A = J_0(N)$, we have that for any finite set S of odd prime not dividing N,

$$\#J_0(N)(\mathbb{Q})_{\text{tor}} \mid \gcd_{p \in S} \#\mathcal{J}_{/p}(\mathbb{F}_p).$$

We now give the current Sage (Version 8.7) implementation of this idea by William Stein.

Algorithm 4.3.1 (Upper bound on rational torsion order)**.** Given a modular Jacobian $J_0(N)$, this algorithm outputs an upper bound for $\#J_0(N)(\mathbb{Q})_{\text{tor}}$. This algorithm computes successive GCD's until it stabilizes for 3 iterations. Of course, increasing the stability threshold could lead to be a better bound.

1. [Initialize] Let $i = 0$, p_0 be the smallest prime greater than 2 not dividing N.

2. [Add another factor] Use Section 3.2 to compute the matrix associated to T_{p_0}. Let $m_i = \operatorname{charpoly}(T_p)(p+1)$. If $i = 0$, set $B_i = m_i$. Otherwise, set $B_i = \gcd(B_{i-1}, m_i)$.

3. [Stable?/Output] If $i \leq 2$, increment i and return to Step 2. Otherwise, if $B_i \neq B_{i-2}$, return to Step 2. Otherwise, B_i has been stable for 3 iterations and we output B_i.

There are two disadvantages to Algorithm 4.3.1.

The first is that is isogeny invariant so we expect the bound to not be tight. In Section 4.5, we show that there exists an abelian variety isogenous to $J_0(30)$ with strictly greater rational torsion order. So Algorithm 4.3.1 will never give a tight bound even if we increase the stability threshold. This Jacobian is the first $J_0(N)$ that Sage (Version 8.7) cannot compute and is the motivating example for this totally split Jacobian project of this thesis.

The second is the loss of information of the group structure. For example, suppose for some A and odd primes p, q of good reduction, we have the group isomorphisms $\mathcal{A}_{/p}(\mathbb{F}_p) \cong \mathbb{Z}/2\times\mathbb{Z}/2$ and $\mathcal{A}_{/q}(\mathbb{F}_q) \cong \mathbb{Z}/4$. If we look only at the orders, we can only deduce $\#A_f(\mathbb{Q})_{\mathrm{tor}} \mid 4$. However, the group structure tells us that as a group $A_f(\mathbb{Q})_{\mathrm{tor}}$ is trivial or $A_f(\mathbb{Q})_{\mathrm{tor}} \cong \mathbb{Z}/2$.

Real Eisenstein Kernel

This next technique avoids both of the mentioned disadvantages of the first technique. This technique was discovered by William Stein and will be elaborated on as part of a forthcoming paper by Hao Chen, the author, and William Stein. The idea give to construct an ideal I^* so that $J_0(N)(\mathbb{Q})_{\mathrm{tor}} \subseteq J_0(N)[I^*]$.

For any odd prime ℓ of good reduction (so $\ell \nmid 2N$), let $\eta_\ell = T_\ell - (\ell + 1)$.

Lemma 4.3.2 (William Stein)**.** *For any odd prime ℓ of good reduction, $J(\mathbb{Q})_{\mathrm{tor}} \subseteq J[\eta_\ell]$.*

Proof. Let ℓ be an odd prime of good reduction. By [Kat81, Appendix], there the reduction modulo ℓ map yields the inclusion $\tau : J(\mathbb{Q})_{\mathrm{tor}} \hookrightarrow \mathcal{J}_{/\ell}(\mathbb{F}_\ell)$. Let F_ℓ be the absolute Frobenius of of $\mathcal{J}_{/\ell}$. By Eicher-Shimura, $T_\ell = F_\ell + \ell/F_\ell$. Let $x \in J(\mathbb{Q})_{\mathrm{tor}}$ so $F_\ell(\tau(x)) = \tau(x)$. We have

$$\tau(\eta_\ell(x)) = (T_\ell - (\ell+1))\tau(x) = (F_\ell + \ell/F_\ell - (\ell+1))\tau(x) = 0.$$

Since τ is injective $x \in J[\eta_\ell]$. □

Let $I = \langle \eta_\ell : \ell \nmid 2N \rangle$. By Lemma 4.3.2, $J(\mathbb{Q})_{\mathrm{tor}} \subseteq J[I]$. Now let $\star$ be the star-involution so $J(\mathbb{C})(1-\star) = J(\mathbb{R})$. and $I^* = I + \langle 1 - \star \rangle$. William Stein calls this the Real Eisenstein Ideal. We have that $J(\mathbb{C})[1-\star] = J(\mathbb{R})$ so combined with Lemma 4.3.2, $J(\mathbb{Q})_{\mathrm{tor}} \subseteq J[I^*]$. Extending I to I^* is an important step in our strategy because it is often the case that $J[I]$ is strictly larger than $J[I^*]$. For instance, if $J = J_0(N)$ with N prime, then by [Maz77, Cor. 16.3], $J[I]$ contains the Shimura subgroup Σ_N which is a finite subgroup of μ-type and order numerator$((N-1)/12)$.

To approximate $J[I^*]$, let $I_r^* = \langle \eta_\ell : \ell \leq r \rangle$ and define $E_r = J[I_r^*]$. We have

$$C_N(\mathbb{Q}) \subseteq J(QQ)_{\text{tor}} \subseteq E_r \subseteq J[I^*]. \tag{4.3.2}$$

4.4 General approach to bound

4.4.1 Galois cohomology

Let A, E be abelian subvarieties of J with E an elliptic curve and $E \not\subseteq A$. Then

$$\begin{tikzcd} 0 \arrow[r] & A \cap E \arrow[r, "d"] & A \times E \arrow[r, "s"] & A + E \arrow[r] & 0, \end{tikzcd} \tag{4.4.1}$$

where $d(x) = (x, -x)$ and $s(x, y) = (x + y)$. By applying Galois cohomology, we obtain the long exact sequence:

$$\begin{tikzcd} 0 \arrow[r] & (A \cap E)(\mathbb{Q}) \arrow[r] & (A \times E)(\mathbb{Q}) \arrow[r] & (A + E)(\mathbb{Q}) \arrow[dll, rounded corners] \\ & H^1(\mathbb{Q}, A \cap E) \arrow[r, "\gamma"] & H^1(\mathbb{Q}, A \times E) \arrow[r] & \ldots. \end{tikzcd} \tag{4.4.2}$$

We now have

$$\#(A + E)(\mathbb{Q}) = \frac{\#(A \times E)(\mathbb{Q}) \# \ker \gamma}{\#(A \cap E)(\mathbb{Q})}.$$

We will use this equality to inductively compute the rational torsion order of J. Suppose we are able to compute the rational torsion order of A for some abelian subvariety A. The rational torsion of E can be identified using Nagell-Lutz. So we are able to compute $\#(A \times E)(\mathbb{Q})$ and $\#(A \cap E)(\mathbb{Q})$. The hard part is $\# \ker \gamma$ and in general, we will only be able to bound this term.

Let $\beta : H^1(\mathbb{Q}, A \cap E) \to H^1(\mathbb{Q}, E)$ be the map induced by the inclusion of $A \cap E$ into E. Then $\ker \gamma \subseteq \ker \beta$. We have that $A \cap E$ is some finite Galois group of E and it is often the case that $A \cap E = E[n]$ for some positive integer n. In this case, by Kummer Theory, we have that

$$\# \ker \gamma \leq \# \ker \beta = \frac{\#E(\mathbb{Q})}{\#(nE(\mathbb{Q}))}.$$

Putting this altogether, when $A \cap E = E[n]$ for some positive integer n,

$$\#(A+E)(\mathbb{Q}) \leq \frac{\#(A \times E)(\mathbb{Q})\#E(\mathbb{Q})}{\#(A \cap E)(\mathbb{Q})\#(nE(\mathbb{Q}))}. \tag{4.4.3}$$

This now yields an inductive algorithm for computing the rational torsion order of any rank-0 abelian totally split subvariety X of $J_0(N)$.

4.4.2 Reducing to smaller abelian subvarieties

We now take advantage to (4.3.2) to show that it often suffices to verify the Generalized Ogg Conjecture on some abelian subvarieties of J.

Proposition 4.4.1. *Let E be finite subset of $J_0(N)(\mathbb{Q})_{\mathrm{tor}}$ containing $C_N(\mathbb{Q})$ (for example $E = E_r$ (4.3.2)). Let $x_1, \ldots, x_r \in E$ be a set of representatives of $E/(C_N(\mathbb{Q}))$. Suppose for each i, there exists an abelian subvariety A_i of $J_0(N)$ satisfying the Generalized Ogg Conjecture and containing x_i. Then $C_N(\mathbb{Q}) = J_0(N)(\mathbb{Q})_{\mathrm{tor}}$ so $J_0(N)$ satisfies the Generalized Ogg Conjecture.*

Proof. We already have $C_N(\mathbb{Q}) \subseteq J_0(N)(\mathbb{Q})_{\mathrm{tor}}$. To show the reverse inclusion, let $x \in J_0(N)(\mathbb{Q})_{\mathrm{tor}} \subseteq E$. Then $x \in x_i + C_N(\mathbb{Q})$ for some representative x_i. This implies $x_i \in J_0(N)(\mathbb{Q})_{\mathrm{tor}}$. But A_i satisfies the Generalized Ogg Conjecture so $x_i \in C_N(\mathbb{Q})$. Hence, $x \in C_N(\mathbb{Q})$. □

Theorem 4.4.2. *There are 45 totally split rank-0 Jacobians $J_0(N)$ (See Table 6). The Generalized Ogg Conjecture has been verified for all but 9 such N's given by*

$$84, 90, 96, 120, 132, 144, 150, 168, 180$$

In these cases, $[J_0(N)(\mathbb{Q})_{\mathrm{tor}} : C_N(\mathbb{Q})]$ bounded by a power of 2. See Table 6.

Proof. We use Section 4.4 to bound $[J_0(N)(\mathbb{Q})_{\mathrm{tor}} : C_N(\mathbb{Q})]$.

If N is not one of

$$84, 90, 96, 120, 132, 144, 150, 168, 180,$$

then we use Algorithm 4.4.3 to show that the index is 1. □

Algorithm 4.4.3. Given a totally split rank-0 Jacobian $J = J_0(N)$ of dimension k, this algorithm will output a bound on $[J(\mathbb{Q})_{\text{tor}} : C_N(\mathbb{Q})]$, where C_N is the cuspidal subgroup of J.

1. [Upper bound by E_{50}] Set $r = 50$ in (4.3.2) and compute $E = E_{50}$.

2. [Set of representatives] Compute a list of elements $x_1, \ldots, x_s \in E_{50}$ that form a set of representatives for $E_{50}/C(N)$.

3. [Decompose J] Decompose J 3.5.1 into $J = \sum_{i=1}^{k} E_j$, where E_j are elliptic curves.

4. [Reduce to smaller abelian varieties] Let V be the set of abelian subvarieties obtained by taking sums of E_j's. Let each x_i, find $A_i \in V$ of minimal dimension such that $x_i \in A_i$.

5. [Galois cohomology] Use Subsection 4.4.1 to verify the Generalized Ogg Conjecture on each A_i.

4.5 Example

Let $J = J_0(30)$. This is the first level for which Sage (Version 8.7) cannot compute the order of the rational torsion subgroup.

4.5.1 Rational Torsion Subgroup

This variety has dimension 3 and Mordell-Weil rank 0.

```
sage: J = J0(30)
sage: J.decomposition()
```

```
[
Simple abelian subvariety 15a(1,30) of dimension 1 of J0(30),
Simple abelian subvariety 15a(2,30) of dimension 1 of J0(30),
Simple abelian subvariety 30a(1,30) of dimension 1 of J0(30)
]
```

```
sage: L = J.lseries()
sage: L.vanishes_at_1()
```

```
False
```

The rational cuspidal subgroup $C(\mathbb{Q})$ provides a lower bound on the rational torsion subgroup. The group $C(\mathbb{Q})$ is of order 192.

```
sage: J.rational_cuspidal_subgroup()
```

```
Finite subgroup with invariants [2, 4, 24] over QQ of Abelian variety J0(30) of dimension 3
```

Let A and B be the old subvariety and new subvariety of $J_0(30)$. The exact sequence

$$0 \longrightarrow A \cap B \xrightarrow{d} A \times B \xrightarrow{s} J \longrightarrow 0, \tag{4.5.1}$$

where $d(x) = (x, -x)$ and $s(x, y) = (x + y)$ yields the sequence

$$\begin{tikzcd}
0 \arrow[r] & (A \cap B)(\mathbb{Q}) \arrow[r] & (A \times B)(\mathbb{Q}) \arrow[r] & J(\mathbb{Q}) \arrow[dll, rounded corners, to path={ -- ([xshift=2ex]\tikztostart.east) |- ([yshift=-1ex]\tikztostart.south) -| ([xshift=-2ex]\tikztotarget.west) -- (\tikztotarget)}] \\
 & H^1(\mathbb{Q}, A \cap B) \arrow[r, "\gamma"] & H^1(\mathbb{Q}, A \times B) \arrow[r] & \dots
\end{tikzcd} \tag{4.5.2}$$

The old subvariety A decomposes as a product of two elliptic curves coming from $J_0(15)$ and the new subvariety B is the elliptic curve with Cremona label $30a1$.

Since $30/15$ is prime, the hypothesis of Corollary 2.2.5 is satisfied so the old subvariety is isomorphic over $\mathbb{Q}$ to $E \times F$, where the Cremona labels are $E : 15a1$, $F : 15a8$. We can compute the rational torsion order of elliptic curves so $\#A(\mathbb{Q}) = 32$ and $\#B(\mathbb{Q}) = 6$. The intersection $A \cap B$ is is isomorphic as groups to $\mathbb{Z}/2 \times \mathbb{Z}/2$ so $A \cap B = B[2]$. This means $(A \cap B)(\mathbb{Q}) \cong \mathbb{Z}/2$.

```
sage: A = J.old_subvariety()
sage: B = J.new_subvariety()
sage: A.intersection(B)[0].invariants()
```

```
[2, 2]
```

Moreover,

$$\begin{aligned}
\ker(H^1(\mathbb{Q}, A \cap B) \to & H^1(\mathbb{Q}, A \times B)) \subseteq \\
& \ker(H^1(\mathbb{Q}, B[2]) \to H^1(\mathbb{Q}, B)) = B(\mathbb{Q})/2B(\mathbb{Q}).
\end{aligned} \tag{4.5.3}$$

This implies $\# \ker \gamma \leq 2$ in (4.5.2). Piecing everything together

$$\# J_0(30)(\mathbb{Q}) = \frac{\# A(\mathbb{Q}) \cdot \# B(\mathbb{Q}) \cdot \# \ker \gamma}{\# (A \cap B)(\mathbb{Q})} \leq 192.$$

It follows that $J_0(30)(\mathbb{Q}) = C(\mathbb{Q})$ and is isomorphic to $\mathbb{Z}/2 \times \mathbb{Z}/4 \times \mathbb{Z}/24$.

4.5.2 Reduction mod p is not enough

We have the isogeny

$$J_0(30) \sim E \times E \times F,$$

where $E : 15a1$ and $F : 30a2$ are elliptic curves with $\# E(\mathbb{Q}) = 8$ and $\# F(\mathbb{Q}) = 12$. This means that $U(S) \geq 8 \cdot 8 \cdot 12 = 768$. This means that the reduction mod p strategy alone is not enough to show that $J(\mathbb{Q})_{\text{tor}}$ is cuspidal.

Chapter 5

ENUMERATING THE ODD ISOGENIES CLASS OF PRIME LEVEL SUBVARIETIES

Let N be a prime number so that $J_0(N)$ is non-trivial so $N = 11$ or $N \geq 17$. Let A be a simple abelian subvariety of $J_0(N)$. The goal of this chapter is to, under certain conditions, enumerate the $\mathbb{Q}$-isomorphism classes of abelian varieties isogenous to A by an odd-degree $\mathbb{Q}$-isogeny. We will call this the *odd-degree isogeny class* of A.

More precisely, let $\mathbb{T}$ be the Hecke algebra of $J_0(N)$ and $\mathbb{T}_A$ be the image of $\mathbb{T}$ in $\mathrm{End}(A)$. There exists a newform $f = \sum a_n q^n$ associated A. By [Shi94, Prop. 7.14], $\mathbb{T}_A$ is isomorphic to an order of the Hecke eigenvalue field, $K_f = \mathbb{Q}(\ldots, a_n, \ldots)$. The goal of this Chapter is to enumerate the odd-degree isogeny class of A when $\mathbb{T}_A$ is integrally closed, $\mathrm{Cl}(\mathbb{T}_A)$ is trivial, and when the hypothesis of Corollary 5.5.4 holds.

Unless otherwise stated, in this chapter, all abelian varieties, isogenies, and isomorphisms are defined over $\mathbb{Q}$.

The image of an odd-degree isogeny, $\varphi : A \to A'$, is determined, up to isomorphism, by its kernel, M, which is a finite $G_{\mathbb{Q}}$-submodule of $A(\overline{\mathbb{Q}})$. We begin by showing every finite $G_{\mathbb{Q}}$-submodule of $A(\overline{\mathbb{Q}})_{\mathrm{odd}}$ is a $\mathbb{T}_A[G_{\mathbb{Q}}]$-module (Proposition 5.1.1). This is useful because the $\mathbb{T}_A$-structure is more easily understood than the $G_{\mathbb{Q}}$-structure. Let $\mathcal{I}_A$ be the image of the Eisenstein ideal $\mathcal{I}$ into $\mathrm{End}(A)$. A prime of $\mathbb{T}_A$ is Eisenstein if it divides $\mathcal{I}_{\mathcal{A}}$ and is non-Eisenstein otherwise. Let $\mathcal{P}_e$ be the set of Eisenstein primes of odd-residue characteristic and $\mathcal{P}_{ne}$ be the set of non-Eisenstein primes of odd-residue characteristic. We will use a theorem of Frank Calegari (Theorem 5.3.1) to prove that the image of an odd-degree isogeny is isomorphic to one whose kernel is supported, as a $\mathbb{T}_A$-module, only on $\mathcal{P}_e$. Finally, we adapt the work of Krzysztof Klosin and Mihran Papikian to enumerate the isomorphic classes of abelian varieties isogenous to A by an isogeny supported on $\mathcal{P}_e$.

5.1 *Finite odd-order Galois Modules are Hecke*

The goal of this section is to prove every finite odd-order $G_{\mathbb{Q}}$-submodule M of $A(\overline{\mathbb{Q}})$ is a Hecke module (Proposition 5.1.1). The Galois action of $J(\overline{\mathbb{Q}})_{\mathrm{odd}}$ has been extensively studied by Mazur [Maz77], so we weaken our hypothesis to M a finite $G_{\mathbb{Q}}$-submodule of $J(\overline{\mathbb{Q}})_{\mathrm{odd}}$. This is allowed because A is $\mathbb{T}[G_{\mathbb{Q}}]$-stable.

It suffices to prove M is $\mathbb{T}$-stable for each $G_{\mathbb{Q}}$-composition factor V of $M[\ell^\infty]$ for $\ell > 2$. The irreducibility of V implies that it is ℓ-torsion. Ribet [Rib97, Proposition 6.1] shows that $\mathbb{T}/\ell\mathbb{T}$ is generated by T_p for primes $p \nmid \ell N$. So we reduce modulo p for $p \nmid \ell N$, and use Eichler-Shimura to derived its $\mathbb{T}$-stability from its $G_{\mathbb{Q}}$-stability.

Proposition 5.1.1. *Suppose M is a finite odd-order $G_{\mathbb{Q}}$-submodule of $J_0(N)$, with N prime. Then M is a $\mathbb{T}[G_{\mathbb{Q}}]$-module.*

Proof. It suffices to show M is $\mathbb{T}$-stable for each ℓ-primary part. Let $\ell > 2$ and assume $M \subseteq J[\ell^\infty]$. Let

$$0 = M_0 \subsetneq \ldots \subsetneq M_n = M$$

be an $G_{\mathbb{Q}}$-composition series of M with composition factors $X_i = M_i/M_{i-1}$. We proceed by induction on n with the base case being the trivial $n = 0$ case.

Assume M_{s-1} is an $\mathbb{T}[G_{\mathbb{Q}}]$-module. We will show M_s is an $\mathbb{T}[G_{\mathbb{Q}}]$-module. Since M_{s-1} is an $\mathbb{T}[G_{\mathbb{Q}}]$-module, for each $t \in \mathbb{T}$, we have a well-defined map $t : X_s \to J(\overline{\mathbb{Q}})/M_{s-1}$. The goal is to show $t(X_s) \subseteq X_s$ for all $t \in \mathbb{T}$. By [Rib91a, Proposition 2], $\mathbb{T}/\ell\mathbb{T}$ is generated by T_p for $p \nmid \ell N$ so it suffices to show $T_p(X_s) \subseteq X_s$ for prime $p \nmid \ell N$.

Fix a prime $p \nmid \ell N$. Since p does not divide N, J has good reduction at p. Fix a place $\mathfrak{p}$ over p. The reduction map yields an isomorphism [ST68, Theorem 1, Lemma 2]

$$\tau : J(\overline{\mathbb{Q}})[\ell^\infty] \xrightarrow{\sim} J_{/\mathbb{F}_p}(\overline{\mathbb{F}}_p)[\ell^\infty]$$

sending $\mathrm{Frob}_{\mathfrak{p}}$ to F_p, where F_p is the absolute Frobenius on $J_{/\mathbb{F}_p}$. Under this isomorphism the natural $\mathbb{T}$-action on $J(\mathbb{Q})$ maps to the natural $\mathbb{T}$-action on $J_{/\mathbb{F}_p}$ [RS01, §5.2]. By Eicher-Shimura, $T_p = F + p/F \in \mathrm{End}(J_{/\mathbb{F}_p})$ so

$$\tau(T_p X_s) = T_p\tau(X_s) = (F + p/F)\tau(X_s) = \tau((\mathrm{Frob}_{\mathfrak{p}} + p/\,\mathrm{Frob}_{\mathfrak{p}})X_s) \subseteq \tau(X_s)$$

hence, $T_p X_s \subseteq X_s$, as desired. □

5.2 Non-Eisenstein modules are kernels of Hecke

In the previous section, we show that every finite odd-order $G_{\mathbb{Q}}$-submodules of $J(\overline{\mathbb{Q}})$ and $A(\overline{\mathbb{Q}})$ are $\mathbb{T}[G_{\mathbb{Q}}]$-modules and $\mathbb{T}_A[G_{\mathbb{Q}}]$-modules, respectively. The goal now is to show if M is a finite-odd order $\mathbb{T}_A[G_{\mathbb{Q}}]$-submodule $A(\overline{\mathbb{Q}})$ supported only on the non-Eisenstein primes as a $\mathbb{T}_A$-module then $M = A[\mathrm{Ann}_{\mathbb{T}_A} M]$. As in the previous section, since A is $\mathbb{T}[G]$-invariant, we can instead take the hypothesis that M is a finite-odd order $\mathbb{T}[G_{\mathbb{Q}}]$-submodule of $J(\overline{\mathbb{Q}})$ supported as a $\mathbb{T}$-module only on the non-Eisenstein primes, then $M = J[\mathrm{Ann}_{\mathbb{T}} M]$.

If M is any $\mathbb{T}[G_{\mathbb{Q}}]$-submodule of $J(\overline{\mathbb{Q}})$, it is always the case that $M \subseteq J[\mathrm{Ann}_{\mathbb{T}} M]$. It is for the reverse inclusion where we need to use the fact that M is supported only on the non-Eisenstein primes of odd-residue characteristic. The crucial fact we use about non-Eisenstein primes is that, by [Maz77, Prop. 14.2], if $\mathfrak{m}$ is a non-Eisenstein of odd residue characteristic, then $J[\mathfrak{m}]$ is an irreducible $G_{\mathbb{Q}}$-module.

We are already able to show that $M = J[\mathrm{Ann}_{\mathbb{T}} M]$ when M is irreducible as a $\mathbb{T}[G_{\mathbb{Q}}]$-submodule.

Proposition 5.2.1. *Let $\mathfrak{m}$ be a non-Eisenstein prime of odd residue characteristic, if M is a nonzero finite irreducible $\mathbb{T}[G_{\mathbb{Q}}]$-submodule of $J(\overline{\mathbb{Q}})$ supported only on $\mathfrak{m}$ as a $\mathbb{T}$-module, then $M = J[\mathfrak{m}]$.*

Proof. Let $\mathfrak{a} = \mathrm{Ann}_{\mathbb{T}}(M)$. We will first show that $\mathfrak{a} = \mathfrak{m}$ by showing $\mathfrak{a}$ is maximal. Let e be the exponent of M as an abelian group. We have that $e \in \mathfrak{a}$ and $\mathbb{T}/e\mathbb{T}$ is a finite ring so it suffices to show that $\mathfrak{a}$ is a prime ideal. Suppose $x, y \notin \mathrm{Ann}_{\mathbb{T}}(M)$. Then yM is a nonzero

$\mathbb{T}[G_{\mathbb{Q}}]$-submodule of the irreducible module M so $yM = M$. Similarly, $xyM = xM$ is nonzero. Therefore, $yx \notin \mathrm{Ann}_{\mathbb{T}}(M)$ so $\mathfrak{a} = \mathfrak{m}$.

Now $M \subseteq J[\mathfrak{m}]$ but $J[\mathfrak{m}]$ is an irreducible $G_{\mathbb{Q}}$-module [Maz77, Proposition 14.2] so $M = J[\mathfrak{m}]$. □

The general case will follow from a trivial adaptation of the work of David Helm [Hel07]. Helm considers the case of Jacobians, J, of Shimura curves. One of the key inputs into Helm's proof is that for the maximal ideals $\mathfrak{m}$ in question is that if $T_{\mathfrak{m}}J$ is the contravariant $\mathfrak{m}$-adic Tate module, then $T_{\mathfrak{m}}J/\mathfrak{m}T_{\mathfrak{m}}J \cong J[\mathfrak{m}]^{\vee}$ is dimension two over $\mathbb{T}/\mathfrak{m}$ and is irreducible as a $G_{\mathbb{Q}}$-module. By [Maz77, Prop. 14.2], this is also the case for $J = J_0(N)$ with N prime and $\mathfrak{m}$ a non-Eisenstein prime of odd residue characteristic.

Theorem 5.2.2 ([Hel07, Corollary 4.8])**.** *Let M be a finite odd-order $G_{\mathbb{Q}}$-module supported, as a $\mathbb{T}$-module, only on the non-Eisenstein primes. If $I = \mathrm{Ann}_{\mathbb{T}}(M)$, then $M = J[I]$.*

Moreover, since A is both $\mathbb{T}[G_{\mathbb{Q}}]$-invariant, if M is a finite odd-order $G_{\mathbb{Q}}$-submodule of $A(\overline{\mathbb{Q}})$ supported, as a $\mathbb{T}_A$-module, only on the non-Eisenstein primes. If $I = \mathrm{Ann}_{\mathbb{T}_A}(M)$, then $M = A[I]$.

Proof. Since $M \subseteq J[I]$ and $\mathrm{Supp}_{\mathbb{T}} M = \mathrm{Supp}_{\mathbb{T}} J[I]$, it suffices to prove $J[I]_{\mathfrak{m}} = M_{\mathfrak{m}}$ for each non-Eisenstein prime of odd residue characteristic. So let $\mathfrak{m}$ be a non-Eisenstein prime of odd residue characteristic. We start by reviewing the contravariant Tate modules of J and proving Lemma 5.2.3.

Let $T_{\mathfrak{m}}J \cong \mathrm{Hom}(J[\mathfrak{m}^{\infty}], \mathbb{Q}_{\ell}/\mathbb{Z}_{\ell})$ be the contravariant Tate module at $\mathfrak{m}$ and $\overline{\rho}_{\mathfrak{m}}$ be the Galois representation associated to $J[\mathfrak{m}]^{\vee}$. Since $\mathfrak{m}$ is an odd non-Eisenstein prime, $\overline{\rho}_{\mathfrak{m}}$ is an irreducible $G_{\mathbb{Q}}$-representation of dimension 2 over $k_{\mathfrak{m}}$ that is isomorphic to $J[\mathfrak{m}]^{\vee}$ [Maz77, Prop. 14.2].

Lemma 5.2.3 ([Hel07, Lemma 4.6])**.** *Let R be a $G_{\mathbb{Q}}$-stable submodule of $T_{\mathfrak{m}}J$ of finite index. Then $R = IT_{\mathfrak{m}}J$ for some ideal I of $\mathbb{T}$.*

Proof. We proceed by induction on the maximal $G_{\mathbb{Q}}$-composition series of $T_{\mathfrak{m}}J/R$ with the base case being the trivial length zero case. Let

$$R = R_n \subsetneq R_{n-1} \subsetneq \cdots \subsetneq R_0 = T_{\mathfrak{m}}J$$

be a $G_{\mathbb{Q}}$-composition series. By induction, $R_{n-1} = I'T_{\mathfrak{m}}J$ for some $I' \subseteq \mathbb{T}$.

Consider $\mathfrak{m}R_{n-1} + R$. This is a $G_{\mathbb{Q}}$-module sitting between R and R_{n-1}. By Nakayama's lemma, if $\mathfrak{m}R_{n-1}R+R = R_{n-1}$, then $R = R_{n-1}$ which is a contradiction. Hence, $\mathfrak{m}R_{n-1}+R = R$ so R contains $\mathfrak{m}R_{n-1}$ and we can form the quotient.

The module $R_{n-1}/\mathfrak{m}R_{n-1}$ is $G_{\mathbb{Q}}$-isomorphic to $(I'/\mathfrak{m}I') \otimes_{\mathbb{T}/\mathfrak{m}} (T_{\mathfrak{m}}J/\mathfrak{m}T_{\mathfrak{m}}J) \cong (I'/\mathfrak{m}I') \otimes_{\mathbb{T}/\mathfrak{m}} J[\mathfrak{m}]^\vee$, where $G_{\mathbb{Q}}$ acts trivially on $I'/\mathfrak{m}I'$. Let V be the image of R in $R_{n-1}/\mathfrak{m}R_{n-1}$. Since V is $G_{\mathbb{Q}}$-invariant, and $J[\mathfrak{m}]^\vee$ is irreducible, V is given by $\hat{V} \otimes J[\mathfrak{m}]^\vee$ for some $\mathbb{T}/\mathfrak{m}$-subspace $\hat{V}$ of $I'/\mathfrak{m}I'$. Let I be the preimage of $\hat{V}$ in I'. Then $IT_mJ = R$, since both contain $\mathfrak{m}R_{n-1}$ and map to V modulo $\mathfrak{m}R_{n-1}$. □

Let $B = J/M$ be the quotient abelian variety. Since M is a $\mathbb{T}$-module, we may equipped with a $\mathbb{T}$-action. So the projection $\phi : J \to B$ is an $\mathbb{T}[G_{\mathbb{Q}}]$-isogeny with $\ker\phi = M$. For any odd non-Eisenstein prime $\mathfrak{m}$, ϕ induces the exact sequence

$$0 \to T_{\mathfrak{m}}B \to T_{\mathfrak{m}}J \to M_{\mathfrak{m}}^\vee \to 0.$$

In particular, the image of $T_{\mathfrak{m}}B$ under ϕ is a finite index $\mathbb{T}[G_{\mathbb{Q}}]$-submodule of $T_{\mathfrak{m}}A$. By Lemma 5.2.3, we can find an ideal I' of $\mathbb{T}$ such that the image of $T_{\mathfrak{m}}B$ is $I'_{\mathfrak{m}}T_{\mathfrak{m}}A$ for all odd non-Eisenstein primes $\mathfrak{m}$. We have $M_{\mathfrak{m}}^\vee = T_{\mathfrak{m}}J/I'T_{\mathfrak{m}}J \cong J[I']_{\mathfrak{m}}^\vee$. Therefore, by taking annihilators of the dual, we have that $I_{\mathfrak{m}} = I'_{\mathfrak{m}}$ and then by taking duals $M_{\mathfrak{m}} = J[I]_{\mathfrak{m}}$, as desired. □

5.3 Bounding non-Eisenstein part

Recall that a prime of $\mathbb{T}_A$ is non-Eisenstein if it does not divides the Eisenstein ideal $\mathbb{T}_A$. There are infinitely many non-Eisenstein primes. The goal of this section is to bound isomorphism classes of A/X with $\operatorname{Supp}_{\mathbb{T}_A} X \subseteq \mathcal{P}_{ne}$ by $\mathrm{Cl}(\mathbb{T}_A)$. In particular, we will prove a theorem of Frank Calegari.

Let $\mathcal{H}$ be a set of integral representatives for $\mathrm{Cl}(\mathbb{T}_A)$ coprime to $2\mathcal{I}_A$. Suppose M is $\mathbb{T}_A$-supported only on the primes of $\mathcal{P}_{ne}$. By Theorem 5.2.2, $M = A[\mathfrak{a}]$ with $\mathfrak{a} = \operatorname{Ann}_{\mathbb{T}_A} M$. Now there exists $s, t \in \mathbb{T}_A$ and $\mathfrak{b} \in \mathcal{H}$, such that $s\mathfrak{a} = t\mathfrak{b}$. We will show that $\varphi = s \circ t^{-1} \in \mathbb{T}_A \otimes \mathbb{Q}$ is well-defined and yields an isomorphism $A/M \to A/A[\mathfrak{b}]$. Lastly, we will make some remarks about the $\mathfrak{p}$-adic valuation of φ that we will use in Section 5.4

Theorem 5.3.1 (Frank Calegari)**.** *Let $A \subsetneq J_0(N)$ be a simple abelian subvariety with N prime. Suppose $\mathbb{T}_A$ is integrally closed. Let M be a $\mathbb{T}_A[G_{\mathbb{Q}}]$-submodule of $A(\overline{\mathbb{Q}})$ supported only on the non-Eisenstein primes of odd residue characteristic. Then there exists $\varphi \in \mathbb{T}_A \otimes \mathbb{Q}$ and $\mathfrak{b} \in H$, such that, there is an isomorphism*

$$\varphi : A/M \to A/A[\mathfrak{b}].$$

Moreover, $v_{\mathfrak{p}}(\varphi) = 0$ if $\mathfrak{p} \in \mathcal{P}_e$ and $v_{\mathfrak{p}}(\varphi) \leq v_{\mathfrak{p}}(\mathfrak{b})$ if $\mathfrak{p} \in \mathcal{P}_{ne}$.

Proof. By Theorem 5.2.2, if $\mathfrak{a} = \operatorname{Ann}_{\mathbb{T}_A} M$, then $M = A[\mathfrak{a}]$. We have that there exists $s, t \in \mathbb{T}_A$ and $\mathfrak{b} \in H$, such that $s\mathfrak{a} = t\mathfrak{b}$. We will justify the following commutative diagram.

$$\begin{tikzcd}
A/A[s\mathfrak{a}] \arrow[r, "\sim", "s"'] \arrow[d, equal] & A/A[\mathfrak{a}] \arrow[d, "\phi", "\wr"'] \\
A/A[t\mathfrak{b}] \arrow[r, "\sim", "t"'] & A/A[\mathfrak{b}],
\end{tikzcd}$$

We will first establish the isomorphism $s : A/A[s\mathfrak{a}] \to A/A[\mathfrak{a}]$.

$$\begin{tikzcd}
0 \arrow[r] & (A/A[\mathfrak{a}])[s] \arrow[r, hook] & A/A[\mathfrak{a}] \arrow[r, two heads, "s"] & A/A[\mathfrak{a}] \arrow[r] & 0 .
\end{tikzcd}$$

We have that $x \in (A/A[\mathfrak{a}])[b]$ if and only if $bx \in A[\mathfrak{a}]$ if and only if $x \in A[s\mathfrak{a}]$. Hence, $(A/A[\mathfrak{a}])[b] = A[s\mathfrak{a}]/A[\mathfrak{a}]$ so $b : A/A[s\mathfrak{a}] \overset{\sim}{\to} A[\mathfrak{a}]$. A similar argument applies for $a : A/A[t\mathfrak{b}] \to A/A[\mathfrak{b}]$.

We have that

$$v_{\mathfrak{p}}(\varphi) = v_{\mathfrak{p}}(t) - v_{\mathfrak{p}}(s) = v_{\mathfrak{p}}(\mathfrak{a}) - v_{\mathfrak{p}}(\mathfrak{b}).$$

If $\mathfrak{p} \in P_e$, then $v_{\mathfrak{p}}(C), v_{\mathfrak{p}}(D) = 0$. Therefore, $v_{\mathfrak{p}}(\varphi) = 0$ if $\mathfrak{p} \in \mathcal{P}_e$ and $v_{\mathfrak{p}}(\varphi) \leq v_{\mathfrak{p}}(\mathfrak{b})$ if $\mathfrak{p} \in \mathcal{P}_{ne}$. □

5.4 *Bounding support and valuations*

Let $A \subseteq J_0(N)$ be a simple abelian subvariety with N prime. Suppose $\mathbb{T}_A$ is integrally closed. Suppose $\psi : A \to A'$ be an odd-isogeny. Then $M = \ker \psi$ is a $G_{\mathbb{Q}}$-submodule of $A(\overline{\mathbb{Q}})_{\text{odd}}$. By Proposition 5.1.1, M is a $\mathbb{T}_A[G_{\mathbb{Q}}]$-module so we can decompose M as $M_{ne} \oplus M_e$, where M_{ne} and M_e are $\mathbb{T}_A[G_{\mathbb{Q}}]$-submodules supported, as $\mathbb{T}_A$-modules, only on $\mathcal{P}_{ne}$ and $\mathcal{P}_e$, respectively. Using Theorem 5.3.1, $A/M_{ne} \cong A/A[\mathfrak{b}]$ for some $\mathfrak{b} \in \mathcal{H}$. The goal of this section is to show $A/M = A/(M_{ne} \oplus M_e) \cong A/(A[\mathfrak{b}] \oplus X_e)$ while controlling the difference between M_e and X_e.

Proposition 5.4.1. *Let $A \subseteq J_0(N)$ be a simple abelian subvariety with N prime. Suppose $\mathbb{T}_A$ is integrally closed. Suppose $\psi : A \to A'$ be an odd-isogeny. Let M, M_{ne}, M_e be as above. Then*

$$A' \cong A/(A[\mathfrak{b}] \oplus X_e),$$

where $\operatorname{Supp}_{\mathbb{T}_A} X_e \subseteq \mathcal{P}_e$. Moreover, for each $\mathfrak{p} \in \mathcal{P}_e$, let $e_{\mathfrak{p}}$ be the smallest nonnegative integer such that $M_e[\mathfrak{p}^\infty] \subseteq A[\mathfrak{p}^{e_{\mathfrak{p}}}]$. Then, for each $\mathfrak{p} \in \mathcal{P}_e$, we have $X_e[\mathfrak{p}^\infty] \subseteq A[\mathfrak{p}^{e_{\mathfrak{p}}}]$.

Proof. By Theorem 5.3.1, there exists $\varphi \in \mathbb{T}_A \otimes \mathbb{Q}$ and $\mathfrak{b} \in \mathcal{H}$, such that $\varphi : A/M_{ne} \to A/A[\mathfrak{b}]$ is an isomorphism with $v_{\mathfrak{p}}(\varphi) = 0$ if $\mathfrak{p} \in \mathcal{P}_e$ and $v_{\mathfrak{p}}(\varphi) \leq v_{\mathfrak{p}}(\mathfrak{b})$ if $\mathfrak{p} \in \mathcal{P}_{ne}$.

Let $\psi : A/M_{ne} \to A/(M_{ne} + M_e)$ be the isogeny corresponding to quotienting by M_e. Let $\psi' : A/A[\mathfrak{b}] \to A(A[\mathfrak{b}]+\varphi(M_e))$. We have that φ is also an isomorphism from $A/(M_{ne}+M_e) \to A(A[\mathfrak{b}] + \varphi(M_e))$.

$$\begin{tikzcd} A/M_{ne} \arrow[r, "\psi"] \arrow[d, "\varphi"] & A/(M_{ne} + M_e) \arrow[d, "\varphi'"] \\ A/A[\mathfrak{b}] \arrow[r, "\psi'"] & A/(A[\mathfrak{b}] + \varphi(M_e)). \end{tikzcd}$$

Since $\varphi(M_e)$ is $\mathbb{T}_A$-module, we can write it as $X_{ne} \oplus X_e$. Let $\mathfrak{p} \in \mathcal{P}_{ne}$. Since M_e is supported away from $\mathfrak{p}$ and $v_{\mathfrak{p}}(\varphi) \leq v_{\mathfrak{p}}(\mathfrak{b})$, $\varphi(M_e)[\mathfrak{p}^\infty] \subseteq A[\mathfrak{b}]$. Therefore, $A[\mathfrak{b}]+\varphi(M_e) = A[\mathfrak{b}]+X_e$. Now if $\mathfrak{p} \in \mathcal{P}_e$ instead, we have that $v_{\mathfrak{p}}(\varphi) = 0$ and $M_e[\mathfrak{p}^\infty] \subseteq A[\mathfrak{p}^\infty]$ so $X_e[\mathfrak{p}^\infty] = \varphi(M_e)[\mathfrak{p}^\infty] \subseteq \varphi(A[\mathfrak{p}^{e_\mathfrak{p}}]) \subseteq A[\mathfrak{p}^{e_\mathfrak{p}}]$. □

As a corollary, we can give an explicit set of primes such that the image of every odd-degree isogeny of A is equivalent to one supported on this set of primes.

Corollary 5.4.2. *Let $\mathcal{P}_\mathcal{H}$ be the union of the set of primes dividing elements of $\mathcal{H}$ with the set of Eisenstein prime of odd-residue characteristic. If A' is isogenous to A by an odd-degree isogeny, $A' \cong A/X$ for some $\mathbb{T}_A[G]$-submodule of $A(\overline{\mathbb{Q}})$ supported on $\mathcal{H}$.*

5.5 Eisenstein part

In this section, we will follow the work of Krzysztof Klosin and Mihran Papikian to enumerate the isomorphic classes of abelian varieties isogenous to A by an isogeny supported on $\mathcal{P}_e$. This section is a straightforward adaption of their work.

Proposition 5.5.1. *[KP18, Prop. 4.5] Let $A \subseteq J_0(N)$ be a simple abelian subvariety with N prime. Let $\mathfrak{p}$ be an Eisenstein prime of $\mathbb{T}_A$ of odd residue characteristic p. Suppose $A[\mathfrak{p}] \neq 0$ and $A[\mathfrak{p}] = J_0(N)[\mathfrak{p}]$. Suppose there exists $\ell \equiv 1 \pmod{p^2N}$ such that $p^3 \nmid \mathcal{A}_{/\ell}(\mathbb{F}_\ell)$, where $\mathcal{A}_{/\ell}$ is the reduction of the Neron model of A at ℓ. Suppose that $M \subseteq A[\mathfrak{p}^\infty]$. If $A[\mathfrak{p}] \not\subseteq M$, then $M \subseteq A[\mathfrak{p}]$.*

Proof. We will assume $A[\mathfrak{p}] \not\subseteq M$ and $M \not\subseteq A[\mathfrak{p}]$, and derive a contradiction by showing $p^3 \mid \#A(\mathbb{F}_\ell)$ for all rational primes $\ell \equiv 1 \pmod{p^2N}$.

Let $K = \mathbb{Q}(M)$. By [Maz77, Cor. 16.3], $A[\mathfrak{p}] = C[p] \oplus \Sigma[p]$. Since $\Sigma[p]$ is of μ-type, $\mathbb{Q}(A[\mathfrak{p}]) = \mathbb{Q}(\mu_p)$. Let $F = \mathbb{Q}(\mu_{pN})$ and $K = \mathbb{Q}(M)$. Then both $A[\mathfrak{p}]$ and M are constant over KF. Since $A[\mathfrak{p}] \not\subseteq M$ and $M \not\subseteq A[\mathfrak{p}]$, we have that $p^3 \mid A(K)_{\mathrm{tor}}$. The goal now is to show that if $\ell \equiv 1 \pmod{p^2N}$ is a rational prime then ℓ is completely split over K. We will do this by showing $K \subseteq \mathbb{Q}(\mu_{p^2N})$.

Lemma 5.5.2 ([KP18, Lem. 4.6])**.** *The number field $K = \mathbb{Q}(M)$ is an abelian extension of $\mathbb{Q}$ unramified away from p, N.*

Proof. Since M is supported only on $\mathfrak{p}$ as a $\mathbb{T}_A$-module, we may view M as a $(\mathbb{T}_A)_\mathfrak{p}$-module. Since M is finite and $(\mathbb{T}_A)_\mathfrak{p}$ is a DVR, we have

$$M \cong (\mathbb{T}_A)_\mathfrak{p}/\mathfrak{p}^{s_1} \times \cdots \times (\mathbb{T}_A)_\mathfrak{p}/\mathfrak{p}^{s_r} \cong (\mathbb{T}_A)/\mathfrak{p}^{s_1} \times \cdots \times (\mathbb{T}_A)/\mathfrak{p}^{s_r}$$

for some $s_1, \ldots, s_r \geq 0$. Since $\dim_{\mathbb{T}_A/\mathfrak{p}} A[\mathfrak{p}] = 2$ and $M[\mathfrak{p}] \cong (\mathbb{T}_A/\mathfrak{p})^r \subsetneq A[\mathfrak{p}]$ so $r = 1$. Therefore, $M \cong \mathbb{T}_A/\mathfrak{p}^{s_1}$.

Recall the elements of $\mathbb{T}_A$ are defined over $\mathbb{Q}$ so they commute with elements of $G_\mathbb{Q}$, therefore,

$$\mathrm{Gal}(K/\mathbb{Q}) \subseteq \mathrm{Aut}_{\mathbb{T}_A}(M) \cong \mathrm{Aut}_{\mathbb{T}_A}(\mathbb{T}_A/\mathfrak{p}^{s_1}) \cong (\mathbb{T}_A/\mathfrak{p}^{s_1})^\times.$$

Since $\mathbb{T}_A$ is isomorphic to an order of a number field, $\mathrm{Gal}(K/\mathbb{Q})$ is abelian. Since A has good reduction away from N, $K/\mathbb{Q}$ is unramified away from p, N. □

Lemma 5.5.3. *The number field K is a subfield of $\mathbb{Q}(\mu_{p^2}, \mu_N)$.*

Proof. By assumption, $(\mathbb{T}_A)_\mathfrak{p}$ is a DVR, so, as a $(\mathbb{T}_A)/\mathfrak{p}$-space, $\mathfrak{p}/\mathfrak{p}^2$ is generated by some $\alpha \in \mathfrak{p}$. This yields the exact sequence

$$0 \longrightarrow A[\mathfrak{p}] \longrightarrow A[\mathfrak{p}^2] \xrightarrow{\alpha} A[\mathfrak{p}] \ .$$

By restricting to M, we have

$$0 \longrightarrow M \cap A[\mathfrak{p}] \longrightarrow M \longrightarrow M \cap A[\mathfrak{p}] \longrightarrow 0 \tag{5.5.1}$$

Since $M \subsetneq A[\mathfrak{p}]$, $M \cap A[\mathfrak{p}]$ is either $C[p]$ or $\Sigma[p]$. As a $\mathbb{Z}$-module, $M \cong \mathbb{Z}/p^2$. Therefore, $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$ acts trivially on $pM = M \cap A[\mathfrak{p}]$. So $\mathrm{Gal}(KF/F)$ can be identified with the subgroup $\{a \in (\mathbb{Z}/p^2) : ap \equiv p \pmod{p^2}\} \subseteq (\mathbb{Z}/p^2)$ of order p so $[KF : F] = 1$ or p.

We have

$$\mathrm{Gal}(\mathbb{Q}(\mu_p^{n_1}, \mu_N^{n_2})/F \cong \mathbb{Z}/p^{n_1 - 1} \times \mathbb{Z}/N^{n_2 - 1}.$$

Since $[KF : F] = 1$ or p, $KF \subseteq F(\mu_p^{n_1})$ is a subfield of degree 1 or p. In either case, $K \subseteq KF \subseteq \mathbb{Q}(\mu_p^2, \mu_N)$. □

Now suppose $\ell \equiv 1 \pmod{p^2N}$ is a rational prime. Then ℓ is completely split over K so, as in Section 4.3.1, by [Kat81, Appendix], there is an inclusion

$$A(K)_{\mathrm{tor}} \hookrightarrow \mathcal{A}_{/\mathbb{F}_\ell}(\mathbb{F}_\ell).$$

Since $p^3 \mid \#A(K)_{\mathrm{tor}}$, $\mathfrak{p}^3 \mid \#\mathcal{A}_{/\mathbb{F}_\ell}(\mathbb{F}_\ell)$, as desired. □

Corollary 5.5.4. *Let A be a simple abelian subvariety of $J_0(N)$ with N prime. Suppose $\mathbb{T}_A$ is integrally closed. Suppose that for all Eisenstein primes $\mathfrak{p}$ of odd residue characteristic p with $A[\mathfrak{p}]$ nontrivial, $A[\mathfrak{p}] = J_0(N)[\mathfrak{p}]$, $\mathfrak{p}$ is principal, and there exists a rational prime $\ell \equiv 1 \pmod{p^2N}$ such that $p^3 \nmid \#\mathcal{A}_{/\mathbb{F}_\ell}(/\mathbb{F}_\ell)$. Then if $\varphi : A \to A'$ is an isogeny with $\operatorname{Supp}_{\mathbb{T}_A} \ker\varphi \subseteq \mathcal{P}_e$, then*

$$A' \cong A/M$$

with $\operatorname{Supp}_{\mathbb{T}_A}(M) \subseteq \mathcal{P}_e$ and $M[\mathfrak{p}^\infty] = (C_N \cap A)[p]$ or $(\Sigma_N \cap A)[p]$ for all $\mathfrak{p} \in \mathcal{P}_e$. Here C_N and Σ_N are the cuspidal and Shimura subgroups of $J_0(N)$.

Proof. We begin by simplifying φ so that we can apply Proposition 5.5.1. Suppose that for some $\mathfrak{p} \in \mathcal{P}_e$, $0 \neq A[\mathfrak{p}] \subseteq \ker\varphi$. By assumption, $\mathfrak{p}$ is principally generated by some $\alpha \in \mathbb{T}_A$. The isogeny φ now factors as $\varphi = \varphi' \circ \alpha$. We have $\operatorname{Im}\varphi' = \operatorname{Im}\varphi = A$ and the strict containment of kernels $\ker\varphi' \subsetneq \ker\varphi$. If needed, we can repeat this process, so we may assume that $\varphi' : A \to A'$ is an isogeny with $\operatorname{Supp}_{\mathbb{T}_A} \ker\varphi' \subseteq \mathcal{P}_e$ and $A[\mathfrak{p}] \not\subseteq \ker\varphi'$ for any $\mathfrak{p} \in \mathcal{P}_e$ with $A[\mathfrak{p}] \neq 0$.

Let $M = \ker\varphi'$. Now by Proposition 5.5.1, $M[\mathfrak{p}^\infty] \subsetneq A[\mathfrak{p}]$ so $M[\mathfrak{p}^\infty] = (C_N \cap A)[p]$ or $(\Sigma_N \cap A)[p]$ for all $\mathfrak{p} \in \mathcal{P}_e$. □

5.6 Combining Eisenstein and non-Eisenstein parts

Theorem 5.6.1. *Suppose A is a simple abelian subvariety of $J_0(N)$ with N prime. Suppose $\mathbb{T}_A$ is integrally closed and $\#\operatorname{Cl}(\mathbb{T}_A) = 1$. Suppose that for all Eisenstein primes $\mathfrak{p}$ of odd residue characteristic p with $A[\mathfrak{p}]$ nontrivial, $A[\mathfrak{p}] = J_0(N)[\mathfrak{p}]$, and there exists a rational* *prime* $\ell \equiv 1 \pmod{p^2N}$ *such that* $p^3 \nmid \#\mathcal{A}_{/\mathbb{F}_\ell}(/\mathbb{F}_\ell)$*. Then if* $\varphi : A \to A'$ *is an isogeny with* $\mathrm{Supp}_{\mathbb{T}_A} \ker \varphi \subseteq \mathcal{P}_e$*, then*

$$A' \cong A/M$$

with $\mathrm{Supp}_{\mathbb{T}_A}(M) \subseteq \mathcal{P}_e$ *and* $M[\mathfrak{p}^\infty] = (C_N \cap A)[p]$ *or* $(\Sigma_N \cap A)[p]$ *for all* $\mathfrak{p} \in \mathcal{P}_e$*. Here* C_N *and* Σ_N *are the cuspidal and Shimura subgroups of* $J_0(N)$*.*

Proof. Since $\mathbb{T}_A$ is principal, by Proposition 5.4.1, we have that $A' \cong A/X$ with X a $\mathbb{T}_A[G_\mathbb{Q}]$-submodule of $A(\overline{\mathbb{Q}})$ such that $\mathrm{Supp}_{\mathbb{T}_A} X \subseteq \mathcal{P}_e$. And now Corollary 5.5.4 yields the desired result. □

5.6.1 Computational Results

For $N \leq 100$, there are 34 simple abelian varieties satisfying the hypothesis of Theorem 5.6.1. In these cases, the hypothesis of Theorem 5.6.1 is satisfied. By applying isomorphism testing (Algorithm 3.7.2), on the result of Theorem 5.6.1, we have

Corollary 5.6.2. *Suppose* A *is a simple abelian subvariety of* $J_0(N)$ *with* $N < 100$ *and where the hypothesis of Theorem 5.6.1 holds. Then the odd-degree isogeny class of* A *is given by* $\{A, A/(\Sigma_N)_{\mathrm{odd}}, A/(C_N)_{\mathrm{odd}}\}$*. Here we are asserting that the elements of this set are pairwise non-isomorphic.*

Chapter 6

TABLES

Table 6.1: Table of nontrivial totally split Jacobians along with dimension and rank

N	dim	rank	N	dim	rank	N	dim	rank	N	dim	rank
11	1	0	38	4	0	80	7	0	198	29	3
14	1	0	40	3	0	84	11	0	200	19	1
15	1	0	42	5	0	90	11	0	216	25	1
17	1	0	44	4	0	96	9	0	240	37	1
19	1	0	45	3	0	99	9	1	288	33	2
20	1	0	48	3	0	100	7	0	300	43	1
21	1	0	49	1	0	108	10	0	336	53	3
22	2	0	50	2	0	112	11	1	360	57	1
24	1	0	52	5	0	114	17	2	384	49	6
26	2	0	54	4	0	120	17	0	396	61	6
27	1	0	56	5	0	121	6	1	400	43	5
28	2	0	57	5	1	128	9	1	432	55	5
30	3	0	60	7	0	132	19	0	576	73	9
32	1	0	64	3	0	144	13	0	600	97	7
33	3	0	66	9	0	150	19	0	720	121	8
34	3	0	72	5	0	168	25	0	1152	161	32
36	1	0	75	5	0	180	25	0	1200	205	28
37	2	1	76	8	0	192	21	1			

Table 6.2: Bound on $[J_0(N)(\mathbb{Q})_{\text{tor}} : C(N)(\mathbb{Q})]$

N	bound	N	bound
84	8	144	64
90	16	150	16
96	64	168	512
120	512	180	128
132	32		

BIBLIOGRAPHY

[AS05] Agashe Agashe and William Stein, *Visible evidence for the Birch and Swinnerton-Dyer conjecture for modular abelian varieties of analytic rank zero*, Math. Comp. **74** (2005), no. 249, 455–484 (electronic), With an appendix by J. Cremona and B. Mazur, http://wstein.org/papers/shacomp/. MR 2085902

[BCDT01] C. Breuil, B. Conrad, F. Diamond, and R. Taylor, *On the modularity of elliptic curves over* $\mathbf{Q}$*: wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001), no. 4, 843–939 (electronic), http://math.stanford.edu/~conrad/papers/tswfinal.pdf. MR 2002d:11058

[BS96] Armand Brumer and Joseph H. Silverman, *The number of elliptic curves over* $\mathbf{Q}$ *with conductor* N, Manuscripta Math. **91** (1996), no. 1, 95–102. MR 1404420

[CS86] Gary Cornell and Joseph H. Silverman (eds.), *Arithmetic geometry*, Springer-Verlag, New York, 1986, Papers from the conference held at the University of Connecticut, Storrs, Connecticut, July 30–August 10, 1984. MR 89b:14029

[DS05] Fred Diamond and Jerry Shurman, *A first course in modular forms*, Graduate Texts in Mathematics, vol. 228, Springer-Verlag, New York, 2005.

[Eme03] Matthew Emerton, *Optimal quotients of modular Jacobians*, Math. Ann. **327** (2003), no. 3, 429–458. MR 2021024 (2005g:11100)

[Har77] R. Hartshorne, *Algebraic Geometry*, Springer-Verlag, New York, 1977, Graduate Texts in Mathematics, No. 52.

[Hel07] David Helm, *On maps between modular Jacobians and Jacobians of Shimura curves*, Israel J. Math. **160** (2007), 61–117. MR 2342491

[Kat81] N. M. Katz, *Galois properties of torsion points on abelian varieties*, Invent. Math. **62** (1981), no. 3, 481–502. MR 82d:14025

[Kem73] George Kempf, *On the geometry of a theorem of Riemann*, Ann. of Math. (2) **98** (1973), 178–185. MR 0349687

[KP18] Krzysztof Klosin and Mihran Papikian, *On Ribet's isogeny for $J_0(65)$*, Proc. Amer. Math. Soc. **146** (2018), no. 8, 3307–3320. MR 3803657

[LB92] Herbert Lange and Christina Birkenhake, *Complex abelian varieties*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 302, Springer-Verlag, Berlin, 1992. MR 1217487

[Lin95] San Ling, *Shimura subgroups and degeneracy maps*, J. Number Theory **54** (1995), no. 1, 39–59. MR 1352635

[Lin97] ———, *On the $\mathbf{Q}$-rational cuspidal subgroup and the component group of $J_0(p^r)$*, Israel J. Math. **99** (1997), 29–54. MR 1469086

[LO91] San Ling and Joseph Oesterlé, *The Shimura subgroup of $J_0(N)$*, Astérisque (1991), no. 196-197, 6, 171–203 (1992), Courbes modulaires et courbes de Shimura (Orsay, 1987/1988). MR 1141458

[Mar05] Greg Martin, *Dimensions of the spaces of cusp forms and newforms on $\Gamma_0(N)$ and $\Gamma_1(N)$*, J. Number Theory **112** (2005), no. 2, 298–331. MR 2141534

[Maz77] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. (1977), no. 47, 33–186 (1978), http://archive.numdam.org/article/PMIHES_1977__47__33_0.pdf.

[Miy73] Isao Miyawaki, *Elliptic curves of prime power conductor with $\mathbf{Q}$-rational points of finite order*, Osaka J. Math. **10** (1973), 309–323. MR 0327776

[Oht14] Masami Ohta, *Eisenstein ideals and the rational torsion subgroups of modular Jacobian varieties II*, Tokyo J. Math. **37** (2014), no. 2, 273–318. MR 3304683

[Ren18] Yuan Ren, *Rational torsion subgroups of modular Jacobian varieties*, J. Number Theory **190** (2018), 169–186. MR 3805452

[Rib75] K. A. Ribet, *Endomorphisms of semi-stable abelian varieties over number fields*, Ann. Math. (2) **101** (1975), 555–562. MR 51 #8120

[Rib90] ———, *Raising the levels of modular representations*, Séminaire de Théorie des Nombres, Paris 1987–88, Birkhäuser Boston, Boston, MA, 1990, http://math.berkeley.edu/~ribet/Articles/dpp.pdf, pp. 259–271.

[Rib91a] Kenneth A. Ribet, *Multiplicities of p-finite mod p Galois representations in $J_0(Np)$*, Bol. Soc. Brasil. Mat. (N.S.) **21** (1991), no. 2, 177–188. MR 1139564

[Rib91b] ———, *The old subvariety of $J_0(pq)$*, Arithmetic algebraic geometry (Texel, 1989), Progr. Math., vol. 89, Birkhäuser Boston, Boston, MA, 1991, pp. 293–307. MR 1085264

[Rib97] ———, *Images of semistable Galois representations*, Pacific J. Math. (1997), no. Special Issue, 277–297, Olga Taussky-Todd: in memoriam. MR 1610883

[RS01] K. A. Ribet and W. A. Stein, *Lectures on Serre's conjectures*, Arithmetic algebraic geometry (Park City, UT, 1999), IAS/Park City Math. Ser., vol. 9, Amer. Math. Soc., Providence, RI, 2001, http://wstein.org/papers/serre/, pp. 143–232. MR 2002h:11047

[Sag19] The Sage Development Team, *Sage Mathematics Software (Version 8.6)*, 2019, http://www.sagemath.org.

[Set75] Bennett Setzer, *Elliptic curves of prime conductor*, J. London Math. Soc. (2) **10** (1975), 367–378. MR 0371904

[Shi94] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Princeton University Press, Princeton, NJ, 1994, Reprint of the 1971 original, Kan Memorial Lectures, 1.

[ST68] J-P. Serre and J. T. Tate, *Good reduction of abelian varieties*, Ann. of Math. (2) **88** (1968), 492–517.

[Ste82] G. Stevens, *Arithmetic on modular curves*, Birkhäuser Boston Inc., Boston, Mass., 1982. MR 87b:11050

[Ste89] ———, *Stickelberger elements and modular parametrizations of elliptic curves*, Invent. Math. **98** (1989), no. 1, 75–106. MR 90m:11089

[Ste00] W. A. Stein, *Explicit approaches to modular abelian varieties*, Ph.D. thesis, University of California, Berkeley (2000).

[Ste07] William Stein, *Modular Forms, A Computational Approach*, Graduate Studies in Mathematics, vol. 79, American Mathematical Society, Providence, RI, 2007, With an appendix by Paul E. Gunnells, http://wstein.org/books/modform/. MR 2289048

[SW04] William Stein and Mark Watkins, *Modular parametrizations of Neumann-Setzer elliptic curves*, Int. Math. Res. Not. (2004), no. 27, 1395–1405. MR 2052021 (2005c:11070)

[TW95] R. Taylor and A. J. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. of Math. (2) **141** (1995), no. 3, 553–572.

[Vat05] V. Vatsal, *Multiplicative subgroups of $J_0(N)$ and applications to elliptic curves*, J. Inst. Math. Jussieu **4** (2005), no. 2, 281–316. MR 2135139

[Wil95] A. J. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) **141** (1995), no. 3, 443–551.

[Yoo16] Hwajong Yoo, *Rational torsion points on Jacobians of modular curves*, Acta Arith. **172** (2016), no. 4, 299–304. MR 3471044