**Title**

Computations in Arithmetic Geometry: Computing with Jacobians of Shimura curves: point counts and isogeny decomposition via trace formula and Censuses of low-genus curves over small finite fields



**ISBN**

9798252435640

**Author**

Huang, Yongyuan

**Publication Date**

2026-06-19

Peer reviewed|Thesis/dissertation

UNIVERSITY OF CALIFORNIA SAN DIEGO

# Computations in Arithmetic Geometry: Computing with Jacobians of Shimura curves: point counts and isogeny decomposition via trace formula and Censuses of low-genus curves over small finite fields

A dissertation submitted in partial satisfaction of the
requirements for the degree Doctor of Philosophy

in

Mathematics

by

Yongyuan Huang

Committee in charge:

Professor Kiran Kedlaya, Chair
Professor Alina Bucur
Professor Nadia Heninger
Professor Aaron Pollack
Professor John Voight

2026

The Dissertation of Yongyuan Huang is approved, and it is acceptable in quality and form for publication on microfilm and electronically.

University of California San Diego

2026

DEDICATION

To my mother, Hui Yang, and to all those who have always unwaveringly supported and believed in me.

TABLE OF CONTENTS

LIST OF TABLES

ACKNOWLEDGEMENTS

The journey of pursuing a doctoral degree in any discipline is never smooth sailing; it requires a tremendous amount of patience, resilience, dedication, and most importantly, honest hard work from many people to reach each milestone along the way. I would like to express my deepest and most sincere gratitude to my advisors Professor Kiran Kedlaya and Professor John Voight for their generosity with their time and ideas, their mathematical wisdom, and their constant support and guidance. Kiran has taught me everything from the very basics of algebraic number theory to the cutting-edge frontier of condensed mathematics, which I still frankly understand only a little. Through countless conversations with Kiran, I have learned how to think about and structure large-scale computations in number theory and how to develop efficient algorithms. I am very grateful for his patience with my questions, no matter how repetitive or trivial they may have been. John (including his encyclopedic book on quaternion algebras and many papers) has taught me everything that I know about Shimura curves and what it means to "compute" modular forms. I am especially grateful for his willingness to advise me on a very interesting and educationally rewarding project despite being 7500 miles away from San Diego.

I feel compelled to acknowledge that my participation in various conferences and workshops that were made possible by funding from the Simons Collaboration on Arithmetic Geometry, Number Theory, and Computation (of which Professor John Voight was PI and Professor Kiran Kedlaya was an affiliated scientist) played a significant role in shaping my research interest and fostering mathematical development. In fact, Part I of this thesis originated from the Shimura Curves in the LMFDB workshop held at Dartmouth College (organized by Professor John Voight and others) in February 2024, and Part II of this thesis is based on a collaboration started after and inspired by Professor Kiran Kedlaya's presentation at the first LMFDB, Computation, and Number Theory conference held in July 2023. It is my strong belief that in-person attendance at well-curated workshops and conferences is severely undervalued for a graduate student's growth; I sincerely hope that future graduate students will be provided with similar privileges and opportunities despite the macroeconomic and political headwinds facing academia.

I would like to thank my committee members, Professor Alina Bucur, Professor Nadia Heninger, and Professor Aaron Pollack, other faculty members of the UCSD number theory and algebraic geometry group, and my fellow graduate students for the irreplaceable role that they have played in my mathematical education. I also thank Eran Assaf, Edgar Costa, Jack J Garzella, and David Roe for numerous helpful conversations about computations in arithmetic geometry. It has been a number of years since I have graduated from Boston University, but I am indebted to some of the current and former members of the Boston University number theory group (Jennifer Balakrishnan, Li-Mei Lim, Anna Medvedovsky, Robert Pollack, David Rohrlich, Glenn Stevens, and Jared Weinstein) for inspiring and encouraging me to pursue arithmetic geometry at the research level.

I am very grateful to my mother for her constant unconditional trust and support throughout my life; I am also grateful to my family, my friends, and my cat for always being there when I needed them the most. I will refrain from listing a long list of names, but you know who you are, and I cannot imagine finishing this degree without your presence.

Part I is, in part, being prepared for submission for publication. The dissertation author is the collaborator and the coauthor for the material below.

- Yongyuan Huang, John Voight "Computing with Jacobians of Shimura curves: point counts and isogeny decomposition via trace formula".

Part II is, in part, being prepared for submission for publication, and, in part, includes material that is already in publication. The dissertation author is the collaborator and the coauthor for the material below.

- Yongyuan Huang, Kiran S. Kedlaya, Jun Bo Lau, "A census of genus 6 curves over $\mathbb{F}_2$," accepted to LuCaNT 2025.

- Yongyuan Huang, Kiran S. Kedlaya, Jun Bo Lau, "A census of genus 5 curves over $\mathbb{F}_3$ and genus 7 curves over $\mathbb{F}_2$."

I would like to thank all of my collaborators for many helpful conversations and for allowing me to include the material in this dissertation.

## VITA

| | |
|---|---|
| 2022 | Bachelor of Arts with Honors in Mathematics, Boston University |
| 2022 | Master of Arts in Mathematics, Boston University |
| 2022-2026 | Graduate Teaching Assistant, Department of Mathematics, University of California San Diego |
| 2026 | Doctor of Philosophy in Mathematics, University of California San Diego |

## PREPRINTS & PUBLICATIONS

- Yongyuan Huang, Kiran S. Kedlaya, Jun Bo Lau, "A census of genus 6 curves over $\mathbb{F}_2$," in LuCaNT: Databases, Algorithms, and Computational Number Theory, Contemporary Mathematics, vol. 840, Amer. Math. Soc., Providence, RI, 2026, pp. 213-227.
- Ryan Batubara, Jack Garzella, Yongyuan Huang, and Maximus Mellberg, "Newton strata realization for hypersurfaces via explicit p-adic cohomology," provisionally accepted to the Seventeenth Algorithmic Number Theory Symposium.
- Yongyuan Huang, John Voight "Computing with Jacobians of Shimura curves: point counts and isogeny decomposition via trace formula".
- Yongyuan Huang, Kiran S. Kedlaya, Jun Bo Lau, "A census of genus 5 curves over $\mathbb{F}_3$ and genus 7 curves over $\mathbb{F}_2$."

ABSTRACT OF THE DISSERTATION

**Computations in Arithmetic Geometry: Computing with Jacobians of Shimura curves: point counts and isogeny decomposition via trace formula and Censuses of low-genus curves over small finite fields**

by

Yongyuan Huang

Doctor of Philosophy in Mathematics

University of California San Diego, 2026

Professor Kiran Kedlaya, Chair

In Part I, we provide an explicit version of the Eichler–Selberg trace formula for Shimura curves with level structure over the rationals. As an application, we provide an algorithm to compute the isogeny decomposition of the Jacobian of Shimura curves into modular abelian varieties using the method that Rouse–Sutherland–Zureick-Brown developed for classical modular curves. We also give a trace formula for definite quaternionic modular forms over the rationals.

In Part II, we compile a complete list of isomorphism class representatives of curves of genus 6 over $\mathbb{F}_2$. We use explicit descriptions of canonical curves in each stratum of

the Brill–Noether stratification of the moduli space $\mathcal{M}_6$, due to Mukai in the generic case. Our computed value of $\#\mathcal{M}_6(\mathbb{F}_2)$ agrees with the Lefschetz trace formula as recently computed by Bergstrom–Canning–Petersen–Schmitt. We also report progress on compiling a corresponding list in genus 7 over $\mathbb{F}_2$ (for which explicit descriptions of canonical curves in each stratum of the Brill–Noether stratification of the moduli space $\mathcal{M}_7$ are also available) and genus 5 over $\mathbb{F}_3$, where the censuses are complete in all except for the generic stratum in both cases.

# Introduction

Number theory is a discipline with a long and rich history rooted in computation and data collection, from the Plimpton 322 clay tablet of the Babylonians (c. 1800 BC), which lists Pythagorean triples, and Gauss's tables of equivalence classes of binary quadratic forms (now known as class groups) in the 19th century, to the formulation of the Birch–Swinnerton-Dyer conjecture [14] in the 1960s based on computations performed on EDSAC 2, and, more recently, to modern databases such as the *L-functions and Modular Forms Database (LMFDB)* [62], whose data are partly computed on high performance clusters such as Google Cloud. On the one hand, the availability of large datasets enables the formulation of conjectures and provides a testing ground for them; on the other hand, the development of effective (and in some cases efficient) algorithms for computing explicit examples is of independent interest and often requires substantial ingenuity. Rapid improvements in the efficiency and accessibility of both hardware and software over the past three decades have substantially advanced the arithmetic geometry community's sustained interest in explicit computation, enabling computations at scales that were previously unattainable. In this context, the present thesis represents a very modest contribution, both in developing new theoretical results and computational techniques, as well as in supplying data that may inform future investigations.

Problems in algorithmic and computational algebraic number theory/arithmetic geometry can be, broadly speaking, divided into five categories.

1. The method for computing certain objects exists both in principle and in practice

but may require careful engineering when running the computation at scale.

2. We know how to compute something in practice, but new mathematical theorems need to be proven to fully justify the computation.

3. We know how to compute something both in principle and in practice, but there is no known efficient (polynomial time on input size) algorithm.

4. An (efficient) algorithm exists in principle but not in practice (i.e. there is no known effective implementation available).

5. No algorithm (either in principle or in practice) is known for how to compute certain objects.

Parts I and II of this thesis fall primarily under categories 2 and 1, respectively. We now proceed, in light of this distinction, to give an overview of the problems addressed in this thesis, with particular emphasis on their place within the broader context of computations in arithmetic geometry. Part I of this thesis is motivated by the problem of computing the isogeny decomposition of the Jacobians of Shimura curves over the rationals into modular abelian varieties indexed by newforms, modeled after a similar procedure for classical modular curves developed by Rouse–Sutherland–Zureick-Brown [78, Section 6]. Modular curves are moduli spaces of elliptic curves with certain level structures, and many aspects of their theory have been extensively studied in the past century. Classical modular forms can be viewed as sections of certain line bundles over modular curves; computations with classical modular forms provide the most direct access to carry out explicit computations on modular curves (e.g. computing their models and the $j$-invariant map). Shimura curves, which parametrize certain abelian surfaces with extra endomorphisms, are the Shimura varieties that most closely parallel modular curves. However, the development of computational methods for Shimura curves and quaternionic modular forms (the analogues of classical modular forms in this setting) has lagged behind that for modular curves and classical modular forms. The key new result in Part I is a precise and explicitly computable trace formula for the action of Hecke operators acting on spaces of quaternionic modular forms of arbitrary level and weight in terms of purely group-theoretic data; similar results are known for classical modular forms, see, e.g., [78, Section 5]. In fact, the trace formulas for classical modular forms played a paramount role in the systematic tabulation of modular forms; see [12, Section 2] and the references therein.

Part II of this thesis is motivated by the study of moduli spaces of curves and the Torelli locus inside the moduli spaces of abelian varieties over finite fields, as well as the tabulations thereof inside the LMFDB. The study of curves, abelian varieties, and their moduli spaces is of vital interest in arithmetic geometry; these objects are especially suitable for computations and data tabulations when the genus of the curves (resp. the dimension of the abelian varieties) and the cardinality of the finite fields are small. Work of Kedlaya [55] enables the enumeration of Weil polynomials, so one can in principle enumerate isogeny classes of abelian varieties of arbitrary dimension over arbitrary finite fields as a consequence of the theorems of Honda [43] and Tate [86]. However, there are no known effective methods to enumerate isogeny or isomorphism classes of curves for genus $g \geq 8$. The enumeration of isomorphism classes of curves even in lower genera requires a careful analysis of the corresponding moduli. In Part II, we discuss our work on building a census of curves of genus 6 and 7 over $\mathbb{F}_2$, building on Mukai's explicit stratification of the moduli space of curves of genus 6 and 7 and the partial census carried out in [59]; we also conduct a census of curves of genus 5 over $\mathbb{F}_3$. Our data can be used to fill existing gaps in the abelian varieties over finite fields section of the LMFDB and to answer questions concerning properties of curves over finite fields that are not yet theoretically understood; furthermore, our work has implications for the study of polynomial point counts of moduli spaces of curves over finite fields.

# Part I

# Computing with Jacobians of Shimura curves: point counts and isogeny decomposition via trace formula

# Chapter 1

# Preliminaries

## 1.1 Quaternion Algebras

We recall the relevant concepts and facts from the theory of quaternion algebra that we need for our purpose here, and refer the reader to [91] for more thorough discussions of many quaternion-related ideas.

A *quaternion algebra* $B$ over $\mathbb{Q}$ is a central simple $\mathbb{Q}$-algebra of dimension 4; equivalently, there are elements $i, j \in B$ such that

$$B \cong \mathbb{Q}\langle i, j, ij \rangle,$$

where $i^2 = a, j^2 = b, ij = -ji$, and $a, b \in \mathbb{Q}^\times$. In this case, we denote $B$ by $\left(\frac{a,b}{\mathbb{Q}}\right)$. An *order* $O$ in $B$ is a rank 4 $\mathbb{Z}$-lattice which is also a subring; a *maximal order* in $B$ is an order that is not properly contained in any other orders.

For each place $v$ of $\mathbb{Q}$ (including the infinite place), we say $B$ is *split* at $v$ if the completion $B \otimes_{\mathbb{Q}} \mathbb{Q}_v \cong M_2(\mathbb{Q}_v)$, and otherwise we say $B$ is *ramified* at $v$, in which case the completion $B \otimes_{\mathbb{Q}} \mathbb{Q}_v$ is a $\mathbb{Q}_v$-division algebra. We say $B$ is *indefinite* if $B$ is unramified at $v = \infty$, and otherwise we say $B$ is *definite*; equivalently, $B$ is indefinite if $B \otimes_{\mathbb{Q}} \mathbb{R} \cong M_2(\mathbb{R})$ and $B$ is definite if $B \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{H} := (-1, -1|\mathbb{R})$. The matrix ring $M_2(\mathbb{Q})$ is perhaps the most well-known example of an indefinite quaternion algebra. The *discriminant* of $B$, denoted by $\mathrm{disc}(B)$, is the product of all ramified places of $B$, which uniquely determines $B$ up to isomorphism. It is a standard fact that the set of ramified places of $B$ has even cardinality.

If $I \subseteq B$ is a lattice, we define its *right order* to be

$$O_R(I) \coloneqq \{\alpha \in B : I\alpha \subseteq I\}.$$

The *left order* $O_L(I)$ can be defined analogously. We say $I$ is *invertible* if there is a two-sided inverse $I' \subseteq B$ such that $II' = O_L(I) = O_R(I')$ and $I'I = O_R(I) = O_L(I')$. Two lattices $I, J \subseteq B$ are in the same right class, denoted by $I \sim_R J$, if there exists an $\alpha \in B^\times$ such that $\alpha I = J$; equivalently, $I$ and $J$ are isomorphic as right $O_R(I) = O_R(J)$-modules. We denote the class of a lattice $I$ by $[I]_R$. Fix an order $O$ in $B$. We define the *right class set* of $O$ to be

$$\mathrm{Cls}\, O = \mathrm{Cls}_R\, O \coloneqq \{[I]_R : I \subseteq B \text{ invertible and } O_R(I) = O\}.$$

It is a fact that $\#\,\mathrm{Cls}\, O$ is finite, and we refer to $\#\,\mathrm{Cls}\, O$ as the *class number of* $O$.

## 1.2 Optimal embeddings

In the sections below, we will frequently consider how orders in an imaginary quadratic field embed into orders in a quaternion algebra. We briefly recall the setup and the results we will use here. We refer the curious readers to [91, Chapter 30] for further details. Let $R$ be a Dedekind domain with $F = \mathrm{Frac}\, R$, and $B$ a quaternion algebra over $F$. (For our applications, it suffices to consider $R = \mathbb{Z}$ and $F = \mathbb{Q}$, or more generally $F$ a totally real field and $R = \mathbb{Z}_F$ its ring of integers.) Let $K \supset F$ be a separable quadratic field extension. Suppose $K \hookrightarrow B$. By the Skolem-Noether theorem, the set of embeddings $K \hookrightarrow B$ can be identified with $K^\times \backslash B^\times$. Let $S \subseteq K$ be a quadratic $R$-order and let $O \subseteq B$ be a quaternion $R$-order. An $R$-algebra embedding $\varphi : S \hookrightarrow O$ is *optimal* if $\varphi(K) \cap O = \varphi(S)$, where $\varphi$ extends to an embedding $\varphi : K \hookrightarrow B$ by extension of scalars. Optimality is a local property by the local-global dictionary for lattices. Let $\mathrm{Emb}(S, O) := \{\text{optimal } S \hookrightarrow O\}$. Define

$$E = E_S = E_{S,O} := \{\beta \in B^\times : \beta^{-1} K \beta \cap O = \beta^{-1} S \beta\}.$$

We have a bijection of sets $K^\times \backslash E \cong \mathrm{Emb}(S, O)$. Let $O^1 \subseteq \Gamma \subseteq N_{B^\times}(O)$. We have a right action of $\Gamma$ on $\mathrm{Emb}(S, O)$ via conjugation as follows: for $\gamma \in \Gamma$, $\varphi \in \mathrm{Emb}(S, O)$, and $\alpha \in S$, $(\gamma \cdot \varphi)(\alpha) := \gamma^{-1}\varphi(\alpha)\gamma$. Let $\mathrm{Emb}(S, O; \Gamma) := \{\Gamma\text{-conjugacy classes of optimal } S \hookrightarrow O\}$. There is a bijection $K^\times \backslash E/\Gamma \cong \mathrm{Emb}(S, O; \Gamma)$ given by $\beta \mapsto \varphi_\beta$, where $\varphi_\beta(\alpha) = \beta^{-1}\alpha\beta$ for $\alpha \in S$. Let $m(S, O; \Gamma) := \#\,\mathrm{Emb}(S, O; \Gamma)$. We refer to the quantity $m(S, O; \Gamma)$ as the number of *global* embeddings. The above discussion carries over if we replace each object by its adelic completion, and we refer to $m(\widehat{S}, \widehat{O}; \widehat{\Gamma}) := \#\,\mathrm{Emb}(\widehat{S}, \widehat{O}; \widehat{\Gamma})$ as the number of *local* embeddings. The number of local and global embeddings is related by a trace formula, c.f. [91, Theorem 30.4.7]. For $O$ maximal, $m(\widehat{S}, \widehat{O}; \widehat{O}^\times)$ can be explicitly computed as follows.

**Lemma 1.2.1.** *Let $R$ be a complete DVR with maximal ideal $\mathfrak{p} = \pi R$, and $S$ an $R$-order with* $\mathrm{Frac}(S) = K$*, a quadratic field. We have*

1. *We have $m(S, M_2(R); \mathrm{GL}_2(R)) = 1$, canonically given by the regular representation of $S$ on itself in the basis $\{1, \gamma\}$ sending*

$$\gamma \mapsto \begin{pmatrix} 0 & -N(\gamma) \\ 1 & \mathrm{Tr}(\gamma) \end{pmatrix}.$$

2. *Suppose $B$ is a division algebra and $O \subseteq B$ its division ring. If $S = R_K$ is integrally*

*closed, then* $m(S, O; O^\times) = 1 - \left(\frac{K}{\mathfrak{p}}\right)$*, where*

$$\left(\frac{K}{\mathfrak{p}}\right) = \begin{cases} 1 & \text{if } \mathfrak{p} \text{ splits completely in } K, \\ 0 & \text{if } \mathfrak{p} \text{ ramifies in } K, \\ -1 & \text{if } \mathfrak{p} \text{ is inert in } K. \end{cases}$$

*In particular, if* $\mathrm{char}(R/\mathfrak{p})$ *is odd and* $K \cong \mathbb{Q}[x]/(x^2 - d)$*, then*

$$\left(\frac{K}{\mathfrak{p}}\right) = \left(\frac{d}{\mathfrak{p}}\right).$$

*If* $S$ *is not integrally closed, then* $\mathrm{Emb}(S, O) = \emptyset$*.*

*Proof.* See [91, Prop. 30.5.3] and its proof. □

**Corollary 1.2.2.** *Let* $B/\mathbb{Q}$ *be a quaternion algebra of discriminant* $D$*,* $O \le B$ *a maximal order,* $K/\mathbb{Q}$ *be a quadratic field, and* $S \subseteq K$ *a quadratic order of conductor* $f := [\mathbb{Z}_K : S]$*. We have*

$$m(\widehat{S}, \widehat{O}; \widehat{O}^\times) = \begin{cases} \prod_{p|D} \left(1 - \left(\frac{K}{p}\right)\right) & \text{if } (D, f) = 1, \\ 0 & \text{if } (D, f) > 1. \end{cases}$$

*Proof.* This follows immediately from Lemma 1.2.1. □

## 1.3 Shimura curves as quotients of the upper half plane and quaternionic modular forms

The goal of this section is to give the classical complex analytic description of Shimura curves. As opposed to directly stating the definition, we start with the general adelic description. Our main reference is [27, §7].

Let $B$ be a quaternion algebra over $\mathbb{Q}$ of discriminant $D$ and $O$ be a maximal order in $B$. Throughout, for any $\mathbb{Z}$-module $M$, let $\widehat{M} := M \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}}$. Fix an open compact subgroup

$\widehat{H} \leq \widehat{O}^\times$ of level $N$ with $(D, N) = 1$ that is *locally norm-maximal*, i.e. $\mathrm{nrd}(\widehat{H}) = \widehat{\mathbb{Z}}^\times$. Let $r = 0$ if $B$ is definite and $r = 1$ otherwise, i.e.

$$B \hookrightarrow B_\infty \cong M_2(\mathbb{R})^r \times \mathbb{H}^{1-r}.$$

Let $\mathcal{H}^\pm$ be the union of the upper and lower half planes. The group $B_\infty^\times$ acts on $(\mathcal{H}^\pm)^r$ on the right transitively with the stabilizer of $(i, \ldots, i) \in \mathcal{H}^r$ being

$$K_\infty \coloneqq (\mathbb{R}^\times \mathrm{SO}_2(\mathbb{R}))^r \times (\mathbb{H}^\times)^{1-r}.$$

**Definition 1.3.1.** We define the *quaternionic Shimura variety* of level $\widehat{H}$ associated to $B$ as the double coset

$$X^B_{\widehat{H}}(\mathbb{C}) \coloneqq B^\times \backslash (B_\infty^\times / K_\infty \times \widehat{B}^\times / \widehat{H}) = B^\times \backslash ((\mathcal{H}^\pm)^r \times \widehat{B}^\times / \widehat{H}).$$

The set $X^B_{\widehat{H}}(\mathbb{C})$ can be equipped with the structure of a complex Riemannian manifold of dimension $r$.

To further unpack this definition, we consider two cases, depending on whether $B$ is indefinite or definite.

First, suppose $B$ is indefinite, in which case the Shimura variety $X^B_{\widehat{H}}(\mathbb{C})$ is also known as the *Shimura curve* of level $\widehat{H}$. Let $\iota : B \to M_2(\mathbb{R})$ be the splitting at the real place. For $\gamma \in B^\times$, if $\iota(\gamma) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, by abuse of notation, we let $\det(\gamma) \coloneqq \det(\iota(\gamma)) = ad - bc$. The group

$$B_+^\times \coloneqq \{\gamma \in B^\times : \det(\gamma) > 0\}$$

acts on $\mathcal{H}$ by linear fractional transformation via $\iota(\gamma)$. We denote this action by $\gamma z$ for $\gamma \in B_+^\times$ and $z \in \mathcal{H}$, again by abuse of notation. Since we also have $B^\times / B_+^\times \cong \mathbb{Z}/2\mathbb{Z}$, we may identify

$$X^B_{\widehat{H}}(\mathbb{C}) = B^\times_+\backslash(\mathcal{H} \times \widehat{B}^\times/\widehat{H}).$$

By strong approximation, the reduced norm map

$$\mathrm{nrd} : B^\times_+\backslash\widehat{B}^\times/\widehat{H} \to \mathbb{Q}^\times_+\backslash\widehat{\mathbb{Q}}^+/\widehat{\mathbb{Z}}^\times \cong \mathrm{Cl}^+\,\mathbb{Z}$$

is a bijection. Since the narrow class group of $\mathbb{Z}$ is trivial, putting $\Gamma_{\widehat{H}} := \widehat{H} \cap B^\times_+$, we conclude that $X^B_{\widehat{H}}(\mathbb{C}) = \Gamma_{\widehat{H}}\backslash\mathcal{H}$.

With the same notation, we can also define the corresponding modular forms.

**Definition 1.3.2.** Suppose $B \neq M_2(\mathbb{Q})$ is indefinite and $k \in \mathbb{Z}_{>0}$ with $k \geq 0$. We define the space of *quaternionic modular forms* for $B$ of weight $k$ and level $\widehat{H}$, denoted by $M^B_2(\widehat{H})$, to be the set of holomorphic functions $f : \mathcal{H} \to \mathbb{C}$ such that

$$(f|\gamma)(z) := f(\gamma z)\frac{(\det\gamma)^{k-1}}{(cz+d)^k} = f(z)$$

for all $\gamma \in \Gamma_{\widehat{H}}$. When $B \neq M_2(\mathbb{Q})$, since the Shimura curve $X^B_{\widehat{H}}(\mathbb{C})$ has no cusps, we define the space of cusp forms to be $S^B_k(\widehat{H}) := M^B_k(\widehat{H})$.

Now suppose $B$ is definite; the Shimura variety $X^B_{\widehat{H}}(\mathbb{C}) = B^\times\backslash\widehat{B}^\times/\widehat{H}$ is a finite set, which one may view as a zero-dimensional Deligne-Mumford stack. In particular, each double coset has a finite stabilizer group.

**Definition 1.3.3.** Suppose $B$ is definite. We define the space of *quaternionic modular forms* for $B$ of weight 2 and level $\widehat{H}$, denoted by $M^B_2(\widehat{H})$, to be the set of functions

$$f : \widehat{B}^\times/\widehat{H} \to \mathbb{C} \text{ such that } f(\gamma\widehat{\alpha}\widehat{H}) = f(\widehat{\alpha}\widehat{H}) \text{ for all } \gamma \in B^\times;$$

equivalently, it is the set of functions

$$f : B^\times \backslash \widehat{B}^\times / \widehat{H} \to \mathbb{C}.$$

*Remark* 1.3.4. When $\widehat{H} = \widehat{O}^\times$, since $B^\times \backslash \widehat{B}^\times / \widehat{O}^\times \cong \mathrm{Cls}(O)$, the right ideal class set of $O$, we recover the classical definition of $M_2^B(\widehat{O}^\times) = \mathrm{Map}(\mathrm{Cls}(O), \mathbb{C})$.

*Remark* 1.3.5. The definition of quaternionic modular forms can be extended to higher weights in both the indefinite and definite case; one can also extend the base field of $B$ from $\mathbb{Q}$ to any totally real field. There is also an adelic description of quaternionic modular forms in the indefinite case. Interested readers are encouraged to consult [27, §7-9].

## 1.4 Hecke operators

As in the classical modular curve case, there are Hecke correspondences on quaternionic Shimura varieties which give rise to linear Hecke operators on the associated spaces of quaternionic modular (and cusp) forms.

For $\widehat{\pi} \in \widehat{B}^\times$, the spaces $M_2^B(\widehat{H})$ and $S_2^B(\widehat{H})$ are equipped with the action of pairwise commuting diagonalizable *Hecke operators* $T_{\widehat{\pi}}$ as follows. We write

$$\widehat{H}\widehat{\pi}\widehat{H} = \bigsqcup_j \widehat{H}\widehat{\pi}_j \tag{1.1}$$

as a finite disjoint union. Suppose $B$ is indefinite. By strong approximation, for each $\widehat{\pi}_j$, there exists $\varpi_j \in B^\times$ such that

$$\widehat{\pi}_j^{-1}\widehat{O}\widehat{\pi} \cap B = \varpi_j^{-1}O. \tag{1.2}$$

For $f \in M_2^B(\widehat{H})$, we define

$$(T_{\widehat{\pi}} f)(z) := \sum_j (f|\varpi_j)(z). \tag{1.3}$$

When $B$ is definite, for $f \in M_2^B(\widehat{H})$, we define

$$(T_{\widehat{\pi}} f)(\widehat{\alpha}\widehat{H}) := \sum_j f(\widehat{\alpha}\widehat{\pi}_j^{-1}\widehat{H}). \tag{1.4}$$

For a rational prime $p \nmid DN$, we denote by $T_p$ the Hecke operator $T_{\widehat{\pi}}$ where $\widehat{\pi} \in \widehat{B}^\times$ is such that $\widehat{\pi}_v = 1$ for $v \neq p$ and $\widehat{\pi}_p = \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \in O \otimes_{\mathbb{Z}} \mathbb{Z}_p \cong M_2(\mathbb{Z}_p)$. By multiplicativity of the Hecke operators, this definition extends to all $n \in \mathbb{N}$ with $(n, DN) = 1$.

# Chapter 2

# Trace formula for quaternionic modular forms

## 2.1 Introduction

### 2.1.1 Motivation

Classical modular curves and Shimura curves play parallel roles in the arithmetic of automorphic forms, but the available computational tools and data are far more developed for the former than for the latter. For modular curves, the *L-functions and Modular Forms Database (LMFDB)* [62] has seen a substantial ongoing effort to tabulate data for arbitrary congruence subgroups. Although comparable data for Shimura curves is lacking, the modular curve case nevertheless provides both a model and a benchmark for what one would like to achieve in the setting of Shimura curves.

A central algorithmic task for modular curves is the efficient computation of point counts over finite fields. These counts have several arithmetic applications: they can be used to test for local obstructions to rational points, to compute zeta functions over finite fields, and, crucially, to determine the isogeny decomposition of the Jacobian into modular abelian varieties indexed by classical newforms, as exhibited by Rouse–Sutherland–Zureick-Brown [78, section 6]. To count points, they provide an algorithmic form of the Eichler–Selberg trace formula [78, section 5], which expresses the trace of the Hecke operator $T_n$ on weight 2 cusp forms of a given level purely in terms of arithmetic and group-theoretic input. This trace formula is derived using the moduli interpretation of the modular curve as a moduli space of elliptic curves with level structure, and the resulting method has been implemented successfully at scale in the LMFDB.

In this paper, we provide the analogous ingredient for Shimura curves over $\mathbb{Q}$: we find alternatives to the moduli argument and provide an explicit, computation-ready Eichler–Selberg trace formula in terms of optimal embeddings of quadratic orders. In weight 2, this yields Frobenius traces and thereby the $\mathbb{Q}$-isogeny decomposition of the Jacobian of the Shimura curve.

### 2.1.2 Main result

We quickly establish some notation to state our results; see Chapter 1 for more precise definitions and further details. Throughout this paper, let $B$ be an indefinite quaternion algebra over $\mathbb{Q}$ of discriminant $D$, and let $O \subset B$ be a maximal order in $B$. We suppose that $D > 1$, though our methods extend to the case $D = 1$ recovering the case of classical modular curves by adding the cusp contribution (see Remark 2.3.6).

Let $\widehat{H} \leq \widehat{O}^\times$ be an open compact subgroup of level $N \geq 1$, arising as the full preimage of a subgroup $H \leq (O/NO)^\times$ with $N$ minimal. Let $\Gamma_{\widehat{H}} := \widehat{H}^\times \cap B^1$, where

$$B^1 := \{\alpha \in B^\times : \operatorname{nrd}(\alpha) = 1\}.$$

Suppose that $\operatorname{nrd}(H) = (\mathbb{Z}/N\mathbb{Z})^\times$; then the associated Shimura curve $X(\widehat{H})$ is canonically defined over $\mathbb{Q}$. For $k \geq 2$, let $S_k(\widehat{H})$ be the space of (quaternionic) cusp forms of weight $k$ and level $\widehat{H}$, equipped with the action of Hecke operators $T_n$ for $n \geq 1$. For a $\mathbb{Z}$-module $M$, we let $\widehat{M} := M \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}}$ denote its adelic completion. There is a natural permutation $\rho$ of $O^\times$ on $O^\times/\widehat{H}$ by left multiplication. Since $\widehat{H} \leq \widehat{O}^\times$ of level $N$, $\rho$ naturally extends to $\widehat{B}^\times_{(N)} := \{(\alpha_p) \in \widehat{B}^\times : \alpha_p \in O_p^\times \text{ for all } p \mid N\}$ acting on $\widehat{O}^\times/\widehat{H}$ by left multiplication; we denote this extended representation also by $\rho$ and its character by $\chi_{\widehat{H}}$. Finally, for an imaginary quadratic order $S$, let $m(\widehat{S}, \widehat{O}; \widehat{O}^\times)$ denote the number of $\widehat{O}^\times$-conjugacy classes of optimal embeddings of $\widehat{S} \hookrightarrow \widehat{O}$, and let $h(S) \coloneqq \operatorname{Pic}(S)$.

A simplified version of our main result is as follows; see Theorem 2.4.2 for the general statement.

**Theorem 2.1.1** (Explicit trace formula). *Let $k \geq 2$ and $n \geq 1$ with $\gcd(n, DN) = 1$. Let $K(\alpha) \supseteq S \coloneqq \mathbb{Z}[\gamma] \supseteq \mathbb{Z}[\alpha] \coloneqq \mathbb{Z}[x]/(x^2 - tx + n)$ be a quadratic order. Let $\widehat{\alpha}_0 \in \widehat{B}^\times_{(N)}$ be the image of $\alpha$ under $K \hookrightarrow B$. Then for $n$ not a square, we have*

$$\operatorname{Tr}\big(T_n \mid S_k^B(\widehat{H})\big) = \delta_{k,2} \sum_{d \mid n} d - \sum_{t^2 - 4n < 0} p_k(t,n) \sum_{S \supseteq \mathbb{Z}[x]/(x^2 - tx + n)} \frac{1}{\# S^\times} h(S) m(\widehat{S}, \widehat{O}; \widehat{O}^\times) \chi_{\widehat{H}}(\widehat{\alpha}_0)$$

*where $\delta_{k,2} = 1, 0$ according as $k = 2$ or not, and $p_k(t,n) \in \mathbb{Z}[t,n]$ is the coefficient of $x^{k-2}$ in the Taylor series expansion of $(1 - tx + nx^2)^{-1}$.*

Theorem 2.1.1 provides an algorithmic version of the Eichler–Selberg trace formula for Shimura curves, analogous to the modular curve case [78, Section 5].

Using Theorem 2.1.1, we can provide a $\mathbb{Q}$-isogeny decomposition of the Jacobian of a Shimura curve $X(\widehat{H})$ into products of modular abelian varieties corresponding to newforms in the sense of Problem 2.2.3 in a manner similar to the modular curve case. We compute traces of Hecke operators in weight $k = 2$ (Corollary 2.3.5, simplifying $p_2(t,n) = 1$). We then query the LMFDB for the possible trace newforms of classical modular forms, and compute the decomposition by linear algebra over $\mathbb{Q}$.

### 2.1.3 Discussion

Although our intended applications are algorithmic, explicit trace formulas have many uses. For trace formulas over definite quaternion orders over totally real fields, there is a rich history: see Voight [91, Remark 41.5.13]. There is a similarly rich story in the indefinite case. Trace formulas for Hecke operators acting on spaces of (quaternionic) modular forms in an analytic setting [82, 41, 51] play a prominent role in the theory of automorphic forms of $\mathrm{GL}_2$. There have since been very many treatments of explicit trace formulas for Hecke operators in an algebraic setting of classical modular forms (those coming from congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$, especially $\Gamma_0(N)$) [97, 23, 72, 73, 3]. Early on, Eichler [31] proved a trace formula for Hecke operators in the weight 2 case for indefinite Eichler orders using topological methods (see Section 2.3). Shimizu [84, 85] treated the case of indefinite quaternion Eichler orders over a totally real field for weight $k > 2$ using Selberg's analytic trace formula; it is not clear if Shimizu's proof can extend to the case of weight $k = 2$ due to analytic issues.

We provide two proofs of Theorem 2.1.1. First, in Section 2.3 we generalize Eichler's topological argument to Shimura curves of arbitrary level $\widehat{H} \leq \widehat{O}^\times$; this proof is essentially self-contained and provides some real intuition into the formula itself, but it works only for weight $k = 2$. Second, in Section 2.4 we deduce the trace formula from the Lefschetz–Verdier trace formula for correspondences [1, Exposé III Corollaire 4.7, Exposé III B Corollaire 1.3], extending the result to arbitrary weight. Together, these give two independent proofs in weight 2 that avoid analysis entirely.

Our result holds for arbitrary level $\widehat{H}$, including unit groups of arbitrary orders as a special case; this for example recovers a recent trace formula of Tu–Yang [88, Proposition 8] (proven using analytic techniques) for certain orders which are not Eichler at $p = 2$. The existence of a trace formula in the generality provided here is well-known to specialists, but we were unable to find an explicit statement in the literature.

Interestingly, our result also reproves the trace formula (minus cusp contribution) for classical modular curves [78, section 5] without appealing to the moduli interpretation of modular curves, replacing it instead with the theory of optimal embeddings. A third proof in weight 2, working with Shimura curves as moduli spaces of abelian surfaces with potential quaternionic multiplication, is given in Section 2.7.2 for trivial level $N = 1$;

extending this argument to general weight and level seems more difficult.

### 2.1.4 Contents

Chapter 2 is organized as follows. We first review the procedure for computing the isogeny decompositions [78, Section 6, Appendix A] in Section 2.2. Then in Section 2.3, we generalize Eichler's topological proof of the trace formula in the weight 2 case; and we further extend it to higher weights in Section 2.4 after recalling the $\ell$-adic Lefschetz–Verdier trace formula for correspondences. We discuss the relevant implementation details of our trace formula in the weight 2 case in Section 2.5, paying special attention to the non-Eichler situation where $\gcd(D, N) > 1$. We provide several explicit examples in Section 2.6. We briefly recall the moduli interpretation of Shimura curves and give a proof of the trace formula in the level 1 case using the moduli approach in Section 2.7. Finally, we give a trace formula for definite quaternion algebras over $\mathbb{Q}$ in Section 2.8, a result that may be of independent interest.

### 2.1.5 Code

We implemented the trace formula proven in this paper in the computer algebra system Magma [16]. Code along with scripts verifying the examples is available online [46].

## 2.2 Jacobians of Shimura curves

We recall the procedure for computing the isogeny decompositions of the Jacobians of Shimura curves, following the framework and key results provided by [78, Section 6, Appendix A]. See also the references therein for further details. The reader can also view this section as our primary motivation for developing a trace formula for quaternionic modular forms in the weight 2 case.

### 2.2.1 Jacobian decomposition

Let $B$ be an indefinite quaternion algebra over $\mathbb{Q}$ of discriminant $D$ and $O$ be a maximal order in $B$. Let $\widehat{H} \leq \widehat{O}^{\times}$ be an open compact subgroup of level $N$ and let $H := \widehat{H} \cap (O/NO)^{\times}$. Let $J_H := \mathrm{Jac}(X_H(D;N))$ be the Jacobian of the Shimura curve $X_H(D;N)$. The Jacobian $J_H$ is an abelian variety over $\mathbb{Q}$ that has good reduction at all primes $p \nmid DN$.

We restate [78, Theorem A.1.7] in our quaternionic setting. Recall that we say an abelian variety $A$ over a number field $F$ is of $\mathrm{GL}_2$-*type* if $\mathrm{End}(A)_F \otimes \mathbb{Q}$ is a number field of degree $\dim A$.

**Theorem 2.2.1.** *Carrying over the same notations, every factor of $J_H$ is of $GL_2$-type over $\mathbb{Q}$. If we moreover assume that $\gcd(D,N) = 1$, then each simple factor of $J_H$ is isogenous over $\mathbb{Q}$ to a modular abelian variety of the form $A_f$, where $f$ is a Galois orbit of $D$-new eigenforms of level dividing $DN^2$ and character of conductor dividing $N$.*

*Proof.* Keeping in mind of our convention that $(D,N) = 1$, as [78, Remark A.1.10] suggests, this follows by the same line of reasoning as in [78, Appendix A], with Hida's result [39, Proposition 4.8] replacing Ribet's observation, and applying the Jacquet-Langlands correspondence relating quaternionic modular forms with classical modular forms. □

*Remark* 2.2.2. We expect Theorem 2.2.1 to still hold with the assumption $\gcd(D,N) = 1$ removed, as suggested by Example 2.6.3. The difficulty in the case when $\gcd(D,N) > 1$ comes from the inexplicit Jacquet-Langlands correspondence where one does not know the level the corresponding classical modular forms a priori. In any event, when the algorithm described in Section 2.2.2 terminates, the output is guaranteed to be correct; we leave open the possibility that the described procedure may not find a solution in the $\gcd(D,N) > 1$ scenario, although we have not found one yet.

It follows from Theorem 2.2.1 that each simple factors of $J_H$ is $\mathbb{Q}$-isogenous to the modular abelian variety associated to the Galois orbit of a ($D$-new) normalized eigenform of weight 2 for $\Gamma_1(N) \cap \Gamma_0(DN^2)$. This space of cusp forms can be decomposed as

$$S_2(\Gamma_1(N) \cap \Gamma_0(DN^2)) = \bigoplus_{\mathrm{cond}(\chi)|N} S_2(\Gamma_0(DN^2), [\chi]),$$

where $[\chi]$ denotes the Galois orbit of the Dirichlet character $\chi$. The trace form $\mathrm{Tr}(f)$ associated to a normalized eigenform $f \in S_2(\Gamma_0(DN^2), [\chi])$, with $q$-expansion defined by

$$\mathrm{Tr}(f)(q) \coloneqq \sum_{n \geq 1} \mathrm{Tr}_{\mathbb{Q}(f)/\mathbb{Q}}(a_n(f))q^n,$$

encodes various arithmetic information about $A_f$. In particular, $a_1(\mathrm{Tr}(f)) = \dim A_f = \dim f \coloneqq [\mathbb{Q}(f) : \mathbb{Q}]$, and by the Eichler-Shimura correspondence, $a_p(\mathrm{Tr}(f)) = \mathrm{Tr}\,\mathrm{Frob}_p\,|A_f$ for each prime $p$.

Given Theorem 2.2.1, we can precisely state the problem of explicitly computing the isogeny decompositions of $J_H$ over $\mathbb{Q}$ as follows.

*Problem* 2.2.3. Let $S(H) \coloneqq \{[f_1], \ldots, [f_m]\}$ be the Galois orbits of the eigenforms $f \in S_2(\Gamma_1(N) \cap \Gamma_0(DN^2))$ with $\dim f \leq \dim J_H = g(H) \coloneqq \mathrm{genus}(X_H(D; N))$. Find $e(H) \coloneqq (e_1, \ldots, e_m) \in \mathbb{Z}^m_{\geq 0}$ with $\sum_{i=1}^m e_i \dim f_i = g(H)$ such that

$$J_H \sim_{\mathbb{Q}} \prod_{i=1}^m A_{f_i}^{e_i}. \tag{2.1}$$

The decomposition 2.1 translates to the $L$-functions side as

$$L(J_H, s) = \prod_{i=1}^m L(A_{f_i}, s)^{e_i}.$$

### 2.2.2 Algorithm

Due to strong multiplicity 1 for the Selberg class of $L$-functions, Problem 2.2.3 can be computationally solved in practice as follows.

1. For each $[f_i] \in S(H)$, obtain the $q$-expansions for $\mathrm{Tr}(f_i)$ from the L-functions and modular forms database [62].

2. Given a sufficiently large $M \in \mathbb{N}$, let $T(M)$ be the $n \times m$ integer matrix whose $i$th column is $[a_1(\mathrm{Tr}(f_i)), a_2(\mathrm{Tr}(f_i)), a_3(\mathrm{Tr}(f_i)), a_5(\mathrm{Tr}(f_i)), \ldots, a_p(\mathrm{Tr}(f_i)), \ldots]$ where $p$ varies over the $n-1$ primes less than $M$ that do not divide $DN$. See Remark

3. Compute the vector $a(H; M) \coloneqq [g(H), a_2(H), a_3(H), a_5(H), \ldots, a_p(H), \ldots]$, where $a_p(H) \coloneqq \mathrm{Tr}\,\mathrm{Frob}_p\, J_H$, and again $p$ ranges over primes less than $M$ that do not divide $DN$.

4. The vector $e(H)$ can be solved from the linear system

$$T(M)e(H) = a(H; M). \tag{2.2}$$

*Remark* 2.2.4. As Sutherland pointed out in a personal communication, it is important that we only use the Dirichlet coefficients $a_p$ for $p$ prime. Suppose $f$ and $g$ correspond to elliptic curves and $X_H$ is a genus two curve with Jacobian isogenous to $f \times g$. We have $a_p(X_H) = a_p(\mathrm{Tr}(f)) + a_p(\mathrm{Tr}(g))$ for all primes $p$, but we typically do not have $a_n(X_H) = a_n(\mathrm{Tr}(f)) + a_n(\mathrm{Tr}(g))$ for all $n$. Indeed, we have

$$\begin{aligned}
a_6(X_H) &= a_2(X_H)a_3(X_H) \\
&= (a_2(f) + a_2(g))(a_3(f) + a_3(g)) \\
&= a_6(f) + a_6(g) + a_2(f)a_3(g) + a_3(f)a_2(g).
\end{aligned}$$

*Remark* 2.2.5. [78, Section 6] gives a precise explanation for the existence of a finite bound $M$ in Step 2 which guarantees the existence and uniqueness of the solution to the linear system (2.2); [78, Section 6] also suggests a method for finding such a bound $M$ in practice.

We need an effective method to compute $a_p(H)$ in order to solve for $e(H)$ in (2.2). By the Eichler-Shimura correspondence, we have $a_p(H) = \operatorname{Tr} T_p | S_2^B(\widehat{H})$ for $p \nmid DN$. This serves as a primary motivation for us to develop a trace formula for quaternionic modular forms of weight 2 in Section 2.3.

## 2.3 Trace formula

### 2.3.1 Setup

Throughout, let $B$ is an indefinite quaternion algebra over $\mathbb{Q}$ of discriminant $D$. Let $O \subset B$ be a maximal order an open compact subgroup $\widehat{H} \leq \widehat{O}^\times$ of level $N$, and an $n \in \mathbb{N}$ such that $(n, DN) = 1$. There is a Hecke-equivariant *Eichler-Shimura isomorphism* [64, section 4]

$$S_2^B(\widehat{H}) \oplus \overline{S_2^B(\widehat{H})} \xrightarrow{\sim} H^1(X_{\widehat{H}}^B(\mathbb{C}), \mathbb{C}). \tag{2.3}$$

After taking the $+$-eigenspaces for complex conjugation on both sides, we have $S_2^B(\widehat{H}) \cong H^1(X_{\widehat{H}}^B(\mathbb{C}), \mathbb{C})^+$. Hence to compute $\operatorname{Tr} T_n | S_2^B(\widehat{H})$, it suffices to compute $\operatorname{Tr} T_n | H^1(X_{\widehat{H}}^B(\mathbb{C}), \mathbb{C})$, an endeavor we undertake in this section.

The main input here is a Lefschetz-type fixed point theorem that relates $\operatorname{Tr} T_n | H^1(X_{\widehat{H}}^B(\mathbb{C}), \mathbb{C})$ with the number of fixed points of $T_n$ as a correspondence of the Shimura curve $X_{\widehat{H}}^B(\mathbb{C})$. Recall the notations from Section 1.3 and Section 1.4. Let

$$\Theta(n) := \Gamma_{\widehat{H}} \backslash \{\varpi \in B_+^\times : \operatorname{nrd}(\varpi) = n\}.$$

As a correspondence, $T_n$ acts on $X_{\widehat{H}}^B(\mathbb{C}) = \Gamma_{\widehat{H}} \backslash \mathcal{H}$ by

$$T_n(\Gamma_{\widehat{H}} z) \coloneqq \sum_{\varpi \in \Theta(n)} \Gamma_{\widehat{H}} \varpi z; \tag{2.4}$$

when $n = m^2$ is a square, we define $T'_n$ by

$$T'_n(\Gamma_{\widehat{H}} z) \coloneqq \sum_{m \neq \varpi \in \Theta(n)} \Gamma_{\widehat{H}} \varpi z. \tag{2.5}$$

*Remark* 2.3.1. Every point is a fixed point of $\Gamma_{\widehat{H}} m$, so Theorem 2.3.3 only makes sense for $T'_n$ when $n$ is a square.

*Remark* 2.3.2. The multiplicity of a fixed point $\Gamma_{\widehat{H}} z$ of $T_n$ is defined to be the sum of its multiplicity over all the branches $\Gamma_{\widehat{H}} \varpi$. Since the Shimura curve $X^B_{\widehat{H}}(\mathbb{C})$ has no cusps, every fixed point of each branch $\Gamma_{\widehat{H}} \varpi$ has multiplicity 1. Extra care with the multiplicities of the fixed points needs to be taken when applying Theorem 2.3.3 to classical modular curves where there may be cuspidal fixed points.

### 2.3.2 Fixed point theorem of Eichler

**Theorem 2.3.3.** *For $n \in \mathbb{N}$ with $(n, DN) = 1$, if $n$ is not a square, we have*

$$\#\textit{fixed points of } T_n = 2 \sum_{d|n} d - \operatorname{Tr} T_n | H^1(X^B_{\widehat{H}}(\mathbb{C}), \mathbb{C}),$$

*and*

$$\#\textit{fixed points of } T'_n = 2 \left( \left( \sum_{d|n} d \right) - 1 \right) - \operatorname{Tr} T'_n | H^1(X^B_{\widehat{H}}(\mathbb{C}), \mathbb{C})$$

*if $n = m^2$.*

*Proof.* We briefly summarize the key ideas here; see [32, §8 Page 97-106] for details. Let $X \coloneqq X^B_{\widehat{H}}(\mathbb{C})$. The main ingredient in Eichler's proof is to define a fine triangulation $\{\tau^j_i\}$ $(j = 0, 1, 2)$ of $X$ satisfying certain conveniently chosen properties. Letting $T_n(\tau^r_i) = \sum_k \overline{\tau}^r_{ik}$, Eichler defines a linear map $\varphi$ on $\overline{\tau}_{ik}^r$ such that

$$\varphi_n(\tau_i^r) \coloneqq \varphi(T_n(\tau_i^r)) = \sum_k \varphi(\overline{\tau}_{ik}^r).$$

It can be shown via direct calculations that $\varphi_n$ is homotoptic to $T_n$ and that $\varphi_n$ commutes with the boundary operator. Let $C_i$ denote the chain groups of $X$, by the Lefschetz-Hopf trace formula, we have

$$\operatorname{Tr}\varphi_n|C_0 - \operatorname{Tr}\varphi_n|C_1 + \operatorname{Tr}\varphi_n|C_2 = \operatorname{Tr}\varphi_n|H^0(X) - \operatorname{Tr}\varphi_n|H^1(X) + \operatorname{Tr}\varphi_n|H^2(X).$$

Since $\varphi_n$ and $T_n$ are homotopic, and by a direct calculation locally at each fixed point, we then have

$$\#\text{ fixed points of } T_n = \operatorname{Tr} T_n|H^0(X) - \operatorname{Tr} T_n|H^1(X) + \operatorname{Tr} T_n|H^2(X),$$

and finally, the result follows from the fact that $\operatorname{Tr} H^0(X) = \operatorname{Tr} H^2(X) = \deg T_n = \sum_{d|n} d$. When $n$ is a square, $\deg T_n' = (\sum_{d|n} d) - 1$ since we have removed the constant branch coming from $\Gamma_{\widehat{H}} m$. $\square$

We count the number of fixed points of $T_n$ (resp. $T_n'$) by relating the fixed points to optimal embeddings quadratic orders in $O$ (recalling Section 1.2) following [32, section 10]. There is a natural permutation $\rho$ of $O^\times$ on $O^\times/\widehat{H}$ by left multiplication. Since $\widehat{H} \leq \widehat{O}^\times$ of level $N$, $\rho$ naturally extends to

$$\widehat{B}_{(N)}^\times \coloneqq \{(\alpha_p) \in \widehat{B}^\times : \alpha_p \in O_p^\times \text{ for all } p \mid N\};$$

we denote this extended representation also by $\rho$ and its character by $\chi_{\widehat{H}}$.

**Theorem 2.3.4.** *Let $B$ be an indefinite quaternion algebra over $\mathbb{Q}$ of discriminant*

*$D \neq 1$. For each quadratic order $S$, let $w_S = \#S^\times/2$ and $h(S) = \#\operatorname{Pic}(S)$. Let $K(\alpha) \supseteq S \coloneqq \mathbb{Z}[\gamma] \supseteq \mathbb{Z}[\alpha] \coloneqq \mathbb{Z}[x]/(x^2 - tx + n)$ be a quadratic order. Let $\widehat{\alpha}_0 \in \widehat{B}^\times_{(N)}$ be the image of $\alpha$ under $K \hookrightarrow B$. Let $n \in \mathbb{N}$ with $(n, DN) = 1$. If $n$ is not a square, we have*

$$\#\textit{fixed points of } T_n = \sum_{t^2-4n<0} \sum_{\substack{S\supseteq \\ \mathbb{Z}[x]/(x^2-tx+n)}} \frac{h(S)}{w_S} m(\widehat{S}, \widehat{O}; \widehat{O}^\times)\chi_{\widehat{H}}(\widehat{\alpha}_0),$$

*where the sums are over*

- *finitely many integers $t \in \mathbb{Z}$ satisfying $t^2 - 4n < 0$ and*
- *quadratic orders $S \supseteq \mathbb{Z}[x]/(x^2 - tx + n)$.*

*If $n = m^2$, we have*

$$\#\textit{fixed points of } T'_n = \sum_{t^2-4n<0} \sideset{}{'}\sum_{\substack{S\supseteq \\ \mathbb{Z}[x]/(x^2-tx+n)}} \frac{h(S)}{w_S} m(\widehat{S}, \widehat{O}; \widehat{O}^\times)\chi_{\widehat{H}}(\widehat{\alpha}_0),$$

*where $\sum'$ means omitting the quadratic orders $S \supseteq \mathbb{Z}[x]/(x^2 - tx + n)$ such that $[S : \mathbb{Z}[x]/(x^2 - tx + n)] = m$ and $t^2 - 4n = -4m^2$ or $-3m^2$.*

*Proof.* Without loss of generality, suppose $\alpha_0 \in \Theta(n)$, $z \in \mathcal{H}$, and $\alpha_0(z) = z$. Suppose $\iota(\alpha_0) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{R})$ with $t \coloneqq \operatorname{trd}(\alpha_0) = a + d =$ and $n \coloneqq \operatorname{nrd}(\alpha_0) = ad - bc$. First suppose $n$ is not a square. Since $\alpha_0(z) = z$ and $z \in \mathcal{H}$, we have $t^2 - 4n < 0$. To any such $\alpha_0$, the order $S \coloneqq O \cap \mathbb{Q}[x]/(x^2 - tx + n)$ is, by definition, optimally embedded in $O$. Each fixed point $\Gamma_{\widehat{O}^\times} z$ on the level 1 Shimura curve $X_{\widehat{O}^\times}$ corresponds to a $O^\times$-conjugacy class of optimal embeddings of $S$ in $O$ [32, Page 134-135], for which there are $m(S, O; O^\times) = h(S)m(\widehat{S}, \widehat{O}; \widehat{O}^\times)$ of them [91, Theorem 30.4.7]. The converse holds as well. Each point $\Gamma_{\widehat{O}^\times} z$ lifts to $[\Gamma_{\widehat{O}^\times} : \Gamma_{\widehat{H}}] = [\widehat{O}^\times : \widehat{H}]$ points on $X_{\widehat{H}}$, since $\widehat{H}$ has surjective determinant. Among the $[\widehat{O}^\times : \widehat{H}]$ lifts of $\Gamma_{\widehat{O}^\times} z$, precisely $\chi_{\widehat{H}}(\widehat{\alpha}_0)$ of them are fixed by $\alpha_0$.

We then have a sum of the form

$$\sum_{t^2-4n<0} \sum_{\substack{S\supseteq \\ \mathbb{Z}[x]/(x^2-tx+n)}} h(S)m(\widehat{S},\widehat{O};\widehat{O}^\times)\chi_{\widehat{H}}(\widehat{\alpha}_0). \tag{2.6}$$

For all $\epsilon \in S^\times$ and $\varpi \in \Theta(n)$, $\varpi$ and $\epsilon\varpi$ have different traces but correspond to the same fixed point unless $\mathrm{tr}(\varpi) = 0$ and $\epsilon = -1$. Thus the sum (2.6) counts each fixed point of $T_n$ $\#S^\times$ times when $t \neq 0$ and $\#S^\times/2$ times when $t = 0$.

We also need to account for the possibility that a point $z \in \mathcal{H}$ may be a fixed point for multiple branches of $T_n$. Suppose we have two distinct $\varpi_1, \varpi_2 \in \Theta(n)$ and both branches $\Gamma\varpi_1$ and $\Gamma\varpi_2$ fixing $\Gamma z$. Let $S_1$ and $S_2$ be the orders corresponding to the $\varpi_1$ and $\varpi_2$, respectively. If $S_1 \neq S_2$, then the fixed point $\Gamma z$ is correctly counted twice in (2.6). However, if $S_1 = S_2$, which occurs when $\varpi_1 = \overline{\varpi}_2$ and $\varpi_1 \neq \epsilon\varpi_2$ for any $\epsilon \in S^\times$, the fixed point $\Gamma z$ is under-counted by a factor of 2 in (2.6) except for when $t = 0$.

Therefore, letting $w_S = \#S^\times/2$, we have

$$\begin{aligned}
\#\text{fixed points of } T_n &= \sum_{t^2-4n<0} \sum_{\substack{S\supseteq \\ \mathbb{Z}[x]/(x^2-tx+n)}} \frac{2}{\#S^\times} h(S)m(\widehat{S},\widehat{O};\widehat{O}^\times)\chi_{\widehat{H}}(\widehat{\alpha}_0) \\
&= \sum_{t^2-4n<0} \sum_{\substack{S\supseteq \\ \mathbb{Z}[x]/(x^2-tx+n)}} \frac{1}{w_S} h(S)m(\widehat{S},\widehat{O};\widehat{O}^\times)\chi_{\widehat{H}}(\widehat{\alpha}_0).
\end{aligned}$$

When $n = m^2$ is a square, the number of fixed points of $T'_n$ is obtained from remove the count of elements $\varpi \in \Theta(n)$ of the form $\epsilon m$ for $\epsilon \in S^\times$ from the above expression. The case where $\epsilon = \pm 1$ is already accounted for, and the rest (namely $\epsilon$ is a third, fourth, or sixth root of unity) are precisely given by expression in the statement of this theorem. $\square$

**Corollary 2.3.5.** *With the same notations and hypotheses as above, let $g$ be the genus of* *the Shimura curve $X^B_{\widehat{H}}$. We have*

$$\operatorname{Tr} T_n | S_2^B(\widehat{H}) = \sum_{d|n} d - \sum_{t^2-4n<0} \sum_{\substack{S\supseteq \\ \mathbb{Z}[x]/(x^2-tx+n)}} \frac{1}{\# S^\times} h(S) m(\widehat{S}, \widehat{O}; \widehat{O}^\times) \chi_{\widehat{H}}(\widehat{\alpha}_0)$$

*if $n$ is not a square, and*

$$\operatorname{Tr} T_n | S_2^B(\widehat{H}) = \left( \sum_{d|n} d \right) - 1 - \sum_{t^2-4n<0} {\sum_{\substack{S\supseteq \\ \mathbb{Z}[x]/(x^2-tx+n)}}}' \frac{1}{\# S^\times} h(S) m(\widehat{S}, \widehat{O}; \widehat{O}^\times) \chi_{\widehat{H}}(\widehat{\alpha}_0) + g$$

*if $n = m^2$.*

*Proof.* This follows immediately from Theorem 2.3.4 and the Eichler-Shimura isomorphism. □

*Remark* 2.3.6. When $D = 1$ (equiv. $B = M_2(\mathbb{Q})$ and $\widehat{O}^\times = \mathrm{GL}_2(\widehat{\mathbb{Z}})$), we have returned to the setting of classical modular curves, in which case the Riemann surface (a.k.a. the open modular curve) $Y_{\widehat{H}} := \Gamma_{\widehat{H}} \backslash \mathcal{H}$ is no longer compact; let $X_{\widehat{H}}$ denote the Borel-Bailey compactification of $Y_{\widehat{H}}$. In this case, Theorem 2.3.4 gives a count of the number of fixed points of $T_n$ acting on $Y_{\widehat{H}}$ (with the same proof). One ought to take into account the additional contributions of cuspidal fixed points from $X_{\widehat{H}} \backslash Y_{\widehat{H}}$ to obtain the trace formula for classical modular forms; the count of cuspidal fixed points can be explicitly computed according to [100, Lemma 3.4].

*Remark* 2.3.7. We can generalize our discussions thus far by taking $B$ to be a quaternion algebra of discriminant of $\mathfrak{D} \neq (1)$ over a totally real field $F$ of degree $n = [F : \mathbb{Q}]$ with a unique split real place, i.e. $B \otimes_{\mathbb{Q}} \mathbb{R} \cong M_2(\mathbb{R}) \times \mathbb{H}^{n-1}$. Our construction of Shimura curves in §1.3 naturally extends with the caveat that the resulting Shimura curves in the setting $F \neq \mathbb{Q}$ may be disconnected. All of our above results immediately generalize to the case when $F$ has narrow class number one. More generally, as before, let Ø be a maximal order in $B$ and $\widehat{H} \leq \widehat{O}^\times$ an open subgroup of level $\mathfrak{N}$ that is locally norm maximal, i.e. $\mathrm{nrd}(\widehat{H}) = \widehat{\mathbb{Z}}_F^\times$. The connected components of the Shimura curve $X^B_{\widehat{H}}(\mathbb{C})$ are indexed by $\mathrm{Cl}^+ \mathbb{Z}_F$. More precisely, for each class $[\mathfrak{a}] \in \mathrm{Cl}^+ \mathbb{Z}_F$, let $\widehat{a} \in \widehat{\mathbb{Z}}_F$ be such that $[\widehat{a}\widehat{\mathbb{Z}}_F \cap \mathbb{Z}_F] = [\mathfrak{a}]$. There exists $\widehat{\alpha} \in \widehat{B}^\times$ such that $\mathrm{nrd}(\widehat{\alpha}) = \widehat{a}$. Let $\Gamma_{\widehat{H},\mathfrak{a}} \coloneqq \widehat{\alpha}\widehat{H}\widehat{\alpha}^{-1} \cap B_+^\times$. We have a bijection

$$X^B_{\widehat{H}}(\mathbb{C}) \xrightarrow{\sim} \bigsqcup_{[\mathfrak{a}] \in \mathrm{Cl}^+ \mathbb{Z}_F} \Gamma_{\widehat{H},\mathfrak{a}} \backslash \mathcal{H}.$$

Recalling Section 1.4, for a prime $\mathfrak{p} \nmid \mathfrak{D}\mathfrak{N}$, we denote by $T_\mathfrak{p}$ the Hecke operator $T_{\widehat{\pi}}$ where $\widehat{\pi} \in \widehat{B}^\times$ is such that $\widehat{\pi}_v = 1$ for $v \neq \mathfrak{p}$ and $\widehat{\pi}_\mathfrak{p} = \begin{pmatrix} \varpi_\mathfrak{p} & 0 \\ 0 & 1 \end{pmatrix} \in O \otimes_{\mathbb{Z}_F} \mathbb{Z}_{F,\mathfrak{p}} \cong M_2(\mathbb{Z}_{F,\mathfrak{p}})$, where $\varpi_\mathfrak{p}$ is a uniformizer at $\mathfrak{p}$. Let $[\mathfrak{b}] = [\mathfrak{a}\mathfrak{p}^{-1}]$, $\widehat{b}\widehat{\mathbb{Z}}_F \cap \mathbb{Z}_F = \mathfrak{b}$, and let $\widehat{\beta} \in \widehat{B}^\times$ be such that $\mathrm{nrd}(\widehat{\beta}) = \widehat{b}$. Let $I_\mathfrak{a} \coloneqq \widehat{\alpha}\widehat{O} \cap B$ and $I_\mathfrak{b} \coloneqq \widehat{\beta}\widehat{O} \cap B$. We define

$$\Theta(\mathfrak{p})_{\mathfrak{a},\mathfrak{b}} \coloneqq \Gamma_{\widehat{H},\mathfrak{a}} \backslash \{\varpi \in I_\mathfrak{a} I_\mathfrak{b}^{-1} \cap B_+^\times : \mathrm{nrd}(I_\mathfrak{a} I_\mathfrak{b}^{-1})\mathfrak{p} = (\mathrm{nrd}(\varpi))\}.$$

Then as a correspondence, we have

$$T_\mathfrak{p}(\Gamma_{\widehat{H},\mathfrak{a}} z) \coloneqq \sum_{\varpi \in \Theta(\mathfrak{p})_{\mathfrak{a},\mathfrak{b}}} \Gamma_{\widehat{H},\mathfrak{b}} \varpi z.$$

We can see from the above description that, in general, $T_\mathfrak{p}$ permutes the components of $X^B_{\widehat{H}}(\mathbb{C})$, in which case there are no fixed points. When $\mathfrak{p}$ is narrowly principal, $T_\mathfrak{p}$ preserves each connected component of $X^B_{\widehat{H}}(\mathbb{C})$, and hence Theorem 2.3.5 can be applied component wise after suitable modifications.

## 2.4 Trace Formula: Indefinite Case and Arbitrary Weights

In this section, we extend Theorem 2.3.4 to arbitrary even weights.

### 2.4.1 Lefshetz–Verdier fixed point formula

Let $\pi : \mathcal{A} \to X^B_{\widehat{H}}$ be the *universal abelian surface* over $X^B_{\widehat{H}}$. The object $\mathcal{A}$ exists as a two-dimensional complex orbifold, and exists as a genuine abelian surface if $\Gamma_{\widehat{H}}$ is torsion free. Let $\mathbb{V}_{\mathbb{Z}} := R^1\pi_*\mathbb{Z}$, and $\mathbb{V}_{\mathbb{C}} := \mathbb{V}_{\mathbb{Z}} \otimes \mathbb{C}$, a rank 4 local system over $X^B_{\widehat{H}}$. By the quaternionic multiplication (QM) structure on $\mathcal{A}$ (see, e.g., [91, Definition 43.6.9]), $\mathbb{V}_{\mathbb{C}} \cong \mathbb{W}_{\mathbb{C}}^2$, where $\mathbb{W}_{\mathbb{C}}$ is a rank 2 local system [21, Page 175]. (Roughly speaking, this is because each rank 4 fiber decomposes as a square of the standard two-dimensional representation of $B \otimes \mathbb{C} \cong M_2(\mathbb{C})$.) The Eichler-Shimura isomorphism (2.3) can be reformulated as

$$S^B_k(\widehat{H}) \oplus \overline{S^B_k(\widehat{H})} \xrightarrow{\sim} H^1(X^B_{\widehat{H}}(\mathbb{C}), \operatorname{Sym}^{k-2} \mathbb{W}_{\mathbb{C}}). \tag{2.7}$$

Our goal is then to compute $\operatorname{Tr} T_n | H^1(X^B_{\widehat{H}}(\mathbb{C}), \operatorname{Sym}^{k-2} \mathbb{V}_{\mathbb{C}})$. For ease of notation, let $X := X^B_{\widehat{H}}$ and $\mathcal{L} = \operatorname{Sym}^{k-2} \mathbb{W}_{\mathbb{C}}$. We need a generalization of the the topological Lefschetz fixed point theorem 2.3.3.

**Theorem 2.4.1.** *Let $X$ be a smooth curve over $\mathbb{C}$ and $C \subseteq X \times X$ be a correspondence with degeneracy maps $X \xleftarrow{c_1} C \xrightarrow{c_2} X$. Suppose $C$ has finitely many fixed points and $C$ intersects the diagonal $\Delta(X)$ transversely. Let $\mathcal{L}$ be a lisse $\mathbb{Z}_\ell$-sheaf on $X$, and $u : c_1^*\mathcal{L} \to c_2^*\mathcal{L}$ a homomorphism of lisse sheaves. We have*

$$\sum_{i=0}^{2} (-1)^i \operatorname{Tr}((c_{2*} \circ u \circ c_1{}^*) | H^i_{\text{ét}}(X, \mathcal{L})) = \sum_{x \in \operatorname{Fix}(C)} \operatorname{Tr} u_x | \mathcal{L}_{c_1(x) = c_2(x)}.$$

*Proof.* This is a simplification of the Lefschetz–Verdier trace formula [1, Exposé III Corollaire 4.7 & Exposé III B Corollaire 1.3]. The step that generalizes [1, Exposé 1.1.3] is provided by [90, Theorem 4.10]. □

For every even $k > 0$, we define the polynomial $p_k(t, N) \in \mathbb{Z}[t, N]$ as the coefficient of $x^{k-2}$ in the power series expansion of $1/(1 - tx + Nx^2)$. If $M \in M_2(\mathbb{Z})$ is a matrix with $\mathrm{Tr}(M) = t$ and $\det(M) = N$, and let $\rho_{k-2} : M_2(\mathbb{Z}) \to \mathrm{Sym}^{k-2}\mathbb{Z}^2$, we then have $\mathrm{Tr}(\rho_{k-2}(M)) = p_k(t, N)$. In particular, $p_2(t, N) = 1$.

### 2.4.2 Trace formula

**Theorem 2.4.2.** *We inherit the notations from Theorem 2.3.4. Let $k \geq 2$ and $n \in \mathbb{N}$ with $(n, DN) = 1$. If $n$ is not a square,*

$$\begin{aligned}\mathrm{Tr}\, T_n | H^1_{\text{ét}}(X^B_{\widehat{H}}(\mathbb{C}), \mathrm{Sym}^{k-2}\mathbb{W}_{\mathbb{C}}) = 2\delta_{k,2} \sum_{d|n} d - \\ \sum_{t^2-4n<0} p_k(t,n) \sum_{\substack{S \supseteq \\ \mathbb{Z}[x]/(x^2-tx+n)}} \frac{1}{w_S} h(S) m(\widehat{S}, \widehat{O}; \widehat{O}^\times) \chi_{\widehat{H}}(\widehat{\alpha}_0);\end{aligned}$$

*otherwise, suppose $n = m^2$, then*

$$\begin{aligned}\mathrm{Tr}\, T_n | H^1_{\text{ét}}(X^B_{\widehat{H}}(\mathbb{C}), \mathrm{Sym}^{k-2}\mathbb{W}_{\mathbb{C}}) = 2\delta_{k,2} \left( \sum_{d|n} d - 1 \right) - \\ \sum_{t^2-4n<0} p_k(t,n) {\sum_{\substack{S \supseteq \\ \mathbb{Z}[x]/(x^2-tx+n)}}}' \frac{1}{w_S} h(S) m(\widehat{S}, \widehat{O}; \widehat{O}^\times) \chi_{\widehat{H}}(\widehat{\alpha}_0) \\ + 2\dim_{\mathbb{C}}(S^B_k(\widehat{H})).\end{aligned}$$

*Proof.* First suppose that $\Gamma_{\widehat{H}}$ is torsion-free, in which case $X \coloneqq X^B_{\widehat{H}}(\mathbb{C})$ is an honest smooth curve and Theorem 2.4.1 directly applies. We replace $\mathbb{W}_{\mathbb{C}}$ by its $\ell$-adic realization $\mathbb{W}_\ell \coloneqq \mathbb{W}_{\mathbb{Z}} \otimes \mathbb{Z}_\ell(1)$ for $\ell \nmid DN$ and apply Theorem 2.4.1 to $\mathcal{L} = \mathbb{W}_\ell$. The $\ell$-adic Tate module $T_\ell(A_\tau)$ of the abelian surface $A_\tau$ is then given by $T_\ell(A_\tau) \cong \mathcal{L}^2_\tau$. In the situation where the correspondence $C$ is the Hecke correspondence, the composition ${c_2}_* \circ u \circ {c_1}^*$ is precisely the action of the Hecke operator $T_n$ on $H^i_{\text{ét}}(X, \mathcal{L})$. A fixed point $\tau \in \mathrm{Fix}(T_n)$ corresponds to the data of a degree $n$ isogeny $\varphi : A_\tau \to A_{\tau'}$ and an isomorphism $i : A_{\tau'} \to A_\tau$. The action $u_\tau | \mathcal{L}_{c_1(\tau) = c_2(\tau)}$ at $\tau \in \mathrm{Fix}(T_n)$ can be explicitly described by $T_\ell(i \circ \varphi) : T_\ell(A_\tau) \to T_\ell(A_\tau)$, which corresponds to a CM action by some order $S$ in an imaginary quadratic field $K$ on the $\mathbb{Z}_\ell$-lattice $T_\ell(A_\tau) \cong \mathbb{Z}_\ell \oplus \tau\mathbb{Z}_\ell$. As in the proof of Theorem 2.3.4, we rearrange the sum over $\mathrm{Fix}(T_n)$ as a sum over CM discriminants $d = t^2 - 4n$, $t \in \mathbb{Z}$. For each $\tau \in \mathrm{Fix}(T_n)$ having CM discriminant $d = t^2 - 4n$, we can view the composition $i \circ \varphi$ as an element $\alpha \in S \supseteq \mathbb{Z}[x]/(x^2 - tx + n)$ satisfying $\alpha^2 - t\alpha + n = 0$ acting on $T_\ell(A_\tau)$ by left multiplication, in which case $\mathrm{Tr}\, u_\tau | \mathcal{L}_{c_1(\tau)=c_2(\tau)} = \mathrm{Tr}\,\alpha | \mathbb{Z}_\ell \oplus \tau\mathbb{Z}_\ell = t = \alpha + \overline{\alpha}$. It follows that $\mathrm{Tr}\, u_\tau | \mathrm{Sym}^{k-2} \mathcal{L}_{c_1(\tau)=c_2(\tau)} = p_k(t,n)$. When $\mathcal{L}$ is a nontrivial local system, i.e. when $k > 2$, $H^0(X, \mathcal{L}) = H^2(X, \mathcal{L}) = 0$.

More generally, we choose $\widehat{H}' \trianglelefteq \widehat{H}$ of finite index and level coprime to $n$ such that $\Gamma_{\widehat{H}'}$ is torsion-free. Let $X' := X^B_{\widehat{H}'}(\mathbb{C})$ and $G := \Gamma_{\widehat{H}}/\Gamma_{\widehat{H}'}$. By the degeneration of the Hochschild-Serre spectral sequence for Galois covers, we have an isomorphism

$$H^i_{\text{ét}}(X, \mathcal{L}) \cong H^i_{\text{ét}}(X', \mathcal{L})^G.$$

As the correspondence $T_n$ commutes with the deck transformations $G$ of $X'$, we have

$$\mathrm{Tr}\, T_n | H^i_{\text{ét}}(X', \mathcal{L})^G = \frac{1}{\#G} \sum_{g \in G} \mathrm{Tr}[(g \circ T_n) | H^i_{\text{ét}}(X', \mathcal{L})]. \tag{2.8}$$

Applying (2.8), Theorem 2.4.1 to each of $q \circ T_n$, and taking $\mathcal{L} = \mathrm{Sym}^{k-2} \mathbb{W}_\ell$, we have

$$\begin{aligned}
\sum_{i=0}^{2}(-1)^i \operatorname{Tr} T_n | H^i_{\text{ét}}(X',\mathcal{L})^G &= \frac{1}{\#G}\sum_{g\in G}\sum_{i=0}^{2}(-1)^i \operatorname{Tr}[(g\circ T_n)|H^i_{\text{ét}}(X',\mathcal{L})] \\
&= \frac{1}{\#G}\sum_{g\in G}\sum_{x\in \operatorname{Fix}(g\circ T_n)} \operatorname{Tr}(u_x|\mathcal{L}_{gc_1(x)=gc_2(x)}) \\
&= \sum_{t^2-4n<0} p_k(t,n) \sum_{\substack{S\supseteq \\ \mathbb{Z}[\alpha]\cong\mathbb{Z}[x]/(x^2-tx+n)}} \frac{1}{w_S} h(S) m(\widehat{S},\widehat{O};\widehat{O}^\times) \\
&\quad \frac{1}{\#G}\sum_{g\in G}\#\{\Gamma_{\widehat{H}'}z : \alpha_0\Gamma_{\widehat{H}'}gz = \Gamma_{\widehat{H}'}z\} \\
&= \sum_{t^2-4n<0} p_k(t,n) \sum_{\substack{S\supseteq \\ \mathbb{Z}[x]/(x^2-tx+n)}} \frac{1}{w_S} h(S) m(\widehat{S},\widehat{O};\widehat{O}^\times)\chi_{\widehat{H}}(\widehat{\alpha}_0).
\end{aligned}$$

EOP □

*Remark* 2.4.3. When $k = 2$, the local system $\operatorname{Sym}^0 \mathbb{V}_{\mathbb{C}}$ is trivial, in which case we are simply counting the number of fixed points of $T_n$; this recovers Eichler's topological Lefschetz fixed point formula as in Theorem 2.3.3.

*Remark* 2.4.4. When $k$ is odd and $-1 \in \widehat{H}$, the space $S_k^B(\widehat{H}) = 0$; there is no content in the statement of Theorem 2.4.2 in these cases.

*Remark* 2.4.5. [99, Theorem 8.8] establishes the Lefschetz–Verdier trace formula for Deligne–Mumford stacks. One can in principle do away with the yoga of taking G-invariants in the proof of Theorem 2.4.2 by proving [90, Theorem 4.10] for DM stacks; we do not plan on doing so.

## 2.5 Implementations

A Magma implementation of the trace formula from Corollary 2.3.5 is provided by the function `IndefiniteTrace` in the file `indefinite.m` in [46]; we make use of the code available in [77] with minor modifications to carry out the procedure for computing isogeny decompositions as in Section 2.2 and the file `newform_decomp.m` in [46]. The only nontrivial components in the implementation of Corollary 2.3.5 are the computation of the characters $\chi_{\widehat{H}}$ and the quantities $m(S, O; \Gamma_{\widehat{H}})$, which we address in this section. The computation of the class numbers $h(S)$ can be viewed as a pre-computation and can be done using readily available Magma intrinsics; the local optimal embedding numbers $m(\widehat{S}, \widehat{O}; \widehat{O}^\times)$ can be computed using Corollary 1.2.2.

*Remark* 2.5.1. This is the appropriate place to emphasize that our assumption of the maximality of $O$ is crucial for the simplicity of the formula in Corollary 1.2.2 and the cleanliness of our implementation. See [91, Remark 30.6.18] for a historical account of various treatments of local embedding numbers for other types of orders. In fact, all of our theoretical results, in particular Theorem 2.3.4, Corollary 1.2.2, and Theorem 2.4.2, hold for arbitrary quaternion orders $O \subseteq B$ and $n$ coprime to $\operatorname{disc}(O) \cdot N$ with the exact same proofs.

Let $\widehat{H} \leq \widehat{O}^\times$ be a finite index subgroup of level $N$. In order to compute the character $\chi_{\widehat{H}}$, we replace $\widehat{H}$ by the subgroup $H \coloneqq (\widehat{H} \cap (O/NO)^\times) \leq (O/NO)^\times$ and work inside the finite group $(O/NO)^\times$. When $(D, N) = 1$, $(O/NO)^\times \cong \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ as we have pointed out, and $\chi_{\widehat{H}}(\widehat{\alpha}_0)$ can be computed as follows.

**Lemma 2.5.2.** *Let $O \subset B$ be a maximal order, $\widehat{H} \leq \widehat{O}^\times$ an open compact subgroup of level $N$ such that $\gcd(n, DN) = 1$ and $\gcd(D, N) = 1$. Let $K(\alpha) \supseteq S \coloneqq \mathbb{Z}[\gamma] \supseteq \mathbb{Z}[\alpha] \coloneqq \mathbb{Z}[x]/(x^2 - tx + n)$ be a quadratic order with $b \coloneqq [S : \mathbb{Z}[\alpha]]$. Let $\widehat{\alpha}_0 \in \widehat{B}^\times_{(N)}$ be the image of $\alpha$ under $K \hookrightarrow B$. We have*

$$\chi_{\widehat{H}}(\widehat{\alpha}_0) = \chi_{\widehat{H}}(A(t, b, S)).$$

*where*

$$A(t,b,S) \coloneqq \begin{cases} \begin{pmatrix} 0 & -n/b \\ b & t \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}), & \textit{if } (b,N)=1, \textit{ and} \\ \begin{pmatrix} (t-b\,\mathrm{Tr}(\gamma))/2 & -bN(\gamma) \\ b & (t+b\,\mathrm{Tr}(\gamma))/2 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) & \textit{otherwise.} \end{cases} \tag{2.9}$$

*Proof.* If $(D,N)=1$, $\widehat{O}_{(N)} \coloneqq \widehat{O} \otimes_{\mathbb{Z}} \mathbb{Z}/N\mathbb{Z} \cong M_2(\mathbb{Z}/N\mathbb{Z})$. Let $\widehat{S}_{(N)} \coloneqq \widehat{S} \otimes_{\mathbb{Z}} \mathbb{Z}/N\mathbb{Z}$. Following the proof of [91, Proposition 30.5.3], we have a canonical optimal embedding $\widehat{S}_{(N)} \hookrightarrow M_2(\mathbb{Z}/N\mathbb{Z})$ given by the regular representation of $\widehat{S}_{(N)}$ on itself. For $\widehat{S}_{(N)}$ in the basis $\{1,\widehat{\gamma}\}$, we have

$$\widehat{\gamma} \mapsto \begin{pmatrix} 0 & -N(\gamma) \\ 1 & \mathrm{Tr}(\gamma) \end{pmatrix} \in M_2(\mathbb{Z}/N\mathbb{Z}). \tag{2.10}$$

When $(b,N)=1$, we may take $\gamma = \alpha/b$; otherwise, we have $\alpha = (t-b\,\mathrm{Tr}(\gamma))/2 + b\gamma$. In both cases, we have $\widehat{\alpha} \mapsto \widehat{\alpha}_0 \coloneqq A(t,b,S) \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ as defined in (2.9) under the optimal embedding (2.10). $\square$

*Remark* 2.5.3. The matrix used in the point-counting formula of [78, (5.1.2) & (5.1.4)] can also be viewed as being obtained from a suitably defined regular representation, c.f. the proof of [29, Theorem 1].

It remains to discuss how to compute with $(O/NO)^\times$ in practice when the level $N=p^e$ where $p|D$ by the CRT, as Magma currently does not have a constructor for the quotient of a quaternion order by a two-sided ideal, let alone constructing its unit group.

Suppose first that $p \neq 2$. The unique division quaternion algebra $B$ over $\mathbb{Q}_p$ can be described by $B \coloneqq \left(\frac{a,b}{\mathbb{Q}_p}\right)$, $I^2=a, J^2=b, IJ=-JI$, where $K \coloneqq \mathbb{Q}_p(\sqrt{a})$ is the unique quadratic unramified extension of $\mathbb{Q}_p$, and $v_p(b)=1$. In this case, $O \coloneqq \mathbb{Z}_K \oplus \mathbb{Z}_K J$ is the unique maximal order in $B$, and $P = OJ$ is the unique maximal two-sided ideal of $O$

with $P^2 = pO$ c.f. [91, Theorems 12.3.2, 13.3.4, 13.3.11]. In practice, given a $\mathbb{Z}$-basis for a maximal order $O \subseteq B$ over $\mathbb{Q}$, we do a random search for $I$ and $J$ in the trace-0 subspace of $O$ satisfying $\left(\frac{-\operatorname{nrd}(I)}{p}\right) = -1$, $v_p(\operatorname{nrd}(J)) = 1$, and $\operatorname{trd}(IJ) = 0$; we then take $a \coloneqq \operatorname{nrd}(I)$ and $b \coloneqq \operatorname{nrd}(J)$. Hence we can view $(O/p^eO)^\times$ as a matrix subgroup of $\mathrm{GL}_2(\mathbb{Z}_K/p^e\mathbb{Z}_K)$ via the embedding $\lambda : B \to M_2(K)$, $I \mapsto \begin{pmatrix} \sqrt{a} & 0 \\ 0 & -\sqrt{a} \end{pmatrix}$, $J \mapsto \begin{pmatrix} 0 & b \\ 1 & 0 \end{pmatrix}$, c.f. [91, Proposition 2.3.1]. When $p = 2$, we instead pick $I$ with odd reduced trace and reduced norm, in which case $IJ = J(\operatorname{trd}(I) - I)$. In this case, let $K = \mathbb{Q}_2(\alpha) \cong \mathbb{Q}_2[x]/(x^2 - \operatorname{trd}(I)x + \operatorname{nrd}(I))$, which is the unique unramified quadratic extension of $\mathbb{Q}_2$. The embedding $\lambda : B \to M_2(K)$ is given by $I \mapsto \begin{pmatrix} \alpha & 0 \\ 0 & \operatorname{trd}(I) - \alpha \end{pmatrix}$, $J \mapsto \begin{pmatrix} 0 & b \\ 1 & 0 \end{pmatrix}$, c.f. [91, Exercise 6.7].

We now describe the generators of $(O/p^eO)^\times$. Let $G_0 \coloneqq (O/p^eO)^\times$ and $G_k \coloneqq (1+P^k)/(1+P^{2e})$, $k = 1, \dots, 2e$. We have the following filtration (also a subnormal series)

$$G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_{2e} = \{1\},$$

where $G_0/G_1 \cong (O/P)^\times \cong \mathbb{F}_{p^2}^\times \cong \langle c \rangle$ and $G_k/G_{k+1} \cong \langle 1+J^k, 1+IJ^k \rangle$ for $k = 1, \dots, 2e-1$, c.f. [91, 13.5.9]. We lift $c$ to an element $\tilde{c} = a + bI \in O$ for some $a, b \in \{0, 1, \dots, p-1\}$. Therefore $(O/p^eO)^\times$ as a subgroup of $\mathrm{GL}_2(\mathbb{Z}_K/p^e\mathbb{Z}_K)$ are generated by the images of $\tilde{c}, 1+J^k, 1+IJ^k$, $k = 1, \dots, 2e-1$, under $\lambda$. We can also immediately see from the above filtration that $\#(O/p^eO)^\times = (p^2-1)p^{2(2e-1)}$.

*Remark* 2.5.4. Since $(O/p^eO)^\times$ is a polycyclic group, one can further refine the above subnormal series for $(O/p^eO)^\times$ so that each successive quotient is cyclic, and directly define $(O/p^eO)^\times$ as a `GrGPC` object in Magma by specifying all the necessary conjugation relations on the generators. This would make the coset computations for $\chi_H$ more efficient. We opt out of this approach as working inside $\mathrm{GL}_2(\mathbb{Z}_K/p^e\mathbb{Z}_K)$ suffices for our purpose.

A simpler, more naïve, and highly inefficient alternative approach would be to embed

$(O/NO)^\times$ into $\mathrm{GL}_4(\mathbb{Z}/N\mathbb{Z})$ by left regular representation. To illustrate the monstrosity of this approach, in Example 2.6.2 to be discussed, one has $[\mathrm{GL}_4(\mathbb{Z}/3\mathbb{Z}) : (O/3O)^\times] = (3^4-1)(3^4-3)(3^4-3^2)(3^4-3^2)/(2^3 \cdot 3^2) = 336,960$, whereas $[\mathrm{GL}_2(\mathbb{Z}_9/3\mathbb{Z}_9) : (O/3O)^\times] = (9^2-1)(9^2-9)/(2^3 \cdot 3^2) = 80$.

## 2.6 Examples

### 2.6.1 Eichler Orders

One of the most well-known families of Shimura curves is the analogue of the modular curves $X_0(N)$s; this family of Shimura curves arise from *Eichler orders*, which we now describe. Let $O \subset B$ be a maximal order and let $N \geq 1$ be coprime to $D$. There is an isomorphism $\iota_N : O \hookrightarrow O \otimes_{\mathbb{Z}} \mathbb{Z}_N \cong M_2(\mathbb{Z}_N)$, where $\mathbb{Z}_N$ denotes the completion of $\mathbb{Z}$ at the ideal $(N)$. Let

$$O(N) \coloneqq \{x \in O : \iota_N(x) \text{ is upper triangular modulo } N\};$$

the order $O(N)$ is called an *Eichler order* of level $N$. Taking $\widehat{H} = \widehat{O}(N)^\times$, we denote the corresponding Shimura curve by $X_0(D; N) \coloneqq X^B_{\widehat{H}}$. Ribet's isogeny theorem [74, 11, 42, 40] applies in this setting, and we have an isogeny defined over $\mathbb{Q}$

$$J(X_0(D;N)) \sim_{\mathbb{Q}} J_0(DN)^{D-\mathrm{new}} \sim_{\mathbb{Q}} \prod_{[f]} A_f^{e_f},$$

where $J_0(DN)$ is the Jacobian of the classical modular curve $X_0(DN)$ and the product runs over Galois orbits of $D$-new newforms of $S_2(\Gamma_0(DN))$. In fact, we have

$$S_2(\Gamma_0(DN))^{D-\mathrm{new}} = \bigoplus_{D|M|DN} (S_2(\Gamma_0(M))^{\mathrm{new}})^{\oplus e(DN/M)},$$

where $e(k) = \#$ positive divisors of $k$. While a trace formula is a priori not needed to determine the isogeny decomposition of $J(X_0(D;N))$, it is nevertheless a useful consistency check and a demonstrative class of examples.

**Example 2.6.1** $(X_0(6,25))$**.** We search in the Classical modular forms section of the LMFDB [62] for weight 2 newforms of level $6 \cdot 25 = 150$ with trivial conductor (character order $= 1$), and keeping only the ones that are 6-new (equiv. level divisible by 6). There are 4 newforms satisfying this requirement:

$$f_1 = \texttt{30.2.a.a}, f_2 = \texttt{150.2.a.a}, f_3 = \texttt{150.2.a.b}, f_4 = \texttt{150.2.a.c}.$$

Hence we have

$$J(X_0(6,25)) \sim_{\mathbb{Q}} A_{f_1}^{e(150/30)} \times A_{f_2}^{e(1)} \times A_{f_3}^{e(1)} \times A_{f_4}^{e(1)} \sim_{\mathbb{Q}} A_{f_1}^2 \times A_{f_2} \times A_{f_3} \times A_{f_4}.$$

For $p \neq 2, 3, 5$, we expect

$$a_p(\widehat{O}(25)^\times) := \operatorname{Tr} T_p | S_2^B(\widehat{O}(25)^\times) = 2a_p(f_1) + a_p(f_2) + a_p(f_3) + a_p(f_4),$$

which we compare with the output of Corollary 2.3.5:

| $p$ | $a_p(\widehat{O}(25)^\times)$ | $a_p(f_1)$ | $a_p(f_2)$ | $a_p(f_3)$ | $a_p(f_4)$ |
|---|---|---|---|---|---|
| 7 | -4 | -4 | 2 | 4 | -2 |
| 11 | 4 | 0 | 2 | 0 | 2 |
| 13 | 2 | 2 | 6 | -2 | -6 |
| 17 | 6 | 6 | 2 | -6 | -2 |
| 19 | -12 | -4 | 0 | -4 | 0 |
| 23 | 0 | 0 | -4 | 0 | 4 |

### 2.6.2 Arbitrary levels

**Example 2.6.2.** Let $B = \left(\frac{3,-1}{\mathbb{Q}}\right)$, $O \subseteq B$ a maximal order with $\mathbb{Z}$-basis $\langle 1, (1+i+j+k)/2, (1-i+j-k)/2, (1-i-j+k)/2\rangle$, and $H = \langle 2+i+j+k, 2, 3+i+j+k\rangle \leq (O/3O)^\times$. The corresponding Shimura curve $X^B_{\widehat{H}}$ has LMFDB label `6.1.3.36.2.a.1` (the Shimura curves section is currently under development and only available in the Alpha version of the LMFDB). The level of $H$ is $N = 3$ and $D = \operatorname{disc} B = 6$. Three Galois orbits of eigenforms $f \in S_2(\Gamma_1(3) \cap \Gamma_0(54))$ have $\dim f \leq g(X^B_{\widehat{H}}) = 2$, with LMFDB labels `27.2.a.a`, `54.2.a.a`, and `54.2.a.b`. For $M = 53$ as described in Section 2.2, the $15 \times 3$ matrix $T(M)$ has independent columns. Computing $a_p(H)$ via the trace formula for $p = 5, 7, 11, \ldots, 53$ yields $a(H; M) = [2, 0, -2, 0, -8, 0, 4, 0, 0, 10, 4, 0, -20, 0, 0]^T$, and the linear system

$$\begin{pmatrix} 1 & 1 & 1 \\ 0 & -3 & 3 \\ -1 & -1 & -1 \\ 0 & 3 & -3 \\ 5 & -4 & -4 \\ 0 & 0 & 0 \\ -7 & 2 & 2 \\ 0 & 6 & -6 \\ 0 & -6 & 6 \\ -4 & 5 & 5 \\ 11 & 2 & 2 \\ 0 & 6 & -6 \\ 8 & -10 & -10 \\ 0 & -6 & 6 \\ 0 & -9 & 9 \end{pmatrix} e(H) = \begin{pmatrix} 2 \\ 0 \\ -2 \\ 0 \\ -8 \\ 0 \\ 4 \\ 0 \\ 0 \\ 10 \\ 4 \\ 0 \\ -20 \\ 0 \\ 0 \end{pmatrix}$$

has the unique solution $e(H) = [0, 1, 1]^T$, corresponding to the Galois orbits `54.2.a.a` and `54.2.a.b` both of dimensions 1 and analytic ranks 0; thus $J_H$ also has analytic rank 0. The Magma script that reproduces this example is available in [46] at `./examples/6.1.3.36.2.a.1.m`.

**Example 2.6.3.** Let $B$ and $O$ be the same as in Example 2.6.2, and let $H = \langle 3+2k, 4-i+2k, 6-i+2k, 3, 5-i+k\rangle \leq (O/4O)^\times$. The corresponding Shimura curve $X^B_{\widehat{H}}$ has LMFDB label `6.1.4.24.1.bj.1`. The level of $H$ in this case is $N = 4 = 2^2$. Five Galois orbits of eigenforms $f \in S_2(\Gamma_1(4) \cap \Gamma_0(96))$ has $\dim f \leq g(X^B_{\widehat{H}}) = 1$, with LMFDB labels `24.2.a.a`, `32.2.a.a`, `48.2.a.a`, `96.2.a.a`, and `96.2.a.b`. Computing $a_p(H)$ via the trace formula for $p = 5, 7, 11$ suffices to identify the newform $f =$ `48.2.a.a` with the property that $X^B_{\widehat{H}} \cong J(X^B_{\widehat{H}}) \sim_{\mathbb{Q}} A_f$. As a corollary of this computation, we have that the Shimura curve $X^B_{\widehat{H}}$ belongs to the elliptic curve isogeny class `48.a`. The Magma script that reproduces this example is available in [46] at `./examples/6.1.4.24.1.bj.1.m`.

## 2.7 Towards a moduli approach

In this section, we give a proof of the trace formula in the weight 2 level 1 case (i.e. $\widehat{H} = \widehat{O}^\times$) via the moduli interpretation of Shimura curves, analogous to the proof of [78, Section 5]; we do not see an apparent way to extend this argument to general weight and level.

### 2.7.1 QM-Abelian Surfaces

We begin by making precise the objects parametrized by Shimura curves, following [91, Chapter 43]. Let $B$ be an indefinite quaternion algebra over $\mathbb{Q}$ of discriminant $D$, and $O$ be a maximal order in $B$. Fix a *principal polarization* of $O$, i.e. an element $\mu \in O$ such that $\mu^2 + D = 0$. Every $O$ has a principal polarization $\mu$ (c.f. [91, 43.6.6]), which induces a positive involution

$$* : \alpha \mapsto \alpha^* := \mu^{-1}\bar{\alpha}\mu$$

on $O$ and hence $B$.

Let $(A, \lambda)$ be a principally polarized abelian surface defined over a field $k$, where $\lambda : A \xrightarrow{\sim} A^\vee$. Let $\mathrm{End}(A)_\mathbb{Q} \coloneqq \mathrm{End}(A) \otimes_\mathbb{Z} \mathbb{Q}$ denote the *rational endomorphism ring* of $A$. Recall that $\lambda$ induces a positive involution, known as the *Rosati involution*, on $\mathrm{End}(A)_\mathbb{Q}$ given by $\dagger : \alpha \mapsto \lambda^{-1}\alpha^\vee\lambda$.

**Definition 2.7.1.** We say $(A, \iota, \lambda)$ is an $(O, \mu)$-*QM (quaternionic multiplication) abelian surface* if there is an embedding $\iota : O \hookrightarrow \mathrm{End}(A)$ such that the following diagram commutes

$$\begin{tikzcd} B \arrow[r, "\iota"] \arrow[d, "*"] & \mathrm{End}(A)_\mathbb{Q} \arrow[d, "\dagger"] \\ B \arrow[r, "\iota"] & \mathrm{End}(A)_\mathbb{Q} \end{tikzcd}$$

where $*$ and $\dagger$ are as above.

*Remark* 2.7.2. By [91, Remark 43.6.27], fixing $A$ and $\iota$, there is a unique principal polarization of $A$ such that its induced Rosati involution is compatible with $\mu$ as in Definition 2.7.1. Hence we may abbreviate the notation $(A, \iota, \lambda)$ by $(A, \iota)$ without confusion.

**Definition 2.7.3.** A *homomorphism* (resp. *isomorphism*) $(A, \iota) \to (A', \iota')$ of principally polarized $(O, \mu)$-QM abelian surfaces is a homomorphism (resp. isomorphism) $\varphi : A \to A'$ of principally polarized abelian surfaces (respecting the polarization, i.e. $\varphi^\vee \circ \lambda' \circ \varphi = \lambda$ (resp. $\varphi^*\lambda' = \lambda$)) such that the following diagram commutes

$$\begin{tikzcd} B \arrow[r, "\iota'"] \arrow[dr, "\iota"'] & \mathrm{End}(A')_\mathbb{Q} \arrow[d, "\varphi^*"] \\ & \mathrm{End}(A)_\mathbb{Q} \end{tikzcd} .$$

We define the *Shimura curve* $X(D; 1)$ to be the coarse moduli space of $(O, \mu)$-QM abelian surfaces.

Let $k$ be a perfect field of characteristic coprime to $D$ and $G_k \coloneqq \mathrm{Gal}(\overline{k}/k)$. Given a QM-abelian surface $(A, \iota)$ defined over $\overline{k}$, each $\sigma \in G_k$ induces an action $(A, \iota)^\sigma \coloneqq (A^\sigma, \iota^\sigma)$ where $A^\sigma$ is defined by the fibered diagram

$$\begin{array}{ccc} A^\sigma & \longrightarrow & A \\ \downarrow & & \downarrow \\ \operatorname{Spec} \overline{k} & \xrightarrow{\sigma} & \operatorname{Spec} \overline{k} \end{array}$$

and $\iota^\sigma(x) := (\iota(x))^\sigma$. Let $X(D;1)(\overline{k})$ be the set of isomorphism classes of $O$-QM abelian surfaces, and $X(D;1)(k) := X(D;1)^{G_k}$.

We continue with the discussion of level structures on $QM$-abelian surfaces following [4, Section 2], parallel to the story of level structures on elliptic curves, c.f. [78, Section 2].

**Definition 2.7.4.** Let $k$ be a perfect field of characteristic coprime to $N$, and $(A, \iota, \lambda) \in X(D;1)(k)$. A *full level N structure* is an isomorphism of rank 1 $O$-modules

$$\alpha : (O/NO) \xrightarrow{\sim} A[N](\overline{k}), m \mapsto \iota(m)(Q)$$

for some $(O/NO)$-basis element $Q \in A[N](\overline{k})$.

Let $\alpha_1$ and $\alpha_2$ be two full level $N$ structures on $(A_1, \iota_1, \lambda_1)$ and $(A_2, \iota_2, \lambda_2)$ corresponding to $Q_1 \in A_1[N](\overline{k})$ and $Q_2 \in A_2[N](\overline{k})$, respectively. We say the tuples $(A_1, \iota_1, \lambda_1, \alpha_1)$ and $(A_2, \iota_2, \lambda_2, \alpha_2)$ are isomorphic if there is an isomorphism

$$\varphi : (A_1, \iota_1, \lambda_1) \to (A_2, \iota_2, \lambda_2)$$

as defined above and $\varphi(Q_1) = Q_2$. We let $[(A_1, \iota_1, \lambda_1, \alpha_1)]$ denote the isomorphism class of this triple. We define $X(D;N)$ to be the Shimura curve parametrizing $O$-QM abelian surfaces with full level $N$ structures.

There is a left action of $(O/NO)^\times$ on the set of full level $N$ structures of $(A, \iota, \lambda)$ as follows: given $a \in (O/NO)^\times$, right multiplication by $a$ gives an isomorphism $r_a : O/NO \to O/NO$ of left $O$-modules. Hence if $\alpha$ is a full level $N$ structure on $(A, \iota, \lambda)$, so is $\alpha \circ r_a$.

Given a subgroup $H \leq (O/NO)^\times$, we say two tuples $(A_i, \iota_i, \lambda_i, \alpha_i)$, $i = 1, 2$ are *$H$-equivalent* if there is an isomorphism $\varphi : (A_1, \iota_1, \lambda_1) \to (A_2, \iota_2, \lambda_2)$, and for some $h \in H$,

$\alpha_2 = r_h \circ \alpha_1 \circ \varphi|_{A_1[N]}$. We let $[(A, \iota, \lambda, \alpha)]_H$ denote the $H$-equivalence class under this equivalence relation. An ***H-level structure*** on an $O$-QM abelian surface $(A, \iota, \lambda)$ is an equivalence class $[(A, \iota, \lambda, \alpha)]_H$.

**Definition 2.7.5.** Let $H \leq (O/NO)^\times$. We define the ***Shimura curve*** $X_H(D; N)$ to be the coarse moduli space of the Deligne-Mumford stack over $\operatorname{Spec} \mathbb{Z}[1/N]$ that parametrizes $O$-QM abelian surfaces with $H$-level structure; equivalently, $X_H(D; N)$ is the coarse space of the stacky quotient $X(D; N)/H$.

*Remark* 2.7.6. It is a classical result [cite Shimura?] that $X_H(D; N)$ is a smooth geometrically integral curve defined over $\mathbb{Q}$.

*Remark* 2.7.7. Let $H \coloneqq \widehat{H} \cap (O/NO)^\times$. There exists a biholomorphism of complex Riemann surfaces

$$\varphi : X^B_{\widehat{H}}(\mathbb{C}) \xrightarrow{\sim} X_H(D; N)(\mathbb{C}),$$

thus bridging the two definitions of Shimura curves that we have given.

### 2.7.2 Point Counting via Moduli

We begin by recalling a classical result which says that QM-abelian surfaces over finite fields are "not so different" from elliptic curves.

**Lemma 2.7.8.** *Let $A$ be an $(O, \mu)$-QM abelian surface defined over $k = \mathbb{F}_q$ with* $\gcd(q, D) = 1$ *and* $\operatorname{char}(\mathbb{F}_q) = p$. *Then $A \sim_k E^2$, where $E$ is an elliptic curve defined over $k$.*

*Proof.* This result first appeared in [95, Lemma 6]. We give an abbreviated argument here (c.f. [22, Proposition 68 and Appendix] for a treatment when $k = \overline{k}$). Let $\ell$ be a prime coprime to $q$ and $T_\ell(A)$ be the $\ell$-adic Tate module of $A$. Since $A$ has $O$-QM over $\mathbb{F}_q$, $T_\ell(A)$ is a rank 1 $O$-module (as $\operatorname{rank}_{\mathbb{Z}} T_\ell(A) = 4$). Hence the $q$-Frobenius $\pi$-action on $T_\ell(A)$ is given by right multiplication by some element $x \in O$. Hence $P_A(T) = f(T)^2$, where $f(T)$ is the reduced characteristic polynomial of $x$ (of degree 2). By Honda-Tate theory

[43][86], either $A \sim_{\mathbb{F}_q} E^2$ where $E$ is an elliptic curve defined over $\mathbb{F}_q$ or $A$ is $\mathbb{F}_q$-simple. We now proceed to rule out the latter case. Suppose $A$ is $\mathbb{F}_q$-simple. Then once again by Honda-Tate theory, $\mathrm{End}(A)_{\mathbb{Q}}$ is a division algebra with center $\mathbb{Q}(\pi)$ with either $\mathbb{Q}(\pi) = \mathbb{Q}$ or a quadratic field $K$. When $\mathbb{Q}(\pi) = \mathbb{Q}$, then $A$ is necessarily $\mathbb{F}_q$-isogenous to the square of a supersingular elliptic curve whose endomorphism algebra is ramified at $p$ and $\infty$, contradicting that $B$ is unramified at $p$. If $\mathbb{Q}(\pi) = K$, then $\mathrm{End}(A)_{\mathbb{Q}}$ is unramified at all finite places, which contradicts the fact that $B$ is a division algebra. □

We now restrict ourselves to $k = \mathbb{F}_p$ and analyze the cases according to whether $E$ is ordinary or supersingular. Since we are interested in counting $\mathbb{F}_p$-isomorphism classes of $O$–QM abelian surfaces, in both cases we start by upgrading Lemma 2.7.8 to a statement about isomorphisms. Recall that $\mathrm{End}_{\mathbb{F}_p}(E)$ of $E/\mathbb{F}_p$ is always an imaginary quadratic order regardless of whether $E$ is ordinary or supersingular.

**Definition 2.7.9.** Let $K$ be a quadratic field and $R$ an order in $M_n(K)$. Then the center $Z(R)$ of $R$ is an order of $K = Z(M_n(K))$. We define the *central conductor* of $R$ to be

$$f_R \coloneqq f_{Z(R)} = [\mathbb{Z}_K : Z(R)],$$

which uniquely determines $Z(R)$.

For $E/\mathbb{F}_p$ an elliptic curve, the (*endomorphism ring*) *conductor* $f_E$ is the conductor of the order $\mathrm{End}(E)$ in the ring of integers $\mathbb{Z}_K$ of $\mathrm{End}(E)_{\mathbb{Q}} = K$ for some imaginary quadratic field $K$.

Let $A/\mathbb{F}_p$ be an abelian surface which is isogenous to $E^2$ over $\mathbb{F}_p$. The *central conductor* $f_A$ of $A$ is the central conductor of the order $\mathrm{End}(A)$ in $\mathrm{End}(A)_{\mathbb{Q}} \cong \mathrm{End}(E^2)_{\mathbb{Q}} \cong M_2(K)$ for some imaginary quadratic field $K$. Denote $Z(\mathrm{End}(A))$ by $O(f_A)$, where $O(f_A)$ is the order in $\mathbb{Z}_K$ of conductor $f_A$. We say $(A, \iota)$ has CM by $O(f_A)$.

**Theorem 2.7.10** (Kani)**.** *If $A/\mathbb{F}_p$ is an abelian surface which is isogenous to $E^2$ over $\mathbb{F}_p$,* *where $E$ is an ordinary elliptic curve defined over $\mathbb{F}_p$, then there exists ordinary elliptic curves $E_1$ and $E_2$ such that we have an isomorphism $A \cong E_1 \times E_2$ over the base field $\mathbb{F}_p$.*

*Furthermore, fixing an ordinary elliptic curve $E/\mathbb{F}_p$ with $\mathrm{End}(E)_{\mathbb{Q}} = K$, an imaginary quadratic field, there exists a bijection between the set of $\mathbb{F}_p$-isomorphism classes $[E']$ of elliptic curves $E'$ isogenous to $E$ with conductor $f_{E'}|f_E$, and the set of $\mathbb{F}_p$-isomorphism classes of abelian surfaces $A/\mathbb{F}_p$ isogenous to $E^2$ with corresponding central conductor $f_A = f_E$. Explicitly, this bijection is given by $[E'] \mapsto [E' \times E]$.*

*Proof.* See [53, Theorems 2, 67]. □

*Remark* 2.7.11. Kani's theorems [53] in fact holds over arbitrary base fields (over fields of characteristic 0, the condition that $E$ is ordinary is appropriately replaced by $E$ is CM).

The following result further strengthens Kan's theorem.

**Proposition 2.7.12.** *Let $(A, \iota)/k$ be a QM abelian surface with CM by $S \subseteq O_K$ for some imaginary quadratic field $K$. Fix $E_1/k$ any elliptic curve with $S$-CM. Then there exists an $S$-CM elliptic curve $E_2/k$, unique up to $k$-isomorphism, such that $A \cong E_1 \times E_2$ over $k$.*

*Proof.* See [80, Corollary 2.14]. □

The analogous result holds for supersingular $E/\mathbb{F}_p$.

**Lemma 2.7.13.** *Let $R$ be a quadratic order, i.e. an order in a degree 2 extension $K$ of $\mathbb{Q}$. Let $M$ be a finitely presented (f.p.) torsion-free $R$-module.*

1. *There exists a unique chain of orders $R_1 \subseteq \cdots \subseteq R_n$ between $R$ and $K$ and invertible ideals $I_1, \ldots, I_n$ of $R_1, \ldots, R_n$, respectively, such that $M \cong I_1 \oplus \cdots \oplus I_n$ as an $R$-module.*

2. *The $I_i$ are not unique, but their product $I_1 \cdots I_n$ is an invertible $R_n$-ideal whose class $[M] \in \mathrm{Pic}\, R_n$ depends only on $M$.*

3. *The isomorphism type of $M$ is uniquely determined by the chain $R_1 \subseteq \cdots \subseteq R_n$ and the class $[M] \in \operatorname{Pic} R_n$.*

*Proof.* See [15]. $\square$

**Proposition 2.7.14.** *Let $A$ be an $O$-QM abelian surface defined over $\mathbb{F}_p$ such that $A \sim_{\mathbb{F}_p} E^2$ where $E$ is a supersingular elliptic curve defined over $\mathbb{F}_p$. Then there exists supersingular elliptic curves $E_1$ and $E_2$ defined over $\mathbb{F}_p$ such that $A \cong E_1 \times E_2$ over $\mathbb{F}_p$.*

*Proof.* Consider the two functors

$$\begin{aligned}\mathscr{H}om(-,E) :&\{\text{f.p. torsion-free left } R\text{-modules}\}^{\text{opp}} \\ &\to \{\text{abelian varieties isogenous to a power of } E\},\end{aligned}$$

and

$$\begin{aligned}\operatorname{Hom}(-,E) :&\{\text{abelian varieties isogenous to a power of } E\} \\ &\to \{\text{f.p. torsion-free left } R\text{-modules}\}^{\text{opp}}.\end{aligned}$$

For $E/\mathbb{F}_p$ supersingular, the above two functors are equivalence of categories [52, Section 7.3] except for the case where $p \equiv 3 \bmod 4$ and $\mathbb{Z}[\sqrt{-p}] \neq \operatorname{End} E$ as shown in the table in [52, Section 7.3]. Without loss generality, we may always assume that $\mathscr{H}om(-,E)$ and $\operatorname{Hom}(-,E)$ are equivalences of categories: for if we are in the case where $p \equiv 3 \bmod 4$ and $\mathbb{Z}[\sqrt{-p}] \neq \operatorname{End} E$, we may replace $E$ by an elliptic curve $E'/k$ isogenous to $E$ such that $\operatorname{End} E' = \mathbb{Z}[\sqrt{-p}]$ [92, Theorem 4.2]. By Lemma 2.7.13(1), a f.p. torsion-free $R$-module is a direct sum of rank 1 f.p. torsion-free $R$-modules. Hence the equivalence of categories together with Lemma 2.7.13(1) implies that $A \cong E_1 \times E_2$ over $\mathbb{F}_p$. $\square$

*Remark* 2.7.15. The above statement also holds over $\mathbb{F}_{p^2}$ (c.f. [52, Theorem 5.3c]) and $\overline{\mathbb{F}}_p$, but is false over $\mathbb{F}_{p^n}$ for $n > 2$, which gives rise to a challenge to extend the present argument beyond $\mathbb{F}_p$.

There is also the following analogue of the second part of Theorem 2.7.10 in the supersingular case.

**Proposition 2.7.16.** *Fix a supersingular elliptic curve $E$ over $\mathbb{F}_p$ such that $R := \operatorname{End} E = \mathbb{Z}[\sqrt{-p}]$. There is a bijection between the set of $\mathbb{F}_p$-isomorphism classes of abelian surfaces $A \sim_k E^2$ such that $f_A | f_E$ and the set of $\mathbb{F}_p$-isomorphism classes of products of elliptic curves $E_1 \times E_2$ where each $E_i$ is $k$-isogenous to $E$ together with $f_{E_i} | f_E$.*

*Proof.* This is a restatement of [52, Theorem 7.11] combined with Proposition 2.7.14. $\square$

The next result explains how to count the number of QM-structures given $A$.

**Lemma 2.7.17.** *The number of $\mathbb{F}_p$-isomorphism classes $(O, \mu)$-QM abelian surfaces $(A, \iota)$ with $CM$ by $S \subseteq \mathbb{Z}_K$ for some imaginary quadratic field $K$ is given by $m(S, O; O^\times)$.*

*Proof.* We need to show that

1. given an $O$-QM abelian surface, we get an optimal embedding $S \hookrightarrow O$
2. an optimal embedding $S \hookrightarrow O$ gives rise to an $O$-QM abelian surface $(A, \iota)$
3. two $O$-QM abelian surfaces $(A_1, \iota_1), (A_2, \iota_2)$ corresponding to optimal embeddings $\varphi_1, \varphi_2 : S \to O$ are isomorphic if and only if $\varphi_1$ and $\varphi_2$ are $O^\times$-conjugate.

Fix an imaginary quadratic field $K$ and an order $S \supseteq \mathbb{Z}_K$. Let $(A, \iota)$ be an $O$-QM abelian surface with $CM$ by $S$. Then Lemma 2.7.12 (or Lemma 2.7.16) combined with [91, Lemma 5.4.7] imply the existence of an embedding $\varphi : K \hookrightarrow B$. A priori, $\varphi(S) \subseteq O'$ for some maximal order $O'$. By strong approximation, $O$ and $O'$ are conjugates, so we may assume without loss of generality that $\varphi : S \hookrightarrow O$. Optimality of $\varphi$ follows from the fact that $Z(\operatorname{End}(A)) = S$ by hypothesis.

Conversely, let $\varphi : S \hookrightarrow O$ be an optimal embedding. After extending scalars and applying [91, Lemma 5.4.7], we obtain an embedding $\iota : B \hookrightarrow M_2(K)$. Let $E$ be an $S$-CM elliptic curve defined over $k$. Take $A = E^2$. Then $(A, \iota)$ is $O$-QM. □

*Remark* 2.7.18. The complex-analytic analogue of Lemma 2.7.17 is [2, Theorem 6.13] specialized to the case $N = 1$.

**Lemma 2.7.19.** *Let $(A, \iota)/\mathbb{F}_p$ be an $(O, \mu)$-QM abelian surface with CM by $\mathbb{Z}[x]/(x^2 - tx + p) \subseteq S \subseteq \mathbb{Z}_K$ for some imaginary quadratic field $K$. Then we have*

$$\#\operatorname{Aut}_k((A, \iota)) = \begin{cases} \#S^\times/2, & \text{if } t \neq 0, \text{ and} \\ \#S^\times & \text{if } t = 0. \end{cases}$$

*Proof.* This follows from the fact that $\pm P$ are $\mathrm{GL}_2(K)$-conjugate if and only if $\mathrm{Tr}(P) = 0$. □

**Theorem 2.7.20.** *Let $p$ be a prime number with $(p, D) = 1$. The number of $\mathbb{F}_p$–points on the Shimura curve $X(D; 1)$ is given by*

$$\#X(D;1)(\mathbb{F}_p) = \sum_{t^2-4p<0} \sum_{\substack{S \supseteq \\ \mathbb{Z}[x]/(x^2-tx+p)}} \frac{h(S)}{\#S^\times} m(\widehat{S}, \widehat{O}; \widehat{O}^\times). \tag{2.11}$$

*Proof.* By Propositions 2.7.12 and 2.7.16, every $\mathbb{F}_p$-point of $X(D; 1)$ corresponds to an $(O, \mu)$-QM abelian surface $(A, \iota)$ with CM by some imaginary imaginary quadratic order $S \supseteq \mathbb{Z}[x]/(x^2 - tx + p)$. By Lemma 2.7.17, there are $m(S, O; O^\times)$ $\mathbb{F}_p$-isomorphism classes of $(O, \mu)$-QM abelian surfaces with CM by $S$, for each such imaginary quadratic order $S$. In addition, when we sum over pairs of integers $(t, p)$ with $t \neq 0$ such that $t^2 - 4p < 0$ and orders $S \supseteq \mathbb{Z}[x]/(x^2 - tx + p)$, each such $S$ is summed twice corresponding to $\pm t$.

Combining all of the above and Lemma 2.7.19, We have

$$
\begin{aligned}
\# X(D,1)(\mathbb{F}_p) &= \frac{1}{2}\sum_{\substack{t^2-4p<0\\ t\neq 0}} \sum_{\substack{S\supseteq\\ \mathbb{Z}[x]/(x^2-tx+p)}} \frac{m(S,O;O^\times)}{\# S^\times/2} + \sum_{\substack{S\supseteq\\ \mathbb{Z}[x]/(x^2-p)}} \frac{m(S,O;O^\times)}{\# S^\times}\\
&= \sum_{t^2-4p<0} \sum_{\substack{S\supseteq\\ \mathbb{Z}[x]/(x^2-tx+p)}} \frac{m(S,O;O^\times)}{\# S^\times}\\
&= \sum_{t^2-4p<0} \sum_{\substack{S\supseteq\\ \mathbb{Z}[x]/(x^2-tx+p)}} \frac{h(S)}{\# S^\times} m(\widehat{S},\widehat{O};\widehat{O}^\times),
\end{aligned}
$$

where in the last equality we have made use of the fact that $m(S,O;O^\times) = h(S)m(\widehat{S},\widehat{O};\widehat{O}^\times)$ as $B$ is indefinite and $\#\operatorname{Cls} O = 1$, c.f. [91, Theorem 28.2.11]. □

## 2.8 Trace formula for definite quaternion algebras

Though not needed for the purpose of computing isogeny decompositions of Jacobians of Shimura curves, we also give a trace formula in the definite case. Let $B$ be a definite quaternion algebra over $\mathbb{Q}$ of discriminant $D$. Let $O$ be an order in $B$, $\widehat{H} \leq \widehat{O}^\times$ an open compact subgroup of level $N$, and $n \in \mathbb{N}$ with $(n, DN) = 1$. We give an explicitly computable trace formula for the Hecke operators $T_n$ acting on the space of weight 2 modular forms of level $\widehat{H}$ as defined in Definition 1.3.3.

Since the set $B^\times\backslash\widehat{B}^\times/\widehat{H}$ is finite, we write

$$\widehat{B}^\times = \coprod_{i=1}^{n} B^\times \widehat{\beta}_i \widehat{H}.$$

Each point $B^\times\widehat{\beta}_i H$ is equipped with a finite stabilizer group $\Gamma_i := \widehat{\beta}_i\widehat{H}\widehat{\beta}_i^{-1} \cap B^\times$. There is an isomorphism of $\mathbb{C}$-vector spaces given by

$$M_2^B(\widehat{H}) \to \bigoplus_{i=1}^{n} H^0(\Gamma_i, \mathbb{C})$$
$$f \mapsto (f(\hat{\beta}_i))_{i=1}^n.$$

We treat all such subgroups $\widehat{H}$ systematically by reducing to the maximal order case; we assume from now on that $O_0(1) = O$ is a maximal order. Define $\operatorname{CoInd}_{\widehat{H}}^{\widehat{O}_0(1)^\times}(\mathbb{C}) = \operatorname{Map}(\widehat{O}_0(1)^\times/\widehat{H}, \mathbb{C})$. There is an isomorphism of $\mathbb{C}$-vector spaces

$$M_2^B(\widehat{H}) \to M_2^B(\widehat{O}_0(1)^\times, \operatorname{CoInd}_{\widehat{H}}^{\widehat{O}_0(1)^\times}(\mathbb{C}))$$

that is Hecke equivariant for all Hecke operators $T_n$ with $(n, N) = 1$. We give a decomposition of $M_2^B(\widehat{O}_0(1)^\times, \operatorname{CoInd}_{\widehat{H}}^{\widehat{O}_0(1)^\times}(\mathbb{C}))$ analogous to the one for $M_2^B(\widehat{H})$ above.

Let $I_1, \ldots, I_h$ be representatives for $\operatorname{Cls} O_0(1)$ with $h = \#\operatorname{Cls} O_0(1)$, and let $I_i := \widehat{\alpha}_i \widehat{O}_0(1) \cap B$. By strong approximation (see, e.g., [91, Proposition 28.5.18]), we may assume that $(\operatorname{nrd}(I_i), DN) = 1$, for $i = 1, \ldots, h$. Let $O_0(1)_i := O_L(I_i) = \widehat{\alpha}_i \widehat{O}_0(1) \widehat{\alpha}_i^{-1} \cap B$ be the left order of $I_i$. We have $(O_0(1)_i)_p = O_0(1)_p$ for all $p \nmid DN$. As before, we have the Hecke equivariant isomorphisms of $\mathbb{C}$-vector spaces

$$M_2^B(\widehat{H}) \cong M_2^B(\widehat{O}_0(1)^\times, \operatorname{CoInd}_{\widehat{H}}^{\widehat{O}_0(1)^\times}(\mathbb{C})) \cong \bigoplus_{i=1}^{h} H^0(O_0(1)_i^\times, \operatorname{CoInd}_{\widehat{H}}^{\widehat{O}_0(1)^\times}(\mathbb{C})).$$

The definition of Hecke operators given in Section 1.4 can be reinterpreted as follows (c.f. [27, Section 8]). For $n \in \mathbb{Z}$, we define

$$\Theta(n)_{i,j} := O_0(1)_i^\times \backslash \{x \in I_i I_j^{-1} : \operatorname{nrd}(x I_i I_j^{-1}) = n\},$$

Let $\Theta(n)_i := \Theta(n)_{i,i}$ and $M_2^B(\widehat{H})_i := H^0(O_0(1)_i^\times, \operatorname{CoInd}_{\widehat{H}}^{\widehat{O}_0(1)^\times}(\mathbb{C}))$. The Hecke operator

$T_n : M_2^B(\widehat{H}) \to M_2^B(\widehat{H})$ is defined component-wise by

$$\begin{aligned}(T_n)_{i,j} : M_2^B(\widehat{H})_i &\to M_2^B(\widehat{H})_j \\ f &\mapsto \sum_{\alpha \in \Theta(n)_{i,j}} \alpha \cdot f.\end{aligned}$$

The space $\mathrm{CoInd}_{\widehat{H}}^{\widehat{O}_0(1)^\times}(\mathbb{C})$ comes with a natural permutation representation $\rho$ of $\widehat{O}_0(1)^\times$ by left multiplication as follows: for $\widehat{u}, \widehat{x} \in \widehat{O}_0(1)^\times$, $h \in \mathrm{CoInd}_{\widehat{H}}^{\widehat{O}_0(1)^\times}(\mathbb{C})$, $(\widehat{u}h)(\widehat{x}\widehat{H}) = h(\widehat{u}\widehat{x}\widehat{H})$. We let $\rho_i$ denote its restrictions to $H^0(O_0(1)_i^\times, \mathrm{CoInd}_{\widehat{H}}^{\widehat{O}_0(1)^\times}(\mathbb{C}))$. Since $H_p = O_0(1)_p^\times$ for all primes $p \nmid N$, the representation $\rho$ factors through $\prod_{p|N} O_0(1)_p^\times$, and hence $\rho$ extends to $\widehat{B}_{(N)}^\times := \{(\alpha_p) \in \widehat{B}^\times : \alpha_p \in O_0(1)_p^\times \text{ for all } p|N\}$, which we also denote by $\rho$ by abuse of notations. In particular, $\rho$ and $\rho_i$ are well-defined on the $\Theta(n)_i$'s.

**Example 2.8.1.** Let $B = \left(\frac{-1,-23}{\mathbb{Q}}\right)$ and

$$O_0(1) = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}\frac{1+j}{2} + \mathbb{Z}i\frac{1+j}{2},$$

a maximal order in $B$. Since $3 \nmid 23$, $O_0(1)_3 \cong M_2(\mathbb{F}_3)$. Consider the Eichler order of level 3

$$O_0(3) = \{x \in O_0(1) : x \text{ upper triangular } \bmod 3\} \leq O_0(1).$$

We have $O_0(1)_3^\times / O_0(3)_3^\times \cong \mathrm{GL}_2(\mathbb{F}_3)/B_2(\mathbb{F}_3)$. Thus $\dim_{\mathbb{C}} \mathrm{CoInd}_{\widehat{O}_0(3)^\times}^{\widehat{O}_0(1)^\times}(\mathbb{C}) = 4$. By Strong Approximation, we have representatives $I_1, I_2, I_3$ of $\mathrm{Cls}\, O_0(1)$ with $N(I_i) = 7^{i-1}$, $i = 1, 2, 3$. Let $O_i = O_L(I_i)$ be the left order of $I_i$. We have $O_i^\times \cong \mathbb{Z}[i]^\times, \mathbb{Z}^\times, \mathbb{Z}[\omega]^\times$, respectively, where $\omega = (-1+\sqrt{3})/2$; $i$ and $\omega$ act on $O_0(1)_3^\times / O_0(3)_3^\times$ as $(1,4)(2,3)$ and $(1,2,4)(3)$, respectively. Hence we obtain that

$$\dim_{\mathbb{C}} H^0(O_i^\times, \mathrm{CoInd}_{\widehat{O}_0(3)^\times}^{\widehat{O}_0(1)^\times}(\mathbb{C})) = 2, 4, 2, \text{ respectively.}$$

To compute the trace of $T_5$ acting on $M_2^B(\widehat{O}_0(3)^\times)$, we begin by computing $\Theta(5)_i$ using the proof of [91, Lemma 41.2.7] (equiv. [26, Algorithm 2.1]). We have

$$\begin{aligned}
&\Theta(5)_1 = \{2+i, 2-i\},\\
&\Theta(5)_2 = \{1-9i/7+j/7+2k/7, 1+9i/7-j/7-2k/7\}, \text{ and}\\
&\Theta(5)_3 = \emptyset.
\end{aligned}$$

We compute the permutation action of the $\Theta(5)_i$'s on $O_0(1)_3^\times/O_0(3)_3^\times$:

| | **permutation representation** | **trace** |
|---|---|---|
| $2+i$ | (1,3,4,2) | 0 |
| $2-i$ | (1,2,4,3) | 0 |
| $1-9i/7+j/7+2k/7$ | (1,4,2,3) | 0 |
| $1+9i/7-j/7-2k/7$ | (1,3,2,4) | 0 |

and conclude that $\operatorname{Tr} T_5|M_2^B(\widehat{O}_0(3)^\times) = 0$.

Before stating the trace formula, we first examine how $\operatorname{Tr}\rho$ differs from $\operatorname{Tr}\rho_i$. From now on, assume $B \not\cong (-1,-1|\mathbb{Q})$ or $(-3,-1|\mathbb{Q})$. By [91, Theorem 11.5.14], $O_0(1)_i^\times$ is isomorphic to one of $\mathbb{Z}^\times, \mathbb{Z}[i]^\times$, or $\mathbb{Z}[\omega]^\times$, where $\omega = (-1+\sqrt{3})/2$.

**Lemma 2.8.1.** *As before, let* $\rho : \widehat{O}_0(1)^\times \to \mathrm{GL}(\mathrm{CoInd}_{\widehat{H}}^{\widehat{O}_0(1)^\times}(\mathbb{C}))$ *and*

$$\rho_i : \widehat{O}_0(1)^\times \to \mathrm{GL}(H^0(O_0(1)_i, \mathrm{CoInd}_{\widehat{H}}^{\widehat{O}_0(1)^\times}(\mathbb{C}))).$$

*We have*

$$\operatorname{Tr}\rho_i(x) = \frac{1}{|O_0(1)_i^\times|}\sum_{u\in O_0(1)_i^\times} \operatorname{Tr}(\rho(ux)), \text{ for all } x \in \widehat{O}_0(1)^\times.$$

*In particular,* $\dim_{\mathbb{C}} H^0(O_0(1)_i, \mathrm{CoInd}_{\widehat{H}}^{\widehat{O}_0(1)^\times}(\mathbb{C})) = \operatorname{Tr}\rho_i(1)$.

*Proof.* For ease of notation, let $R \coloneqq O_0(1)_i$, and $V \coloneqq \mathrm{CoInd}_{\widehat{H}}^{\widehat{O}_0(1)^\times}(\mathbb{C})$. Consider the projection operator $P : V \to V^{R^\times}$ defined by averaging over $R^\times$:

$$P(v) \coloneqq \frac{1}{|R^\times|} \sum_{u \in R^\times} \rho(u)v.$$

For $x \in \widehat{O}_0(1)^\times$, the trace $\operatorname{Tr}\rho'(x)$ is the contribution of $\operatorname{Tr}\rho(x)$ to $V^\times$, and is hence given by

$$\operatorname{Tr}\rho'(x) = \operatorname{Tr}(P \circ \rho(x)) = \frac{1}{|R^\times|} \sum_{u \in R^\times} \operatorname{Tr}(\rho(ux)).$$

$\square$

**Theorem 2.8.2** (Trace Formula: Definite Case)**.** *Let $B$ be a definite quaternion algebra over $\mathbb{Q}$ of discriminant $D$, $O_0(1)$ a maximal order in $B$, and $\widehat{H} \leq \widehat{O}_0(1)^\times$ an open compact subgroup of level $N$. Let $\chi_{\widehat{H}}$ denote the character of $\rho$, and $A(t, b, S)$ be the same as in (2.9). For all square-free $n \in \mathbb{N}$ with $(n, DN) = 1$, we have that the trace of the Hecke operator $T_n$ acting on $M_2^B(\widehat{H})$ is given by*

$$\operatorname{Tr} T_n = \sum_{t^2 - 4n < 0} \sum_{\substack{S \supseteq \\ \mathbb{Z}[x]/(x^2 - tx + n)}} \frac{m(S, O_0(1); \Gamma_{\widehat{H}})}{w_S}.$$

*The sum is over*

- *finitely many integers $t \in \mathbb{Z}$ satisfying $t^2 - 4n < 0$ and*
- *quadratic orders $S \supseteq \mathbb{Z}[x]/(x^2 - tx + n)$.*

*We have adopted the following notations:*

- $w_i = \#O_0(1)_i^\times$*,* $w_S = \#S^\times$*, and* $h(S) = \#\operatorname{Pic}(S)$
- *For each $t \in \mathbb{Z}$ with $t^2 - 4n < 0$, let $K = \mathbb{Q}(\gamma)$ with $\mathrm{minpoly}_{\mathbb{Q}}(\gamma) = x^2 - tx + n$. Fix one embedding $K \hookrightarrow B$ with $\gamma \mapsto \alpha_0$.*

*Proof.* Since $B$ is definite, each $\alpha \in \Theta(n)_i$ has discriminant $\operatorname{disc}(\alpha) = t^2 - 4n < 0$, since we have assumed that $n$ is square-free. Thus we sum over finitely many $t \in \mathbb{Z}$ satisfying $t^2 - 4n < 0$. From the component-wise decomposition of $T_n$ and by Lemma 2.8.1, we have

$$\begin{aligned}
\operatorname{Tr} T_n &= \sum_{i=1}^{h} \sum_{\alpha \in \Theta(n)_i} \operatorname{Tr} \rho_i(\alpha) && (2.12)\\
&= \sum_{t^2-4n<0} \sum_{i=1}^{h} \sum_{\substack{\alpha \in \Theta(n)_i \\ \operatorname{trd}\alpha = t, \operatorname{nrd}\alpha = n}} \operatorname{Tr} \rho_i(\alpha) && (2.13)\\
&= \sum_{t^2-4n<0} \sum_{i=1}^{h} \sum_{\substack{\alpha \in \Theta(n)_i \\ \operatorname{trd}\alpha = t, \operatorname{nrd}\alpha = n}} \left( \frac{1}{w_i} \sum_{u \in O_0(1)_i^\times} \operatorname{Tr} \rho(u\alpha) \right) && (2.14)\\
&= \sum_{t^2-4n<0} \sum_{i=1}^{h} \frac{1}{w_i} \sum_{\substack{\alpha \in \Theta(n)_i \\ \operatorname{trd}\alpha = t, \operatorname{nrd}\alpha = n}} \left( \sum_{u \in O_0(1)_i^\times} \operatorname{Tr} \rho(u\alpha) \right) && (2.15)\\
&= \sum_{t^2-4n<0} \sum_{i=1}^{h} \frac{1}{w_i} \sum_{\substack{\alpha \in O_0(1)_i \\ \operatorname{trd}\alpha = t, \operatorname{nrd}\alpha = n}} \operatorname{Tr} \rho(\alpha). && (2.16)
\end{aligned}$$

Since $\operatorname{disc}(\alpha) < 0$, $\alpha \notin \mathbb{Q}$, and $\mathbb{Z}[\alpha] \cong \mathbb{Z}[x]/(x^2 - tx + n)$ is a domain. There is a one-to-one correspondence between $\{\alpha \in O_0(1)_i : \operatorname{trd}\alpha = t, \operatorname{nrd}\alpha = n\}$ and

$$\{\text{optimal } S \hookrightarrow O_0(1)_i : \text{quadratic orders } \mathbb{Z}[\alpha] \subseteq S \subset K\}.$$

Let $E_{S,i} = E_{S,O_0(1)_i}$. Recall that there is a bijection between $\operatorname{Emb}(S, O_0(1)_i; O_0(1)_i^\times)$ and $K^\times \backslash E_{S,i} / O_0(1)_i^\times$. The action of conjugation by $\mu \in O_0(1)_i^\times$ centralizes the embedding $S \hookrightarrow O_0(1)_i$ if and only if $\mu \in S^\times$. Hence we have

$$\sum_{\substack{\alpha \in O_0(1)_i \\ \operatorname{trd}\alpha = t, \operatorname{nrd}\alpha = n}} \operatorname{Tr} \rho(\alpha) = \sum_{\substack{S \supseteq \\ \mathbb{Z}[x]/(x^2 - tx + n)]}} \frac{w_i}{w_S} \sum_{\beta \in K^\times \backslash E_{S,i} / O_0(1)_i^\times} \operatorname{Tr} \rho(\beta^{-1}\alpha_0\beta). \tag{2.17}$$

Let $\widehat{E}_{\widehat{S}} = \{\widehat{\beta} \in \widehat{B}^\times : \widehat{\beta}^{-1}\widehat{K}\widehat{\beta} \cap \widehat{O}_0(1) = \widehat{\beta}^{-1}\widehat{S}\widehat{\beta}\}$. By the proof of [91, Theorem

30.4.7], there is a surjection of pointed sets

$$K^\times\backslash\widehat{E}_S/\widehat{O}_0(1)^\times \cong \coprod_{i=1}^{h}\operatorname{Emb}(S, O_0(1)_i; O_0(1)_i^\times) \cong \coprod_{i=1}^{h} K^\times\backslash E_{S,i}/O_0(1)_i^\times \twoheadrightarrow \widehat{K}^\times\backslash\widehat{E}_{\widehat{S}}/\widehat{O}_0(1)^\times, \tag{2.18}$$

and the fiber over each point is isomorphic to $K^\times\backslash\widehat{K}^\times/\widehat{S}^\times \cong \operatorname{Pic} S$. Continuing from (2.16), (2.17), and applying (2.18), we have

$$\operatorname{Tr} T_n = \sum_{t^2-4n<0}\sum_{i=1}^{h}\sum_{\substack{S\supseteq\\ \mathbb{Z}[x]/(x^2-tx+n)}}\frac{1}{w_S}\sum_{\beta\in K^\times\backslash E_{S,i}/O_0(1)_i^\times}\operatorname{Tr}\rho(\beta^{-1}\alpha_0\beta) \tag{2.19}$$

$$= \sum_{t^2-4n<0}\sum_{\substack{S\supseteq\\ \mathbb{Z}[x]/(x^2-tx+n)}}\frac{h(S)}{w_S}\sum_{\widehat{\beta}\in\widehat{K}^\times\backslash\widehat{E}_{\widehat{S}}/\widehat{O}_0(1)^\times}\operatorname{Tr}\rho(\widehat{\beta}^{-1}\alpha_0\widehat{\beta}). \tag{2.20}$$

In the last equality, we apply strong approximation to ensure that $\widehat{\beta}\alpha_0\widehat{\beta}$ is $p$-integral for all $p|N$.

The desired result now follows from Lemma 2.5.2. $\square$

**Corollary 2.8.3.** *With the same notations as in Theorem 2.8.2, for all $n \in \mathbb{N}$ with $(n, DN) = 1$, we have*

$$\operatorname{Tr} T_n = \sum_{\substack{t^2-4n<0,\\ S\supseteq\\ \mathbb{Z}[x]/(x^2-tx+n)}}\frac{m(S, O_0(1); \Gamma_{\widehat{H}})}{w_S} + \delta\operatorname{mass}(\operatorname{Cls} O_0(1))[\widehat{O}_0(1)^\times : \widehat{H}],$$

*where $\delta = 1, 0$ according as $n$ is square or not, and*

$$\operatorname{mass}(\operatorname{Cls} O_0(1)) \coloneqq 2\sum_{i=1}^{h}\frac{1}{w_i}.$$

*Proof.* Nothing changes from Theorem 2.8.2 when $n$ is not a square. When $n = k^2$, $k \in \mathbb{N}$, is a perfect square, we additionally have $\alpha = \pm k \in \Theta(n)_i$ for $i = 1, \ldots, h$. Since $k \in \mathbb{N}$,

$\operatorname{Tr}\rho(\pm k) = \operatorname{Tr}\rho(1)$, and hence the additional contribution to $\operatorname{Tr} T_n$ is given by

$$2\sum_{i=1}^{h} \frac{1}{w_i} \operatorname{Tr}\rho(1) = \operatorname{mass}(\operatorname{Cls} O_0(1)) \dim \operatorname{CoInd}_{\widehat{H}}^{\widehat{O}_0(1)^\times}(\mathbb{C}) = \operatorname{mass}(\operatorname{Cls} O_0(1))[\widehat{O}_0(1)^\times : \widehat{H}].$$

$\square$

**Acknowledgments**

Chapter 2 is, in part, based on the following paper being prepared for submission for publication, of with the dissertation author is a coauthor and collaborator.

- Yongyuan Huang, John Voight "Computing with Jacobians of Shimura curves: point counts and isogeny decomposition via trace formula".

# Part II

# Census of low-genus curves over small finite fields

# Chapter 3

# Census of curves of genus 5 over $\mathbb{F}_3$ and genus 6 & 7 over $\mathbb{F}_2$

## 3.1 Introduction

### 3.1.1 Overview

For $g > 1$, let $\mathcal{M}_g$ denote the moduli stack of curves of genus $g$. (All "curves" herein are smooth, projective, and geometrically irreducible unless otherwise specified.) For each prime power $q$, the set $\mathcal{M}_g(\mathbb{F}_q)$ of $\mathbb{F}_q$-valued points of $\mathcal{M}_g$ is finite; it is naturally identified with the set of isomorphism classes of curves of genus $g$ over $\mathbb{F}_q$. We equip $\mathcal{M}_g(\mathbb{F}_q)$ with the measure which gives the isomorphism class of a curve $C$ the weight $\frac{1}{\#\mathrm{Aut}(C)}$, as in the Lefschetz trace formula for Deligne–Mumford stacks [6]. Indeed, $\mathcal{M}_g(\mathbb{F}_q) \coloneqq \{x : \mathrm{Spec}(\mathbb{F}_q) \to \mathcal{M}_g\}$ is a groupoid, and the point count on $\mathcal{M}_g$ that we have defined is the groupoid cardinality

$$\#\mathcal{M}_g(\mathbb{F}_q) \coloneqq \sum_{[C]\in\mathcal{M}_g(\mathbb{F}_q)} \frac{1}{\#\,\mathrm{Aut}(C)}.$$

Here we count automorphisms of $C$ over $\mathbb{F}_q$ itself, not its base extension to an algebraic closure. Let $M_g$ denote the coarse moduli space of $\mathcal{M}_g$. The resulting stacky point count $\#M_g(\mathbb{F}_q)$ can also be interpreted as the number of geometric isomorphism classes of genus $g$ curves which admit a model over $\mathbb{F}_q$ (see Lemma 3.1.5 for the relationship between these two counting problems).

Since $\mathcal{M}_g$ has relative dimension $3g-3$ over $\mathbb{Z}$, the set $\mathcal{M}_g(\mathbb{F}_q)$ has order roughly $q^{3g-3}$ and thus is feasible to compute for small values of $g$ and $q$. We precisely state the computation of the set $\mathcal{M}_g(\mathbb{F}_q)$ as the *Census Problem* as follows.

*Problem* 3.1.1 (Census Problem). Given a prime power $q$ and $g > 0$, find one curve representing each isomorphism class in $\mathcal{M}_g(\mathbb{F}_q)$ and compute the $\mathbb{F}_q$-automorphism group of each representative curve.

A complete census of curves of genus $g$ over $\mathbb{F}_q$ is available in the following cases:

1. $g \leq 3$ and various $q$ by Sutherland and Howe [44] (see https://www.lmfdb.org/Variety/Abelian/Fq/Completeness for a complete list of $q$'s),

2. $g = 4, q = 2$ by Xarles [94],

3. $g = 4, q = 3$ by Howe [44] for the hyperelliptic case and Bergström–Faber–Payne [9] for the non-hyperelliptic case, and

4. $g = 5, q = 2$ by Dragutinović [28].

In this chapter, we discuss our work extending the censuses of curves to the following cases:

1. $g = 6$ and $q = 2$,

2. $g = 5$ and $q = 3$, and

3. $g = 7$ and $q = 2$.

### 3.1.2 Motivations

We discuss two primary motivations for our work.

### The Torelli locus

Let $\mathcal{A}_g$ denote the moduli space of $g$-dimensional principally polarized abelian varieties. There is an open embedding known as the *Torelli map*

$$\mathcal{T} : \mathcal{M}_g \to \mathcal{A}_g, X \mapsto \mathrm{Jac}(X).$$

We define the *open Torelli locus* $\mathcal{T}_g^\circ$ to be the image of $\mathcal{T}$, which is dense inside $\mathcal{A}_g$ for $g = 1, 2, 3$. However, since $\mathcal{A}_g$ has relative dimension $g(g+1)/2$ over $\operatorname{Spec}\mathbb{Z}$ for $g \geq 2$, $\mathcal{T}_g^\circ$ has positive codimension inside $\mathcal{A}_g$ for $g \geq 4$. Over finite fields, one can enumerate isogeny classes of abelian varieties by enumerating Weil polynomials by the Honda-Tate Theorem [43, 86], as is done to create the abelian varieties over finite fields section of the LMFDB [30]. It is then natural to ask the following.

*Question* 3.1.2. Which isogeny classes of principally polarized abelian varieties of dimension $g$ over $\mathbb{F}_q$ contain the Jacobian(s) of curve(s) of genus $g$ over $\mathbb{F}_q$?

**Example 3.1.1.** There are $235,942$ out of $267,465$ isogeny classes of abelian five-folds over $\mathbb{F}_3$ for which we do not know whether they contain Jacobians.

*Question* 3.1.3. Taking the numerator of the zeta function of a curve of genus $g$ over $\mathbb{F}_q$ defines a map $L : \mathcal{M}_g \to \{\text{degree } 2g\ q\text{-Weil polynomials}\}$. Given any arbitrary $q$-Weil polynomial of degree $2g$, what is $L^{-1}(f)$?

*Remark* 3.1.4. Question 3.1.3 naturally arises in [59], where a partial census of curves of genera 6 and 7 is needed to resolve the relative class number one problem for function fields; this also serves as a starting point for lots of our work discussed in this chapter, c.f. [59, Section 8].

### Polynomial point count of $\mathcal{M}_g$ and $\mathcal{M}_{g,n}$

Let $N_g(q) \coloneqq \#M_g(\mathbb{F}_q)$ be the number of geometric isomorphism classes of smooth projective curves of genus $g$ that are defined over $\mathbb{F}_q$. We also have $N_g(q) = \#\mathcal{M}_g(\mathbb{F}_q)$ by the following fact.

**Lemma 3.1.5.** *Let $\mathcal{X}$ be a Deligne–Mumford stack over a finite field $\mathbb{F}_q$ admitting a coarse moduli space $X$. Then $\#\mathcal{X}(\mathbb{F}_q) = \#X(\mathbb{F}_q)$.*

*Proof.* See [9, Proposition 1.3(3)]. $\square$

Well-known calculations have shown that

- $N_0(q) = 1$,
- $N_1(q) = q$,
- $N_2(q) = q^3$,
- $N_3(q) = q^6 + q^5 + 1$ [63], and
- $N_4(q) = q^9 + q^8 + q^7 - q^6$ [9].

Let $\mathcal{X}$ be a Deligne-Mumford stack. We have, by Behrend's extension of the Grothendieck-Lefschetz trace formula to Deligne-Mumford stacks [6, Theorem 3.1.2], that

$$\#\mathcal{X}(\mathbb{F}_q) = \sum_i (-1)^i \operatorname{Tr}(\operatorname{Frob}_q^* \,|H_c^i(\mathcal{X}, \mathbb{Q}_\ell)),$$

the alternating sum of the graded trace of Frobenius acting on the $\ell$-adic cohomology of $\mathcal{X}$ with compact support for any $(\ell, q) = 1$. We say $\mathcal{X}$ has a *polynomial point count* when there exists a polynomial $P(q) \in \mathbb{Z}[q]$ such that $\mathcal{X}(\mathbb{F}_q) = P(q)$ for all prime powers $q$. The above results imply that $\mathcal{M}_g$ has a polynomial point count for $g \leq 4$. [19] has also shown that $\mathcal{M}_5$ and $\mathcal{M}_6$ have polynomial point counts, and more recently [20, Theorem 1.1] shows that $\mathcal{M}_g$ has a polynomial point count if and only if $g \leq 8$; the aforementioned results all rely a very careful analysis of the cohomology groups of $\mathcal{M}_g$ and the Grothendieck-Lefschetz trace formula. The rational cohomology of $\mathcal{M}_g$ can be computed using the tautological Chow ring. The latter can be computed using the SageMath package described in [25];

by so doing, one can recover the explicit polynomials for $g = 4, 5,$ and 6 (see [10, Section 4] or [9, Theorem 1.5] for $g = 4$ and [8] for $g = 5, 6$). In particular, we have

$$N_5(q) = q^{12} + q^{11} + q^{10} - q^8 + 1, \text{ and} \tag{3.1}$$

$$N_6(q) = q^{15} + q^{14} + 2q^{13} + q^{12} - q^{10} + q^3 - 1. \tag{3.2}$$

The computation of the polynomial formula for $N_7(q)$ and $N_8(q)$ remains infeasible using [25] at the time of writing. In general, a putatively complete census of $\mathcal{M}_g(\mathbb{F}_q)$ only gives a lower bound for $N_g(q)$. The polynomial formula for $N_g(q)$ can sometimes also serve as an independent check of the completeness of the census, c.f. Section 3.6.

Let $\mathcal{M}_{g,n}$ be the moduli stack of $n$-pointed genus $g$ curves (where the points are distinct and indistinguishable) and $N_{q,n} := \#\mathcal{M}_{g,n}(\mathbb{F}_q)$. [20, Theorem 1.4] shows that the smallest integer $n$ such that $N_{g,n}$ is not a polynomial is $\max\{\lceil(25 - 3g)/2\rceil, 0\}$, for $g \geq 1$. In particular, $\mathcal{M}_{g,n}$ has a polynomial point count when $3g + 2n < 25$. In such cases, consequent of the Lefschetz trace formula, the polynomial formula for $N_{g,n}(q)$ can also in principle be computed in terms of the tautological Chow ring [25, 8], but this computation becomes quite difficult for large $g, n$. Our results supplement these computations by allowing us to read off the exact values of $\#\mathcal{M}_{6,n}(\mathbb{F}_2), \#\mathcal{M}_{5,n}(\mathbb{F}_3)$, and $\#\mathcal{M}_{7,n}(\mathbb{F}_2)$ (as well as $\#\mathcal{M}_{6,n}/S_n(\mathbb{F}_2)$, etc.) for any $n$, thereby reducing the number of cohomology groups needed to pin down the full formulas. Knowing these polynomials would also be beneficial to the computation of the polynomial formula for $N_7(q)$ and $N_8(q)$.

### 3.1.3 Main Results and Applications

Our main result is as follows.

**Theorem 3.1.6.** *We obtain an explicit list of isomorphism class representatives for*

$\mathcal{M}_6(\mathbb{F}_2)$*: it consists of* 72227 *elements, and for the weighting by automorphisms we have*

$$\#\mathcal{M}_6(\mathbb{F}_2) = 68615. \tag{3.3}$$

A tabulation of curves of genus $g$ also yields, for every positive integer $n$, a point count for the stack $\mathcal{M}_{g,n}$ of $n$-pointed genus $g$ curves (where the points are distinct and distinguishable) or more generally any quotient of $\mathcal{M}_{g,n}$ by a subgroup of $S_n$. For example, Theorem 3.1.6 yields the following.

**Corollary 3.1.7.** *We have*

$$\#\mathcal{M}_{6,1}(\mathbb{F}_2) = 223317, \tag{3.4}$$

$$\#(\mathcal{M}_{6,2}/S_2)(\mathbb{F}_2) = 471210, \tag{3.5}$$

$$\#\mathcal{M}_{6,2}(\mathbb{F}_2) = 650838, \tag{3.6}$$

$$\#(\mathcal{M}_{6,3}/S_3)(\mathbb{F}_2) = 927153, \tag{3.7}$$

$$\#\mathcal{M}_{6,3}(\mathbb{F}_2) = 1679646, \tag{3.8}$$

$$\#(\mathcal{M}_{6,4}/S_4)(\mathbb{F}_2) = 1794569. \tag{3.9}$$

In all but the last case, [20, Theorem 1.5] implies that the point count over $\mathbb{F}_q$ is a polynomial in $q$, but as of now the computation of these polynomials remains infeasible using [25]. Our computation provides one linear constraint on the coefficients of the polynomial, and thus reduces by one the number of rational cohomology groups that need to be computed in order to determine the polynomial. (One could adapt our methods to perform a census over $\mathbb{F}_3$ and thus obtain a second linear constraint; we do not plan to do this.)

Our final results for genus $5/\mathbb{F}_3$ and genus $7/\mathbb{F}_2$ are pending ongoing computations.

Our general strategy for solving Problem 3.1.1 goes as follows:

1. For each stratum, start by constructing a finite "covering" set of curves that is guaranteed to meet every isomorphism class and is "not too redundant".

2. Apply a separate postprocessing step to remove redundancies.

Our aim is to design Step (1) as carefully as possible so that Step (2) does not become computationally intractable under the computational resources available to us. Step (2) typically involves making extensive use of Magma's implementation of function fields to identify isomorphic curves and compute their automorphism groups. Step (1), in comparison, requires a concrete description of the stratification of the moduli space $\mathcal{M}_g$ of interest.

For $g = 5, q = 3$, our approach mirrors and extends the work of [28]; in particular, we separately tabulate hyperelliptic curves, trigonal curves, and complete intersections of three quadrics in $\mathbf{P}^4$. One difference is that since now $q$ is odd, we can handle the hyperelliptic case using the approach of Howe [44].

On the other hand, in the cases $g = 6, 7$ and $q = 2$, our approach follows the partial census carried out in [59]: for each stratum in the Brill–Noether stratification of $\mathcal{M}_6$ and $\mathcal{M}_7$, respectively, we use the descriptions of general canonical curves in each stratum (due to Mukai [67] for the generic stratum) to construct a covering set for the isomorphism classes of curves over $\mathbb{F}_2$ in that stratum. In several cases, we use the ***orbit lookup trees*** introduced by Kedlaya (c.f. [59, Appendix A], and further improved in [58]) to efficiently compute orbit representatives for the action of a group $G$ on $n$-element subsets (resp. $n$-dimensional subspaces) of a finite set $S$ (resp. a finite dimensional vector space $V$) equipped with a left $G$-action for small values of $n$.

A list of isomorphism class representatives, as well as the SageMath [79] and Magma [16] code used to generate it, can be found at

https://github.com/junbolau/genus-6

for curves of genus 6 over $\mathbb{F}_2$, https://github.com/stevehuang235/genus-5-F3

for curves of genus 5 over $\mathbb{F}_3$, and

https://github.com/junbolau/genus-7

for curves of genus 7 over $\mathbb{F}_2$.

Our censuses answer Question 3.1.3 in the respective cases; for example, one can now prove the following statements via a query of our table of curves.

- Out of the 164937 isogeny classes of abelian sixfolds over $\mathbb{F}_2$, 38327 of them contain at least one Jacobian, representing all 20 of the possible Newton polygons, and that the maximum number of Jacobians in a single isogeny class is 20.
- The maximum number of $\mathbb{F}_2$-points on a curve of genus 6 is 10, achieved by exactly two curves [75].
- There are 70 supersingular curves of genus 6 over $\mathbb{F}_2$, with 28 distinct zeta functions.
- The only groups that arise as automorphism groups of curves of genus 6 over $\mathbb{F}_2$ are

$$C_1, C_2, C_3, C_4, C_2 \times C_2, C_5, C_6, S_3, C_{10}, D_5, D_{10}, A_5.$$

- There is no curve of genus 6 over $\mathbb{F}_2$ with any of the three possible zeta functions for an *excessive* genus 6 curve allowed by [34, Theorem 3.2]. We thus recover [34, Theorem 5.1]: the maximum gonality of a curve of genus 6 over $\mathbb{F}_2$ is 6.
- There is no curve $C$ of genus 6 over $\mathbb{F}_2$ with $\#C(\mathbb{F}_{2^4}) = 0$. This recovers the previous assertion as well as a nonexistence statement made in [56, Section 6].
- There is a unique curve $C$ of genus 6 over $\mathbb{F}_2$ with $(\#C(\mathbb{F}_{2^i}))_{i=1}^6 = (0,0,0,20,15,90)$ [57, Lemma 10.2].

- As reported in [59, Table 1], there are 52 curves with zeta functions matching one of the options in [59, Table 2]. As shown in [57], this list includes every curve of genus 6 admitting an étale double cover with trivial relative class group.

- All 31 possible Newton polygons for abelian varieties of dimension 7 over $\mathbb{F}_2$ occur for Jacobians.

### 3.1.4 Contents

This chapter is organized as follows. We review the background on the classification of low genus curves in Section 3.2, including Mukai's stratification of $\mathcal{M}_6$ and $\mathcal{M}_7$. We discuss our data generation process for curves of genus 5 over $\mathbb{F}_3$ in Section 3.3, for curves of genus 6 over $\mathbb{F}_2$ in Section 3.4, and for curves of genus 7 over $\mathbb{F}_2$ in Section 3.5. We conclude by addressing the consistency check of Theorem 3.1.6 in Section 3.6, including a comment on possible consistency check for our upcoming results in genus 5 and 7.

### 3.1.5 Acknowledgments

We thank Samir Canning for discussions about [8], David Roe for importing our data into the abelian varieties over finite fields section of the LMFDB [62], and Edgar Costa for assistance with the server at MIT.

## 3.2 Background on the Classification of Curves and the Brill-Noether Stratifications

Throughout this discussion, let $C$ be a curve of genus $g$ over a finite field $k$ and let $\overline{k}$ be an algebraic closure of $k$. Let $K$ be the canonical divisor on $C$, and $|K|$ be the canonical linear system.

A $g^r_d$ on $C$ is a linear system of dimension $r$ and degree $d$, which if basepoint-free defines a degree $d$ morphism $C \to \mathbf{P}^r_k$. We call $C$ *hyperelliptic* if there is a finite morphism $C \to \mathbf{P}^1_k$ of degree 2, or equivalently if $C$ admits a $g^1_2$ (which is automatically basepoint-free if $g \geq 1$). We call the morphism $\iota \colon C \to \mathbf{P}^{g-1}_k$ defined by $|K|$ the *canonical morphism*. For $g \geq 2$, $|K|$ is very ample if and only if $C$ is not hyperelliptic. Thus if $C$ is nonhyperelliptic, the canonical morphism $\iota$ is an embedding, and if $C$ is hyperelliptic, $\iota$ factors as a degree 2 morphism $C \to \mathbf{P}^1_k$ followed by the Veronese embedding $\mathbf{P}^1_k \to \mathbf{P}^{g-1}_k$. In particular, every genus two curve is hyperelliptic, and every genus three curve is either hyperelliptic or a smooth plane quartic.

For $g \geq 4$, we say $C$ is *trigonal* if $C$ admits a $g^1_3$ but not a $g^1_2$; let $\mathcal{T}_g$ be the stack of smooth trigonal curves. The moduli space $\mathcal{T}_g$ admits a stratification by locally closed substacks $\mathcal{T}_{g,n}$ where $n$ runs over integers with $0 \leq n \leq \frac{g+2}{3}$ and $n \equiv g \pmod 2$. The integer $n$ denotes the *Maroni invariant* of a trigonal curve $C$, defined as the unique nonnegative integer $n$ such that the trigonal cover $C \to \mathbf{P}^1_k$ factors through a closed embedding

$$C \to \mathbf{F}_n := \mathbf{P}_{\mathbf{P}^1_k}(\mathcal{O}_{\mathbf{P}^1_k} \oplus \mathcal{O}(n)_{\mathbf{P}^1})$$

in such a way that the structure map $\mathbf{F}_n \to \mathbf{P}^1_k$ restricts to the trigonal cover $C \to \mathbf{P}^1_k$. Note that $\mathbf{F}_n$ is ruled by the fibers of the structure map; it is in fact the $n$th Hirzebruch surface (which for $n = 0$ degenerates to $\mathbf{P}^1_k \times_k \mathbf{P}^1_k$), and can also be represented as an $(n, 1)$-hypersurface in $\mathbf{P}^1_k \times_k \mathbf{P}^2_k$.

Last but not least, we say $C$ is *bielliptic* if it admits a degree 2 map to a genus 1 curve over $k$. Any such map gives rise to a $g^1_4$, but not conversely.

It is a classical result that the moduli space $\mathcal{M}_5$ of smooth curves of genus 5 can be stratified into the following locally closed substacks: the locus $\mathcal{H}_5$ of hyperelliptic curves of genus 5, the locus $\mathcal{T}_5$ of trigonal curves of genus 5, and the locus $\mathcal{U}_5$ of canonical curves of genus 5 which are complete intersections of three quadrics in $\mathbf{P}^4$.

A foundational result of Petri (also attributed to Babbage, Chisini, and Enriques) crucial to the classification of higher genera says that the homogenous ideal defining a canonical curve $C$ is generated by quadrics, unless $C$ is trigonal or a smooth plane quintic when $g = 6$. Due to work of Mukai [67] following Petri's results, we have the following classification of genus 6 curves over finite fields.

**Theorem 3.2.1.** *Let $C$ be a curve of genus $6$ over a finite field $k$. Then one (and only one) of the following holds.*

*(1) The curve $C$ is hyperelliptic.*

*(2) The curve $C$ is bielliptic.*

*(3) The curve $C$ occurs as a smooth quintic in $\mathbf{P}^2_k$.*

*(4) The curve $C$ is trigonal of Maroni invariant $0$. In this case, $C$ occurs as a curve of bidegree $(3,4)$ in $\mathbf{P}^1_k \times \mathbf{P}^1_k$.*

*(5) The curve $C$ is trigonal of Maroni invariant $2$. In this case, $C$ occurs as a complete intersection of type $(2,1)\cap(1,3)$ in $\mathbf{P}^1_k \times_k \mathbf{P}^2_k$, where the $(2,1)$-hyperplane is isomorphic to the Hirzebruch surface $\mathbf{F}_2$.*

*(6) The curve $C$ occurs as a transverse intersection of four hyperplanes, a quadric hypersurface, and the $6$-dimensional Grassmannian $\mathrm{Gr}(2,5)$ in $\mathbf{P}^9_k$.*

*Proof.* Most of the above follows from Petri's theorem. For the details in the last case, see [59, Theorem 3.1] and the references therein. □

*Remark* 3.2.2. As stated in [71, Theorem 4.1], the space $\mathcal{M}_6$ can be stratified into locally closed substacks consisting of the loci corresponding to each of the cases in Theorem 3.2.1. In particular:

(1) The locus $\mathcal{H}_6$ of hyperelliptic curves of genus 6 has dimension 11.

(2) The locus $\mathcal{B}_6$ of bielliptic curves of genus 6 has dimension 10.

(3) The locus $\mathcal{Q}_6$ of smooth plane quintic curves of genus 6 has dimension 12.

(4) The locus $\mathcal{T}_{6,0}$ of trigonal curves of genus 6 with Maroni invariant 0 has dimension 13.

(5) The locus $\mathcal{T}_{6,2}$ of trigonal curves of genus 6 with Maroni invariant 2 has dimension 12.

(6) The locus $\mathcal{M}_6^{\mathrm{BN}}$ of generic curves of genus 6 has dimension 15 (it is open in $\mathcal{M}_6$).

One can also describe the Brill–Noether stratification of $\mathcal{M}_7$ explicitly, as in [57].

**Theorem 3.2.3.** *Let $C$ be a curve of genus 7 over a finite field $k$. Then one (and only one) of the following holds.*

1. *The curve $C$ is hyperelliptic.*

2. *The curve $C$ is trigonal of Maroni invariant 3. In this case, $C$ occurs as a hypersurface of degree 9 in $\mathbf{P}(1:1:3)_k$.*

3. *The curve $C$ is trigonal of Maroni invariant 1. In this case, $C$ occurs as a complete intersection of type $(1,1) \cap (3,3)$ in $\mathbf{P}^1_k \times_k \mathbf{P}^2_k$.*

4. *The curve $C$ is bielliptic.*

5. *The curve $C$ is not bielliptic but admits a $g^2_6$ which is self-adjoint (squares to the canonical class). In this case, $C$ is a complete intersection of type $(3) \cap (4)$ in $\mathbf{P}(1:1:1:2)_k$, where the degree 3 hypersurface can be taken to be defined by $x_0 y + P_3(x_1, x_2) = 0$ for some separable cubic $P_3$.*

6. *The curve $C$ admits a pair of distinct $g^2_6$'s. In this case, $C$ occurs as a complete intersection of type $(1,1) \cap (1,1) \cap (2,2)$ in $\mathbf{P}^2_k \times_k \mathbf{P}^2_k$.*

7. *The curve $C$ does not admit a $g^2_6$ but $C_{\overline{k}}$ does. In this case, $C$ occurs as a complete intersection of type $(1,1) \cap (1,1) \cap (2,2)$ in the quadratic twist of $\mathbf{P}^2_k \times_k \mathbf{P}^2_k$.*

8. *The curve $C$ admits a $g^1_4$ but $C_{\overline{k}}$ does not admit a $g^2_6$. In this case, $C$ occurs as a complete intersection of type $(1,1) \cap (1,2) \cap (1,2)$ in $\mathbf{P}^1_k \times_k \mathbf{P}^3_k$ in which the $(1,1)$-hypersurface is a $\mathbf{P}^2$-bundle over $\mathbf{P}^1$.*

9. *The curve $C$ does not admit a $g^1_4$. In this case, $C$ occurs as a transverse intersection of 9 hyperplanes and the orthogonal Grassmannian $\mathrm{OG}^+(5,10)$ in $\mathbf{P}^{15}_k$.*

*Proof.* Most of the above follows from Petri's theorem. For the rest, see [57, Theorem 3.2, §7], and the references therein. □

*Remark* 3.2.4. We list the dimensions of the corresponding strata in moduli in Table 3.1. Note that cases (6) and (7) of Theorem 3.2.3 together correspond to a single stratum in $\mathcal{M}_7$, as the distinction between them is not stable under base change.

*Remark* 3.2.5. Curves as in case (9) of Theorem 3.2.3 are known as *Brill–Noether-general* curves (c.f. [71, Theorem 4.1]). We will henceforth refer to them as *generic* curves of genus 7.

*Remark* 3.2.6. [59, Remark 3.3] points out that the bielliptic curves of genus 7 also occur as complete intersections of type $(3) \cap (4)$ in $\mathbf{P}(1:1:1:2)$. We further clarify this description to avoid confusion. According to the paragraphs preceding and following [68, Proposition 6.4], if we let $x_0, x_1, x_2, y$ be the coordinates on $\mathbf{P}(1:1:1:2)$, the degree 3 hypersurface is defined by $Q(x_0, x_1, x_2)$ for some cubic $Q$ when $C$ is bielliptic, unlike the shape of the cubic in case (5) of Theorem 3.2.3. Hence the two descriptions are mutually exclusive and have no intersections.

## 3.3 Tabulation of curves of genus 5 over $\mathbb{F}_3$

We have the following polynomial point counts of $\mathcal{M}_5$ as well as each of its stratum.

$$\#\mathcal{M}_5(\mathbb{F}_q) = q^{12} + q^{11} + q^{10} - q^8 + 1, \text{(c.f. Equation 3.1)} \tag{3.10}$$

$$\#\mathcal{H}_5(\mathbb{F}_q) = q^{2\cdot 5-1}, \text{ and} \tag{3.11}$$

$$\#\mathcal{T}_5(\mathbb{F}_q) = q^{11} + q^{10} - q^8 + 1; \tag{3.12}$$

to be precise, the first of these equalities is from [8], the second is folklore (see [17, Proposition 7.1] and discussion therein), and the third is from [93]. Specializing to $q = 3$, we obtain the theoretically predicted stacky counts $\#\mathcal{M}_5(\mathbb{F}_3) = 761,077, \#\mathcal{H}_5(\mathbb{F}_3) = 19,683, \#\mathcal{T}_5(\mathbb{F}_3) = 229,636$, and hence $\#\mathcal{U}_5(\mathbb{F}_3) = 511,758$. The table of hyperelliptic curves of genus 5 over $\mathbb{F}_3$ was computed by E. Howe using the algorithms in [44] and its stacky point count agrees with the theoretically predicted count of $19,683$. We henceforth only address the two remaining cases.

### 3.3.1 Trigonal

Our tabulation of trigonal curves of genus 5 makes use of its description as certain singular plane curves, which we now recall. Let $C$ be a projective plane curve in $\mathbf{P}^2$. A singular point of $C$ is said to have *delta invariant* 1 if it is either a node (an ordinary double point), where a curve is locally of the form $xy = 0$, or an ordinary cusp, i.e. locally of the form $y^2 = x^3$. The following is a standard fact.

**Proposition 3.3.1.** *A smooth curve $C$ of genus 5 is trigonal if and only if it can be represented as a plane quintic with exactly one singular point of delta invariant 1 (and no other singularities). Furthermore, any isomorphism of such curves $C_1$ and $C_2$ extends to an automorphism of $\mathbf{P}^2$.*

By the above result, a trigonal curve of genus 5 over $\mathbb{F}_3$ has a single nodal or cuspidal

$\mathbb{F}_3$-rational singular point, so we can restrict to enumerating $\mathrm{PGL}_3(\mathbb{F}_3)$-equivalence classes of quintics in inhomogeneous form with zero constant and linear terms, and each of the following three cases for the quadratic terms:

1. split node: $x^2 - y^2$,

2. nonsplit node: $x^2 + y^2$, and

3. potentially cuspidal: $y^2$.

We have $\dim_{\mathbb{F}_3} H^0(\mathbf{P}^2, \mathcal{O}_{\mathbf{P}^2}(5)) = \binom{5+2}{2} = 21$, and hence each of the above cases correspond to a 15-dimensional $\mathbb{F}_3$-subspace $V_i$, $i = 1, 2, 3$, of $H^0(\mathbf{P}^2, \mathcal{O}_{\mathbf{P}^2}(5))$ (the vanishing of the constant and linear terms together with the condition on the quadratic terms impose 6 independent equations on the 21 coefficients). With this said, our procedure for enumerating the set of isomorphism classes of trigonal curves of genus 5 over $\mathbb{F}_3$ goes as follows:

1. Enumerate the orbit representatives of the action of $\mathrm{PGL}_3(\mathbb{F}_3)$ on $V_i$ by explicitly constructing the Cayley graph of the action of $\mathrm{PGL}_3(\mathbb{F}_3)$ on $V_i$. The code that carries out this step can be found in `enum_trigonal.sage` and `find_orbits.sage`.

2. Verify using Magma that the curves obtained from (1) are indeed of genus 5. The code that carries out this step can be found in `curve_check.m`.

3. Although this step is in principle not necessary, as an extra sanity check, we verify using Magma that the curves left over from (2) are indeed pairwise non-isomorphic. The code that carries out this step can be found in `isomclass_check.m`.

We also compute the zeta function and $\mathbb{F}_3$-automorphism group of each curve along the way of Steps (2) and (3). All the aforementioned scripts are contained in the directory `./Census/trigonal/` of our genus 5 repository.

### 3.3.2 Intersection of quadrics in $\mathbf{P}^4$

In principle, we would like to enumerate $\mathrm{PGL}_3(\mathbb{F}_3)$-orbits of $\mathrm{Gr}(3, H^0(\mathbf{P}^4, \mathcal{O}_{\mathbf{P}^4}(2))$ according to [58] and select the ones which give rise to a smooth curve. Since

$$\dim \mathrm{Gr}(3, H^0(\mathbf{P}^4, \mathcal{O}_{\mathbf{P}^4}(2))) = 3 \cdot (15 - 3) = 36,$$

we always run out of memory on all machines available to us when running the above computation. In practice, we start the enumeration process by computing representatives of $\mathrm{PGL}_3(\mathbb{F}_3)$-orbits of $\mathrm{Gr}(2, H^0(\mathbf{P}^4, \mathcal{O}_{\mathbf{P}^4}(2))$ according to [58]; there are 191 of them, of which 29 of them are smooth, 84 of them have a zero-dimensional singular subscheme, 60 of them have a one-dimensional singular subscheme, and 18 of them have a two-dimensional singular subscheme. For each of the two-dimensional spaces of quadrics in $\mathbf{P}^4$ that has a singular subscheme of dimension less than 2, there are $3^{13}$ ways to extend that to a three-dimensional space, thereby being a candidate curve of genus 5 over $\mathbb{F}_3$. After filtering out the non-smooth ones, it remains to check for pairwise isomorphisms. In this particular case, we compute an isomorphism invariant that we refer to as the *Hilbert hash* which we now describe.

Let $C = \mathrm{Proj}\, \mathbb{F}_3[x_0, x_1, x_2, x_3, x_4]/(f_1, f_2, f_3)$ where $f_i \in \mathbb{F}_3[x_0, x_1, x_2, x_3, x_4]_2$. For each of the $(3^5 - 1)/(3 - 1) = 121$ hyperplanes $H$ in $\mathbf{P}^4(\mathbb{F}_3)$, the intersection $Z_H \coloneqq H \cap C$ is a zero-dimensional scheme of degree 8 by Bézout's Theorem. We associate to $Z_H$ the set $S_H \coloneqq \{(n, d, m)\}$, meaning that there are $n$ points of degree $d$ and multiplicity $m$ in $Z_H$ satisfying $\sum ndm = 8$. The multiset $\{S_H\}_{H \in \mathrm{Gr}(1, \mathbf{P}^4(\mathbb{F}_3))}$ is an isomorphism invariant of $C$. One method for computing $S_H$ is as follows. By abuse of notation, we denote the linear form defining $H$ also by $H$. Let

$$I \coloneqq \langle f_1, f_2, f_3, H \rangle = \bigcap_{i=1}^{k} I_i$$

be the primary decomposition of the ideal $I$, and let $I_{i,\mathrm{rad}}$ be the radical of $I_i$. Let $P_J$ denote the Hilbert polynomial of the ideal $J$, which is a constant if the corresponding projective scheme is zero-dimensional. Each ideal $I_i$ corresponds to a $\mathbb{F}_3$-point $P_i$ of $Z_H$ of degree $d = P_{I_{i,\mathrm{rad}}} = [\mathbb{F}_3(P_i) : \mathbb{F}_3]$ and multiplicity $m = P_{I_i}/d$. We also describe an alternative method to compute $S_Z$ that does not involve the inefficient routine of computing primary decomposition. Let $\widetilde{g}$ denote the dehomogenization of a homogeneous polynomial $f \in \mathbb{F}_3[x_0, x_1, x_2, x_3, x_4]$ obtained from evaluating $g$ at $x_0 = 1$, and let $\widetilde{J}$ denote the dehomogenization of $J$. Let $\langle f \rangle = \mathrm{Elim}_3\, \widetilde{I} := \widetilde{I} \cap \mathbb{F}_3[x_4]$ be the 3-rd elimination ideal of $\widetilde{I}$. If $\deg_{x_4} f = 8$, then the factorization of $f$ over $\mathbb{F}_3$ encodes the same information as $S_H$; in particular, the tuple $(n, d, m)$ means that $f$ has $n$ degree $d$ factors of multiplicity $m$. We precompute all the possible factorization patterns of degree 8 polynomials in one variable over $\mathbb{F}_3$ to speed up the computation.

*Remark* 3.3.2. While there is no guarantee that $\deg_{x_4} f = 8$ for a given arbitrary hyperplane $H$, we always by default start with the latter approach and resort to the primary decomposition approach only when necessary. We have found that this speeds up the computation significantly in practice.

*Remark* 3.3.3. We discovered that the intrinsic `PrimaryDecomposition` in Magma was giving incorrect results in some cases; this bug has since been resolved in Magma V.2.29.3.

### 3.3.3 Progress Report

Our computation of $\mathcal{T}_5(\mathbb{F}_3)$ is complete, and we have $\#\mathcal{T}_5(\mathbb{F}_3) = 229,636$ as predicted by Equation 3.12. We have computed the Hilbert hash of all the candidate curves in the generic stratum and the pairwise isomorphism check is ongoing.

## 3.4 Tabulation of curves of genus 6 over $\mathbb{F}_2$

We begin by recording a few convenient facts that allow us to more efficiently search and filter putative genus 6 curves.

1. Using an analogue of the explicit formula from analytic number theory, Serre (c.f. [83, Theorem 5.3.2, 7.1 Table 1] shows that a curve of genus 6 has at most 10 $\mathbb{F}_2$-points, which is a notable refinement from the Hasse-Weil bound 15.

2. LMFDB contains a complete list of isogeny classes of abelian varieties of dimension 6 over $\mathbb{F}_2$ and their corresponding $L$-polynomials. Using the fact that a curve and its Jacobian have the same Weil polynomial, we recover a finite set containing the tuple $(\#C(\mathbb{F}_{2^i}))_{i=1}^{6}$ for any curve $C$ of genus 6 over $\mathbb{F}_2$. The relevant code written in SageMath can be found in `./Census/Shared/weil_poly_utils.sage` in our code base (taken from [59]). We make use of this list when it would presumptively speed up our tabulation process.

To simplify the code somewhat, initially we only construct a finite set of genus 6 curves over $\mathbb{F}_2$ which meets every isomorphism class with "limited redundancies". We use a separate postprocessing step to remove these redundancies (see Section 3.4.7).

### 3.4.1 Hyperelliptic curves

Here we follow the strategy used in [94, 28] where the enumerations were done in cases $g = 4, 5$. This strategy is adapted to characteristic 2; for a good approach in odd characteristic, see [44].

Any hyperelliptic curve of genus $g$ over $\mathbb{F}_2$ can be represented as $y^2 + q(x)y = p(x)$ with $p(x), q(x) \in \mathbb{F}_2[x]$ and $2g + 1 \leq \max\{2\deg(q(x)), \deg(p(x))\} \leq 2g + 2$. Xarles presented a method to determine the isomorphism class of a hyperelliptic curve using the action of $\mathrm{PGL}_2(\mathbb{F}_2)$ on $\mathbb{F}_2[x]_{\leq g+1}$.

**Lemma 3.4.1.** *([94], Lemma 1) Let $H_1, H_2$ be hyperelliptic curves represented by the equations $y^2 + q_i(x)y = p_i(x)$ for $i \in \{1, 2\}$ respectively as above. Suppose that $H_1 \cong H_2$. Then there exists $A \in \mathrm{PGL}_2(\mathbb{F}_2)$ such that $q_2(x) = \psi_{g+1}(A)(q_1(x))$, where the action of*

$\mathrm{PGL}_2(\mathbb{F}_2)$ *on* $\mathbb{F}_2[x]_{\leq n}$ *is given by*

$$\psi_n(A)(q(x)) := (cx+d)^n q\left(\frac{ax+b}{cx+d}\right), \qquad A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PGL}_2(\mathbb{F}_2).$$

We compute orbit representatives for this action, test for pairwise isomorphism, and record the resulting curves. The implementation of this method can be found in the folder `./Census/hyperelliptic/` in our code base.

### 3.4.2 Bielliptic curves

Here we follow a construction from [59] for enumerating bielliptic curves of genus 7 over $\mathbb{F}_2$. As the core elements of the argument exhibit no dependence at all on the genus, it is straightforward to replicate in genus 6; this case was not needed in [59] because in that setting (where the zeta function is heavily restricted) one can use a more conceptual argument to rule out bielliptic curves of genus 6.

By Riemann–Hurwitz plus the fact that double covers in characteristic 2 have only wild ramifications, the map from a bielliptic curve $C$ of genus 6 to its elliptic quotient $E$ has ramification divisor of the form $2D$ where $D$ is an effective divisor of degree $g-1=5$ on $E$. We may thus generate all bielliptic curves by enumerating over a set of isomorphism class representatives of elliptic curves $E$ over $\mathbb{F}_2$ (there are 5 of them). For each $E$, we use Magma to enumerate over all effective divisors $D$ of degree 5. For each $D$, we enumerate over all order-2 quotients of the ray class group of $2D$, form the corresponding abelian extension, then check to see if it indeed has genus 6 (and if so record the resulting curve). The implementation of this method can be found in `./Census/bielliptic/` in our code base.

### 3.4.3 Smooth plane quintic curves

Since the space of quintic polynomials over $\mathbb{F}_2$ has dimension $\binom{7}{2} = 21$, we can skip the removal of redundancy using the action of $\mathrm{GL}(3, \mathbb{F}_2)$; we simplify identify all of the nonsingular polynomials and record the resulting smooth curves. The implementation of this method can be found in `./Census/plane_quintic/` in our code base.

### 3.4.4 Trigonal curves of Maroni invariant 0

In this case, we are looking for $(3,4)$-curves in $\mathbf{P}^1 \times \mathbf{P}^1$, and we follow the strategy used in [59]. We first compute orbit representatives for the action of $\mathrm{PGL}_2(\mathbb{F}_2) \times \mathrm{PGL}_2(\mathbb{F}_2)$ on *all* subsets of $(\mathbf{P}^1 \times \mathbf{P}^1)(\mathbb{F}_2)$. For each orbit representative, we identify the $(3,4)$-polynomials which vanish on the points in the chosen subset and do not vanish elsewhere; since we are working over $\mathbb{F}_2$, this is an affine subspace of the vector space of $(3,4)$-polynomials. We then pick out the nonsingular polynomials and record the resulting smooth curves. The implementation of this method can be found in `./Census/trigonal_maroni_0/` in our code base.

### 3.4.5 Trigonal curves of Maroni invariant 2

In this case, we are looking for complete intersections of type $(2,1) \cap (1,3)$ in $\mathbf{P}^1 \times \mathbf{P}^2$. More specifically, if we write $\mathbf{P}^1 \times \mathbf{P}^2 = \operatorname{Proj} \mathbb{F}_2[x_0, x_1; y_0, y_1, y_2]$, then we may take the $(2,1)$-hypersurface $X_1$ to be

$$(x_0^2 + x_1^2)y_1 + x_0 x_1 y_2 = 0. \tag{3.13}$$

Indeed, over a field of characteristic 0, the equation of the Hirzebruch surface $\mathbf{F}_n$ is isomorphic to the hypersurface defined by $x_0^n y_1 - x_1^n y_2$ in $\mathbf{P}^1 \times \mathbf{P}^2$ (c.f. [47] Exercise 2.4.5), and we obtain (3.13) by taking $n = 2$ and making a change of variables to get an equation with smooth mod-2 reduction.

The hypersurface (3.13) is fixed by the group $G$ generated by the three involutions

$$x_0 \leftrightarrow x_1; \qquad y_0 \mapsto y_0 + y_1; \qquad y_0 \mapsto y_0 + y_2.$$

We now proceed as in the previous case: we compute orbit representatives for the action of $G$ on all subsets of $X_1$; for each orbit representative, we identify the $(1,3)$-polynomials which vanish on the points in the chosen subset and do not vanish elsewhere; we then pick out the nonsingular polynomials and record the resulting smooth curves. The implementation of this method can be found in `./Census/trigonal_maroni_2/` in our code base.

### 3.4.6 Generic curves

Here we follow a modified version of the strategy used in [59]. This is the most computationally intensive case. We first identify orbit representatives for the action of $\mathrm{PGL}_5(\mathbb{F}_2)$ on 4-tuples of points in $\mathbf{P}^{9\vee}(\mathbb{F}_2)$. Each 4-tuple defines 4 linear forms and hence 4 hyperplanes on $\mathbf{P}^9$; we next compute representatives for the linear action of $\mathrm{PGL}_4(\mathbb{F}_2)$ on such 4-tuples preserving the intersection of the 4 hyperplanes. We record all cases where the intersection of the 4 hyperplanes with the Grassmannian $\mathrm{Gr}(2,5)$ is irreducible with singular locus of codimension greater than 1; there are 17 such intersections, of which 7 are smooth, corresponding to the fact that quintic del Pezzo surfaces over a finite field are indexed by conjugacy classes in $S_5$ (e.g., see [87, Table 1]).

For each of these 17 intersections, we first record all the quadrics defined on the span of the 4 linear forms, which reduces the enumeration of quadrics from a $\binom{10}{2} = 55$-dimensional space to a $\binom{7}{2} = 21$-dimensional space); we then record the cases where the intersection is smooth of genus 6. The implementation of this method can be found in `./Census/generic/` in our code base.

### 3.4.7 Postprocessing

For each stratum, the computation described above yields a finite set of curves of genus 6 over $\mathbb{F}_2$ lying in that stratum and including at least one representative of each isomorphism class. It then remains to remove redundant representatives.

For this, we first hash the curves by their zeta function, or equivalently by the function $C \mapsto (\#C(\mathbb{F}_{2^i})_{i=1}^6)$. Within each hash class, we use Magma to construct the function field of each curve, then use `Isomorphisms` to test whether any pair of curves is isomorphic. Once this is done, we compute the automorphism group of each curve that remains.

For the record, we mention some bugs in Magma that we had to work around. These were fixed in subsequent releases based on our reports.

- For two function fields, the intrinsic `Isomorphisms` returns a list of all isomorphisms between the two fields, but in some cases with repeated entries. This caused the intrinsic `AutomorphismGroup` to yield errors in certain cases, for which we computed the group structure directly from the output of `Isomorphisms`.
- For two function fields, the intrinsic `IsIsomorphic` sometimes returned `false` even when the two fields are isomorphic. We instead tested whether `Isomorphisms` returns a nonempty list.

## 3.5 Tabulation of curves of genus 7 over $\mathbb{F}_2$

### 3.5.1 Hyperelliptic curves

We adopt the same strategy in [94, 28, 45] where the enumerations were done in cases $g = 4, 5, 6$ in characteristic 2; for a good approach in odd characteristics, see [44].

Any hyperelliptic curve of genus $g$ over $\mathbb{F}_2$ can be represented as $y^2 + q(x)y = p(x)$ with $p(x), q(x) \in \mathbb{F}_2[x]$ and $2g + 1 \leq \max\{2\deg(q(x)), \deg(p(x))\} \leq 2g + 2$. To determine the isomorphism class of a hyperelliptic curve, one uses the action of $\mathrm{PGL}_2(\mathbb{F}_2)$ on $\mathbb{F}_2[x]_{\leq g+1}$:

**Lemma 3.5.1.** *([94], Lemma 1) Let $H_1, H_2$ be hyperelliptic curves represented by the equations $y^2 + q_i(x)y = p_i(x)$ for $i \in \{1,2\}$ respectively as above. Suppose that $H_1 \cong H_2$. Then there exists $A \in \mathrm{PGL}_2(\mathbb{F}_2)$ such that $q_2(x) = \psi_{g+1}(A)(q_1(x))$, where the action of $\mathrm{PGL}_2(\mathbb{F}_2)$ on $\mathbb{F}_2[x]_{\leq n}$ is given by*

$$\psi_n(A)(q(x)) := (cx+d)^n q\left(\frac{ax+b}{cx+d}\right), \qquad A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PGL}_2(\mathbb{F}_2).$$

We compute orbit representatives for this action, test for pairwise isomorphism, and record the resulting curves. The implementation of this method can be found in `./Census/hyperelliptic/` in our code base.

### 3.5.2 Trigonal curves of Maroni invariant 3

In this case, we are looking for hypersurfaces of degree 9 in the weighted projective space $\mathbf{P}(1:1:3)$. This weighted projective space $\mathbf{P}(1:1:3)$ is obtained from blowing down the Hirzebruch surface $\mathbf{F}_3$ along a certain exceptional curve, and by intersection theory, a trigonal curve has zero intersection with the exceptional curve. This means that any trigonal curve does not pass through the singular point $[0:0:1]$ in $\mathbf{P}(1:1:3)$. We use orbit lookup trees to enumerate orbit representatives for the action of the subgroup of $\mathrm{PGL}_3(\mathbb{F}_2)$ fixing $[0:0:1]$ on subsets of the nonsingular points of $\mathbf{P}(1:1:3)(\mathbb{F}_2)$ of size at most 6. For each orbit representative, we then solve for polynomials in $\mathbb{F}_2[x_0, x_1, x_2]_{(1:1:3)}$ of weighted degree 9 that pass through exactly those points.

The implementation of this method can be found in `./Census/trigonal_maroni_3/` in our code base.

### 3.5.3 Trigonal curves of Maroni invariant 1

In this case, we are looking for complete intersections of type $(1,1) \cap (3,3)$ in $\mathbf{P}^1 \times \mathbf{P}^2$. We first compute orbit representatives for the action of $\mathrm{PGL}_2(\mathbb{F}_2) \times \mathrm{PGL}_3(\mathbb{F}_2)$

on subsets of $(\mathbf{P}^1 \times \mathbf{P}^2)(\mathbb{F}_2)$ of size at most 9 using orbit lookup trees. Since the trigonal map here arises from the projection to $\mathbf{P}^1$, we disallow subsets of $(\mathbf{P}^1 \times \mathbf{P}^2)(\mathbb{F}_2)$ when there are more than three points above any one point of $\mathbf{P}^1$.

For each orbit representative, to enumerate all complete intersections of type $(1,1),(3,3)$ passing through these points, we use the following facts:

1. the $(1,1)$ hypersurface is a $\mathbf{P}^1$-bundle over $\mathbf{P}^1$, the Hirzebruch surface $\mathbf{F}_1$ containing $C$, which is necessarily smooth.

2. The $(3,3)$ hypersurface is specified modulo the ideal generated by the $(1,1)$ hypersurface.

3. Given the $(1,1)$ hypersurface, we identify $(3,3)$-polynomials which vanish precisely on the chosen subset by solving a system of linear equations.

The implementation of this method can be found in
`./Census/trigonal_maroni_1/` in our genus 7 code base.

### 3.5.4 Bielliptic curves

Here we follow the strategy used in [59] to enumerate bielliptic curves of genus 7; therein bielliptic curves of genus 6 were ruled out without any enumeration, but the enumeration strategy is genus-independent.

By Riemann–Hurwitz and the fact that double covers in characteristic 2 have only wild ramifications, the map from a bielliptic curve $C$ of genus 7 to its elliptic quotient $E$ has ramification divisor of the form $2D$ where $D$ is an effective divisor of degree $g-1=6$ on $E$. We generate all bielliptic curves by enumerating over the 5 isomorphism classes elliptic curves $E$ over $\mathbb{F}_2$. For each elliptic curve $E$ at the base, we use Magma to enumerate over all effective divisors $D$ of degree 6. For each effective divisor $D$, we enumerate over all order-2 quotients of the ray class group of $D$, form the corresponding abelian extension, then check to see if it indeed has genus 7. The implementation of this method can be found in `./Census/bielliptic/` in our code base.

### 3.5.5 Self-adjoint $g^2_6$

In this case, we are looking for complete intersections of type $(3)\cap(4)$ in the weighted projective space $\mathbf{P}(1:1:1:2)$ not passing through the singular point $[0:0:0:1]$. Let $\mathbf{P}(1:1:1:2) = \operatorname{Proj}\mathbb{F}_2[x_0,x_1,x_2,y]_{(1:1:1:2)}$. The degree 3 hypersurface can be taken to be defined by $x_0y + P_3(x_1,x_2) = 0$, for some separable cubic $P_3$. In particular, $P_3$ is one of $\{x_1x_2(x_1+x_2), x_1(x_1^2+x_1x_2+x_2^2), x_1^3+x_1x_2^2+x_2^3\}$. For each fixed cubic hypersurface $H_3$, subsets of points vanishing on $H_3$ of size at most 10, excluding the singular point $[0:0:0:1]$, give rise to affine conditions that we use to find the quartic hypersurfaces passing through precisely those points by solving a system of linear equations.

The implementation of this method can be found in `./Census/self-adjoint_g26/` in our genus 7 code base.

### 3.5.6 Rational $g^2_6$

This subsection addresses case (6) of Theorem 3.2.3. We say $C$ has *rational* $g^2_6$ if $C$ admits a pair of distinct $g^2_6$'s over $\mathbb{F}_2$, or equivalently $C$ has a $g^2_6$ defined over $\mathbb{F}_2$ that does not square to the canonical class. In this case, we are looking for complete intersections of type $(1,1)\cap(1,1)\cap(2,2)$ in $\mathbf{P}^2\times\mathbf{P}^2$. Similar as before, we proceed by first computing orbit representatives for the action of $\mathrm{PGL}_3(\mathbb{F}_2)\times\mathrm{PGL}_3(\mathbb{F}_2)$ on subsets of $(\mathbf{P}^2\times\mathbf{P}^2)(\mathbb{F}_2)$ of size at most 10 using orbit lookup trees. Moreover, we impose the condition that no three points project to the same point on either copy of $\mathbf{P}^2$, for otherwise it creates a triple point and hence $C$ would have been trigonal. Our curve enumeration procedure follows a similar outline as before. For each orbit representative $O$, we first find all 2-dimensional subspaces of the 9-dimensional space of $(1,1)$-polynomials that pass through the points in $O$. Then for each such 2-dimensional subspace, we find, by solving a system of linear equations, the $(2,2)$-hypersurfaces such that the $\mathbb{F}_2$-rational points of the triple intersection $(1,1)\cap(1,1)\cap(2,2)$ are precisely the points in $O$. A naïve implementation of this procedure will result in an intractable postprocessing step when $O$ contains no $\mathbb{F}_2$-points. Indeed, in this case, one would need to enumerate over $2^{\dim Gr(2,9)} = 2^{14}$ intersections of type $(1,1)\cap(1,1)$. To remedy this, for each orbit representative $O$, we compute the $\mathrm{PGL}_3(\mathbb{F}_2)\times\mathrm{PGL}_3(\mathbb{F}_2)$-orbits of all 2-dimensional subspaces of the 9-dimensional space of $(1,1)$-polynomials that pass through the points in $O$ before proceeding forward. Finally, we also discard all reducible $(1,1)\cap(1,1)$ intersections during the enumeration phase.

The implementation of the method described above can be found in `./Census/rational_g26/` in our genus 7 code base.

### 3.5.7 Irrational $g_6^2$

This subsection addresses case (7) of Theorem 3.2.3. We say $C$ has *irrational* $g_6^2$ if $C$ does not have a $g_6^2$ defined over $\mathbb{F}_2$ but has a $g_6^2$ defined over $\overline{\mathbb{F}}_2$. We are now looking for complete intersections of type $(1,1)\cap(1,1)\cap(2,2)$ in the (nontrivial) quadratic twist of $\mathbf{P}^2\times\mathbf{P}^2$. We view the $\mathbb{F}_2$-rational points of the quadratic twist $X$ of $\mathbf{P}^2\times\mathbf{P}^2$ as a subset of $(\mathbf{P}^2\times\mathbf{P}^2)(\mathbb{F}_4)$. In particular, a $\mathbb{F}_2$-point of $X$ can be represented by $(P,\sigma(P))$ for $P\in\mathbf{P}^2(\mathbb{F}_4)$ and $\sigma$ the Frobenius generator of $\mathrm{Gal}(\mathbb{F}_4/\mathbb{F}_2)$. Viewing $\mathrm{PGL}_3(\mathbb{F}_4)$ as a subgroup of $\mathrm{PGL}_6(\mathbb{F}_4)$ via $g\mapsto\begin{bmatrix} g & 0\\ 0 & \sigma(g)\end{bmatrix}$, $\mathrm{PGL}_3(\mathbb{F}_4)$ acts on $X(\mathbb{F}_2)$. We use orbit lookup trees to compute the $\mathrm{PGL}_3(\mathbb{F}_4)$ orbits of subsets of $X(\mathbb{F}_2)$ of size at most 10. We then proceed as in §3.5.6 after making suitable modifications to obtain the coefficients of the $(1,1)$ and $(2,2)$ polynomials in $X$ of the candidate curves.

The key difference between the irrational $g_6^2$ case and the rational $g_6^2$ case is in how we represent the curves computationally for the postprocessing step. To start, we are not aware of a way to directly instantiate the ambient space $X$ in any computer algebra systems. Moreover, the $(1,1)$ and $(2,2)$ monomials of $X$ involve constants in $\mathbb{F}_4$, although the curves themselves are defined over $\mathbb{F}_2$. In order to descent the $(1,1)$ and $(2,2)$ monomials to $\mathbb{F}_2$, we embed $X$ to $\mathbf{P}^8$ via the twisted Segre embedding (c.f. [24, §4.3] for the twisted Segre embedding $\mathbf{P}^1 \times \mathbf{P}^1 \to \mathbf{P}^3$) as follows. Let $\alpha$ be a root of $x^2+x+1 \in \mathbb{F}_2[x]$, let $x_{ij}$, $i,j = 0,1,2$ be the coordinates of $\mathbf{P}^8$, and let $x_i, y_j$, $i,j = 0,1,2$ be the coordinates of $\mathbf{P}^2 \times \mathbf{P}^2$. We can take the twisted Segre embedding of $\mathbf{P}^2 \times \mathbf{P}^2$ to have coordinates

$$
\begin{aligned}
x_{ii} &= x_i y_i, \\
x_{ij} &= x_i y_j + x_j y_i \ (i < j), \\
x_{ij} &= \alpha x_i y_j + (\alpha+1) x_j y_i \ (i > j).
\end{aligned}
$$

The image of the quadratic twist $X$ of $\mathbf{P}^2 \times \mathbf{P}^2$ inside $\mathbf{P}^8$ is then defined by the following equations:

$$
\begin{aligned}
f_1 &= x_{00}x_{11} + x_{01}^2 + x_{01}x_{10} + x_{10}^2, \\
f_2 &= x_{00}x_{22} + x_{02}^2 + x_{02}x_{20} + x_{20}^2, \\
f_3 &= x_{11}x_{22} + x_{12}^2 + x_{12}x_{21} + x_{21}^2, \\
f_4 &= x_{00}x_{12} + x_{01}x_{20} + x_{10}x_{02}, \\
f_5 &= x_{02}x_{11} + x_{10}x_{12} + x_{01}x_{21}, \\
f_6 &= x_{02}x_{12} + x_{12}x_{20} + x_{02}x_{21} + x_{01}x_{22}.
\end{aligned}
$$

The $(1,1)$ and $(2,2)$-hypersurfaces in $X$ then correspond to hypersurfaces of degree 1 and 2, respectively, in $\mathbf{P}^8$ under the twisted Segre embedding. Each of our candidate curves in thus cut out in $\mathbf{P}^8$ by $f_1, \ldots, f_8$, two hyerplanes, and a quadric. In essence, the twisted Segre embedding allows us to "untwist" the quadratic twist.

The implementation of this method can be found in `./Census/irrational_g26/` in our genus 7 code base.

*Remark* 3.5.2. The rational and irrational $g^2_6$ strata together form the $g^2_6$ stratum of $\mathcal{M}_7$ in the geometric sense. As shown in Table 3.1, the rational and irrational $g^2_6$ strata both have a fractional weighted count, but together they do add up to an integer as predicted.

### 3.5.8 Tetragonal

In this case, we look for complete intersection of type $(1,1)\cap(1,2)\cap(1,2)$ in $\mathbf{P}^1\times\mathbf{P}^3$. Let $x_i, y_j, (i=0,1; j=0,1,2,3)$ be the coordinates of $\mathbf{P}^1\times\mathbf{P}^3$. The $(1,1)$-hypersurface defines a $\mathbf{P}^2$-bundle over $\mathbf{P}^1$, and we fix a smooth $(1,1)$-hypersurface $X_1$ in $\mathbf{P}^1\times\mathbf{P}^2$ defined by $f_0 = x_0y_0 + x_1y_1$. We first compute orbit representatives for the action of $\mathrm{PGL}_2(\mathbb{F}_2)\times\mathrm{PGL}_4(\mathbb{F}_2)$ on subsets of $X_1(\mathbb{F}_2)$ of size at most 10 using orbit lookup trees. We disallow subsets of $X_1(\mathbb{F}_2)$ in which 5 points have the same image in $\mathbf{P}^1$.

For each orbit representative, to enumerate all complete intersections of type $(1,1),(1,2),(1,2)$ passing through these points of $X_1$, we use the following facts:

1. The first $(1,2)$-polynomial $f_1$ is specified modulo the ideal $\langle f_0\rangle$, and the second $(1,2)$-polynomial $f_2$ is specified modulo the ideal $\langle f_0, f_1\rangle$.

2. Given the first two hypersurfaces defined by $f_0$ and $f_1$, every $\mathbb{F}_2$-point of $\mathbf{P}^1\times\mathbf{P}^2$ lying on the intersection of the first two hypersurfaces but not in our specified orbit representative defines an affine condition on the third hypersurface. We can thus identify candidates for the second $(1,2)$-polynomial by solving a system of linear equations.

The implementation of this method can be found in `./Census/tetragonal/` in our genus 7 code base.

### 3.5.9 Generic curves

We refer the reader to [59, Section 7] and [68] for further details. In this case, one should think of the 9 hyperplanes as cutting out a copy of $\mathbf{P}^6$ inside $\mathbf{P}^{15}$ that serves as the codomain of the canonical embedding of $C$ and the quadrics defining the orthogonal Grassmannian $\mathrm{OG}^+(5,10)$ as the equations that define $C$ inside $\mathbf{P}^6$. Here $\mathrm{OG}^+(5,10)$ embeds into $\mathbf{P}^{15}$ via the *spinor embedding* analogous to the Plücker embedding. Let $\mathbf{P}^{15} = \operatorname{Proj}\mathbb{F}_2[x_0, x_{12}, x_{13}, x_{14}, x_{15}, x_{23}, x_{24}, x_{25}, x_{34}, x_{35}, x_{45}, x_{1234}, x_{1235}, x_{1345}, x_{2345}]$. By Mukai [68], $\mathrm{OG}^+(5,10)$ is cut out inside $\mathbf{P}^{15}$ by the equations

$$\begin{gathered}
x_0x_{2345} + x_{23}x_{45} + x_{24}x_{35} + x_{25}x_{34},\\
x_{12}x_{1345} + x_{13}x_{1245} + x_{14}x_{1235} + x_{15}x_{1234},\\
x_0x_{1345} + x_{13}x_{45} + x_{14}x_{35} + x_{15}x_{34},\\
x_{12}x_{2345} + x_{23}x_{1245} + x_{24}x_{1235} + x_{25}x_{1234},\\
x_0x_{1245} + x_{12}x_{45} + x_{14}x_{25} + x_{15}x_{24},\\
x_{13}x_{2345} + x_{23}x_{1345} + x_{34}x_{1235} + x_{35}x_{1234},\\
x_0x_{1235} + x_{12}x_{35} + x_{13}x_{25} + x_{15}x_{23},\\
x_{14}x_{2345} + x_{24}x_{1345} + x_{34}x_{1245} + x_{45}x_{1234},\\
x_0x_{1234} + x_{12}x_{34} + x_{13}x_{24} + x_{14}x_{23},\\
x_{15}x_{2345} + x_{25}x_{1345} + x_{35}x_{1245} + x_{45}x_{1235}.
\end{gathered}$$

We have that $\mathrm{OG}^+(5,10)$ is preserved by $\mathrm{SO}^+(10)$. We would ideally want to compute $\mathrm{SO}^+(10)$-orbits of 6-planes inside $\mathbf{P}^{15}$ (equiv. of $\mathrm{Gr}(7,16)$), but we again run into memory constraints. Instead, we compute $\mathrm{SO}^+(10)$-orbits of 5-planes (equiv. of $\mathrm{Gr}(6,16)$) inside $\mathbf{P}^{15}$ via [58] with the property that no 2-plane contains 4 points of $\mathrm{OG}^+(5,10)$ by [59, Lemma 7.1(a)]; there are 160655 orbit representatives. Each 5-plane corresponds to an intersection of 10 hyperplanes in $\mathbf{P}^{15}$; we rule out the 8219 orbit representatives which have a positive dimensional intersection with $\mathrm{OG}^{+}(5,10)$ (for otherwise it would imply that the canonical embedding factors through $\mathbf{P}^5$, which cannot be the case). For each of the remaining 152436 5-planes, there are $2^{\dim \mathrm{Gr}(1,16-6)} = 2^9$ ways to extend it to a 6-plane. These give rise to all the possible candidate generic curves of genus 7 over $\mathbb{F}_2$.

The implementation of this method can be found in `./Census/generic` in our genus 7 code base.

*Remark* 3.5.3. We discovered some instances where `PrimaryDecomposition` can be extremely slow in Magma, which has been resolved in releases after Magma V.2.28-24.

### 3.5.10 Postprocessing

For each stratum, the computation described above yields a finite set of curves of genus 7 over $\mathbb{F}_2$ lying in that stratum and including at least one representative of each isomorphism class. It then remains to remove redundant representatives.

For this, we first hash the curves by their zeta function, or equivalently by the function $C \mapsto (\#C(\mathbb{F}_{2^i})_{i=1}^{7})$. Within each hash class, we use Magma to construct the function field of each curve, then use `Isomorphisms` to test whether any pair of curves is isomorphic. Once this is done, we compute the automorphism group of each curve that remains.

### 3.5.11 Progress Report

We have enumerated $\mathbb{F}_2$-points of $\mathcal{M}_7$ in all but the generic stratum, where the computation is still ongoing; preliminary results are reported in Table 3.1. We can identify some features of the data that comport with theoretical predictions.

- We have $\#\mathcal{H}_7(\mathbb{F}_2) = 2^{13}$.
- We have $\#\mathcal{B}_7(\mathbb{F}_2) = 2^{12} - 2^{10} - 2^7 + 2^5 - 2^3 - 2$ which agrees with the formula from

**Table 3.1.** Preliminary point counts (unweighted and weighted) over $\mathbb{F}_2$ of the various strata of $\mathcal{M}_7$. The cases "rational $g^2_6$" and "irrational $g^2_6$" together constitute a single stratum.

| Stratum | Dimension | Unweighted | Weighted |
|---|---|---|---|
| $\mathcal{H}_7$ | 13 | 16544 | 8192 |
| $\mathcal{B}_7$ | 12 | 6205 | 2970 |
| $\mathcal{T}_{7,3}$ | 13 | 8340 | 8264 |
| $\mathcal{T}_{7,1}$ | 15 | 42857 | 42725 |
| self-adjoint $g^2_6$ | 15 | 24925 | 24580 |
| rational $g^2_6$ | 16 | 43012 | 42240.5 |
| irrational $g^2_6$ | | 50791 | 49982.5 |
| tetragonal | 17 | 171102 | 169850 |
| $\mathcal{M}_7^{\mathrm{BN}}$ | 18 | ? | ? |

[45, Proposition 4.5] for $q$ odd, in contrast with the situation in genus 6 over $\mathbb{F}_2$, c.f. [45, Remark 4.6].

- Each stratum has integral weighted point count, as predicted by Lemma 3.1.5. In particular, the sum of the rational and irrational $g^2_6$ counts is integral.

## 3.6 Consistency Check in genus 6

The proof of Theorem 3.1.6 implicitly depends on the correctness both of the relevant features of the underlying computational systems (in particular SageMath and Magma) and of our implementation of the search strategies described above. It is thus highly desirable to perform some logically independent consistency checks of the resulting data. We describe several such checks here.

### 3.6.1 Point counting on $\mathcal{M}_6$

We first verify the numerical assertion (3.3). By [19, Corollary 1.6], there exists a monic polynomial $P(T) \in \mathbb{Z}[T]$ of degree 15 such that $\#\mathcal{M}_6(\mathbb{F}_q) = P(q)$ for every prime power $q$. On account of the Lefschetz trace formula for Deligne–Mumford stacks [6, Theorem 3.1.2], it is a feasible but challenging computation to extract the exact polynomial by computing in the tautological ring of $\mathcal{M}_6$ as indicated (and implemented) in [25].

**Theorem 3.6.1.** *For every prime power $q$, we have*

$$\#\mathcal{M}_6(\mathbb{F}_q) = q^{15} + q^{14} + 2q^{13} + q^{12} - q^{10} + q^3 - 1.$$

*In particular, $\#\mathcal{M}_6(\mathbb{F}_2) = 68615$ as asserted in Theorem 3.1.6.*

*Proof.* See [8]. □

Given Theorem 3.6.1, one can give an alternate proof of Theorem 3.1.6 by independently checking the following two concrete assertions:

- For each tabulated curve $C$, the order of $\#\mathrm{Aut}(C)$ is no greater than the reported value.

- No two of the tabulated curves lying in the same stratum are isomorphic. (For an extra consistency check, we tested this in Magma also for pairs of curves not lying in the same stratum.)

Given these assertions, one may then directly verify from our data that $\#\mathcal{M}_6(\mathbb{F}_q) \geq 68615$ with equality if and only if our census is complete. Combining with Theorem 3.6.1 then yields Theorem 3.1.6.

*Remark* 3.6.2. The same logic described in Section 3.6.1 applies to our forthcoming result on $\#\mathcal{M}_5(\mathbb{F}_3)$. In fact, the polynomial point counts for

$$\#\mathcal{M}_{5,1}(\mathbb{F}_q), \#\mathcal{M}_{5,2}(\mathbb{F}_q), \#(\mathcal{M}_{5,2}/S_2)(\mathbb{F}_q), \#\mathcal{M}_{5,3}(\mathbb{F}_q), \text{ and } \#(\mathcal{M}_{5,3}/S_3)(\mathbb{F}_q)$$

are all known [8], all of which provide additional logically independent consistency check.

### 3.6.2 Point counts with marked points

As noted earlier, given Theorem 3.1.6 one can count the $\mathbb{F}_2$-points of any moduli stack corresponding to genus 6 curves with some additional marked structure, as in Corollary 3.1.7. This count will always yield an integer consequent of Lemma 3.1.5.

### 3.6.3 Point counts in strata

Point counts of some strata of $\mathcal{M}_6$ are also known, and can be used to check the corresponding sections of our table. See Table 3.2 for a summary of this discussion.

- For hyperelliptic curves, it is straightforward to compute that

  $$\#\mathcal{H}_6(\mathbb{F}_q) = q^{11};$$

  see [7] for much stronger results.

- For plane quintics, Gorinov [35] showed that $\mathcal{Q}_6$ has trivial rational cohomology, yielding

  $$\#\mathcal{Q}_6(\mathbb{F}_q) = q^{12}.$$

  This has been rederived by elementary means by Wennink [93].

- For bielliptic curves, Kedlaya [45, Proposition 4.5] has shown that

  $$\#\mathcal{B}_g(\mathbb{F}_q) = \frac{q^{2g} - q^{2g-4} - q^{2g-5} + (-1)^{g+1}q}{q^2+1}$$

  for $6 \leq g \leq 11$ and for every odd prime $q$. This formula does not hold for $q = 2$; it predicts $\#\mathcal{B}_6(\mathbb{F}_2) = 742$, whereas the computed value is 744 (see Table 3.2). See also [45, Remark 4.4].

We are not aware of any prior computation of $\#\mathcal{T}_{6,n}(\mathbb{F}_q)$. Comparing the values for

**Table 3.2.** Point counts (unweighted and weighted) over $\mathbb{F}_2$ of the various strata of $\mathcal{M}_6$. When known, the weighted point count over $\mathbb{F}_q$ is also listed.

| Stratum | Unweighted | Weighted | Weighted count over $\mathbb{F}_q$ |
|---|---|---|---|
| $\mathcal{H}_6$ | 4134 | 2048 | $q^{11}$ |
| $\mathcal{B}_6$ | 1530 | 744 | $q^{10} - q^8 - q^5 + q^3 - q$ ($q$ odd) |
| $\mathcal{Q}_6$ | 4204 | 4096 | $q^{12}$ |
| $\mathcal{T}_{6,0}$ | 7282 | 7166 | ? |
| $\mathcal{T}_{6,2}$ | 6181 | 6148 | ? |
| $\mathcal{M}_6^{\mathrm{BN}}$ | 48896 | 48413 | ? |
| $\mathcal{M}_6$ | 72227 | 68615 | $q^{15} + q^{14} + 2q^{13} + q^{12} - q^{10} + q^3 - 1$ |

$q = 2$ with Zheng's results on the stable cohomology of $\mathcal{T}_{g,n}$ [98] suggests that

$$\#\mathcal{T}_{6,0}(\mathbb{F}_q) \approx q^{13} - q^{10}, \qquad \#\mathcal{T}_{6,2}(\mathbb{F}_q) \approx q^{12} + q^{11}.$$

While there is no reason to expect a dearth of lower-order terms, for $q = 2$ these expressions come astonishingly close to the computed counts (7168 and 6144 in place of the actual values 7166 and 6148).

*Remark* 3.6.3. The polynomial point count of $\#\mathcal{M}_7(\mathbb{F}_q)$ is not known as of the writing of this thesis; in fact, our experimentally obtained count of $\#\mathcal{M}_7(\mathbb{F}_2)$ may be needed to determine the polynomial for $\#\overline{\mathcal{M}}_7(\mathbb{F}_q)$ in [8]. The polynomial point count for $\#\mathcal{M}_7(\mathbb{F}_q)$ that one may eventually obtain using this method would no longer provide a logically independent consistency check of our computational result.

**Acknowledgments**

Chapter 3 is, in part, based on the following papers, one published and one being prepared for submission for publication, of with the dissertation author is a coauthor and collaborator.

• Yongyuan Huang, Kiran S. Kedlaya, Jun Bo Lau, "A census of genus 6 curves over $\mathbb{F}_2$," accepted to LuCaNT 2025.

- Yongyuan Huang, Kiran S. Kedlaya, Jun Bo Lau, “A census of genus 5 curves over $\mathbb{F}_3$ and genus 7 curves over $\mathbb{F}_2$,” in preparation.

# Bibliography


[1] *Cohomologie $l$-adique et fonctions $L$*, volume Vol. 589 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin-New York, 1977. Séminaire de Géometrie Algébrique du Bois-Marie 1965–1966 (SGA 5), Edité par Luc Illusie.

[2] Montserrat Alsina and Pilar Bayer. *Quaternion orders, quadratic forms, and Shimura curves*, volume 22 of *CRM Monograph Series*. American Mathematical Society, Providence, RI, 2004.

[3] Eran Assaf. A note on the trace formula. https://arxiv.org/abs/2311.03523, 2023. 21 pages.

[4] Eran Assaf, Jef Laga, Freddy Saia, Ciaran Schembri, Ari Shnidman, Jacob Swenberg, and John Voight. On explicit moduli problems for shimura curves. Work in progress, 2025.

[5] László Babai, Gene Cooperman, Larry Finkelstein, Eugene Luks, and Ákos Seress. Fast Monte Carlo algorithms for permutation groups. volume 50, pages 296–308. 1995. 23rd Symposium on the Theory of Computing (New Orleans, LA, 1991).

[6] Kai A. Behrend. The Lefschetz trace formula for algebraic stacks. *Invent. Math.*, 112(1):127–149, 1993.

[7] Jonas Bergström. Equivariant counts of points of the moduli spaces of pointed hyperelliptic curves. *Doc. Math.*, 14:259–296, 2009.

[8] Jonas Bergström, Samir Canning, Dan Petersen, and Johannes Schmitt. in preparation.

[9] Jonas Bergström, Carel Faber, and Sam Payne. Polynomial point counts and odd cohomology vanishing on moduli spaces of stable curves. *Ann. of Math. (2)*, 199(3):1323–1365, 2024.

[10] Jonas Bergström and Orsola Tommasi. The rational cohomology of $\overline{\mathscr{M}}_4$. *Math. Ann.*, 338(1):207–239, 2007.

[11] M. Bertolini and H. Darmon. Heegner points on Mumford-Tate curves. *Invent. Math.*, 126(3):413–456, 1996.

[12] Alex J. Best, Jonathan Bober, Andrew R. Booker, Edgar Costa, John E. Cremona, Maarten Derickx, Min Lee, David Lowry-Duda, David Roe, Andrew V. Sutherland, and John Voight. Computing classical modular forms. In *Arithmetic Geometry, Number Theory, and Computation*, Simons Symposia, pages 131–213. Springer, 2021.

[13] B. J. Birch. How the number of points of an elliptic curve over a fixed prime field varies. *J. London Math. Soc.*, 43:57–60, 1968.

[14] Bryan J. Birch and H. P. F. Swinnerton-Dyer. Notes on elliptic curves. i. *Journal für die reine und angewandte Mathematik*, 212:7–25, 1963.

[15] Z. I. Borevi ˇ c and D. K. Faddeev. Integral representations of quadratic rings. *Vestnik Leningrad. Univ.*, 15(19):52–64, 1960.

[16] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. version 2.28-3 obtained via https://magma.maths.usyd.edu.au/.

[17] Bradley W. Brock and Andrew Granville. More points than expected on curves over finite field extensions. volume 7, pages 70–91. 2001. Dedicated to Professor Chao Ko on the occasion of his 90th birthday.

[18] Samir Canning and Hannah Larson. The bielliptic locus in genus 11. *Michigan Math. J.*, 2024. https://arxiv.org/abs/2209.09715.

[19] Samir Canning and Hannah Larson. On the Chow and cohomology rings of moduli spaces of stable curves. *Journal of the European Mathematical Society*, 2024. https://arxiv.org/abs/2208.02357.

[20] Samir Canning, Hannah Larson, Sam Payne, and Thomas Willwacher. Moduli spaces of curves with polynomial point counts. 2024. https://arxiv.org/abs/2410.19913.

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

[22] Pete L. Clark. *Rational Points on Atkin-Lehner Quotients of Shimura Curves*. PhD thesis, Harvard University, Cambridge, Massachusetts, 2003. Available at: http://alpha.math.uga.edu/~pete/thesis.pdf.

[23] Henri Cohen. Trace des opérateurs de Hecke sur $\Gamma_0(N)$. In *Séminaire de Théorie des Nombres (1976–1977)*, pages Exp. No. 4, 9. Centre National de Recherche Scientifique, Laboratoire de Théorie des Nombres, Talence, 1977.

[24] Alain Couvreur and Iwan Duursma. Evaluation codes from smooth quadric surfaces and twisted Segre varieties. *Des. Codes Cryptogr.*, 66(1-3):291–303, 2013.

[25] Vincent Delecroix, Johannes Schmitt, and Jason van Zelm. admcycles—a Sage package for calculations in the tautological ring of the moduli space of stable curves. *J. Softw. Algebra Geom.*, 11(1):89–112, 2021.

[26] Lassina Dembélé and Steve Donnelly. Computing Hilbert modular forms over fields with nontrivial class group. In *Algorithmic number theory*, volume 5011 of *Lecture Notes in Comput. Sci.*, pages 371–386. Springer, Berlin, 2008.

[27] Lassina Dembélé and John Voight. Explicit methods for Hilbert modular forms. In *Elliptic curves, Hilbert modular forms and Galois deformations*, Adv. Courses Math. CRM Barcelona, pages 135–198. Birkhäuser/Springer, Basel, 2013.

[28] Dušan Dragutinović. Computing binary curves of genus five. *J. Pure Appl. Algebra*, 228(4):Paper No. 107522, 19, 2024.

[29] W. Duke and Á. Tóth. The splitting of primes in division fields of elliptic curves. *Experiment. Math.*, 11(4):555–565, 2002.

[30] Taylor Dupuy, Kiran Kedlaya, David Roe, and Christelle Vincent. Isogeny classes of abelian varieties over finite fields in the LMFDB. In *Arithmetic geometry, number theory, and computation*, Simons Symp., pages 375–448. Springer, Cham, [2021] ©2021.

[31] Martin Eichler. über die Darstellbarkeit von Modulformen durch Thetareihen. *J. Reine Angew. Math.*, 195:156–171 (1956), 1955.

[32] Martin Eichler. Modular correspondences and their representations. *J. Indian Math. Soc. (N.S.)*, 20:163–206, 1956.

[33] Xander Faber and Jon Grantham. Binary curves of small fixed genus and gonality with many rational points. *J. Algebra*, 597:24–46, 2022.

[34] Xander Faber, Jon Grantham, and Everett W. Howe. On the maximum gonality of a curve over a finite field. *Algebra Number Theory*, 19(8):1637–1662, 2025.

[35] Alexei G. Gorinov. Real cohomology groups of the space of nonsingular curves of degree 5 in $\mathbf{C}\mathrm{P}^2$. *Ann. Fac. Sci. Toulouse Math. (6)*, 14(3):395–434, 2005.

[36] Matthew Greenberg and John Voight. Computing systems of Hecke eigenvalues associated to Hilbert modular forms. *Math. Comp.*, 80(274):1071–1092, 2011.

[37] Robin Hartshorne. *Residues and duality*, volume No. 20 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin-New York, 1966. Lecture notes of a seminar on the work of A. Grothendieck, given at Harvard 1963/64, With an appendix by P. Deligne.

[38] Jeffery Hein, Gonzalo Tornaria, and John Voight. Computing hilbert modular forms as orthogonal modular forms. https://arxiv.org/abs/2506.21981, 2025.

[39] Haruzo Hida. On abelian varieties with complex multiplication as factors of the Jacobians of Shimura curves. *Amer. J. Math.*, 103(4):727–776, 1981.

[40] H. Hijikata, A. Pizer, and T. Shemanske. Orders in quaternion algebras. *J. Reine Angew. Math.*, 394:59–106, 1989.

[41] Hiroaki Hijikata. Explicit formula of the traces of Hecke operators for $\Gamma_0(N)$. *J. Math. Soc. Japan*, 26:56–82, 1974.

[42] Hiroaki Hijikata, Arnold K. Pizer, and Thomas R. Shemanske. The basis problem for modular forms on $\Gamma_0(N)$. *Mem. Amer. Math. Soc.*, 82(418):vi+159, 1989.

[43] Taira Honda. Isogeny classes of abelian varieties over finite fields. *J. Math. Soc. Japan*, 20:83–95, 1968.

[44] Everett W. Howe. Enumerating hyperelliptic curves over finite fields in quasilinear time. *Res. Number Theory*, 11(1):Paper No. 26, 24, 2025.

[45] Yongyuan Huang, Kiran S. Kedlaya, and Jun Bo Lau. A census of genus 6 curves over $\mathbb{F}_2$. In *LuCaNT: Databases, Algorithms, and Computational Number Theory*, volume 840 of *Contemporary Mathematics*, pages 213–227. American Mathematical Society, Providence, RI, 2026.

[46] Yongyuan Huang and John Voight. shimura-jacobian. https://github.com/stevehuang235/shimura_jacobian, 2026. GitHub repository.

[47] Daniel Huybrechts. *Complex Geometry*. Universitext. Springer Berlin, Heidelberg, 2004.

[48] Manabu Ide and Shigeru Mukai. Canonical curves of genus eight. *Proc. Japan Acad. Ser. A Math. Sci.*, 79(3):59–64, 2003.

[49] Yasutaka Ihara. Hecke Polynomials as congruence $\zeta$ functions in elliptic modular case. *Ann. of Math. (2)*, 85:267–295, 1967.

[50] Hirofumi Ishikawa. On the trace formula for Hecke operators. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.*, 20:217–238, 1973.

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

[52] Bruce W. Jordan, Allan G. Keeton, Bjorn Poonen, Eric M. Rains, Nicholas Shepherd-Barron, and John T. Tate. Abelian varieties isogenous to a power of an elliptic curve. *Compos. Math.*, 154(5):934–959, 2018.

[53] Ernst Kani. Products of CM elliptic curves. *Collect. Math.*, 62(3):297–339, 2011.

[54] Nathan Kaplan and Ian Petrow. Elliptic curves over a finite field and the trace formula. *Proc. Lond. Math. Soc. (3)*, 115(6):1317–1372, 2017.

[55] Kiran S. Kedlaya. Search techniques for root-unitary polynomials. In Kristin E. Lauter and Kenneth A. Ribet, editors, *Computational Arithmetic Geometry*, volume 463 of *Contemporary Mathematics*, pages 71–81. American Mathematical Society, 2008.

[56] Kiran S. Kedlaya. The relative class number one problem for function fields, I. *Res. Number Theory*, 8(4):Paper No. 79, 21, 2022. associated repository https://github.com/kedlaya/same-class-number.

[57] Kiran S. Kedlaya. The relative class number one problem for function fields, II. 2023. https://arxiv.org/abs/2206.02084.

[58] Kiran S. Kedlaya. Orbit lookup trees. https://github.com/kedlaya/orbits/blob/main/orbits.pdf, 2024. GitHub repository preprint.

[59] Kiran S. Kedlaya. The relative class number one problem for function fields, III. In *LuCaNT: LMFDB, computation, and number theory*, volume 796 of *Contemp. Math.*, pages 55–73. Amer. Math. Soc., [Providence], RI, [2024] ©2024. associated repository https://github.com/kedlaya/same-class-number.

[60] Momonari Kudo and Shushi Harashita. Representation of non-special curves of genus 5 as plane sextic curves and its application to finding curves with many rational points. *J. Symbolic Comput.*, 122:Paper No. 102272, 15, 2024.

[61] Kristin Lauter. Non-existence of a curve over $\mathbf{F}_3$ of genus 5 with 14 rational points. *Proc. Amer. Math. Soc.*, 128(2):369–374, 2000.

[62] The LMFDB Collaboration. The L-functions and modular forms database. https://www.lmfdb.org, 2024. [Online; accessed 6 January 2024].

[63] Eduard Looijenga. Cohomology of $\mathscr{M}_3$ and $\mathscr{M}_3^1$. In *Mapping class groups and moduli spaces of Riemann surfaces (Göttingen, 1991/Seattle, WA, 1991)*, volume 150 of *Contemp. Math.*, pages 205–228. Amer. Math. Soc., Providence, RI, 1993.

[64] Yozô Matsushima and Goro Shimura. On the cohomology groups attached to certain vector valued differential forms on the product of the upper half planes. *Ann. of Math. (2)*, 78:417–449, 1963.

[65] Pietro Mercuri, Oana Padurariu, Frederick Saia, and Claudio Stirpe. Point counts, automorphisms, and gonalities of shimura curves. https://arxiv.org/abs/2507.15992, 2025. 32 pages.

[66] Toshitsune Miyake. *Modular forms*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, english edition, 2006. Translated from the 1976 Japanese original by Yoshitaka Maeda.

[67] Shigeru Mukai. Curves and Grassmannians. In *Algebraic geometry and related topics (Inchon, 1992)*, volume I of *Conf. Proc. Lecture Notes Algebraic Geom.*, pages 19–40. Int. Press, Cambridge, MA, 1993.

[68] Shigeru Mukai. Curves and symmetric spaces. I. *Amer. J. Math.*, 117(6):1627–1644, 1995.

[69] Shigeru Mukai. Curves and symmetric spaces, II. *Ann. of Math. (2)*, 172(3):1539–1558, 2010.

[70] Shigeru Mukai. Curves and symmetric spaces III: BN-special vs. 1-PS degeneration. *Proc. Indian Acad. Sci. Math. Sci.*, 132(2):Paper No. 57, 9, 2022.

[71] Nikola Penev and Ravi Vakil. The Chow ring of the moduli space of curves of genus six. *Algebr. Geom.*, 2(1):123–136, 2015.

[72] Alexandru A. Popa. On the trace formula for Hecke operators on congruence subgroups. *Proc. Amer. Math. Soc.*, 146(7):2749–2764, 2018.

[73] Alexandru A. Popa. On the trace formula for Hecke operators on congruence subgroups, II. *Res. Math. Sci.*, 5(1):Paper No. 3, 24, 2018.

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

[75] Alessandra Rigato. Uniqueness of low genus optimal curves over $\mathbb{F}_2$. In *Arithmetic, geometry, cryptography and coding theory 2009*, volume 521 of *Contemp. Math.*, pages 87–105. Amer. Math. Soc., Providence, RI, 2010.

[76] Christophe Ritzenthaler. Existence d'une courbe sur $\mathbb{F}_3$ de genre 5 avec 13 points rationnels. arXiv:math/0302147.

[77] Jeremy Rouse, Andrew V. Sutherland, and David Zureick-Brown. ell-adic-galois-images. https://github.com/AndrewVSutherland/ell-adic-galois-images, 2021. Source code related to the paper "$\ell$-adic images of Galois for elliptic curves over $\mathbb{Q}$".

[78] Jeremy Rouse, Andrew V. Sutherland, and David Zureick-Brown. $\ell$-adic images of Galois for elliptic curves over $\mathbb{Q}$ (and an appendix with John Voight). *Forum Math. Sigma*, 10:Paper No. e62, 63, 2022. With an appendix with John Voight.

[79] The Sage Developers. *SageMath, the Sage Mathematics Software System*, 2023. DOI 10.5281/zenodo.6259615.

[80] Frederick Saia. CM points on Shimura curves via QM-equivariant isogeny volcanoes. *Pacific J. Math.*, 332(2):321–384, 2024.

[81] Hiroshi Saito. On Eichler's trace formula. *J. Math. Soc. Japan*, 24:333–340, 1972.

[82] A. Selberg. Harmonic analysis and discontinuous groups in weakly symmetric Riemannian spaces with applications to Dirichlet series. *J. Indian Math. Soc. (N.S.)*, 20:47–87, 1956.

[83] Jean-Pierre Serre. *Rational points on curves over finite fields*, volume 18 of *Documents Mathématiques (Paris) [Mathematical Documents (Paris)]*. Société Mathématique de France, Paris, [2020] ©2020. With contributions by Everett Howe, Joseph Oesterlé and Christophe Ritzenthaler.

[84] Hideo Shimizu. On traces of Hecke operators. *J. Fac. Sci. Univ. Tokyo Sect. I*, 10:1–19, 1963.

[85] Hideo Shimizu. On zeta functions of quaternion algebras. *Ann. of Math. (2)*, 81:166–193, 1965.

[86] John Tate. Endomorphisms of abelian varieties over finite fields. *Invent. Math.*, 2:134–144, 1966.

[87] Andrey Trepalin. Del Pezzo surfaces over finite fields. *Finite Fields Appl.*, 68:101741, 32, 2020.

[88] Fang-Ting Tu and Yifan Yang. Jacquet-langlands correspondence for non-eichler orders. https://arxiv.org/abs/2509.02985, 2025.

[89] Jason van Zelm. Nontautological bielliptic cycles. *Pacific J. Math.*, 294(2):495–504, 2018.

[90] Yakov Varshavsky. Local terms for transversal intersections. *Compos. Math.*, 159(5):985–1004, 2023.

[91] John Voight. *Quaternion algebras*, volume 288 of *Graduate Texts in Mathematics*. Springer, Cham, [2021] ©2021.

[92] William C. Waterhouse. Abelian varieties over finite fields. *Ann. Sci. École Norm. Sup. (4)*, 2:521–560, 1969.

[93] Thomas Wennink. Counting the number of trigonal curves of genus 5 over finite fields. *Geom. Dedicata*, 208:31–48, 2020.

[94] Xavier Xarles. A census of all genus 4 curves over the field with 2 elements. 2020. https://arxiv.org/abs/2007.07822.

[95] Hiroyuki Yoshida. On an analogue of the Sato conjecture. *Invent. Math.*, 19:261–277, 1973.

[96] Chia-Fu Yu. Endomorphism algebras of QM abelian surfaces. *J. Pure Appl. Algebra*, 217(5):907–914, 2013.

[97] Don Zagier. Traces des opérateurs de Hecke. In *Séminaire Delange-Pisot-Poitou, 17e année: 1975/76, Théorie des nombres: Fasc. 2*, pages Exp. No. 23, 12. Secrétariat Math., Paris, 1977.

[98] Angelina Zheng. Stable Cohomology of the Moduli Space of Trigonal Curves. *Int. Math. Res. Not. IMRN*, (2):1123–1153, 2024.

[99] Weizhe Zheng. Six operations and Lefschetz-Verdier formula for Deligne-Mumford stacks. *Sci. China Math.*, 58(3):565–632, 2015.

[100] David Zywina. Possible indices for the galois image of elliptic curves over $\mathbb{Q}$. *Mathematics of Computation*, 88(317):2695–2710, 2019.