UNIVERSITY OF CALIFORNIA SAN DIEGO

Arithmetic of Algebraic Curves

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

in

Mathematics

by

Mingjie Chen

Committee in charge:

Professor Kiran Kedlaya, Chair
Professor Alina Bucur
Professor Russell Impagliazzo
Professor Dragos Oprea
Professor Cristian Popescu

2022

Copyright

Mingjie Chen, 2022

All rights reserved.

The dissertation of Mingjie Chen is approved, and it is acceptable in quality and form for publication on microfilm and electronically.

University of California San Diego

2022

TABLE OF CONTENTS

Dissertation Approval Page . . . iii

Table of Contents . . . iv

List of Figures . . . vii

List of Tables . . . viii

Acknowledgements . . . ix

Vita . . . x

Abstract of the Dissertation . . . xi

I Coleman integration on modular curves **1**

Chapter 1 Preliminaries . . . 2

1.1 Modular curves . . . 2

1.2 Modular forms . . . 5

1.3 Hecke operators . . . 6

1.4 Coleman integration . . . 8

Chapter 2 Coleman integration on modular curves . . . 11

2.1 Introduction . . . 11

2.2 Main strategy . . . 13

2.3 $X_0(N)$ . . . 16

2.3.1 Example – $X_0(37)$ . . . 17

2.4 $X_0^+(N)$ . . . 19

2.4.1 Preliminaries . . . 19

2.4.2 Expected rational points . . . 20

2.4.3 Basis of $H^0(X, \Omega^1)$ . . . 20

2.4.4 Hecke operator action . . . 20

2.4.5 Uniformizer . . . 21

2.4.6 Example – $X_0^+(67)$ . . . 21

2.5 $X_{ns}^+(N)$ . . . 23

2.5.1 Preliminaries . . . 23

2.5.2 Expected rational points . . . 24

2.5.3 Basis of $H^0(X, \Omega^1)$ . . . 25
2.5.4 Hecke operator action . . . 25
2.5.5 Example – $X_{ns}^+(13)$ . . . 26
2.6 Remarks on computation . . . 29

II Supersingular elliptic curves and isogeny graphs 32

Chapter 3 Preliminaries . . . 33
3.1 Elliptic curves with complex multiplication . . . 33
3.2 Elliptic curves over finite fields . . . 35
3.2.1 Ordinary and supersingular elliptic curves . . . 35
3.2.2 Isogeny class . . . 36
3.2.3 Kernel ideals and quotients . . . 38
3.2.4 Reduction of CM elliptic curves . . . 40
3.3 Isogeny graph . . . 41
3.3.1 Ordinary case . . . 41
3.3.2 Supersingular case . . . 43

Chapter 4 Orienteering with one endomorphism . . . 45
4.1 Introduction . . . 45
4.1.1 Main theorem . . . 47
4.1.2 Other algorithms presented . . . 49
4.1.3 Comparison with [99] . . . 50
4.1.4 Other contributions . . . 52
4.1.5 Outline . . . 52
4.2 Background . . . 53
4.2.1 Notations and conventions . . . 53
4.2.2 Runtime lemmata . . . 55
4.3 Oriented isogeny graphs . . . 57
4.3.1 Orientations . . . 58
4.3.2 Oriented isogeny graphs . . . 58
4.3.3 Frobenius and class group actions . . . 59
4.3.4 Volcano structure . . . 62
4.3.5 From oriented isogeny graph to isogeny graph . . . 63
4.3.6 Graph statistics and heuristics . . . 64
4.4 Navigating the K-oriented ℓ-isogeny graph . . . 66
4.4.1 Conjugate orientations and orientations from endomorphisms . . . 66

4.4.2 ℓ-primitivity, ℓ-suitability, and direction finding . . . 67
4.5 Representing orientations and endomorphisms . . . 69
4.5.1 Representations and functionality . . . 69
4.5.2 Functionality for rationally represented endomorphisms . . . 71
4.5.3 Functionality for isogeny chain endomorphisms . . . 71
4.5.4 Poly-rep runtime . . . 77
4.6 Orientation-finding for $j = 1728$ . . . 78
4.6.1 In terms of 1, **i**, **j**, **k** . . . 79
4.6.2 As an isogeny chain endomorphism . . . 85
4.6.3 Curves other than $j = 1728$ . . . 86
4.6.4 Heuristics . . . 86
4.7 Supporting algorithms for walking on oriented curves . . . 87
4.7.1 Computing an ℓ-primitive endomorphism . . . 87
4.7.2 Rim walking via the class group action . . . 88
4.7.3 Ascending to the rim using an orientation . . . 91
4.7.4 Ascending and walking the rim using the endomorphism ring . . . 93
4.8 Classical path-finding to $j = 1728$ . . . 95
4.9 Proof of the Main Theorem and Special Cases . . . 99
4.9.1 Proof of Theorem 4.1.1 . . . 99
4.9.2 Special cases . . . 99
4.10 Division by $[\ell]$ . . . 101

Chapter 5 On $\mathbb{F}_p$-roots of the Hilbert class polynomial modulo p . . . 108
5.1 Introduction . . . 108
5.2 Reinterpretation of the $\mathbb{F}_p$-roots . . . 110
5.3 The $\mathrm{Pic}(\mathcal{O})[2]$-action on $\mathcal{H}_p$ and the nonemptiness criterion . . . 117

Bibliography . . . 123

Figure 4.1: On the left hand side is a component of $\mathcal{G}_K$ for $p = 179$, $\ell = 2$ and $K = \mathbb{Q}(\sqrt{-47})$. On the right hand side is the supersingular 2-isogeny graph over $\mathbb{F}_{p^2}$. The green 5-cycle represents the rim of the volcano. 60

LIST OF TABLES

Table 2.1: Coleman integrations on $X_0(37)$ 19
Table 2.2: Two rational points on $X_0^+(67)$ 21
Table 2.3: Coleman integrations on $X_0^+(67)$) 23
Table 2.4: Coleman integrations on $X_{ns}^+(13)$ 30

ACKNOWLEDGEMENTS

There are many people whom I would like to express my sincere thanks to. First of all, I would like to thank my advisor, Dr Kiran Kedlaya, for long-term support and many helpful advice. Especially for suggesting computing Coleman integrations on modular curves as my research project, which turns out to be very interesting and suitably challenging.

I am very grateful to my parents for their constant support and unconditional trust in me throughout my life. I am also grateful to my boyfriend Woonam Lim for his love and for being there whenever I needed. There are also many friends who have taken important parts in my life at San Diego. Lots of my memorable moments in San Diego were shared with Jun Bo Lau, Zeyu Liu, Nandagopal Ramachandran, Sindhana P.S., Shubham Sinha, Wei Yin, Minxin Zhang and many others. It is my great fortune to have met them and became close friends with them.

Chapters 2 is, in full, being prepared for submission for publication. The dissertation author was the collaborator and the coauthor for the material below.

• Mingjie Chen, Kiran S. Kedlaya, Jun Bo Lau "Coleman integration on modular curves".

Chapters 4 is, in full, being prepared for submission for publication. The dissertation author was the collaborator and the coauthor for the material below.

• Sarah Arpin; Mingjie Chen; Kristin E. Lauter; Renate Scheidler; Katherine E. Stange; Ha T. N. Tran "Orienteering with one endomorphism".

Chapters 5 is, in full, being prepared for submission for publication. The dissertation author was the collaborator and the coauthor for the material below.

• Mingjie Chen, Jiangwei Xue "On $\mathbb{F}_p$-roots of the Hilbert class polynomial modulo p".

I would like to thank all the collaborators – Sarah Arpin, Kiran Kedlaya, Jun Bo Lau, Kristin Lauter, Renate Schidler, Kate Stange, Ha Tran, Jiangwei Xue – for many helpful conversations and permitting to include the materials to this dissertation.

VITA

2016	B. S. in Mathematics, Wuhan University
2016-2022	Graduate Teaching Assistant, University of California San Diego
2022	Ph. D. in Mathematics, University of California San Diego

ABSTRACT OF THE DISSERTATION

Arithmetic of Algebraic Curves

by

Mingjie Chen

Doctor of Philosophy in Mathematics

University of California San Diego, 2022

Professor Kiran Kedlaya, Chair

In this dissertation, we present a collection of results regarding the arithmetic of algebraic curves. More specifically, the curves involved are modular curves and elliptic curves. In the first part, we present an algorithm that computes a p-adic integration called Coleman integration on modular curves. Different from other methods, our algorithm does not require the knowledge of a model of the curve. The ability of computing such integrals aids the problem of finding rational points on modular curves. In the second part, we consider elliptic curves defined over finite fields of characteristic p. In particular, we are interested in supersingular elliptic curves. We first present a work on path-finding on supersingular ℓ-isogeny graphs using the theory of orientations. We then present a work on counting the number of $\mathbb{F}_p$-roots of the Hilbert class polynomial $\mathcal{H}_{\mathcal{O}}(x)$ modulo p, in the case when the $\mathbb{F}_{p^2}$-roots are supersingular j-invariants.

Part I

Coleman integration on modular curves

Chapter 1

Preliminaries

1.1 Modular curves

One way to define a modular curve is to define it as the quotient of the extended upper half plane $\mathcal{H}^+ := \mathcal{H} \cup \mathbb{Q} \cup \{\infty\}$ where $\mathcal{H} := \{z \in \mathbb{C} : \operatorname{Im} z > 0\}$. We define the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathcal{H}^+$ to be $\gamma(z) = \frac{az+b}{cz+d}$, where $z \in \mathcal{H}$ and $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. To define a modular curve as a quotient, we need the following definitions of subgroups of $\mathrm{SL}_2(\mathbb{Z})$.

Definition 1.1.1. Let N be a positive integer. The *principal congruence subgroup of level N* is

$$\Gamma(N) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) : \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \pmod{N}\}.$$

Definition 1.1.2. A subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$ is a *congruence subgroup* if $\Gamma(N) \subseteq \Gamma$ for some $N \in \mathbb{Z}^+$, in which case Γ is a congruence subgroup of level N.

Example 1.1.3. Besides $\Gamma(N)$, the two most important congruence subgroups are:

$$\Gamma_0(N) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) : \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right) \pmod{N}\},$$

$$\Gamma_1(N) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) : \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right) \pmod{N}\}.$$

Example 1.1.4. One also considers congruence subgroups Γ_H that are lifted from subgroups H

of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ defined by

$$\Gamma_H = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) : \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \pmod N \in H\}.$$

Definition 1.1.5. For any congruence subgroup $\Gamma \in \mathrm{SL}_2(\mathbb{Z})$, the *modular curve* $Y(\Gamma)$ is defined to be the set of orbits $\Gamma\backslash\mathcal{H} = \{\Gamma\tau : \tau \in \mathcal{H}\}$. If $\Gamma = \Gamma(N)$, $\Gamma_0(N)$ or $\Gamma_1(N)$, we denote the quotients of $\mathcal{H}$ by $Y(N)$, $Y_0(N)$ or $Y_1(N)$ respectively.

According to [37, Chapter 2], $Y(\Gamma)$ has a structure of connected Riemann surface. We define cusps of Γ as Γ-orbits of $\mathbb{Q} \cup \{\infty\}$. Adjoining cusps to the modular curve $Y(\Gamma)$ by considering the quotients $\Gamma\backslash\mathcal{H}^+$ turns it into a compact Riemann surface, and therefore an algebraic curve over $\mathbb{C}$. This is again called as a modular curve and is denoted by $X(\Gamma)$. If $\Gamma = \Gamma(N), \Gamma_0(N)$ or $\Gamma_1(N)$, we denote the quotients of $\mathcal{H}^+$ by Γ by $X(N)$, $X_0(N)$ or $X_1(N)$ respectively. When Γ is of the form Γ_H for some $H \subseteq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, we also denote the curve $Y(\Gamma_H)$ by Y_H and the compact Riemann surface $X(\Gamma_H)$ by X_H.

The most interesting point of view to take for modular curves is to view them as moduli space of elliptic curves with torsion data. Recall that a complex elliptic curve E is isomorphic to $\mathbb{C}/\Lambda_\tau$ for some $\tau \in \mathcal{H}$ where Λ_τ is the lattice generated by 1 and τ. Moreover, $\mathbb{C}/\Lambda_{\tau_1} \cong \mathbb{C}/\Lambda_{\tau_2}$ if and only if there exists $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that $\gamma(\tau_1) = \tau_2$. This establishes an one-to-one correspondence between the set of isomorphism classes of complex elliptic curves and the $\mathrm{SL}_2(\mathbb{Z})$-orbits of $\mathcal{H}$.

Associating each complex elliptic curve with different torsion data gives various bijections between elliptic curves with torsion data and complex points on modular curves. We illustrate the case when the modular curve X is $X_0(N)$. An *enhanced elliptic curve* for $\Gamma_0(N)$ is an ordered pair (E, C) where E is a complex elliptic curve and C is a cyclic subgroup of E of order N. Two pairs (E_1, C_1) and (E_2, C_2) are equivalent if there exists an isomorphism between E_1 and E_2 that takes C_1 to C_2. We denote the set of these equivalence classes by $S_0(N)$. [37, Theorem 1.5.1] demonstrates the bijection between $S_0(N)$ and $Y_0(N)$.

So far, the discussion about modular curves are all done from the transcendental point of view. In fact, $X_0(N)$ and $X_1(N)$ have models defined over $\mathbb{Q}$. In [37, Chapter 7], the nonsingular projective algebraic curves $X_0(N)_{alg}$ and $X_1(N)_{alg}$ over $\mathbb{Q}$ are defined by specifying the function

fields. Extending the field to $\mathbb{C}$ gives rise to two complex curves $X_0(N)_{alg,\mathbb{C}}$ and $X_1(N)_{alg,\mathbb{C}}$. They are shown to be isomorphic to the previously defined curves $X_0(N)$ and $X_1(N)$ as the corresponding curves have the same function fields.

In general, let H be any subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ such that:

1. $-I \in H$;
2. the determinant map $\det : H \to (\mathbb{Z}/N\mathbb{Z})^\times$ is surjective.

Taking the approach as in the previous paragraph where one considers the function field, the modular curves X_H defined earlier can be shown to be smooth projective algebraic curves over $\mathbb{Q}$ as well. In fact, the modular curves $X_0(N)$ and $X_1(N)$ can be also be viewed this way. One can verify that $X_0(N)$ corresponds to the choice $H = \{\left(\begin{smallmatrix} a & 0 \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) : a, d \in (\mathbb{Z}/N\mathbb{Z})^\times, c \in \mathbb{Z}/N\mathbb{Z}\}$, and $X_1(N)$ corresponds to $H = \{\left(\begin{smallmatrix} a & 0 \\ c & \pm 1 \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) : a \in (\mathbb{Z}/N\mathbb{Z})^\times, c \in \mathbb{Z}/N\mathbb{Z}\}$.

The noncuspidal $\overline{\mathbb{Q}}$-points on X_H corresponds to isomorphism classes of pairs (E, ϕ) where E is an elliptic curve defined over $\overline{\mathbb{Q}}$ and ϕ is an isomorphism between $E[N]$ and $\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$. Here two pairs (E_1, ϕ_1), (E_2, ϕ_2) are isomorphic if there is an isomorphism ψ of elliptic curves and element $h \in H$ such that the following diagram commutes:

$$\begin{array}{ccc} E_1[N] & \xrightarrow{\phi_1} & (\mathbb{Z}/N\mathbb{Z})^2 \\ \downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle h} \\ E_2[N] & \xrightarrow{\phi_2} & (\mathbb{Z}/N\mathbb{Z})^2. \end{array}$$

There is a natural definition of the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ action on non-cuspidal $\overline{\mathbb{Q}}$-points on X_H. Let $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, then

$$\sigma \cdot (E, \phi) := (E^\sigma, \phi \circ \sigma^{-1}).$$

We say that a point (E, ϕ) is $\mathbb{Q}$-rational if it is invariant under the $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ action. Clearly, a necessary condition for (E, ϕ) to be $\mathbb{Q}$-rational is that E is defined over $\mathbb{Q}$. In the case of $X_0(N)$, the $\mathbb{Q}$-rational points can be described more explicitly. They are elliptic curves E defined over $\mathbb{Q}$ such that E has a cyclic N-subgroup that is invariant under $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ action. Equivalently, $\mathbb{Q}$-rational points on $X_0(N)$ are elliptic curves E defined over $\mathbb{Q}$ such that E admits an outgoing

degree N isogeny defined over $\mathbb{Q}$.

1.2 Modular forms

In this section, we give a brief introduction to modular forms. All the contents presented here can be found in [37] with more details.

For any $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ and any integer k, we define the weight-k operator $[\gamma]_k$ on functions $f : \mathcal{H} \to \mathbb{C}$ by

$$(f[\gamma]_k)(\tau) = (c\tau + d)^{-k} f(\gamma(\tau)).$$

Definition 1.2.1. [37, Definition 1.2.3] Let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ and let k be an integer. A function $f : \mathcal{H} \to \mathbb{C}$ is a *modular form of weight k with respect to* Γ if

1. f is holomorphic;
2. f is weight-k invariant under Γ (i.e., $f[\gamma]_k = f$ for all $\gamma \in \Gamma$);
3. $f[\alpha]_k$ is holomorphic at ∞ for all $\alpha \in \mathrm{SL}_2(\mathbb{Z})$.

The set of modular forms of weight k with respect to Γ is denoted by $\mathcal{M}_k(\Gamma)$.

Each congruence subgroup Γ contains a matrix of the form $\left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right)$ for some minimal positive integer h and obviously h is at most N. In fact, h might be a proper factor of N. This indicates that a modular form $f \in \mathcal{M}_k(\Gamma)$ is $h\mathbb{Z}$-periodic and has a Fourier expansion $\sum_{n=0}^{\infty} a_n q_h^n$ where $q_h = e^{2\pi i \tau / h}$.

Definition 1.2.2. Let f be a modular form of weight k with respect to Γ. If $a_0 = 0$ in the Fourier expansion of $f[\alpha]_k$ for all $\alpha \in \mathrm{SL}_2(\mathbb{Z})$, then f is a *cusp form*. We denote the set of cusp forms of weight k with respect to Γ by $\mathcal{S}_k(\Gamma)$.

Example 1.2.3. The j-invariant is a modular function (i.e. weight 0) on the upper half plane

$$j : \mathcal{H} \to \mathbb{C}, \quad j(\tau) = 1728 \frac{(g_2(\tau))^3}{g_2(\tau)^3 - 25 g_3(\tau)^2} = \frac{1}{q} + 744 + 196884q + \cdots$$

where

$$q = e^{2\pi i\tau},$$
$$g_2(\tau) = 60 \sum_{(m,n)\neq(0,0)} \frac{1}{(m+n\tau)^4},$$
$$g_3(\tau) = 140 \sum_{(m,n)\neq(0,0)} \frac{1}{(m+n\tau)^6}.$$

We denote the $\mathbb{C}$-vector space of holomorphic differentials of a modular curve $X(\Gamma)$ by $H^0(X(\Gamma), \Omega^1)$. This space can be related to the space of weight 2 cusp forms $\mathcal{S}_2(\Gamma)$ as follows.

Proposition 1.2.1. *[37, Section 3.3] There is an isomorphism of $\mathbb{C}$-vector spaces*

$$\begin{array}{ccc} \mathcal{S}_2(\Gamma) & \xrightarrow{\sim} & H^0(X(\Gamma), \Omega^1) \\ f(\tau) & \longmapsto & f(\tau)d\tau. \end{array}$$

1.3 Hecke operators

Hecke operators are important operators for modular curves. They play a vital role in Chapter 2 when designing the algorithm for computing Coleman integration on modular curves. There are several ways one could define an Hecke operator, and the way we choose here is the transcendental one, via double coset operator.

Definition 1.3.1. Let Γ_1,Γ_2 be two congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$, $\alpha \in \mathrm{GL}_2(\mathbb{Q})^+$. We define the double coset operator $[\Gamma_1\alpha\Gamma_2]_k$ from $\mathcal{M}_k(\Gamma_1)$ to $\mathcal{M}_k(\Gamma_2)$ by

$$f[\Gamma_1\alpha\Gamma_2]_k := \sum f[\beta_i]_k,$$

where $f \in \mathcal{M}_k(\Gamma_1)$, $\{\beta_i\}_i$ is a set of coset representatives of $\Gamma_1\backslash\Gamma_1\alpha\Gamma_2$ and $f[\alpha]_k(\tau) = \det(\alpha)^{k-1}(c\tau+d)^{-k}f(\alpha\cdot\tau)$ is the slash-k operator.

The following two lemmas combined show that this union is finite.

Lemma 1.3.1. *[83, Lemma 5.1.] Let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ and let α be an element of $\mathrm{GL}_2(\mathbb{Q})^+$. Then $(\alpha^{-1}\Gamma\alpha \cap \mathrm{SL}_2(\mathbb{Z}))$ is again a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$.*

Lemma 1.3.2. *[83, Lemma 5.1.2] There is a bijection between the coset space $\Gamma_1\backslash\Gamma_1\alpha\Gamma_2$ and the coset space $(\alpha^{-1}\Gamma_1\alpha\cap\Gamma_2)\backslash\Gamma_2$, with the map given by $\Gamma_1\beta\mapsto(\alpha^{-1}\Gamma_1\alpha\cap\Gamma_2)\alpha^{-1}\beta$.*

Let H be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ and $\Gamma_H\subseteq\mathrm{SL}_2(\mathbb{Z})$ be the lift of H to $\mathrm{SL}_2(\mathbb{Z})$. Let p be a prime does not divide N. [6, Section 4.4.1] gives an adelic description of the Hecke operator T_p as a correspondence. They also relate this description to double cosets, which we use as a definition of T_p.

Definition 1.3.2. [6, Lemma 4.4.15] Let $p\nmid N$ be a prime and $\alpha\in\mathrm{M}_2(\mathbb{Z})$ be such that $\det(\alpha)=p$ and $\alpha\,(\mathrm{mod}\ N)\in H$. The Hecke operator T_p is defined to be T_α. Here T_α denotes the double coset operator $[\Gamma_H\alpha\Gamma_H]$.

The coset representatives of $\Gamma_H\backslash\Gamma_H\alpha\Gamma_H$ can be hard to compute directly, the following lemma provides a bijection that makes the computation easier.

Lemma 1.3.3. *[79, Lemma 3.29(5)] Let α be as in Lemma 1.3.2. If $\Gamma_H\alpha\Gamma_H=\cup_i\Gamma_H\alpha_i$ is a disjoint union, then $\mathrm{SL}_2(\mathbb{Z})\alpha\,\mathrm{SL}_2(\mathbb{Z})=\cup_i\mathrm{SL}_2(\mathbb{Z})\alpha_i$.*

It follows immediately from this lemma that if $\mathrm{SL}_2(\mathbb{Z})\alpha\,\mathrm{SL}_2(\mathbb{Z})=\cup_i\mathrm{SL}_2(\mathbb{Z})\alpha_i$ with $\alpha_i\in\Gamma_H$, then $\Gamma_H\alpha\Gamma_H=\cup_i\Gamma_H\alpha_i$ holds. Therefore, the computation of Hecke operators T_p for a subgroup $H\subseteq\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ can be broken into the following steps.

1. Find $\alpha\in\mathrm{M}_2(\mathbb{Z})$ such that $\det(\alpha)=p$ and $\alpha\,(\mathrm{mod}\ N)\in H$.
2. Compute α_i's such that $\mathrm{SL}_2(\mathbb{Z})=\cup_i(\mathrm{SL}_2(\mathbb{Z})\cap\alpha^{-1}\,\mathrm{SL}_2(\mathbb{Z})\alpha)\alpha_i$.
3. Use lemma 1.3.2 and compute β_i's such that $\mathrm{SL}_2(\mathbb{Z})\alpha\,\mathrm{SL}_2(\mathbb{Z})=\cup_i\mathrm{SL}_2(\mathbb{Z})\beta_i$.
4. For each β_i, find $\gamma_i\in\mathrm{SL}_2(\mathbb{Z})$ such that $\gamma_i\beta_i\in\Gamma_H$. The set $\{\gamma_i\beta_i\}$ will be the set of the desired coset representatives of $\Gamma_H\backslash\Gamma_H\alpha\Gamma_H$.

Hecke operators T_p also act on the divisor group of modular curve $X(\Gamma)$. For a point P given as a coset $\Gamma\tau$,

$$T_p(\Gamma\tau):=\sum_i\Gamma\beta_i(\tau). \tag{1.3.1}$$

Here $\{\beta_i\}_i$ is a set of coset representatives $\Gamma_1\backslash\Gamma_1\alpha\Gamma_2$.

Example 1.3.3. Let N be an integer and p a prime such that $p \nmid N$, we consider the modular curve $X_0(N)$. For the Hecke operator T_p, α can be taken to be $\left(\begin{smallmatrix}1 & 0\\ 0 & p\end{smallmatrix}\right)$. The coset representatives are given by $\{\left(\begin{smallmatrix}1 & 0\\ 0 & p\end{smallmatrix}\right), \left(\begin{smallmatrix}1 & 1\\ 0 & p\end{smallmatrix}\right), \ldots, \left(\begin{smallmatrix}1 & p-1\\ 0 & p\end{smallmatrix}\right), \left(\begin{smallmatrix}p & 0\\ 0 & 1\end{smallmatrix}\right)\}$. It is worth mentioning that in this example we have a clear moduli interpretation of the Hecke operator action on divisors. Recall that a point on the modular curve $X_0(N)$ is a pair (E, C), where E is an elliptic curve and C is a cyclic subgroup of order N. Then

$$T_p(E, C) = \sum_{D\subseteq E[p],\ |D| = p} (E/D, (C + D)/D).$$

More generally, for $H \leq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ and p coprime to N, we obtain the modular curve X_H and its fiber product $X_H(p) := X_0(p)\times_{X(1)}X_H$. There are two degeneracy maps $\alpha, \beta : X_H(p) \to X_H$ defining the Hecke operator at p where one forgets the cyclic group of order p and the other quotients out by the cyclic group. By Picard functoriality, for a point $(E, \mathfrak{n}) \in X_H$ where the level structure $\mathfrak{n}$ is determined by H, we have an algebraic description of the Hecke operator at p:

$$T_p(E, \mathfrak{n}) := \alpha^*\beta_*(E, \mathfrak{n}) = \sum_{f:E\to E', deg(f)=p} (E', f(\mathfrak{n})).$$

This will be used in our computations since the j-invariants of the elliptic curves E' appearing in the summation are p-isogenous to E, which implies that their j-invariants satisfy p-th modular polynomial, i.e., $\Phi_p(j(E), j(E')) = 0$.

1.4 Coleman integration

In the 1980s, Coleman wrote a series of papers [24–26] where he developed a theory of p-adic line integration on curves and varieties with good reduction at p, which are now known as Coleman integrals. There are many arithmetic applications of Coleman integrals, among which are the abelian Chabauty method and quadratic Chabauty method. We record useful properties of the Coleman integral.

Theorem 1.4.1. *(Coleman) Let $X/\mathbb{Q}_p$ be a nice*[1] *curve with good reduction at p, let J be the Jacobian of X. Then there is a p-adic integral*

$$\int_P^Q \omega \in \overline{\mathbb{Q}}_p$$

with $P, Q \in X(\overline{\mathbb{Q}}_p), \omega \in H^0(X, \Omega^1)$ satisfying:

1. *The integral is $\overline{\mathbb{Q}}_p$ linear in ω.*
2. *There is an open subgroup of $J(\mathbb{Q}_p)$ such that $\int_P^Q \omega$ can be computed in terms of power series in some uniformizer by formal term-by-term integration. In particular, $\int_P^P \omega = 0$.*
3. $$\int_P^Q \omega + \int_{P'}^{Q'} \omega = \int_P^{Q'} \omega + \int_{P'}^{Q} \omega$$

   Thus, we can define $\int_D \omega$, where $D \in Div_X^0(\overline{\mathbb{Q}}_p)$. Also, if D is principal, $\int_D \omega = 0$.
4. *The integral is compatible with the action of $Gal(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$.*
5. *Let $P_0 \in X(\overline{\mathbb{Q}}_p)$ be fixed. Then the set of $P \in X(\overline{\mathbb{Q}}_p)$ reducing to $X(\overline{\mathbb{F}}_p)$ such that $\int_{P_0}^P \omega = 0$ is finite.*
6. *We have additivity of endpoints:*
   $$\int_P^Q \omega = \int_P^R \omega + \int_R^Q \omega.$$
7. *If $U \subseteq X, V \subseteq Y$ are wide open subspaces of the rigid analytic spaces X, Y, ω a 1-form on V, a rigid analytic map $\phi : U \to V$, then we have this change of variables formula:*
   $$\int_P^Q \phi^* \omega = \int_{\phi(P)}^{\phi(Q)} \omega.$$
8. *$\int_P^Q df = f(Q) - f(P)$.*
9. *If $P, Q \in X(\mathbb{Q}_p)$ then $\int_P^Q \omega \in \mathbb{Q}_p$.*

[1] smooth, projective, and geometrically irreducible

Definition 1.4.2. In the case when P and Q reduce to the same point in $X_{\mathbb{F}_p}(\overline{\mathbb{F}}_p)$, i.e., they lie in the same residue disc. We say that the integral $\int_P^Q \omega$ is a *tiny integral*.

Remark 1.4.3. Explicitly, if P and Q are in the same residue disc, then the tiny integral can be computed easily by formally integrating the power series and evaluating at the endpoints:

$$\int_P^Q \omega = \int_{t(P)}^{t(Q)} \omega(t) = \int_{t(P)}^{t(Q)} \sum a_i t^i dt = \sum \frac{a_i}{i+1}(t(Q) - t(P))^{i+1}.$$

Coleman's construction is quite suitable for explicit computation. In [10], the authors gave an algorithm for computing single Coleman integrals for hyperelliptic curves. Their method is based on an algorithm developed by Kedlaya [51] for computing the Frobenius action on the de Rham cohomology of hyperelliptic curves. In [13], this algorithm is generalized to arbitrary smooth curves, building on the algorithms of [90, 91] that generalize the computation of the Frobenius action on the de Rham cohomology on hyperelliptic curves to smooth curves. Despite recent developments of explicit computation of Coleman integration, these algorithms can not be applied to modular curves with large level. The reason being that such modular curves tend to have large gonality, hence it is hard to find nice plane affine models. However, such models are required in current implementation of the algorithms. This is the motivation of Chapter 2 where we introduce a new method for computing Coleman integration that does not require such models.

Chapter 2

Coleman integration on modular curves

2.1 Introduction

In the 1980s, Coleman developed a p-adic theory of line integrals on curves and higher dimensional varieties with good reduction at p [24–26]. This has found many applications in, for example, computing torsion points on Jacobian of curves (Manin-Mumford conjecture), p-adic heights, and so on. One of the most recent applications lie in explicit Mordell, more specifically, the abelian Chabauty and Kim's nonabelian Chabauty program in finding rational points on curves of genus $g \geq 2$.

In this chapter, the curves we are interested in are modular curves, which are special types of algebraic curves whose $\mathbb{Q}$-rational points classify elliptic curves E over $\mathbb{Q}$ with torsion data. Therefore, understanding rational points will provide information on the possible Galois actions on the torsion subgroup E_{tors} of E. Regarding this, Serre has made the famous uniformity conjecture.

Conjecture 2.1.1. *(Serre's uniformity conjecture). There is a positive constant C such that, the representation*

$$\rho_{E,p} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_p),$$

of the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$*, is surjective for every elliptic curve E over $\mathbb{Q}$ without*

complex multiplication and for all prime numbers $p > C$.

This was shown by himself to be implied by the following [77].

Conjecture 2.1.2. *Let H be a proper subgroup of $GL_2(\mathbb{F}_p)$ such that $\det: H \to \mathbb{F}_p^\times$ is surjective. There is a positive constant C_H such that, for all primes $p > C_H$, the only rational points on modular curves $X_H(p)$ of level p, defined over $\mathbb{Q}$, are the "expected points".*

Expected points on modular curves are CM elliptic curves with extra conditions imposed on $\mathrm{End}(E)$ depending on the H we are considering, and any points that are not expected are called as *exceptional*. As suggested by the name, expected points are easy to find, thus finding rational points on modular curves is mainly about finding exceptional points.

By the classification of maximal subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$, it is enough to consider the following H for Conjecture 2.1.2: Borel, normalizer of split Cartan, normalizer of non-split Cartan and exceptional subgroups. The current status of Serre's uniformity conjecture is that it has been verified (see [15,16,64,66]), except for the case when H is the normalizer of the non-split Cartan subgroup $C_{ns}^+(p)$ in $\mathrm{GL}_2(\mathbb{F}_p)$.

As a generalization of Serre's uniformity question, Mazur's Program B [65] asks for all of the possible Galois actions on torsion subgroups of elliptic curves without complex multiplication. This roughly amounts to determining the rational points on all modular curves.

One of the computational tools in finding solutions of diophantine equations is the Quadratic Chabauty method developed by Balakrishnan, Dogra, Müller, Tuitman, and Vonk [7,8,11,12]. The Quadratic Chabauty Method is developed to allow curves X with $r = g$ and it has proven itself to be a powerful tool. One example is the successful application of this method on the "cursed" curve $X_{ns}^+(13)$ to provably find all the rational points there [8]. Curves on which the Quadratic Chabauty Method can be applied have to satisfy a Quadratic Chabauty bound given in terms of the rank of Jacobian, genus of the curve and Néron–Severi rank of the Jacobian. Modular curves are considered as ideal playground for the Quadratic Chabauty Method in the sense that most of them satisfy the Quadratic Chabauty bound [82].

Even though most modular curves satisfy the Quadratic Chabauty bound, it seems impractical to apply this method to modular curves with large level. The main reason is that these curves

have large gonality and there seems to be no good way to write down nice affine plane models, which are required as the inputs of the current Quadratic Chabauty algorithm. Thus it would be ideal to get around the difficulty in finding nice affine patches, and instead develop a model-free version of the Quadratic Chabauty method. An important arithmetic value to compute in the Quadratic Chabauty algorithm is the Coleman integration. In Chapter 2, we present a model-free algorithm that computes Coleman integration on modular curves, the main idea is to take advantage of the Hecke operator to break these integrals into a sum of simpler ones, which are *tiny integrals*.

2.2 Main strategy

In this section, we explain the main strategy of our model free calculation, which works for all modular curves as well as their the Atkin-Lehner quotients, but the details can vary for each type of modular curves. We will later explain our algorithms in detail for the cases when the modular curves are of the form $X_0(N)$, $X_0^+(N)$ and $X_{ns}^+(N)$ with N being an integer prime.

Let $X/\mathbb{Q}$ be a modular curve that corresponds to a congruence subgroup Γ. Let Q, R be two $\mathbb{Q}$-rational points and $\{\omega_1, \ldots, \omega_g\}$ be a $\mathbb{Q}$-basis of $H^0(X, \Omega^1)$. Let p be a prime where X has good reduction ($p \nmid N$). We denote the Hecke operator T_p action matrix with respect to this basis by A, i.e.,

$$T_p^* \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_g \end{pmatrix} = A \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_g \end{pmatrix}.$$

Therefore,

$$\begin{pmatrix} \int_R^Q T_p^* \omega_1 \\ \vdots \\ \int_R^Q T_p^* \omega_g \end{pmatrix} = A \begin{pmatrix} \int_R^Q \omega_1 \\ \vdots \\ \int_R^Q \omega_g \end{pmatrix}.$$

On the other hand, for any $\omega \in H^0(X, \Omega^1)$, we have

$$\int_R^Q T_p^*(\omega) = \int_{T_p(R)}^{T_p(Q)} \omega = \sum_{i=0}^{p} \int_{R_i}^{Q_i} \omega,$$

where $T_p(Q) = \sum_{i=0}^{p} Q_i$ and $T_p(R) = \sum_{i=0}^{p} R_i$.

We substitute $\int_R^Q T_p^*(\omega_j)$ by $\sum_{i=0}^{p} \int_{R_i}^{Q_i} \omega_j$ and subtract both sides from $(p+1)\int_R^Q T_p^*(\omega_j)$ which leads to the following:

$$\begin{pmatrix} \sum_{i=0}^{p} \int_{Q_i}^{Q} \omega_1 - \sum_{i=0}^{p} \int_{R_i}^{R} \omega_1 \\ \vdots \\ \sum_{i=0}^{p} \int_{Q_i}^{Q} \omega_g - \sum_{i=0}^{p} \int_{R_i}^{R} \omega_g \end{pmatrix} = ((p+1)I - A) \begin{pmatrix} \int_R^Q \omega_1 \\ \vdots \\ \int_R^Q \omega_g \end{pmatrix}.$$

Note that due to Eichler-Shimura relation [37, Theorem 8.7.2], the integrals on the left hand side are all tiny integrals and therefore local power series expansions which are easy to compute. Also, the matrix $(p+1)I - A$ is invertible due to the Ramanujan bound $|a_p| \leq 2\sqrt{p}$. Therefore, we have converted the problem of computing Coleman integral into the problem of finding a basis of $\mathcal{S}_2(\Gamma)$ and computing tiny integrals of the form $\sum_{i=0}^{p} \int_{Q_i}^{Q} \omega$ on the basis (in fact, computing $\sum_{i=0}^{p} \int_{Q_i}^{Q} \omega$ for a basis element ω is not different from doing that for an arbitrary $\omega \in H^0(X(\Gamma), \Omega^1)$).

In the following sections, we will address these problems for modular curves $X_0(N)$, $X_0^+(N)$ and $X_{ns}^+(N)$ respectively. Our strategy takes a transcendental approach. The main tasks are the following:

Task 2.2.1. Let X denote the modular curve defined by the congruence subgroup Γ.

1. Find a $\mathbb{Q}$-rational point Q on X and find $\tau \in \mathcal{H}$ such that $\Gamma\tau$ corresponds to Q.
2. Compute a basis for the $\mathbb{C}$-vector space $\mathcal{S}_2(\Gamma)$, which gives rise to a $\mathbb{Q}$-basis of $H^0(X(\Gamma), \Omega^1)$ via Proposition 1.2.1. The $\mathbb{Q}$-basis exists since we are considering modular curves defined over $\mathbb{Q}$.
3. Compute the T_p action on the basis elements of $\mathcal{S}_2(\Gamma)$ as well as rational points Q of X. This boils down to a double coset space computation.
4. Compute the summation of tiny integrals $\sum_{i=0}^{p} \int_{Q_i}^{Q} \omega$ for $\omega \in H^0(X(\Gamma), \Omega^1)$.

We will address the first 3 tasks for the aforementioned modular curves separately as the methods vary for each type. Before going into the details, we first present a general algorithm which solves Task 4, assuming the knowledge of Task 1, 2 and 3.

Algorithm 2.2.2. Computing $\sum_{i=0}^{p} \int_{Q_i}^{Q} \omega$.

Inputs:

- A good prime p which does not divide $j(Q)$ and $j(Q) - 1728$.
- A cusp form $f \in \mathcal{S}_2(\Gamma)$ given by its q_h-expansion where $q = e^{2\pi i \tau/h}$. We denote the corresponding 1-form by ω.
- $\tau_0 \in \mathcal{H}$ such that $\Gamma\tau_0$ corresponds to a rational point Q on X, and $q_0 := e^{2\pi i \tau_0/h}$.

Outputs:

- The sum of tiny Coleman integrals $\sum_{i=0}^{p} \int_{Q_i}^{Q} \omega \in \mathbb{Q}_p$, where $T_p(Q) = \sum_{i=0}^{p} Q_i$.

Steps:

1. Write ω_i's as a power series of an uniformizer u. I.e. find $x_i \in \mathbb{Q}, i = 0, \ldots, n$ (n is some fixed precision depending on the p-adic precision required) such that

$$\omega = (\sum_{i=0}^{n} x_i (u)^n + \mathcal{O}((u)^{n+1}))d(u). \tag{2.2.1}$$

   These x_i's can be found using the following steps:

   (a) Write u, ω_i as power series expansions of $q - q_0$ by differentiating their q-expansions and evaluating at q_0:

$$\begin{aligned} u &= \sum_{i=1}^{C_1} a_i (q - q_0)^i + O((q - q_0)^{C_1+1}), \\ \omega &= \sum_{i=0}^{C_2} b_i (q - q_0)^i + O((q - q_0)^{C_2+1}) dq, \\ d(u) &= (\sum_{i=1}^{C_1} i a_i (q - q_0)^{i-1} + O((q - q_0)^{C_1})) dq, \end{aligned}$$

where C_1, C_2 are some fixed precision determined by n and the norm of q_0. The coefficients a_i, b_i's are in $\mathbb{C}$.

(b) Replace ω, u, $d(u)$ in equation (2.2.1) by their power series expansions in $q - q_0$. Comparing the coefficients of $(q - q_0)^k$ on both sides gives us the following linear system:

$$\begin{bmatrix} a_1 & 0 & 0 & \dots & 0 \\ 2a_2 & a_1^2 & 0 & \dots & 0 \\ 3a_3 & 3a_1a_2 & a_1^3 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ (n+1)a_{n+1} & \sum_{i=1}^{n} a_i(n+1-i)a_{n+1-i} & * & \dots & a_1^{n+1} \end{bmatrix} \cdot \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix}$$

(c) Solve this linear system and get complex approximations of x_i's.

(d) Recover x_i's as elements in $\mathbb{Q}$ using `algdep` from `PARI/GP`. This is likely to succeed given enough complex precision.

2. Calculate $j(Q_i)$ as algebraic integers. This can be computed transcendentally by evaluating the q-expansion of the j-function on $\beta_i(\tau_0)$ as in equation (1.3.1) and then obtain the algebraic approximation. On the other hand, the roots of the modular polynomial $\Phi_p(x, j(Q)) = 0$ are the j-invariants of elliptic curves that are p-isogenous to Q. This gives an algebraic method to compute $j(Q_i)$. The reason for computing $j(Q_i)$ is due to the fact that the j-function is often used as an uniformizer.

3. Compute the sum of tiny integrals $\sum_{i=0}^{p} \int_{Q}^{Q_i} \omega \approx \sum_{i=0}^{p} \int_{0}^{u(Q_i)} (\sum_{j=0}^{n} x_j t^j dt)$ and its p-adic expansion.

2.3 $X_0(N)$

We will consider modular curves $X_0(N)$ in this section. We will denote $X_0(N)$ by X. The noncuspidal rational points on X can be found via LMFDB [61], given as elliptic curves E over $\mathbb{Q}$ such that E admits a $\mathbb{Q}$-rational isogeny to E' of degree N. Given one such point Q, the correct coset representative $\Gamma_0(N)\tau_0$ can be found by first computing $\tilde{\tau}_0$ such that $\mathrm{SL}_2(\mathbb{Z})\tilde{\tau}_0$ corresponds

to E (i.e., $j(\tilde{\tau}_0) = j(E)$) and then iterate through coset representatives γ_i of $\Gamma_0(N)/\operatorname{SL}_2(\mathbb{Z})$ to find i such that $\gamma_i(\tilde{\tau}_0)$ satisfies:

$$j(\gamma_i(\widetilde{\tau_0})) = j(N\gamma_i(\widetilde{\tau_0})) = j(E).$$

We then choose $\tau_0 = \gamma_i(\tilde{\tau}_0)$.

The basis of $\mathcal{S}_2(\Gamma_0(N))$ is easy to find, see [86]. We have also discussed the Hecke operator T_p action in Example 1.3.3. Note that computing both the basis of $\mathcal{S}_2(\Gamma_0(N))$ and the Hecke operator T_p action on forms are implemented in `SageMath` [89].

Let $\omega \in H^0(X, \Omega^1)$, $Q \in X(\mathbb{Q})$. We follow Algorithm 2.2.2 to compute $\sum_{i=0}^{p} \int_{Q_i}^{Q} \omega$. In this case, we choose the uniformizer u to be $j(\tau) - j(Q)$.

2.3.1 Example – $X_0(37)$

Curve data In this example, we consider the modular curve $X = X_0(37)$. X is a hyperelliptic curve and has a plane model $y^2 = -x^6 - 9x^4 - 11x^2 + 37$ [67]. There are four rational points $Q = (1, -4)$, $R = (-1, -4)$, $S = (1, 4)$, $T = (-1, 4)$, where Q, R are noncuspidal rational points and S, T are cuspidal rational points. [67] also gives the q-expansion of x, y.

Rational points Using the fact that the modular j-function is a modular function on $X_0(37)$ and that $X_0(37)$ is hyperelliptic, we express j-function as a rational function of coordinates x, y and compute that $j(Q) = -9317 = -7 \cdot 11^3$, $j(R) = -162677523113838677 = -7 \cdot 137^3 \cdot 2083^3$.

The points Q, R correspond to elliptic curves E together with a cyclic subgroup of order 37, or equivalently, with a degree 37-isogeny. This information could be found in LMFDB [61]. Following the method in Section 2.3, we obtain the upper half plane representatives of Q, R as follows:

$$\tau_Q \approx 0.5 + 0.17047019819380 \cdot i \in \mathcal{H},$$

$$\tau_R \approx 0.5 + 0.39635999889406 \cdot i \in \mathcal{H}.$$

Basis of differential forms The computation of a basis of the space $\mathcal{S}_2(\Gamma_0(N))$, as well as the Hecke operator action on forms in $\mathcal{S}_2(\Gamma_0(N))$ can be done using `SageMath`. This way, we obtain an eigenbasis $\{f_0,\ f_1\}$ of the vector space $\mathcal{S}_2(\Gamma_0(37))$. Explicitly:

$$f_0 = q + q^3 - 2q^4 + O(q^6),$$
$$f_1 = q - 2q^2 - 3q^3 + 2q^4 - 2q^5 + O(q^6).$$

Hecke action We choose p to be 3, and $T_3(f_0) = f_0, T_3(f_1) = -3f_1$. Therefore the Hecke operator matrix T_3 is $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -3 \end{smallmatrix}\right)$.

Algorithm 2.2.2 and results Let ω_0, ω_1 be 1-forms that correspond to cusp forms $-\frac{1}{2}f_0$, $-\frac{1}{2}f_1$ respectively. We compute Coleman integrals on ω_0, ω_1. The reason for multiplying the cusp forms by $-\frac{1}{2}$ is that this way, $\omega_0 = \frac{dx}{y}$ and $\omega_1 = \frac{xdx}{y}$.

Now we explain in detail how to calculate $\sum_{i=0}^{p}\int_{Q_i}^{Q}\omega_1$ using Algorithm 2.2.2. In Step 1, we obtain rational coefficients x_i in the expansion of ω_1 about $j = j(Q)$:

$$\begin{aligned}\omega_1 =&(-9317) + \frac{717409}{2\cdot 37\cdot 47}(j-j(Q)) + \frac{253086749261192}{37^2\cdot 47^3}(j-j(Q))^2\\ &+ \frac{176804544077038351043955}{37^3\cdot 47^5}(j-j(Q))^3 + O((j-j(Q))^4)\ \ d(j-j(Q)).\end{aligned}$$

In Step 2, we compute the j-invariants $j(Q_i)$ of Q_i's for $i = 0, \ldots, 3$. They are roots of the modular polynomial $\Phi_3(j(Q), X) = 0$. In Step 3, substitute the roots in below expression, which is a sum of local power series:

$$\begin{aligned}\sum_{i=0}^{3}\int_{Q_i}^{Q}\omega_1 = \sum_{i=0}^{3}\int_{j(Q_i)-j(Q)}^{0}&(-9317) + \frac{717409}{2\cdot 37\cdot 47}t + \frac{253086749261192}{37^2\cdot 47^3}t^2\\ &+ \frac{176804544077038351043955}{37^3\cdot 47^5}t^3 + \cdots dt.\end{aligned}$$

Our results are listed in the table. We can verify them by comparing with the results given by using the hyperelliptic model of this curve. They are also verified by comparison with Balakrishnan-Tuitman's implementation in `MAGMA` [9].

Table 2.1: Coleman integrations on $X_0(37)$

$\sum_{i=0}^{3} \int_{Q_i}^{Q} \omega_0$	$O(3^{14})$
$\sum_{i=0}^{3} \int_{Q_i}^{Q} \omega_1$	$3^2 + 3^3 + 3^9 + 3^{10} + 2 \cdot 3^{11} + 3^{12} + 2 \cdot 3^{13} + O(3^{14})$
$\sum_{i=0}^{3} \int_{R_i}^{R} \omega_0$	$O(3^{14})$
$\sum_{i=0}^{3} \int_{R_i}^{R} \omega_1$	$3^2 + 3^3 + 3^9 + 3^{10} + 2 \cdot 3^{11} + 3^{12} + 2 \cdot 3^{13} + O(3^{14})$

2.4 $X_0^+(N)$

2.4.1 Preliminaries

We review briefly some background on the curves $X_0^+(N)$ which is necessary for our algorithm. We then talk about the model free algorithm for Coleman integrals on these curves. We will sometimes denote $X_0^+(N)$ by X for convenience.

The Atkin-Lehner involution $W_N = \frac{1}{\sqrt{N}} \left(\begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix}\right)$ is a well defined map on $\Gamma_0(N)$-orbits of $\mathcal{H}$. This map is an involution, i.e., $W_N W_N$ gives the identity map on orbits. Compactifying the quotient of $\mathcal{H}$ by $\Gamma_0^+(N) := \Gamma_0(N) \cup W_N \Gamma_0(N)$ gives us a modular curve, denoted by $X_0^+(N)$. This modular curve has a moduli interpretation:

Proposition 2.4.1. *Suppose $\Gamma_0(N)\tau \in X_0(N)$ corresponds to the elliptic curve with torsion data $(E_1, \phi : E_1 \to E_2)$, then $W_N(\Gamma_0(N)\tau)$ corresponds to $(E_2, \hat{\phi} : E_2 \to E_1)$, where $\hat{\phi}$ is the dual isogeny.*

Proof. $\Gamma_0(N)\tau$ corresponds to $(E_\tau, \langle \frac{1}{N}, \tau \rangle)$ up to isomorphism. As $W_N(\tau) = \frac{-1}{N\tau}$, $W_N(\Gamma_0(N)\tau)$ corresponds to $[E_{\frac{1}{N\tau}}, \langle \frac{1}{N}, \frac{1}{N\tau} \rangle]$. Note that the relation between complex tori over $\Gamma_0(N)$ and elliptic curves with a cyclic subgroup of order N is captured by the following isomorphism $E_\tau / \langle \frac{1}{N}, \tau \rangle \cong \mathbb{C} / \langle \frac{1}{N}, \tau \rangle$. It is clear that $\langle \frac{1}{N}, \tau \rangle = \tau \langle 1, \frac{1}{N\tau} \rangle$, hence $E_{\frac{1}{N\tau}}$ is indeed isomorphic to $E_\tau / \langle \frac{1}{N}, \tau \rangle$. What is left to do is to check that the dual isogeny of $\phi : E \to E_\tau / \langle \frac{1}{N}, \tau \rangle$ is indeed the isogeny induced by $E_{\frac{1}{N\tau}}$. This can be checked by first computing the dual isogeny and comparing kernels. □

2.4.2 Expected rational points

Let N be a prime. For locating the expected points Q that correspond to CM elliptic curve E on $X = X_0^+(N)$, we follow Mercuri's method [70] as follows. We start with the list of discriminants of orders in imaginary quadratic number fields with class number one (see for instance [85]):

$$\mathcal{D} = \{-3, -4, -7, -8, -11, -12, -16, -19, -27, -28, -43, -67, -163\}. \tag{2.4.1}$$

Let E be an elliptic curve with complex multiplication such that the discriminant Δ_E of its endomorphism ring $\mathcal{O}_E$ is a class number one discriminant, i.e. $E_\Delta \in \mathcal{D}$. Elliptic curves E such that p splits or ramifies in $\mathcal{O}_E$ give rise to rational points on X [43]. Having found such a discriminant Δ_E, we denote the corresponding rational point by Q and we use the following steps to find the correct coset representative.

Step 1: Let us denote τ_E to be the generator of $\mathcal{O}_E$. We factor (N) to be the product of two principal ideals $\mathfrak{N}\bar{\mathfrak{N}}$ in $\mathcal{O}_E$. Denote by α the generator of $\mathfrak{N}$.

Step 2: Find integers c, d such that $\alpha = c\tau_E + d$. Find another two integers a, b such that the matrix $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$.

Step 3: Let $\tau_Q = \gamma(\tau_E)$. Then τ_Q will be our choice of coset representative for our point.

2.4.3 Basis of $H^0(X, \Omega^1)$

The basis of $H^0(X, \Omega^1)$ can be found using the following lemma.

Lemma 2.4.1. *[42, Chapter 2, Lemma 2] The holomorphic differentials $\Omega^1(X_0(N)/W_N)$ on X are isomorphic as a $\mathbb{C}$-vector space to the $\mathbb{C}$-span of the set*

$$S = \{f \in \mathcal{S}_2(N) | f|W_N = f\}.$$

2.4.4 Hecke operator action

Lemma 2.4.2. *The coset representatives of $(\alpha^{-1}\Gamma_0^+(N)\alpha \cap \Gamma_0^+(N))\backslash\Gamma_0^+(N)$ is the same as that of $(\alpha^{-1}\Gamma_0(N)\alpha \cap \Gamma_0(N))\backslash\Gamma_0(N)$.*

Proof. We first simplify the set $\alpha^{-1}\Gamma_0^+(N)\alpha \cap \Gamma_0^+(N)$.

$$\begin{aligned}\alpha^{-1}\Gamma_0^+(N)\alpha \cap \Gamma_0^+(N) &= \alpha^{-1}(\Gamma_0(N) \cup W_N\Gamma_0(N))\alpha \cap (\Gamma_0(N) \cup W_N\Gamma_0(N)) \\ &= (\alpha^{-1}\Gamma_0(N)\alpha \cap \Gamma_0(N)) \cup (\alpha^{-1}(W_N\Gamma_0(N))\alpha \cap W_N\Gamma_0(N))\end{aligned}$$

We prove the lemma by first listing the coset representatives of $\Gamma_0(N)\alpha\Gamma_0(N)$, and then we show that these matrices are in different $\alpha^{-1}\Gamma_0^+(N)\alpha \cap \Gamma_0^+(N)$-orbits. Last we show that any matrix in $\Gamma_0^+(N)$ is in one of the orbits in the list. We omit the details as they are straightforward. □

Remark 2.4.1. Lemma 2.4.2 implies that the Hecke operator T_p for X has the same coset representatives as T_p for $X_0(N)$. I.e., $\{\left(\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right), \left(\begin{smallmatrix}1&1\\0&p\end{smallmatrix}\right), \ldots, \left(\begin{smallmatrix}1&p-1\\0&p\end{smallmatrix}\right), \left(\begin{smallmatrix}p&0\\0&1\end{smallmatrix}\right)\}$.

2.4.5 Uniformizer

Let Q be a rational point that corresponds to an unordered pair $\{\phi : E_1 \to E_2, \hat{\phi} : E_2 \to E_1\}$. Unlike the case for $X_0(N)$, one can no longer choose $j(\tau)$ as the uniformizer. Instead one uses $j(\tau) + j_N(\tau)$ where $j_N(\tau) := j(N \cdot \tau)$, which is invariant under W_N. Therefore, in Step 2 of Algorithm 2.2.2, instead of computing $j(Q_i)$, one needs to compute $j(NQ_i) + j(Q_i)$. $j(Q_i)$'s are the roots of $\Phi_p(x, j(E_1)) = 0$, and $j(NQ_i)$'s are the roots of $\Phi_p(x, j(E_2)) = 0$. To match the correct pairs of roots for each Q_i, we should combine the information given by roots of modular polynomials with the result given by the transcendental method as explained in Algorithm 2.2.2 Step 2.

2.4.6 Example – $X_0^+(67)$

Curve data We consider $X_0^+(67)$, a hyperelliptic curve with equation $y^2 = x^6 + 2x^5 + x^4 - 2x^3 + 2x^2 - 4x + 1$. We consider the following rational points and their upper half plane representatives and discriminants:

Table 2.2: Two rational points on $X_0^+(67)$

	D	(x, y)	τ
R	-8	$(0, -1)$	$\frac{\sqrt{-2}+2}{3\sqrt{-2}+7}$
S	-12	$(1, 1)$	$\frac{\sqrt{-3}+9}{\sqrt{-3}+8}$

Uniformizers Compared to the $X_0(N)$, we use $j + j_N$ instead as the uniformizer since it is invariant under the Atkin-Lehner involution.

Expected points We explain how we obtained the following two rational points and their upper half plane representatives. R is the pair $\{\phi_1 : E_1 \to E_1, \hat{\phi}_1 : E_1 \to E_1\}$, with $j(E_1) = -2^{18}3^35^3$. $E_1/\mathbb{Q}$ has CM by the ring of integers $\mathcal{O}_{K_1}$ of $K_1 = \mathbb{Q}(\sqrt{-43})$. The fact that 67 splits in $\mathcal{O}_{K_1}$ implies that such pair of isogenies uniquely exists. Similarly, S is the pair $\{\phi_2 : E_2 \to E_2, \hat{\phi}_2 : E_2 \to E_2\}$, with $j(E_2) = 2^65^3$. $E_2/\mathbb{Q}$ has CM by the ring of integers $\mathcal{O}_{K_2}$ of $K_2(= \mathbb{Q}(\sqrt{-2}))$, 67 splits in $\mathcal{O}_{K_2}$ as well. Note that both R and S are not fixed by the Atkin-Lehner involution, as that corresponds to the case when 67 is ramified.

Recall that we have $j(R) = 2^65^3$, $D(R) = -8$, hence $\tau_R = \sqrt{-2}$. Following the steps described in Section 2.4.2, we have $(67) = (7 + 3\sqrt{-2})(7 - 3\sqrt{-2}), 7 + 3\sqrt{-2} = 7 + 3 \cdot \sqrt{-2} \implies \hat{\gamma} = \left(\begin{smallmatrix} 1 & 2 \\ 3 & 7 \end{smallmatrix}\right) \implies \hat{\tau}_R = \hat{\gamma}\tau_R = \frac{\sqrt{-2}+2}{3\sqrt{-2}+7} \approx 0.298507462686567 + 0.0211076651100462 \cdot i$.

Similarly, we have $j(S) = 2^43^35^3$, $D(S) = -12$, $\tau_S = \sqrt{-3}$. $(67) = (8+\sqrt{-3})(8-\sqrt{-3})$, $8+\sqrt{-3} = 8 + 1 \cdot \sqrt{-3} \implies \hat{\gamma} = \left(\begin{smallmatrix} -1 & -9 \\ 1 & 8 \end{smallmatrix}\right) \implies \hat{\tau}_S = \hat{\gamma}\tau_S = -\frac{\sqrt{-3}+9}{\sqrt{-3}+8} \approx 1.11940298507463 - 0.0258515045905802 \cdot i$.

Basis of differential forms From the 5-dimensional space of cusp forms for $\Gamma_0(67)$, one could compute the action of W_{67} on the space and find a 2-dimensional subspace spanned by cusp forms invariant under the Atkin-Lehner involution (for example, by using `SageMath` [89]):

$$\begin{aligned} \omega_0 = f_0\ dq/q &= 2q - 3q^2 - 3q^3 + 3q^4 - 6q^5 + O(q^6)\ \ dq/q, \\ \omega_1 = f_1\ dq/q &= -q^2 + q^3 + 3q^4 + O(q^6)\ \ dq/q. \end{aligned}$$

Hecke action Let $p = 13$ be a good prime. The Hecke matrix on this subspace is $T_{13} = \left(\begin{smallmatrix} -7/2 & 15/2 \\ 3/2 & -7/2 \end{smallmatrix}\right)$.

Algorithm 2.2.2 and results Following Step 1 of Algorithm 2.2.2, we list, for example, a power series expansion of the differential form ω_0 at $j = j(R)$:

$$\omega_0 = \frac{-1}{2^7 \cdot 5^2 \cdot 7^2} + \frac{3047}{2^{15} \cdot 5^5 \cdot 7^6}(j - j(R)) + \frac{-38946227}{2^{24} \cdot 5^8 \cdot 7^{10}}(j - j(R))^2 + \frac{33888900627}{2^{32} \cdot 5^{10} \cdot 7^{14}} + \frac{-110823337943341}{2^{42} \cdot 5^{13} \cdot 7^{17}}(j - j(R))^3 + O((j - j(R))^4) \quad d(j - j(R)).$$

In the modification of Step 2, we follow 2.4.5 to find the Hecke images. Next, we compute the integrals as in 3 and the values of the Coleman integrals can be easily verified with Balakrishnan-Tuitman's implementation on `MAGMA` since $X_0^+(67)$ is hyperelliptic.

Table 2.3: Coleman integrations on $X_0^+(67)$)

$\sum_{i=0}^{3} \int_{R_i}^{R} \omega_0$	$2 \cdot 13 + 13^2 + 3 \cdot 13^3 + 7 \cdot 13^4 + 11 \cdot 13^5 + 8 \cdot 13^6 + 8 \cdot 13^7 + 7 \cdot 13^8 + O(13^9)$
$\sum_{i=0}^{3} \int_{R_i}^{R} \omega_1$	$11 \cdot 13 + 8 \cdot 13^2 + 6 \cdot 13^3 + 8 \cdot 13^4 + 3 \cdot 13^5 + 6 \cdot 13^6 + 6 \cdot 13^7 + 7 \cdot 13^8 + O(13^9)$
$\sum_{i=0}^{3} \int_{S_i}^{S} \omega_0$	$10 \cdot 13 + 8 \cdot 13^2 + 2 \cdot 13^5 + 5 \cdot 13^6 + 10 \cdot 13^7 + 2 \cdot 13^8 + O(13^9)$
$\sum_{i=0}^{3} \int_{S_i}^{S} \omega_1$	$3 \cdot 13 + 7 \cdot 13^2 + 2 \cdot 13^3 + 10 \cdot 13^4 + 8 \cdot 13^5 + 5 \cdot 13^6 + 8 \cdot 13^8 + O(13^9)$

2.5 $X_{ns}^+(N)$

2.5.1 Preliminaries

We first recall the definition of a non-split Cartan subgroup and its normalizer in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. Let $\{1, \alpha\}$ be a basis of the 2-dimensional $\mathbb{F}_p$-vector space $\mathbb{F}_{p^2}^\times$. Let $\beta \in \mathbb{F}_{p^2}^\times$ and $\beta = x + y\alpha$. Suppose α has minimal polynomial $X^2 - tX + n$ over $\mathbb{F}_p$, define the following map that sends β to the matrix that corresponds to multiplication by β under basis $\{1, \alpha\}$.

$$\begin{aligned} i_\alpha : \mathbb{F}_{p^2}^\times &\to \mathrm{GL}_2(\mathbb{F}_p) \\ \beta &\mapsto \left(\begin{smallmatrix} x & -ny \\ y & x+ty \end{smallmatrix}\right). \end{aligned}$$

Given the choice of basis $\{1, \alpha\}$, the nonsplit Cartan subgroup C_{ns} of $\mathrm{GL}_2(\mathbb{F}_p)$ is the image of i_α. The normalizer C_{ns}^+ of C_{ns} in $\mathrm{GL}_2(\mathbb{F}_p)$ is obtained by adjoining the conjugation matrix on

$\mathbb{F}_{p^2}^{\times}$. Note that changing the basis will change C_{ns} and C_{ns}^{+} by conjugation.

It would be easier to choose α in basis $\{1, \alpha\}$ to be a square root ϵ of a quadratic non-residue in $\mathbb{F}_p$. Then ϵ satisfies $X^2 - \epsilon^2 = 0$, and C_{ns}^{+} is of the following form:

$$\{\begin{pmatrix} x & \epsilon^2 y \\ y & x \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \text{ where } (x, y) \in \mathbb{F}_p \times \mathbb{F}_p - \{(0,0)\}\}.$$

Suppose that β is chosen to be a generator of the cyclic group $\mathbb{F}_{p^2}^{\times}$. Then we can easily write down the generators of C_{ns}^{+}.

For example, if $p = 13$ and $\epsilon = \sqrt{7}$, one generator of $\mathbb{F}_{13^2}^{\times}$ is $1 + \epsilon$. Hence in this case, we have

$$C_{ns}^{+}(13) = \langle \begin{pmatrix} 1 & 7\times 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \rangle.$$

2.5.2 Expected rational points

We assume we already have a basis of weight 2 cusp forms on $X_{ns}^{+}(N)$.

Step 1: Among the list of imaginary quadratic discriminants of class number 1 (2.4.1), those discriminants Δ such that N is inert in the corresponding quadratic order $\mathcal{O}_\Delta$ give rise to expected $\mathbb{Q}$-points on $X_{ns}^{+}(N)$ [65]. Let $\{P_1, \cdots, P_r\}$ be the expected points, then we can easily get corresponding $\{\tau_{P_1}, \cdots \tau_{P_r}\}$ that gives the $\mathrm{SL}_2(\mathbb{Z})$-orbits for each P_i on the upper half plane.

Step 2: Take P, τ from the lists above, $\mathrm{SL}_2(\mathbb{Z})\tau = \cup \Gamma_{ns}^{+}(N)\tau_j$, where $\Gamma_{ns}^{+}(N)$ is the lift of $C_{ns}^{+}(N)$ in $\mathrm{SL}_2(\mathbb{Z})$. We know that there is one-to-one correspondence

$$\mathcal{H}/\Gamma_{ns}^{+}(N) \to \text{ noncuspidal } \mathbb{C}\text{-points of } X_{ns}^{+}(N),$$

hence there is a unique τ_{j_Q} such that $\Gamma_{ns}^{+}(N)\tau_{j_Q}$ corresponds to P. To get each τ_j, we need

to compute coset representatives of $\Gamma_{ns}^+(N)$ in $\mathrm{SL}_2(\mathbb{Z})$. We consider the following map:

$$\mathrm{SL}_2(\mathbb{Z})/\Gamma_{ns}^+(N) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/C_{ns}^+(N) \cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$$
$$\Gamma_{ns}^+(N)g \mapsto (C_{ns}^+(N) \cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}))\bar{g}.$$

This map is well defined and a bijection. Hence to find coset representatives of $\Gamma_{ns}^+(N)$ in $\mathrm{SL}_2(\mathbb{Z})$, it suffices to find coset representatives of $C_{ns}^+(N) \cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ in $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$.

Step 3: Suppose we found that $\{g_1, \cdots, g_s\}$ is a set of coset representatives of $\Gamma_{ns}^+(N)$ in $\mathrm{SL}_2(\mathbb{Z})$, then $\tau_j := g_j(\tau)$. We find the correct τ_{j_0} by evaluating the $\mathbb{Q}$-basis $\{f_1, f_2, f_3\}$ at each τ_j to see which one gives us a rational point.

2.5.3 Basis of $H^0(X, \Omega^1)$

In [104], Zywina explains how to compute the action of the slash-k operator of the matrices $S := \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and $T := \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ (via a numerically approximated matrix) on $S_2(\Gamma(N), \mathbb{Q}(\zeta_N))$. For a group $H \leq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ with $\det(H) = (\mathbb{Z}/N\mathbb{Z})^\times$ and $-I \in H$ (e.g., the nonsplit Cartan), one could compute the action of the generators of H on $S_2(\Gamma(N), \mathbb{Q}(\zeta_N))$. This can be essentially broken down into understanding the actions of $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ and matrices of the form $\left(\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right)$ on the q-expansions of the cusp forms. Then, using the isomorphism $\mathcal{S}_2(\Gamma(N), \mathbb{Q}(\zeta_N))^H \to H^0(X_H, \Omega^1)$, one finds a basis of differentials needed for our computation. We use Zywina's algorithm implemented in `MAGMA` to compute the basis of differentials.

2.5.4 Hecke operator action

There are two sides to the Hecke operator action T_p: on modular forms and on points. Before we begin, we assume that the double coset representatives $\Gamma_{ns}^+(N)\backslash\Gamma_{ns}^+(N)\alpha\Gamma_{ns}^+(N)$ have been computed for some α of determinant p, following the steps in Section 1.3.

1. On modular forms. Let $f \in \mathcal{S}_2(\Gamma_{ns}^+(N))$. Recall that the after obtaining the coset representatives $\{\alpha_i, i = 0, \cdots, p\}$ for $\Gamma_{ns}^+(N)\backslash\Gamma_{ns}^+(N)\alpha\Gamma_{ns}^+(N)$, we have the double coset operator $[\Gamma_{ns}^+(N)\alpha\Gamma_{ns}^+(N)]_2 f = \sum f|[\alpha_i]_2$ where the slash-k operator is defined as $f[\alpha](\tau) =$

$\det(\alpha)^{k-1}(c\tau+d)^{-k}f(\alpha\cdot\tau)$ in Section 1.3. As we shall see in the next example, the double coset representatives for T_p will have the form $\alpha_i = \varepsilon\varepsilon'\left(\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right)\beta$ or $\varepsilon\varepsilon'\beta\left(\begin{smallmatrix}p&0\\0&1\end{smallmatrix}\right)$ where ε,ε' are determinant 1 matrices related to the computation of α and β comes from the standard cosets of $\Gamma^0(p)\backslash\operatorname{SL}_2(\mathbb{Z})$. The computation breaks down as follows:

Step 1: Let $\mathcal{B}$ be a basis of $\mathcal{S}_2(\Gamma(N),\mathbb{Q}(\zeta_N))$. Zywina's code will output a basis $\mathcal{B}'=\{f_j\}_j$ of $\mathcal{S}_2(\Gamma(N),\mathbb{Q}(\zeta_N))^{\Gamma^+_{ns}(N)}$. We use the code again to compute $\tilde{f}_j := f_j|_2[\varepsilon\varepsilon']$. Denote by C the matrix of linear operator $\varepsilon\varepsilon'$ with respect to the basis $\mathcal{B}$ and by v_j the coordinate of f_j under the basis $\mathcal{B}$, then the coordinate of $\tilde{f}_j$ is Cv_j and hence $\tilde{f}_j = \mathcal{B}Cv_j$.

Step 2a: We compute $\tilde{f}_j|[\left(\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right)\beta]$ following the formulas in Section 2 of Chapter 5 in [37].

Step 2b: For the last coset, we take advantage of the fact that $\left(\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right)\left(\begin{smallmatrix}mp&n\\N&1\end{smallmatrix}\right)=\left(\begin{smallmatrix}m&n\\N&p\end{smallmatrix}\right)\left(\begin{smallmatrix}p&0\\0&1\end{smallmatrix}\right)$. So α_p is of the form $\varepsilon\varepsilon\beta\left(\begin{smallmatrix}p&0\\0&1\end{smallmatrix}\right)$ which is a product of three determinant 1 matrices and a determinant p matrix. The slash operators on the left three matrices can be computed via Zywina's code and the last action can be computed easily: it corresponds to the shift-by-p operator.

Step 3: The matrix corresponding to the Hecke operator T_p on cusp forms can be obtained by linear algebra.

2. On points. There are two ways of doing this. Either we can use the explicit double coset representatives or we use the p-th modular polynomial. Each approach has its (dis)advantages: we can evaluate cusp forms on explicit representatives but this will require a closer analysis of the group structure of $C^+_{ns}(N)$ and high enough complex precision; the modular polynomials give us the j-invariants of p-isogenous points but the polynomials have large coefficients.

2.5.5 Example – $X^+_{ns}(13)$

Curve data from basis of cusp forms In this example, we consider the curve $X = X^+_{ns}(13)$, known as the "cursed" curve [8]. Let $C^+_{ns}(13)$ be defined by choosing the quadratic non-residue to be 7 as in Section 2.5.1, and let $\Gamma^+_{ns}(13)$ be the lift of $C^+_{ns}(13)$ in $\operatorname{SL}_2(\mathbb{Z})$. Using Zywina's `MAGMA`

implementation [104] , we obtain a basis of cusp forms as follows:

$$\begin{aligned}
f_0 =&(3\zeta_{13}^{11}+\zeta_{13}^{9}+3\zeta_{13}^{8}+\zeta_{13}^{7}+\zeta_{13}^{6}+3\zeta_{13}^{5}+\zeta_{13}^{4}+3\zeta_{13}^{2}+1)q\\
&+(-\zeta_{13}^{10}-2\zeta_{13}^{9}-\zeta_{13}^{7}-\zeta_{13}^{6}-2\zeta_{13}^{4}-\zeta_{13}^{3}-2)q^2+O(q^3),\\
f_1 =&(4\zeta_{13}^{11}+2\zeta_{13}^{9}+5\zeta_{13}^{8}+5\zeta_{13}^{5}+2\zeta_{13}^{4}+4\zeta_{13}^{2})q\\
&+(-3\zeta_{13}^{11}-5\zeta_{13}^{10}-4\zeta_{13}^{9}-4\zeta_{13}^{8}-4\zeta_{13}^{7}-4\zeta_{13}^{6}-4\zeta_{13}^{5}-4\zeta_{13}^{4}-5\zeta_{13}^{3}-3\zeta_{13}^{2}-2)q^2+O(q^3),\\
f_2 =&(\zeta_{13}^{10}-2\zeta_{13}^{7}-2\zeta_{13}^{6}+\zeta_{13}^{3})q\\
&+(-\zeta_{13}^{11}-2\zeta_{13}^{10}-2\zeta_{13}^{8}-2\zeta_{13}^{5}-2\zeta_{13}^{3}-\zeta_{13}^{2}+2)q^2+O(q^3),
\end{aligned}$$

where ζ_{13} is a 13-th primitive root of unity and $q=e^{\frac{2\pi i\tau}{13}}$. Following the method in [42] and using the basis found above, we can find the canonical model of X to be

$$\begin{aligned}
&X^4-\frac{7}{12}X^3Y-\frac{37}{30}X^2Y^2+\frac{37}{30}XY^3-\frac{3}{10}Y^4-\frac{61}{60}X^3Z+\frac{41}{15}X^2YZ\\
&-\frac{103}{60}XY^2Z+\frac{19}{60}Y^3Z-\frac{23}{6}X^2Z^2+\frac{87}{20}XYZ^2-\frac{14}{15}Y^2Z^2-\frac{199}{60}XZ^3\\
&+\frac{97}{60}YZ^3-\frac{11}{15}Z^4=0,
\end{aligned}\tag{2.5.1}$$

here X, Y and Z corresponds to f_0, f_1 and f_2 respectively. The rational points can be found by a box search to be: $\{(\frac{3}{5}:2:1)$, $(-2:2:1)$, $(-2:\frac{-9}{2}:1)$, $(-2:\frac{-7}{3}:1)$, $(\frac{7}{3}:2:1)$, $(\frac{5}{4}:2:1)$, $(11:\frac{43}{2}:1)\}$.

Uniformizers Since $S_2(\Gamma_{ns}^{+}(13))\subseteq S_2(\Gamma(13))$, the j-function is a uniformizer for the nonsplit Cartan curve.

Expected points Among the discriminants D in list (2.4.1), we find D such that 13 is inert in the corresponding order $\mathcal{O}_D$. This list $\{-7,-8,-11,-19,-28,-67,-163\}$ contains discriminants that give rise to 7 expected rational points on X. We pick Q to be the point that corresponds to discriminant -7, and R to be the point that corresponds to discriminant -11. Following the notations in Section 2.5.2, we have $\tau_7=\frac{1}{2}+\frac{1}{2}\sqrt{-7}$ and $\tau_{11}=\frac{1}{2}+\frac{1}{2}\sqrt{-11}$. We then compute the

coset representatives of $\mathrm{SL}_2(\mathbb{Z})/\Gamma^+_{ns}(13)$,

$$\{g_0, \ldots, g_{77}\} = \{T^i,\ (T^2)ST^i,\ (T^3)ST^i,\ (T^4)ST^i,\ (T^5)ST^i,\ (T^{12})ST^i \text{ for } i = 0, \ldots, 12\},$$

here $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ are the two generators of $\mathrm{SL}_2(\mathbb{Z})$. By evaluating f_0, f_1, f_2 at $g_i(\tau_7)$ and $g_i(\tau_{11})$ for $i = 0, \ldots, 77$, we obtain the correct $\Gamma^+_{ns}(13)$-orbit representatives for Q and R, $\tau_Q = \frac{4+2\sqrt{-7}}{3+\sqrt{-7}}, \tau_R = \frac{13+\sqrt{-11}}{2}$. The way to locate the correct coset in the case of Q is to find the unique i such that $\frac{f_0(g_i(\tau_7))}{f_2(g_i(\tau_7))}$ and $\frac{f_1(g_i(\tau_7))}{f_2(g_i(\tau_7))}$ are rational numbers. Applying the same method to all the 7 discriminants, we get their corresponding rational points as computed from the model above.

Double coset We choose p to be 11. Let $\alpha = \left(\begin{smallmatrix} -778 & -241 \\ 297 & -1012 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 0 \\ 0 & 11 \end{smallmatrix}\right)$ be the element $\alpha \in M_2(\mathbb{Z})$ with $\det(\alpha) = 11$, $\alpha \pmod{13} \in C^+_{ns}(13)$. To find the double coset representatives we start with finding the coset representatives for $\mathcal{S} := (\alpha^{-1}\,\mathrm{SL}_2(\mathbb{Z})\alpha \cap \mathrm{SL}_2(\mathbb{Z}))\backslash\,\mathrm{SL}_2(\mathbb{Z}) = \Gamma^0(11)\backslash\,\mathrm{SL}_2(\mathbb{Z})$. For each $\beta \in \mathcal{S}$, we found a corresponding $\gamma \in \Gamma^0(11)$ such that the representative $\beta' = \gamma\beta \in \Gamma^+_{ns}(13)$. We define the set of coset representatives to be $\mathcal{S}' := (\alpha^{-1}\Gamma^+_{ns}(13)\alpha \cap \Gamma^+_{ns}(13))\backslash\Gamma^+_{ns}(13)$ and the set of corresponding γ's to be Γ.

$\mathcal{S} = \{\left(\begin{smallmatrix} 1 & i \\ 0 & 1 \end{smallmatrix}\right), i = 0, 1, \ldots, 10\} \cup \{\left(\begin{smallmatrix} 66 & 5 \\ 13 & 1 \end{smallmatrix}\right)\}$,

$\Gamma = \{\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ -2 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 11 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & -55 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 22 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & -44 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 33 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & -33 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 44 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & -22 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} -1 & -55 \\ 0 & -1 \end{smallmatrix}\right),$
$\left(\begin{smallmatrix} 1 & -44 \\ 0 & 1 \end{smallmatrix}\right)\}$,

$\mathcal{S}' = \{\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 1 \\ -2 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 13 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & -52 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 26 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & -39 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 39 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & -26 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 52 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & -13 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} -1 & -65 \\ 0 & -1 \end{smallmatrix}\right),$
$\left(\begin{smallmatrix} -506 & -39 \\ 13 & 1 \end{smallmatrix}\right)\}$.

From the bijection

$$\Gamma^+_{ns}(13)\backslash\Gamma^+_{ns}(13)\alpha\Gamma^+_{ns}(13) \to (\alpha^{-1}\Gamma^+_{ns}(13)\alpha \cap \Gamma^+_{ns}(13))\backslash\Gamma^+_{ns}(13)$$
$$\Gamma^+_{ns}(13)\delta \mapsto (\alpha^{-1}\Gamma^+_{ns}(13)\alpha \cap \Gamma^+_{ns}(13))\alpha^{-1}\delta,$$

we can get the double coset representatives of $\Gamma_{ns}^{+}(13)\backslash\Gamma_{ns}^{+}(13)\alpha\Gamma_{ns}^{+}(13)$:

$$\begin{aligned}\mathcal{S}_\alpha = \{&\left(\begin{smallmatrix}-13 & 4\\ 42 & -13\end{smallmatrix}\right)\left(\begin{smallmatrix}1 & 0\\ 0 & 11\end{smallmatrix}\right)\left(\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right)\left(\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right), \left(\begin{smallmatrix}-13 & 4\\ 42 & -13\end{smallmatrix}\right)\left(\begin{smallmatrix}1 & 0\\ 0 & 11\end{smallmatrix}\right)\left(\begin{smallmatrix}1 & 0\\ -2 & 1\end{smallmatrix}\right)\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right), \ldots,\\ &\left(\begin{smallmatrix}-13 & 4\\ 42 & -13\end{smallmatrix}\right)\left(\begin{smallmatrix}1 & 0\\ 0 & 11\end{smallmatrix}\right)\left(\begin{smallmatrix}-1 & -55\\ 0 & -1\end{smallmatrix}\right)\left(\begin{smallmatrix}1 & 10\\ 0 & 1\end{smallmatrix}\right), \left(\begin{smallmatrix}-13 & 4\\ 42 & -13\end{smallmatrix}\right)\left(\begin{smallmatrix}1 & 0\\ 0 & 11\end{smallmatrix}\right)\left(\begin{smallmatrix}1 & -44\\ 0 & 1\end{smallmatrix}\right)\left(\begin{smallmatrix}66 & 5\\ 13 & 1\end{smallmatrix}\right)\}\\ =\{&\left(\begin{smallmatrix}-13 & 4\\ 42 & -13\end{smallmatrix}\right)\left(\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right)\left(\begin{smallmatrix}1 & 0\\ 0 & 11\end{smallmatrix}\right)\left(\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right), \left(\begin{smallmatrix}-13 & 4\\ 42 & -13\end{smallmatrix}\right)\left(\begin{smallmatrix}1 & 0\\ -22 & 1\end{smallmatrix}\right)\left(\begin{smallmatrix}1 & 0\\ 0 & 11\end{smallmatrix}\right)\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right), \ldots,\\ &\left(\begin{smallmatrix}-13 & 4\\ 42 & -13\end{smallmatrix}\right)\left(\begin{smallmatrix}-1 & -5\\ 0 & -1\end{smallmatrix}\right)\left(\begin{smallmatrix}1 & 0\\ 0 & 11\end{smallmatrix}\right)\left(\begin{smallmatrix}1 & 10\\ 0 & 1\end{smallmatrix}\right), \left(\begin{smallmatrix}-13 & 4\\ 42 & -13\end{smallmatrix}\right)\left(\begin{smallmatrix}1 & -4\\ 0 & 1\end{smallmatrix}\right)\left(\begin{smallmatrix}1 & 0\\ 0 & 11\end{smallmatrix}\right)\left(\begin{smallmatrix}66 & 5\\ 13 & 1\end{smallmatrix}\right) = \left(\begin{smallmatrix}-13 & 4\\ 42 & -13\end{smallmatrix}\right)\left(\begin{smallmatrix}1 & -4\\ 0 & 1\end{smallmatrix}\right)\left(\begin{smallmatrix}6 & 5\\ 13 & 11\end{smallmatrix}\right)\left(\begin{smallmatrix}11 & 0\\ 0 & 1\end{smallmatrix}\right)\}.\end{aligned}$$

Hecke operator action on forms The reason for the presentation of elements in $\mathcal{S}_\alpha$ is our use of the Hecke operators as double coset operators as mentioned earlier in this section. The action of the right two matrices is well known [37] while the left two matrices can be computed via Zywina's code. The output is the Hecke matrix $A = \left(\begin{smallmatrix}0 & -1 & 2\\ 4 & -4 & 3\\ -1 & 1 & 4\end{smallmatrix}\right)$.

Algorithm 2.2.2 and results Now we explain in detail how to calculate $\sum_{i=0}^{p}\int_{Q_i}^{Q}\omega$ using Algorithm 2.2.2. In Step 1 of Algorithm 2.2.2, we compute a power series expansion of the differential form ω_0 at $j = j(Q)$:

$$\begin{aligned}\omega_0 = &\frac{1}{3^4\cdot 5^2\cdot 13} + \frac{23}{3^{10}\cdot 5^5\cdot 13}(j-j(Q)) + \frac{4}{3^{13}\cdot 5^7\cdot 13}(j-j(Q))^2\\ &+ \frac{437174}{3^{22}\cdot 5^{10}\cdot 13^3}(j-j(Q))^3 + \frac{138504533}{3^{28}\cdot 5^{13}\cdot 13^4}(j-j(Q))^4 + O((j-j(Q))^5)\ \ d(j-j(Q)).\end{aligned}$$

The Hecke images can be found by computing the roots of the modular polynomial equation $\Phi_{11}(j(Q), x) = 0$. Next, we compute the integrals as in Step 3. We record our results in the following Table.

2.6 Remarks on computation

Choice of p Aside from avoiding the bad primes of the modular curves, we omit those primes appearing in the denominators of x_i's for x_i's in equation 2.2.1. In practice, we omit the bad primes, prime factors of $j(P)$ and prime factors of $j(P) - 1728$. We do not have an explanation for this, but it has been verified repeatedly in our computational experiments.

Table 2.4: Coleman integrations on $X_{ns}^{+}(13)$

$\sum_{i=0}^{11}\int_{Q_i}^{Q}\omega_0$	$10\cdot 11^{-1}+9+9\cdot 11+6\cdot 11^2+7\cdot 11^3+9\cdot 11^4+O(11^5)$
$\sum_{i=0}^{11}\int_{Q_i}^{Q}\omega_1$	$8\cdot 11^{-1}+7+7\cdot 11+2\cdot 11^2+6\cdot 11^3+6\cdot 11^4+O(11^5)$
$\sum_{i=0}^{11}\int_{Q_i}^{Q}\omega_2$	$10\cdot 11^{-1}+8+8\cdot 11+11^2+9\cdot 11^4+O(11^5)$
$\sum_{i=0}^{11}\int_{R_i}^{R}\omega_0$	$7\cdot 11^{-1}+2+3\cdot 11+9\cdot 11^2+3\cdot 11^3+5\cdot 11^4+O(11^5)$
$\sum_{i=0}^{11}\int_{R_i}^{R}\omega_1$	$6+6\cdot 11+11^3+5\cdot 11^4+O(11^5)$
$\sum_{i=0}^{11}\int_{R_i}^{R}\omega_2$	$7\cdot 11^{-1}+4+11+10\cdot 11^2+10\cdot 11^3+5\cdot 11^4+O(11^5)$

Choice of the upper half plane representative In computing $\omega = \sum x_j(j-j(P))^i dj$, we compared Taylor expansions of both sides at $q = q(P)$ and used linear algebra over $\mathbb{C}$ to recover the coefficients x_i. Therefore, the accuracy of the x_i's depends on the convergence of the Taylor expansions. To achieve faster convergence, we want the imaginary part of $\tau(P)$ to be as large as possible. Therefore, we might try to find a better upper half plane representative for the point in the same coset. However, in practice, it is not easy to find an improvement.

Remark 2.6.1. In the case of $X_0^+(N)$, the Atkin-Lehner involutions can be used in to perform the task. However, for a CM elliptic curve E with discriminant Δ_E, the situation is not so ideal. Let (c,d) be an integer solution to the norm equation $|c\tau_E+d|^2 = N$ and let $\hat{\gamma}$ be the lift of (c,d) in $\mathrm{SL}_2(\mathbb{Z})$. Then the upper-half plane representative has imaginary part $\mathrm{Im}(\hat{\tau}) = \mathrm{Im}(\hat{\gamma}\cdot\tau_E) = \frac{\mathrm{Im}(\tau_E)}{|c\tau_E+d|^2} = \frac{\sqrt{-\Delta_E}}{2}\cdot\frac{1}{N}$, so the imaginary part decreases as $O(\frac{1}{N})$.

Fast algorithm for differentiating j-function We recall some formulas from [23].

$$\begin{aligned} a(q) &= 1+\sum_{n>0}(-1)^n(q^{n(3n-1)/2}+q^{n(3n+1)/2}),\\ \Delta(q) &= qa(q)^{24},\\ f(q) &= \frac{\Delta(2q)}{\Delta(q)},\\ j(q) &= \frac{(256f(q)+1)^3}{f(q)}. \end{aligned}$$

Our goal is to compute the Taylor series expansion of j at $q_0 := e^{2\pi i\tau_0}$ for some τ_0 in upper

half plane. As the coefficients of the q-expansion of the j map are very large, we can not evaluate the j map (and the derivatives of j) by plugging in q_0 to the q-expansion, especially when q_0 has absolute value close to 1. Instead, the exponents in the q-expansion of $a(q)$ grow quadratically, which ensures better convergence. So we try to express the j map and its derivatives as an algebraic expression of that of $a(q)$ using the above formulas and hence compute the Taylor series of j by first computing that of $a(q)$.

Chapter 2 is, in full, being prepared for submission for publication. The dissertation author was the collaborator and the coauthor for the material below.

- Mingjie Chen, Kiran S. Kedlaya, Jun Bo Lau "Coleman integration on modular curves".

Part II

Supersingular elliptic curves and isogeny graphs

Chapter 3

Preliminaries

3.1 Elliptic curves with complex multiplication

Most of the materials presented here can be found in [29].

Let $E/\mathbb{C}$ be an elliptic curve and let $\mathrm{End}(E)$ denote its endomorphism ring consisting of endomorphisms defined over $\mathbb{C}$. Let $\mathcal{O}$ be an imaginary quadratic order in an imaginary quadratic field K, we say that the elliptic curve E has *complex multiplication* (CM) by $\mathcal{O}$ if $\mathrm{End}(E) \cong \mathcal{O}$. We also define the endomorphism algebra of E to be $\mathrm{End}(E) \otimes \mathbb{Q}$, this is isomorphic to K when E has CM by $\mathcal{O}$.

Consider the set of CM elliptic curves over $\mathbb{C}$ with isomorphic endomorphism rings

$$\mathcal{E}\ell\ell_{\mathcal{O}}(\mathbb{C}) := \{\text{elliptic curves } E/\mathbb{C} : \mathrm{End}(E) \cong \mathcal{O}\}/\sim,$$

where $E \sim E'$ if they are isomorphic over $\mathbb{C}$. The set of two-dimensional lattices $\Lambda \subseteq \mathbb{C}$ up to homothety is in bijection with the set of isomorphism classes of elliptic curves over $\mathbb{C}$, where one sends the lattice Λ to $\mathbb{C}/\Lambda$. One can show that $\mathrm{End}(\mathbb{C}/\Lambda) \cong \mathcal{O}$ if and only if Λ is an invertible ideal of $\mathcal{O}$. Therefore, this implies the existence of a bijection

$$\begin{array}{ccc} \mathcal{C}\ell(\mathcal{O}) & \longleftrightarrow & \mathcal{E}\ell\ell_{\mathcal{O}}(\mathbb{C}) \\ [\mathfrak{a}] & \longmapsto & E_{\mathfrak{a}} := \mathbb{C}/\mathfrak{a}. \end{array}$$

Moreover, it turns out that $\mathcal{E}\ell\ell_{\mathcal{O}}(\mathbb{C})$ is a $\mathcal{C}\ell(\mathcal{O})$-torsor. Let $\mathfrak{a}$ be an invertible $\mathcal{O}$-ideal, we

define the action of $\mathfrak{a}$ on $E_{\mathfrak{b}}$ to be

$$\mathfrak{a}E_{\mathfrak{b}} = E_{\mathfrak{a}^{-1}\mathfrak{b}}.$$

This induces an action of $\mathcal{C}\ell(\mathcal{O})$ on $\mathcal{E}\ell\ell_{\mathcal{O}}(\mathbb{C})$ and one can show that this action is free and transitive.

The following theorem shows that CM elliptic curves are all defined over some number fields.

Theorem 3.1.1. *[29, Theorem 11.1] Let $\mathcal{O}$ be an order in an imaginary quadratic field K, and $E/\mathbb{C}$ be an elliptic curve with complex multiplication by $\mathcal{O}$. Then the j-invariant $j(E)$ is an algebraic integer and $K(j(E))$ is the ring class field of the order $\mathcal{O}$.*

Theorem 3.1.2. *[29, Corollary 11.37] Let $\mathcal{O}$ be an order in an imaginary quadratic field K, and let L be the ring class field of $\mathcal{O}$. Let E be an elliptic curve with complex multiplication by $\mathcal{O}$ that corresponds to an invertible $\mathcal{O}$-ideal $\mathfrak{b}$, i.e., $E \cong E_{\mathfrak{b}}$. Let $\mathfrak{a}$ be an invertible $\mathcal{O}$ ideal, define $\sigma_{\mathfrak{a}}(j(E_{\mathfrak{b}}))$ by the formula*

$$\sigma_{\mathfrak{a}}(j(E_{\mathfrak{b}})) = j(E_{\mathfrak{a}^{-1}\mathfrak{b}}).$$

Then $\sigma_{\mathfrak{a}}$ is a well-defined element of $\mathrm{Gal}(L/K)$, and $\mathfrak{a} \mapsto \sigma_{\mathfrak{a}}$ induces an isomorphism

$$\mathcal{C}\ell(\mathcal{O}) \xrightarrow{\sim} \mathrm{Gal}(L/K).$$

Let us denote by $H_{\mathcal{O}}(x)$ the minimal polynomial of $j(E)$ over $\mathbb{Q}$. $H_{\mathcal{O}}(x)$ has integer coefficients as $j(E)$ is an algebraic integer. As a simple corollary of 3.1.2, we obtain the following formula for $H_{\mathcal{O}}(x)$.

$$H_{\mathcal{O}}(x) = \prod_{E \in \mathcal{E}\ell\ell_{\mathcal{O}}(\mathbb{C})} (x - j(E)),$$

where $E \in \mathcal{E}\ell\ell_{\mathcal{O}}(\mathbb{C})$ should be interpreted as choosing one representative from each isomorphism class.

This polynomial $H_{\mathcal{O}}(x)$ is called as the *Hilbert class polynomial* of $\mathcal{O}$, and will be the main object of study in Chapter 5. We end the discuss here by stating some useful results regarding the discriminant of $H_{\mathcal{O}}(x)$.

Theorem 3.1.3. *[29, Theorem 13.28] Let $\mathcal{O}$ be an order in an imaginary quadratic field K and*

let D be its discriminant. Let p be a prime dividing the discriminant of $H_{\mathcal{O}}(x)$. Then $p \leq |D|$.

3.2 Elliptic curves over finite fields

In this section, p will denote a prime integer, k will denote a finite field of characteristic p. κ will be a finite extension of k and $\bar{k}$ will be the algebraic closure of k.

3.2.1 Ordinary and supersingular elliptic curves

Let E be an elliptic curve defined over k. We will denote the endomorphism ring of E consisting of endomorphisms over $\bar{k}$ by $\mathrm{End}(E)$. If we want to consider endomorphisms defined over a specific field κ, we will denote the corresponding endomorphism ring as $\mathrm{End}_{\kappa}(E)$.

Elliptic curves defined over finite fields are divided into two types – *ordinary* and *supersingular*. We present here the definition given in terms of endomorphism ring, for more equivalent definitions, see [83, Section V.3].

Definition 3.2.1. An elliptic curve E over k is *supersingular* if $\mathrm{End}(E)$ is a maximal order in a quaternion algebra. If E is not supersingular, E is called *ordinary*. In the ordinary case, $\mathrm{End}(E)$ is an order of a quadratic imaginary field.

The following is an useful fact about the defining field of supersingular elliptic curves.

Lemma 3.2.1. *[83, Section V.3, Theorem 3.1] Let E be a supersingular elliptic curve, then the j-invariant $j(E) \in \mathbb{F}_{p^2}$.*

In fact, the endomorphism algebra of supersingular elliptic curves E/k is the unique (up to isomorphism) quaternion algebra over $\mathbb{Q}$ that is ramified at p and ∞. We will fix one such quaternion algebra and denote it by $\mathcal{B}$. We will see that each maximal order in $\mathcal{B}$ arises as the endomorphism ring of some supersingular elliptic curve E.

Lemma 3.2.2. *[95, Lemma 42.4.1] Let $\mathcal{R} \subseteq \mathcal{B}$ be a maximal order. Then there exist one or two supersingular elliptic curves E up to isomorphism over $\overline{\mathbb{F}}_p$ such that $\mathrm{End}(E) \cong \mathcal{R}$. There exist two such elliptic curves if and only if $j(E) \in \mathbb{F}_{p^2} \backslash \mathbb{F}_p$ and if and only if the unique two-sided ideal of $\mathcal{R}$ of reduced norm p is not principal.*

3.2.2 Isogeny class

In this section, we will investigate isogeny classes of elliptic curves over finite fields. Two elliptic curves E, E' over k are said to be isogenous over k if there exists an isogeny $\varphi : E \to E'$ and φ is defined over k. Let $\#k = q$, we define the Frobenius endomorphism π_p on E to be

$$\begin{array}{ccc} E & \longrightarrow & E \\ P = (x, y) & \longmapsto & \pi_q(P) = (x^q, y^q). \end{array}$$

Theorem 3.2.2. *[87, Theorem 1] Let E and E' be elliptic curves defined over k, and let f and f' be the characteristic polynomials of their Frobenius endomorphisms. Then the following statements are equivalent:*

(a) E and E' are k-isogenous.

(b) $f = f'$.

(c) The zeta functions of E and E' are the same.

(d) E and E' have the same number of points in κ for every finite extension κ of k.

We can give the explicit formula of the number of κ-rational points on E via the characteristic polynomial.

Theorem 3.2.3. *[83, Theorem 2.3.1] Let E/k be an elliptic curve and $\#k = q$. Let $t = q + 1 - \#E(k)$.*

1. *The Frobenius endomorphism π_q satisfies*

$$\pi_q^2 - t\pi_q + q = 0 \quad \text{in } \mathrm{End}(E).$$

2. *Let $\alpha, \beta \in \mathbb{C}$ be the roots of the polynomial $X^2 - tX + q$. Then α and β are complex conjugates satisfying $|\alpha| = |\beta| = \sqrt{q}$, and for every $n \geq 1$,*

$$\#E(\kappa) = q^n + 1 - \alpha^n - \beta^n, \quad n = [\kappa : k].$$

We will from now on refer t in Theorem 3.2.3 as the *trace* of the elliptic curve E/k. Clearly, the possible values for t determine the possible characteristic polynomials of π_q and therefore the isogeny classes for elliptic curves over k. Note that due to Hasse's bound [83, Section V.1, Theorem 1.1], t satisfies that $|t| \leq 2\sqrt{q}$. The following theorem discusses the possible values of t within this range and divide them into different types.

Theorem 3.2.4. *[98, Theorem 4.1] The isogeny classes of elliptic curves over k where $\#k = q = p^n$ are in one-to-one correspondence with the rational integers t having $|t| \leq 2\sqrt{q}$ and satisfying some one of the following conditions:*

(a) $(t, p) = 1$;

(b) if n is even: $t = \pm 2\sqrt{q}$;

(c) if n is even and $p \not\equiv 1 \pmod 3$: $t = \pm\sqrt{q}$;

(d) if n is odd and $p = 2$ or 3: $t = \pm p^{\frac{n+1}{2}}$;

(e) if either (i): n is odd or (ii): n is even and $p \not\equiv \pmod 4$: $t = 0$.

The first of these are not supersingular; the second are and have all their endomorphisms defined over k; the rest are but do not have all their endomorphisms defined over k.

Note that in case (b), the Frobenius endomorphism π_q is a rational integer $\sqrt{q}$, while in all other cases, π_q is an imaginary quadratic element of degree 2.

Theorem 3.2.4 did not talk about the defining field of endomorphisms in the first case, i.e., the ordinary case. We will see that all endomorphisms are defined over k. Before proving this, we first recall a result of Lenstra.

Theorem 3.2.5. *[57, Theorem 1] Let k be a finite field, let E be an elliptic curve over k, and put $R = \mathrm{End}_k(E)$. Let $\pi_q \in R$ be the Frobenius endomorphism of E. Further, let κ be a finite field extension of k, and denote by $n = [\kappa : k]$ the extension degree. Suppose $\pi_q \notin \mathbb{Z}$. Then R has rank 2 over $\mathbb{Z}$, and there is an isomorphism $E(\kappa) \cong R/R(\pi_q^n - 1)$ of R-modules.*

Lemma 3.2.3. *Let E be an ordinary elliptic curve defined over a finite field k, and let κ be a finite extension of k of degree n. Then $\mathrm{End}_k(E) = \mathrm{End}_\kappa(E)$.*

Proof. Denote $\mathrm{End}_k(E)$ by R and $\mathrm{End}_\kappa(E)$ by R'. Clearly, $R \subseteq R'$. Let π_q denote the Frobenius endomorphism on E/k and π' denote the Frobenius endomorphism on E/κ. Then $\pi' = \pi_q^n$. Clearly π_q, $\pi' \notin \mathbb{Z}$. According to Theorem 3.2.5, we have $E(\kappa) \cong R/R(\pi_q^n - 1) = R/R(\pi' - 1)$. On the other hand, if we view E as an elliptic curve defined over κ, we would have $E(\kappa) \cong R'/R'(\pi' - 1)$. Therefore, $R/R(\pi' - 1) \cong R'/R'(\pi' - 1)$ and this implies that $R = R'$. □

3.2.3 Kernel ideals and quotients

In this section, we will consider an elliptic curves E over a finite field k together with an isomorphism $\iota_E : A \cong \mathrm{End}(E) \otimes \mathbb{Q}$ where A is some semi-simple algebra. The algebra A could be an imaginary quadratic field or a quaternion algebra depending on whether E is ordinary or supersingular. Given an isogeny $\varphi : E \to E'$, we have $\iota_{E'} : A \to \mathrm{End}(E') \otimes \mathbb{Q}$ naturally induced by ι_E as follows:

$$\iota_{E'}(a) = \frac{1}{n}\varphi \circ \iota_E(a) \circ \hat{\varphi} \text{ for } a \in A,$$

where n is the degree of φ and $\hat{\varphi}$ is the dual isogeny of φ. Let R denote the preimage of $\mathrm{End}(E)$ under ι_E. R is an order in an imaginary quadratic field when E is ordinary, and a maximal order in a quaternion algebra when E is supersingular. Let I be a left ideal in R, we define

$$E[I] = \cap_{\alpha \in I} \ker(\alpha),$$

here we are implicitly identifying α with $\iota_E(\alpha) \in \mathrm{End}(E)$, and we will be making this identification repeatedly in the following discussions without explanation. This is a finite set, and this induces an isogeny $\varphi_I : E \to E_I$, where $E_I := E/E[I]$. The quotient elliptic curve E_I depends only on the R-module structure of I.

Proposition 3.2.1. *[98, Proposition 3.7] If I and J are isomorphic R-modules, then $E_I \cong E_J$.*

The converse implication of Proposition 3.2.1 is also true if we impose extra conditions on I.

Definition 3.2.6. Let I be a left ideal in R, I is a *kernel ideal* if $I = \{\rho \in R \mid \rho(E[I]) = 0\}$.

Theorem 3.2.7. *[98, Theorem 3.11] Let I and J be kernel ideals. Then $E_I \cong E_J$ if and only if*

I and J are isomorphic R-modules, if and only if $I = J\lambda$ for some invertible element $\lambda \in A$.

Naturally, the isogeny φ_I induces an isomorphism $\iota_{E_I} : A \to \mathrm{End}(E_I) \otimes \mathbb{Q}$. We are interested in how $\mathrm{End}(E_I)$ is related to $\mathrm{End}(E)$. The best way to see this is to compare the preimages $R = \iota_E^{-1}(\mathrm{End}(E))$ and $R_I := \iota_{E_I}^{-1}(\mathrm{End}(E_I))$ in A.

Proposition 3.2.2. *[98, Proposition 3.9] R_I contains the right order of I, and equals to it if and only if I is a kernel ideal.*

Ordinary case

Let us now consider the case when E/k is an ordinary elliptic curve. Things are easy in this case as R is commutative and a left ideal in R is always a two-sided ideal.

Theorem 3.2.8. *[98, Theorem 4.5] Let E/k be an ordinary elliptic curve and R is an imaginary quadratic order that is isomorphic to $\mathrm{End}(E)$. Then every ideal $I \subseteq R$ is a kernel ideal. Moreover, quotienting by ideals $I \subseteq R$ induces a free and transitive action of $\mathcal{C}\ell(R)$ on the set of isomorphism classes of ordinary curves over k with endomorphism ring isomorphic to R.*

Supersingular case

We consider now the case when E/k is a supersingular elliptic curve. Recall that A is a quaternion algebra and R is a maximal order. For the interest of Chapter 5, we will discuss left ideals $I \subseteq R$ that arise in a particular way.

Let $K \subseteq A$ be an imaginary quadratic field, $\mathcal{O} \subseteq K$ be an imaginary quadratic order such that $K \cap R = \mathcal{O}$. Let $\mathfrak{a}$ be an invertible $\mathcal{O}$-ideal. We define an left ideal I to be $R\mathfrak{a}$.

Lemma 3.2.4. *[98, Theorem 3.15] $I = R\mathfrak{a}$ is a kernel ideal.*

Lemma 3.2.5. $R_I = \mathfrak{a}^{-1}R\mathfrak{a} \subseteq A$.

Proof. According to Proposition 3.2.2, R_I equals to the right order of I.

$$\mathcal{O}_r(I) := \{x \in A \mid Ix \subseteq I\} = \{x \in A \mid R\mathfrak{a}x \subseteq R\mathfrak{a}\} = \mathfrak{a}^{-1}R\mathfrak{a}.$$

□

3.2.4 Reduction of CM elliptic curves

Let $\mathcal{O}$ be an order in an imaginary quadratic field K. In this section, we will investigate the relation between elliptic curves in characteristic 0 and characteristic p via reduction. We will pay special attention to the relation between endomorphism rings.

Theorem 3.2.9. *[56, Section 13.4, Theorem 12] Let E be an elliptic curve over a number field L with complex multiplication by $\mathcal{O}$. Let $\mathfrak{p}$ be a prime in L over p such that E has good reduction modulo $\mathfrak{p}$, and we denote the reduction by $\bar{E}$. The curve $\bar{E}$ is supersingular if and only if p does not split in K. Suppose that p splits completely in k. Let c be the conductor of $\mathcal{O}$, and write $c = p^r c_0$ where $p \nmid c_0$. Then:*

(a) $\mathrm{End}(\bar{E}) = \mathbb{Z} + c_0\mathcal{O}_K$ *is the order in K with conductor c_0.*

(b) If $p \nmid c$, then the map $\varphi \mapsto \bar{\varphi}$ is an isomorphism of $\mathrm{End}(E)$ *onto* $\mathrm{End}(\bar{E})$.

The following is a simple generalization of the result in 3.2.9 to the case when the reduction $\bar{E}$ is supersingular. We will need this for Chapter 5. Let us fix an isomorphism $\iota : K \to \mathrm{End}^0(E)$, the reduction induces an injective map from K to $\mathrm{End}^0(\bar{E})$. In the following theorem, we will identify elements in K with their images in $\mathrm{End}^0(\bar{E})$.

Theorem 3.2.10. *Let us continue with the setting in 3.2.9 and instead assume that p does not split in K. Then*

$$\mathrm{End}(E) \cap K = \mathbb{Z} + c_0\mathcal{O}_K.$$

We end this section with an important theorem of Deuring.

Theorem 3.2.11. *(Deuring's lifting theorem) Let E_0 be an elliptic curve over a finite field k of characteristic p, and let φ_0 be an endomorphism that is nontrivial. Then there exists an elliptic curve E defined over a number field, an endomorphism φ, and a prime $\mathfrak{p}$ over p where E has good reduction, such that E_0 is isomorphic to $\bar{E}$ and φ_0 corresponds to $\bar{\varphi}$ under the isomorphism.*

3.3 Isogeny graph

Let p be a prime and k be a finite field with cardinality equals to $q = p^n$ for some $n \geq 1$. Let ℓ be a prime that's different from p. In this section, we will consider the ℓ-isogeny graph $\mathcal{G}_\ell(k)$ of elliptic curves defined over k.

Precisely, we are interested in elliptic curves defined over k up to $\bar{k}$-isomorphism, therefore we will use j-invariants of elliptic curves as vertices of the ℓ-isogeny graph. The pair (j, j') is an edge if j' is a root of the modular polynomial $\Phi_\ell(j, x)$. The multiplicity of an edge is determined by the multiplicity of j' as a root of $\Phi_\ell(j, x)$. The ℓ-isogeny graph $\mathcal{G}_\ell(k)$ a directed graph. The existence of the dual isogeny ensures that if (j, j') an edge in $\mathcal{G}_\ell(k)$ then so is (j', j). If j, $j' \neq 0$, 1728, then (j, j') and (j', j) have the same multiplicity.

This graph $\mathcal{G}_\ell(k)$ will not be connected, there is no isogeny between an ordinary curve and a supersingular one. In what follows, we will consider two subgraphs, the ordinary subgraph $\mathcal{O}_\ell(k)$ and the supersingular one $\mathcal{S}_\ell(k)$. We will look at their properties and the structure of their connected components. In fact, we will see that the supersingular subgraph $\mathcal{S}_\ell(k)$ is connected.

3.3.1 Ordinary case

In order to explain the structure of the connected components of the ordinary ℓ-isogeny graph $\mathcal{O}_\ell(k)$, let us first introduce the definition of a certain type of graph – volcanoes.

Definition 3.3.1. An *ℓ-volcano V of depth d* is a connected undirected graph whose vertices are partitioned into one or more levels $V_0, \ldots, V_d$ such that the following hold:

(i) The subgroup on V_0 (the *surface*) is a regular graph of degree at most 2.

(ii) For $i > 0$, each vertex in V_i has exactly one neighbor in the level V_{i-1} and this accounts for every edge not on the surface.

(iii) For $i < d$, each vertex in V_i has degree $\ell + 1$.

It turns out that the connected components of ordinary ℓ-isogeny graph has volcano structure, and one level V_i corresponds to a fixed imaginary quadratic order $\mathcal{O}_i$ for $i = 0, \ldots, d$. We

also call the 0-th level the rim of the volcano. Note that there are several possibilities for the rim: a singleton with up to 2 self loops, two vertices connected by one or two edges, and three or more vertices that form a simple cycle.

Definition 3.3.2. Let $\varphi : E \to E'$ be an isogeny of degree ℓ and let $\mathcal{O}$, $\mathcal{O}' \subseteq K$ be two orders such that $\mathrm{End}(E) \cong \mathcal{O}$, $\mathrm{End}(E') \cong \mathcal{O}'$. One of the following holds:

(a) $\mathcal{O} \subseteq \mathcal{O}'$, and we say that φ is *ascending*;

(b) $\mathcal{O} = \mathcal{O}'$, and we say that φ is *horizontal*;

(c) $\mathcal{O} \supseteq \mathcal{O}'$, and we say that φ is *descending*.

Recall that E has $\ell+1$ ℓ-isogenies, the following proposition counts the number of ℓ-isogenies that are ascending, horizontal and descending respectively.

Proposition 3.3.1. *[55, Proposition 23] Let K be an imaginary quadratic field with discriminant D and $\mathcal{O} \subseteq K$ be an order. Let E/k be an ordinary elliptic curve such that $\mathrm{End}(E) \cong \mathcal{O}$. We use $\left(\frac{D}{\ell}\right)$ to denote the Legendre symbol. If ℓ does not divide the conductor of $\mathcal{O}$, E has no ascending ℓ-isogeny, $\left(\frac{D}{\ell}\right)+1$ horizontal ℓ-isogenies, and $\ell-\left(\frac{D}{\ell}\right)$ descending ℓ-isogenies. If ℓ divides the conductor of $\mathcal{O}$, E has exactly one ascending ℓ-isogeny, no horizontal ℓ-isogeny, and ℓ descending ℓ-isogenies. Furthermore, every codomain of a descending ℓ-isogeny has exactly $[\mathcal{O}^\times : (\mathbb{Z} + \ell\mathcal{O})^\times]$ ℓ-isogenies from E.*

The following proposition gives information about the size, and the depth of the ℓ-isogeny volcano.

Theorem 3.3.3. *[55, Proposition 23] Let V be an component of $\mathcal{O}_\ell(k)$, then V is an ℓ-volcano for which the following hold:*

(a) The vertices in level V_i all have the same endomorphism ring $\mathcal{O}_i$. $\ell \nmid [\mathcal{O}_K : \mathcal{O}_0]$ and $[\mathcal{O}_i : \mathcal{O}_{i+1}] = \ell$ for $0 \le i < d$.

(b) If $\left(\frac{D_0}{\ell}\right) \ge 0$, then $\mid V_0 \mid$ is the order of $[\mathfrak{l}]$ in $\mathcal{C}\ell(\mathcal{O})$; otherwise $\mid V_0 \mid = 1$.

(c) The depth of V is $d = \nu_\ell((t^2 - 4q)/D_0)/2$, where $t^2 = (\mathrm{tr}\,\pi_q)^2$ for $E \in V$.

Remark 3.3.4. In the definition of $\mathcal{O}_\ell(k)$, two elliptic curves E, E' over k are connected by an edge when there is an ℓ-isogeny φ defined over $\bar{k}$ between them. In fact, we can show that the isogeny φ is always defined over k (assuming $j(E) \neq 0$, 1728). Consider the action of Frobenius on φ, which gives rise to another ℓ-isogeny $\varphi^{(p)} : E \to E'$. However, there is only one unique ℓ-isogeny between E and E' according to Proposition 3.3.1, therefore, $\varphi = \varphi^{(p)}$ and we can conclude that φ is defined over k.

Remark 3.3.5. The vertices in $\mathcal{O}_\ell(k)$ are $\bar{k}$-isomorphism classes of ordinary elliptic curves defined over k, and one $\bar{k}$-isomorphism class corresponds to two k-isomorphism classes — two representatives E, E' over k are the quadratic twists of each other. Combining this with Remark 3.3.4, we see that the ordinary elliptic curves in one ordinary ℓ-isogeny volcano belong to two isogeny classes, with trace being t, $-t$ respectively. However, two ordinary curves being in the same isogeny class does not imply that they are in the same ℓ-isogeny class.

Example 3.3.6. Let $p = 3571$ and $\ell = 3$. The components of the graph $\mathcal{O}_3(\mathbb{F}_p)$ lie in 119 different isogeny classes, note that we are identifying the isogeny classes corresponds to t and $-t$ ($t \neq 0$) for the reasons explained in Remark 3.3.5. Let us consider the isogeny class for $t = 25$. We then have $4p = t^2 - f^2 D$ where $f^2 D$ will be the discriminant of the order $\mathbb{Z}[\pi_p]$. This equation gives that $f = 3$ and $D = -1451$. This isogeny class consists of one type of 3-volcano of depth 1 where the 0-th level corresponds to $\mathcal{O}_0 = \mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{-1451}}{2}]$ and the 1st level corresponds to $\mathcal{O}_1 = \mathbb{Z}[\sqrt{-1451}]$. Moreover, there is only one such 3-volcano as $\#\mathcal{C}\ell(K)$ equals to the order of $[\mathfrak{l}]$ in the class group where $\mathfrak{l}$ is one of the prime ideals sitting above 3.

3.3.2 Supersingular case

Recall that the j-invariants of supersingular elliptic curves are all in $\mathbb{F}_{p^2}$, we will consider the supersingular ℓ-isogeny graph $\mathcal{S}_\ell(\mathbb{F}_{p^2})$. This is a regular graph of degree $\ell + 1$, precisely, every vertex has out-degree $\ell + 1$ and vertices not adjacent or equal to 0 or 1728 have in-degree $\ell + 1$ as well.

Theorem 3.3.7. *[55, Corollary 78] The supersingular ℓ-isogeny graph $\mathcal{S}_\ell(\mathbb{F}_{p^2})$ is connected.*

$\mathbb{F}_p$-supersingular ℓ-isogeny graph Now we focus on supersingular elliptic curves defined over $k = \mathbb{F}_p$. Different from the definition of $\mathcal{S}_\ell(\mathbb{F}_{p^2})$, we will consider $\mathbb{F}_p$-isomorphism classes instead of $\overline{\mathbb{F}}_p$-isomorphism classes, and we will consider isogenies defined over $\mathbb{F}_p$ instead of over $\overline{\mathbb{F}}_p$. We will denote this $\mathbb{F}_p$-supersingular ℓ isogeny graph by $\mathcal{S}_{p,\ell}$. We emphasis here that the graph $\mathcal{S}_{p,\ell}$ is not a subgraph of $\mathcal{S}_\ell(\mathbb{F}_{p^2})$ as two elliptic curves being isomorphic over $\overline{\mathbb{F}}_p$ does not imply that they are isomorphic over $\mathbb{F}_p$. Since we require both the curve and the isogeny to be defined over $\mathbb{F}_p$, this graph $\mathcal{S}_{p,\ell}$ is no longer connected. In [36], Delfs and Galbraith described a volcano structure for $\mathcal{S}_{p,\ell}$ as follows.

Theorem 3.3.8. *Let $p > 3$ be a prime.*

(a) $p \equiv 1 \pmod 4$: There are $h(-4p)$ $\mathbb{F}_p$-isomorphism classes of supersingular elliptic curves over $\mathbb{F}_p$, all having the same endomorphism ring $\mathbb{Z}[\sqrt{-p}]$. From every one there is one outgoing $\mathbb{F}_p$-rational horizontal 2-isogeny as well as two horizontal ℓ-isogenies for every prime $\ell > 2$ with $\left(\frac{-p}{\ell}\right) = 1$.

(b) $p \equiv 3 \pmod 4$: There are two levels in the supersingular isogeny graph. From each vertex there are two horizontal ℓ-isogenies for every prime $\ell > 2$ with $\left(\frac{-p}{\ell}\right) = 1$.

(i) If $p \equiv 7 \pmod 8$, on each level $h(-p)$ vertices are situated. Surface and floor are connected $1:1$ with 2-isogenies and on the surface we also have two horizontal 2-isogenies from each vertex.

(ii) If $p \equiv 3 \pmod 8$: we have $h(-p)$ vertices on the surface and $3h(-p)$ on the floor. Surface and floor are connected $1:3$ with 2-isogenies, and there are no horizontal 2-isogenies.

Chapter 4

Orienteering with one endomorphism

4.1 Introduction

The security of isogeny-based cryptosystems depends upon a constellation of hard problems. Central are the path-finding problem (to find a path between two specified elliptic curves in a supersingular ℓ-isogeny graph), and the endomorphism ring problem (to compute the endomorphism ring of a supersingular elliptic curve). Only exponential algorithms are known for general path-finding, in the absence of information beyond the j-invariants. However, if the endomorphism rings are known, the KLPT algorithm allows for polynomial-time pathfinding [54]. In fact, it is known that the pathfinding and endomorphism ring problems are equivalent [38, 100].

A natural question to ask is whether knowledge of a single explicit endomorphism (which generates only a rank 2 subring of the rank 4 endomorphism ring) can be used for path-finding. Answering this question is the goal of this chapter: we give explicit algorithms transforming knowledge of one endomorphism into a way-finding tool that can detect ascending, descending and horizontal directions with regards to the corresponding orientation, and use this to walk to $j = 1728$.

The question of the security of one endomorphism has recently been 'in the air,' for example, with the uber isogeny assumption of [33]. Knowledge of a small explicit endomorphism is known to be a weakness [63]. As this work was being completed, a related study was also made available [99]; see Section 4.1.3 for a comparison with this paper.

By *explicit endomorphism*, we mean one given in some form in which its action on the curve is computable, and its minimal polynomial is known (but note that, given an endomorphism, both its norm and trace are in many cases computable; see Section 4.2.2). For example, such an endomorphism may be given as a rational map, or a composition chain of rational maps, and these are the two cases we focus on in this chapter. The data of such an endomorphism is equivalent to the data of an *orientation* of the supersingular elliptic curve, namely a map $\iota : K \to \mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}(E)$, where K is the imaginary quadratic field generated by a root of the minimal polynomial of the endomorphism.

The study of orientations provides some structure to the supersingular isogeny graph, which has recently been exploited [27, 72]. In particular, the ℓ-isogeny graph of *oriented* supersingular elliptic curves over $\overline{\mathbb{F}}_p$ has a volcano structure familiar from the ordinary case. This graph maps onto the supersingular ℓ-isogeny graph over $\overline{\mathbb{F}}_p$. Our approach is to use the orientation provided by a given explicit endomorphism to discern ascending, descending and horizontal directions with regards to the volcano. This provides a sort of tool for 'orienteering.'

The core result of our work is an algorithm that finds an ℓ-isogeny path from a given supersingular elliptic curve E to an initial curve E_{init}, given a single explicit endomorphism of E. We take E_{init} to be the curve with j-invariant $j = 1728$, but other choices are possible (see Section 4.6.3). The overall plan is as follows. First, climb the oriented volcano from E, oriented by the given endormorphism, to the volcano rim (using the given endomorphism as our 'orienteering tool'). Then, by orienting the curve $j = 1728$ with the same field, we can climb to the rim from there also. Finally, we attempt to meet by circling the rim.

This approach is limited by our ability to traverse a potentially large segment of the rim, or to hit the same rim in a large cordillera of volcanoes, whose size is generally equal to the class number of the corresponding quadratic order. If we simply walk the rim, then, classically, the runtime depends linearly on this class number, which can be expected to be exponential in $\log p$. We show that a large endomorphism which nevertheless walks us to a rim of small class number introduces a vulnerability to isogeny based cryptosystems.

4.1.1 Main theorem

We rely on a number of heuristic assumptions: (i) The Generalized Riemann Hypothesis (hereafter referred to as GRH). (ii) Powersmoothness in a quadratic sequence or form is as for random integers (a powersmooth analogue of the heuristic assumption underlying the quadratic sieve; see Heuristics 4.5.7. (iii) The orientations of a fixed j-invariant are distributed reasonably across all suitable volcanoes (Heuristic 4.3.3). (iv) This distribution is independent of a certain integer factorization (Heuristic 4.6.5). (v) The aforementioned integer factorization is prime with the same probability as a random integer (Heuristic 4.6.3; this heuristic is similar to those used in [35] and [54]).

We state our main results, whose proofs can be found in Section 4.9.1. We use the notation $L_x(y) = \exp(O((\log x)^y(\log\log x)^{1-y}))$. The following theorem gives a classical algorithm for ℓ-isogeny pathfinding that is subexponential in $\log p$ times a certain class number, for a wide range of input endomorphisms.

Theorem 4.1.1. *Choose a small prime ℓ and assume the heuristic assumptions*[1] *given above. Let $\theta \in \mathrm{End}(E)$ be an endomorphism of degree d, such that that $L_d(1/2) \geq \mathrm{poly}(\log p)$. Suppose θ can be evaluated on points $P \in E(\mathbb{F}_{p^k})$ in time $T_\theta(k,p)$. Let Δ' be the ℓ-fundamental part of the discriminant Δ of θ (obtained*[2] *by removing the largest even power of ℓ), and assume that $|\Delta'| \leq p^2$. Let $h_{\Delta'}$ be the class number of the quadratic order of discriminant Δ'. Then there is a classical algorithm that finds an ℓ-isogeny path of length $O(\log p + h_{\Delta'})$ from E to the curve E_{init} of j-invariant $j = 1728$ in runtime $T_\theta(L_d(1/2),p) + h_{\Delta'}L_d(1/2)$.*

Note that the runtime depends on the class number $h_{\Delta'}$ which can be significantly smaller than h_Δ. This allows for $\mathrm{poly}(\log p)$ time algorithms for some large endomorphisms, which we discuss in a moment.

Note also that the point evaluation condition on θ is for generality. Any θ which is represented in terms of rational maps has $T_\theta(k,p) = \mathrm{poly}(d,k,\log p)$, hence the final runtime would be $h_{\Delta'}\,\mathrm{poly}(d\log p)$. But θ could be represented as a composition chain of isogenies in such a way that $T_\theta(k,p)$ is subexponential in d, leading to a runtime of $h_{\Delta'}L_d(1/2)\,\mathrm{poly}(\log p)$.

[1] See Proposition 4.8.1 for the exact subset of heuristics needed.
[2] Except when $\ell = 2$, if $\Delta = 2^{2k}\Delta''$ where $4 \nmid \Delta''$ and $\Delta'' \equiv 2, 3 \pmod 4$, then we set $\Delta' := 4\Delta''$.

Furthermore, we have a polynomial-time algorithm if the endomorphism has small degree, or even just small discriminant (Theorem 4.9.1); the cryptographic weakness caused by such endomorphisms is already known by other methods [63]. There are also some large endomorphisms which are insecure, in the sense that they admit polynomial-time algorithms if they can be evaluated in polynomial time. Specifically, modifications of the algorithm lead to special cases:

1. If ℓ is inert in the field associated to Δ, the runtime improves for endomorphisms in suitable form to $L_d(1/2) + h_{\Delta'} \operatorname{poly}(\log p)$, and the path-length is improved to $O(\log p)$ (Proposition 4.8.1).

2. If, in addition to the above, $\Delta' = \Delta$, then the runtime improves further to $h_{\Delta'} \operatorname{poly}(\log p)$ (Proposition 4.8.1).

3. If the norm of the endomorphism has $B(p)$-powersmooth factorization and its discriminant is coprime to ℓ, then the runtime improves to $h_{\Delta'} \operatorname{poly}(B(p) \log p)$ (Theorem 4.9.4).

4. If the input endomorphism is of size $\operatorname{poly}(\log p)$ (in trace, norm and discriminant), then the runtime improves to $\operatorname{poly}(\log p)$ (Theorem 4.9.1) (these endomorphisms were already known to present a security risk [63]).

5. If norm and discriminant have suitable factorizations, then the runtime can improve to $\operatorname{poly}(\log p)$ even for non-small endomorphisms (Theorem 4.9.2). This shows that **there are large insecure endomorphisms** (Corollary 4.9.3) (to our knowledge, this is the first time this has been demonstrated, although it is possible to deduce this using similar methods from [99]; see Section 4.1.3).

A corollary to Theorem 4.1.1 is that these insecure large endomorphisms exist for every supersingular curve. We state an informal version here.

Corollary 4.1.2 (Corollary 4.9.3)**.** *Under the same heuristic assumptions as before, every supersingular curve admits an endomorphism which can be revealed in polynomial space in a form that allows for polynomial-time evaluation, and gives rise to a classical algorithm to walk to* E_{init} *in* $\operatorname{poly}(\log p)$ *time.*

The classical algorithm of Theorem 4.1.1 first transforms the input endomorphism to a powersmooth isogeny chain, which to our knowledge is the most efficient type of representation. However, we have endeavoured to write our component algorithms to handle an abstract notion of an input endomorphism offering certain functionalities (Section 4.5.1), in anticipation of their potential application to different types of endomorphism representations.

4.1.2 Other algorithms presented

Some of the explicit building blocks of the results above may have independent applications. In particular, we provide algorithms for the following tasks, among others:

1. Section 4.4 provides methods for detecting ascending, descending and horizontal directions in general.

2. Section 4.5.3 presents a technique for obtaining a prime-power powersmooth isogeny chain endomorphism from the same quadratic order as a given endomorphism (Algorithm 4.5.3).

3. Section 4.6 discusses an algorithm which computes an orientation on the elliptic curve of j-invariant 1728 (or other suitable curves; see Section 4.6.3) by an ℓ-power multiple of a given discriminant (Algorithm 4.6.1). In other words, given a quadratic order $\mathcal{O}$, it finds $j = 1728$ somewhere in the cordillera of an order containing $\mathcal{O}$. In fact, it finds arbitrarily many such orientations, moving gradually further 'down' the volcanoes. This algorithm runs in heuristic polynomial time when the discriminant is coprime to p and less than p^2 in absolute value.

4. Section 4.7.2 concerns a method for computing the class group action of $\mathrm{Cl}(\mathcal{O})$ on $\mathrm{SS}_{\mathcal{O}}$, the set of curves primitively oriented by $\mathcal{O}$. In fact, we demonstrate how to navigate $\mathrm{SS}_{\mathcal{O}}$ using the class group action of $\mathrm{Cl}(\mathcal{O}')$ for any $\mathcal{O}' \subseteq \mathcal{O}$.

5. Section 4.10 contains an efficient algorithm for dividing an isogeny by $[\ell]$ (Algorithm 4.10.2), originally outlined by McMurdy, which is more efficient than naive algorithms for this task. We make McMurdy's approach explicit for arbitrary ℓ (he only made explicit the case $\ell = 2$, which is more straightforward.).

4.1.3 Comparison with [99]

The only other work that pertains to path-finding algorithms using an orientation is found in the excellent article [99], which covers a web of reductions between a wide variety of hard problems related to orientations, and appeared as this paper was nearing completion. That work is largely concerned with theoretical complexity reductions, although one can derive classical and quantum pathfinding algorithms from these reductions, for an abstract class of orientations (see item (4)). By contrast, in this article we focus on explicit algorithms, runtimes, and endomorphism representations, as well as numerical examples. However, it is possible to compare the region of overlap between the two articles, which is *runtimes for classical and quantum path-finding in the presence of one endomorphism*. To do so, there are several important points about the method of comparison:

1. The paper [99] actually provides reductions from the endomorphism ring problem, which is known to be polynomially equivalent to the path-finding problem. We will ignore this distinction.

2. The paper [99] solves the endomorphism ring problem by reducing it to the vectorization problem and solving that by the best known classical or quantum algorithms. Our algorithms can't strictly be interpreted as reductions to the vectorization problem. For example, in the classical Algorithm 4.8.1, we attempt to relate two oriented curves without knowing their common class group orbit (see Remark 4.8.1).

3. The paper [99] uses methods largely contained in the theory of quaternion algebras, overlapping very little with our methods.

4. The paper [99] applies to an abstract class of *efficiently representable endomorphisms*, and provides reductions which are polynomial in the length of the representation. The definition permits endomorphisms which are exponentially large. In our paper we discuss explicit representations and their concrete practical efficiency (Section 4.5), and our algorithm runtimes take the conversion of arbitrary endomorphisms into suitable representations into account. Therefore, in order to compare, we will assume that input endomorphisms are in powersmooth

prime-power isogeny chain form (see Section 4.5.3). To change into such a form can incur a subexponential runtime, depending on the form of the input endomorphism (Algorithm 4.5.3).

For the above reasons, we compare only runtime statements. Overall, the runtimes implied for pathfinding in the presence of an endomorphism are reassuringly similar between the two papers.

1. The paper [99] assumes the stronger hypothesis that the discriminant of the input endomorphism has a known factorization. We do not assume this. Although the reduction to vectorization in [99] requires a factorization, in practice vectorization is more difficult than factorization, so this does not affect the runtime comparison.

2. In contrast to our work, the work [99] is not heuristic beyond a dependence on GRH and the solution to the vectorization problem ([99, Proposition 4]). We plan to address some of our heuristics in a follow-up paper [4].

3. Comparing the classical algorithm of Theorem 4.1.1, namely Algorithm 4.8.1, with the algorithm implied by [99, Proposition 7, Section 3 Subsection 'Computing the action', Theorem 4], we obtain similar runtimes, with the following distinctions. Both algorithms depend polynomially on the size of the representation of the endomorphism. In the case that $\Delta = \Delta'$ (the endomorphism is already at the rim), both algorithms depend on the class number h_Δ; ours linearly, and [99] in square root. In the case that $\Delta \neq \Delta'$, both depend instead on the smaller class number $h_{\Delta'}$, but ours depends on the smoothness bound of the relative conductor, while that of [99] depends upon the powersmoothness bound of the relative conductor. (We ascend volcanoes, so that our relative conductors are typically ℓ-power, but one can also alternate choices of ℓ; see the proof of Theorem 10.2 for a discussion.)

4. Continuing the comparison of item (3), our classical algorithm directly produces a path whose length depends on the class number (since it traverses a volcano rim). A reduction to the vectorization problem as in the algorithm implied in [99] produces a path of $\mathrm{poly}(\log p)$ length, by solving the vectorization problem to find a smooth isogeny, and then, by an equivalence implied in [100], tranforming that into an ℓ-isogeny. See Remark 4.8.1.

5. For every curve, we show that certain large degree endomorphisms can be expressed in

poly$(\log p)$ space and admit a classical path-finding algorithm in poly$(\log p)$ time (Corollary 4.9.3). In fact, these same endomorphisms would be susceptible to the methods of [99], although this implication is not considered there.

6. Finally, [99, Proposition 6] describes a probabilistic polynomial-time algorithm for computing a primitive orientation of an elliptic curve by some quadratic order of discriminant Δ. However, that algorithm only applies to orders with $|\Delta| < 2\sqrt{p} - 1$ and relies on lattice reduction to find the smallest element in the order. Our method works for $|\Delta| < p^2$ and finds orientations further 'down the volcano,' but is presented for $j = 1728$ only (but generalizes to other initial curves with good endomorphism rings in the sense of Section 4.6.3).

4.1.4 Other contributions

We give careful runtime analyses for various tasks related to endomorphisms represented as rational functions or as composition chains of isogenies, including evaluation, translation, division-by-$[\ell]$, and Waterhouse twisting. Additionally, we provide a review and some modest extensions to the theory of orientations as described in [72]; see Section 4.3, in particular Section 4.3.3.

In a follow-up paper [4], we establish a theoretical bijection between volcano rims and cycles in the ℓ-isogeny graph, and address some of the aforementioned heuristics for oriented supersingular ℓ-isogeny graphs used in this chapter.

Throughout the chapter we demonstrate our algorithms with a running example first introduced in Example 4.3.2. The examples are given in more detail in SageMath [89] worksheets with accompanying PDF details, available on GitHub [5].

4.1.5 Outline

In Section 4.2, we set some notations and conventions and also state a few runtime lemmata. In Section 4.3, we introduce the main object of study, namely oriented ℓ-isogeny graphs and their properties, including some heuristic behaviour. In Section 4.4, the relationship between an endomorphism and an orientation is explained, and we also introduce a few new definitions that aid in navigating the oriented ℓ-isogeny graph. In Section 4.5, we discuss the representation

of endomorphisms, along with the basic functionalities for these representations required for later algorithms. We then compute orientations for the supersingular elliptic curve of j-invariant 1728 in Section 4.6. In Section 4.9, we discuss the proofs of our main theorem as well as some special cases. Lastly, we leave to Section 4.10 the technical explanation of McMurdy's division-by-ℓ algorithm and provide its runtime analysis. Throughout the chapter, to aid in reading, important assumptions will be rendered in **bold**.

4.2 Background

4.2.1 Notations and conventions

Throughout the chapter, let p **be a cryptographically sized prime** (upon which runtimes will depend), and let ℓ **be a small prime** (whose size will be assumed $O(1)$ for runtimes). In particular, $\ell \neq p$. We will assume **both** p **and** ℓ **are defined once throughout the chapter** (so, for example, they will not be repeated as an input to every algorithm).

Every elliptic curve considered in the chapter is to be assumed to be a **supersingular curve** over $\overline{\mathbb{F}}_p$. All such curves can be defined over $\mathbb{F}_{p^2}$. Every isogeny and endomorphism is assumed to have domains and codomains which are curves of this type. We use the notation $\mathrm{End}(E)$ for the endomorphism ring of the elliptic curve E over $\overline{\mathbb{F}}_p$, and $\mathrm{End}^0(E) := \mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}(E)$ for the endomorphism algebra of E. We use the notation O_E for the identity element of an elliptic curve E, and $j(E)$ for the j-invariant. We use the variables φ and ψ to denote isogenies, while θ is generally reserved for endomorphisms. The dual isogeny to an isogeny φ is denoted by $\widehat{\varphi}$. Let $E^{(p)}$ denote the curve obtained by the action of Frobenius on E (acting on the Weierstrass coefficients). Let $\pi_p : E \to E^{(p)}$ denote the Frobenius isogeny, given by $\pi_p(x, y) = (x^p, y^p)$. Note that Frobenius is an endomorphism if E is defined over $\mathbb{F}_p$. Frobenius also acts on any isogeny $\varphi : E \to E'$ (acting on its coefficients) to give $\varphi^{(p)} : E^{(p)} \to (E')^{(p)}$ of the same degree. Unless otherwise specified (such as Frobenius), **isogenies will be assumed to be separable** throughout the chapter (many of the algorithms herein would not apply to inseparable endomorphisms or isogenies).

There is only one fixed supersingular ℓ-isogeny graph under consideration at any time, which we denote simply by $\mathcal{G}$. Namely, this is the graph whose vertices are $\overline{\mathbb{F}}_p$-isomorphism classes of

supersingular elliptic curves (which we will often refer to simply by their j-invariants), and whose directed edges are ℓ-isogenies (when there are no extra automorphisms, we can identify dual pairs to create an undirected graph).

We consider imaginary quadratic fields $K = \mathbb{Q}(\sqrt{\Delta})$, where $\Delta < 0$ is a fundamental discriminant. Then the ring of integers has the form $\mathcal{O}_K = \mathbb{Z}[\omega]$, where

$$\omega = \begin{cases} \frac{1+\sqrt{\Delta}}{2} & \Delta \equiv 1 \pmod 4, \\ \frac{\sqrt{\Delta}}{2} & \Delta \equiv 0 \pmod 4. \end{cases}$$

Since we sometimes have multiple quadratic orders under consideration, we use the notation $(\alpha, \beta)_{\mathcal{O}}$ for the ideal generated by α and β in $\mathcal{O}$. The (possibly non-maximal) orders $\mathcal{O}$ of K are parametrized by a positive integer called the conductor. If $\mathcal{O}$ has conductor f, then $\mathcal{O} = \mathbb{Z}[f\omega]$. If $\ell \nmid f$, then we say that both $\mathcal{O}$ and its discriminant are *ℓ-fundamental*. Given a discriminant Δ, its *ℓ-fundamental part* is the unique ℓ-fundamental discriminant dividing Δ.

Write $B_{p,\infty}$ for the rational quaternion algebra ramified at p and ∞. **Every quadratic field K is assumed to embed in the quaternion algebra** $B_{p,\infty}$, i.e. to be an imaginary quadratic field in which p does not split [95, Proposition 14.6.7(v)]; the only exception is in the discussion of Heuristic 4.6.3. Every quadratic order $\mathcal{O}$ is assumed to generate such a field K, and to **have discriminant not divisible by** p. Every quadratic discriminant is assumed to be the discriminant of such a quadratic order $\mathcal{O}$, and we write $\Delta_{\mathcal{O}}$. We denote by $\mathcal{O}_K$ the maximal order of the quadratic field K and reserve Δ_K for the discriminant of $\mathcal{O}_K$.

Complex conjugation (which is also the action of $\mathrm{Gal}(K/\mathbb{Q})$) is denoted by an overline: $\alpha \mapsto \overline{\alpha}$. We use the notation $\mathrm{Cl}(\mathcal{O})$ and $h_{\mathcal{O}}$ for the class group and class number, respectively, of a quadratic order $\mathcal{O}$.

The reduced norm and trace of $B_{p,\infty}$ coincide with the norm and trace of an element when it is considered as a quadratic algebraic number; when we discuss norm and trace it is always this we refer to.

For runtime analyses we use big O notation, including soft $\widetilde{O}$ for absorbing log factors. The notation $\mathbf{M}(n)$ will indicate the runtime of field operations (addition, multiplication, inversion) in

a finite field of cardinality n; here, we note that $\mathbf{M}(n^k) = O(\mathbf{M}(n))$ when k is constant. In the later portions of the chapter we are mainly concerned with the distinction between polynomial, subexponential and exponential algorithms. We write runtime as $\text{poly}(x)$ if there exists a polynomial f so the runtime is $O(f(x))$. When we are concerned only with whether runtime is polynomial, we will suppress the notation $\mathbf{M}$, by assuming that $\mathbf{M}(n) = \text{poly}(\log n)$. For subexponential runtimes, we use notation $L_x(y) = \exp(O((\log x)^y (\log \log x)^{1-y}))$.

For general background on isogeny-based cryptography and supersingular isogeny graphs, we will assume the reader is familiar with a resource such as [38, Section 2] or [32].

4.2.2 Runtime lemmata

In this section, we recall some basic runtimes for isogenies and torsion points, etc. The first lemma is standard.

Lemma 4.2.1. *Given $P, Q \in E[N]$, and $0 \leq a, b < N$, computing $[a]P + [b]Q$ takes time $O((\log N)\boldsymbol{M}(p^{N^2}))$.*

Lemma 4.2.2 ([14, Corollary 2.5])**.** *Let $\varphi : E \to E'$ be an isogeny between two supersingular curves, both defined over $\mathbb{F}_{p^2}$. Then φ is defined over $\mathbb{F}_{p^{12}}$. If neither of $j(E)$ or $j(E')$ are 0 or 1728, then φ is defined over $\mathbb{F}_{p^4}$.*

Lemma 4.2.3. *Let t denote the smallest integer such that $E[N] \subseteq E(\mathbb{F}_{p^t})$. In particular, $t \leq N^2 - 1$. Finding a basis of $E[N]$ has runtime $\widetilde{O}(N^4(\log p)\boldsymbol{M}(p^{N^2}))$.*

Proof. This can be proven by adapting the second paragraph of the proof of Lemma 5 in [44]. In particular, the limiting runtime is the call to [97], which takes time $\widetilde{O}(N^4(\log p)\mathbf{M}(p^{N^2}))$. See also [14, Lemma 6.9]. □

Lemma 4.2.4. *Consider an isogeny $\varphi : E \to E'$ of degree d, and a point $P \in E(\mathbb{F}_{p^t})$, where $12 \mid t$. Then computing $\varphi(P)$ takes time $O(d\boldsymbol{M}(p^t))$. In particular, if $P \in E[N]$, then the time taken is $O(d\boldsymbol{M}(p^{\text{lcm}(12,N^2)}))$.*

Proof. Write φ as a rational map $\varphi(x, y) = (\varphi_1(x), \varphi_2(x)y)$; here the denominators and numerators of $\varphi_1(x)$ and $\varphi_2(x)$ are polynomials in x of degree at most $3d$. By Lemma 4.2.2, we can assume

that their coefficients are in $\mathbb{F}_{p^{12}} \subseteq \mathbb{F}_{p^t}$. To compute $\varphi(P)$, we apply Horner's algorithm [53, p. 467], which requires $O(d)$ operations in the field. Assume that P is an N-torsion point on E. Then t can be chosen such that $t \leq \mathrm{lcm}(t, N^2)$ by Lemma 4.2.3. □

In the case that $\varphi = [n]$ for some integer n, it is more efficient to use a standard a double-and-add approach, which will also take polynomial time in the degree.

Lemma 4.2.5 ([93], [81, Theorem 3.5], [48, Section 5.1]). *Vélu's formulas for an isogeny of degree d compute the isogeny in time $\widetilde{O}(d\boldsymbol{M}(p^{d^2}))$.*

By Lemma 4.2.2, the isogeny created has coefficients in the field $\mathbb{F}_{p^{12}}$.

Lemma 4.2.6. *Let $\varphi : E \to E'$ and $\psi : E' \to E''$ be isognies represented as rational maps, of respective degrees d and d', where E, E', E'', φ and ψ are defined over some finite field $\mathbb{F}$. Then computing the composition $\psi \circ \varphi : E \to E''$ as a rational map takes time $\widetilde{O}(dd'\boldsymbol{M}(\#\mathbb{F}))$.*

Proof. As usual, write $\varphi = \left(\frac{u(x)}{v(x)}, \frac{s(x)}{t(x)}y\right)$ where $u(x), v(x), s(x), t(x) \in \mathbb{F}[x]$ are polynomials of degree $O(d)$ with $\gcd(u, v) = \gcd(s, t) = 1$. Similarly, write $\psi = \left(\frac{u'(x)}{v'(x)}, \frac{s'(x)}{t'(x)}y\right)$ with analogous conditions on $u'(x)$, $v'(x)$, $s'(x)$, $t'(x) \in \mathbb{F}[x]$. Then

$$\psi \circ \varphi = \left(\frac{u'(\frac{u(x)}{v(x)})}{v'(\frac{u(x)}{v(x)})}, \frac{s'(\frac{u(x)}{v(x)})}{t'(\frac{u(x)}{v(x)})} \frac{s(x)}{t(x)} y \right) .$$

Obtaining $\psi \circ \varphi$ requires computing four compositions of the form $f(\frac{u(x)}{v(x)})$ where $f \in \{u', v', s', t'\}$ has degree $O(d')$. Writing $f(x) = \sum_{i=0}^{n} f_i x^i$ with $n = O(d')$, we have

$$f\left(\frac{u(x)}{v(x)}\right) = \frac{F(u(x), v(x))}{v(x)^n} \quad \text{where} \quad F(x, y) = \sum_{i=0}^{n} f_i x^i y^{n-i} .$$

The computation of $F(u(x), v(x))$ is dominated by computing the powers of $u(x)$ and $v(x)$ which can be accomplished in time $\widetilde{O}(dd'\mathbf{M}(\#\mathbb{F}))$ using fast polynomial multiplication [46]. An alternative way to compute $F(u(x), v(x))$ that is slightly faster but has asymptotically the same runtime is via the Horner-like recursion

$$F_n(x) = f_n , \qquad F_{i-1}(x) = f_{i-1} v(x)^{n-i+1} + F_i(x) u(x) \quad (n \geq i \geq 1) ,$$

where it is easy to see that $F_0(x) = F(u(x), v(x))$. □

Lemma 4.2.7. *Let E be an elliptic curve defined over some finite field $\mathbb{F}$, $\theta \in \mathrm{End}(E)$ an endomorphism represented as a rational map, and N an integer. Then computing the endomorphism $\theta + [N] \in \mathrm{End}(E)$ as a rational map takes time $\widetilde{O}(\max\{\deg\theta, N^2\}\boldsymbol{M}(\#\mathbb{F}))$.*

Proof. By [83, Exercise 3.7, pp. 105f.], we have

$$[N](x,y) = \left(\frac{\phi_N(x)}{\psi_N(x)^2}, \frac{\omega_N(x,y)}{\psi_N(x,y)^3}\right) ,$$

where $\phi_N = x\psi_N^2 - \psi_{N+1}\psi_{N-1}$, $\omega_n = (\psi_{N+2}\psi_{N-1}^2 - \psi_{N-2}\psi_{N+1}^2)/4y$ and ψ_n is the n-th division polynomial on E. The required division polynomials have degree $O(N^2)$ and can be computed in $O(\log(N))$ steps using the recursive formulas

$$\psi_{2n+1} = \psi_{n+2}\psi_n^3 - \psi_{n-1}\psi_{n+1}^3 , \quad \psi_{2n} = \frac{1}{2y}\psi_n(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2) .$$

Using the point addition formulas on E and fast polynomial multiplication techniques [46], the rational map $\theta + [N]$ can be computed using $\widetilde{O}(\max\{\deg\theta, N^2\})$ operations in $\mathbb{F}$. □

Throughout the chapter, we will assume that **all endomorphisms are provided with a trace and norm** (which is the same as degree) that carries through computations; see Section 4.5.1. If the trace is not provided, then it can be computed using [99, Lemma 1], [38, Lemma 4], [14, Theorem 3.6].

4.3 Oriented isogeny graphs

In this section, we recall and strengthen basic results about oriented isogeny graphs, mainly based on work of Colò-Kohel [27] and Onuki [72], and provide some minor new extensions of the general theory.

4.3.1 Orientations

Fixing a curve E, we have $\mathrm{End}^0(E) \cong B_{p,\infty}$. The field K embeds into $B_{p,\infty}$ if and only if p does not split in K. There may be many distinct such embeddings. We define a *K-orientation* of an elliptic curve to be an embedding $\iota : K \to \mathrm{End}^0(E)$. If $\mathcal{O}$ is an order of K, then an *$\mathcal{O}$-orientation* is a K-orientation such that $\iota(\mathcal{O}) \subseteq \mathrm{End}(E)$. We say that a K-orientation ι is a *primitive* $\mathcal{O}$-orientation if $\iota(\mathcal{O}) = \mathrm{End}(E) \cap \iota(K)$. It will often be expedient to have a local notion of primitivity: for a prime ℓ, we say that a K-orientation ι is an ℓ-primitive $\mathcal{O}$-orientation if it is an $\mathcal{O}$-orientation and the index $[\mathrm{End}(E) \cap \iota(K) : \iota(\mathcal{O})]$ is coprime to ℓ. In particular, a primitive $\mathcal{O}$-orientation is exactly one which is ℓ-primitive for all primes ℓ.

If $\varphi : E \to E'$ is an isogeny of degree ℓ, where ι is a K-orientation of E, then there is an induced K-orientation $\iota' = \varphi_*(\iota)$ on E' defined $\varphi_*(\iota)(\omega) := \frac{1}{\ell}\varphi \circ \iota(\omega) \circ \widehat{\varphi} \in \mathrm{End}^0(E')$ for any $\alpha \in K$.

4.3.2 Oriented isogeny graphs

A *K-oriented elliptic curve* is a pair (E, ι) where $\iota : K \to \mathrm{End}^0(E)$ is a K-orientation. An isogeny of K-oriented elliptic curves $\varphi : (E, \iota) \to (E', \iota')$ is an isogeny $\varphi : E \to E'$ such that $\iota' = \varphi_*(\iota)$; we call this a K-oriented isogeny and write $\varphi \cdot (E, \iota) = (\varphi(E), \varphi_*(\iota))$. One verifies directly that $\varphi_2 \cdot \varphi_1 \cdot (E, \iota) = (\varphi_2 \circ \varphi_1) \cdot (E, \iota)$. A K-oriented isogeny is a *K-isomorphism* if it is an isomorphism of the underlying curves.

Fixing a quadratic field K, we define the graph $\mathcal{G}_K$ of K-oriented supersingular curves over $\overline{\mathbb{F}}_p$. This is the graph whose vertices are K-isomorphism classes of pairs (E, ι) and which has an edge connecting (E, ι) and (E', ι') for each K-oriented isogeny (defined over $\overline{\mathbb{F}}_p$) of degree ℓ between these oriented curves. If $\varphi : (E, \iota) \to (E', \iota')$ is a K-oriented isogeny, then $\widehat{\varphi} : (E', \iota') \to (E, \iota)$ is also one (since $\widehat{\varphi}_*(\iota') = \widehat{\varphi}_*(\varphi_*(\iota)) = [\ell]_*(\iota) = \iota$). Therefore the edges may be taken to be undirected by pairing isogenies with their duals, when the vertices involved are not $j = 0$ or 1728. Also, isogenies are taken up to equivalence, meaning we quotient by the same isomorphisms as for the vertices; see [72, Definition 4.1]. The graph has (out-)degree $\ell + 1$ at every vertex. (Note that our graph differs slightly from the definition in [72, Section 4], where only the images of curves over a number field with complex multiplication are included; we discuss this distinction in the next section.)

Every K-orientation is a primitive $\mathcal{O}$-orientation for a unique order $\mathcal{O} := \iota(K) \cap \mathrm{End}(E)$. Therefore, the set of vertices of $\mathcal{G}_K$ is stratified by the order $\mathcal{O}$ by which a vertex is primitively oriented.

Definition 4.3.1. Let $\mathrm{SS}_{\mathcal{O}}$ denote the set of isomorphism classes of K-oriented curves for which the orientation is a primitive $\mathcal{O}$-orientation.

This is a simplification of the notation $\mathrm{SS}^{pr}_{\mathcal{O}}(p)$ found in the literature [72, Section 3] [27, Section 3]. This set is non-empty if and only if p is not split in K and does not divide the conductor of $\mathcal{O}$ [72, Proposition 3.2]. As mentioned in Section 4.2.1, we make those assumptions throughout the chapter.

Let $\varphi : (E, \iota) \to (E', \iota')$ be a K-oriented ℓ-isogeny. Suppose that ι is a primitive $\mathcal{O}$-orientation and ι' is a primitive $\mathcal{O}'$-orientation. There are exactly three possible cases:

1. $\mathcal{O} = \mathcal{O}'$, in which case we say φ is *horizontal*,
2. $\mathcal{O} \supsetneq \mathcal{O}'$, in which case $[\mathcal{O} : \mathcal{O}'] = \ell$ and we say φ is *descending*,
3. $\mathcal{O} \subsetneq \mathcal{O}'$, in which case $[\mathcal{O}' : \mathcal{O}] = \ell$ and we say φ is *ascending*.

Example 4.3.2 (Introducing our running example). To illustrate the algorithms in this chapter, we consider supersingular elliptic curves defined over $\overline{\mathbb{F}}_p$ for $p = 179$. As $p \equiv 3 \pmod 4$, the curve $E : y^2 = x^3 - x$ with $j(E) = 1728$ is supersingular. This curve is well-known to have extra automorphisms, and its endomorphism ring is generated by the endomorphisms $[1], [i], \frac{[1]+\pi_p}{2}, \frac{[i]+[i]\circ\pi_p}{2}$, where $[i](x, y) := (-x, iy)$ and π_p is as defined in Section 4.2.1. We define $K := \mathbb{Q}(\sqrt{-47})$ with $\Delta = -47$ and $\omega = \frac{1+\sqrt{-47}}{2}$. We consider the oriented 2-isogeny graph of supersingular elliptic curves with respect to this imaginary quadratic field K.

4.3.3 Frobenius and class group actions

In this section, we slightly strengthen results of Onuki [72] to give an action on oriented isogenies by a direct product of the class group with Frobenius.

Consider the effect of the Frobenius isogeny on an oriented curve, namely $\pi_p \cdot (E, \iota) = (E^{(p)}, \iota^{(p)})$ where $\iota^{(p)} := (\pi_p)_*(\iota)$. For any isogeny φ, we have $\pi_p \circ \varphi(x, y) = \varphi^{(p)}(x^p, y^p) = \varphi^{(p)} \circ$

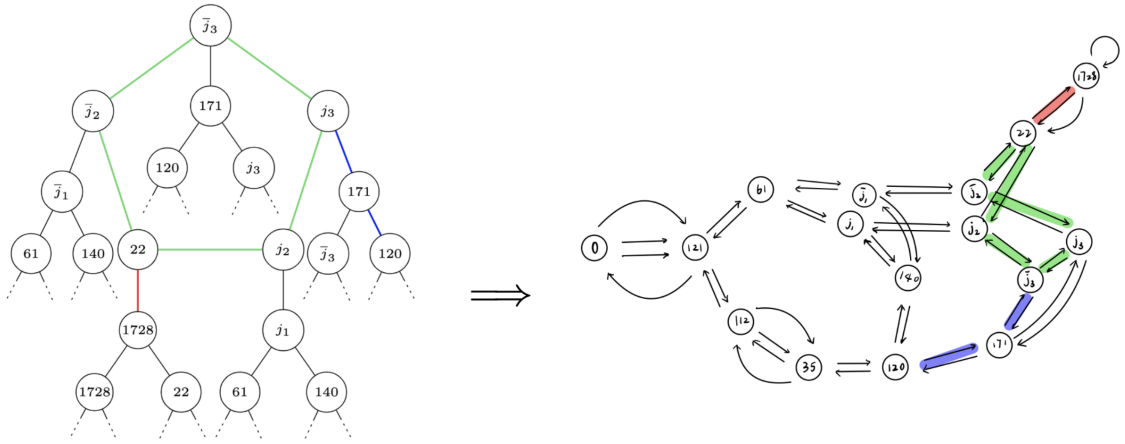

Figure 4.1: On the left hand side is a component of $\mathcal{G}_K$ for $p = 179$, $\ell = 2$ and $K = \mathbb{Q}(\sqrt{-47})$. On the right hand side is the supersingular 2-isogeny graph over $\mathbb{F}_{p^2}$. The green 5-cycle represents the rim of the volcano.

$\pi_p(x, y)$. Hence, one has $(\pi_p)_*(\iota)(\alpha) = \frac{1}{p}\pi_p \circ \iota(\alpha) \circ \widehat{\pi_p} = \frac{1}{p}\iota(\alpha)^{(p)} \circ \pi_p \circ \widehat{\pi_p} = \iota(\alpha)^{(p)}$. Since $\varphi \mapsto \varphi^{(p)}$ gives an isomorphism $\mathrm{End}(E) \cong \mathrm{End}(E^{(p)})$, we see that π_p is horizontal, so this gives an action on $\mathrm{SS}_{\mathcal{O}}$ for any $\mathcal{O}$ by the two-element group $\{1, \pi_p\} = \langle \pi_p \rangle$. In fact, it is an action on the graph, not just the vertices, i.e. it preserves adjacency.

Let $\mathcal{O}$ be a quadratic order of K. Next we define an action of $\mathrm{Cl}(\mathcal{O})$ on $\mathrm{SS}_{\mathcal{O}}$. For an invertible ideal $\mathfrak{a}$ of $\mathcal{O}$ embedded into $\mathrm{End}(E)$ via a K-orientation ι, there exists a horizontal isogeny $\varphi_{\mathfrak{a}}$ defined by the kernel $E[\iota(\mathfrak{a})] := \cap_{\theta \in \iota(\mathfrak{a})} \ker(\theta)$ [72, Proposition 3.5], and we write

$$\mathfrak{a} \cdot (E, \iota) := \varphi_{\mathfrak{a}} \cdot (E, \iota).$$

A different choice of $\varphi_{\mathfrak{a}}$ with the same kernel gives an isomorphic oriented curve [72, Section 3.3], so this is well-defined on the oriented ℓ-isogeny graph.

Proposition 4.3.1. *The definitions above give a transitive action of* $\mathrm{Cl}(\mathcal{O}) \times \langle \pi_p \rangle$ *on* $\mathrm{SS}_{\mathcal{O}}$ *whose point stabilizers are either all trivial or all* $\langle \pi_p \rangle$*. In particular,* $\#\,\mathrm{SS}_{\mathcal{O}} \in \{h_{\mathcal{O}}, 2h_{\mathcal{O}}\}$.

Proof. We have $\pi_p \cdot \varphi_{\mathfrak{a}} \cdot (E, \iota) = (\varphi_{\mathfrak{a}})^{(p)} \cdot \pi_p \cdot (E, \iota)$. To avoid confusion we momentarily use the

more specific notation $\varphi_{\mathfrak{a}}^{E}$ to denote the isogeny $\varphi_{\mathfrak{a}}$ with domain E. Then

$$\begin{aligned}\ker((\varphi_{\mathfrak{a}}^{E})^{(p)}) = \ker(\varphi_{\mathfrak{a}}^{E^{(p)}})^{(p)} = E[\iota(\mathfrak{a})]^{(p)} = \cap_{\theta\in\iota(\mathfrak{a})}\ker(\theta)^{(p)} \\ = \cap_{\theta\in\iota(\mathfrak{a})}\ker(\theta^{(p)}) = \cap_{\theta\in\iota^{(p)}(\mathfrak{a})}\ker(\theta) = E^{(p)}[\iota^{(p)}(\mathfrak{a})].\end{aligned} \tag{4.3.1}$$

The calculation above implies that $(\varphi_{\mathfrak{a}}^{E})^{(p)} = \varphi_{\mathfrak{a}}^{E^{(p)}}$. Thus

$$\pi_p \cdot \mathfrak{a} \cdot (E,\iota) = \mathfrak{a} \cdot \pi_p \cdot (E,\iota). \tag{4.3.2}$$

The definition of $\mathfrak{a}\cdot(E,\iota)$ gives a transitive action of $\mathrm{Cl}(\mathcal{O})$ on a subset $\mathrm{SS}'_{\mathcal{O}}$ of $\mathrm{SS}_{\mathcal{O}}$ which contains at least one of (E,ι) or $\pi_p\cdot(E,\iota)$ [72, Theorem 3.4]. In particular, $\mathrm{SS}'_{\mathcal{O}}$ forms one orbit under $\mathrm{Cl}(\mathcal{O})$. But by (4.3.2) above, the action is also well defined as an action of classes on all of $\mathrm{SS}_{\mathcal{O}}$. Hence there is a well-defined action of $\mathrm{Cl}(\mathcal{O})$ on $\mathrm{SS}_{\mathcal{O}}$.

The restriction of this action to $\mathrm{Cl}(\mathcal{O})$ acts freely and transitively on a subset of $\mathrm{SS}_{\mathcal{O}}$ which contains at least one of (E,ι) or $(E^{(p)},\iota^{(p)})$ [72, Theorem 3.4], from which the rest of the statement follows. Transitivity implies that the stabilizers are all of the same size. □

Suppose $\mathcal{O}'\subseteq\mathcal{O}$ are two quadratic orders. Then there is a homomorphism $\rho:\mathrm{Cl}(\mathcal{O}')\to\mathrm{Cl}(\mathcal{O})$. Using the previous proposition, this immediately gives a group action of $\mathrm{Cl}(\mathcal{O}')\times\langle\pi_p\rangle$ on $\mathrm{SS}_{\mathcal{O}}$. It turns out that the explicit form of this action can be computed in the same way as the original action in the following sense.

Proposition 4.3.2. *Let $\mathcal{O}'\subseteq\mathcal{O}$ with index f. Let $\mathfrak{a}'\in\mathrm{Cl}(\mathcal{O}')$ have norm coprime to f. Suppose that E has a K-orientation ι which is $\mathcal{O}$-primitive. Let $\varphi_{\mathfrak{a}'}$ be defined as the isogeny with kernel $\cap_{\theta\in\iota(\mathfrak{a}')}\ker(\theta)$. Then $\mathfrak{a}'\cdot(E,\iota)=\varphi_{\mathfrak{a}'}(E,\iota)$.*

Proof. Let $\mathfrak{a}:=\mathfrak{a}'\mathcal{O}$ be the extension to $\mathcal{O}$. In particular, $\iota(\mathfrak{a}')\subseteq\iota(\mathfrak{a})\subseteq\mathrm{End}(E)$. We will show $\cap_{\theta\in\iota(\mathfrak{a}')}\ker(\theta)=\cap_{\theta\in\iota(\mathfrak{a})}\ker(\theta)$. From that, we would complete the proof, since

$$\mathfrak{a}'\cdot(E,\iota)=\mathfrak{a}\cdot(E,\iota)=\varphi_{\mathfrak{a}}(E,\iota)=\varphi_{\mathfrak{a}'}(E,\iota).$$

We immediately have $\cap_{\theta\in\iota(\mathfrak{a}')}\ker(\theta)\supseteq\cap_{\theta\in\iota(\mathfrak{a})}\ker(\theta)$. We will show the index between these two

groups must divide a power of f. But the larger of the groups has cardinality coprime to f by hypothesis. So this would imply they are equal.

Write $\mathfrak{a}' = \alpha_1\mathcal{O}' + \alpha_2\mathcal{O}'$ and $\mathcal{O} = \mathbb{Z} + g\omega\mathbb{Z}$ using the notation of Section 4.2.1. Then

$$\cap_{\theta\in\iota(\mathfrak{a}')} \ker(\theta) = \ker(\iota(\alpha_1)) \cap \ker(\iota(\alpha_2)) \cap \ker(\iota(\alpha_1 f g\omega)) \cap \ker(\iota(\alpha_2 f g\omega)),$$
$$\cap_{\theta\in\iota(\mathfrak{a})} \ker(\theta) = \ker(\iota(\alpha_1)) \cap \ker(\iota(\alpha_2)) \cap \ker(\iota(\alpha_1 g\omega)) \cap \ker(\iota(\alpha_2 g\omega)).$$

We have $\ker(\iota(\alpha_i g\omega)) \subseteq \ker(\iota(\alpha_i f g\omega))$ with index f^2. Thus the index of $\cap_{\theta\in\iota(\mathfrak{a})} \ker(\theta)$ inside $\cap_{\theta\in\iota(\mathfrak{a}')} \ker(\theta)$ must divide a power of f. □

This has the consequence that one need not know $\mathcal{O}$ in order to compute the action of $\mathcal{O}'$ on $\mathrm{SS}_{\mathcal{O}}$.

4.3.4 Volcano structure

Any component of the oriented ℓ-isogeny graph has a *volcano structure* (see Figure 4.1), which is made precise by the following statement. (This behaviour is similar to the ordinary ℓ-isogeny graph, except here volcanoes have no floor; they descend forever.) Here we remind the reader that $p \neq \ell$ throughout the chapter.

Proposition 4.3.3 ([72, Proposition 4.1]). *Consider a vertex (E, ι) of the oriented ℓ-isogeny graph associated to K, a quadratic field of discriminant Δ. Suppose that ι is a primitive $\mathcal{O}$-orientation for E. If ℓ does not divide the conductor of $\mathcal{O}$, then the following hold.*

1. *There are no ascending edges from (E, ι).*
2. *There are $\left(\frac{\Delta}{\ell}\right) + 1$ horizontal edges incident with (E, ι).*
3. *There are $\ell - \left(\frac{\Delta}{\ell}\right)$ descending edges from (E, ι).*

If ℓ divides the conductor of $\mathcal{O}$, then the following hold.

1. *There is exactly one ascending edge from (E, ι).*
2. *The remaining ℓ edges incident with (E, ι) are descending.*

Furthermore, it is possible for the descending edges to be multiple, i.e. two descending edges may go to the same vertex. This occurs if and only if the unit group changes cardinality between the two relevant orders [72, Proposition 4.1]. In particular, this phenomenon may only occur if descending from a rim corresponding to the Gaussian or Eisenstein maximal orders, so it is quite limited. Further, by definition, edges which differ in type (ascending, horizontal or descending) cannot have the same oriented codomain.

Proposition 4.3.3 implies that each connected component of the oriented ℓ-isogeny graph is a *volcano*, containing a *rim* (comprised of the vertices with no ascending edges). From each vertex on the rim a tree radiates infinitely downward. Furthermore, only elements of $\mathrm{SS}_{\mathcal{O}}$ for which $\mathcal{O}$ is ℓ-fundamental can be at a rim. Fixing such an order $\mathcal{O}$, we can define a subgraph of the full K-oriented ℓ-isogeny graph given by those components whose rims consists of (E, ι) with ι a primitive $\mathcal{O}$-orientation. Since the components are volcanoes, we refer to this as the *$\mathcal{O}$-cordillera*. The vertices at the rims are exactly $\mathrm{SS}_{\mathcal{O}}$.

The action of an ideal class $[\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O})$ gives a permutation on $\mathrm{SS}_{\mathcal{O}}$, which we can visualize as a directed graph. This consists of cycles, all of which are the same size, given by the order of $[\mathfrak{a}]$ in $\mathrm{Cl}(\mathcal{O})$. Applying this to a prime ideal $\mathfrak{l}$ of $\mathcal{O}$ lying above ℓ, the *rims* of the $\mathcal{O}$-cordillera are exactly these cycles. The rims are individually singletons, single– or double-connected pairs, or cycles, and are all of the same size dividing $h_{\mathcal{O}}$. If ℓ is inert, they are each singletons. If ℓ is ramified, they are each of size 2 with one connecting edge (the isogeny and its dual are identified). If ℓ splits into two classes of order 2, we obtain a rim of size two with two connecting edges. Otherwise, the rims are non-trivial cycles in the oriented ℓ-isogeny graph, of size equal to the order of $[\mathfrak{l}] \in \mathrm{Cl}(\mathcal{O})$. We summarize the discussion as follows.

Proposition 4.3.4. *Let $\mathcal{O}$ be ℓ-fundamental. Let R_ℓ be the order of $[\mathfrak{l}] \in \mathrm{Cl}(\mathcal{O})$, for $\mathfrak{l}$ a prime of $\mathcal{O}$ lying above ℓ. The $\mathcal{O}$-cordillera consists of $\#\mathrm{SS}_{\mathcal{O}} / R_\ell$ volcanoes of rim size R_ℓ.*

4.3.5 From oriented isogeny graph to isogeny graph

There is a graph quotient $\mathcal{G}_K \to \mathcal{G}$ induced by forgetting the orientation.

Proposition 4.3.5. *Under this quotient, every component of $\mathcal{G}_K$ (i.e. every volcano) covers $\mathcal{G}$.*

Proof. Fix a volcano $\mathcal{V} \subset \mathcal{G}_K$. Choose a vertex $(E, \iota) \in \mathcal{V}$. The image E under the above map lies on $\mathcal{G}$. Since both $\mathcal{V}$ and $\mathcal{G}$ are regular of degree $\ell + 1$ at every vertex, the image of $\mathcal{V}$ must be all of $\mathcal{G}$. □

As a corollary, every j-invariant occurs on every volcano infinitely many times. Given p, a result of Kaneko [50, Theorem 2'] implies that the multiple occurrences of a given j-invariant cannot occur too quickly as one descends the oriented ℓ-isogeny volcano. In fact, there is at most one occurrence in the range $|\Delta| < p$ (here Δ is the discriminant corresponding to a certain level in the volcano).

4.3.6 Graph statistics and heuristics

In the ℓ-isogeny graph $\mathcal{G}$, two vertices are at distance d if the shortest path between them in the graph consists of d edges. This is known to be $\leq 2 \log p$ [73, Theorem 1]. In fact, for most pairs of vertices, the distance between them is at most $(1 + \epsilon) \log p$ (see [75, Theorem 1.5] for a precise statement).

We will use the following heuristic to justify the runtimes in the chapter. In a follow-up paper [4], we discuss this and some related heuristics in more detail.

Heuristic 4.3.3. *Let $\mathcal{O}$ be a quadratic order. Consider the finite union $\mathcal{S}$ of $\mathcal{O}'$-cordilleras for all $\mathcal{O}' \supseteq \mathcal{O}$. Fix a j-invariant j_0. Consider the set*

$$\mathcal{J}_{j_0,L} = \{(j_0, \iota) \in \mathcal{S} : \textit{appearing at level } \leq L\}.$$

Let $v : \mathcal{J}_{j_0,L} \to \{V : \textit{volcano of } \mathcal{S}\}$ be the function taking a vertex to the volcano upon which it lies. Then, as $L \to \infty$, the probability that $v((j_0, \iota)) = V$ for any volcano V is proportional to the number of descending edges from the rim of V.

Briefly, one expects this because sufficiently long random walks from any rim vertex will visit all vertices with a uniform distribution [44, Theorem 1]. This observation suffices to prove the case the rims are singletons; other cases should behave similarly.

The following lemma is useful for runtime analyses of our main algorithms (Proposition 4.8.1.

It states that the Hurwitz class number $H(\mathcal{O})$ (approximately the cardinality of the union of the sets $\mathrm{SS}_{\mathcal{O}}$ involved in $\mathcal{S}$ in Heuristic 4.3.3) is only marginally bigger than the regular class number $h_{\mathcal{O}}$ (approximately the size of the largest $\mathrm{SS}_{\mathcal{O}}$ in the union).

Lemma 4.3.1. *Let $\mathcal{O}$ be an imaginary quadratic order of conductor f in some quadratic field K with class number $h_{\mathcal{O}}$ and Hurwitz class number*

$$H_{\mathcal{O}} = \sum_{\mathcal{O} \subseteq \mathcal{O}' \subseteq \mathcal{O}_K} \frac{2}{w'} h_{\mathcal{O}'},$$

where the sum ranges over all the quadratic orders $\mathcal{O}'$ containing $\mathcal{O}$ and where $h_{\mathcal{O}'}$ and w' denote the class number and order of the unit group of $\mathcal{O}'$, respectively. Then $H_{\mathcal{O}} \leq h_{\mathcal{O}} O((\log\log f)^2)$ as $f \to \infty$.

Proof. Let $\mathcal{O}'$ be a quadratic order containing $\mathcal{O}$ and $f' = [\mathcal{O}' : \mathcal{O}]$ the index of $\mathcal{O}$ in $\mathcal{O}'$. Then f' divides f. By [29, Corollary 7.28], we have

$$h_{\mathcal{O}} = \frac{f' h_{\mathcal{O}'}}{w'/w} \prod_{\substack{q \mid f' \\ q \text{ prime}}} \left(1 - \left(\frac{\Delta}{q}\right) \frac{1}{q}\right),$$

where $w \in \{2, 4, 6\}$ is the size of the unit group $\mathcal{O}^*$. Thus,

$$h_{\mathcal{O}'} \leq \frac{w'}{w f'} h_{\mathcal{O}'} \prod_{\substack{q \mid f' \\ q \text{ prime}}} \left(1 - \frac{1}{q}\right)^{-1} = \frac{w'}{w \varphi(f')} h_{\mathcal{O}},$$

were $\varphi(\cdot)$ denotes Euler's phi function. It follows that

$$H_{\mathcal{O}} \leq \sum_{\mathcal{O} \subseteq \mathcal{O}' \subseteq \mathcal{O}_K} \frac{2}{w} \frac{1}{\varphi(f')} h_{\mathcal{O}} = \left(\sum_{f' \mid f} \frac{1}{\varphi(f')}\right) \frac{2}{w} h_{\mathcal{O}} \ .$$

By [2, Exercise 3.9 (a)], we have

$$\frac{n}{\varphi(n)} < \frac{\pi^2}{6} \frac{\sigma(n)}{n}$$

for all integers $n \geq 3$, where $\sigma(\cdot)$ is the sum of divisors function. From Robin's Theorem [74], we

obtain $\sigma(n)/n < c \log\log n$ for all $n \geq 3$ and some constant c. Therefore,

$$\sum_{3 \leq f' | f} \frac{1}{\varphi(f')} < \frac{c\pi^2}{6} \sum_{3 \leq f' | f} \frac{\log\log f'}{f'} < \frac{c\pi^2}{6} (\log\log f) \sum_{f' | f} \frac{1}{f'} = \frac{c\pi^2}{6} (\log\log f) \frac{\sigma(f)}{f} < \frac{(c\pi)^2}{6} (\log\log f)^2 ,$$

and hence $H_{\mathcal{O}} = h_{\mathcal{O}} O((\log\log f)^2)$. □

4.4 Navigating the K-oriented ℓ-isogeny graph

4.4.1 Conjugate orientations and orientations from endomorphisms

Motivated by our computational goals, we replace the abstract data of an orientation with the more computational data of an endomorphism. Given an element $\theta \in \mathrm{End}(E)$ along with its minimal polynomial $f(x)$, we can infer a unique $\mathbb{Z}[\theta]$-orientation only up to conjugation. Namely, if α is a quadratic irrational root of $f(x)$, then we define $\iota_\theta(\alpha) = \theta$ and extend to a ring homomorphism. The conjugate orientation is defined by $\widehat{\iota_\theta}(\alpha) = \widehat{\theta}$, or equivalently, by $\widehat{\iota_\theta}(\overline{\alpha}) = \theta$. An example in [72, Section 3.1] demonstrates a pair of $\mathrm{Gal}(K/\mathbb{Q})$-conjugate K-oriented curves which are not isomorphic. In other words, given $\varphi \in \mathrm{End}(E)$, one may be in either of two locations in the oriented ℓ-isogeny graph: (E, ι) or $(E, \widehat{\iota})$. However, locally at least, navigating from either location looks the same, in the sense of ascending/descending/horizontal edges and j-invariants.

Lemma 4.4.1. *The map $(E, \iota) \mapsto (E, \widehat{\iota})$ is a graph isomorphism and an involution, taking $\mathrm{SS}_{\mathcal{O}}$ back to itself for each $\mathcal{O}$. If $\varphi : (E, \iota) \to (E', \iota')$ is a K-oriented ℓ-isogeny, then $\varphi : (E, \widehat{\iota}) \to (E', \widehat{\iota'})$ is a K-oriented ℓ-isogeny, and the type (ascending, descending, or horizontal) is the same.*

Proof. The map is clearly a bijection on vertices. Observe that the dual of $\widehat{\varphi} \circ \iota \circ \varphi$ is $\widehat{\varphi} \circ \widehat{\iota} \circ \varphi$. From this it follows that the map is a graph isomorphism. The observation about type follows from the fact that $\mathrm{SS}_{\mathcal{O}}$ is taken back to itself. □

As consequences of this lemma, for two vertices (E, ι) and $(E, \widehat{\iota})$, we have the following:

1. the j-invariant is the same at both vertices;

2. both vertices are at the same volcano level;

3. if the vertices are not at a rim, the ascending isogeny from either vertex is the same;

4. if the vertices are at the rim, the pair of horizontal isogenies from either vertex is the same;

5. if we apply any fixed sequence of ℓ-isogenies from both vertices, the sequence of j-invariants appearing on the resulting paths is the same.

For these reasons, it will not, in practice, be necessary for us to know which of two conjugate orientations we are dealing with. Therefore we do not make any choice between the two. In the remainder of the chapter, we will not dwell on this distinction, and will work with endomorphisms instead of orientations.

Remark 4.4.1. It is a natural question to ask when a subset of the four oriented curves (E, ι), $(E^{(p)}, \iota^{(p)})$, $(E, \widehat{\iota})$ and $(E^{(p)}, \widehat{\iota}^{(p)})$ coincide. This question may have importance to a more detailed runtime analysis than we present in this paper, for example. See the thesis of the first author [3].

4.4.2 ℓ-primitivity, ℓ-suitability, and direction finding

Having associated an endomorphism to an orientation, we can now define the following.

Definition 4.4.2. Let $\theta \in \mathrm{End}(E)$ be an endomorphism and α the corresponding quadratic element (up to conjugation). Then θ (as well as α) is called *ℓ-primitive* if the associated orientations $\iota_\theta : \alpha \mapsto \theta$ and $\widehat{\iota_\theta} : \overline{\alpha} \mapsto \theta$ are ℓ-primitive $\mathbb{Z}[\alpha]$-orientations. Moreover, θ (as well as α) is called *N-suitable*, for an integer N, if α is of the form $f\omega + kN$ where k is some integer, f is the conductor of $\mathbb{Z}[\alpha]$, and $f\omega$ is the generator of $\mathbb{Z}[\alpha]$ as described in the conventions of Section 4.2.1.

The purpose of this definition is made clear by the following lemma.

Lemma 4.4.2. *If $\theta \in \mathrm{End}(E)$ is ℓ-suitable, then θ is not ℓ-primitive if and only if $\theta/\ell \in \mathrm{End}(E)$.*

Proof. The endomorphism θ is not ℓ-primitive if and only if there exists a (unique) order $\mathcal{O}' \subseteq \mathrm{End}(E)$ of index $\ell = [\mathcal{O}' : \mathbb{Z}[\theta]]$. But this happens if and only if $\theta/\ell \in \mathrm{End}(E)$, since under the ℓ-suitability hypothesis, $\mathbb{Z}[\theta/\ell]$ is precisely this order $\mathcal{O}'$. □

Lemma 4.4.3. *Let $\alpha \in O_K \setminus \mathbb{Z}$ with trace t and norm n. Let f be the conductor and Δ_K the fundamental discriminant of $\mathbb{Z}[\alpha]$. Then*

$$\{T \in \mathbb{Z} : \alpha + T \text{ is } N\text{-suitable}\} = \begin{cases} \frac{f-t}{2} + N\mathbb{Z} & \Delta_K \equiv 1 \pmod 4 \\ \frac{-t}{2} + N\mathbb{Z} & \Delta_K \equiv 0 \pmod 4 \end{cases}.$$

In our algorithms, we sometimes choose an optimal T in the sense of the following definition.

Definition 4.4.3. If $\alpha + T$ has the smallest possible non-negative trace amongst all ℓ-suitable translates of α, we say that $\alpha + T$ is a *minimal ℓ-suitable translate*.

Proposition 4.4.1. *Suppose $\psi : E \to E'$ is an ℓ-isogeny and $\theta \in \mathrm{End}(E)$ is an ℓ-suitable ℓ-primitive endomorphism. Then*

1. *ψ is ascending if and only if $[\ell]^2 \mid \psi \circ \theta \circ \widehat{\psi}$ in $\mathrm{End}(E')$.*
2. *ψ is horizontal if and only if $[\ell] \mid \psi \circ \theta \circ \widehat{\psi}$ but $[\ell]^2 \nmid \psi \circ \theta \circ \widehat{\psi}$ in $\mathrm{End}(E')$.*
3. *ψ is descending if and only if $[\ell] \nmid \psi \circ \theta \circ \widehat{\psi}$ in $\mathrm{End}(E')$.*

Proof. Let ι' be the induced orientation on E' of $\iota : \alpha \mapsto \theta$ via ψ. Let $\mathcal{O}, \mathcal{O}' \subseteq K$ be two orders such that ι is $\mathcal{O}$-primitive and ι' is $\mathcal{O}'$-primitive. The three cases in the proposition corresponds to the cases when $\mathcal{O} \subsetneq \mathcal{O}'$, $\mathcal{O} = \mathcal{O}'$ and $\mathcal{O} \supsetneq \mathcal{O}'$ respectively. Therefore, ψ is ascending, horizontal and descending correspondingly. □

The previous proposition demonstrates that it is enough to check the action of $\psi \circ \theta \circ \widehat{\psi}$ on $E[\ell]$ to determine whether the isogeny is ascending or descending. However, we can also write down the ascending or horizontal endomorphisms directly by analysing the eigenspaces of θ on $E[\ell]$, as follows. Note that a version of this for Frobenius is used in CSIDH [18] to walk horizontally, earlier used in [52, Section 3.2] and [34, Section 2.3].

Proposition 4.4.2. *Suppose $\theta \in \mathrm{End}(E)$ is ℓ-suitable and ℓ-primitive. Let $\psi : E \to E'$ be an ℓ-isogeny with kernel $\langle P \rangle \subset E[\ell]$. Then ψ is ascending if and only if $\theta(P) = 0$, and ψ is horizontal if and only if P is an eigenvector of the action of θ on $E[\ell]$ having non-zero eigenvalue. Otherwise ψ is descending.*

Proof. Suppose $\alpha \mapsto \theta$ gives a K-orientation on E, for $K = \mathbb{Q}(\alpha)$. Then for each non-zero eigenvalue $\lambda \in \mathbb{Z}/\ell\mathbb{Z}$ of θ acting on $E[\ell]$, the ideal $\mathfrak{l} := (\alpha - \lambda, \ell)_{\mathcal{O}}$ is an invertible prime ideal above (ℓ) in $\mathcal{O} := \mathbb{Z}[\alpha]$. The isogeny with kernel $E[\mathfrak{l}]$ is horizontal [72, Proposition 3.5] and has kernel $\langle P \rangle$ where $\theta(P) = [\lambda]P$ and $[\ell]P = O_E$. No other ℓ-isogenies are horizontal [72, Proposition 4.1]. (Note that, as usual, [72] only uses the class group action on the image of curves over number fields with CM, but by the more general action including Frobenius described in Proposition 4.3.1, it holds in our case also.)

Next, suppose that $\lambda = 0$. Then $\mathfrak{l} := (\alpha, \ell)_{\mathcal{O}}$ is a non-invertible ideal, and the corresponding ideal action is ascending [72, Proposition 3.5]. In this case $E[\mathfrak{l}] = \langle P \rangle$ where $[\ell]P = O_E$ and $\theta(P) = 0$. There is only one ascending isogeny [72, Proposition 4.1]. □

4.5 Representing orientations and endomorphisms

4.5.1 Representations and functionality

We remind the reader that throughout the chapter, isogenies and endomorphisms will be assumed separable unless otherwise stated (see Section 4.2.1). In this section, we discuss two types of representations of an endomorphism. The first is the most basic.

Definition 4.5.1. A *rationally represented isogeny* is an isogeny given by a rational map. A *rationally represented endomorphism* is an endomorphism which is rationally represented as an isogeny.

We may also represent endomorphisms of large degree (e.g. not polynomial in $\log p$) by writing them as a chain of isogenies of manageable degree.

Definition 4.5.2. An *isogeny chain isogeny* $\varphi : E_0 \to E_k$ is an isogeny which is given in the form of a sequence of rationally represented isogenies $(\varphi_i : E_{i-1} \to E_i)_{i=1}^{k}$ which compose to φ, i.e. $\varphi_k \circ \varphi_{k-1} \circ \cdots \circ \varphi_2 \circ \varphi_1 = \varphi$.

Let $B > 0$. Recall that an integer is called *B-smooth* (or *B-friable*) if its largest prime factor is less than B. It is called *B-powersmooth* (or *B-ultrafriable*) if its largest prime power factor is

less than B. In order to handle isogeny chain endomorphisms, we will generally *refactor* them, meaning we will replace the chain with another chain representing the same endomorphism, but whose component isogenies have coprime prime power degrees. Moreover, we also fix a powersmooth bound B for the prime power degrees. In Section 6, we explain our choice of B for the best algorithm runtime.

Definition 4.5.3. An isogeny chain whose component isogenies have coprime prime power degrees is called a *prime-power* isogeny chain. Moreover, it is called a *B-powersmooth prime-power* isogeny chain if its component isogenies have coprime prime power degrees less than B.

For isogenies represented in any manner, we will need the following functionality:

1. **Evaluation at ℓ-torsion**: Given $\theta \in \mathrm{End}(E)$, and $P \in E[\ell]$, compute $\theta(P) \in E[\ell]$. (See Lemma 4.2.4.)
2. **ℓ-suitable translation**: Given $\theta \in \mathrm{End}(E)$, compute $\theta + [t] \in \mathrm{End}(E)$, for some $t \in \mathbb{Z}$, so that $\theta + [t]$ is ℓ-suitable (Definition 4.4.2) and again separable. (See Lemma 4.2.7 for rational representations and Algorithm 4.5.3 for isogeny chains.) Note that for powersmooth prime power isogeny chains, by computing an ℓ-suitable translation, we always mean that we compute a translate that is a B-powersmooth prime power isogeny chain unless otherwise specified. This is exactly what Algorithm 4.5.3 does.
3. **Division by ℓ**: Given $\theta \in \mathrm{End}(E)$ such that $\theta = [\ell] \circ \theta'$, compute $\theta' \in \mathrm{End}(E)$. (See Algorithm 4.10.2 for rational representations and Algorithm 4.5.2 for isogeny chains.)
4. **Waterhouse twisting**: Given $\theta \in \mathrm{End}(E)$ and $\varphi : E \to E'$ an ℓ-isogeny, compute $\varphi \circ \theta \circ \widehat{\varphi} \in \mathrm{End}(E')$. (See Lemma 4.2.6 for rational representations and Algorithm 4.5.1 for isogeny chains.)

We have endeavoured to write the chapter in a modular fashion, so that these two types of representations — or another unforeseen type of representation, as long as it provides these functionalities — can be used at will. In particular, we write our algorithms (Sections 4.7.1 onwards) in terms of these functionalities (writing for example $\theta \leftarrow \theta/[\ell]$ for division by ℓ, to be implemented according to the endomorphism representation chosen).

Although isogeny chain endomorphisms may have large degree, we assume that for any type of endomorphism representation, **the overall degree, trace and discriminant are polynomially bounded in** p.

As discussed in Section 4.2.2, it can be rather involved to compute the trace of an endomorphism. However, the manipulations we perform in our algorithms transform the trace predictably. Therefore, it is to our advantage to attach the trace data to all endomorphisms under consideration and update it as needed. For either rationally represented or isogeny chain endomorphisms, our data type will be the following.

Definition 4.5.4. A *traced endomorphism* is a tuple of data (E, θ, t, n) where $\theta \in \mathrm{End}(E)$ is either rationally represented or an isogeny chain, and t and n are the reduced trace and norm (degree) of θ, respectively.

4.5.2 Functionality for rationally represented endomorphisms

In the case of a rationally represented endomorphism, we can evaluate at ℓ-torsion directly (Lemma 4.2.4). We can translate by an integer by adding the rational maps under the group law (Lemma 4.2.7). We can Waterhouse twist by composing the maps (Lemma 4.2.6). However, division by ℓ requires a dedicated algorithm. In Section 4.10, we describe the algorithm of McMurdy [69] for exactly this purpose, and analyse its runtime in greater detail. For the completeness of this section, we record here that the runtime of dividing an isogeny $\varphi : E_1 \to E_2$ of supersingular elliptic curves defined over $\mathbb{F}_{p^2}$ (Algorithm 4.10.2) is $O(\deg^2(\varphi)\mathbf{M}(p))$.

4.5.3 Functionality for isogeny chain endomorphisms

An isogeny chain representation of an endomorphism can be more space efficient than its rational representation, and more efficient to compute with. Computing the Waterhouse twist of an isogeny chain endomorphism is essentially trivial: include the twisting isogenies in the chain. To evaluate at ℓ-torsion, we evaluate the sequence of maps one-by-one (Lemma 4.2.4); the runtime depends polynomially on the largest degree of their component isogenies.

In this section, we give algorithms for the more onerous tasks of division-by-ℓ and translation

by integers. Their runtimes will depend polynomially on the largest prime power appearing in the degree of the endomorphism, which must therefore be kept small for efficiency. To address this problem, which arises when translating to something ℓ-suitable, we use a search step to find a translate of powersmooth degree.

In order to keep the largest prime power in the degree below a certain bound, we will be interested in B-powersmooth prime power isogeny chains. In the lastsection of this section, we balance the runtime considerations by choosing a subexponential powersmoothness bound B for the degree of an isogeny chain endomorphism. Thus, working with a general such endomorphism is a subexponential endeavour.

Although our concern is with endomorphisms, both Algorithm 4.5.1 and Algorithm 4.5.2 would work for an isogeny in general.

Refactoring an isogeny chain

If an endomorphism is not in the prime power isogeny chain form, we can refactor it. To achieve this, one factors the degree, then builds the new chain from scratch kernel-by-kernel, as described in Algorithm 4.5.1. In fact, any endomorphism that can be evaluated at arbitrary points on the curve can be converted to an isogeny chain representation using this algorithm.

Remark 4.5.5. In principle, it is possible to refactor into degrees that are primes as opposed to prime powers. However, this doesn't circumvent the need for powersmoothness (in practice, it would provide some savings, e.g. in Vélu's formulas, but it wouldn't avoid the overall polynomial dependence on the powersmoothness bound). During refactoring, for any prime power factor q^k of the degree, the endomorphism needs to be evaluated on the q^k-torsion, which should therefore be defined over a field of manageable size. See [21, Section 5.2.1] for a nice discussion of this issue in another context.

Proposition 4.5.1. *Let B be the largest prime power dividing $\deg\theta$. Then Algorithm 4.5.1 is correct and has runtime $O(\log\deg\theta)$ times the maximum of the following three runtimes: $O(B^2(\log p))$, $O(B^2(\log B)\boldsymbol{M}(p^{B^2}))$ and the runtime of evaluation of θ on $O(B)$-torsion, and space requirement of $O(B^2\log p)$. In particular, if θ is an integer translate of an isogeny chain with B-powersmooth*

Algorithm 4.5.1: Refactoring an isogeny chain

Input: A traced endomorphism (E, θ, t, n) in any form in which it can be evaluated (such as rationally represented or a translation of an isogeny chain), of degree coprime to p.

Output: The same traced endomorphism $(E, \theta, t, n) \in \mathrm{End}(E)$ in prime-power isogeny chain form.

```
H ← []
E_0 ← E
Write n = ∏_{j=0}^{u} q_j^{k_j} by factoring.
For j = 0, ..., u do
    Compute a basis for E[q_j^{k_j}].
    Compute G_j = ker(θ) ∩ E[q_j^{k_j}] by evaluating θ on E[q_j^{k_j}].
    Compute a rationally represented isogeny φ_j : E_j → E_{j+1} given by the kernel
      φ_{j-1} ∘ ... ∘ φ_0(G_j), using Velu's formulas.
    Append (φ_j : E_j → E_{j+1}) to H.
Return (E, θ, t, n) where θ is given by the isogeny chain H.
```

degree, then the runtime is $O((\log \deg \theta) B^2 \boldsymbol{M}(p^{B^2}))$.

Proof. The **For** loop builds an isogeny chain for θ. One can see this by induction: assuming $\theta = \nu' \circ \nu$ where $\nu := \varphi_{j-1} \circ \ldots \circ \varphi_0$, we have by construction that $\nu(G_j)$ vanishes under ν'. Hence θ factors through $\varphi_j \circ \nu$.

To write the factorization of n is at worst $O(B \log^2 B)$ in time (by trial division), but $O(\log n)$ in space. For each prime power factor (so at most $\log n$ times), we must do each of the following: (i) Compute a basis for the torsion subgroup in time and space $O(B^2 \log p)$ by Lemma 4.2.3. (ii) Evaluate θ on the basis (iii) List the elements of the kernel G_j; this involves computing all linear combinations of the basis images and recording those combinations which vanish; and then computing the corresponding linear combinations of the original torsion points, a total of $B^2 + B$ linear combinations; by Lemma 4.2.1, this takes time $O(B^2(\log B)\mathbf{M}(p^{B^2}))$. (iv) Apply Vélu's formulas in time $O(B\mathbf{M}(p^{B^2}))$ by Lemma 4.2.5. Writing down the resulting isogeny takes $O(B)$ coefficients in a subfield of $\mathbb{F}_{p^{12}}$ (Lemma 4.2.2), hence we use $O(B \log p)$ space for each isogeny of the chain.

If θ is a translate of an isogeny chain whose component degrees are bounded by B, we can further estimate the time taken to evaluate θ on the torsion basis. This involves one evaluation

for each component isogeny (at most $\log n$ such). Each evaluation of a component φ_i takes time $O((\deg \varphi_i)\mathbf{M}(p^{B^2}))$ by Lemma 4.2.4. (Evaluation of the integer translation is of smaller runtime by Lemma 4.2.1; since the integer is taken modulo the torsion, its size is irrelevant.) □

Remark 4.5.6. The exponent of the dependence on B can surely be improved here; for example, if B is prime, then our bound on the number of linear combinations on which to evaluate θ is a substantial overestimate.

Division by ℓ

In this section, we demonstrate in Algorithm 4.5.2 how to divide an isogeny chain endomorphism by $[\ell]$.

Algorithm 4.5.2: Dividing-by-$[\ell]$ for an endomorphism given as a prime-power isogeny chain.

Input: A traced endomorphism (E, θ, t, n) in prime-power isogeny chain form , such that $\theta(E[\ell]) = \{O_E\}$.
Output: A traced endomorphism $(E, \theta', t', n') \in \mathrm{End}(E)$ such that $\theta = [\ell] \circ \theta'$, in prime-power isogeny chain form.

1 $i \leftarrow$ the index at which the chain has ℓ-power degree.
2 Modify the chain for θ by replacing φ_i with $\varphi_i/[\ell]$ using Algorithm 4.10.2.
3 $t \leftarrow t/\ell$
4 $n \leftarrow n/\ell^2$.
5 **Return** (E, θ, t, n).

Proposition 4.5.2. *Let B be an upper bound on the degrees of the prime powers in θ. Then Algorithm 4.5.2 is correct and runs in time $O(B^2 \operatorname{poly}(\log p))$.*

Proof. The runtime is negligible except for the call to Algorithm 4.10.2. By Proposition 4.10.3, that algorithm runs in time $O(\deg^2(\varphi_i)\mathbf{M}(p))$ (and we bound $\mathbf{M}(p)$ by $\operatorname{poly}(\log p)$ as discussed in Section 4.2.1). □

Finding a B-powersmooth ℓ-suitable translate

As discussed, we wish to keep the powersmoothness bound B on the degree of an isogeny chain endomorphism low when translating by an integer. Since our goal is to find ℓ-suitable endo-

morphisms, and translation by ℓ preserves ℓ-suitability, we may search amongst nearby translates for one which is B-powersmooth for our desired bound B.

Algorithm 4.5.3: Computing a B-powersmooth ℓ-suitable translate in prime-power isogeny-chain form.

Input: A traced endomorphism (E, θ, t, n) in prime-power isogeny chain form , and a powersmoothness bound B (where $B = \infty$ is acceptable).

Output: A traced endomorphism (E, θ', t', n') which satisfies $\mathbb{Z}[\theta'] = \mathbb{Z}[\theta]$ but where θ' is ℓ-suitable, and is given as a separable prime-power isogeny chain, with prime powers $\leq B$.

1 Compute the minimal ℓ-suitable translate T for θ (Lemma 4.4.3).
2 Try values $n(b) = n + (T + b\ell)t + (T + b\ell)^2$ for small integers b, to find b such that $n(b)$ is B-powersmooth and coprime to p.
3 $\theta' \leftarrow$ a refactored prime-power isogeny chain for $\theta + T + b\ell$, using Algorithm 4.5.1.
4 $t' \leftarrow t + 2T + 2b\ell$
5 $n' \leftarrow n + (T + b\ell)t + (T + b\ell)^2$.
6 **Return** (E, θ', t', n')

Proposition 4.5.3. *Algorithm 4.5.3 is correct, and the runtime is that of Algorithm 4.5.1 plus the time taken for Step 2.*

Proof. The ℓ-suitability of the output is guaranteed by Lemma 4.4.3. □

Choosing a powersmoothness bound B

In practice, we need to balance the runtimes of the various functionalities of an isogeny chain endomorphism by choosing an appropriate powersmoothness bound B.

The number of B-smooth and B-powersmooth numbers below a bound X is asymptotically the same, provided that $B/\log^2 X \to \infty$ [88] (another reference shows they are asymptotically proportional, provided $\log B/(\log\log X) \to \infty$ [28, Section 3.1]). In our situation, we expect to handle endomorphisms which may have degree as much as exponential in $\log p$. Fortunately, we can, at least heuristically, find subexponentially smooth translates in subexponential time [28, Section 3.1].

Heuristic 4.5.7. *Given integers n, t, and T, values of the function $f(b) = n + (T + b\ell)t + (T + b\ell)^2$, as $b \to \infty$, are powersmooth with the same probability as randomly chosen integers of the same size.*

This is the powersmooth analogue of the heuristic assumption underlying the quadratic sieve; see [30].

Proposition 4.5.4. *Assume Heuristic 4.5.7. Let $\theta \in \mathrm{End}(E)$ have degree d such that $L_d(1/2) > \mathrm{poly}(\log p)$. Then Algorithm 4.5.3 produces a $L_d(1/2)$-powersmooth prime power isogeny chain of total degree $O(d)$. Furthermore, on $L_d(1/2)$-powersmooth prime power isogeny chains of total degree $O(d)$, the maximum runtime of Algorithm 4.5.1, Algorithm 4.5.2 and Algorithm 4.5.3 is $L_d(1/2)$, and the output of these algorithms is again an $L_d(1/2)$-powersmooth prime power isogeny chain of total degree $O(d)$.*

Proof. We have seen that all the runtimes in Algorithms 4.5.1 through 4.5.3 are polynomial in B, $\log \deg \theta$ ($= \mathrm{poly}(\log p)$ by assumption), and $\log p$, with the exception of Step 2 in Algorithm 4.5.3. Hence, taking $B = L_d(1/2)$, the runtime (except for this step) will be $L_d(1/2)$.

As far as Step 2, under Heuristic 4.5.7, we can call on [28, Section 3.1] (note that the L-notation in the reference differs from ours here). According to [28, Section 3.1], the probability that a random integer between 1 and d is B-powersmooth is $1/L_d(1/2)$. Testing values of b between 1 and $L_d(1/2)$, we do indeed have $n(b) < d$. Thus, we expect to find a B-powersmooth integer, by Heuristic 4.5.7. For each b-value, to see whether $n(b)$ is B-powersmooth, we use naive division in time $O(B \log^2 B)$. Therefore, in total, one will find $L_d(1/2)$-powersmooth integers in time $L_d(1/2)$.

□

A few important notes for the remainder of the chapter: **we will assume $B = L_{\deg \theta}(1/2)$, where θ is the initial input endomorphism, when dealing with isogeny chains, and that whenever we perform an ℓ-suitable translation on an isogeny chain, we choose a B-powersmooth prime power ℓ-suitable translate.**

Example 4.5.8 (**Computing an ℓ-suitable translation** via Algorithm 4.5.3)**.** We continue with our running example, computing an ℓ-suitable translation of a degree-47 endomorphism θ on the curve $E_{1728} : y^2 = x^3 - x$ for $\ell = 2$. Here θ is given as a rational map:

$$\theta(x, y) = \left(\frac{99x^{47} + 22x^{46} + \cdots + 77}{x^{46} + 40x^{45} + \cdots + 77}, \frac{113ix^{69} + 157ix^{68} + \cdots + 63i}{x^{69} + 60x^{68} \cdots + 158} y \right).$$

The traced endomorphism is $(E_{1728}, \theta, 0, 47)$. In Step 1, we compute the minimal 2-suitable translate T using Lemma 4.4.3. From the traced endomorphism, we compute $\Delta_\theta = t^2 - 4n = 0^2 - 4 \cdot 47 = -188$. This implies that the fundamental discriminant is -47 and the conductor is 2. Therefore the 2-suitable translates are of the form $\theta + T$ for T in $1 + 2\mathbb{Z}$, and the minimal 2-suitable translate is obtained for $T = 1$. In Step 2, we find $b = 0$ produces $n(b) = 2^4 \cdot 3$, which is B-powersmooth for $B = 50$. In Step 3, we factor $\theta + 1$ into an isogeny chain $\theta' = \varphi_{171} \circ \varphi_{1728}$ where $\deg(\varphi_{1728}) = 16$ and $\deg(\varphi_{171}) = 3$, which requires a call to Algorithm 4.5.1. Here,

$$\varphi_{1728}(x, y) = \left(\frac{x^{16} + (156i + 63)x^{15} + \cdots + 56i + 36}{x^{15} + (156i + 63)x^{14} + \cdots + 10i + 71}, \frac{x^{23} + (55i + 95)x^{22} + \cdots + 105i + 82}{x^{23} + (55i + 95)x^{22} + \cdots + 26i + 87} y \right)$$

and

$$\varphi_{171}(x, y) = \left(\frac{x^3 + (102i + 30)x^2 + (31i + 74)x + 10i + 158}{x^2 + (102i + 30)x + 98i + 130}, \frac{x^3 + (153i + 45)x^2 + (3i + 88)x + 102i + 108}{x^3 + (153i + 45)x^2 + (115i + 32)x + 45i + 174} y \right).$$

The quantities in Steps 4 and 5 can be computed immediately from the values of t, n, T, b, and ℓ, yielding $t' = 2$ and $n' = 48$. The algorithm returns $(E_{1728}, \theta', t', n')$.

4.5.4 Poly-rep runtime

In the last two sections, we computed the runtimes of the basic operations for rationally represented and isogeny chain endomorphisms. We summarize here.

Proposition 4.5.5. *Suppose θ is an isogeny whose trace t, norm n and discriminant Δ are all at most polynomial in p. If θ is rationally represented, then:*

1. *Evaluating at ℓ-torsion takes time $O(n \operatorname{poly}(\log p))$ (Lemma 4.2.4).*
2. *Waterhouse twisting by an ℓ-isogeny takes time $\widetilde{O}(n \operatorname{poly}(\log p))$ (Lemma 4.2.6).*
3. *Dividing by ℓ takes time $O(n^2 \operatorname{poly}(\log p))$ (Proposition 4.10.3).*
4. *Computing an ℓ-suitable translate takes time $\widetilde{O}(\max\{n, t^2\} \operatorname{poly}(\log p))$ (Lemma 4.2.7).*

If θ of degree $O(d)$ is represented as a B-powersmooth prime power isogeny chain with $B = L_d(1/2)$ as described in Section 6, then, assuming Heuristic 4.5.7 (see Proposition 4.5.4):

1. *Evaluating at ℓ-torsion takes time $L_d(1/2)$ (Lemma 4.2.4).*

2. *Waterhouse twisting takes time $L_d(1/2)$ (Proposition 4.5.1).*

3. *Dividing by ℓ takes time $L_d(1/2)$ (Proposition 4.5.2).*

4. *Computing a B-powersmooth ℓ-suitable translate takes time $L_d(1/2)$ (Proposition 4.5.3).*

Of course, in individual situations, these runtimes may be much lower (for example, dividing an isogeny chain by $[\ell]$ may depend only on the power of ℓ if no refactoring is necessary).

In the following algorithms, we will need to call all of these operations many times. It will be convenient to set the following definition.

Definition 4.5.9. We define the *representation runtime* of a given representation (rationally represented or isogeny chain) to be the maximum runtime of implementing the following operations: evaluating at ℓ-torsion, ℓ-suitable translation, division-by-ℓ, and Waterhouse twisting by an ℓ-isogeny. We say that an algorithm has *poly-rep runtime* if its runtime is bounded above by a constant power of $\log p$ times the relevant representation runtime.

Note that our definition above means that, **throughout the chapter** $\mathrm{poly}(\log p) \leq$ **poly-rep**.

4.6 Orientation-finding for $j = 1728$

For many cryptographic applications, a curve with known endomorphism ring is assumed. Most commonly used is the curve with $j = 1728$, which is supersingular when $p \equiv 3 \pmod 4$. For simplicity, this is the curve we will consider here, but our algorithm can be modified to suit other situations (see below). We will use the model given by $E_{\text{init}} : y^2 = x^3 - x$, which has endomorphism ring

$$\left\langle 1, \mathbf{i}, \frac{\mathbf{i}+\mathbf{k}}{2}, \frac{1+\mathbf{j}}{2} \right\rangle, \quad \mathbf{i}^2 = -1, \mathbf{j}^2 = -p, \mathbf{k} = \mathbf{ij}.$$

In particular, $\mathbf{i}$ is given by $(x, y) \mapsto (-x, \sqrt{-1}y)$ and $\mathbf{j}$ is the Frobenius endomorphism[3] $(x, y) \mapsto (x^p, y^p)$.

Let $\mathcal{O}$ be an imaginary quadratic order of conductor coprime to ℓ such that $\mathcal{O}$ embeds in $B_{p,\infty}$. In this section we give an algorithm for finding an endomorphism $\varphi \in \mathrm{End}(E_{\mathrm{init}})$, generating a suborder $\mathcal{O}' \subseteq \mathcal{O}$ of discriminant $\ell^{2r}\Delta_{\mathcal{O}}$ for the minimal possible r. In other words, we wish to find an ℓ-primitive orientation by a suborder $\mathcal{O}'$ of $\mathcal{O}$. Or, rephrased again, we want to find an orientation for E_{init} placing it at its highest level (nearest to the rims) in the oriented supersingular isogeny graph cordillera with rims at $\mathcal{O}$. Alternatively, the algorithm can be run continuously, to return all ℓ-primitive orientations by suborders of $\mathcal{O}$ in order of increasing r.

The algorithm we provide (Algorithm 4.6.1) has similarities to [54, Integer Representation, Section 3.2], where the difference arises because we seek a given discriminant instead of a given norm. In fact, this algorithm applies more generally to curves over $\mathbb{F}_p$ satisfying the hypotheses of [54, Section 3.2]; in Section 4.6.3 we make some comments on adapting this algorithm for other initial curves of known endomorphism ring.

An algorithm for a similar problem appears in [99, Section 4.3]. However, that algorithm finds the 'smallest' quadratic order only: it requires the discriminant be bounded above by $2\sqrt{p}-1$. We wish to find orientations by more general orders.

4.6.1 In terms of 1, i, j, k

The goal of Algorithm 4.6.1 is to find such an endomorphism as a linear combination of 1, $\mathbf{i}$, $\mathbf{j}$, $\mathbf{k}$.

The idea is to solve a norm equation for E_{init} under extra conditions that guarantee that the result is an element of the desired quadratic order. The algorithm depends on Cornacchia's algorithm, which is discussed in [23, Section 1.5.2] and [41, Section 3.1]. It solves the equation $x^2 + y^2 = n$ when a square root of -1 modulo n is known (e.g., such a square root can be found if n is factored).

Remark 4.6.1. Algorithm 4.6.1 can be adapted to run continuously, finding many K-orientations

[3] Note that some papers use the model $y^2 = x^3 + x$, such as [38, Section 5.1]; this model is a quartic twist of ours and under the induced isomorphism of the endomorphism rings, the element which is realized as Frobenius is not preserved. The model we choose for this chapter has 2-torsion conveniently defined over $\mathbb{F}_p$. See [84].

Algorithm 4.6.1: Computing an orientation for the initial curve.

Input: A discriminant $\Delta_{\mathcal{O}}$ coprime to p, which is the discriminant of an ℓ-fundamental quadratic order $\mathcal{O}$ that embeds into $B_{p,\infty}$.

Output: (θ, r) where $\theta \in \mathrm{End}(E_{\mathrm{init}})$ is represented as a linear combination of 1, **i**, **j**, **k**, with $\mathbb{Z}[\theta] = \mathcal{O}' \subseteq \mathcal{O}$ where $[\mathcal{O} : \mathcal{O}'] = \ell^r$. Furthermore, θ is ℓ-primitive. (Here E_{init} and **i**, **j** and **k** are as in the introduction to this section, namely the specified model of $j = 1728$.)

$r \leftarrow -1$.
repeat
  $r \leftarrow r + 1$.
  Find the smallest positive x such that $x^2 \equiv -\Delta_{\mathcal{O}}\ell^{2r} \pmod{p}$.
  While $x < \sqrt{-\Delta_{\mathcal{O}}\ell^{2r}}$ **do**
    $D \leftarrow (-\Delta_{\mathcal{O}}\ell^{2r} - x^2)/p$.
    If $D \equiv 1 \pmod 4$ **then**
      If *D is prime* **then**
        Find a square root of -1 modulo D.
        Use Cornacchia's algorithm to find y and z such that $y^2 + z^2 = D$.
        If *y is odd* **then**
          Swap y and z.
        If *x is even* **then**
          $\theta \leftarrow \frac{1}{2} + \frac{x}{2}\mathbf{i} + \frac{z}{2}\mathbf{j} + \frac{y}{2}\mathbf{k}$.
        else
          $\theta \leftarrow \frac{x}{2}\mathbf{i} + \frac{y}{2}\mathbf{j} + \frac{z}{2}\mathbf{k}$.
        break *the* ***While*** *loop*
    $x \leftarrow x + p$
until *θ is defined*
$c \leftarrow 0$
While $c < r$ **do**
  Translate θ to be minimally ℓ-suitable (Lemma 4.4.3).
  If $\theta/\ell \in \mathrm{End}(E_{\mathrm{init}})$ **then**
    $\theta \leftarrow \theta/\ell$.
    $c \leftarrow c + 1$
  else
    break *the* ***While*** *loop*
Return *θ as a linear combination,* $r - c$

of 1728. Simply continue the loops instead of breaking them, returning a solution θ every time one is found.

Remark 4.6.2. If one wishes to find *all* possible solutions, remove the requirements that D be a prime congruent to 1 (mod 4), although this will adversely affect runtime (Cornacchia's algorithm will require factoring D). Furthermore, we must make sure Cornacchia's algorithm returns *all* solutions, and we must include solutions obtained by changing the sign of x on each solution already obtained. We must also be aware that later solutions may fail to be ℓ-primitive; these can be discarded. With these adjustments, every orientation of the form specified will eventually be found by the algorithm (not every θ, but every embedding of $\mathcal{O}'$ into $\mathrm{End}(E_{\mathrm{init}})$ for all $\mathcal{O}'$) – see the proof of Proposition 4.6.1 for relevant details.

Because of the primality testing step, the algorithm terminates only heuristically. We separately prove its correctness (if it returns) and then give a heuristic runtime.

In what follows, write $\Delta := \Delta_{\mathcal{O}}$ for convenience.

Proposition 4.6.1. *Any solution returned by Algorithm 4.6.1 is correct.*

Proof. We attempt to solve the problem for each fixed r increasing from $r = 0$.

If the order $\mathcal{O}'$ of index ℓ^r in $\mathcal{O}$ has even discriminant (namely $\Delta\ell^{2r}$), then we seek an element of reduced trace zero and reduced norm $-\Delta\ell^{2r}/4$. Such an element must generate $\mathcal{O}'$, and $\mathcal{O}'$ must contain a generator of this form. Write the element as $\theta = \frac{x}{2}\mathbf{i} + \frac{y}{2}\mathbf{j} + \frac{z}{2}\mathbf{k}$. Then, simplifying the equation, the norm condition is

$$x^2 + py^2 + pz^2 = -\Delta\ell^{2r}.$$

Any solutions must have $x^2 < \sqrt{-\Delta\ell^{2r}}$, and for a valid x, solutions y and z are found by Cornacchia's algorithm applied to

$$y^2 + z^2 = (-\Delta\ell^{2r} - x^2)/p.$$

In order to be contained in $\mathrm{End}(E_{\mathrm{init}})$, we require $x \equiv z \pmod 2$ and y is even. The variable r is incremented if no solution exists, or if Cornacchia's algorithm is not applied because D is not a prime congruent to 1 (mod 4) (in which case we may miss solutions).

If $\Delta\ell^{2r}$ is odd, we instead seek an element of reduced trace 1 and reduced norm $(-\Delta\ell^{2r}+1)/4$. Such an element will again necessarily generate $\mathcal{O}'$, and $\mathcal{O}'$ must contain a generator of this form. Writing the element as $\theta = \frac{1}{2} + \frac{x}{2}\mathbf{i} + \frac{y}{2}\mathbf{j} + \frac{z}{2}\mathbf{k}$, after slightly simplifying the norm equation, we must solve the same equation as before:

$$x^2 + py^2 + pz^2 = -\Delta\ell^{2r}.$$

However, in order to lie in $\mathrm{End}(E_{\mathrm{init}})$, such an element must satisfy the conditions that $x \equiv z \pmod 2$ and y is *odd* (note the parity difference). The rest of this case is as above.

If θ is not ℓ-primitive, the algorithm will translate and divide by ℓ until it is. □

For the runtime analysis, and the assertion that the algorithm returns a solution at all, we need a heuristic similar to that used for torsion-point attacks [35, Heuristic 1] and the KLPT algorithm [54, Section 3.2].

Heuristic 4.6.3. *Fix integers $D > 0$ and $b > 0$, and a prime p coprime to Db that splits in the real quadratic field $\mathbb{Q}(\sqrt{D})$. Ranging through pairs*

$$\left\{(r,x) : 0 < x, x^2 < Db^{2r}, 0 \le r, Db^{2r} - x^2 \equiv 0 \pmod p\right\},$$

consider the value

$$N(r,x) = \frac{Db^{2r} - x^2}{p}.$$

The probability that $N(r,x)$ is a prime congruent to 1 modulo 4 is at least $O(1/(\log D \log N(r,x)))$, where the implied constant is independent of p, D, and b.

We now give a brief justification for this heuristic by passing to the real quadratic field $\mathbb{Q}(\sqrt{D})$. Write $D = f^2 d$ where $d > 0$ is squarefree. We have $N(r,x) = q$ if and only if $\pm pq = N(x + fb^r\sqrt{d})$. Hence we need to estimate the probability, given that $N(x + fb^r\sqrt{d})$ is divisible by p, that it is of the form $\pm pq$ for some other prime q. We analyse instead the probability, for $\alpha \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ (having no assumptions on the form of α), given that $N(\alpha)$ is divisible by p, that it is of the form $\pm pq$ for some prime q. Heuristically, we assume that this will be the same probability.

Given that p splits, we have a prime $\mathfrak{p}$ above p in the maximal order of $\mathbb{Q}(\sqrt{d})$. Hence $N(\alpha)$ has the form $-pq$ if and only if there is a prime ideal $\mathfrak{q}$ of norm q satisfying $\mathfrak{pq} = (\alpha)$ (or $\overline{\mathfrak{p}}\mathfrak{q} = (\alpha)$). If $p \mid N(\alpha)$, then replacing $\mathfrak{p}$ with $\overline{\mathfrak{p}}$ if necessary, this occurs if and only if the integral ideal $(\alpha)\mathfrak{p}^{-1} \in [\mathfrak{p}]^{-1}$ has norm q.

Therefore, we estimate the probability that integral elements in $[\mathfrak{p}]^{-1}$ of size X have prime norm. This is bounded below by the probability that integers of size X have a norm which is a prime represented by the class $[\mathfrak{p}]^{-1}$. This in turn is bounded below by $\frac{1}{h \log X}$ where h is the class number of $\mathbb{Q}(\sqrt{d})$. We apply this estimate with $X = N(r, x)$.

Finally, following the Cohen-Lenstra heuristics for real quadratic fields, it may be reasonable to expect the class number $h_{\mathbb{Q}(\sqrt{d})}$ to have an expected value bounded by $O(\log d)$, since the number of prime factors of d is around $\log \log d$ (see [101] for a result for prime discriminants and recall that the 2-part of the class group is controlled by the number of prime factors of d).

Heuristic 4.6.3 has been confirmed numerically in some small cases; we will consider this heuristic in more detail in [4]. The corresponding heuristic, in the case of the KLPT norm equation, has been verified by Wesolowski [100]; it would be nice to know if similar methods apply here.

Proposition 4.6.2. *Suppose Heuristic 4.6.3 holds and Δ is coprime to p. If $|\Delta| < p^2$, then Algorithm 4.6.1 returns a solution of norm at most $p^2 \log^{2+\epsilon}(p)$ with $r = O(\log p)$ in time $O(\log^{6+\epsilon}(p))$. If instead $|\Delta| > p^2$, then the algorithm will return a solution with $r = O(1)$ and norm $O(|\Delta|)$ in time $O(\sqrt{|\Delta|} \log^{4+\epsilon}(\Delta)(\log p)p^{-1})$.*

Running the algorithm continuously, subsequent solutions should be found in the same runtime, with r expected to increase by 1, and their norms expected to increase by a constant factor of ℓ^2 at each subsequent solution.

Proof. Suppose r is of size at most $u \log_\ell p$, where u is positive (otherwise r is not positive). Then $\sqrt{-\Delta \ell^{2r}} \leq |\Delta|^{1/2} p^u$. Thus, we expect to iterate the **While** loop at Step 5 at most $X(\Delta, u) := \lceil |\Delta|^{1/2} p^{u-1} \rceil + 1$ times. Each time we enter the loop, we obtain a value $D = (-\Delta \ell^{2r} - x^2)/p$ of size $\leq pX(\Delta, u)^2$. The probability that D is prime and $1 \pmod 4$ is heuristically $1/(4 \log(p^{1/2} X(\Delta, u)))$ (Heuristic 4.6.3). Hence we expect to reach Cornacchia's algorithm once u is large enough such

that

$$X(\Delta, u) \geq 4 \log(p^{1/2} X(\Delta, u)) > 1.$$

Reaching it will terminate the algorithm. This is a mild condition, satisfied asymptotically when $X(\Delta, u) \geq (\log p)^{1+\epsilon}$. In fact, it suffices to take $\sqrt{|\Delta|} p^u \geq p \log^{1+\epsilon}(p)$, or equivalently,

$$u \log p \geq \log p - \frac{1}{2} \log |\Delta| + (1+\epsilon) \log \log p. \tag{4.6.1}$$

In particular, $u > 1$ is always enough, and if $|\Delta| > p^{2+\epsilon}$, then any positive value for u will suffice. (An informal explanation of this behaviour: even for a volcano with a trivial rim, distance $(1+\epsilon) \log p$ down its sides is enough to capture all j-invariants. At the same time, if Δ is large enough that the rim likely captures all j-invariants, then we needn't descend the volcano at all.) This shows that the algorithm needs to increase r at most $O(\log p)$ times before it reaches Cornacchia's algorithm.

For $|\Delta| \leq p^{2+\epsilon}$, the optimal value of u is given by (4.6.1). However, since u cannot be negative, when $|\Delta| > p^{2+\epsilon}$, the optimal value of u is 0. (Again, informally: the class group will be of size $\approx \sqrt{|\Delta|} > p$, and we will find all $\approx \frac{p}{12}$ supersingular j-invariants already on the rim of an isogeny volcano.)

We first determine the overall runtime in terms of $X(\Delta, u)$ and p. The primality test can be run in time $O(\log^{4+\epsilon} D)$ for example, using the Miller-Rabin algorithm [76, Section 2]. This algorithm is probabilistic, so there is a negligible possibility that Cornacchia's algorithm may fail on false positives.

Once D is a prime congruent to 1 (mod 4), we must find a square root of -1 with which to run Cornacchia's algorithm. There is a nice analysis of this exact situation in [41, Section 3.1], which concludes that it takes probabilistic time $\widetilde{O}(\log^2 D)$, which is negligible compared to the primality testing.

Thus, for the final runtime, we increment r at most $O(\log p)$ times, running a primality test of cost $O(\log^{4+\epsilon} D)$ at most $O(X(\Delta, u))$ times for each r, before reaching a point where Cornacchia's algorithm is invoked. Using $D \leq p X(\Delta, u)^2$, this gives runtime $O(X(\Delta, u)(\log p)(\log p + 2 \log X(\Delta, u))^{4+\epsilon})$.

In the case of large $|\Delta| > p^{2+\epsilon}$, we put $u = 0$ and obtain $X(\Delta, u) = O(\sqrt{|\Delta|}/p)$ and

asymptotically $X(\Delta, u) > p^\epsilon$. This yields a runtime of $O(\sqrt{|\Delta|}\log^{4+\epsilon}(\Delta)(\log p)p^{-1})$. In this case $r = O(1)$ and the norm of the solution is bounded by $O(|\Delta|)$.

In the case of small $|\Delta| \leq p^2$, we optimize u according to (4.6.1) and obtain $X(\Delta, u) = O(\log^{1+\epsilon}(p))$ and asymptotically $X(\Delta, u) < p$. This gives $O(\log^{6+\epsilon}(p))$. At the same time, the norm of the solution found is bounded by $|\Delta|\ell^{2r} \leq p^2 X(\Delta, u)^2 \leq p^2 \log^{2+2\epsilon}(p)$.

Once r has reached $O(\log p)$, we expect solutions for each r with high probability. Therefore, running the algorithm continuously, subsequent solutions should be found in the same runtime as the first, and their sizes should be increasing by an expected constant factor of ℓ^2 at each subsequent solution. □

Example 4.6.4 (**Computing an orientation for the initial curve** via Algorithm 4.6.1)**.** We return to our working example $p = 179$, $\Delta = -47$, $\ell = 2$, and $E_{1728} : y^2 = x^3 - x$. Note that $\log_\ell(p) \sim 7.48$, so that we expect the algorithm to succeed reliably once $r = 7$ or 8, if not earlier. Beginning with $r = 0$, in Step 4 we compute the smallest positive x such that $x^2 = 47 \pmod{179}$, namely $x = 88$. As $x = 88$ exceeds $\sqrt{47} \approx 6.9$, we return to Step 3 and increment r to $r = 1$. This reflects the fact that the curve E_{1728} does not admit a $\mathbb{Q}(\sqrt{-47})$-orientation on the rim. Continuing, we find the smallest positive integer x such that $x^2 \equiv 188 \pmod{179}$, namely $x = 3$. As $x = 3 < \sqrt{47 \cdot 4} \approx 13.7$, we define $D = (47 \cdot 4 - 3^2)/179 = 1$ in Step 6. Cornacchia's algorithm returns $1^2 + 0^2 = 1$. We obtain the element $\frac{3\mathbf{i}+\mathbf{k}}{2} \in \mathrm{End}(E_{1728})$. This indicates (correctly) that E_{1728} admits an orientation on level $r = 1$ of the $\mathbb{Q}(\sqrt{-47})$-oriented 2-isogeny volcano, see the node with j-invariant 1728 in Figure 4.1. If we continue to run the algorithm, looking for pairs (r, θ) for r up to 8, we return three more pairs:

$$\left(r = 7, \theta = \frac{371}{2}\mathbf{i} + 29\mathbf{j} + \frac{13}{2}\mathbf{k}\right), \left(r = 8, \theta = \frac{153}{2}\mathbf{i} + 27\mathbf{j} + \frac{119}{2}\mathbf{k}\right), \left(r = 8, \theta = \frac{511}{2}\mathbf{i} + 41\mathbf{j} + \frac{95}{2}\mathbf{k}\right).$$

4.6.2 As an isogeny chain endomorphism

Since $\mathbf{i}$ and $\mathbf{j}$ are known endomorphisms which can be evaluated at points, any combination of these can also be evaluated at points. Therefore the output of Algorithm 4.6.1 can be fed into Algorithm 4.5.3, and an ℓ-suitable isogeny chain endomorphism will result. Thus, in poly-rep time (that is, depending on B, the powersmoothness bound), we can obtain the output of Algorithm 4.6.1

as an isogeny-chain endomorphism.

4.6.3 Curves other than $j = 1728$

Algorithm 4.6.1 can be adapted to work for certain curves E_{init} other than the curve with $j = 1728$. In particular, if the endomorphism ring $\text{End}(E)$ of a curve E defined over $\mathbb{F}_p$ is of the form $\mathcal{O} + \mathbf{j}\mathcal{O}$, where $\mathbf{j}$ is the Frobenius endomorphism and $\mathcal{O}$ is a quadratic order, then the adaptation of Algorithm 4.6.1 is clear, where we use the principal norm form of $\mathcal{O}$ in place of x^2+y^2. As before, this will reduce to Cornacchia's algorithm. Instead of primes that are 1 (mod 4), we seek primes that split in the field and are coprime to the conductor of $\mathcal{O}$; this requires a Legendre symbol computation. The runtime is essentially unchanged. This adaptation follows the discussion in [54, Section 3.2].

4.6.4 Heuristics

We now formalize a heuristic about the behaviour of Algorithm 4.6.1 needed for what follows. This is a version of Heuristic 4.3.3 specific to the algorithm we use.

Heuristic 4.6.5. *Let $\mathcal{O}$ be a quadratic order. Let $\mathcal{S}$ be the finite union of $\mathcal{O}'$-cordilleras where $\mathcal{O}' \supseteq \mathcal{O}$. Then Algorithm 4.6.1 running continuously will (i) eventually produce solutions on every volcano of $\mathcal{S}$, and (ii) produce solutions which are approaching the distribution described in Heuristic 4.3.3 (i.e. with probabilities proportional to the number of descending edges from the rim).*

If $\mathcal{S}$ has only one volcano, this heuristic is immediate as long as the algorithm produces infinitely many solutions (which happens by Proposition 4.6.2, under heuristic assumptions from Section 4.3.6). If Algorithm 4.6.1 returned *all* orientations of 1728, then this heuristic would follow directly from Heuristic 4.3.3. The difficulty is that it finds only those solutions where the primality testing step succeeds. In other words, we cannot rule out the unlikely possibility that the primality condition causes all the orientations of 1728 to be missed on some individual volcano. Thus, we seem to require a version of Heuristic 4.6.3 which asserts that the primality is independent of whether the eventual solution is on any fixed volcano of the cordillera. We consider Heuristic 4.6.5 more closely in the companion paper [4].

4.7 Supporting algorithms for walking on oriented curves

4.7.1 Computing an ℓ-primitive endomorphism

Recall from Definition 4.4.2 that an endomorphism θ is ℓ-primitive if the associated orientation is ℓ-primitive. If θ is chosen to be ℓ-suitable, then equivalently, θ is ℓ-primitive if it cannot be divided by $[\ell]$ in $\mathrm{End}(E)$ (Lemma 4.4.2). Therefore, given θ, we can translate it to become ℓ-suitable and then divide by $[\ell]$ as often as possible to obtain an ℓ-primitive endomorphism.

Algorithm 4.7.1: Computing an ℓ-primitive endomorphism given an endomorphism.

Input: A traced endomorphism (E, θ, t, n) providing the functionality of Section 4.5.1.
Output: A traced endomorphism (E, θ', t', n') which is ℓ-primitive, and the ℓ-valuation of the index $[\mathbb{Z}[\theta'] : \mathbb{Z}[\theta]]$.

If $t^2 - 4n$ *is* ℓ*-fundamental* **then**
  Return (E, θ, t, n) and 0.
$(E, \theta, t, n) \leftarrow$ an ℓ-suitable translate of (E, θ, t, n)
$c \leftarrow 0$
While $[\ell] \mid \theta$ **do**
  $(E, \theta, t, n) \leftarrow (E, \theta/[\ell], t/\ell, n/\ell^2)$
  $c \leftarrow c + 1$
  If $t^2 - 4n$ *is* ℓ*-fundamental* **then**
    Return (E, θ, t, n) and c.
  $(E, \theta, t, n) \leftarrow$ an ℓ-suitable translate of (E, θ, t, n)
Return (E, θ, t, n) and c.

Proposition 4.7.1. *Algorithm 4.7.1 is correct, and runs in poly-rep time (see Definition 4.5.9).*

Proof. If $t^2 - 4n$ is ℓ-fundamental, then the conductor of the quadratic order generated by θ is not divisible by ℓ; in this case θ is already ℓ-primitive. In order to check if any order of superindex ℓ contains $\mathbb{Z}[\theta]$ within $\mathrm{End}(E)$, we first translate θ to be ℓ-suitable, and then check whether it is divisible by $[\ell]$ within $\mathrm{End}(E)$. If it is, we divide by ℓ and repeat.

For runtime, the algorithm translates to an ℓ-suitable translate, tests for divisibility by ℓ, and divides by ℓ, at most a polynomial number of times (since we assume that the discriminant of $\mathbb{Z}[\theta]$ is bounded by a power of p; see Section 4.5.1). □

Example 4.7.1 (Computing an ℓ-primitive endomorphism via Algorithm 4.7.1**).** We apply

Algorithm 4.7.1 to the output of Example 4.5.8, namely $(E_{1728}, \theta', t', n')$ where $\theta' = \varphi_{171} \circ \varphi_{1728}, t' = 2, n' = 48$. This is not at the rim, but is already ℓ-suitable. We find $[2] \nmid \theta'$ by evaluating on $E_{1728}[2]$; hence we return the input unchanged.

4.7.2 Rim walking via the class group action

In the case that an orientation is available, one can walk the rim of the oriented ℓ-isogeny volcano using the class group action. Walking a cycle generated by the class group action was first described in Broker-Charles-Lauter [17] in the case of ordinary curves, which carry an orientation by Frobenius. This was later used in CSIDH [18], and it was remarked that it extends to orientations by $\mathbb{Q}(\sqrt{-np})$ in Chenu-Smith [22]. In this section we provide a generalization of the same algorithm to arbitrary orientations. The algorithm walks the rim from a specified start curve in an arbitrary direction until it encounters a specified end curve. This path is computed using the action of the class group on the *oriented* curves in the rim of the *oriented* volcano. As such, it requires knowledge of the orientation, so the steps of the algorithm must pull the orientation (i.e. the endomorphism) along with them. More precisely, the ideal we wish to apply to (E, θ) is given in terms of θ, so that one can use the methods of Broker-Charles-Lauter [17, Section 3] with θ in place of Frobenius. One can apply the Waterhouse twist of θ, and divide by ℓ to carry along θ in the computation.

The algorithm works by applying the action of $\mathrm{Cl}(\mathcal{O})$ to a rim of elements primitively oriented by a quadratic order $\mathcal{O}$. In fact, using $\mathrm{Cl}(\mathcal{O})$ works just as well if the rim is primitively oriented by $\mathcal{O}' \supseteq \mathcal{O}$, where $\ell \nmid [\mathcal{O}' : \mathcal{O}]$. This allows us to walk on any rim associated to an ℓ-fundamental discriminant Δ, without knowing for sure that the orientation is primitive with respect to Δ. See Proposition 4.3.2.

Calling Algorithm 4.7.2 on identical input curves (i.e. $(E_{\mathrm{init}}, \iota_{\mathrm{init}}) = (E_{\mathrm{target}}, \iota_{\mathrm{target}})$ yields the entire rim of the ℓ-oriented isogeny graph.

Proposition 4.7.2. *Algorithm 4.7.2 is correct. Each step of the rim walk has poly-rep runtime. The number of steps is bounded $O(h_{\mathcal{O}})$. Furthermore, if θ is in prime-power isogeny chain form with any powersmoothness bound B, then each step of the rim-walk has runtime polynomial in B.*

Proof. If $\ell \mid t^2 - 4n$, then either we are not at the rim, or the field discriminant is not coprime

Algorithm 4.7.2: Walking along the rim of the oriented supersingular ℓ-isogeny graph

Input: An ℓ-primitive traced endomorphism $(E_1, \theta_1, t_1, n_1)$ providing the functionality of Section 4.5.1, and a target curve E_2.

Output: If E_1 and E_2 are on the same volcano rim in the oriented isogeny graph for the field $\mathbb{Q}(\theta)$, with discriminant coprime to ℓ, the algorithm returns a path of oriented horizontal ℓ-isogenies from $(E_1, \theta_1, t_1, n_1)$ to a vertex with curve E_2. Otherwise returns FAILURE.

If $\ell \mid t^2 - 4n$ **then**
  Return FAILURE.
$H \leftarrow []$.
If $j(E_1) = j(E_2)$ **then**
  Return H.
Compute $\mathcal{O} \cong \mathbb{Z}[\theta]$, the quadratic order generated by θ (using trace and norm), together with an explicit isomorphism given in the form of $\alpha_\theta \in \mathcal{O}$ corresponding to θ.
If ℓ *is inert in* $\mathcal{O}$ **then**
  Return FAILURE.
Compute $\tau \in \mathcal{O}$ such that $\mathfrak{l} = (\ell, \tau)_\mathcal{O}$ is a prime ideal of $\mathcal{O}$ above ℓ.
Compute $a, b \in \mathbb{Z}$ so that $\tau = a + b\alpha_\theta$.
$(E, \theta, t, n) \leftarrow (E_1, \theta_1, t_1, n_1)$.
repeat
  Compute $E[\ell]$.
  Compute $E[\mathfrak{l}] \leftarrow E[\ell] \cap \ker(a + b\theta)$ by evaluating $a + b\theta$ on $E[\ell]$.
  Use Vélu's algorithm to compute the ℓ-isogeny $\nu : E \to E'$ with kernel $E[\mathfrak{l}]$.
  $(E, \theta, t, n) \leftarrow (E', \nu \circ \theta \circ \widehat{\nu}, t\ell, n\ell^2)$.
  $(E, \theta, t, n) \leftarrow (E, \theta/[\ell], t/\ell, n/\ell^2)$.
  Append $(\nu, (E, \theta, t, n))$ to H.
until $(j(E), \theta, t, n) = (j(E_1), \theta_1, t_1, n_1)$ *or* $j(E) = j(E_2)$
If $j(E) = j(E_2)$ **then**
  Return H
else
  Return FAILURE

to ℓ. If $j(E_1) = j(E_2)$, we have already completed our task. Assuming neither of those cases, we compute the abstract quadratic order $\mathcal{O}$ generated by θ using its minimal polynomial, and associate an abstract element α_θ to θ.

The volcano rim in question is contained in $\mathrm{SS}_{\mathcal{O}'}$ for some $\mathcal{O}' \supseteq \mathcal{O}$, where the index of containment $f = [\mathcal{O}' : \mathcal{O}]$ is coprime to ℓ (by ℓ-primitivity). If ℓ is inert in $\mathcal{O}$, then it is also inert in $\mathcal{O}'$. Hence the rim of the associated volcano is trivial; since $j(E_1) \neq j(E_2)$, this indicates there is no valid path to be found. Otherwise, ℓ is split or ramified in $\mathcal{O}$, so we factor it and compute a and b and τ as in the algorithm. Namely, we have the factorzation $\ell\mathcal{O} = (\ell, \tau)_{\mathcal{O}}(\ell, \overline{\tau})_{\mathcal{O}}$ in $\mathcal{O}$. Then $\ell\mathcal{O}' = (\ell, \tau)_{\mathcal{O}'}(\ell, \overline{\tau})_{\mathcal{O}'}$ in $\mathcal{O}'$. Therefore, the isogeny computed is the action of the ideal $\mathfrak{l} \in \mathrm{Cl}(\mathcal{O}')$ lying above ℓ in $\mathcal{O}'$ on $\mathrm{SS}_{\mathcal{O}'}$ as desired, which is thus a horizontal isogeny. The **repeat** clause walks the rim step by step.

We stop if we meet E_2 or return to our (oriented) starting point. The latter occurs only if we have walked the entire rim, which means E_2 was not on that rim.

For runtime, all individual steps are polynomial, except for calls to evaluate at ℓ-torsion points, Waterhouse twist and divide by ℓ. The number of repeats is equal to the path length from E_1 to E_2 along the rim. The size of the rim is $O(h_{\mathcal{O}})$ (Section 4.3.4).

For the final statement, note that no ℓ-suitable translation is needed in the algorithm. In fact, the norm of the endomorphism remains constant as one walks the rim. □

Example 4.7.2 (**Walking along the rim of the oriented supersingular ℓ-isogeny graph** via Algorithm 4.7.2)**.** As before, we have $K = \mathbb{Q}(\sqrt{-47})$. We use Algorithm 4.7.2 on input $\ell = 2$, $(E_{22}, \theta_{22}, t_{22}, n_{22})$ and target curve E_{22} to compute the entire rim of the oriented 2-isogeny volcano for purposes of demonstration. The endomorphism θ_{22} is a primitive $\mathcal{O}_K$-orientation, so the curve E_{22} lies on the rim of a $\mathcal{O}_K$-oriented isogeny volcano. Step 9 computes the prime ideal $\ell = (2, \omega)_{\mathcal{O}_K}$. In Step 13, we compute $E_{22}[2] = \{\mathcal{O}_{E_{22}}, (2, 0), (156i + 178, 0), (23i + 178, 0)\}$. We obtain $E_{22}[\mathfrak{l}] = \langle(156i + 178, 0)\rangle$ in Step 14. Velu's formulas in Step 15 compute the isogeny $\varphi_{22} : E_{22} \to E_{99i+107}$. The codomain of φ_{22} is $E_{99i+107} : y^2 = x^3 + (26i + 88)x + (141i + 104)$. In Step 16, we compute the traced endomorphism $(E_{99i+107}, \theta_{99i+107}, t_{99i+107}, n_{99i+107})$ with $\theta_{99i+107} := \frac{1}{2}\varphi_{22} \circ \theta_{22} \circ \hat{\varphi}_{22}$, an endomorphism of degree 12. Step 18 appends the isogeny φ_{22} and the traced endomorphism $(E_{99i+107}, \theta_{99i+107}, t_{99i+107}, n_{99i+107})$ to H.

In the next rim step, starting with $(E_{99i+107}, \theta_{99i+107}, t_{99i+107}, n_{99i+107})$, we compute the isogeny

$$\varphi_{99i+107} : E_{99i+107} \to E_{5i+109}.$$

The isogeny $\varphi_{99i+107}$ and traced endomorphism $(E_{5i+109}, \theta_{5i+109}, t_{5i+109}, n_{5i+109})$ are appended to H in Step 18.

In the next rim step, we find the isogeny $\varphi_{5i+109} : E_{5i+109} \to E_{174i+109}$ and corresponding traced endomorphism $(E_{174i+109}, \theta_{174i+109}, t_{174i+109}, n_{174i+109})$ with $\theta_{174i+109} = \frac{1}{2}(\varphi_{5i+109}) \circ \theta_{5i+109} \circ \hat{\varphi}_{5i+109}$.

A fourth step along the rim produces the isogeny $\varphi_{174i+109} : E_{174i+109} \to E_{80i+107}$ and traced endomorphism $(E_{80i+107}, \theta_{80i+107}, t_{80i+107}, n_{80i+107})$.

The final step along the rim produces the isogeny $\varphi_{80i+107} \to E'_{22}$ with codomain $E'_{22} : y^2 = (125i+98)x + (84i+152)$ and induced traced endomorphism $(E'_{22}, \theta'_{22}, t'_{22}, n'_{22})$. The codomain E'_{22} is isomorphic to E_{22} via an isomorphism ρ, and we use the same isomorphism ρ to confirm that E'_{22} and E_{22} are in fact isomorphic as oriented curves by computing $\theta'_{22} = \rho \circ \theta_{22} \circ \rho^{-1}$.

Algorithm 4.7.2 terminates and returns the rim cycle

$$E_{22} \xrightarrow{\varphi_{22}} E_{99i+107} \xrightarrow{\varphi_{99i+107}} E_{5i+109} \xrightarrow{\varphi_{5i+109}} E_{174i+109} \xrightarrow{\varphi_{174i+109}} E'_{22} \cong E_{22}$$

of length 5 (see the green rim cycle in Figure 4.1). Indeed, K has class number 5, and the ideal class of $\mathfrak{l}$ generates the class group of K.

4.7.3 Ascending to the rim using an orientation

The other major component of navigating the supersingular ℓ-isogeny graph using an orientation is to walk to the rim. We can use Proposition 4.4.2 to determine the ascending direction and walk up. This is described in Algorithm 4.7.3. The number of steps to the rim is expected to be $\log(p)$ in general; see Section 4.3.6.

Proposition 4.7.3. *Algorithm 4.7.3 is correct and has poly-rep runtime times the distance to the rim.*

Algorithm 4.7.3: Walking to the rim of the oriented ℓ-isogeny graph.

Input: An ℓ-primitive traced endomorphism (E, θ, t, n) providing the functionality of Section 4.5.1.

Output: The shortest path from (E, θ, t, n) to the rim of the oriented ℓ-isogeny volcano upon which (E, θ, t, n) lies.

1 $H \leftarrow []$.
2 $k \leftarrow \left\lfloor \frac{\nu_\ell(t^2-4n)}{2} \right\rfloor$.
3 **If** $\ell = 2$ *and* $(t^2 - 4n)/2^{2k} \not\equiv 1 \pmod 4$ **then**
4 $\quad k \leftarrow k - 1$
5 **For** $j = 1, \ldots, k$ **do**
6 $\quad$ Compute $E[\ell]$.
7 $\quad (E, \theta, t, n) \leftarrow$ an ℓ-suitable translate of (E, θ, t, n).
8 $\quad$ Compute a generator P for $E[\ell] \cap \ker(\theta)$.
9 $\quad$ Use Vélu's algorithm to compute the ℓ-isogeny $\nu : E \to E'$ with kernel $\langle P \rangle$.
10 $\quad (E, \theta, t, n) \leftarrow (E', \nu \circ \theta \circ \hat{\nu}, t\ell, n\ell^2)$
11 $\quad (E, \theta, t, n) \leftarrow (E, \theta/[\ell^2], t/\ell^2, n/\ell^4)$
12 $\quad$ Append $(\nu, (E, \theta, t, n))$ to H.
13 **Return** H

Proof. The number of steps to the rim is given by the number of times ℓ^2 divides the discriminant of θ (we assume θ is ℓ-primitive); this is k in Step 2. We translate θ to be ℓ-suitable, which implies that $\nu \circ \theta \circ \widehat{\nu}$ can be divided by $[\ell]$ twice when ν is ascending. Since there is no horizontal direction (by the choice of k in Step 2), there exists a non-trivial $P \in E[\ell] \cap \ker(\theta)$. This gives the ascending isogeny by Proposition 4.4.2. Once we have found the ascending isogeny, we divide the Waterhouse twist of θ by $[\ell]^2$ (Step 11), and the result is ℓ-primitive, in preparation for the next loop iteration. For each iteration of the **For** loop, the work is clearly poly-rep. □

Example 4.7.3 (**Walking to the rim of the oriented ℓ-isogeny graph for rationally represented endomorphisms** via Algorithm 4.7.3)**.** We apply Algorithm 4.7.3 to the output of Step 4 of Example 4.8.2, namely E_{120} and θ_{120} having $t_{120} = 0$, $n_{120} = 188$. We find that we expect to take two steps to the rim. Since θ_{120} is already 2-suitable, we evaluate it on $E_{120}[2]$ and obtain the kernel $\langle (121i + 4, 0) \rangle$ for the ascending isogeny. The codomain is E_{171}. Waterhouse twisting and dividing by $[2]$ twice, we obtain an endomorphism θ' which is not 2-suitable, but Lemma 4.4.3 shows that $\theta_{171} := \theta' + [1]$ is 2-suitable. The second ascending step is similar; this has kernel $\langle (121i + 131, 0) \rangle$ and codomain E_{5i+109}. The two ascending steps are in blue in Figure 4.1.

Example 4.7.4 (**Walking to the rim of the oriented ℓ-isogeny graph for isogeny chain**

endomorphisms via Algorithm 4.7.3). We begin with input $(E_{1728}, \varphi_{171} \circ \varphi_{1728}, 2, 48)$, from Step 8 of Example 4.8.2. This will require one step to the rim and is already [2]-suitable. Evaluating on $E_{1728}[2]$, we obtain a kernel of $\langle (178, 0) \rangle$ for the ascending isogeny; the codomain is E_{22}. Waterhouse twisting yields an isogeny-chain which is not prime-power refactored, namely $\varphi'_{1728} \circ \varphi_{171} \circ \varphi_{1728} \circ \widehat{\varphi'}_{1728}$ having component degrees 2, 3, 16, 2, respectively. We could apply Algorithm 4.5.1, but we proceed in a slightly more expedient manner. We rewrite $\varphi'_{1728} \circ \varphi_{171}$, having degrees 2 and 3, respectively, in a form having degrees 3 and 2, respectively. Thus, we evaluate $\varphi'_{1728} \circ \varphi_{171}$ on the 2-torsion to obtain the kernel $\langle (29i + 50, 0) \rangle$ determining $\varphi'_{171} : E_{171} \to E_{174i+109}$. Then we apply φ'_{171} to the generator of $\ker(\varphi'_{1728} \circ \varphi_{171}) \cap E_{171}[3] = \langle (128i + 164, 28i + 90) \rangle$ to obtain a kernel for which Vélu gives $\varphi_{174i+109} : E_{174i+109} \to E_{22}$. We obtain the refactored isogeny chain $\varphi_{174i+109} \circ \varphi'_{171} \circ \varphi_{1728} \circ \widehat{\varphi'}_{1728}$. We can then divide the 2-power degree component $\varphi'_{171} \circ \varphi_{1728} \circ \widehat{\varphi'}_{1728}$ by [2] twice and let $\varphi'_{22} := \varphi'_{171} \circ \varphi_{1728} \circ \widehat{\varphi'}_{1728}/[4]$. Replacing this in our isogeny chain above, we now have an isogeny that gives the one step up to the rim (see the red step in Figure 4.1):

$$(E_{1728}, \varphi_{171} \circ \varphi_{1728}, 2, 48) \xrightarrow{\varphi'_{1728}} (E_{22}, \varphi_{174i+109} \circ \varphi'_{22}, 1, 12).$$

4.7.4 Ascending and walking the rim using the endomorphism ring

When we find an orientation of $j = 1728$, we have more information than just the specified orientation: we also know the endomorphism ring. This extra information allows us to navigate the oriented graph in polynomial time using known algorithms.

Specifically, with Algorithm 4.7.4 given here, we can walk up the volcano and traverse the rim (being careful not to back-track by comparing to our previous steps), where each step is polynomial in $\log p$ and the length of the representation of θ. To get started, we use E_{init} as the curve defining $B_{p,\infty}$ as in [100], and take the path P to be the trivial path.

Proposition 4.7.4. *Under GRH, Algorithm 4.7.4 is correct and runs in expected polynomial time in the following quantities:* $\log p$*, the size of the representation of* θ*, and the length of the path* P*.*

Proof. Each of the cited algorithms runs in the time specified under GRH. We determine which steps are ascending or horizontal by testing whether $\beta/\ell^{s+1}, \beta/\ell^{s+2} \in \mathfrak{O}$, by Proposition 4.4.1.

Algorithm 4.7.4: Extending a path from E_{init} by an ascending or horizontal step.

Input: A fixed endomorphism $\theta \in \text{End}(E_{\text{init}})$. An elliptic curve E and path P from E_{init} to E, with no descending steps, and s equal to the number of ascending steps in the path P.

Output: For each of the available horizontal or ascending steps $E \to E'$ (with regards to the orientation induced by θ), returns the data (E', P', s'), where P' is the path obtained from P by extending it by the extra step, and s' is the number of ascending steps in the path P'.

$H \leftarrow []$
For *each* ℓ*-isogeny* $\nu : E \to E'$ *departing* E **do**
  $P' \leftarrow$ the path formed by appending ν to P.
  $(\varphi : E_{\text{init}} \to E') \leftarrow$ the isogeny associated to the path P'.
  Compute a $\mathbb{Z}$-basis of the maximal quaternion order $\mathfrak{O}$ of E' and connecting ideal I between E_{init} and E' using [100, Algorithm 3] from the path P'.
  Compute $\text{End}(E')$ together with an isomorphism $\Psi : \text{End}(E') \to \mathfrak{O}$, using [100, Algorithm 6].
  $\beta \leftarrow \Psi(\varphi \circ \theta \circ \widehat{\varphi})$ (The ability to evaluate $\Psi(\varphi \circ \theta \circ \widehat{\varphi})$ for $\theta \in \text{End}(E_{\text{init}})$ is also obtained when [100, Algorithm 6] is performed in the last step.)
  $\beta \leftarrow \beta + T$ where $T \in \mathbb{Z}$ is chosen so that $\beta + T$ is the minimal ℓ^s-suitable translate of $\varphi \circ \theta \circ \widehat{\varphi}$ using Lemma 4.4.3.
  If $\beta/\ell^{s+1} \in \mathfrak{O}$ **then**
    $s' \leftarrow s$
    If $\beta/\ell^{s+2} \in \mathfrak{O}$ **then**
      $s' \leftarrow s' + 1$
    Append (E', P', s') to H.
Return H.

Since β is represented as a linear combination of a basis of $\mathrm{End}(E')$, this involves dividing the coefficients, which is polynomial time. □

4.8 Classical path-finding to $j = 1728$

We now present an algorithm which, given a suitable endomorphism on a curve in the supersingular graph, will find a path to the initial curve, under heuristic assumptions. An illustration of the method is given in Figure 4.1: we walk from the initial endomorphism to its rim; find an orientation of E_{init} and walk from that orientation of E_{init} to its rim; and hope to collide on the same rim.

Algorithm 4.8.1: Finding a path to E_{init}.

Input: A traced endomorphism (E, θ, t, n) providing the functionality of Section 4.5.1, where the discriminant of θ is coprime to p.

Output: A path in the ℓ-isogeny graph between E and E_{init}.

1 $(E, \theta, t, n) \leftarrow (E, \theta/[\ell^k], t/\ell^k, n/\ell^{2k})$ which is ℓ-primitive, using Algorithm 4.7.1.
2 $\Delta_\theta \leftarrow t^2 - 4n$.
3 $\Delta \leftarrow$ the ℓ-fundamental part of Δ_θ.
4 Call Algorithm 4.7.3 on input (E, θ, t, n) to produce an ascending path H_2 from (E, θ, t, n) to $(E_1, \theta_1, t_1, n_1)$ on the rim, i.e. where $\mathbb{Z}[\theta_1] \subseteq \mathrm{End}(E_1)$ is ℓ-fundamental.
5 Call Algorithm 4.7.2 on input $(E_1, \theta_1, t_1, n_1)$ to walk the rim until we encounter E_1 again, storing the j-invariants encountered as a list L.
6 **repeat**
7 Call Algorithm 4.6.1 on input Δ, to obtain a new solution $\theta_{\text{init}} = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$. (Algorithm 4.6.1 can be suspended and then resumed to find subsequent solutions; see Remark 4.6.1)
8 Using the methods of Section 4.7.4, produce an ascending path H_1 from E_{init} with endomorphism θ_{init} up to the rim, i.e. to a traced endomorphism $(E_0, \theta_0, t_0, n_0)$ having ℓ-fundamental $\mathbb{Z}[\theta_0] \subseteq \mathrm{End}(E_0)$.
9 **until** $E_0 \in L$ *or* $E_0^{(p)} \in L$
10 Compute H_{rim}, the path from E_1 to E_0 or $E_0^{(p)}$, using L.
11 **If** H_{rim} *joins* E_1 *to* E_0 **then**
12 $H \leftarrow H_2 H_{rim}^{-1} H_1^{-1}$, a path from E_{init} to E.
13 **else**
14 From H_1, compute the conjugate path $H_1^{(p)}$ from E_{init} to $E_0^{(p)}$.
15 $H \leftarrow H_2 H_{rim}^{-1} (H_1^{(p)})^{-1}$, a path from E_{init} to E.

Proposition 4.8.1. *Assume GRH, Heuristic 4.6.3, and the assumptions of Section 4.5.1. Con-*

sider an endomorphism $\theta \in \mathrm{End}(E)$ in rationally-represented or prime-power isogeny-chain form as described in Section 4.5.4, whose discriminant is coprime to p and has ℓ-fundamental part Δ satisfying $|\Delta| < p^2$. Write $\mathcal{O}_\Delta$ for the order of discriminant Δ. Algorithm 4.8.1 produces a path of length $O(\log p + h_{\mathcal{O}_\Delta})$ to E_{init} in the supersingular ℓ-isogeny graph, under Heuristic 4.6.5 part (i). The runtime is expected poly-rep times $O(h_{\mathcal{O}_\Delta})$, under Heuristic 4.6.5 part (ii). Furthermore, the following hold:

1. *If ℓ is inert in K, then the runtime improves to $h_{\mathcal{O}_\Delta}\,\mathrm{poly}(\log p)$+poly-rep, and the path length improves to $O(\log p)$.*
2. *If ℓ is inert in K and the discriminant of θ is already ℓ-fundamental, then the runtime improves to $h_{\mathcal{O}_\Delta}\,\mathrm{poly}(\log p)$ and the path length improves to $O(\log p)$.*
3. *If Δ is a fundamental discriminant, ℓ is split in K and a prime above ℓ generates the class group $\mathrm{Cl}(\mathcal{O}_\Delta)$, then the dependence on Heuristic 4.6.5 is removed.*

Proof. Let θ be the input to the algorithm. The pair (E, ι_θ), where $\iota_\theta : K \to \mathrm{End}(E)$ is the orientation given by θ, lies somewhere on the oriented ℓ-isogeny graph associated to K. More specifically, it lies on a volcano of the $\mathcal{O}$-cordillera for some order $\mathcal{O}$ whose discriminant divides the ℓ-fundamental discriminant Δ computed in Step 3. In other words, if we write $\mathcal{O}_\Delta$ for the order of discriminant Δ, then $\mathcal{O} \supseteq \mathcal{O}_\Delta$. Since all endomorphisms throughout the chapter are taken to have norm and discriminant at worst polynomial in p, the distance of (E, ι_θ) to the rim is at worst polynomial in $\log p$, and so walking to the rim (Step 4) is poly-rep by Proposition 4.7.3. Next, we walk around the rim; the runtime depends on the size of the rim and we defer that question to later in the proof.

When Δ is passed on to Algorithm 4.6.1 in Step 7, the result (which is returned in polynomial time by Proposition 4.6.2 under Heuristic 4.6.3) is an endomorphism of $\mathrm{End}(E_{\mathrm{init}})$ which gives an oriented elliptic curve lying somewhere on a volcano in an $\mathcal{O}'$-cordillera, where again $\mathcal{O}' \supseteq \mathcal{O}_\Delta$. (We do not necessarily have $\mathcal{O} = \mathcal{O}'$.) This has norm polynomial in p by Proposition 4.6.2. By Proposition 4.6.2 again, the distance to the rim is $O(\log p)$, so walking to the rim is expected polynomial time by Proposition 4.7.4. Hence each **repeat** iteration has expected polynomial time.

Walking to the rim in Step 8, E_0 lies on the rim of a volcano. This volcano is somewhere in the set of volcanoes $\mathcal{S}$ defined as the finite union of the $\mathcal{O}$-cordilleras for all $\mathcal{O} \supseteq \mathcal{O}_\Delta$. Note that its conjugate $E_0^{(p)}$ also lies on a rim in $\mathcal{S}$. Now E_1 also lies on a rim of $\mathcal{S}$. If E_0 (or $E_0^{(p)}$) and E_1 lie on the same rim, the algorithm will discover this. If not, then one continues the calls to Algorithm 4.6.1, and another endomorphism will be found. Under Heuristic 4.6.5 part (i), eventually one of these will produce E_0 or $E_0^{(p)}$ on the same rim as E_1. The algorithm will then succeed.

Let R denote the number of descending edges from the rim containing E_0, referred to in this paragraph as the *adjusted rim size* (which is bounded above and below by a constant multiple of the rim size). The sum of the adjusted rim sizes of all rims of $\mathrm{SS}_\mathcal{O}$ for all $\mathcal{O} \supseteq \mathcal{O}_\Delta$ is $O(H_{\mathcal{O}_\Delta})$ (Propositions 4.3.1 and 4.3.4). By Lemma 4.3.1, this is $O(h_{\mathcal{O}_\Delta}(\log\log|\Delta|)^2)) = O(h_{\mathcal{O}_\Delta})\,\mathrm{poly}(\log p)$. By Heuristic 4.6.5 part (ii), the number of times we must **repeat** is therefore $O(h_{\mathcal{O}_\Delta}/R)\,\mathrm{poly}(\log p)$. Each iteration performs Steps 7 and 8 and then checks membership in L. By Proposition 4.6.2, under GRH, Step 7 runs in polynomial time in $\log p$ and provides a solution θ_{init} of norm at most $p^2\log^{2+\epsilon} p$. Then θ_{init} can be written as a linear combination of the $\mathbb{Z}$-basis of $\mathrm{End}(E_{\mathrm{init}})$ with integer coefficients of size $O(\log p)$. Hence Step 8 requires a runtime polynomial in $\log p$ by Proposition 4.7.4; we store the j-invariant of the output for comparison to L. Thus, each iteration is expected polynomial time times $O(R)$ (to check membership in L). The walk to produce L in Step 5 takes at most $O(R)$ steps, each of which is poly-rep. Hence the runtime is poly-rep (for Step 4) plus $O(h_{\mathcal{O}_\Delta})\cdot\mathrm{poly}(\log p) + O(R)\cdot(\text{poly-rep})$.

This runtime is overall bounded by $O(h_{\mathcal{O}_\Delta})$ times poly-rep. But if ℓ is inert, then E_0 lies on a rim of size 1, so we don't need Step 5, and we have poly-rep plus $h_{\mathcal{O}_\Delta}\,\mathrm{poly}(\log p)$. If θ is already at the rim, then we don't need Step 4. Combined with inertness, this gives runtime $h_{\mathcal{O}_\Delta}\,\mathrm{poly}(\log p)$.

Finally, if Δ is a fundamental discriminant, ℓ is split and a prime above ℓ generates $\mathrm{Cl}(\mathcal{O}_\Delta)$, then there is only one volcano, obviating the need for Heuristic 4.6.5. □

The restriction that $|\Delta| < p^2$ is required to ensure that Algorithm 4.6.1 is heuristically polynomial time. If $|\Delta|$ is larger, and ℓ is inert, this failure of polynomial time could become the bottleneck. On the other hand, suppose ℓ is split in K. Under the Cohen-Lenstra heuristics, class groups are usually cyclic, and most elements of a cyclic group are generators, so with high

probability, Heuristic 4.6.5 will not be necessary.

It is also possible to use Algorithm 4.7.3 at Step 4, instead of the methods of Section 4.7.4. This results in a worse runtime, but removes the dependence on GRH.

Remark 4.8.1. One might hope to modify Algorithm 4.8.1 to produce a shorter path along with a square-root runtime improvement, by removing Step 5, and in each **repeat**, attempting to solve a vectorization problem between E_0 and E_{init}. Unfortunately, we cannot: the problem is that we do not know the correct quadratic order $\mathcal{O}$ with respect to which these oriented curves are primitively oriented. To overcome this, one might try to factor Δ and ascend with respect to any square factors, to guarantee that Δ is fundamental. Ascending would be polynomial in the largest squared prime factor of Δ, which could be very costly. An alternative that would usually work may be to try guessing Δ, working backward from the largest (and hence most likely) divisors. Just assuming Δ is fundamental would work much of the time.

Example 4.8.2 (**Finding a path to** E_{init} via Algorithm 4.8.1)**.** We again let $p = 179$, $\Delta = -47$, $\ell = 2$, and $E_{\text{init}} = E_{1728} : y^2 = x^3 - x$. As input, we consider the curve $E_{120} : y^2 = x^3 + (7i + 86)x + (45i + 174)$ with $j(E_{120}) = 120$, and a trace endomorphism given as $(E_{120}, \theta_{120}, t_{120}, n_{120})$ with $t_{120} = 20, n_{120} = 2^5 \cdot 3^2$ and

$$\theta_{120}(x, y) = \left(\frac{(122i + 167)x^{288} + (17i + 68)x^{287} + \cdots + 174i + 157}{x^{287} + (78i + 156)x^{286} + \cdots + 16i + 54}, \frac{(69i + 109)x^{431} + (60i + 178)x^{430} + \cdots + 98i + 124}{x^{431} + (146i + 53)x^{430} + \cdots + 44i + 89} \right).$$

We apply Algorithm 4.8.1 to find a path from E_{120} to E_{1728} (see Figure 4.1). Step 1 on input $(E_{120}, \theta_{120}, t_{120}, n_{120})$ produces the ℓ-suitable and ℓ-primitive traced endomorphism $\theta_{120} \leftarrow \theta_{120} + [-10]$ with $t_{120} \leftarrow 0$ and $n_{120} \leftarrow 188$. Here $\Delta' = t_{120}^2 - 4n_{120} = -752$ and its ℓ-fundamental part is $\Delta = -47$. Step 4 calls Algorithm 4.7.3 on input $(E_{120}, \theta_{120}, t_{120}, n_{120})$ to produce the following ascending path H_2 to the rim, see Example 4.7.3:

$$H_2 : (E_{120}, \theta_{120}, 0, 188) \xrightarrow{\varphi_{120}} (E_{171}, \theta_{171}, 0, 47) \xrightarrow{\varphi_{171}} (E_{5i+109}, \theta_{5i+109}, 1, 12).$$

Now we apply Algorithm 4.7.2 on input $(E_{5i+109}, \theta_{5i+109}, t_{5i+109}, n_{5i+109})$ to walk the rim in Step 5 as in Example 4.7.2. The list of all the j-invariants is $L = \{5i+109, 174i+109, 80i+107, 22, 99i+107\}$. In Step 7, calling Algorithm 4.6.1 on input Δ, we obtain $\theta_{1728} = (3i+k)/2$ as in Example 4.6.4. For

simplicity in this example, we use Algorithm 4.7.3 in Step 8, instead of the methods of Section 4.7.4. We apply Algorithms 4.5.3 and 4.7.1 (see Section 4.6.2) to $(E_{1728}, \theta_{1728}, 0, 47)$ to obtain an ℓ-primitive isogeny-chain endomorphism $\theta'_{1728} = \varphi_{171} \circ \varphi_{1728}$ where $\deg(\varphi_{1728}) = 16$, $\deg(\varphi_{171}) = 3$ and with $t_{1728} = 2$, $n_{1728} = 48$ as in Example 4.5.8. We call Algorithm 4.7.3 on input $(E_{1728}, \varphi_{171} \circ \varphi_{1728}, 2, 48)$ to produce the following ascending path (see Example 4.7.4):

$$H_1 : (E_{1728}, \varphi_{171} \circ \varphi_{1728}, 2, 48) \xrightarrow{\varphi'_{1728}} (E_{22}, \varphi_{174i+109} \circ \varphi'_{22}, 1, 12).$$

Finally, since $j(E_{22}) = 22 \in L$, joining the previous paths, we obtain a path from E_{1728} to E_{120} (see the whole path in Figure 4.1) as

$$H : E_{1728} \xrightarrow{\varphi'_{1728}} E_{22} \xrightarrow{\varphi_{22}} E_{99i+107} \xrightarrow{\varphi_{99i+107}} E_{5i+109} \xrightarrow{\hat{\varphi}_{171}} E_{171} \xrightarrow{\hat{\varphi}_{120}} E_{120}.$$

4.9 Proof of the Main Theorem and Special Cases

4.9.1 Proof of Theorem 4.1.1

Proof of Theorem 4.1.1. Suppose θ is such an endomorphism. Then set $B = L_d(1/2)$. We can apply Algorithm 4.5.3 (having Algorithm 4.5.1 as a subroutine) to θ, whose runtime depends on the evaluation of θ on inputs in a field $\mathbb{F}_{p^{O(B^2)}}$. The runtime for this conversion is therefore $T_\theta(L_d(1/2), p)$. The result is a prime-power isogeny-chain representation of θ. We can then use Algorithm 4.8.1, with the representation runtime being $L_d(1/2)$, by Proposition 4.5.5. The classical runtime follows from Proposition 4.8.1. □

4.9.2 Special cases

In this section, we refer to an endomorphism as *insecure* if access to such an endomorphism allows for a polynomial time path-finding algorithm. Endomorphisms of small size are known to be insecure [63]. We obtain a version of this from our methods also.

Theorem 4.9.1. *Assume the situation of Theorem 4.1.1. In the following special cases, the runtime and path length of Algorithm 4.8.1 is polynomial in* $\log p$*:*

1. *The input endomorphism is rationally represented in polynomial space.*

2. $h_{\mathcal{O}_\Delta} = \text{poly}(\log p)$ *and* ℓ *is coprime to* Δ *and inert in* K*. In this case, the endomorphism is not even needed as input; only its existence, trace and norm are needed.*

Proof. The second case is a consequence of Algorithm 4.8.1 and Proposition 4.8.1, in which the hypotheses imply Steps 4 and 5 are unnecessary. The first is a consequence of the observation that such endomorphisms have polynomially sized discriminants and class numbers. □

The following result demonstrates the existence of non-small endomorphisms which are insecure.

Theorem 4.9.2. *Suppose* $\Delta = f^2\Delta'$ *where* Δ' *is a discriminant of* $\text{poly}(\log p)$ *size,* f *is* $\text{poly}(\log p)$*-smooth, and* θ *is* f*-suitable with* $\text{poly}(\log p)$*-powersmooth norm, and represented in some fashion so that it can be evaluated in* $\text{poly}(\log p)$ *time on points of* $\text{poly}(\log p)$ *size. Then there is an algorithm to find an* $O(\log p)$*-powersmooth isogeny to* E_{init} *in time* $\text{poly}(\log p)$*.*

Proof. The dependence on ℓ throughout the chapter has been suppressed by assuming $\ell = O(1)$, but it is at worst polynomial throughout. We refactor θ in $\text{poly}(\log p)$ time (this is possible by Proposition 4.5.1 and the evaluation runtime assumption), to obtain an isogeny chain. Taking each prime ℓ dividing f in turn, we ascend as for as possible on the oriented ℓ-isogeny volcano. By f-suitability, we can ascend without any further translation or refactoring. Having ascended, we obtain an endomorphism of discriminant Δ' of $\text{poly}(\log p)$ size and trace zero, and hence call on Theorem 4.9.1 with respect to some suitable ℓ. □

The following corollary guarantees that every elliptic curve has an insecure endomorphism. Recall that most curves do not have small endomorphisms. It is known that there are curves having no endomorphisms of norm smaller than $p^{2/3-\epsilon}$ (see [62, Proposition B.5], [40, Section 4], [103, Proposition 1.4]). Therefore the endomorphisms guaranteed by the following corollary are frequently large.

Corollary 4.9.3. *Let* p *be such that* $p \equiv 3 \pmod 4$*, and let* E *be any supersingular elliptic curve over* $\mathbb{F}_{p^2}$*. The endomorphism ring* $\text{End}(E)$ *contains an endomorphism which can be presented in*

$\mathrm{poly}(\log p)$ *space and evaluated in* $\mathrm{poly}(\log p)$ *time, and knowledge of that endomorphism allows for a classical* $\mathrm{poly}(\log p)$*-time algorithm to find a path to* $j = 1728$.

Proof. Consider the Gaussian field $\mathbb{Q}(i)$. Let $L = \prod_i \ell_i$ be a product of the first $O(\log p)$ odd primes. We claim that $\mathrm{End}(E)$ contains $\mathbb{Z}[Li]$. To see this, we use [44, Theorem 1], which asserts that E can be reached by a random walk from E_{init} of $j = 1728$ (which exists since $p \equiv 3 \pmod 4$) with degree L. Then $\mathrm{End}(E)$ must contain $\mathbb{Z}[Li]$ (in fact, it may contain a strictly larger order, if the steps are not all descending with respect to the Gaussian field). Taking the element Li, represented as a $\mathrm{poly}(\log p)$-powersmooth isogeny chain, we apply Theorem 4.9.2. □

This proof is not constructive, and it is indeed not easy to find such an endomorphism. Examples of such endomorphisms exist in any field with $\mathrm{poly}(\log p)$ discriminant; indeed one can take any element of the form $L(\omega + k)$ for $k \in \mathbb{Z}$ and a $\mathrm{poly}(\log p)$-powersmooth L such that $N(\omega + k)$ is $\mathrm{poly}(\log p)$-powersmooth.

Finally, we remark on one more special case. When the norm of θ is well-behaved, and we are already at the rim with respect to ℓ (perhaps by choosing ℓ judiciously), then we have improved dependence on p. Note that in the following theorem, there is no requirement on the factorization of Δ.

Theorem 4.9.4. *Suppose the norm of* θ *has powersmoothness bound* $B(p)$*, and suppose that* Δ *is coprime to* ℓ*. Then there is an algorithm to find an* ℓ*-isogeny path of length* $O(\log p + h_{\mathcal{O}})$ *to* E_{init} *in time* $h_{\mathcal{O}}\,\mathrm{poly}(B(p)\log p)$.

Proof. Use Algorithm 4.8.1. By the assumption on Δ, we need not ascend with θ (that is, we skip Step 4). We only walk horizontally, and those steps are polynomial in $B(p)$ by Proposition 4.7.2. □

4.10 Division by $[\ell]$

We conclude with a detailed description and analysis of McMurdy's algorithm (Algorithm 4.10.2) which can be used to divide any *isogeny* (not just an endomorphism) by $[\ell]$ if it is

a multiple of $[\ell]$. Given a rationally represented traced endomorphism, we apply Algorithm 4.10.2 and then adjust the trace and norm accordingly.

We follow the notation of McMurdy [69]. Let E_1 and E_2 be two supersingular elliptic curves given by respective short Weierstrass equations

$$E_1 : y^2 = W_1(x), \qquad E_2 : y^2 = W_2(x).$$

with $W_1(x), W_2(x) \in \mathbb{F}_{p^2}[x]$. Denote by $\psi_{E_1,\ell}$ the ℓ-division polynomial of E_1, made monic, and let $X_i(x)$ and $Y_i(x)$ be the rational functions representing the multiplication-by-ℓ map on E_i, i.e. $[\ell]_{E_i}(x, y) = (X_i(x), Y_i(x)y)$ for $i = 1, 2$. For a polynomial $P(x) = (x - r_1) \cdots (x - r_n)$ with coefficients in some field $\mathbb{F}$ whose roots r_i lie in some field extension $\mathbb{F}'$ of $\mathbb{F}$, and a rational function $T(x)$ over FF', define

$$P(x)\big|T := (x - T(r_1)) \cdots (x - T(r_n)).$$

Given $[\ell]\varphi : E_1 \to E_2$ as a pair of rational maps, where $\varphi : E_1 \to E_2$ is an isogeny, the rational maps of φ are obtained as follows.

Proposition 4.10.1 ([69, Proposition 2.6]). *Suppose that $\varphi : E_1 \to E_2$ is a separable isogeny such that $([\ell]\varphi)(x, y) = (F(x), G(x)y)$ for rational functions $F(x), G(x)$. Write $F(x)$ in lowest terms, i.e. as either $\frac{c_F \cdot P(x)}{W_1(x)Q(x)}$ when $\ell = 2$ or $\frac{c_F \cdot P(x)}{\psi_{E_1,\ell}(x)^2 Q(x)}$ when $\ell \neq 2$, with monic polynomials $P(x), Q(x)$. Set*

$$p(x) = P(x)\big|X_1, \;\; q(x) = Q(x)\big|X_1.$$

Then $p(x) = p_0(x)^{\ell^2}$ and $q(x) = q_0(x)^{\ell^2}$ for monic polynomials $p_0(x), q_0(x)$. Moreover, we have $\varphi(x, y) = (f(x), g(x)y)$, where $f(x) = c_F \ell^2 \cdot \frac{p_0(x)}{q_0(x)}$ and $g(x) = \frac{G(x)}{Y_2(f(x))}$.

Algorithm 4.10.1 computes the polynomials $p(x)$ and $q(x)$ as given in Proposition 4.10.1. The main division-by-$[\ell]$ process (Algorithm 4.10.2) then calls Algorithm 4.10.1 twice.

Division by $\ell = 2$ has been implemented by McMurdy [69] (code available at [68]). Division by odd primes $\ell > 2$ is complicated by the non-vanishing of the y-coordinates of the ℓ-torsion points. Fix an odd prime $\ell > 2$. In order to compute $p(x) = P(x)\big|X_1$ and $q(x) = Q(x)\big|X_1$ in Steps 3 and 4 of Algorithm 4.10.2, we compute the rational map $N_P = \prod_i P(\mathbf{x}_i)$ as a function of

Algorithm 4.10.1: Computing the polynomial $P(x)\big|X_1$

Input: An elliptic curve E_1, a monic polynomial $P(x)$ defined over $\mathbb{F}_{p^m}$, and the rational map $X_1(x)$ associated to E_1.

Output: $P(x)\big|X_1$.

1 Compute a root ζ of X_1.

2 Compute the x-coordinates x_i of the points $S_i = (x_i, y_i) \in E_1[\ell]$, indexed by $i = 1, \ldots, \ell^2 - 1$ so that $x_{i+\frac{\ell^2-1}{2}} = x_i$, using the ℓ-th division polynomial (note that we do not compute the y_i here). Let $S_0 = O_{E_1}$.

3 Compute the x-coordinates $\mathbf{x}_i(x, y, y_i)$ for $1 \leq i \leq \frac{\ell^2-1}{2}$ of the maps representing point addition $(x, y) + S_i$ on E_1, using the values of x_i computed in step 2 but leaving y_i's as indeterminates. Set $\bar{\mathbf{x}}_i(x, y, y_i) = \mathbf{x}_i(x, y, -y_i)$ which is the x-coordinate of the point addition $(x, y) + (-S_i)$.

4 $N(x) \leftarrow P(x)$ and $D(x) \leftarrow 1$.

5 **For** $i = 1, \ldots, \frac{\ell^2-1}{2}$ **do**

6 Compute $P(\mathbf{x}_i(x, y, y_i))$ and $P(\bar{\mathbf{x}}_i(x, y, y_i))$ (as rational functions in x, y and y_i) using Horner's algorithm.

7 Compute the numerator N_i and denominator D_i of $P(\mathbf{x}_i)P(\bar{\mathbf{x}}_i)$ as polynomials in x, y and y_i.

8 Replace y^2 with $W_1(x)$ and y_i^2 with $W_1(x_i)$ in N_i. Denote the result by $N_i(x)$, as no y's or y_i's should remain.

9 Replace y_i^2 with $W_1(x_i)$ in D_i. Denote the result by $D_i(x)$, as no y's or y_i's should remain.

10 $N(x) \leftarrow N(x) \cdot N_i(x)$, and $D(x) \leftarrow D(x) \cdot D_i(x)$.

11 $N_P(x) \leftarrow \frac{N(x)}{D(x)}$, $i \leftarrow 0$, $p(x) \leftarrow 0$.

12 **For** $i = 0, \ldots, \deg(P(x))$ **do**

13 $a_i \leftarrow N_P(\zeta)$.

14 $p(x) \leftarrow p(x) + a_i x^i$.

15 $N_P(x) \leftarrow N_P(x) - a_i x^i$.

16 $N_P(x) \leftarrow N_P(x)/X_1(x)$.

17 **Return** $p(x)$.

Algorithm 4.10.2: Division by $[\ell]$.

Input: Elliptic curves E_1, E_2, rational maps $F(x)$ and $G(x)$ where $([\ell]\varphi)(x,y) = (F(x), G(x)y)$ for some isogeny $\varphi : E_1 \to E_2$.

Output: Rational maps $f(x)$ and $g(x)$ such that $\varphi(x,y) = (f(x), g(x)y)$.

1 Determine c_F, and the monic polynomials $P(x)$ and $Q(x)$ such that $F(x) = \frac{c_F \cdot P(x)}{W_1(x) \cdot Q(x)} (\ell = 2)$ or $F(x) = \frac{c_F \cdot P(x)}{(\psi_{E_1,\ell}(x))^2 \cdot Q(x)} (\ell \neq 2)$.

2 Compute $X_1(x)$ and $Y_2(x)$.

3 Compute $p(x) \leftarrow P(x)\big|X_1$ using Algorithm 4.10.1 on input $E_1, P(x), X_1(x)$.

4 Compute $q(x) \leftarrow Q(x)\big|X_1$ using Algorithm 4.10.1 on input $E_1, Q(x), X_1(x)$. In this step we can skip Steps 1–4 in Algorithm 4.10.1 since they were already performed in Step 3 of this algorithm.

5 Compute $p_0(x) \leftarrow p(x)^{1/\ell^2}$ and $q_0(x) \leftarrow q(x)^{1/\ell^2}$ using a truncated variant of Newton's method.

6 $f(x) \leftarrow c_F \ell^2 \cdot \frac{p_0(x)}{q_0(x)}$, $g(x) \leftarrow \frac{G(x)}{Y_2(f(x))}$.

7 **Return** $f(x), g(x)$.

the variable x only. In contrast to the case of 2-torsion points, the ℓ-torsion points on E_1 have non-zero y-coordinates, so some $\mathbf{x}_i$ depend not only on x (as in the case $\ell = 2$) but also on y and y_i for $i \leq (\ell^2 - 1)/2$. As a consequence, N_P also depends on these variables. To overcome this obstruction, we employ a new technique presented in Steps 5–11 of Algorithm 4.10.1. In these steps, we compute the products $\mathbf{x}_i \cdot \bar{\mathbf{x}}_i$, and hence the products $P(\mathbf{x}_i) \cdot P(\bar{\mathbf{x}}_i)$. Each product $P(\mathbf{x}_i) \cdot P(\bar{\mathbf{x}}_i)$ is a rational map in x, y^2, and y_i^2 $(i \leq (\ell^2 - 1)/2)$ by Lemma 4.10.1. We replace y^2 (respectively y_i^2) with $W_1(x)$ (respectively $W_1(x_i)$) to obtain rational maps in the variable x only.

Example 4.10.1 (Computing the polynomial $P(x)\big|X_1$ via Algorithm 4.10.1). Let $\ell = 3$, $p = 179$, and $E_{1728} : y^2 = x^3 - x$ the supersingular elliptic curve over $\overline{\mathbb{F}}_p$ with $j = 1728$. Let $X_1(x)$, $Y_1(x)$ be associated to multiplication-by-3, i.e.

$$[3]_{E_{1728}}(x,y) = (X_1(x), Y_1(x)y) \quad \text{where} \quad X_1(x) = \frac{20x^9 + 61x^7 + 63x^5 + 175x^3 + x}{x^8 + 175x^6 + 63x^4 + 61x^2 + 20}\ .$$

Let $P(x) = x^{18} + 122x^{16} + 136x^{14} + 65x^{12} + 29x^{10} + 150x^8 + 114x^6 + 43x^4 + 57x^2 + 178$. We compute $p(x) = P(x)\big|X_1$ using Algorithm 4.10.1 as follows.

In Steps 1 and 2, we may choose $\zeta = 0$. Let $\mathbb{F}_{p^4}$ be generated by $\mathbf{a}$ having minimal polynomial $x^4 + x^2 + 109x + 2$. We obtain $S_0 = O_{E_{1728}}, S_1 = (103, y_1), S_2 = (76, y_2), S_3 = (24\mathbf{a}^3 + 39\mathbf{a}^2 + 119\mathbf{a} + 102, y_3), S_4 = (155\mathbf{a}^3 + 140\mathbf{a}^2 + 60\mathbf{a} + 77, y_4), S_5 = -S_1, S_6 = -S_2, S_7 = -S_3, S_8 = -S_4$. In Steps 3,

we compute $\mathbf{x}_i(x, y, y_i)$ and $\bar{\mathbf{x}}_i(x, y, y_i)$ as $\mathbf{x}_0 = x, \bar{\mathbf{x}}_i = \mathbf{x}_i(x, y, -y_i), \forall i, 1 \leq i \leq 4$ where

$$\mathbf{x}_1(x, y, y_1) = \frac{-x^3 + y^2 - 2yy_1 + y_1^2 - 76x^2 + 48x + 68}{x^2 - 27x + 48},$$

$$\mathbf{x}_2(x, y, y_2) = (-x^3 + y^2 - 2yy_2 + y_2^2 + 76x^2 + 48x - 68)/(x^2 + 27x + 48),$$

$$\mathbf{x}_3(x, y, y_3)$$
$$= \frac{-x^3 + y^2 - 2yy_3 + y_3^2 + (24\mathbf{a}^3 + 39\mathbf{a}^2 - 60\mathbf{a} - 77)x^2 - 46x + (30\mathbf{a}^3 + 4\mathbf{a}^2 - 75\mathbf{a} + 38)}{(x^2 + (-48\mathbf{a}^3 - 78\mathbf{a}^2 - 59\mathbf{a} - 25)x - 46)},$$

$$\mathbf{x}_4(x, y, y_4)$$
$$= \frac{-x^3 + y^2 - 2yy_4 + y_4^2 + (-24\mathbf{a}^3 - 39\mathbf{a}^2 + 60\mathbf{a} + 77)x^2 - 46x + (-30\mathbf{a}^3 - 4\mathbf{a}^2 + 75\mathbf{a} - 38}{x^2 + (48\mathbf{a}^3 + 78\mathbf{a}^2 + 59\mathbf{a} + 25)x - 46}.$$

In Steps 4–11: We compute the norm $N_P(x)$ of $P(x)$ by first computing $P(\mathbf{x}_i) \cdot P(\bar{\mathbf{x}}_i) = \frac{N_i}{D_i}, 1 \leq i \leq 4$. We then have $N(x) = P(x)\prod_i N_i = 14x^{162} + 157x^{160} + \cdots + 22x^2 + 165$ and $D(x) = \prod_i D_i = x^{144} + 107x^{142} + \cdots + 90x^2 + 75$. Hence $N_P(x) = \frac{N(x)}{D(x)}$. Finally, we compute all the coefficients of $p(x)$ by repeating Steps 13–16. The result is

$$p(x) = x^{18} + 170x^{16} + 36x^{14} + 95x^{12} + 126x^{10} + 53x^8 + 84x^6 + 143x^4 + 9x^2 + 178.$$

Example 4.10.2 (Division by $\ell = 3$ via Algorithm 4.10.2). As before, let $p = 179$ and $E_{1728} : y^2 = x^3 - x$ the supersingular elliptic curve over $\overline{\mathbb{F}}_p$ of j-invariant $j(E_{1728}) = 1728$ as in Example 4.10.1. Then the endomorphism ring of E_{1728} contains the endomorphism $[i]$ defined as $[i](x, y) := (-x, iy)$ with $i \in \mathbb{F}_{p^2}$ and $i^2 = -1$.

The map $\theta = 1 + [i]$ is a separable endomorphism and we have $([3]\theta)(x, y) = \left(\frac{F_1(x)}{F_2(x)}, \frac{G_1(x)}{G_2(x)}y\right)$, defined over $\mathbb{F}_{p^2}$, with

$$F_1(x) = 169ix^{18} + 33ix^{16} + 72ix^{14} + 66ix^{12} + 68ix^{10} + 111ix^8 + 113ix^6 + 107ix^4 + 146ix^2 + 10i$$

$$F_2(x) = x^{17} + 8x^{15} + 45x^{13} + 124x^{11} + 110x^9 + 124x^7 + 45x^5 + 8x^3 + x$$

$$G_1(x) = (58i + 58)x^{26} + (170i + 170)x^{24} + \cdots + (170i + 170)x^2 + 58i + 58,$$

$$G_2(x) = x^{26} + 12x^{24} + 2x^{22} + 66x^{20} + 128x^{18} + 44x^{16} + 171x^{14} + 44x^{12} + 128x^{10} + 66x^8$$
$$+ 2x^6 + 12x^4 + x^2.$$

We apply Algorithm 4.10.2 to divide $[3]\theta$ by 3 to obtain $\theta = [f(x), g(x)y]$ as follows.

In Step 1, we write $F(x) = \frac{c_F \cdot P(x)}{(\psi_{E_{1728},3}(x))^2 \cdot Q(x)}$ where $c_F = 169i$, $\psi_{E_{1728},3}(x) = x^4 + 177x^2 + 119$ and

$$P(x) = x^{18} + 122x^{16} + \cdots 57x^2 + 178, \qquad Q(x) = x^9 + 12x^7 + 30x^5 + 143x^3 + 9x.$$

In Step 2, we compute X_1 and Y_2 using the formula for multiplication by 3 map on E_{1728}. Here, X_1 is as given in Example 4.10.1 and

$$Y_2 = \frac{126x^{12} + 92x^{10} + 153x^8 + 136x^6 + 139x^4 + 63x^2 + 159}{x^{12} + 173x^{10} + 11x^8 + 175x^6 + 56x^4 + 59x^2 + 53}.$$

Then we compute $p(x) = P(x)\big|X_1$ and $q(x) = Q(x)\big|X_1$ in Steps 3 and 4 using Algorithm 4.10.1 to obtain $p(x) = x^{18} + 170x^{16} + \cdots + 9x^2 + 178$, and $q(x) = x^9$. In Step 5, computing 9-th roots of $p(x)$ and $q(x)$ yields $p_0(x) = x^2 + 178$ and $q_0(x) = x$. The final output is

$$f(x) = c_F \ell^2 \cdot \frac{p_0(x)}{q_0(x)} = \frac{89ix^2 + 90i}{x}, \quad g(x) = \frac{G(x)}{Y_2(f(x))} = \frac{(134i + 134)x^2 + 134i + 134}{x^2}.$$

To determine the complexity of Algorithm 4.10.1, we first prove the following lemma which is needed in the proof of Proposition 4.10.2.

Lemma 4.10.1. *Fix $0 \leq i \leq \frac{\ell^2-1}{2}$, the products $\mathbf{x}_i\bar{\mathbf{x}}_i$ and $P(\mathbf{x}_i)P(\bar{\mathbf{x}}_i)$ are rational functions in x, y^2, and y_i^2.*

Proof. By direct computation, both $\mathbf{x}_i + \bar{\mathbf{x}}_i$ and $\mathbf{x}_i\bar{\mathbf{x}}_i$ are rational functions in x, y^2, and y_i^2. As a symmetric polynomial in $\mathbf{x}_i$ and $\bar{\mathbf{x}}_i$, the quantity $P(\mathbf{x}_i)P(\bar{\mathbf{x}}_i)$ is a polynomial in $\mathbf{x}_i + \bar{\mathbf{x}}_i$ and $\mathbf{x}_i\bar{\mathbf{x}}_i$, hence also a rational function in x, y^2 and y_i^2. □

Proposition 4.10.2. *Algorithm 4.10.1 is correct and has runtime $O(\deg^2(P)\boldsymbol{M}(p^m))$.*

Proof. Algorithm 4.10.1 is correct by [69, Pages 8–9] and Lemma 4.10.1. Steps 1-3 are negligible because they require a fixed number of operations in an extension of $\mathbb{F}_{p^2}$ of degree $O(\ell^2)$. Since $P(x) \in \mathbb{F}_{p^m}[x]$ and $E_1[\ell]$ is defined over an extension of $\mathbb{F}_{p^2}$ of degree at most ℓ^2 by Lemma 4.2.3, all

the arithmetic in the remaining steps takes place in a field extension of $\mathbb{F}_{p^2}$ of degree $\mathrm{lcm}(\ell^2, m) = O(m)$.

In the first loop (steps 5-10), the most costly steps are 7 and 10 which both require $O(\deg^2(P))$ operations; the remaining steps are linear in $\deg P$ when Horner's algorithm is used. In the second loop (steps 12-11), $p(x)$ is computed as described in [69, Page 9]. Step 13 requires $O(\deg P)$ field operations using Horner's algorithm again. Since X_1 has degree $O(\ell^2)$, step 11 also takes $O(\deg P)$ operations. Hence the second loop takes $O(\deg^2(P))$ field operations. □

Proposition 4.10.3. *Algorithm 4.10.2 is correct and has runtime* $O(\deg^2(\varphi)\boldsymbol{M}(p))$.

Proof. The correctness of Algorithm 4.10.2 follows from [69, Proposition 2.6]. By Lemma 4.2.2, φ is defined over $\mathbb{F}_{p^{12}}$, so all the rational functions appearing in the algorithm belong to $\mathbb{F}_{p^{12}}(x)$. We also note that $P(x)$ and $Q(x)$ have degree $O(\deg \varphi)$, hence so do $p(x)$, $q(x)$, $p_0(x)$ and $q_0(x)$.

Since $\psi_{E_1,\ell}(x)$ and $W_1(x)$ have fixed degree, step 1 requires $O(\deg \varphi)$ field operations. Steps 5 and 6 take $\widetilde{O}(\deg \varphi)$ operations using fast polynomial arithmetic; see [46, Theorem 1.2]. Here, to extract an ℓ^2-th root of $p(x)$, we apply a truncated variant of Newton's method (see [96, Sections 9.4 and 9.6]) to the polynomial $H(y) = y^{\ell^2} - p(x)$ and compute the sequence of polynomials

$$f_0(x) = x^{\deg p}\ , \qquad f_{i+1}(x) = f_i(x) - \left\lfloor \frac{H(f_i(x))}{H'(f_i(x)} \right\rfloor \quad (i \geq 0)$$

to obtain $p_0(x)$ after at most $\lceil \log_2(\deg p) \rceil$ iterations; similarly for $q_0(x)$.

The runtime of Algorithm 4.10.2 is thus dominated by steps 3 and 4, which have runtime $O(\deg^2(\varphi)\mathbf{M}(p^{12})) = O(\deg^2(\varphi)\mathbf{M}(p))$. □

Chapters 4 is, in full, being prepared for submission for publication. The dissertation author was the collaborator and the coauthor for the material below.

• Sarah Arpin; Mingjie Chen; Kristin E. Lauter; Renate Scheidler; Katherine E. Stange; Ha T. N. Tran "Orienteering with one endomorphism".

Chapter 5

On $\mathbb{F}_p$-roots of the Hilbert class polynomial modulo p

5.1 Introduction

Let $\mathcal{O}$ be an order in an imaginary quadratic field K, and $\mathrm{Pic}(\mathcal{O})$ be the Picard group of $\mathcal{O}$, i.e. the group of isomorphism classes of invertible fractional $\mathcal{O}$-ideals under multiplication. The Hilbert class polynomial $H_{\mathcal{O}}(x)$ attached to $\mathcal{O}$ is defined to be

$$H_{\mathcal{O}}(x) = \prod_{[\mathfrak{a}]\in \mathrm{Pic}(\mathcal{O})} (x - j(\mathbb{C}/\mathfrak{a})), \tag{5.1.1}$$

where $[\mathfrak{a}]$ denotes the isomorphism class of the invertible fractional $\mathcal{O}$-ideal $\mathfrak{a}$, and $j(\mathbb{C}/\mathfrak{a})$ stands for the j-invariant of the complex elliptic curve $\mathbb{C}/\mathfrak{a}$. It is well known that $H_{\mathcal{O}}(x)$ has integral coefficients, and it is irreducible over $\mathbb{Q}$ (see [29, §13] and [56, Chapter 10, App., p.144]).

Let $p \in \mathbb{N}$ be a prime number, and $\widetilde{H}_{\mathcal{O}}(x) \in \mathbb{F}_p[x]$ be the polynomial obtained by reducing $H_{\mathcal{O}}(x) \in \mathbb{Z}[x]$ modulo p. Suppose that p is non-split in K so that the roots of $\widetilde{H}_{\mathcal{O}}(x)$ are supersingular j-invariants, which are known to lie in $\mathbb{F}_{p^2}$. It's natural to ask how many of them are actually in $\mathbb{F}_p$. Castryck, Panny, and Vercauteren answered this question in [19, Theorem 26] for special cases when $p \equiv 3 \pmod 4$, K is of the form $\mathbb{Q}(\sqrt{-l})$ with l prime, $l < (p+1)/4$ and $\mathcal{O}$ is an order

containing $\sqrt{-l}$. Their method as in [19, Section 5.2] counts the $\mathbb{F}_p$-roots by constructing supersingular elliptic curves over $\mathbb{F}_p$. We take a different approach here by reinterpreting the $\mathbb{F}_p$-roots in terms of quaternion orders, which allows us to answer the question in more generality.

Our main result is as follows.

Theorem 5.1.1. *Let K be an imaginary quadratic field and $\mathcal{O}$ be an order in K. Let p be a prime inert in K and strictly greater than $|\operatorname{disc}(\mathcal{O})|$, and $\mathcal{H}_p$ be set of $\mathbb{F}_p$-roots of $\widetilde{H}_{\mathcal{O}}(x)$. If $\mathcal{H}_p$ is nonempty, then it admits a regular (i.e. free and transitive) action by the 2-torsion subgroup $\operatorname{Pic}(\mathcal{O})[2] \subset \operatorname{Pic}(\mathcal{O})$. In particular, the number of $\mathbb{F}_p$-roots of $\widetilde{H}_{\mathcal{O}}(x)$ is either zero or $|\operatorname{Pic}(\mathcal{O})[2]|$.*

Moreover, $\mathcal{H}_p \neq \emptyset$ if and only if for every prime factor ℓ of $\operatorname{disc}(\mathcal{O})$, either condition (i) or (ii) below holds for ℓ depending on its parity:

(i) $\ell \neq 2$ and the Legendre symbol $\left(\frac{-p}{\ell}\right) = 1$;

(ii) $\ell = 2$ and one of the following conditions holds:

(a) $p \equiv 7 \pmod 8$;

(b) $-p + \frac{\operatorname{disc}(\mathcal{O})}{4} \equiv 0,\ 1$ or $4 \pmod 8$;

(c) $-p + \operatorname{disc}(\mathcal{O}) \equiv 1 \pmod 8$.

The assumption that $|\operatorname{disc}(\mathcal{O})| < p$ immediately implies that p does not divide the discriminant of $H_{\mathcal{O}}(x)$ by an influential work of Gross and Zagier [45]. Therefore, $\widetilde{H}_{\mathcal{O}}(x)$ has no repeated roots. We provide an alternative proof of this fact under the current assumptions in Corollary 5.2.4.

Remark 5.1.2. After the first of version of this manuscript appeared on arXiv, Jianing Li kindly informed us that a similar result to Theorem 5.1.1 has firstly been obtained in [102, Theorem 1.1] under the assumption that $|\operatorname{disc}(\mathcal{O})| < 4\sqrt{p/3}$. Moreover, Li et al. used a method similar to [102] and generalized it much further in a joint work [58]. Their result is as follows. Let $j_0 = j(\mathbb{C}/\mathcal{O})$, and put $L := \mathbb{Q}(j_0)$. If p coprime to the index $[\mathcal{O}_L : \mathbb{Z}[j_0]]$ (e.g. if $p \nmid \operatorname{disc}(\mathcal{O})$), then they completely determined the factorization of $\widetilde{H}_{\mathcal{O}}(x)$ in $\mathbb{F}_p[x]$. Partial results are also obtained without the co-primality condition. In particular, the results of Theorem 5.1.1 has been covered in [58, Theorem 4.1]. On the other hand, the current project was initiated in May 2021 during an online discussion between the authors. Unaware of the significant progress made by aforementioned

works, we worked independently and obtained Theorem 5.1.1 by a completely different method: we count the $\mathbb{F}_p$-roots by demonstrating a regular action using quaternion orders, whereas the aforementioned works count by studying the factorization of p in L.

For the reader's convenience, we reproduce the celebrated formula of Gauss on the order of $\mathrm{Pic}(\mathcal{O})[2]$.

Theorem 5.1.3 ([29, Proposition 3.11]). *Let r be the number of odd primes dividing* $\mathrm{disc}(\mathcal{O})$. *Define the number μ as follows: if* $\mathrm{disc}(\mathcal{O}) \equiv 1 \pmod 4$, *then $\mu = r$, and if* $\mathrm{disc}(\mathcal{O}) \equiv 0 \pmod 4$, *then* $\mathrm{disc}(\mathcal{O}) = -4n$, *where $n > 0$, and μ is determined as follows:*

$$\mu = \begin{cases} r & \text{if } n \equiv 3 \pmod 4; \\ r+1 & \text{if } n \equiv 1, 2 \pmod 4; \\ r+1 & \text{if } n \equiv 4 \pmod 8; \\ r+2 & \text{if } n \equiv 0 \pmod 8. \end{cases}$$

Then $|\mathrm{Pic}(\mathcal{O})[2]| = 2^{\mu-1}$.

This chapter is organized as follows. In section 5.2, we give a reinterpretation of $\mathcal{H}_p$ in terms of quaternion orders. In section 5.3, we show that there is a regular action of $\mathrm{Pic}(\mathcal{O})[2]$ on $\mathcal{H}_p$ whenever $\mathcal{H}_p \neq \emptyset$, and provide a nonemptiness criterion for $\mathcal{H}_p$. Throughout the chapter, the prime $p \in \mathbb{N}$ is assumed to be non-split in K. The notation $B_{p,\infty}$ is reserved for the unique quaternion $\mathbb{Q}$-algebra ramified precisely at p and infinity. Given a set X and an equivalence relation on X, the equivalence class of an element $x \in X$ is denoted by $[x]$.

5.2 Reinterpretation of the $\mathbb{F}_p$-roots

As mentioned before, we are going to reinterpret the $\mathbb{F}_p$-roots of $\widetilde{H}_{\mathcal{O}}(x)$ in terms of quaternion orders. For this purpose, we first describe more concretely the reduction of singular moduli with complex multiplication by $\mathcal{O}$. Assume that the prime p is non-split in K. For the moment, we make no assumption on the discriminant of the order $\mathcal{O} \subset K$.

Let $\mathcal{E}\ell\ell(\mathcal{O})$ be the set of isomorphism classes of elliptic curves over $\overline{\mathbb{Q}}$ with complex multiplication by $\mathcal{O}$. It is canonically identified with the singular j-invariants with complex multiplication by $\mathcal{O}$ (i.e. the roots of $H_{\mathcal{O}}(x) \in \mathbb{Z}[x]$). The Picard group $\mathrm{Pic}(\mathcal{O})$ acts regularly on $\mathcal{E}\ell\ell(\mathcal{O})$ via $\mathfrak{a}$-transformation [80, §7] and [71, §1]:

$$\mathrm{Pic}(\mathcal{O}) \times \mathcal{E}\ell\ell(\mathcal{O}) \to \mathcal{E}\ell\ell(\mathcal{O}), \qquad ([\mathfrak{a}], E) \mapsto E^{\mathfrak{a}}. \tag{5.2.1}$$

More concretely, if we pick $\mathfrak{a}$ to be an integral ideal of $\mathcal{O}$ and write $E[\mathfrak{a}]$ for the finite group scheme $\cap_{a\in\mathfrak{a}} E[a]$, then $E^{\mathfrak{a}} = E/E[\mathfrak{a}]$ by [98, Corollary A.4]. Here $E[a] = \ker(E \xrightarrow{a} E)$. See [71, Proposition 1.26] and [98, Appendix] for the functorial characterization of $E^{\mathfrak{a}}$. Alternatively, since $\mathfrak{a}$ is an invertible $\mathcal{O}$-ideal, $E^{\mathfrak{a}}$ can also be identified canonically with the Serre tensor construction $\mathfrak{a}^{-1} \otimes_{\mathcal{O}} E$ (see [1, §1] and [20, §1.7.4]). Fix a member $E_0 \in \mathcal{E}\ell\ell(\mathcal{O})$. The regular action in (5.2.1) gives rise to a $\mathrm{Pic}(\mathcal{O})$-equivariant bijection $\xi : \mathcal{E}\ell\ell(\mathcal{O}) \to \mathrm{Pic}(\mathcal{O})$ that sends E_0 to the identity element $[\mathcal{O}] \in \mathrm{Pic}(\mathcal{O})$.

Similarly, let $\mathcal{E}\ell\ell^{ss}_{/\overline{\mathbb{F}}_p}$ be the set of isomorphism classes of supersingular elliptic curves over $\overline{\mathbb{F}}_p$, which is canonically identified with the set of supersingular j-invariants in $\mathbb{F}_{p^2}$. From [83, Theorem V.3.1], an elliptic curve $E/\overline{\mathbb{F}}_p$ is supersingular if and only if its endomorphism algebra $\mathrm{End}^0(E) := \mathrm{End}(E) \otimes \mathbb{Q}$ is a quaternion $\mathbb{Q}$-algebra. Assume that this is the case. Then $\mathrm{End}^0(E)$ coincides with the unique quaternion $\mathbb{Q}$-algebra $B_{p,\infty}$ ramified precisely at p and infinity, and $\mathrm{End}(E)$ is a maximal order in $\mathrm{End}^0(E)$ by [98, Theorem 4.2]. For simplicity, put $B := B_{p,\infty}$ and let $\mathrm{Typ}(B)$ be the *type set* of B, that is, the set of isomorphism (i.e. $B^\times$-conjugacy) classes of maximal orders in B. We obtain the following canonical map, which is known to be surjective [95, Corollary 42.2.21]:

$$\rho : \mathcal{E}\ell\ell^{ss}_{/\overline{\mathbb{F}}_p} \twoheadrightarrow \mathrm{Typ}(B), \qquad E \mapsto [\mathrm{End}(E)]. \tag{5.2.2}$$

Let $\mathcal{R}$ be a maximal order in B, and $\mathrm{Cl}(\mathcal{R})$ be its left ideal class set, that is, the set of isomorphism (i.e. right $B^\times$-equivalent) classes of fractional left ideals of $\mathcal{R}$ in B. Given a fractional left ideal I of $\mathcal{R}$, we write $\mathcal{R}_r(I)$ for the right order of I, which is defined as follows:

$$\mathcal{R}_r(I) := \{x \in B \mid Ix \subseteq I\}.$$

Sending a fractional left $\mathcal{R}$-ideal to its right order induces a surjective map

$$\Upsilon : \mathrm{Cl}(\mathcal{R}) \twoheadrightarrow \mathrm{Typ}(B), \qquad [I] \mapsto [\mathcal{R}_r(I)]. \tag{5.2.3}$$

The Deuring correspondence [95, Corollary 42.3.7] establishes a bijection between $\mathrm{Cl}(\mathcal{R})$ and $\mathcal{E}\ell\ell^{ss}_{/\overline{\mathbb{F}}_p}$. One direction of this correspondence goes as follows. From the surjectivity of ρ, we may always fix $E_{\mathcal{R}} \in \mathcal{E}\ell\ell^{ss}_{/\overline{\mathbb{F}}_p}$ such that $\mathrm{End}(E_{\mathcal{R}}) = \mathcal{R}$. Then the member of $\mathcal{E}\ell\ell^{ss}_{/\overline{\mathbb{F}}_p}$ corresponding to a left ideal class $[I] \in \mathrm{Cl}(\mathcal{R})$ is the I-transform $E^I_{\mathcal{R}}$ of $E_{\mathcal{R}}$. If I is chosen to be an integral left ideal of $\mathcal{R}$, then $E^I_{\mathcal{R}}$ can be identified with the quotient $E_{\mathcal{R}}/E_{\mathcal{R}}[I]$ by [98, Corollary A.4] again. From [95, Corollary 42.3.7], we have

$$\mathrm{End}(E^I_{\mathcal{R}}) \simeq \mathcal{R}_r(I). \tag{5.2.4}$$

Let $\mathfrak{P}$ be a place of $\overline{\mathbb{Q}}$ lying above p, and $r_{\mathfrak{P}} : \mathcal{E}\ell\ell(\mathcal{O}) \to \mathcal{E}\ell\ell^{ss}_{/\overline{\mathbb{F}}_p}$ be the reduction map modulo $\mathfrak{P}$. For each $E \in \mathcal{E}\ell\ell(\mathcal{O})$, we write $\widetilde{E}$ for the reduction of E modulo $\mathfrak{P}$. From [56, §9.2], reducing E_0 modulo $\mathfrak{P}$ gives rise to an embedding $\iota : \mathcal{O} \hookrightarrow \mathcal{R}_0 := \mathrm{End}(\widetilde{E}_0)$. By an abuse of notation, we still write ι for both of the following two induced maps:

$$K \hookrightarrow B \quad \text{and} \quad \mathrm{Pic}(\mathcal{O}) \xrightarrow{[\mathfrak{a}] \mapsto [\mathcal{R}_0 \iota(\mathfrak{a})]} \mathrm{Cl}(\mathcal{R}_0). \tag{5.2.5}$$

For simplicity, we identify K with its image in B via ι and write $\mathcal{R}_0\mathfrak{a}$ for $\mathcal{R}_0\iota(\mathfrak{a})$.

Now we are ready to give a concrete description of $r_{\mathfrak{P}} : \mathcal{E}\ell\ell(\mathcal{O}) \to \mathcal{E}\ell\ell^{ss}_{/\overline{\mathbb{F}}_p}$.

Proposition 5.2.1. *The reduction map $r_{\mathfrak{P}}$ fits into a commutative diagram as follows:*

$$\begin{array}{ccccc}
\mathcal{E}\ell\ell(\mathcal{O}) & \xrightarrow{r_{\mathfrak{P}}} & \mathcal{E}\ell\ell^{ss}_{/\overline{\mathbb{F}}_p} & & \\
\xi \updownarrow \simeq & & \delta \updownarrow \simeq & \searrow^{\rho} & \\
\mathrm{Pic}(\mathcal{O}) & \xrightarrow{\iota} & \mathrm{Cl}(\mathcal{R}_0) & \xrightarrow{\Upsilon} & \mathrm{Typ}(B).
\end{array}$$

Here ξ is the $\mathrm{Pic}(\mathcal{O})$-equivariant bijection that sends the fixed member $E_0 \in \mathcal{E}\ell\ell(\mathcal{O})$ to $[\mathcal{O}] \in \mathrm{Pic}(\mathcal{O})$, and δ is the Deuring correspondence obtained by taking $E_{\mathcal{R}_0} = \widetilde{E}_0$.

Proof. According to [80, Proposition 15, §11], $\mathfrak{a}$-transforms are preserved under good reductions[1]. This implies that for every $[\mathfrak{a}] \in \mathrm{Pic}(\mathcal{O})$, we have

$$\widetilde{E_0^{\mathfrak{a}}} = (\widetilde{E}_0)^{\mathfrak{a}} = (\widetilde{E}_0)^{\mathcal{R}_0\mathfrak{a}},$$

so the left square commutes. The right triangle commutes because of (5.2.4). □

Corollary 5.2.1. *For any* $[\mathfrak{a}] \in \mathrm{Pic}(\mathcal{O})$*, we have* $\mathrm{End}(\widetilde{E_0^{\mathfrak{a}}}) \simeq \mathfrak{a}^{-1}\mathcal{R}_0\mathfrak{a}$.

Proof. This follows directly from Proposition 5.2.1 since the right order of $\mathcal{R}_0\mathfrak{a}$ is precisely $\mathfrak{a}^{-1}\mathcal{R}_0\mathfrak{a}$. □

Remark 5.2.2. Let $\mathcal{O}_K$ be the ring of integers of K, and f be the conductor of $\mathcal{O}$ so that $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$. Write $f = p^m f'$ with $p \nmid f'$, and put $\mathcal{O}' := \mathbb{Z} + f'\mathcal{O}_K$. According to [72, Lemma 3.1], $\iota(K) \cap \mathcal{R}_0 = \iota(\mathcal{O}')$. For any invertible fractional ideal $\mathfrak{a}$ of $\mathcal{O}$, we have $\mathcal{R}_0\mathfrak{a} = (\mathcal{R}_0\mathcal{O}')\mathfrak{a} = \mathcal{R}_0(\mathcal{O}'\mathfrak{a})$. It follows that the map $\iota : \mathrm{Pic}(\mathcal{O}) \to \mathrm{Cl}(\mathcal{R}_0)$ factors through the following canonical homomorphism

$$\varpi : \mathrm{Pic}(\mathcal{O}) \to \mathrm{Pic}(\mathcal{O}'), \qquad [\mathfrak{a}] \mapsto [\mathcal{O}'\mathfrak{a}].$$

From this, one easily deduces that $\widetilde{H}_{\mathcal{O}}(x) = (\widetilde{H}_{\mathcal{O}'}(x))^{|\ker(\varpi)|}$.

Now assume that $\mathcal{O}$ is maximal at p (i.e. $p \nmid f$). From Remark 5.2.2, $\iota : \mathcal{O} \to \mathcal{R}_0$ is an *optimal embedding* of $\mathcal{O}$ into $\mathcal{R}_0$, that is, $\iota(K) \cap \mathcal{R}_0 = \iota(\mathcal{O})$. Given an arbitrary maximal order $\mathcal{R}$ of B, we write $\mathrm{Emb}(\mathcal{O}, \mathcal{R})$ for the set of optimal embeddings of $\mathcal{O}$ into $\mathcal{R}$. The unit group $\mathcal{R}^\times$ acts on $\mathrm{Emb}(\mathcal{O}, \mathcal{R})$ by conjugation, and there are only finitely many orbits. Put $m(\mathcal{O}, \mathcal{R}, \mathcal{R}^\times) := |\mathcal{R}^\times \backslash \mathrm{Emb}(\mathcal{O}, \mathcal{R})|$, the number of $\mathcal{R}^\times$-conjugacy classes of optimal embeddings from $\mathcal{O}$ into $\mathcal{R}$. We recall below a precise formula by Elkies, Ono and Yang for the cardinality of each fiber of the reduction map $r_{\mathfrak{P}} : \mathcal{E}\ell\ell(\mathcal{O}) \to \mathcal{E}\ell\ell^{ss}_{/\overline{\mathbb{F}}_p}$.

Lemma 5.2.1 ([39, Lemma 3.3])**.** *Suppose that* $\mathcal{O}$ *is maximal at* p*. Then for any member* $E \in \mathcal{E}\ell\ell^{ss}_{/\overline{\mathbb{F}}_p}$*, we have*

$$|r_{\mathfrak{P}}^{-1}(E)| = \varepsilon \cdot m(\mathcal{O}, \mathcal{R}, \mathcal{R}^\times),$$

[1] A priori, the statement of [80, Proposition 15, §11] requires that $\mathcal{O} = \mathcal{O}_K$, the maximal order of K. Nevertheless, the result here holds for general $\mathcal{O}$ here since $\mathfrak{a}$ is an invertible $\mathcal{O}$-ideal by our assumption.

where $\mathcal{R} = \mathrm{End}(E)$*, and* $\varepsilon = 1/2$ *or* 1 *according as* p *is inert or ramified in* K*.*

A priori, [39, Lemma 3.3] is only stated for the maximal order $\mathcal{O}_K$. Nevertheless, the same proof there applies more generally to quadratic orders maximal at p. Alternatively, using Proposition 5.2.1 and the Deuring lifting theorem[2] [56, Theorem 14, §13.5] [45, Proposition 2.7], one easily sees that Lemma 5.2.1 is equivalent to to the following purely arithmetic result, whose independent proof will be left for the interested reader.

Lemma 5.2.2. *Keep* $\mathcal{O}$ *and* ε *as in Lemma 5.2.1. Let* $\mathcal{R}$ *be a maximal order in* B*, and* $\varphi : \mathcal{O} \hookrightarrow \mathcal{R}$ *be an optimal embedding. Denote the induced map* $\mathrm{Pic}(\mathcal{O}) \to \mathrm{Cl}(\mathcal{R})$ *by* φ *as well. Then for each* $[I] \in \mathrm{Cl}(\mathcal{R})$*, we have*

$$|\varphi^{-1}([I])| = \varepsilon \cdot m(\mathcal{O}, \mathcal{R}_r(I), \mathcal{R}_r(I)^\times).$$

We immediately obtain the following corollaries from Lemma 5.2.1.

Corollary 5.2.3. *Suppose that* $\mathcal{O}$ *is maximal at* p*. The* j*-invariant of a supersingluar elliptic curve* $E/\overline{\mathbb{F}}_p$ *is a root of* $\widetilde{H}_{\mathcal{O}}(x)$ *if and only if* $\mathcal{O}$ *can be optimally embedded into* $\mathrm{End}(E)$*.*

This matches well with Corollary 5.2.1. Indeed, a classical result of Chevalley, Hasse and Noether [47, §4] says that any maximal order of B that contains a copy of $\mathcal{O}$ optimally is isomorphic to $\mathfrak{a}^{-1}\mathcal{R}_0\mathfrak{a}$ for some $[\mathfrak{a}] \in \mathrm{Pic}(\mathcal{O})$.

Corollary 5.2.4. *If* $p > |\mathrm{disc}(\mathcal{O})|$*, then the reduction map* $r_{\mathfrak{P}} : \mathcal{E}\ell\ell(\mathcal{O}) \to \mathcal{E}\ell\ell^{ss}_{/\overline{\mathbb{F}}_p}$ *is injective. In particular,* $\widetilde{H}_{\mathcal{O}}(x)$ *has no repeated roots.*

We give a simple proof that is independent of the result of Gross and Zagier [45].

Proof. Since p does not split in K and is strictly greater than $|\mathrm{disc}(\mathcal{O})|$, it is necessarily inert in K. From Lemma 5.2.1, it suffices to show that $|\mathrm{Emb}(\mathcal{O}, \mathcal{R})| \leq 2$ for any maximal order $\mathcal{R}$ in B. Since $p > |\mathrm{disc}(\mathcal{O})|$, Kaneko's inequality [50, Theorem 2'] forces any two optimal embeddings $\varphi, \varphi' : \mathcal{O} \to \mathcal{R}$ to have the same image. On the other hand, φ and φ' share the same image if and only if $\varphi' = \varphi$ or $\bar{\varphi}$, the complex conjugate of φ. The desired inequality $|\mathrm{Emb}(\mathcal{O}, \mathcal{R})| \leq 2$ follows immediately. □

[2] Here the Deuring lifting theorem guarantees that the optimal embedding $\iota : \mathcal{O} \to \mathcal{R}_0$ is "non-special", that is, every optimal embedding $\varphi : \mathcal{O} \to \mathcal{R}$ is realizable as $\mathrm{End}(E) \to \mathrm{End}(\widetilde{E})$ for some $E \in \mathcal{E}\ell\ell(\mathcal{O})$.

Remark 5.2.5. In another direction, Elkies, Ono and Yang [39, Theorem 1.4] showed that there exists a bound N_p such that the reduction map $r_{\mathfrak{P}} : \mathcal{E}\ell\ell(\mathcal{O}_K) \to \mathcal{E}\ell\ell^{ss}_{/\overline{\mathbb{F}}_p}$ is surjective whenever $|\operatorname{disc}(\mathcal{O}_K)| > N_p$. This bound is first effectivized by Kane [49] conditionally upon the generalized Riemann hypothesis. Liu et al. further improved this bound in [60, Corollary 1.3].

Let us return to the task of interpreting $\mathbb{F}_p$-roots of $\widetilde{H}_{\mathcal{O}}(x) \in \mathbb{F}_p[x]$ in terms of maximal orders in B. For the rest of this section, we keep the additional assumption that $p > |\operatorname{disc}(\mathcal{O})|$. We recall from [36, Proposition 2.4] a classical result on supersingular elliptic curves in characteristic p.

Lemma 5.2.3. *Let $p > 3$ and let E be a supersingular elliptic curve over $\overline{\mathbb{F}}_p$. Then $j(E) \in \mathbb{F}_p$ if and only if there exists $\psi \in \operatorname{End}(E)$ such that $\psi^2 = -p$.*

Recall that $\mathcal{H}_p$ denotes the set of $\mathbb{F}_p$-roots of $\widetilde{H}_{\mathcal{O}}(x)$, which can be identified canonically with a subset of $\mathcal{E}\ell\ell^{ss}_{/\overline{\mathbb{F}}_p}$.

Lemma 5.2.4. *The map $\rho : \mathcal{E}\ell\ell^{ss}_{/\overline{\mathbb{F}}_p} \to \operatorname{Typ}(B)$ in (5.2.2) induces a bijection between $\mathcal{H}_p$ and the following subset $\mathcal{T}_p \subseteq \operatorname{Typ}(B)$:*

$$\mathcal{T}_p := \{[\mathcal{R}] \in \operatorname{Typ}(B) \mid \operatorname{Emb}(\mathcal{O}, \mathcal{R}) \neq \emptyset, \text{ and } \exists \alpha \in \mathcal{R} \text{ such that } \alpha^2 = -p\}. \tag{5.2.6}$$

Proof. Combining Corollary 5.2.3 and Lemma 5.2.3, we see that $\rho(\mathcal{H}_p) = \mathcal{T}_p$. Now it follows from [95, Lemma 42.4.1] that $\rho : \mathcal{H}_p \to \mathcal{T}_p$ is injective, and hence bijective. □

We give another characterization of $\mathcal{T}_p$ by presenting the quaternion algebra $B = B_{p,\infty}$ more concretely. Let $d \in \mathbb{N}$ be the unique square-free positive integer such that $K = \mathbb{Q}(\sqrt{-d})$. The assumption that p is inert in K amounts to the equality $\left(\frac{-d}{p}\right) = -1$. Let $\left(\frac{-d,-p}{\mathbb{Q}}\right)$ be the quaternion $\mathbb{Q}$-algebra with standard basis $\{1, \mathbf{i}, \mathbf{j}, \mathbf{k}\}$ such that

$$\mathbf{i}^2 = -d, \quad \mathbf{j}^2 = -p \quad \text{and} \quad \mathbf{k} = \mathbf{ij} = -\mathbf{ji}. \tag{5.2.7}$$

We identify $K = \mathbb{Q}(\sqrt{-d})$ with $\mathbb{Q}(\mathbf{i})$, and $\mathcal{O}$ with the corresponding order in $\mathbb{Q}(\mathbf{i})$. Put $\Lambda := \mathcal{O} + \mathbf{j}\mathcal{O}$, which is an order (of full rank) in the above quaternion algebra. Consider the following finite set

of maximal orders:

$$S^{\mathrm{opt}} := \left\{ \mathscr{R} \subset \left(\frac{-d,-p}{\mathbb{Q}}\right) \,\middle|\, \mathscr{R} \text{ is a maximal order containing } \Lambda \text{ and } \mathscr{R} \cap \mathbb{Q}(\mathbf{i}) = \mathcal{O} \right\}. \tag{5.2.8}$$

Here the superscript "opt" stands for "$\mathcal{O}$-optimal".

Proposition 5.2.2. *Let $\mathcal{R}$ be a maximal order in B. We have $[\mathcal{R}] \in \mathcal{T}_p$ if and only if $\mathcal{R} \simeq \mathscr{R}$ for some $\mathscr{R} \in S^{\mathrm{opt}}$. In particular, $\mathcal{H}_p \neq \emptyset$ if and only if $\left(\frac{-d,-p}{\mathbb{Q}}\right) \simeq B$ and $S^{\mathrm{opt}} \neq \emptyset$.*

Proof. Clearly, if $\mathcal{R} \simeq \mathscr{R}$ for some $\mathscr{R} \in S^{\mathrm{opt}}$, then $[\mathcal{R}] \in \mathcal{T}_p$. Conversely, suppose that $[\mathcal{R}] \in \mathcal{T}_p$, that is, $\mathcal{R}$ contains a copy of $\mathcal{O}$ optimally, and there exists $\alpha \in \mathcal{R}$ with $\alpha^2 = -p$. Then $\mathcal{R}\alpha$ is the unique two sided prime ideal of $\mathcal{R}$ lying above p. From [94, Exercise I.4.6], $\mathcal{R}$ is normalized by α, which implies that $\mathcal{O}_\alpha := \alpha\mathcal{O}\alpha^{-1}$ is still a quadratic order optimally embedded in $\mathcal{R}$. If $\mathcal{O}_\alpha \neq \mathcal{O}$, then $|\operatorname{disc}(\mathcal{O})| \geq p$ by Kaneko's inequality [50, Theorem 2'], contradicting to our assumption that $|\operatorname{disc}(\mathcal{O})| < p$. Thus $\mathcal{O}_\alpha = \mathcal{O}$, and conjugation by α induces an automorphism $\sigma \in \operatorname{Aut}(\mathcal{O})$. If σ is the identity, then α lies in the centralizer of $\mathcal{O}$ in B, which is just K. This contradicts to the assumption $|\operatorname{disc}(\mathcal{O})| < p$ again. It follows that σ is the unique nontrivial automorphism of $\mathcal{O}$, i.e. the complex conjugation. We conclude that $\Lambda_{\mathcal{R}} := \mathcal{O} + \alpha\mathcal{O} \subset \mathcal{R}$ is isomorphic to Λ, and $B = \Lambda_{\mathcal{R}} \otimes_{\mathbb{Z}} \mathbb{Q} \simeq \Lambda \otimes_{\mathbb{Z}} \mathbb{Q} = \left(\frac{-d,-p}{\mathbb{Q}}\right)$. Consequently, $\mathcal{R}$ is isomorphic to some member of S^{opt}. The last statement follows from the bijection $\mathcal{H}_p \simeq \mathcal{T}_p$ in Lemma 5.2.4. □

Lemma 5.2.5. *The isomorphism $\left(\frac{-d,-p}{\mathbb{Q}}\right) \simeq B$ holds if and only if $\left(\frac{-p}{\ell}\right) = 1$ for every odd prime factor ℓ of d.*

Proof. For the moment, let ℓ be either a prime number or ∞. Write $(-d,-p)_\ell$ for the Hilbert symbol of $-d$ and $-p$ relative to $\mathbb{Q}_\ell$ (where $\mathbb{Q}_\infty = \mathbb{R}$). From [94, Corollaire II.1.2], $\left(\frac{-d,-p}{\mathbb{Q}}\right)$ is split at ℓ if and only if $(-d,-p)_\ell = 1$. Clearly, $(-d,-p)_\infty = -1$.

Now assume that ℓ is an odd prime. By our assumption, p is an odd prime satisfying

$\left(\frac{-d}{p}\right) = -1$. From [78, Theorem 1, §III.1], we easily compute that

$$(-d,-p)_\ell = \begin{cases} 1 & \text{if } \ell \nmid (dp); \\ -1 & \text{if } \ell = p; \\ \left(\frac{-p}{\ell}\right) & \text{if } \ell | d. \end{cases}$$

Therefore, if $\left(\frac{-d,-p}{\mathbb{Q}}\right) \simeq B$, then necessarily $\left(\frac{-p}{\ell}\right) = 1$ for every odd prime factor ℓ of d.

Conversely, if $\left(\frac{-p}{\ell}\right) = 1$ for every odd prime factor ℓ of d, then $(-d,-p)_2 = 1$ by the product formula [78, Theorem 2, §III.2]. Hence this condition is also sufficient for the isomorphism $\left(\frac{-d,-p}{\mathbb{Q}}\right) \simeq B$. □

5.3 The $\mathrm{Pic}(\mathcal{O})[2]$-action on $\mathcal{H}_p$ and the nonemptiness criterion

Throughout this section, we assume that p is inert in $K = \mathbb{Q}(\sqrt{-d})$ and strictly greater than $|\operatorname{disc}(\mathcal{O})|$. Assume further that the quaternion $\mathbb{Q}$-algebra $\left(\frac{-d,-p}{\mathbb{Q}}\right)$ is ramified precisely at p and infinity, for otherwise $\mathcal{H}_p = \emptyset$. Denote $\left(\frac{-d,-p}{\mathbb{Q}}\right)$ simply by B henceforth and let $\{1, \mathbf{i}, \mathbf{j}, \mathbf{k}\}$ be the standard basis of B as in (5.2.7). We identify K with the subfield $\mathbb{Q}(\mathbf{i})$ of B. Then conjugation by $\mathbf{j}$ stabilizes K and sends each $x \in K$ to its complex conjugate $\bar{x}$. Let $\Lambda = \mathcal{O} + \mathbf{j}\mathcal{O}$, and S^{opt} be the set of maximal orders in (5.2.8).

First, we assume that $\mathcal{H}_p \neq \emptyset$ and exhibit a regular action of $\mathrm{Pic}(\mathcal{O})[2]$ on $\mathcal{H}_p$. Since the reduction map $r_{\mathfrak{P}} : \mathcal{E}\ell\ell(\mathcal{O}) \to \mathcal{E}\ell\ell^{ss}_{/\overline{\mathbb{F}}_p}$ is injective by Corollary 5.2.4, the regular action of $\mathrm{Pic}(\mathcal{O})$ on $\mathcal{E}\ell\ell(\mathcal{O})$ induces a regular action of $\mathrm{Pic}(\mathcal{O})$ on the image $r_{\mathfrak{P}}(\mathcal{E}\ell\ell(\mathcal{O}))$ (or equivalently, on the full set of roots of $\widetilde{H}_{\mathcal{O}}(x)$). We show that this action restricts to a regular $\mathrm{Pic}(\mathcal{O})[2]$-action on $\mathcal{H}_p$.

Proposition 5.3.1. *Let $E_0 \in \mathcal{E}\ell\ell(\mathcal{O})$ be a member satisfying $j(\widetilde{E}_0) \in \mathbb{F}_p$. Given $[\mathfrak{a}] \in \mathrm{Pic}(\mathcal{O})$, we have $j(\widetilde{E_0^{\mathfrak{a}}}) \in \mathbb{F}_p$ if and only if $[\mathfrak{a}]$ is a 2-torsion. In particular, $\mathrm{Pic}(\mathcal{O})[2]$ acts regularly on $\mathcal{H}_p$.*

Proof. Put $\mathcal{R}_0 := \mathrm{End}(\widetilde{E}_0)$ and $\mathcal{R} := \mathfrak{a}^{-1}\mathcal{R}_0\mathfrak{a}$ so that $\mathrm{End}(\widetilde{E_0^{\mathfrak{a}}}) \simeq \mathcal{R}$ by Corollary 5.2.1. From Lemma 5.2.3, it is enough to show that there exists $\alpha \in \mathcal{R}$ with $\alpha^2 = -p$ if and only if $[\mathfrak{a}] \in \mathrm{Pic}(\mathcal{O})[2]$. By Proposition 5.2.2, we may assume that $\mathcal{R}_0 \in S^{\mathrm{opt}}$, that is, $\mathcal{R}_0$ is a maximal order in

B satisfying $\mathcal{R}_0 \supseteq \mathcal{O} + \mathbf{j}\mathcal{O}$ and $\mathcal{R}_0 \cap K = \mathcal{O}$. Then

$$\mathcal{R} \cap K = \mathfrak{a}^{-1}(\mathcal{R}_0 \cap K)\mathfrak{a} = \mathcal{O}, \quad \text{and} \quad \mathcal{R} \supseteq \mathfrak{a}^{-1}\mathbf{j}\mathfrak{a} = \mathfrak{a}^{-1}\bar{\mathfrak{a}}\mathbf{j}. \tag{5.3.1}$$

First, suppose that $[\mathfrak{a}] \in \mathrm{Pic}(\mathcal{O})[2]$. Then $\mathfrak{a}^{-1}\bar{\mathfrak{a}} = \mathcal{O}a$ for some $a \in K^\times$. Moreover, $N_{K/\mathbb{Q}}(\mathcal{O}a) = N_{K/\mathbb{Q}}(\mathfrak{a}^{-1}\bar{\mathfrak{a}}) = \mathbb{Z}$, so $N_{K/\mathbb{Q}}(a) = 1$. Therefore $\alpha := a\mathbf{j} \in \mathcal{R}$ satisfies that $\alpha^2 = a\bar{a}\mathbf{j}^2 = -p$.

Conversely, suppose that $\alpha \in \mathcal{R}$ is an element satisfying $\alpha^2 = -p$. From the proof of Proposition 5.2.2, we must have $\alpha x = \bar{x}\alpha$ for every $x \in \mathcal{O}$. Thus $\mathbf{j}^{-1}\alpha$ centralizes $\mathcal{O}$, so there exists $a \in K^\times$ such that $\alpha = \mathbf{j}a$. Moreover, $N_{K/\mathbb{Q}}(a) = 1$ since $\alpha^2 = \mathbf{j}^2\bar{a}a$. Now we have

$$\mathcal{R} \supset \mathfrak{a}^{-1}\bar{\mathfrak{a}}\mathbf{j} \cdot \alpha = \mathfrak{a}^{-1}\bar{\mathfrak{a}}\mathbf{j} \cdot \mathbf{j}a = -pa\mathfrak{a}^{-1}\bar{\mathfrak{a}}. \tag{5.3.2}$$

We claim that $\mathcal{R} \supset a\mathfrak{a}^{-1}\bar{\mathfrak{a}}$. It suffices to show that $\mathcal{R}_\ell \supset a\mathfrak{a}_\ell^{-1}\bar{\mathfrak{a}}_\ell$ for every prime $\ell \in \mathbb{N}$, where the subscript $_\ell$ indicates ℓ-adic completion at ℓ. If $\ell \neq p$, then $(-p) \in \mathcal{R}_\ell^\times$, so the containment follows directly from (5.3.2). If $\ell = p$, then $\mathcal{R}_p$ coincides with the unique maximal order of the division quaternion $\mathbb{Q}_p$-algebra B_p. More concretely, $\mathcal{R}_p = \{z \in B_p \mid \mathrm{nrd}(z) \in \mathbb{Z}_p\}$, where $\mathrm{nrd}(z)$ denotes the reduced norm of $z \in B_p$. On the other hand, for any $x_p \in \mathfrak{a}_p^{-1}$ and $y_p \in \mathfrak{a}_p$, we have $x_p y_p \in \mathcal{O}_p$, and hence $\mathrm{nrd}(ax_p\bar{y}_p) = \mathrm{nrd}(x_p)\,\mathrm{nrd}(\bar{y}_p) = \mathrm{nrd}(x_p y_p) \in \mathbb{Z}_p$. Since $\mathfrak{a}_p^{-1}\bar{\mathfrak{a}}_p$ is generated by elements of the form $x_p\bar{y}_p$, it follows that $\mathcal{R}_p \supset a\mathfrak{a}_p^{-1}\bar{\mathfrak{a}}_p$. The claim is verified. Now $a\mathfrak{a}^{-1}\bar{\mathfrak{a}} \subseteq \mathcal{R} \cap K = \mathcal{O}$, which implies that $a\bar{\mathfrak{a}} \subseteq \mathfrak{a}$. Comparing discriminants on both sides, we get $\mathrm{disc}(a\bar{\mathfrak{a}}) = N_{K/\mathbb{Q}}(a)^2\,\mathrm{disc}(\bar{\mathfrak{a}}) = \mathrm{disc}(\mathfrak{a})$. Therefore, $a\bar{\mathfrak{a}} = \mathfrak{a}$, so $[\mathfrak{a}] \in \mathrm{Pic}(\mathcal{O})[2]$. □

Now we drop the assumption that $\mathcal{H}_p \neq \emptyset$ and derive a non-emptiness criterion for $\mathcal{H}_p$. From Proposition 5.2.2, $\mathcal{H}_p \neq \emptyset$ if and only if $S^{\mathrm{opt}} \neq \emptyset$ (as we have already assumed that $\left(\frac{-d,-p}{\mathbb{Q}}\right) \simeq B_{p,\infty}$). For each prime $\ell \in \mathbb{N}$, let us put

$$S_\ell^{\mathrm{opt}} := \{\mathcal{R}_\ell \subseteq B_\ell \mid \mathcal{R}_\ell \text{ is a maximal order containing } \Lambda_\ell \text{ and } \mathcal{R}_\ell \cap K_\ell = \mathcal{O}_\ell\}.$$

The local-global correspondence of lattices [31, Proposition 4.21] establishes a bijection between S^{opt} and $\prod_\ell S_\ell^{\mathrm{opt}}$, where the product runs over all prime ℓ. Since the reduced discriminant of B

is p and the reduced discriminant of Λ is $p\,\mathrm{disc}(\mathcal{O})$ by [59, Lemmas 2.7 and 2.9], Λ is maximal at every prime ℓ coprime to $\mathrm{disc}(\mathcal{O})$. Moreover, for each such ℓ, the maximal order Λ_ℓ automatically satisfies the condition $\Lambda_\ell \cap K_\ell = \mathcal{O}_\ell$ by its definition $\Lambda_\ell = \mathcal{O}_\ell + j\mathcal{O}_\ell$. Hence for $\ell \nmid \mathrm{disc}(\mathcal{O})$, the set S_ℓ^{opt} has a single element Λ_ℓ, and the bijection above simplifies as

$$S^{\mathrm{opt}} \longleftrightarrow \prod_{\ell \mid \mathrm{disc}(\mathcal{O})} S_\ell^{\mathrm{opt}}. \tag{5.3.3}$$

Lemma 5.3.1. *Let ℓ be a prime factor of $\mathrm{disc}(\mathcal{O})$. Then $S_\ell^{\mathrm{opt}} \neq \emptyset$ if and only if $-p \in N_{K/\mathbb{Q}}(\mathcal{O}_\ell^\times)$. Moreover, if $S_\ell^{\mathrm{opt}} \neq \emptyset$, then there is a regular action of $H^1(K/\mathbb{Q}, \mathcal{O}_\ell^\times)$ on S_ℓ^{opt}, so any fixed member of S_ℓ^{opt} gives rise to a bijection $S_\ell^{\mathrm{opt}} \simeq H^1(K/\mathbb{Q}, \mathcal{O}_\ell^\times)$.*

The Galois cohomological description of S_ℓ^{opt} is nice to know but not used elsewhere in this chapter.

Proof. By our assumption, $\mathrm{disc}(\mathcal{O})$ is coprime to p, so B splits at the prime ℓ. This allows us to identify B_ℓ with the matrix algebra $M_2(\mathbb{Q}_\ell)$. Let $V_\ell = \mathbb{Q}_\ell^2$ be the unique simple B_ℓ-module. Every maximal order $\mathcal{R}_\ell$ in B_ℓ is of the form $\mathrm{End}_{\mathbb{Z}_\ell}(L_\ell)$ for some $\mathbb{Z}_\ell$-lattice $L_\ell \subseteq V_\ell$, and L_ℓ is uniquely determined by $\mathcal{R}_\ell$ up to $\mathbb{Q}_\ell^\times$-homothety. In other words, $\mathrm{End}_{\mathbb{Z}_\ell}(L_\ell) = \mathrm{End}_{\mathbb{Z}_\ell}(L'_\ell)$ if and only if $L_\ell = cL'_\ell$ for some $c \in \mathbb{Q}_\ell^\times$. If $\mathcal{R}_\ell \in S_\ell^{\mathrm{opt}}$, then the inclusion $\Lambda_\ell \subseteq \mathcal{R}_\ell$ puts a Λ_ℓ-module structure on L_ℓ. Moreover, the Λ_ℓ-lattice L_ℓ is $\mathcal{O}_\ell$-*optimal* in the sense that $\mathrm{End}_{\mathbb{Z}_\ell}(L_\ell) \cap K_\ell = \mathcal{O}_\ell$. Conversely, if M_ℓ is an $\mathcal{O}_\ell$-optimal Λ_ℓ-lattice in V_ℓ, then $\mathrm{End}_{\mathbb{Z}_\ell}(M_\ell)$ is a member of S_ℓ^{opt}. We have established the following canonical bijection

$$\mathcal{S}_\ell^{\mathrm{opt}} \longleftrightarrow \mathcal{M} := \{\mathcal{O}_\ell\text{-optimal } \Lambda_\ell\text{-lattices } L_\ell \subset V_\ell\}/\mathbb{Q}_\ell^\times. \tag{5.3.4}$$

Recall that $\Lambda_\ell = \mathcal{O}_\ell + \mathbf{j}\mathcal{O}_\ell$, where $\mathbf{j}^2 = -p$ and $\mathbf{j}x = \bar{x}\mathbf{j}$ for any $x \in \mathcal{O}_\ell$. If there exists $a \in \mathcal{O}_\ell^\times$ satisfying $a\bar{a} = -p$, then we can put a Λ_ℓ-module structure on $\mathcal{O}_\ell$ as follows:

$$(x + \mathbf{j}y) \cdot z = xz + \bar{y}\bar{z}a, \qquad \forall x, y, z \in \mathcal{O}_\ell.$$

Since $B_\ell = \Lambda_\ell \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$, this also puts a B_ℓ-module structure on $K_\ell = \mathcal{O}_\ell \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$. Consequently, it

identifies K_ℓ with the unique simple B_ℓ-module V_ℓ, and in turn identifies $\mathcal{O}_\ell$ with a Λ_ℓ-lattice L_ℓ in V_ℓ. Necessarily, L_ℓ is $\mathcal{O}_\ell$-optimal since $\mathrm{End}_{\mathbb{Z}_\ell}(L_\ell) \cap K_\ell = \mathrm{End}_{\mathcal{O}_\ell}(L_\ell) = \mathrm{End}_{\mathcal{O}_\ell}(\mathcal{O}_\ell) = \mathcal{O}_\ell$. We have shown that if $-p \in N_{K/\mathbb{Q}}(\mathcal{O}_\ell^\times)$, then $S_\ell^{\mathrm{opt}} \neq \emptyset$.

Conversely, suppose that $S_\ell^{\mathrm{opt}} \neq \emptyset$ and let M_ℓ be an $\mathcal{O}_\ell$-optimal Λ_ℓ-lattice in V_ℓ. The inclusion $\mathcal{O}_\ell \subset \Lambda_\ell$ equips M_ℓ with an $\mathcal{O}_\ell$-module structure satisfying $\mathrm{End}_{\mathcal{O}_\ell}(M_\ell) = \mathcal{O}_\ell$. Being a quadratic $\mathbb{Z}_\ell$-order, $\mathcal{O}_\ell$ is both Gorenstein and semi-local. It follows from [92, Characterization B 4.2] that M_ℓ is a free $\mathcal{O}_\ell$-module of rank one. Pick a basis e so that $M_\ell = \mathcal{O}_\ell e$. Since M_ℓ is at the same time a module over Λ_ℓ, we have $je = ae$ for some $a \in \mathcal{O}_\ell$. Necessarily, $\bar{a}a = -p$ because

$$-pe = \mathbf{j}^2 e = \mathbf{j}(\mathbf{j}e) = \mathbf{j}(ae) = \bar{a}je = \bar{a}ae.$$

This also implies that $a \in \mathcal{O}_\ell^\times$ since $\ell \neq p$. Therefore, $S_\ell^{\mathrm{opt}} \neq \emptyset$ if and only if $-p \in N_{K/\mathbb{Q}}(\mathcal{O}_\ell^\times)$.

Had we picked a different basis e' for M_ℓ, then $e' = ue$ for some $u \in \mathcal{O}_\ell^\times$. It follows that

$$\mathbf{j}e' = \mathbf{j}(ue) = \bar{u}\mathbf{j}e = \bar{u}ae = u^{-1}\bar{u}ae'.$$

Correspondingly, a is changed to $u^{-1}\bar{u}a$. Therefore, we have defined the following map:

$$\Phi : \mathcal{M} \to \{a \in \mathcal{O}_\ell^\times \mid a\bar{a} = -p\}/\sim, \tag{5.3.5}$$

where $a \sim a'$ if and only if there exists some $u \in \mathcal{O}_\ell^\times$ such that $a' = a(\bar{u}/u)$. We have already seen that Φ is surjective. Suppose that $\Phi([M_1]) = \Phi([M_2])$ for $[M_r] \in \mathcal{M}$ with $r = 1, 2$. By the above discussion, we can choose suitable $\mathcal{O}_\ell$-base e_r for M_r such that they give rise to the same $a \in \mathcal{O}_\ell^\times$. Then the $\mathcal{O}_\ell$-linear map sending e_1 to e_2 defines a Λ_ℓ-isomorphism between M_1 and M_2. Since $\mathrm{Aut}_{B_\ell}(V_\ell) = \mathbb{Q}_\ell^\times$, it follows that M_1 and M_2 are $\mathbb{Q}_\ell^\times$-homothetic, so Φ is injective as well.

Lastly, if the right hand side of (5.3.5) is nonempty, then it admits a regular action by $H^1(K/\mathbb{Q}, \mathcal{O}_\ell^\times) = \{b \in \mathcal{O}_\ell^\times \mid \bar{b}b = 1\}/\sim$ via multiplication. The second part of the lemma follows by combining the bijections (5.3.4) and (5.3.5) with the above action. □

Lemma 5.3.2. *Let ℓ be a prime factor of* $\mathrm{disc}(\mathcal{O})$. *Then $-p \in N_{K/\mathbb{Q}}(\mathcal{O}_\ell^\times)$ if and only if either condition (i) or (ii) below holds for ℓ depending on its parity:*

(i) $\ell \neq 2$ *and* $\left(\frac{-p}{\ell}\right) = 1$*;*

(ii) $\ell = 2$ *and one of the following conditions holds:*

(a) $p \equiv 7 \pmod 8$*;*

(b) $-p + \frac{\mathrm{disc}(\mathcal{O})}{4} \equiv 0,\ 1$ *or* $4 \pmod 8$*;*

(c) $-p + \mathrm{disc}(\mathcal{O}) \equiv 1 \pmod 8$.

Proof. For simplicity, put $D := \mathrm{disc}(\mathcal{O})$ and $\delta = \frac{1}{2}\sqrt{D}$. We claim that $\mathcal{O}_\ell = \mathbb{Z}_\ell + \mathbb{Z}_\ell\delta$. It is well known that $\mathcal{O} = \mathbb{Z} + \mathbb{Z}(D + \sqrt{D})/2$. The claim is obviously true if $4|D$. If $4 \nmid D$, then $\ell \neq 2$, so the claim is true in this case as well. Given an element $a + b\delta \in \mathcal{O}_\ell$ with $a, b \in \mathbb{Z}_\ell$, we have $N_{K/\mathbb{Q}}(a + b\delta) = a^2 - b^2D/4$. Therefore, $-p \in N_{K/\mathbb{Q}}(\mathcal{O}_\ell^\times)$ if and only if the equation

$$x^2 - y^2\frac{D}{4} = -p \tag{5.3.6}$$

has a solution in $\mathbb{Z}_\ell^2$.

First, suppose that ℓ is odd. Then equation (5.3.6) is solvable in $\mathbb{Z}_\ell^2$ if and only if $\left(\frac{-p}{\ell}\right) = 1$. Indeed, suppose $\left(\frac{-p}{\ell}\right) = 1$ so that $-p$ is a square in $\mathbb{F}_\ell$. By Hensel's lemma [95, Lemma 12.2.17], the equation $x^2 = -p$ has a solution $x_0 \in \mathbb{Z}_\ell$. Hence $(x_0, 0)$ is a solution of (5.3.6) in $\mathbb{Z}_\ell^2$. Conversely, suppose (5.3.6) has a solution $(x_0, y_0) \in \mathbb{Z}_\ell^2$. Reducing (5.3.6) modulo ℓ shows that $x_0 \pmod \ell$ is a square root of $-p$ in $\mathbb{F}_\ell$, i.e. $\left(\frac{-p}{\ell}\right) = 1$.

For the rest of the proof we assume that $\ell = 2$, which implies that $4|D$. First, suppose that $(x, y) \in \mathbb{Z}_2^2$ is a solution of (5.3.6). Since $x^2,\ y^2 \equiv 0,\ 1$ or $4 \pmod 8$ and at least one of x, y lies in $\mathbb{Z}_2^\times$ because p is odd, we see that the pair (x^2, y^2) takes on five possibilities modulo 8:

$$(x^2, y^2) \equiv (0,1),\ (1,0),\ (1,1),\ (1,4) \text{ and } (4,1) \pmod 8.$$

Each possibility puts the following respective constraint on p and D:

$$-p + \frac{D}{4} \equiv 0 \pmod 8, \qquad -p \equiv 1 \pmod 8, \qquad -p + \frac{D}{4} \equiv 1 \pmod 8,$$
$$-p + D \equiv 1 \pmod 8, \qquad -p + \frac{D}{4} \equiv 4 \pmod 8.$$

We have proved the necessity part of the lemma for the case $\ell = 2$.

Conversely, let us show that the above congruence conditions are also sufficient. From the discussion above, each of these conditions guarantees the existence of a solution $(\tilde{x}, \tilde{y})$ of equation (5.3.6) in $(\mathbb{Z}/8\mathbb{Z})^2$ such that either $\tilde{x}$ or $\tilde{y}D/4$ lies in $(\mathbb{Z}/8\mathbb{Z})^\times$. Now from a multivariate version of Hensel's lemma [95, Lemma 12.2.8], the pair $(\tilde{x}, \tilde{y})$ lifts to a solution of (5.3.6) in $\mathbb{Z}_2^2$. The sufficiency is proved.

Therefore, $-p \in N_{K/\mathbb{Q}}(\mathcal{O}_2^\times)$ if and only if one of the following conditions holds:

(a) $p \equiv 7 \pmod 8$;

(b) $-p + \frac{\mathrm{disc}(\mathcal{O})}{4} \equiv 0,\ 1 \text{ or } 4 \pmod 8$;

(c) $-p + \mathrm{disc}(\mathcal{O}) \equiv 1 \pmod 8$.

□

Proof of Theorem 5.1.1. If $\mathcal{H}_p \neq \emptyset$, then there is a regular action of $\mathrm{Pic}(\mathcal{O})[2]$ on $\mathcal{H}_p$ by Proposition 5.3.1. The criterion for the nonemptiness of $\mathcal{H}_p$ follows from combining Proposition 5.2.2 with equation (5.3.3) and Lemmas 5.2.5, 5.3.1 and 5.3.2. □

Chapters 5 is, in full, being prepared for submission for publication. The dissertation author was the collaborator and the coauthor for the material below.

- Mingjie Chen, Jiangwei Xue "On $\mathbb{F}_p$-roots of the Hilbert class polynomial modulo p".

Bibliography

[1] Z. Amir-Khosravi. Serre's tensor construction and moduli of abelian schemes. *Manuscripta Math.*, 156(3-4):409–456, 2018.

[2] T. M. Apostol. *Introduction to analytic number theory*. Undergraduate Texts in Mathematics. Springer-Verlag, New York-Heidelberg, 1976.

[3] S. Arpin. PhD thesis, University of Colorado Boulder. In preparation for May 2022.

[4] S. Arpin, M. Chen, K. E. Lauter, R. Scheidler, K. E. Stange, and H. T. N. Tran. Orientations and cycles in supersingular isogeny graphs, 2022. In preparation.

[5] S. Arpin, M. Chen, K. E. Lauter, R. Scheidler, K. E. Stange, and H. T. N. Tran. Win5 github repository, 2022. `https://github.com/SarahArpin/WIN5`.

[6] E. Assaf. Computing classical modular forms for arbitrary congruence subgroups. *arXiv: Number Theory*, 2020.

[7] J. Balakrishnan and N. Dogra. Quadratic chabauty and rational points ii: Generalised height functions on selmer varieties. *International Mathematics Research Notices*, 04 2017.

[8] J. Balakrishnan, N. Dogra, J. S. Müller, J. Tuitman, and J. Vonk. Explicit Chabauty-Kim for the split Cartan modular curve of level 13. *Ann. of Math. (2)*, 189(3):885–944, 2019.

[9] J. Balakrishnan and J. Tuitman. Magma code. `https://github.com/jtuitman/Coleman`, 2022.

[10] J. S. Balakrishnan, R. W. Bradshaw, and K. S. Kedlaya. Explicit coleman integration for hyperelliptic curves. In G. Hanrot, F. Morain, and E. Thomé, editors, *Algorithmic Number Theory*, pages 16–31, Berlin, Heidelberg, 2010. Springer Berlin Heidelberg.

[11] J. S. Balakrishnan and N. Dogra. Quadratic Chabauty and rational points, I: p-adic heights. *Duke Math. J.*, 167(11):1981–2038, 2018. With an appendix by J. Steffen Müller.

[12] J. S. Balakrishnan and N. Dogra. An effective Chabauty-Kim theorem. *Compos. Math.*, 155(6):1057–1075, 2019.

[13] J. S. Balakrishnan and J. Tuitman. Explicit coleman integration for curves. *Math. Comput.*, 89:2965–2984, 2020.

[14] E. Bank, C. Camacho-Navarro, K. Eisenträger, T. Morrison, and J. Park. Cycles in the supersingular l-isogeny graph and corresponding endomorphisms. In *Research Directions in Number Theory*, pages 41–66. Springer, 2019.

[15] Y. Bilu and P. Parent. Serre's uniformity problem in the split Cartan case. *Ann. of Math. (2)*, 173(1):569–584, 2011.

[16] Y. Bilu, P. Parent, and M. Rebolledo. Rational points on $X_0^+(p^r)$. *Ann. Inst. Fourier (Grenoble)*, 63(3):957–984, 2013.

[17] R. Bröker, D. Charles, and K. Lauter. Evaluating large degree isogenies and applications to pairing based cryptography. In *Pairing-based cryptography—Pairing 2008*, volume 5209 of *Lecture Notes in Comput. Sci.*, pages 100–112. Springer, Berlin, 2008.

[18] W. Castryck, T. Lange, C. Martindale, L. Panny, and J. Renes. CSIDH: an efficient post-quantum commutative group action. In *Advances in cryptology—ASIACRYPT 2018. Part III*, volume 11274 of *Lecture Notes in Comput. Sci.*, pages 395–427. Springer, Cham, 2018.

[19] W. Castryck, L. Panny, and F. Vercauteren. *Rational Isogenies from Irrational Endomorphisms*, pages 523–548. 05 2020.

[20] C.-L. Chai, B. Conrad, and F. Oort. *Complex multiplication and lifting problems*, volume 195 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 2014.

[21] D. X. Charles, K. E. Lauter, and E. Z. Goren. Cryptographic hash functions from expander graphs. *J. Cryptology*, 22(1):93–113, 2009.

[22] M. Chenu and B. Smith. Higher-degree supersingular group actions. *Mathematical Cryptology*, 2021.

[23] H. Cohen. *A Course in Computational Algebraic Number Theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag Berlin Heidelberg, 1993.

[24] R. Coleman and E. de Shalit. p-adic regulators on curves and special values of p-adic L-functions. *Invent. Math.*, 93(2):239–266, 1988.

[25] R. F. Coleman. Effective Chabauty. *Duke Mathematical Journal*, 52(3):765 – 770, 1985.

[26] R. F. Coleman. Torsion points on curves and p-adic abelian integrals. *Ann. of Math. (2)*, 121(1):111–168, 1985.

[27] L. Colò and D. Kohel. Orienting supersingular isogeny graphs. *J. Math. Cryptol.*, 14(1):414–437, 2020.

[28] J.-S. Coron and D. Naccache. Security analysis of the gennaro-halevi-rabin signature scheme. In *EUROCRYPT*, 2000.

[29] D. A. Cox. *Primes of the form $x^2 + ny^2$*. Pure and Applied Mathematics (Hoboken). John Wiley & Sons, Inc., Hoboken, NJ, second edition, 2013. Fermat, class field theory, and complex multiplication.

[30] E. Croot, A. Granville, R. Pemantle, and P. Tetali. On sharp transitions in making squares. *Annals of Mathematics*, 175(3):1507–1550, 2012.

[31] C. W. Curtis and I. Reiner. *Methods of representation theory. Vol. I.* Wiley Classics Library. John Wiley & Sons, Inc., New York, 1990. With applications to finite groups and orders, Reprint of the 1981 original, A Wiley-Interscience Publication.

[32] L. De Feo. Mathematics of isogeny based cryptography. 2017. https://arxiv.org/abs/1711.04062.

[33] L. De Feo, C. Delpech de Saint Guilhem, T. B. Fouotsa, P. Kutas, A. Leroux, C. Petit, J. Silva, and B. Wesolowski. *Séta: Supersingular Encryption from Torsion Attacks*, pages 249–278. Advances in Cryptology – ASIACRYPT 2021. Springer International Publishing, Cham, 2021.

[34] L. De Feo, J. Kieffer, and B. Smith. Towards practical key exchange from ordinary isogeny graphs. In *Advances in cryptology—ASIACRYPT 2018. Part III*, volume 11274 of *Lecture Notes in Comput. Sci.*, pages 365–394. Springer, Cham, 2018.

[35] V. de Quehen, P. Kutas, C. Leonardi, C. Martindale, L. Panny, C. Petit, and K. E. Stange. *Improved Torsion-Point Attacks on SIDH Variants*, pages 432–470. Advances in Cryptology – CRYPTO 2021. Springer International Publishing, Cham, 2021.

[36] C. Delfs and S. D. Galbraith. Computing isogenies between supersingular elliptic curves over $\mathbb{F}_p$. *Designs, Codes and Cryptography*, 78(425-440), 2016.

[37] F. Diamond and J. Shurman. *A first course in modular forms*, volume 228 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2005.

[38] K. Eisenträger, S. Hallgren, K. Lauter, T. Morrison, and C. Petit. Supersingular isogeny graphs and endomorphism rings: reductions and solutions. In *Advances in cryptology—EUROCRYPT 2018. Part III*, volume 10822 of *Lecture Notes in Comput. Sci.*, pages 329–368. Springer, Cham, 2018.

[39] N. Elkies, K. Ono, and T. Yang. Reduction of CM elliptic curves and modular function congruences. *Int. Math. Res. Not.*, (44):2695–2707, 2005.

[40] N. D. Elkies. The existence of infinitely many supersingular primes for every elliptic curve over $\mathbf{Q}$. *Invent. Math.*, 89(3):561–567, 1987.

[41] F. Fité and A. V. Sutherland. Sato-Tate groups of $y^2 = x^8 + c$ and $y^2 = x^7 - cx$. In *Frobenius distributions: Lang-Trotter and Sato-Tate conjectures*, volume 663 of *Contemp. Math.*, pages 103–126. Amer. Math. Soc., Providence, RI, 2016.

[42] S. D. Galbraith. Equations for modular curves. *DPhil thesis, University of Oxford*, 1996.

[43] S. D. Galbraith. Rational points on $X_0^+(p)$. *Experiment. Math.*, 8(4):311–318, 1 1999.

[44] S. D. Galbraith, C. Petit, and J. Silva. Identification protocols and signature schemes based on supersingular isogeny problems. *J. Cryptology*, 33(1):130–175, 2020.

[45] B. H. Gross and D. B. Zagier. On singular moduli. *J. Reine Angew. Math.*, 355:191–220, 1985.

[46] D. Harvey and J. van Der Hoeven. Polynomial multiplication over finite fields in time $O(n \log n)$. 2019. https://hal.archives-ouvertes.fr/hal-02070816/document.

[47] T. Ibukiyama. On maximal orders of division quaternion algebras over the rational number field with certain optimal embeddings. *Nagoya Math. J.*, 88:181–195, 1982.

[48] S. Ionica and A. Joux. Pairing the volcano. In *Algorithmic number theory*, volume 6197 of *Lecture Notes in Comput. Sci.*, pages 201–208. Springer, Berlin, 2010.

[49] B. Kane. CM liftings of supersingular elliptic curves. *J. Théor. Nombres Bordeaux*, 21(3):635–663, 2009.

[50] M. Kaneko. Supersingular j-invariants as singular moduli mod p. *Osaka J. Math.*, 26(4):849–855, 1989.

[51] K. S. Kedlaya. Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology. *J. Ramanujan Math. Soc.*, 16(4):323–338, 2001.

[52] J. Kieffer. Accelerating the couveignes rostovtsev stolbunov key exchange protocol. Master's thesis, l'Université Paris IV, 2018. https://arxiv.org/pdf/1804.10128.pdf.

[53] D. E. Knuth. *The art of computer programming. Vol. 2.* Addison-Wesley Series in Computer Science and Information Processing. Addison-Wesley Publishing Co., Reading, Mass., second edition, 1981. Seminumerical algorithms.

[54] D. Kohel, K. Lauter, C. Petit, and J.-P. Tignol. On the quaternion ℓ-isogeny path problem. *LMS Journal of Computation and Mathematics*, 2014.

[55] D. R. Kohel. *Endomorphism rings of elliptic curves over finite fields.* PhD thesis, University of California at Berkeley, 1996.

[56] S. Lang. *Elliptic functions*, volume 112 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1987. With an appendix by J. Tate.

[57] H. W. Lenstra, Jr. Complex multiplication structure of elliptic curves. *J. Number Theory*, 56(2):227–241, 1996.

[58] J. Li, S. Li, and Y. Ouyang. Factorization of hilbert class polynomials over prime fields, 2021. https://arxiv.org/abs/2108.00168.

[59] Q. Li, J. Xue, and C.-F. Yu. Unit groups of maximal orders in totally definite quaternion algebras over real quadratic fields. *Trans. Amer. Math. Soc.*, 374(8):5349–5403, 2021.

[60] S.-C. Liu, R. Masri, and M. P. Young. Rankin-Selberg L-functions and the reduction of CM elliptic curves. *Res. Math. Sci.*, 2:Art. 22, 23, 2015.

[61] T. LMFDB Collaboration. The L-functions and modular forms database. http://www.lmfdb.org, 2022.

[62] J. Love and D. Boneh. Supersingular curves with small non-integer endomorphisms, 2020. https://arxiv.org/abs/1910.03180.

[63] J. Love and D. Boneh. Supersingular curves with small noninteger endomorphisms. In *ANTS XIV—Proceedings of the Fourteenth Algorithmic Number Theory Symposium*, volume 4 of *Open Book Ser.*, pages 7–22. Math. Sci. Publ., Berkeley, CA, 2020.

[64] B. Mazur. Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.*, (47):33–186 (1978), 1977. With an appendix by Mazur and M. Rapoport.

[65] B. Mazur. Rational points on modular curves. In J.-P. Serre and D. B. Zagier, editors, *Modular Functions of one Variable V*, pages 107–148, Berlin, Heidelberg, 1977. Springer Berlin Heidelberg.

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

[67] B. Mazur and P. Swinnerton-Dyer. Arithmetic of weil curves. *Invent Math*, 25:1–61, 1974.

[68] K. McMurdy. https://phobos.ramapo.edu/~kmcmurdy/research/SAGE_ssEndos/. Accessed Jan 10, 2022.

[69] K. McMurdy. Explicit representation of the endomorphism rings of supersingular elliptic curves. https://phobos.ramapo.edu/~kmcmurdy/research/McMurdy-ssEndoRings.pdf, 2014.

[70] P. Mercuri. Equations and rational points of the modular curves $X_0^+(p)$. *The Ramanujan Journal*, 47:291–308, 2016.

[71] J. S. Milne. The fundamental theorem of complex multiplication, 2007. https://arxiv.org/abs/0705.3446.

[72] H. Onuki. On oriented supersingular elliptic curves. *Finite Fields Appl.*, 69:101777, 18, 2021.

[73] A. K. Pizer. Ramanujan graphs and Hecke operators. *Bull. Amer. Math. Soc. (N.S.)*, 23(1):127–137, 1990.

[74] G. Robin. Grandes valeurs de la fonction somme des diviseurs et hypothèse de Riemann. *J. Math. Pures Appl. (9)*, 63(2):187–213, 1984.

[75] N. T. Sardari. Diameter of Ramanujan graphs and random Cayley graphs. *Combinatorica*, 39(2):427–446, 2019.

[76] R. Schoof. Four primality testing algorithms. In *Algorithmic number theory: lattices, number fields, curves and cryptography*, volume 44 of *Math. Sci. Res. Inst. Publ.*, pages 101–126. Cambridge Univ. Press, Cambridge, 2008.

[77] J.-P. Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Inv. Math.*, 15:259–3319, 1972.

[78] J.-P. Serre. *A course in arithmetic*. Graduate Texts in Mathematics, No. 7. Springer-Verlag, New York-Heidelberg, 1973. Translated from the French.

[79] G. Shimura. *Introduction to the arithmetic theory of automorphic functions*, volume 11 of *Publications of the Mathematical Society of Japan*. Princeton University Press, Princeton, NJ, 1994. Reprint of the 1971 original, Kanô Memorial Lectures, 1.

[80] G. Shimura. *Abelian varieties with complex multiplication and modular functions*, volume 46 of *Princeton Mathematical Series*. Princeton University Press, Princeton, NJ, 1998.

[81] D. Shumow. Isogenies of elliptic curves: a computational approach. Master's thesis, University of Washington, 2009. https://arxiv.org/abs/0910.5370.

[82] S. Siksek. Quadratic chabauty for modular curves. *Preprint, 1704.00473*, 04 2017.

[83] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[84] K. E. Stange. Frobenius and the endomorphism ring of $j = 1728$, 2021. http://math.colorado.edu/~kstange/papers/1728.pdf.

[85] H. M. Stark. On complex quadratic fields with class-number two. *Mathematics of Computation*, 29(129):289–302, 1975.

[86] W. Stein. *Modular forms, a computational approach*, volume 79 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2007. With an appendix by Paul E. Gunnells.

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

[88] G. Tenenbaum. On ultrafriable integers. *Q. J. Math.*, 66(1):333–351, 2015.

[89] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 9.4)*, 2022. https://www.sagemath.org.

[90] J. Tuitman. Counting points on curves using a map to $\mathbf{P}^1$, I. *Math. Comput.*, 85:961–981, 2016.

[91] J. Tuitman. Counting points on curves using a map to $\mathbf{P}^1$, II, volume = 45, journal = Finite Fields and Their Applications, doi = 10.1016/j.ffa.2016.12.008. pages 301–322, 05 2017.

[92] C. U.Jensen and A. Thorup. Gorenstein orders. *Journal of Pure and Applied Algebra*, 219(3):551–562, 2015.

[93] J. Vélu. Isogénies entre courbes elliptiques. *C. R. Acad. Sci. Paris Sér. A-B*, 273:A238–A241, 1971.

[94] M.-F. Vignéras. *Arithmétique des algèbres de quaternions*, volume 800 of *Lecture Notes in Mathematics*. Springer, Berlin, 1980.

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

[96] J. von zur Gathen and J. Gerhard. *Modern computer algebra*. Cambridge University Press, Cambridge, third edition, 2013.

[97] J. von zur Gathen and V. Shoup. Computing Frobenius maps and factoring polynomials. *Comput. Complexity*, 2(3):187–224, 1992.

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

[99] B. Wesolowski. Orientations and the supersingular endomorphism ring problem. Cryptology ePrint Archive, Report 2021/1583, 2021. https://iacr.org/2021/1583.

[100] B. Wesolowski. The supersingular isogeny path and endomorphism ring problems are equivalent. *FOCS 2021-62nd Annual IEEE Symposium on Foundations of Computer Science*, 2022.

[101] H. C. Williams and H. te Riele. New computations concerning the Cohen-Lenstra Heuristics. *Experimental Mathematics*, 12(1):99 – 113, 2003.

[102] G. Xiao, L. Luo, and Y. Deng. Supersingular j-invariants and the class number of $\mathbb{Q}(-p)$. *International Journal of Number Theory*. https://doi.org/10.1142/S1793042122500555.

[103] T. Yang. Minimal cm liftings of supersingular elliptic curves. *Pure and applied mathematics quarterly*, 4(4):1317–1326, 2008.

[104] D. Zywina. Computing actions on cusp forms. *arXiv: Number Theory*, 2020.