ABSTRACT

Title of dissertation: NUMBER THEORETIC ALGORITHMS
FOR ELLIPTIC CURVES

Juliana V. Belding, Doctor of Philosophy, 2008

Dissertation directed by: Professor Lawrence Washington
Department of Mathematics

We present new algorithms related to both theoretical and practical questions in the area of elliptic curves and class field theory. The dissertation has two main parts, as described below.

Let $\mathcal{O}$ be an imaginary quadratic order of discriminant $D < 0$, and let $K = \mathbb{Q}(\sqrt{D})$. The class polynomial H_D of $\mathcal{O}$ is the polynomial whose roots are precisely the j-invariants of elliptic curves with complex multiplication by $\mathcal{O}$. Computing this polynomial is useful in constructing elliptic curves suitable for cryptography, as well as in the context of explicit class field theory. In the first part of the dissertation, we present an algorithm to compute H_D p-adically where p is a prime inert in K and not dividing D. This involves computing the canonical lift $\tilde{E}$ of a pair (E, f) where E is a supersingular elliptic curve and f is an embedding of $\mathcal{O}$ into the *endomorphism ring* of E. We also present an algorithm to compute H_D modulo p for p inert which is used in the Chinese remainder theorem algorithm to compute H_D.

For an elliptic curve E over any field K, the Weil pairing e_n is a bilinear map on the points of order n of E. The Weil pairing is a useful tool in both the theory of elliptic curves and the application of elliptic curves to cryptography. However, for K of characteristic p, the classical Weil pairing on the points of order p is trivial. In the second part of the dissertation, we consider E over the dual numbers $K[\epsilon]$ and define a non-degenerate "Weil pairing on p-torsion." We show that this pairing satisfies many of the same properties of the classical pairing. Moreover, we show that it directly relates to recent attacks on the discrete logarithm problem on the p-torsion subgroup of an elliptic curve over the finite field $\mathbb{F}_q$. We also present a new attack on the discrete logarithm problem on *anomalous* curves using a lift of E over $\mathbb{F}_p[\epsilon]$.

NUMBER THEORETIC ALGORITHMS FOR ELLIPTIC CURVES

by

Juliana V. Belding

Dissertation submitted to the Faculty of the Graduate School of the
University of Maryland, College Park in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
2008

Advisory Committee:
Dr. Lawrence Washington, Advisor
Dr. William Gasarch
Dr. Thomas Haines
Dr. Kartik Prasanna
Dr. Harry Tamvakis

To my parents

David French Belding

and

Susan Brand Belding.

Acknowledgments

First off, thank you to my advisor, Dr. Larry Washington. His broad knowledge of mathematics and his hands-on approach to theory have provided me with many wonderful opportunities to learn. I am especially grateful for his patience with all manner of questions and his invaluable feedback on many a paper draft and practice talk. His commitment to communicating mathematics clearly and energetically to a variety of audiences is a true model for me in my future work.

Thank you to Dr. Reinier Bröker who first introduced me to the beautiful connection between primes of the form $x^2 + Dy^2$ and elliptic curves and who encouraged me to look into developing a p-adic algorithm using supersingular curves. His role as a mentor, mathematical resource and editor have been invaluable to me.

Thank you to Dr. Helen Grundman for encouraging me to pursue mathematics as an undergraduate, and then later as a graduate student. Her continuing belief in me and her thoughtful advice throughout this journey have been touchstones for me.

Thank you to the University of Maryland Math department faculty, staff and fellow graduate students for making this a wonderful place to study and work. I am also indebted to the financial support of the VIGRE program which allowed me to pursue my work and travel to research conferences.

Thank you to the EDGE program for moral and financial support and for continuing camaraderie. In particular, thank you to Amy Marienello-Finkbiner and Happy Tull, fellow UMd graduates.

Thank you to my friends, both far and near, for providing commiseration, sup-

port, humor and perspective. I especially want to thank Poorani Subramanian and Jane Holsapple-Long, who have lived and breathed mathematics alongside me as roommates and officemates.

Thank you to my parents for their unwavering love and encouragement throughout this pursuit. Their weekly phone calls were a wonderful reminder of life outside graduate school.

Lastly, thank you to my partner Leanne for her wisdom, encouragement, humor and love throughout these past five years.

Table of Contents

Chapter 1

Introduction

In this dissertation, we present new algorithms related to both theoretical and practical questions in the area of elliptic curves and class field theory. The dissertation has two main parts. In the first part, we present an algorithm to compute the *class polynomial* of an imaginary quadratic order using the *canonical lift* of a *supersingular* elliptic curve. In the second part, we define a *Weil pairing* on the p-torsion of an *ordinary* elliptic curve over the *dual numbers* of the field K. We give a brief overview of each part in this section.

Computing class polynomials using the canonical lift of a supersingular elliptic curve

Let $\mathcal{O}$ be an imaginary quadratic order of discriminant $D < 0$, and let $K = \mathbb{Q}(\sqrt{D})$ denote the corresponding imaginary quadratic field. Let p be a prime inert in K with p not dividing D. In this case, we say p is *inert with respect to* D. In Chapter 2, we present an algorithm to compute the *canonical lift* $\tilde{E}$ of a pair (E, f) where E is a supersingular elliptic curve over $\overline{\mathbb{F}}_p$ and f is an embedding of $\mathcal{O}$ into the *endomorphism ring* of E. The curve $\tilde{E}$ is a curve over $\overline{\mathbb{Q}}_p$ reducing to E such that the induced embedding of endomorphism rings is precisely the embedding f.

In particular, the curve $\tilde{E}$ has complex multiplication by $\mathcal{O}$ and therefore its j-invariant is a root of the *class polynomial of* $\mathcal{O}$, denoted $H_D(X)$. The polynomial $H_D(X)$

is a minimal polynomial of the extension $H_{\mathcal{O}}/K$, where $H_{\mathcal{O}}$ is the *ring class field of* $\mathcal{O}$. Thus computing the polynomial $H_D(X)$ is of interest for explicit class field theory. Moreover, computing $H_D(X)$ is useful in constructing elliptic curves suitable for cryptographic purposes. In Chapter 2, we present an algorithm to compute $H_D(X)$ p-adically using the canonical lift of (E, f) where p is inert with respect to D. We also present an algorithm to compute $H_D(X)$ modulo p for p inert which is used in the Chinese remainder theorem approach to computing $H_D(X)$.

A Weil pairing on the p-torsion of an ordinary elliptic curve over the dual numbers

Let K be any field. The *Weil pairing* is a bilinear map e_n on the points of order n of an elliptic curve E over a field K. The Weil pairing is a useful tool in both the theory of elliptic curves and in the application of elliptic curves to cryptography. In particular, for n not divisible by the characteristic of K, the Weil pairing e_n can be used to reduce the *discrete logarithm problem* on elliptic curves to that in the multiplicative subgroup of a finite field.

For K of characteristic p, the classical Weil pairing on the points of order p is trivial. In Chapter 3, we consider E over the ring of dual numbers $K[\epsilon] \simeq K[x]/(x^2)$. We define a non-degenerate "Weil pairing on p-torsion" on E over $K[\epsilon]$ and prove that this shares many of the same properties of the classical pairing. Moreover, we show that it directly relates to recent attacks on the discrete logarithm problem on the p-torsion subgroup of an elliptic curve over $\mathbb{F}_q$. We also present a new attack on the discrete logarithm problem on *anomalous* curves using a lift of E over $\mathbb{F}_p[\epsilon]$.

Chapter 2

Computing class polynomials using the canonical lift of a supersingular elliptic curve

2.1 Introduction

Let $\mathcal{O}$ be an imaginary quadratic order of discriminant $D < 0$, and let $K = \mathbb{Q}(\sqrt{D})$ denote the corresponding imaginary quadratic field. Let E be an elliptic curve over $\mathbb{C}$, and let $\mathrm{End}_{\mathbb{C}}(E)$ denote the ring of endomorphisms of E defined over $\mathbb{C}$. The curve E has *complex multiplication by* $\mathcal{O}$ if $\mathrm{End}_{\mathbb{C}}(E) \simeq \mathcal{O}$. It is a result of class field theory that E is isomorphic to a curve defined over $H_{\mathcal{O}}$, the *ring class field* of $\mathcal{O}$. The ring class field $H_{\mathcal{O}}$ is an algebraic extension of K with Galois group isomorphic to the ideal class group $Cl(\mathcal{O})$ via the *Artin map*. The *class polynomial of* $\mathcal{O}$ is the polynomial whose roots are precisely the j-invariants of all isomorphism classes of curves over $\mathbb{C}$ with complex multiplication by $\mathcal{O}$. This polynomial, denoted $H_D(X)$, is a minimal polynomial of the extension $H_{\mathcal{O}}/K$. In the case of $\mathcal{O}$ equal to $\mathcal{O}_K$, the ring of integers of K, this is known as the *Hilbert class polynomial of* K. Algorithms to compute the polynomial H_D are of interest for explicit class field theory as well as for constructing elliptic curves used in cryptography [8, Sec. 18.1].

In this chapter, we present a new algorithm to compute $H_D(X)$ using a p-adic lifting technique where p is a prime inert in K with p not dividing D. In this case we say p is *inert with respect to* D. The algorithm is based on computing the *canonical lift* of an elliptic curve over $\overline{\mathbb{F}}_p$ together with its endomorphism ring, as proposed in [10]. We first give an overview of the known methods to compute the class polynomial $H_D(X)$ followed by a brief explanation of the p-adic approach for p inert with respect to D.

The j-invariants of curves with complex multiplication by $\mathcal{O}$ are *algebraic integers* and therefore the polynomial $H_D(X)$ has integer coefficients [45, Thm. 10.9]. The classical method to compute H_D is to compute each root j_i in the field $\mathbb{C}$ to high enough accuracy so that in expanding the product $\prod_{i=1}^{h(\mathcal{O})}(X - j_i)$ we can recognize the coefficients as actual integers. There are good bounds on the size of the coefficients of $H_D(X)$ which are based on the correspondence of binary quadratic forms of discriminant D with ideals of $\mathcal{O}$. Let (a, b, c) denote the form $ax^2 + bxy + cy^2$, and let Q be a set of primitive reduced binary quadratic forms (a, b, c) of discriminant D representing the class group $Cl(\mathcal{O})$. From [17, Sec. 6], we have the following bound on the number of decimal digits of the largest coefficient of H_D:

$$C = 2.48h(D) + \pi\sqrt{|D|} \sum_{(a_i,b_i,c_i)\in Q} \frac{1}{a_i}. \tag{2.1}$$

Each root j_i is computed as the value of the modular function $j(z)$ for $z = \frac{-b_i+\sqrt{D}}{2a_i}$. The drawback of this method is that in expanding $\prod_i(X - j_i)$, we potentially lose accuracy at each multiplication due to round-off error. While this does not appear to be a problem in practice, there are not rigorously proven good estimates for the amount of accuracy of the roots j_i needed to offset the round-off error. For discussion of this issue, see [17].

To circumvent the problem of round-off error, Couveignes and Henocq in 2002 proposed computing the roots j_i in a p-adic setting [10]. The advantage of working with the p-adics is that there is no round-off error when multiplying or adding p-adic integers. Therefore, knowing the roots j_i to a certain p-adic accuracy means that we know the coefficients of the polynomial $\prod_i (X - j_i)$ to that same p-adic accuracy. Using the bound (2.1), we can then recognize the coefficients of the expanded product as integers. A main difference in the p-adic approach is that a single root $\tilde{j}$ of $H_D(X)$ is computed to sufficient p-adic accuracy using a lifting technique, and then the remaining roots of $H_D(X)$ are computed to that same accuracy using the Galois action of the class group $Cl(\mathcal{O})$ on the set of roots.

To compute the root $\tilde{j}$, we compute the *canonical lift* of a pair $(\bar{E}, f)$, where $\bar{E}$ is an elliptic curve in characteristic p and $f : \mathcal{O} \hookrightarrow \operatorname{End}(\bar{E})$ is an embedding. The canonical lift is the curve $\tilde{E}$ defined over $H_{\mathcal{O}}$ and unique up to isomorphism such that $\bar{E} \equiv \tilde{E} \bmod \mathfrak{p}$ for $\mathfrak{p}$ a prime above p, and such that induced embedding of endomorphism rings $\operatorname{End}(\tilde{E}) \hookrightarrow \operatorname{End}(\bar{E})$ is precisely f.

In the case of a prime p that splits principally in K with p not dividing D, the curve $\bar{E}$ is ordinary. This implies that the endomorphism rings of $\bar{E}$ and its canonical lift $\tilde{E}$ are isomorphic, and f is an isomorphism. There is thus a one-to-one correspondence between curves $\tilde{E}$ over $\overline{\mathbb{Q}}_p$ with $\operatorname{End}(\tilde{E}) \simeq \mathcal{O}$ and ordinary curves $\bar{E}$ over $\overline{\mathbb{F}}_p$ with $\operatorname{End}(E) \simeq \mathcal{O}$. The main idea of [10] is to first compute the induced action of $Cl(\mathcal{O})$ on the set of curves $\bar{E}$ with endomorphism ring isomorphic to $\mathcal{O}$. This action lifts uniquely to an action on the curves over $\overline{\mathbb{Q}}_p$ and can be used to define a p-adic analytic map. Then using a variant of Newton's method, we can compute an approximation to the canonical lift of $\bar{E}$. The j-invariant of this curve is an approximation to a root of $H_D(X)$. Computing the canonical lift in this case has been developed into an explicit algorithm [5]. As the lower bound on the smallest prime splitting principally is $|D|/4$, there is motivation for working with primes which are inert with respect to D. Under the Generalized Riemann Hypothesis (GRH), the upper bound on the smallest such prime is $O((\log|D|)^2)$, thus an algorithm to compute $H_D(X)$ based on computing the canonical lift for p inert is potentially faster.

In the case of p inert with respect to D, there are two main differences which arise when defining and computing the canonical lift. The first is that the curve $\bar{E}$ is *supersingular* and thus f is not an isomorphism. The correspondence between curves over $\overline{\mathbb{Q}}_p$ with $\mathrm{End}(\tilde{E}) \simeq \mathcal{O}$ and supersingular curves over $\overline{\mathbb{F}}_p$ with $\mathrm{End}(\bar{E})$ containing $\mathcal{O}$ is *not* one-to-one but depends instead on how the order $\mathcal{O}$ embeds into $\mathrm{End}(\bar{E})$. Therefore, we must compute the induced action of $Cl(\mathcal{O})$ on the set of *pairs* $(\bar{E}, f)$ where $\bar{E}$ is a supersingular curve and f is an embedding $\mathcal{O} \hookrightarrow \mathrm{End}(\bar{E})$. We address this by using the connection between supersingular elliptic curves over $\overline{\mathbb{F}}_p$ and the quaternion algebra $\mathcal{A}_{p,\infty}$ *ramified at* p *and* ∞. The second difference is that the curve $\bar{E}$ may have j-invariant 0 or 1728 if $p \not\equiv 1 \bmod 12$. Curves with these j-invariants have extra automorphisms which make computing the canonical lift more delicate. We address this by working with the *Legendre form* of an elliptic curve which accounts for the extra automorphisms of the curves. We are then able to explicitly compute the canonical lift of (E, f) for any $p \geq 3$. (For the case of $p = 2$ inert in K and D a fundamental discriminant, see [33].)

In Section 2.2, we describe the theory of supersingular elliptic curves over $\overline{\mathbb{F}}_p$ and *maximal orders* of $\mathcal{A}_{p,\infty}$. In Section 2.3, we define the canonical lift of a pair $(\bar{E}, f)$, where $\bar{E}$ is a supersingular elliptic curve and f is an *optimal* embedding of $\mathcal{O}$ into $\mathcal{A}_{p,\infty}$, and define an action of the class group $Cl(\mathcal{O})$ on the set of such pairs. In Section 2.4, we present an algorithm to compute the canonical lift of $(\bar{E}, f)$ for $p \equiv 1 \bmod 12$. We also use the action of $Cl(\mathcal{O})$ to give an algorithm to compute $H_D(X)$ modulo p for p inert with respect to D. This algorithm is used in the recently proposed "multi-prime" algorithm for class polynomials which computes $H_D(X) \bmod p$ for many small primes p and then recovers H_D using the Chinese Remainder theorem [2].

In Section 2.5, we introduce the *Legendre form* L of an elliptic curve to address the case of $p \not\equiv 1 \bmod 12$. In Sections 2.6 and 2.7, we discuss the *modular function* λ *of level 2* and use it to define an action of a generalized class group of K on the set of curves in Legendre form with complex multiplication by $\mathcal{O}$. In Section 2.8, we present the algorithm to compute the canonical lift of $(\bar{L}, f)$ for $p \not\equiv 1 \bmod 12$ using a p-adic analytic map ρ_α. Finally, in Section 2.9, we give a p-adic lifting algorithm to compute the polynomial $H_D(X)$ for p inert with respect to D.

For completeness, we mention another known method to compute $H_D(X)$ as discussed in [11, Section 13]. Let m be a positive integer such that $\mathcal{O}$ has a primitive element of norm m. The polynomial $H_D(X)$ is an irreducible factor of the *modular polynomial* $\phi_m(X, X)$. As there are algorithms for computing $\phi_m(X, Y)$ and for factoring polynomials, in theory this gives another way to compute $H_D(X)$. However, the size of the coefficients of modular polynomials is exponential in m. As the smallest m such that $\mathcal{O}$ has a primitive element of norm m is roughly the size of D, this approach to computing H_D is not feasible in practice.

2.2 Supersingular curves and quaternion algebras over $\mathbb{Q}$

2.2.1 Brief introduction to quaternion algebras over $\mathbb{Q}$

A *quaternion algebra over* $\mathbb{Q}$ is a central, simple $\mathbb{Q}$-algebra of dimension four. By simple, we mean that the algebra has no non-trivial two-sided ideals. The results in the next three sections can be found in [42, Chap. I - III] unless otherwise noted. Let $\mathcal{A}$ be a quaternion algebra over $\mathbb{Q}$. The following proposition gives a concrete characterization of $\mathcal{A}$.

Proposition 2.2.1 *The following are equivalent:*

1. *$\mathcal{A}$ is a central, simple $\mathbb{Q}$-algebra of dimension four.*

2. *$\mathcal{A} = L + L\beta$ where L is a separable 2-dimensional $\mathbb{Q}$-algebra, $\beta^2 = b$ for $b \in \mathbb{Q}^*$ and $\beta\alpha = \bar{\alpha}\beta$ for all $\alpha \in L$, where $\bar{\alpha}$ denotes the non-trivial automorphism of L. This is denoted $\left(\frac{L,b}{\mathbb{Q}}\right)$.*

3. *$\mathcal{A} = \mathbb{Q}[\alpha, \beta]$ where $\alpha^2 = a, \beta^2 = b$ for $a, b \in \mathbb{Q}^*$ and $\alpha\beta = -\beta\alpha$. This is denoted $\left(\frac{a,b}{\mathbb{Q}}\right)$.*

Consider the algebra $\mathcal{A}$ defined by $\mathcal{A} = L+L\beta$ where L is a separable 2-dimensional $\mathbb{Q}$-algebra, β is an element of $\mathcal{A}$ with $\beta^2 = b$ and $\beta\alpha = \bar{\alpha}\beta$ for all $\alpha \in L$, where $\bar{\alpha}$ denotes the non-trivial automorphism of L. The algebra $\mathcal{A}$ has an *involution* or *conjugation* which comes from extending the non-trivial automorphism of L to $\mathcal{A}$ by defining $\bar{\beta} = -\beta$. The *reduced trace* and *norm* of $\mathcal{A}$ are defined as

$$tr(\gamma) = \gamma + \bar{\gamma}, \quad n(\gamma) = \gamma\bar{\gamma}.$$

For $\mathcal{A} = \left(\frac{a,b}{\mathbb{Q}}\right)$, we let $L = \mathbb{Q}(\alpha)$ and write $\mathcal{A} = \left(\frac{L,b}{\mathbb{Q}}\right)$. Then for $\gamma = x+y\alpha+z\beta+w\alpha\beta \in \mathcal{A}$, we have

$$tr(\gamma) = 2x, \quad n(\gamma) = x^2 - ay^2 - bz^2 + abw^2.$$

Thus $tr(\gamma), n(\gamma) \in \mathbb{Q}$, and every element of $\mathcal{A}$ is a root of a characteristic polynomial in $\mathbb{Q}[X]$:

$$X^2 - t(\gamma)X + n(\gamma).$$

A *division algebra* or *skew field* is an algebra such that all non-zero elements have inverses. It is a classic result that a quaternion algebra $\mathcal{A}$ over $\mathbb{Q}$ is either isomorphic to $M(2, \mathbb{Q})$, the algebra of two-by-two matrices over $\mathbb{Q}$, or to a division algebra. The following proposition gives a necessary and sufficient condition for $\mathcal{A}$ to be a division algebra.

Proposition 2.2.2 *[42, Cor. 2.4] The quaternion algebra $\mathcal{A} = \left(\frac{L,b}{\mathbb{Q}}\right)$ is a division algebra if and only if L is a field and $b \notin n(L)$.*

A quaternion algebra $\mathcal{A}$ is *ramified at the prime p* if $\mathcal{A} \otimes_{\mathbb{Q}} \mathbb{Q}_p$ is a division algebra and *ramified at ∞* if $\mathcal{A} \otimes_{\mathbb{Q}} \mathbb{R}$ is a division algebra. Let $\mathcal{A}_{p,\infty}$ denote a quaternion algebra which is ramified at precisely these two places. For all primes $\ell \neq p$, $\mathcal{A}_{p,\infty} \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \simeq M(2, \mathbb{Q}_\ell)$, the algebra of two-by-two matrices over $\mathbb{Q}_\ell$. There is a unique such algebra up to isomorphism and we define $\mathcal{A}_{p,\infty}$ to be the *quaternion algebra $\mathcal{A}_{p,\infty}$ over $\mathbb{Q}$ ramified at p and ∞*. An explicit characterization of $\mathcal{A}_{p,\infty}$ as $\left(\frac{a,b}{\mathbb{Q}}\right)$ for $a, b \in \mathbb{Q}^*$ is found in [42, Exercise III.5.2].

2.2.2 Supersingular elliptic curves and the quaternion algebra $\mathcal{A}_{p,\infty}$

In this section, we make explicit the connection between supersingular elliptic curves and the maximal orders of $\mathcal{A}_{p,\infty}$. Let $\mathcal{A}$ be a quaternion algebra over $\mathbb{Q}$. The *set of integers* of $\mathcal{A}$ consists of all elements $\gamma \in \mathcal{A}$ such that $tr(\gamma)$, $n(\gamma)$ are integers. Unlike the case of a number field, the set of integers is not necessarily a ring, and therefore it does not make sense to consider *the* maximal order of $\mathcal{A}$. A *ring of integers* of $\mathcal{A}$ is a set of integers of $\mathcal{A}$ which forms a ring under the operations of addition and multiplication. We define an *order* R of $\mathcal{A}$ to be a ring of integers of $\mathcal{A}$ containing $\mathbb{Z}$ with $R \otimes_{\mathbb{Z}} \mathbb{Q} = \mathcal{A}$. A *maximal order* is an order not properly contained in any other order.

Given an order R, we call J a *left ideal of the order* R if J is a left ideal of the ring R, that is, $RJ \subset J$, *and* if J is a finitely-generated $\mathbb{Z}$-module contained in $\mathcal{A}$ with $J \otimes_{\mathbb{Z}} \mathbb{Q} = \mathcal{A}$. The ideal J is *integral* if $J \subset R$. Similarly, we call J a *right ideal of* R if $JR \subset J$. Given an ideal J of any order, the *left order of* J is the order containing *all* elements $x \in \mathcal{A}$ such that $xJ \subset J$. This is denoted $R_l(J)$. Similarly, we let $R_r(J)$ denote the *right order of* J. Any order R is its own left and right order.

The *norm* $n(J)$ of the ideal J is the positive generator of the subgroup generated by the image of the norm map $n : J \to \mathbb{Z}$. In other words, $n(J)$ is the greatest common divisor of the set $\{n(\gamma) | \gamma \in J\}$. The *inverse* of an ideal is the set $J^{-1} = \{\gamma \in \mathcal{A} : J\gamma J \subset J\}$. For ideals I, J, we have the following properties:

$$JJ^{-1} = R_l(J) = R_r(J^{-1})$$

$$J^{-1}J = R_l(J^{-1}) = R_r(J)$$

$$R_r(IJ) = R_r(J), \quad R_l(IJ) = R_l(I).$$

Let I, J be left ideals of R. If $I = Jx$ for some $x \in \mathcal{A}$, we say I and J are *right-isomorphic* as left R-modules. The *left ideal classes* of R are the right-isomorphism classes of ideals $[J_i]$ such that $R = R_l(J_i)$. We have the analogous definition for right ideal classes, and the map $J \mapsto J^{-1}$ gives a bijection between left and right ideal classes of R.

Let R be a maximal order of $\mathcal{A}$ and $\{J_i\}$ a set of left ideal class representatives. The number of classes is the same for any maximal order of $\mathcal{A}$, and therefore we define the *class number $h_{\mathcal{A}}$ of $\mathcal{A}$* as the number of left ideal classes of R.

Two orders R and R' are of the *same type* if they are conjugate by an element of $\mathcal{A}$, that is, if there exists $h \in \mathcal{A}$ such that $hRh^{-1} = R'$. The *type number $t_{\mathcal{A}}$ of $\mathcal{A}$* is the number of conjugacy classes of maximal orders. It is a fact that every conjugacy class of maximal orders of $\mathcal{A}$ appears in the set $\{R_r(J_i)\}$ at least once, and so $t_{\mathcal{A}} \leq h_{\mathcal{A}}$.

We now give the connection between supersingular elliptic curves and maximal orders of $\mathcal{A}_{p,\infty}$. A *supersingular curve E* is an elliptic curve over $\overline{\mathbb{F}}_p$ such that the subgroup of p-torsion points of E over $\overline{\mathbb{F}}_p$ is trivial. We begin by giving a characterization of the supersingular curves over $\overline{\mathbb{F}}_p$ and their automorphism groups.

Proposition 2.2.3 *Every supersingular elliptic curve over $\overline{\mathbb{F}}_p$ is isomorphic to a curve defined over $\mathbb{F}_{p^2}$. For $p \neq 2, 3$ and $j(E) \neq 0, 1728$, the automorphism group $\mathrm{Aut}(E)$ of E is $\pm\mathrm{Id}$. For $j(E) = 0, 1728$ and $p \neq 2, 3$, the group $\mathrm{Aut}(E)$ is cyclic of order 6 and 4, respectively. For $p = 2, 3$, the curve with $j = 0$ is supersingular and $\mathrm{Aut}(E)$ is cyclic of order 24 and 12, respectively.*

A curve with $j = 0$ is supersingular if and only if $p \not\equiv 1 \bmod 3$. A curve with $j = 1728$ is supersingular if and only if $p \not\equiv 1 \bmod 4$.

Proof: The first fact follows from the definition of a supersingular curve. As E has no p-torsion points, the endomorphism $[p]$ of E is inseparable of degree p^2, and thus is the map π_p^2, where π_p is the the Frobenius map $(x, y) \mapsto (x^p, y^p)$. Therefore π_p^2 fixes the coefficients of the Weierstrass equation of E and $j(E)$ as well. Thus $j(E)$ is in $\mathbb{F}_{p^2}$. A proof of the statements concerning $\mathrm{Aut}(E)$ is found in [38, Appendix A].

Let E be a curve in characteristic zero with $j = 0$, respectively 1728, which is defined over $\mathbb{Q}$ and has good reduction modulo p. The curve E has complex multiplication by the ring of integers of $K = \mathbb{Q}(\sqrt{-3})$, respectively $\mathbb{Q}(\sqrt{-1})$, and reduces modulo p to a curve $E_p/\overline{\mathbb{F}}_p$. This curve is supersingular if and only if p does not split in K [26, Thm. 13.4.12]. Thus, the curve E_p with $j = 0$ is supersingular if and only if p does not split in the field K which is true if and only if $p \not\equiv 1 \bmod 3$. Similarly, a curve with $j = 1728$ is supersingular if and only if p does not split in $K = \mathbb{Q}(\sqrt{-1}))$ which is true if and only if $p \not\equiv 1 \bmod 4$. □

Theorem 2.2.4 *[14, 2.1-2.4,10.]*

1. *The number of isomorphism classes of supersingular elliptic curves over $\mathbb{F}_{p^2}$ is equal to the class number h_p of $\mathcal{A}_{p,\infty}$.*

2. *The number of $\mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$-conjugacy classes of j-invariants of supersingular elliptic curves over $\mathbb{F}_{p^2}$ is equal to the type number t_p of $\mathcal{A}_{p,\infty}$.*

3. *Let R be any maximal order of $\mathcal{A}_{p,\infty}$ and let $\{J_i\}$ be a set of left ideal class represen-*

tatives for R. There is a one-to-one correspondence between the set of isomorphism classes $[E_i]$ of supersingular elliptic curves over $\mathbb{F}_{p^2}$ and the set of maximal orders $\{R_r(J_i)\}$ such that $\operatorname{End}(E_i) \simeq R_r(J_i)$.

If E is defined over $\mathbb{F}_p$, there exists a unique J_i such that $\operatorname{End}(E_i) \simeq R_r(J_i)$ and the correspondence of part 3 is well-defined. However, for curves over $\mathbb{F}_{p^2}$ that are not defined over $\mathbb{F}_p$, the correspondence is only determined up to conjugation. For any pair of Galois conjugates E and E^p, we have $\operatorname{End}(E) \simeq \operatorname{End}(E^p)$ via the Frobenius map π_p. Thus, there exist two classes $[J_i]$ and $[J_k]$ with $\operatorname{End}(E) \simeq R_r(J_i) \simeq R_r(J_k)$, and there is no canonical choice of maximal order $R_r(J_i)$ with respect to E. We have only that the pair (E, E^p) corresponds to the pair (J_i, J_k). However, if we fix a set of representatives J_i, we can uniquely establish the correspondence of part 3, as we now explain.

Let E be a supersingular curve with a fixed isomorphism $i : R \xrightarrow{\sim} \operatorname{End}(E)$. For J a left ideal of R, we define $E[J]$ as the subgroup

$$E[J] = \bigcap_{\alpha \in i(J)} \ker(\alpha).$$

This subgroup determines an isogeny $\varphi_J : E \to E' = E/E[J]$, unique up to isomorphism.

Remark 2.2.1

Though the curve $E' = E/E[J]$ is only defined up to isomorphism over $\mathbb{F}_{p^2}$, there is a canonical choice of E'. An isogeny φ is called *normalized* if $\varphi^*\omega' = \omega$ where ω and ω' are the invariant differentials of E and E' respectively. The normalized isogeny with kernel $E[J]$ is unique up to automorphisms of E'. In the remainder of this chapter, we use the notation $E/E[J]$ to denote the unique curve E' such that the isogeny $E \to E'$ with kernel $E[J]$ is normalized. The curve $E/E[J]$ can be explicitly computed given E and $E[J]$ using Vélu's formulas [41].

The degree of the isogeny φ_J with kernel $E[J]$ is equal to $n(J)$, the norm of J ([46, Thm. 3.15]). Furthermore, if I is another left ideal of R, the curves $E/E[J]$ and $E/E[I]$ are isomorphic if and only if I and J are right-isomorphic [46, Thm. 3.11].

The isogeny $\varphi_J : E \to E' = E/E[J]$ induces an isomorphism i_J:

$$\begin{array}{cccc} i_J : & \mathcal{A}_{p,\infty} & \xrightarrow{\sim} & \mathrm{End}(E') \otimes \mathbb{Q} \\ & \alpha & \mapsto & \varphi_J i(\alpha) \widehat{\varphi}_J \otimes (\deg \varphi_J)^{-1}. \end{array} \tag{2.2}$$

We have the following proposition.

Proposition 2.2.5 *[46, Prop. 3.9, 3.12]*

1. *The maximal order $i_J^{-1}(\mathrm{End}(E/E[J]))$ is equal to $R_r(J)$, the right order of J.*

2. *Let I be a left ideal of $R_r(J)$. Let $E'[I]$ denote the subgroup*

$$E'[I] = \bigcap_{\alpha \in i_J(I)} \ker(\alpha)$$

and $\varphi_I : E' \to E'/E'[I]$ the corresponding isogeny. Then the composition

$$\varphi_I \circ \varphi_J : E \to E'/E'[I]$$

is the isogeny $\varphi_{JI} : E \to E/E[JI]$ determined by the left R-ideal JI.

Let $\{J_i\}$ be a set of representatives of left ideal classes of R, with $J_1 = R$. Consider the map

$$J_i \mapsto [E_i] \text{ where } E_i = E/E[J_i]. \tag{2.3}$$

Note that $E_1 = E$. By the previous proposition, this gives the one-to-one correspondence of Theorem 2.2.4, part 3.

We note also that given a separable isogeny $\varphi : E \to E'$, the kernel of φ determines a left ideal of R:

$$I = i^{-1}\big(\{\alpha \in \mathrm{End}(E) : \alpha(P) = P_\infty \text{ for all } P \in \ker(\varphi)\}\big).$$

Here P_∞ denotes the identity element of the group $E(\overline{\mathbb{F}}_p)$. The norm of I is prime to p and equal to $\deg \varphi$. For any prime $\ell \neq p$, the ℓ-isogeny graph of supersingular curves over $\mathbb{F}_{p^2}$ is connected and has diameter $O(p)$ [29]. Therefore there exists a separable ℓ-power isogeny between any two supersingular curves and every ideal class of R has a representative with norm equal to a prime power of ℓ, for any prime $\ell \neq p$. Algorithms to compute a set $\{J_i\}$ of left ideal class representatives of R and the set of their respective right orders $\{R_r(J_i)\}$ can be found in [44, 9] and are implemented in the computer algebra program MAGMA [9].

The following table gives the number of supersingular curves modulo p.

p	h_p
$2, 3$	1
$\equiv 5 \bmod 12$	$\frac{p+7}{12}$
$\equiv 7 \bmod 12$	$\frac{p+5}{12}$
$\equiv 11 \bmod 12$	$\frac{p+13}{12}$
$\equiv 13 \bmod 12$	$\frac{p-1}{12}$

This follows from Eichler's mass formula for $\mathcal{A}_{p,\infty}$ ([19, Section 1]) and the characterization of the automorphism groups of supersingular curves modulo p found in Proposition 2.2.3.

2.3 The canonical lift of a supersingular elliptic curve and an optimal embedding

Let $\mathcal{O}$ be an imaginary quadratic order of discriminant $D < 0$, and let $K = \mathbb{Q}(\sqrt{D})$ denote the corresponding imaginary quadratic field. Let E be an elliptic curve over $\mathbb{C}$ with complex multiplication by $\mathcal{O}$. By class field theory, E is isomorphic to a curve defined over $H_{\mathcal{O}}$, the *ring class field* of $\mathcal{O}$. The ring class field $H_{\mathcal{O}}$ is an algebraic extension of K with Galois group isomorphic to the ideal class group $Cl(\mathcal{O})$ via the Artin map. Let p be a prime inert with respect to D. That is, p is inert in K and $p \nmid D$. Let $\mathfrak{p}$ be any prime of $H_{\mathcal{O}}$ lying above p. A key property of the ring class field $H_{\mathcal{O}}$ of $\mathcal{O}$ is that the principal ideal $(p) \subset \mathcal{O}$ splits completely in $H_{\mathcal{O}}$. Therefore, the residue class field extension over $\mathbb{Z}/(p)$ is of degree two, and we can view $H_{\mathcal{O}}$ as a subfield of the unramified degree 2 extension F of $\mathbb{Q}_p$.

We may assume E is defined over F by a *minimal Weierstrass model* with discriminant $\triangle_{min}$. If p does not divide $\triangle_{min}$, then E/F has good reduction modulo p, or equivalently, $E/H_{\mathcal{O}}$ has good reduction modulo $\mathfrak{p}$. The reduced curve $E_p \equiv E \bmod \mathfrak{p}$ is supersingular ([26, Thm. 13.4.12]) and is defined over the finite field $\mathbb{F}_{p^2}$. As discussed in Section 2.2.2, its endomorphism ring is a maximal order in the quaternion algebra $\mathcal{A}_{p,\infty}$ ramified at p and ∞ [14, 2.4].

Let $\mathbb{Z}_F$ denote the ring of integers of F. The reduction map $\mathbb{Z}_F \to \mathbb{F}_{p^2}$ induces an embedding $f : \mathcal{O} \simeq \operatorname{End}(E) \hookrightarrow \operatorname{End}(E_p)$. As we discuss in this section, the essence of the *Deuring lifting theorem* is that this process can be reversed ([26, Thm. 13.5.14]). That is, given a supersingular elliptic curve $\bar{E}$ over $\mathbb{F}_{p^2}$ and an embedding $f : \mathcal{O} \hookrightarrow \operatorname{End}(\bar{E})$, there exists a *canonical* choice of curve $\tilde{E}$ over $H_{\mathcal{O}}$ with $\bar{E} \equiv \tilde{E} \bmod \mathfrak{p}$ for $\mathfrak{p}$ a prime above p, such that the induced embedding $\operatorname{End}(\tilde{E}) \hookrightarrow \operatorname{End}(\bar{E})$ is precisely f. This curve $\tilde{E}$ is defined as the *canonical lift* of the pair (E, f), as we explain in detail in this section. We begin by discussing *optimal embeddings* of $\mathcal{O}$ into $\mathcal{A}_{p,\infty}$.

Remark 2.3.1

We restrict to discriminants $D < -4$ in the remainder of the chapter. The cases of $D = -3$ and $D = -4$ are well-understood as a curve with complex multiplication by the order $\mathcal{O}$ of discriminant D has automorphisms other than $\pm\mathrm{Id}$. There is a single class of curves with complex multiplication by $\mathcal{O}$, namely those with j-invariant 0 and 1728, respectively [38, III.10] .

2.3.1 Optimal embeddings of a quadratic imaginary order $\mathcal{O}$ into $\mathcal{A}_{p,\infty}$

Given $\mathcal{O}$, an order of a quadratic imaginary field K, an *embedding of $\mathcal{O}$ into $\mathcal{A}$* is an injective $\mathbb{Z}$-algebra homomorphism from $\mathcal{O}$ into $\mathcal{A}$. Let $f : \mathcal{O} \hookrightarrow \mathcal{A}$ be such an embedding and let R be a maximal order of $\mathcal{A}_{p,\infty}$. The embedding f is called *optimal with respect to R* if $f(K) \cap R = f(\mathcal{O})$. As the set $f(K) \cap R$ is an order of $f(K)$, a commutative subfield of $\mathcal{A}$, every embedding of the ring of integers $\mathcal{O}_K$ of K into R is necessarily optimal.

An embedding $f : \mathcal{O} \hookrightarrow \mathcal{A}$ induces an embedding $f : K \hookrightarrow \mathcal{A}$ and there exists $\beta \in \mathcal{A}_{p,\infty}$ with $\beta^2 = b \in \mathbb{Q}^*$ such that $\mathcal{A} = \left(\frac{f(K),b}{\mathbb{Q}}\right)$. Writing $\mathcal{O} = \mathbb{Z}[\tau]$, the embedding $f : \mathcal{O} \hookrightarrow \mathcal{A}$ can be given by $f(\tau) = y$, where y is an element of $\mathcal{A}$ which is a root of $X^2 - tr(\tau)X + n(\tau)$, the characteristic polynomial of τ. Here tr, n agree with the trace and norm of K since $\mathcal{A} = \left(\frac{f(K),b}{\mathbb{Q}}\right)$.

Any two embeddings f, g of $\mathcal{O}$ give an isomorphism of $f(K)$ and $g(K)$, as commutative subfields of $\mathcal{A}$. By the Skolem-Noether Theorem [42, Thm. I.2.1], this isomorphism extends to an *inner automorphism* of $\mathcal{A}$. Therefore, if $f(\tau) = y$, there exists $x \in \mathcal{A}^*$ such that $g(\tau) = xyx^{-1}$.

Two embeddings $f, g : \mathcal{O} \hookrightarrow R$ are *equivalent* if there exists a unit $u \in R^*$ such that $g(\tau) = uf(\tau)u^{-1}$. Since R^* is contained in the normalizer of R, f is optimal if and only if g is optimal. Thus we can consider equivalence classes of optimal embeddings $\mathcal{O} \hookrightarrow R$.

The following proposition characterizes when an embedding $\tau \mapsto y \in R$ is optimal with respect to R.

Proposition 2.3.1 *Let τ be an integer of a quadratic imaginary field K with $\tau \notin \mathbb{Z}$. Let the characteristic polynomial of τ be $T(X) = X^2 - tX + n$. Let $\triangle$ be the discriminant of K and let m be the conductor of the order $\mathcal{O} = \mathbb{Z}[\tau]$. Consider an embedding $g : \mathcal{O} \hookrightarrow R$ given by $g(\tau) = y$, where $y = [y_1, y_2, y_3, y_4]$ is expressed in terms of a $\mathbb{Z}$-basis $\{r_i\}$ of R with $r_1 = 1$. Let*

$$a_1 = \begin{cases} y_1 - \frac{t}{2} & \triangle \equiv 0 \mod 4 \\ y_1 - \frac{t-m}{2} & \triangle \equiv 1 \mod 4 \end{cases}$$

and let $a_i = y_i$ *for* $i = 2, 3, 4$*. Then* g *is optimal with respect to* R *if and only if there exist* $i, j \in \{1, ..., 4\}$ *such that* $\gcd(a_i, a_j) = 1$.

Proof: The embedding g is optimal if and only if the order $g(\mathcal{O})$ equals $g(K) \cap R$, or equivalently, if and only if for any order $\mathcal{O}'$ containing $\mathcal{O}$, the order $g(\mathcal{O}')$ is not contained in R. Let $c \in \mathbb{Z}^+$ divide m and let $\mathcal{O}'$ be the order of conductor c. Let $d = \frac{m}{c}$.

If $\triangle \equiv 0 \bmod 4$, since $t^2 - 4n = m^2\triangle$, we have that $\frac{t}{2}$ is an integer. We can write the ring of integers $\mathcal{O}_K$ as $\mathbb{Z}[\frac{1}{m}(\tau - \frac{t}{2})]$ and thus $\mathcal{O}' = \mathbb{Z}[\frac{1}{d}(\tau - \frac{t}{2})]$.

The element $g(\frac{1}{d}(\tau - \frac{t}{2}))$ of $\mathcal{A}$ expressed in terms of the basis for R is then $\frac{1}{d}[y_1 - \frac{t}{2}, y_2, y_3, y_4]$. Letting $a_1 = y_1 - \frac{\tau}{2}$ and $a_i = y_i$ for $i = 2, 3, 4$, we see that this is an element of R if and only if d divides a_i for all i.

If $\triangle \equiv 1 \bmod 4$, we have that $\frac{t-m}{2}$ is an integer and we can write the ring of integers $\mathcal{O}_K$ as $\mathbb{Z}[\frac{1}{m}(\tau - \frac{t-m}{2})]$. Thus we have $\mathcal{O}' = \mathbb{Z}[\frac{1}{d}(\tau - \frac{t-m}{2})]$.

The element $g(\frac{1}{d}(\tau - \frac{t-m}{2}))$ of $\mathcal{A}$ expressed in terms of the basis for R is then $\frac{1}{d}[y_1 - \frac{t-m}{2}, y_2, y_3, y_4]$. Letting $a_1 = y_1 - \frac{t-m}{2}$ and $a_i = y_i$ for $i = 2, 3, 4$, we have that this is an element of R if and only if d divides a_i for all i.

In either case, we have that if there exist $i, j \in \{1, ..., 4\}$ such that $\gcd(a_i, a_j) = 1$, the order $g(\mathcal{O}')$ cannot be in R for any order $\mathcal{O}'$ of conductor c dividing m. We also have that if d divides $\gcd(a_1, a_2, a_3, a_4)$, then $g(\mathcal{O}')$ will be contained in R. Therefore, the embedding g is optimal if and only if there exist $i, j \in \{1, ..., 4\}$ such that $\gcd(a_i, a_j) = 1$. $\square$.

Note that given $D < -4$, with $D = m^2\triangle$, for $\triangle$ a fundamental discriminant, we may write the order $\mathcal{O}$ of discriminant D as $\mathbb{Z}[\tau]$ with the minimal polynomial of τ

$$T(X) = \begin{cases} X^2 + m^2\frac{\triangle}{4} & D \equiv 0 \mod 4 \\ X^2 - mX + m^2\frac{1-\triangle}{4} & D \equiv 1 \mod 4. \end{cases}$$

In this case, the embedding given by $g(\tau) = [y_1, ..., y_4]$ is an optimal embedding if and only if $\gcd(y_i, y_j) = 1$ for some $i, j \in \{1, ..., 4\}$.

For example, consider $\mathcal{A}_{7,\infty} = \left(\frac{-1,-7}{\mathbb{Q}}\right)$, where $i^2 = -1, j^2 = -7$ and $ij = -ji$. The order $R = \mathbb{Z}[1, i, \frac{1}{2}(i + k), \frac{1}{2}(1 + j)]$ is the unique maximal order of $\mathcal{A}_{7,\infty}$, up to conjugation. Let $D = -4 \cdot 51$. The order $\mathcal{O}$ of discriminant D can be written as $\mathbb{Z}[\tau]$ where τ is a root of $T(X) = X^2 + 51$. We can verify that $y = [2, -5, 2, -4]$ is an element of $\mathcal{A}_{7,\infty}$ with characteristic polynomial $T(X)$. Letting $f(\tau) = y$, by the proposition, we have that g is an optimal embedding since $\gcd(-5, 2) = 1$. In particular, $\frac{\tau+1}{2} \notin R$, and thus R doesn't contain $f(\mathcal{O}_K)$, where $\mathcal{O}_K$ is the ring of integers of K.

Assume there exists an optimal embedding of $\mathcal{O}$ into R. We can explicitly compute this embedding of $\mathcal{O}$ into R using the quadratic form given by the norm of $\mathcal{A}_{p,\infty}$ in terms of a basis for R. This is the approach used in Algorithm A.0.2 in Appendix A. The number of embeddings of $\mathcal{O} = \mathbb{Z}[\tau]$ into the maximal orders of $\mathcal{A}_{p,\infty}$ is directly related to $h(\mathcal{O})$, the class number of $\mathcal{O}$, as the following result of Eichler shows.

Proposition 2.3.2 *[16, Prop. 5] Let R be a maximal order of $\mathcal{A}_{p,\infty}$, and let $\{J_i\}_{i=1}^{h_p}$ be a set of ideal class representatives. Let $n(\mathcal{O}, R_r(J_i))$ denote the number of equivalence* *classes of optimal embeddings $\mathcal{O} \hookrightarrow R_r(J_i)$. Then*

$$\sum_{i=1}^{h_p} n(\mathcal{O}, R_r(J_i)) = 2h(\mathcal{O}).$$

We let $\mathrm{Emb}_D(\mathcal{A}_{p,\infty})$ denote the set of equivalence classes of optimal embeddings $\mathcal{O} \hookrightarrow R_r(J_i)$ where we identify "complex conjugate" embeddings $\tau \mapsto y$ and $\tau \mapsto \bar{y}$. By the proposition, $\mathrm{Emb}_D(\mathcal{A}_{p,\infty})$ has cardinality $h(\mathcal{O})$. We will see in Section 2.3.4 that there is a natural action of the class group $Cl(\mathcal{O})$ on this set which will be useful in computing the canonical lift of (E, f).

2.3.2 Optimal embeddings $f : \mathcal{O} \hookrightarrow \mathrm{End}(E)$

Let $\mathcal{O}$ be a quadratic imaginary order of discriminant $D < -4$. Let p be a prime inert with respect to D. As mentioned in the introduction to this section, the ring class field $H_{\mathcal{O}}$ embeds into F, the unramified degree 2 extension of $\mathbb{Q}_p$. Thus all curves over $\overline{\mathbb{Q}}_p$ with complex multiplication by $\mathcal{O}$ are isomorphic to curves defined over F. Let E be a curve defined over F with complex multiplication by $\mathcal{O}$. Of the *two* isomorphisms $\gamma : \mathcal{O} \xrightarrow{\sim} \mathrm{End}(E)$, we can make a well-defined choice, called the *normalized* isomorphism. We choose γ such that for any $y \in \mathcal{O}$ and invariant differential ω of E, we have $\omega \circ \gamma(y) = y\omega$, where y is viewed as an element of F under the embedding $H_{\mathcal{O}} \hookrightarrow F$. We call E a 'normalized' elliptic curve to indicate that we have chosen the normalized isomorphism. Let $\mathrm{Ell}_D(F)$ be the set of isomorphism classes of normalized elliptic curves E/F with endomorphism ring $\mathcal{O}$.

For supersingular curves over $\overline{\mathbb{F}}_p$, we have a similar notion of a *normalized embedding* $f : \mathcal{O} \hookrightarrow \mathrm{End}(E)$. Let $\mathcal{O} \to \mathbb{F}_{p^2}$ be one of the two possible reduction maps of $\mathcal{O}$

modulo p. For any $y \in \mathcal{O}$, and invariant differential ω of E, we have $\omega \circ f(y) = y\omega$ where y is viewed as an element of $\mathbb{F}_{p^2}$ under the map $\mathcal{O} \to \mathbb{F}_{p^2}$.

Two embeddings f, g are *equivalent* if there exists an automorphism h of E such that $g(y) = hf(y)h^{-1}$ for all $y \in \mathcal{O}$. Let $a \in \overline{\mathbb{F}}_p$ be such that $\omega \circ h = a\omega$. Then

$$\omega \circ (hf(y)h^{-1}) = (a\bar{y}a^{-1})\omega = \bar{y}\omega.$$

Thus any embedding equivalent to a normalized embedding is also normalized.

Let $\mathrm{Emb}_D(\mathbb{F}_{p^2})$ be the set of equivalence classes of pairs (E, f) with $E/\mathbb{F}_{p^2}$ a supersingular elliptic curve and $f : \mathcal{O} \hookrightarrow \mathrm{End}(E)$ a normalized *optimal* embedding. Recall that an embedding is called *optimal* if $f(\mathcal{O})$ is equal to the ring $f(K) \cap \mathrm{End}(E)$. Writing $\mathcal{O} = \mathbb{Z}[\tau]$, the pairs (E, f) and (E', f') are *equivalent* if there exists an isomorphism $h : E \xrightarrow{\sim} E'$ of elliptic curves such that $hf(\tau)h^{-1} = f'(\tau)$.

The set $\mathrm{Emb}_D(\mathbb{F}_{p^2})$ is in bijection with $\mathrm{Emb}_D(\mathcal{A}_{p,\infty})$, the set of equivalence classes of optimal embeddings $\mathcal{O} \hookrightarrow R_r(J_i)$ where $\{J_i\}$ is a fixed set of integral left ideal class representatives for a maximal order R of $\mathcal{A}_{p,\infty}$ in which $\mathcal{O}$ optimally embeds. There is a bijection between $\mathrm{Emb}_D(\mathbb{F}_{p^2})$ and $\mathrm{Emb}_D(\mathcal{A}_{p,\infty})$ as we now show.

By the bijection from Theorem 2.2.4, part 3, there exists an isomorphism class of supersingular curves whose endomorphism rings are isomorphic to R. Let E be such a curve and fix an isomorphism $i : \mathcal{A}_{p,\infty} \to \mathrm{End}(E) \otimes \mathbb{Q}$. As described in Section 2.2.2, the curves $E_i = E/E[J_i]$ represent the h_p isomorphism classes of supersingular elliptic curves over $\overline{\mathbb{F}}_p$. Letting φ_{J_i} denote the isogeny $E \to E_i$, the isomorphism $R_r(J_i) \simeq \mathrm{End}(E_i)$ can be explicitly given by

$$i_{J_i} : \alpha \mapsto \varphi_{J_i} i(\alpha)\widehat{\varphi}_{J_i} \otimes (\deg \varphi_{J_i})^{-1}.$$

Let $g : \mathcal{O} \hookrightarrow R_r(J_i)$ be an optimal embedding defined by $g(\tau) = y$. Then the embeddings $\tau \mapsto i_{J_i}(y)$ and $\tau \mapsto i_{J_i}(\bar{y})$ are both optimal embeddings and exactly one is normalized. We call this $f : \mathcal{O} \to \mathrm{End}(E_i)$ and define

$$\Psi : \mathrm{Emb}_D(\mathcal{A}_{p,\infty}) \to \mathrm{Emb}_D(\mathbb{F}_{p^2})$$

by $\Psi(g) = (E_i, f)$. It is straightforward to show that this definition is independent of the choice of E.

Proposition 2.3.3 *The map* $\Psi : \mathrm{Emb}_D(\mathcal{A}_{p,\infty}) \to \mathrm{Emb}_D(\mathbb{F}_{p^2})$ *is a bijection.*

Proof: If g and g' are equivalent embeddings, then $g'(\tau) = hg(\tau)h^{-1}$ for some $h \in R_r(J_i)^*$. The embeddings f, f' differ by conjugation by $i_{J_i}(h)$, an automorphism of E_i, and therefore (E_i, f) and (E_i, f') are equivalent. Thus Ψ is well defined.

Let $(E, f) \in \mathrm{Emb}_D(\mathbb{F}_{p^2})$. Then $E \simeq E_i$ for some i, so without loss of generality, we assume $E = E_i$ and consider (E_i, f). As $f : \mathcal{O} \hookrightarrow \mathrm{End}(E_i)$ is an optimal embedding, the embedding $g = i_{J_i}^{-1} \circ f : \mathcal{O} \to R_r(J_i)$ is optimal. By construction, $\Psi(g)$ equals (E_i, f) and so Ψ is surjective. By Theorem 2.2.4, the sets have the same cardinality, thus we have that Ψ is a bijection. □

2.3.3 The canonical lift of (E, f)

In this section, we define the notion of the canonical lift of a pair (E, f) of the set $\mathrm{Emb}_D(\mathbb{F}_{p^2})$. Recall that the reduction map $\mathbb{Z}_F \to \mathbb{F}_{p^2}$ induces an embedding $f : \mathcal{O} \xrightarrow{\gamma} \mathrm{End}(E) \hookrightarrow \mathrm{End}(E_p)$. Thus a curve E corresponds to a pair (E_p, f) and there is a natural map

$$\pi : \mathrm{Ell}_D(F) \to \mathrm{Emb}_D(\mathbb{F}_{p^2}).$$

The *Deuring lifting theorem* implies that the converse is true: given $(E, f) \in \mathrm{Emb}_D(\mathbb{F}_{p^2})$, there exists a curve $\tilde{E}$ over F which reduces to E modulo p such that the induced embedding is precisely f.

Theorem 2.3.4 *[26, 13.5.14], [20, Prop. 2.7]*

Let E be an elliptic curve over $\overline{\mathbb{F}}_p$ and ϕ an endomorphism of E. There exists a curve $\tilde{E}$ defined over $\overline{\mathbb{Q}}$ with endomorphism β and a prime $\mathfrak{p}$ over p such that $\tilde{E} \equiv E \bmod \mathfrak{p}$ and $\beta \bmod \mathfrak{p}$ corresponds to the endomorphism ϕ. That is, the following diagram commutes

$$\begin{tikzcd}
\tilde{E} \arrow[r, "\beta"] \arrow[d] & \tilde{E} \arrow[d] \\
E \arrow[r, "\phi"] & E.
\end{tikzcd}$$

Furthermore, the pair $(\tilde{E}, \beta)$ is unique up to isomorphism.

We now show that the map π sending E to (E_p, f) is a well-defined bijection.

Theorem 2.3.5 *Let $D < -4$ be a quadratic imaginary discriminant. If p is inert with respect to D, then the reduction map $\pi : \mathrm{Ell}_D(F) \to \mathrm{Emb}_D(\mathbb{F}_{p^2})$ is a well-defined bijection.*

Proof: The induced embedding is indeed normalized, since γ is normalized and differential forms behave well with respect to reduction [26, Section 9.4, p. 120].

To show f that is optimal, it suffices to show $f(\mathrm{End}(E)) = f(\mathrm{End}(E) \otimes \mathbb{Q}) \cap \mathrm{End}(E_p)$. Let $S = f(\mathrm{End}(E)) \otimes \mathbb{Q}$. Write $\mathcal{O}' = S \cap \mathrm{End}(E_p)$, and let m be the index

$[\mathcal{O}' : f(\mathrm{End}(E))]$. We first show that $(m,p) = 1$. Let $\mathcal{O}$ be the order of discriminant D. Since $\mathrm{End}(E) \simeq \mathcal{O}$, the integer m is a divisor of the conductor of $\mathcal{O}$ in $\mathcal{O}_K$, the ring of integers of $K = \mathbb{Q}(\sqrt{D})$. Since p is inert with respect to D, we have that m is relatively prime to p.

Now consider any δ in $\mathcal{O}'$. There exists $\gamma \in \mathrm{End}(E)$ with $m\delta = f(\gamma)$, and since $(m,p) = 1$, the endomorphism $f(\gamma)$ annihilates the m-torsion $E_p[m]$. Therefore γ annihilates $E[m]$ and γ is a multiple of m inside $\mathrm{End}(E)$. Thus δ is contained in $f(\mathrm{End}(E))$, and $\mathcal{O}' = f(\mathrm{End}(E))$.

To show surjectivity, we use the Deuring lifting theorem. Let $(E, f : \mathcal{O} \hookrightarrow \mathrm{End}(E))$ be in $\mathrm{Emb}_D(\mathbb{F}_{p^2})$. Writing $\mathcal{O} = \mathbb{Z}[\tau]$, we have $f(\tau) \in \mathrm{End}(E)$. By Theorem 2.3.4, there is a curve $\tilde{E}$ over $\overline{\mathbb{Q}}$ with endomorphism β, and a prime $\mathfrak{p}$ over p with $\beta \equiv f(\tau) \bmod \mathfrak{p}$. Identifying τ and β, we have that the ring $\mathrm{End}(\tilde{E})$ is an order of $K = \mathbb{Q}(\tau)$ containing $\mathcal{O} = \mathbb{Z}[\tau]$. Let $\mathcal{O}' = \mathrm{End}(\tilde{E})$ and let $m = [\mathcal{O}' : \mathcal{O}]$. We show that $m = 1$ and therefore that $\mathrm{End}(\tilde{E})$ is precisely the order $\mathcal{O}$. As $\mathrm{End}(\tilde{E})$ injects into $\mathrm{End}(E)$, we have that $f(\mathcal{O}')$ is contained in $\mathrm{End}(E)$ and $[f(\mathcal{O}') : f(\mathcal{O})]$ is m. As the embedding f is optimal, $f(\mathcal{O})$ equals $f(K) \cap \mathrm{End}(E)$ and thus $m = 1$. Since f is normalized, the map $\tau \mapsto \beta$ gives the normalized isomorphism $\gamma : \mathcal{O} \xrightarrow{\sim} \mathrm{End}(\tilde{E})$. Therefore, the embedding $\mathcal{O} \xrightarrow{\gamma} \mathrm{End}(\tilde{E}) \hookrightarrow \mathrm{End}(E)$ is precisely f. By the theory of complex multiplication, $j(\tilde{E})$ is in $H_{\mathcal{O}}$, the ring class field of $\mathcal{O}$, which embeds in F since p is inert in K. Therefore, without loss of generality, we may assume $\tilde{E} \in \mathrm{Ell}_D(F)$. This proves the surjectivity of the map π.

Finally to show injectivity, consider $E, E' \in \mathrm{Ell}_D(F)$ with $\pi(E) = \pi(E') = (E_p, f)$. By the uniqueness of the lift of (E_p, f) in the Deuring lifting theorem, we have that E is isomorphic to E'. □

Definition 2.3.6 *The canonical lift* $\widetilde{E}$ *of a pair* $(E, f) \in \mathrm{Emb}_D(\mathbb{F}_{p^2})$ *is the inverse* $\pi^{-1}(E, f)$ *in* $\mathrm{Ell}_D(F)$.

This definition generalizes the notion of a canonical lift for ordinary elliptic curves to supersingular curves. In the remaining sections, we describe an algorithm to explicitly compute the canonical lift of (E, f), based on ideas from [10]. In particular, this algorithm gives an explicit way to lift a supersingular curve E and an endomorphism of E to the curve $\tilde{E}$ whose existence is guaranteed by the Deuring lifting theorem.

2.3.4 An action of the class group $Cl(\mathcal{O})$ on $\mathrm{Emb}_D(\mathbb{F}_{p^2})$

The integral ideals of $\mathcal{O}$ act on $\mathrm{Ell}_D(F)$ via

$$j(E) \mapsto j(E)^{\mathfrak{a}} = j(E/E[\mathfrak{a}]),$$

where $E[\mathfrak{a}]$ is the group

$$E[\mathfrak{a}] = \bigcap_{\alpha \in \mathfrak{a}} \ker(\alpha).$$

These are the points of E annihilated by all endomorphisms in $\mathfrak{a} \subset \mathrm{End}(E)$, using the fixed isomorphism $\mathcal{O} \simeq \mathrm{End}(E)$. As principal ideals act trivially, this action factors through the class group $Cl(\mathcal{O})$. If m is the conductor of $\mathcal{O}$, the group $Cl(\mathcal{O})$ is defined as the quotient of the group of ideals of $\mathcal{O}$ prime to m by the group of principal ideals of $\mathcal{O}$ prime to m. It is well-known that the $Cl(\mathcal{O})$-action is transitive and free [26, Thm. 10.3.5].

The bijection $\mathrm{Ell}_D(F) \to \mathrm{Emb}_D(\mathbb{F}_{p^2})$ from Theorem 2.3.5 induces a transitive and free action of the class group on the set $\mathrm{Emb}_D(\mathbb{F}_{p^2})$, which we describe now. Writing $\mathcal{O} = \mathbb{Z}[\tau]$, let $\beta \in \mathrm{End}(E)$ be the image of τ under the normalized isomorphism $\mathcal{O} \xrightarrow{\sim} \mathrm{End}(E)$. For an $\mathcal{O}$-ideal $\mathfrak{a} = (\ell, c + d\tau)$ of norm ℓ, let $\varphi_{\mathfrak{a}} : E \to E^{\mathfrak{a}}$ be the isogeny of complex multiplication-curves with kernel $E[\mathfrak{a}] = E[\ell] \cap \ker(c + d\beta)$. Consider the tensor product $\mathrm{End}(E^{\mathfrak{a}}) \otimes_{\mathbb{Z}} \mathbb{Q}$. By [26, 9.4 Diff 1], the normalized isomorphism $\mathcal{O} \xrightarrow{\sim} \mathrm{End}(E^{\mathfrak{a}}) \otimes_{\mathbb{Z}} \mathbb{Q}$ is now given by

$$\tau \mapsto \varphi_{\mathfrak{a}} \beta \widehat{\varphi}_{\mathfrak{a}} \otimes_{\mathbb{Z}} (\deg \varphi_{\mathfrak{a}})^{-1}.$$

The image of τ is an actual endomorphism of $E^{\mathfrak{a}}$ since the endomorphism $\varphi_{\mathfrak{a}} \beta \widehat{\varphi}_{\mathfrak{a}}$ kills the ℓ-torsion of $E^{\mathfrak{a}}$. This is because $\widehat{\varphi}_{\mathfrak{a}}$ kills one generator of the ℓ-torsion and maps the other generator to the kernel of $\varphi_{\mathfrak{a}}$, which is stabilized by β. Thus $\varphi_{\mathfrak{a}} \beta \widehat{\varphi}_{\mathfrak{a}}$ is of the form $\ell\delta$ for some $\delta \in \mathrm{End}(E^{\mathfrak{a}})$.

We have $E_p^{\mathfrak{a}} = (E^{\mathfrak{a}})_p$ and $f^{\mathfrak{a}}$ is the composition

$$f^{\mathfrak{a}} : \mathcal{O} \xrightarrow{\sim} \mathrm{End}(E^{\mathfrak{a}}) \hookrightarrow \mathrm{End}(E_p^{\mathfrak{a}}).$$

We have

$$f^{\mathfrak{a}}(\tau) = \overline{\varphi}_{\mathfrak{a}} f(\tau) \widehat{\overline{\varphi}}_{\mathfrak{a}} \otimes_{\mathbb{Z}} (\deg \overline{\varphi}_{\mathfrak{a}})^{-1}. \tag{2.4}$$

Note that if $\mathfrak{a}$ is a principal ideal, then $\varphi_{\mathfrak{a}}$ is an endomorphism of E. As $\mathrm{End}(E)$ is commutative, we have $f = f^{\mathfrak{a}}$. This confirms the fact that principal ideals act trivially.

We now describe a way to explicitly compute the embedding $f^{\mathfrak{a}}$, via the bijection of Proposition 2.3.3. This will be useful for the algorithm in Section 2.4, in which we need to determine the kernel of $f^{\mathfrak{a}}(\mathfrak{b})$ for $\mathfrak{a}, \mathfrak{b} \in Cl(\mathcal{O})$ with the norms of $\mathfrak{a}$ and $\mathfrak{b}$ not necessarily relatively prime. Loosely speaking, we can compute the action of $\mathfrak{a}$ on the corresponding embedding in $\mathrm{Emb}_D(\mathcal{A}_{p,\infty})$ and "translate" the resulting embedding back to an element of $\mathrm{Emb}_D(\mathbb{F}_{p^2})$, which will be the pair $(E^{\mathfrak{a}}, f^{\mathfrak{a}})$.

Given a supersingular curve $E/\mathbb{F}_{p^2}$ such that $\mathcal{O}$ embeds optimally into $\mathrm{End}(E)$, we fix an isomorphism

$$i : \mathcal{A}_{p,\infty} \xrightarrow{\sim} \mathrm{End}(E) \otimes \mathbb{Q}.$$

The order $R = i^{-1}(\mathrm{End}(E))$ is a maximal order of $\mathcal{A}_{p,\infty}$. Via this isomorphism, we view the embedding f as an element of $\mathrm{Emb}_D(\mathbb{F}_{p^2})$:

$$g = i^{-1} \circ f : \mathcal{O} \hookrightarrow R \subset \mathcal{A}_{p,\infty}.$$

For an ideal $\mathfrak{a}$ of $\mathcal{O}$, we compute the curve $E^{\mathfrak{a}} = \overline{\varphi}_{\mathfrak{a}}(E)$, where $\overline{\varphi}_{\mathfrak{a}}$ is the isogeny with kernel $E[f(\mathfrak{a})]$. We choose an auxiliary isogeny $\varphi_J : E \to E/E[J] = E^{\mathfrak{a}}$, where J is a left ideal of $\mathrm{End}(E)$. This induces an isomorphism $i_J : \mathcal{A}_{p,\infty} \xrightarrow{\sim} \mathrm{End}(E^{\mathfrak{a}}) \otimes \mathbb{Q}$ given by

$$\alpha \mapsto \varphi_J i(\alpha) \widehat{\varphi}_J \otimes (\deg \varphi_J)^{-1}.$$

Let $g = i_J^{-1} \circ f : \mathcal{O} \to R$ be given by $g(\tau) = y$. By Proposition 2.2.5, the maximal order $i_J^{-1}(\mathrm{End}(E^{\mathfrak{a}}))$ is equal to $R_r(J)$, the right order of J. Furthermore, the left R-ideal $Rg(\mathfrak{a})$ is right-isomorphic to J as an R-module, since they both determine the same isogenous curve, up to isomorphism ([46, Thm 3.11]). Therefore, there exists an $x \in \mathcal{A}_{p,\infty}$ with $Rg(\mathfrak{a}) = Jx$. We have that $y \in R_r(Rg(\mathfrak{a}))$, the right order of $Rg(\mathfrak{a})$, since the element $y = g(\tau)$ commutes with $g(\mathfrak{a})$ and is an element of R. Since $Rg(\mathfrak{a}) = Jx$, y is in

$x^{-1}R_r(J)x$, the right order of Jx. Therefore we obtain an embedding $\tau \mapsto xyx^{-1} \in R_r(J)$. The claim is that $i_J(xyx^{-1})$ is precisely $f^{\mathfrak{a}}(\tau)$.

Proposition 2.3.7 *Let $\mathfrak{a}$ be an ideal of $\mathcal{O}$. Let φ_J be an isogeny $E \to E^{\mathfrak{a}}$, where J is a left ideal of $\mathrm{End}(E)$. Let $f : \mathcal{O} = \mathbb{Z}[\tau] \to \mathrm{End}(E)$, and let the embedding $g = i_J^{-1} \circ f : \mathcal{O} \to R$ be given by $g(\tau) = y$. Then the induced embedding $f^{\mathfrak{a}} : \mathcal{O} \hookrightarrow \mathrm{End}(E^{\mathfrak{a}})$ is precisely*

$$f^{\mathfrak{a}}(\tau) = i_J(xyx^{-1}) \in \mathrm{End}(E^{\mathfrak{a}})$$

where $x \in \mathcal{A}_{p,\infty}$ is such that $Rg(\mathfrak{a}) = Jx$. The embedding $f^{\mathfrak{a}}$ is independent of the choice of J.

Proof: Let $R_J = R_r(J)$. The ideal $Rg(\mathfrak{a})$ is the product of ideals $J \cdot R_J x$. Thus by Proposition 2.2.5, the isogeny $\overline{\varphi}_{\mathfrak{a}}$ is the composition $\varphi_{R_J x} \circ \varphi_J$, where $\varphi_{R_J x}$ is the isogeny determined by the ideal $R_J x$. Since $R_J x$ is principal, this is precisely $i_J(x) = \varphi_J i(x) \widehat{\varphi}_J \otimes (\deg \varphi_J)^{-1}$. Thus $\overline{\varphi}_{\mathfrak{a}} = i_J(x) \circ \varphi_J = \varphi_J \circ i(x)$. Note that $i(x) \in \mathrm{End}(E) \otimes \mathbb{Q}$ defines an isogeny of E and thus $i(x)^{-1}$ is simply $\widehat{i(x)} \otimes (\deg i(x))^{-1}$.

The original embedding is given by $f(\tau) = i(y)$, and the induced embedding is $f^{\mathfrak{a}}(\tau) = \overline{\varphi}_{\mathfrak{a}} i(y) \widehat{\overline{\varphi}}_{\mathfrak{a}} \otimes (\deg \overline{\varphi}_{\mathfrak{a}})^{-1}$. Then

$$\begin{aligned}
f^{\mathfrak{a}}(\tau) &= \overline{\varphi}_{\mathfrak{a}} i(y) \widehat{\overline{\varphi}}_{\mathfrak{a}} \otimes (\deg \overline{\varphi}_{\mathfrak{a}})^{-1} \\
&= (\varphi_J \circ i(x)) i(y) (\widehat{i(x)} \circ \widehat{\varphi}_J) \otimes (\deg i(x) \deg \varphi_J)^{-1} \\
&= (\varphi_J \circ i(x)) i(y) (\widehat{i(x)} \circ \widehat{\varphi}_J) \otimes (\deg i(x) \deg \varphi_J)^{-1} \\
&= \varphi_J i(xyx^{-1}) \widehat{\varphi}_J \otimes (\deg \varphi_J)^{-1}
\end{aligned}$$

which is precisely $i_J(xyx^{-1})$. □

For $(p-1)|12$, the class number of $\mathcal{A}_{p,\infty}$ is one, and there is a single supersingular elliptic curve up to isomorphism. Thus $E^{\mathfrak{a}}$ is isomorphic to E, and $Rg(\mathfrak{a})$ is right-isomorphic to R. There exists $x \in \mathcal{A}_{p,\infty}$ with $Rg(\mathfrak{a}) = Rx$, and we get the embedding $\tau \mapsto xyx^{-1} \in R$. Note that $x \in R$ since $g(\mathfrak{a})$ is an integral ideal, and so $i(x)$ is an endomorphism of E. As $\overline{\varphi}_{\mathfrak{a}}$ and $i(x)$ both have the same kernel, we have that $\overline{\varphi}_{\mathfrak{a}} = h \circ i(x)$, for an isomorphism $h : E \to E^{\mathfrak{a}}$. Let i_h be the isomorphism given by $i_h(\alpha) = hi(\alpha)h^{-1}$ for all $\alpha \in \mathcal{A}_{p,\infty}$. Then the argument in the above proof shows that the embedding $f^{\mathfrak{a}} : \mathcal{O} \hookrightarrow \mathrm{End}(E^{\mathfrak{a}})$ is given by $f^{\mathfrak{a}}(\tau) = i_h(xyx^{-1})$.

2.3.5 An action of $Cl(\mathcal{O})$ on $\mathrm{Emb}_D(\mathcal{A}_{p,\infty})$

Via the bijection of Proposition 2.3.3, the action of $Cl(\mathcal{O})$ on $\mathrm{Emb}_D(\mathbb{F}_{p^2})$ induces an action on $\mathrm{Emb}_D(\mathcal{A}_{p,\infty})$ which is necessarily transitive and free. This action is essentially what has been described in the discussion of how to explicitly compute $f^{\mathfrak{a}}$. However, we now work in reference to a fixed maximal order R and a fixed set of left R-ideal class representatives $\{J_i\}$. This is convenient for the algorithms in the next sections, where we will compute the action first in $\mathrm{Emb}_D(\mathcal{A}_{p,\infty})$ and then translate back via a fixed set of isomorphisms i_{J_i} to elements of $\mathrm{Emb}_D(\mathbb{F}_{p^2})$. While the action of $Cl(\mathcal{O})$ on $\mathrm{Emb}_D(\mathcal{A}_{p,\infty})$ depends on a particular choice of maximal order R and set of left ideal class representatives $\{J_i\}$, Proposition 2.3.7 shows that the translation of this action back to $\mathrm{Emb}_D(\mathbb{F}_{p^2})$ via i_{J_i} is well-defined.

Given $g : \mathcal{O} \to R_r(J_k)$, an optimal embedding defined by $g(\tau) = y$ and an ideal $\mathfrak{a}$

of $Cl(\mathcal{O})$, we compute $g^{\mathfrak{a}}(\tau)$ where $g^{\mathfrak{a}}$ is the result of the action induced via Ψ :

$$g^{\mathfrak{a}} := \Psi^{-1}(\Psi(g)^{\mathfrak{a}}).$$

There exists an $x \in \mathcal{A}_{p,\infty}$ and a left ideal J_m such that $J_k g(\mathfrak{a}) = J_m x$. Multiplying on the left by J_k^{-1}, we get $J_k^{-1} J_k g(\mathfrak{a}) = J_k^{-1} J_m x$ which is the same as $R_r(J_k) g(\mathfrak{a}) = J_k^{-1} J_m x$. The integral left $R_r(J_k)$-ideal $n(J_k) J_k^{-1}$ defines the dual isogeny $\widehat{\varphi}_{J_k}$. Thus, by Proposition 2.2.5, the ideal $J = n(J_k) J_k^{-1} J_m$ defines an isogeny $\varphi_J = \varphi_{J_m} \widehat{\varphi}_{J_k} : E_k \to E \to E_m$. The claim is that $g^{\mathfrak{a}}(\tau) = xyx^{-1}$.

Let $(E_k, f) \in \mathrm{Emb}_D(\mathbb{F}_{p^2})$ be the image of g under Ψ. Since $J_k g(\mathfrak{a}) = J_m x$, we have that $E_k / E_k[f(\mathfrak{a})] \simeq E_m$ by [46, Thm. 3.11]. The pairs $(E_k, f)^{\mathfrak{a}}$ and $(E_m, f^{\mathfrak{a}})$ are equal under the equivalence relation of $\mathrm{Emb}_D(\mathbb{F}_{p^2})$, and so $\Psi(g)^{\mathfrak{a}} = (E_m, f^{\mathfrak{a}})$ and $g^{\mathfrak{a}} = \Psi^{-1}(E_m, f^{\mathfrak{a}}) = i_{J_m}^{-1} \circ f^{\mathfrak{a}}$.

We now apply Proposition 2.3.7 with $E = E_k$, $R = R_r(J_k)$, $i = i_{J_k}$ and φ_J the auxiliary isogeny. We have that

$$f^{\mathfrak{a}}(\tau) = \varphi_J i_{J_k}(xyx^{-1}) \widehat{\varphi}_J \otimes (\deg \varphi_J)^{-1}.$$

Using the fact that $i_{J_k} = \varphi_{J_k} i(-) \widehat{\varphi}_{J_k} \otimes (\deg \varphi_{J_k})^{-1}$ and that $\varphi_J = \varphi_{J_m} \widehat{\varphi}_{J_k}$, we get

$$\begin{aligned} f^{\mathfrak{a}}(\tau) &= \varphi_J \varphi_{J_k} i(xyx^{-1}) \widehat{\varphi}_{J_k} \widehat{\varphi}_J \otimes (\deg \varphi_{J_k} \deg \varphi_J)^{-1} \\ &= \varphi_{J_m} i(xyx^{-1}) \widehat{\varphi}_{J_m} \otimes (\deg \varphi_{J_m})^{-1} \\ &= i_{J_m}(xyx^{-1}). \end{aligned}$$

Therefore, to compute the action of $\mathfrak{a} \in Cl(\mathcal{O})$ on $g : \mathcal{O} \to R_r(J_k) \in \mathrm{Emb}_D(\mathcal{A}_{p,\infty})$, we choose $x \in \mathcal{A}_{p,\infty}$ and a left R-ideal class representative J_m such that $J_k g(\mathfrak{a}) = J_m x$, and let $g^{\mathfrak{a}}(\tau) = xyx^{-1}$. In particular, this gives a straightforward way to compute the class polynomial of $H_{\mathcal{O}}$ modulo a prime p inert in K, as we describe in the next section. We summarize in the following algorithm, the details of which are found in Appendix A. We assume we have fixed a $\mathbb{Z}$-basis $\{r_i\}$ for R. All computations in $\mathcal{A}_{p,\infty}$ take place with respect to this basis and the right orders of J_m and J_k are not explicitly computed.

Algorithm 2.3.1

INPUT:

- A basis $\{r_i\}$ of the order R
- An optimal embedding g given by $g(\tau) = y \in R_r(J_k)$ where $y = [y_1, ..., y_4]$ is in terms of $\{r_i\}$
- An integral ideal $\mathfrak{a} \in Cl(\mathcal{O})$ of norm a with $\mathfrak{a} = (a, c + d\tau)$

OUTPUT:

- The value $g^{\mathfrak{a}}(\tau) = w \in \mathcal{A}_{p,\infty}$, with w given in terms of $\{r_i\}$ as $[w_1, ..., w_4]$
- The left R-ideal class representative J_m such that $g^{\mathfrak{a}}$ is optimal with respect to $R_r(J_m)$

The following lemma shows that $w_i \in \mathbb{Q}$ will have denominator at most a divisor of $n(J_m)$. This fact is useful in the algorithms to compute the canonical lift in Sections 2.4 and 2.8.

Lemma 2.3.8 *Let $g(\tau) = y$ give an optimal embedding of $\mathcal{O}$ into $R_r(J_m)$ and let $g^{\mathfrak{a}}(\tau) = w$. Let $[w_1, ..., w_4]$ be the expression of w in terms of a basis for the maximal order R. Then $w_i \in \frac{1}{n(J_m)}\mathbb{Z}$.*

Proof: Let $h : \tau \mapsto z \in R$ be an optimal embedding into R. As the action is transitive, there exists an integral ideal $\mathfrak{a}_k \in Cl(\mathcal{O})$ such that $h^{\mathfrak{a}_k} = g$. Thus $g^{\mathfrak{a}} = (h^{\mathfrak{a}_k})^{\mathfrak{a}} = h^{\mathfrak{a}_k \mathfrak{a}}$ and there exists $v \in \mathcal{A}_{p,\infty}$ such that $Rh(\mathfrak{a}_k\mathfrak{a}) = J_m v$. We thus have $w = vzv^{-1}$. As $z \in R$, it is expressed as $[z_1, ..., z_4]$ with $z_i \in \mathbb{Z}$. Thus any denominators in the expression of w in terms of the basis for R must come from the denominators of v and v^{-1}, expressed in terms of the basis $\{e_i\}$.

As the ideal $\mathfrak{a}_m = \mathfrak{a}_k\mathfrak{a}$ is integral, we have that $J_m v = Rh(\mathfrak{a}_m)$ is contained in R. Thus, for every $\gamma \in J_m$, we have $\gamma v = r$ for some $r \in R$. In particular, for $n(\gamma) = \gamma\bar{\gamma}$, we have $n(\gamma)v = \bar{\gamma}r \in R$. Therefore, expressing v in terms of an integral basis for R, the denominators must divide $n(\gamma)$, for any γ. Therefore, the denominators are divisors of $n(J_m)$.

Now let $\alpha \in f(\mathfrak{a})$ and let $a \in \mathbb{Z}$ be the norm of α. As a is in $h(\mathfrak{a})$, we have that $Ra \subset J_m v$. As $J_m \subset R$, there exists $r \in R$ such that $av^{-1} = r$. Therefore, expressing v^{-1} in terms of an integral basis for R, its denominators must divide $n(\alpha)$ for all $\alpha \in \mathfrak{a}$. Thus, the denominators can at most be divisors of $n(\mathfrak{a})$.

As $w = vzv^{-1}$, the w_i can have denominators at most dividing $n(J_m)n(\mathfrak{a})$. However, the action is independent of the choice of ideal class representative, thus we may compute the value of w with respect to $\mathfrak{b}$, a representative with norm relatively prime to $n(\mathfrak{a})$, and this does not change the values of the w_i. Therefore, $w_i \in \frac{1}{n(J_m)}\mathbb{Z}$. □

2.3.5.1 Example

We illustrate the above algorithm by computing the action of $Cl(\mathcal{O})$ on an embedding in $\mathrm{Emb}_D(\mathcal{A}_{p,\infty})$ for $p = 37$ and $D = -56$. The ideal $\mathfrak{a} = (3, 1 + \tau)$ generates the class group $Cl(\mathcal{O})$, which is of order 4.

Let $\{1, i, j, k\}$ be the basis of $\mathcal{A}_{p,\infty}$ with $i^2 = -2, j^2 = j - 5, ij = k$. This basis is also a $\mathbb{Z}$-basis for a maximal order R. Writing $\mathcal{O} = \mathbb{Z}[\tau]$, the element $y = [0, 1, 1, -1] \in R$ satisfies $X^2 + 56 = 0$. As D is fundamental, this determines an optimal embedding $g : \mathcal{O} \to R$.

We compute the action of $\mathfrak{a}^i$, for $i = 1, ..., 4$ on the embedding g. The ideal $Rg(\mathfrak{a})$ is right-isomorphic to R via $x_1 = [1, 1, 0, 0]$. Thus $g^{\mathfrak{a}}(\tau) = x_1 y_0 x_1^{-1} = [-1, 0, 1, 1] \in R$, which we denote as y_1.

To compute $g^{\mathfrak{a}^2}$, we compute the action of $\mathfrak{a}$ on $g^{\mathfrak{a}}$. The ideal $Rg^{\mathfrak{a}}(\mathfrak{a})$ is right-isomorphic to J_2 via right-multiplication by $x_2 = [-1/2, 1/2, 1/2, 0]$. Then $g^{\mathfrak{a}^2}(\tau) = x_2 y_1 x_2^{-1} = [0, 1, 1, -1] \in R_2$, which we denote as y_2.

To compute $g^{\mathfrak{a}^3}$, we compute the action of $\mathfrak{a}$ on $g^{\mathfrak{a}^2}$. That is, we find the ideal class representative which is right-isomorphic to $J_2 g^{\mathfrak{a}^2}(\mathfrak{a})$. We find that $J_2 g^{\mathfrak{a}^2}(\mathfrak{a})$ is equivalent to J_3 via right-multiplication by $x_3 = [-1, -1, 0, 0]$. Then $g^{\mathfrak{a}^3}(\tau) = x_3 y_2 x_3^{-1} = [-1, 0, 1, 1] \in R_3$, which we denote as y_3.

As $\mathfrak{a}^4$ is principal, $g^{\mathfrak{a}^4}$ should be the original embedding g. To check this, we consider the ideal $J_3 g^{\mathfrak{a}^3}(\mathfrak{a})$ and find that it is right-isomorphic to R via right-multiplication by $x_4 = [-1, -1, 0, 0]$. Then $g^{\mathfrak{a}^4}(\tau) = x_4 y_3 x_4^{-1} = [0, 1, 1, -1] \in R$, which is precisely the original embedding. This confirms that the principal ideal $\mathfrak{a}^4$ acts trivially.

2.3.6 An algorithm to compute $H_D \bmod p$ for p inert with respect to D

In this section we present an algorithm to compute $H_D \bmod p$ for p inert with respect to D. This is used in the multi-prime algorithm [2] used to compute H_D. We remark that for a prime p with $(p-1)|12$, there is a unique supersingular j-invariant in characteristic p, and computing the class polynomial of $\mathcal{O}$ modulo p is trivial. For example, for $D \equiv 5 \bmod 8$, the prime $p = 2$ is inert in $\mathcal{O}$ and we immediately have $H_D(X) \bmod 2 = X^{h(\mathcal{O})}$.

Algorithm 2.3.2

INPUT:

- An imaginary quadratic discriminant $D < -4$
- A prime p inert in $\mathbb{Q}(\sqrt{D})$ with $p \nmid D$

OUTPUT: The polynomial $H_D(X) \bmod p$, where H_D is the class polynomial of $\mathcal{O}$

1. Write $\mathcal{O}$ as $\mathbb{Z}[\tau]$ where τ has characteristic polynomial

$$T(X) = \begin{cases} X^2 - X + \frac{1-D}{4} & D \equiv 1 \bmod 4 \\ X^2 + \frac{D}{4} & D \equiv 0 \bmod 4. \end{cases}$$

2. Compute an optimal embedding $g : \mathcal{O} \hookrightarrow \mathcal{A}_{p,\infty}$ given by $g(\tau) = y$ using Algorithm A.0.2. Let R be a maximal order that contains $g(\mathcal{O})$ optimally and fix a basis $\{r_i\}$ of R.

3. Choose a set $\{J_i\}$ of left R-ideal class representatives. This determines the set

$\mathrm{Emb}_D(\mathcal{A}_{p,\infty})$ of optimal embeddings of $\mathcal{O}$ into $\mathcal{A}_{p,\infty}$ with respect to some order $R_r(J_i)$, used in the set up for Algorithm 2.3.1.

4. Using Algorithm 2.3.1, compute $g^{\mathfrak{a}}$ and the corresponding left ideal class $J_{i_{\mathfrak{a}}}$ for each $\mathfrak{a} \in Cl(\mathcal{O})$.

5. For each J_i, compute the right orders $R_r(J_i)$. Use Algorithm A.0.1 to compute the correspondence between $\mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$-conjugacy classes of supersingular j-invariants over $\mathbb{F}_{p^2}$ and the set of maximal orders $\{R_r(J_i)\}$, up to conjugacy.

6. Using the above correspondence, identify each $J_{i_{\mathfrak{a}}}$ with a $\mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$-conjugacy class of supersingular j-invariant, denoted $j^{\mathfrak{a}}$.

7. Return $H_D(X) \bmod p = \prod_{\mathfrak{a} \in Cl(\mathcal{O})}(X - j^{\mathfrak{a}})$.

In Step 2 we use Algorithm A.0.2 in Appendix A to compute an element $y \in \mathcal{A}_{p,\infty}$ satisfying the same minimal polynomial as a generator τ of $\mathcal{O}$ and such that $\tau \mapsto y$ gives an optimal embedding into R, for some a maximal order of $\mathcal{A}_{p,\infty}$.

In Step 3, we compute a set of left ideal class representatives $\{J_i\}$. Algorithms to compute a set $\{J_i\}$ of left ideal class representatives of R and the set of their respective right orders $\{R_r(J_i)\}$ can be found in [44, 9] and are implemented in the computer algebra program MAGMA [9].

For Step 4, let $Cl(\mathcal{O}) = \bigoplus \langle \mathfrak{a}_i \rangle$ be a decomposition of the class group into a direct product of cyclic groups generated by integral prime ideals $\mathfrak{a}_i$ of order h_i and norm ℓ_i not dividing p. To compute $g^{\mathfrak{a}}$, we first successively compute the action of the $\mathfrak{a}_i$ on the embedding $f(\tau) = y$ using Algorithm 2.3.1. That is, we take $h_1 - 1$ successive applications of $\mathfrak{a}_1$ to get $f^{\mathfrak{a}_1}, \ldots, f^{\mathfrak{a}_1^{h_1-1}}$. To each of these, $\mathfrak{a}_2$ is applied $h_2 - 1$ times, and so forth. This gives a sequence (with possible repetition) of ideal class representatives $J_{i_\mathfrak{a}}$ of R, each corresponding to a maximal order $R_r(J_{i_\mathfrak{a}})$. We remark that in this step we do not need to have explicitly computed the right orders $\{R_r(J_i)\}$.

For Step 5, to compute the set of right orders $\{R_r(J_i)\}$, we use the algorithm in [9]. To compute the correspondence, we use an algorithm of Cerviño [6] which associates to each $\mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$-conjugacy class j of supersingular j-invariants a maximal order of $\mathcal{A}_{p,\infty}$, up to conjugacy. This algorithm is based on comparing the the elements of specified norm n and trace t of the maximal orders $R_r(J_i)$ with the endomorphisms of trace t and degree n in $\mathrm{End}(E_i)$ where the E_i are representatives of the isomorphism classes of supersingular curves. For more detail, see Algorithm A.0.1 in Appendix A.

Using the list from Step 5, we associate to each $J_{i_\mathfrak{a}}$ from Step 4 the corresponding $\mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$-conjugacy class of supersingular j-invariant, denoted $j^\mathfrak{a}$. This gives a list of size $h(\mathcal{O})$ of $\mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$-conjugacy classes of j-invariants. We compute $H_D(X)$ as the product of factors $(X-j)$ for all j on the list. For j in $\mathbb{F}_p$, we include one factor of $(X-j)$ for each time j appears on the list. The j-invariants not in $\mathbb{F}_p$ appear an even number of times since the roots of $H_D \bmod p$ which are not in $\mathbb{F}_p$ come in conjugate pairs. Thus for $j \notin \mathbb{F}_p$, we include the factor $(X-j)(X-\bar{j})$ for every two times j appears on the list. We expand $\prod(X - j^\mathfrak{a})$ modulo p to obtain $H_D(X) \bmod p$.

This algorithm is used in the *multi-prime algorithm* to compute the class polynomial $H_D(X)$ ([2]). The polynomial $H_D(X)$ is computed modulo p for sufficiently many primes

p which either split principally or are inert in K. Then $H_D(X)$ is computed modulo the product of these primes using the Chinese Remainder theorem. If the product of primes is greater than $2 \cdot 10^C$, where C is the bound in Section 2.1, the coefficients can be recognized as integers and we obtain the polynomial $H_D(X)$.

2.3.6.1 Example

We illustrate the algorithm with an example. Let $p = 53$ and $D = -71$. We compute $H_{-71} \bmod 53$. The order $\mathcal{O}$ of discriminant D can be written as $\mathbb{Z}[\tau]$ for τ with characteristic polynomial $T(X) = X^2 - X + 18$.

There are four $\mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$-conjugacy classes of supersingular j-invariants over $\mathbb{F}_{p^2}$:

$$j = 0, 46, 50, 28 \pm 9\sqrt{2}.$$

The quaternion algebra $\mathcal{A}_{p,\infty}$ has a basis $\{1, i, j, k\}$ with $i^2 = -2, j^2 = -35, ij = k$. We compute an embedding given by $f(\tau) = y = 1/2 - 3/2i + 1/2j$, where y is a root of $X^2 - X + 18 = 0$. This lies in the maximal order R with basis $\{1, i, (2-i-k)/4, -(1+i+j)/2\}$. As D is a fundamental discriminant, the embedding is automatically optimal.

We calculate a set of left ideal class representatives $J_1, ..., J_5$ and their corresponding maximal orders $R_1, ..., R_5$. The ideal $\mathfrak{a} = (2, 3 + \tau)$ generates the class group of $\mathcal{O}$, which is of order 7. Computing the action of $\mathfrak{a}$ successively yields a sequence of left ideals

$$J_5, J_3, J_1, J_3, J_4, J_2, J_2$$

which corresponds to a sequence of embeddings into the right orders

$$R_5, R_3, R_1, R_3, R_4, R_2, R_2.$$

We now establish the correspondence of the R_i with the four $\mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$-conjugacy classes of supersingular j-invariants. We use Algorithm A.0.1 as described in Step 5. In this case, it suffices to look at the elements of norm less than or equal to two. Before doing so, we test which of the five orders are conjugate. In this way, we determine that R_4 and R_5 correspond to the class $j = 28 \pm 9\sqrt{2}$. By computing the units of the remaining orders, we find that all orders except R_1 have unit group ± 1. Thus R_1 corresponds to $j = 0$. It remains to determine the correspondence of the orders R_2, R_3 with $j = 46$ and 50. In this case, it suffices to look at elements of norm 2. We take the curve $y^2 = x^3 + 40x + 26$ with $j = 46$. Computing the isogenous curves for each factor of the two-division polynomial reveals that this curve has no endomorphisms of degree 2. As the basis for R_2 contains an element of norm 2, this immediately identifies $j = 46$ with the order R_3 and $j = 50$ with R_2.

Computing $H_D(X) \bmod p$ is a matter of counting how many times the order R_i appears in the sequence above. Using the correspondence, we obtain the sequence of $\mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$-conjugacy classes

$$28 \pm 9\sqrt{2}, 46, 0, 46, 28 \pm 9\sqrt{2}, 50, 50.$$

We then compute

$$H_{-71}(X) \bmod 53 = X(X-46)^2(X-50)^2(X^2+50X+39).$$

2.4 Computing the canonical lift of (E, f) for $p \equiv 1 \bmod 12$

2.4.1 The map ρ_α for the case of $p \equiv 1 \bmod 12$

In this section we give an algorithm to compute the canonical lift of $(E_o, f) \in \mathrm{Emb}_D(\mathbb{F}_{p^2})$ where p is inert with respect to D and $p \equiv 1 \bmod 12$. By Proposition 2.2.3, the condition $p \equiv 1 \bmod 12$ ensures that the elliptic curves with j-invariants $0, 1728$ are *not* supersingular. The case where one of these two curves is supersingular is more technical due to the extra automorphisms of the curve and is addressed in Sections 2.5-2.8.

Let $\mathbb{C}_p$ be the completion of an algebraic closure of $\mathbb{Q}_p$. The field $\mathbb{C}_p$ is algebraically closed. Let $\eta = (E_o, f)$ be an element of $\mathrm{Emb}_D(\mathbb{F}_{p^2})$ and let $\tilde{E}$ denote its canonical lift. We define a 'disc' above η containing all possible candidates for the j-invariant $\tilde{E}$. These are pairs $(j(E), f)$ with $j(E) \equiv j(E_o)$ modulo $\mathfrak{p}$, where $\mathfrak{p}$ is the prime above p in the smallest extension of $\mathbb{Q}_p$ in which $j(E)$ lies. We denote this disc by

$$X_D(\eta) = \{(j(E), f) \mid j(E) \in \mathbb{C}_p, j(E) \equiv j(E_o) \bmod \mathfrak{p}\}.$$

Ignoring the second coordinate, this is simply the open p-adic disc of radius one around $j(E_o)$ viewed as an element of F.

The reason for including the second coordinate f is as follows. While there may be multiple curves $E \in \mathrm{Ell}_D(F)$ which reduce to E_o modulo p, only one such curve (up to isomorphism) satisfies the condition that the induced embedding $\mathrm{End}(E) \hookrightarrow \mathrm{End}(E_o)$ is equivalent to f, namely the canonical lift $\tilde{E}$. By including the second coordinate f, we establish a bijection between the set of discs $X_D(\eta)$ and the set $\mathrm{Ell}_D(F)$. This is the statement of Theorem 2.3.5. We then view of the pair $(j(\tilde{E}), f)$ as the "center" of $X_D(\eta)$

and adapt the key idea of [10] to construct a p-adic analytic map from the disc to itself that has this pair as a fixed point. Using this map, we can "zero in" on the canonical lift of η.

Let $\mathfrak{a}$ be an ideal of $\mathcal{O}$ of norm N which is coprime to p. We define a map

$$\rho_{\mathfrak{a}} : \bigcup_{\eta} X_D(\eta) \to \bigcup_{\eta} X_D(\eta)$$

as follows. For $(j(E), f) \in X_D(\eta)$, the ideal $f(\mathfrak{a}) \subset \mathrm{End}(E_o)$ defines a subgroup $E_o[f(\mathfrak{a})]$ of $E_o[N]$. As $(N, p) = 1$, the subgroup $E_o[f(\mathfrak{a})]$ lifts canonically to a subgroup of the N-torsion of E which we denote $E[\mathfrak{a}]$. We define

$$\rho_{\mathfrak{a}}(j(E), f) = (j(E/E[\mathfrak{a}]), f^{\mathfrak{a}}),$$

where $f^{\mathfrak{a}}$ is as described in Section 2.3.4. When the embedding f is clear, we also denote by $\rho_{\mathfrak{a}}$ the induced map on the open p-adic disc of radius one in $\mathbb{C}_p$ around $j(E_o)$.

For principal ideals $\mathfrak{a} = (\alpha)$, we have $f^{(\alpha)} = f$ and thus the map ρ_α stabilizes every disc. Furthermore, as f is the induced embedding $\mathcal{O} \xrightarrow{\sim} \mathrm{End}(\tilde{E}) \hookrightarrow \mathrm{End}(E_o)$, the subgroup $\widetilde{E}[(\alpha)]$ is precisely the kernel of α viewed as an endomorphism of $\tilde{E}$. Therefore, $\tilde{E}/\tilde{E}[\alpha]$ is isomorphic to $\tilde{E}$, and the map ρ_α fixes $j(\widetilde{E})$. Since $j(E_o)$ does not equal $0, 1728$, the map ρ_α is *p-adic analytic* by [5, Theorem 4.2]. That is, there exist $a_i \in \mathbb{Z}_F$ such that

$$\rho_\alpha(x) - j(\tilde{E}) = \sum_{i \geq 1} a_i (x - j(\tilde{E}))^i,$$

for all $x \in X_D(\eta)$. This comes from an interpretation of ρ_α as a map on modular curves. In Section 2.8.1, we will define a similar map in order to handle the case of $p \neq 1 \bmod 12$. Though the map is more technical, we are able to establish analogous results, and thus we defer more detail on ρ_α to that section.

By [5, Lemma 4.3], the derivative of ρ_α at $j(\widetilde{E})$ is equal to $\alpha/\overline{\alpha} \in \mathbb{Z}_F$. If $\alpha/\overline{\alpha} - 1$ is a p-adic unit, we can use a modified version of Newton's method to converge to $j(\widetilde{E})$ starting from a random lift $(j_0, f) \in X_D(\eta)$. As described in [5], the sequence $\{j_k\}$ with

$$j_{k+1} = j_k - \frac{\rho_\alpha(j_k) - j_k}{\alpha/\overline{\alpha} - 1}, \tag{2.5}$$

converges quadratically to $j(\widetilde{E})$. This is the key idea of the algorithm presented in the next section.

2.4.2 An algorithm to compute the canonical lift of (E, f)

We now present the algorithm to compute the canonical lift of the pair (E, f) of the set $Emb_D(\mathbb{F}_{p^2})$ to a specified p-adic accuracy for $p \equiv 1 \mod 12$. We use "accuracy" to mean how p-adically close the computed value is to the actual value in terms of the number of p-adic digits to which they agree. We use "precision" to mean the number of p-adic digits which we keep track of in computations. The overall structure of the algorithm is modeled after the algorithm to compute the canonical lift in the case of an ordinary elliptic curve ([5]). Both the theory and technical details differ however, as we are working with supersingular curves.

Algorithm 2.4.1

INPUT:

- E, a supersingular curve modulo p
- A maximal order R of $\mathcal{A}_{p,\infty}$ with $\mathrm{End}(E) \simeq R$ and a basis $\{r_i\}$ of R

- An explicit isomorphism $i : R \to \text{End}(E)$ specified by an identification of bases $\{r_i\}$ of R and $\{e_i\}$ of $\text{End}(E)$

- An optimal embedding $f : \mathcal{O} = \mathbb{Z}[\tau] \hookrightarrow \text{End}(E)$ given by $f(\tau) = y = [y_1, ..., y_4]$ expressed in terms of $\{e_i\}$

- $r \in \mathbb{Z}$ such that 2^r is greater than or equal to the desired p-adic accuracy

OUTPUT: The canonical lift $j(\tilde{E})$ of (E, f) to 2^r p-adic digits accuracy.

1. Choose $\alpha = a + b\tau \in \mathbb{Z}[\tau]$ such that $\frac{\alpha}{\bar{\alpha}} - 1$ is a p-adic unit by searching the set

   $$S_A = \{a + b\tau \mid a, b \in \mathbb{Z}, b \not\equiv 0 \bmod p, a + b\tau \text{ prime to } D, \text{ and } n(a + b\tau) \leq A\}$$

   where the bound A is greater than $n(\tau)$. If the set is empty, we increase A until this is not the case. Let $\prod_{i=1}^{m} \mathfrak{b}_i$ be the factorization of α into prime ideals and let $\mathfrak{a}_n = \prod_{i=1}^{n} \mathfrak{b}_i$ for $n = 1, ..., m$.

2. Choose the smallest prime ℓ relatively prime to $n(\alpha)$. Compute $\{J_i\}$, a set of left R-ideal class representatives, each with norm a power of ℓ and the set of right orders $\{R_r(J_i)\}$. This determines the set $\text{Emb}_D(\mathcal{A}_{p,\infty})$ used in the set up of Algorithm 2.3.1. Compute the corresponding set of elliptic curves $E_i = E/E[i(J_i)]$.

3. Using Algorithm 2.3.1, compute the action of $\alpha = \prod_{i=1}^{m} \mathfrak{b}_i$ on the embedding g given by $g(\tau) = y$ in a successive manner to obtain a sequence of embeddings $\{g^{\mathfrak{a}_n}\}$ for $n = 0, 1, ..., m - 1$ where $g^{\mathfrak{a}_n} : \mathcal{O} \hookrightarrow R_r(J_{i_n})$ with $i_n \in \{1, ..., h_p\}$. The embedding $g^{\mathfrak{a}_n}$ is obtained by computing the action of $\mathfrak{b}_n$ on the embedding $g^{\mathfrak{a}_{n-1}}$.

4. Compute $E[f(\mathfrak{a}_1)]$ and the polynomial $P_1(X)$ whose roots are the x-coordinates of the points of $E[f(\mathfrak{a}_1)]$. For $n = 1, ..., m-1$, let $f^{\mathfrak{a}_n} = i_{J_{i_n}} \circ g^{\mathfrak{a}_n}$ and let $E^{\mathfrak{a}_n} = E_{i_n}$. Compute the subgroup $E^{\mathfrak{a}_n}[f^{\mathfrak{a}_n}(\mathfrak{b}_{n+1})]$ and the corresponding kernel polynomial $P_n(X) \in F[X]$. In this way, obtain the cycle of isogenies

$$E \overset{\mathfrak{b}_1}{\to} E^{\mathfrak{a}_1} \overset{\mathfrak{b}_2}{\to} E^{\mathfrak{a}_2} ... \overset{\mathfrak{b}_m}{\to} E^{(\alpha)} = E. \tag{2.6}$$

5. Let j_0 be an arbitrary lift of $j(E)$ to 2 digits precision.

6. For $k = 0, 1, 2, ..., r-1$, repeat the following steps. The k^{th} iteration produces j_{k+1}, the 2^{k+1}-digit approximation to $\tilde{j}$. Computations are done to 2^{k+1} digits precision.

   (a) Let E_k be a curve with j-invariant j_k which reduces to E. Compute $\rho_\alpha(j_k)$ by lifting the cycle of isogenies (2.6) in a step-by-step manner to a cycle of isogenies over F:

   $$E_k \overset{\mathfrak{b}_1}{\to} E_k^{\mathfrak{a}_1} \overset{\mathfrak{b}_2}{\to} E_k^{\mathfrak{a}_2} ... \overset{\mathfrak{b}_m}{\to} E_k^{(\alpha)}. \tag{2.7}$$

   (b) Compute

   $$j_{k+1} = j_k - \frac{\rho_\alpha(j_k) - j_k}{\alpha/\bar{\alpha} - 1}$$

   to obtain $j_{k+1} \in F$, the 2^{k+1}-digit approximation to $j(\tilde{E})$.

7. Return j_{r-1}, the 2^r p-adic digit approximation to $\tilde{j}$.

In Step 1, we want to choose α not only such that $\alpha/\bar{\alpha} - 1$ is p-adic unit but also such that α is "smooth," that is, factors into the product of ideals of small norm. This is key to computing the map ρ_α. Recall that ρ_α corresponds to an isogeny of degree $n(\alpha)$, the norm of α, which is on the same order as D. For large D, it is not feasible to compute the isogeny directly. However if $n(\alpha)$ has small prime factors, we can compute this as a sequence of isogenies of small degree.

The condition $b \not\equiv 0 \bmod p$ is necessary and sufficient for $\alpha/\bar{\alpha} - 1$ to be a p-adic unit. Since $p \nmid D$, the prime p is inert in K and does not divide the conductor of $\mathcal{O}$. Thus the minimal polynomial $T(X)$ of τ is irreducible modulo p and $\tau \not\equiv \bar{\tau} \bmod p$. Thus if $p \nmid b$, then $\bar{\alpha} = a + b\bar{\tau}$ is invertible and $\alpha \not\equiv \bar{\alpha} \bmod p$.

To find an α satisfying these conditions, we fix $A > n(\tau)$ and $B = 20$ and search the set

$$S_A = \{a + b\tau \mid a, b \in \mathbb{Z}, b \not\equiv 0 \bmod p, a + b\tau \text{ prime to } D, \text{ and } n(a + b\tau) \leq A\}$$

for elements α such that $n(\alpha)$ is B-smooth. That is, the smallest prime factor of $n(\alpha)$ is less than B. We also may impose the additional condition that $\gcd(a, b) = 1$ to ensure the isogeny corresponding to α is not an integer multiple of an isogeny of smaller degree. The condition that $a + b\tau$ is prime to D implies that the principal ideal (α) is prime to the conductor of $\mathcal{O}$. If there are no such α we may increase either A, B or both until we find an α satisfying the conditions. (There are more sophisticated sieving methods that could be used to improve the efficiency of this search.)

Remark 2.4.1

We can give a heuristic upper bound on the size of A needed to find a B-smooth element α where $B = \lfloor \exp \sqrt{\log |D|} \rfloor$. This uses the following lemma from [10].

Lemma 2.4.1 *[10, Lem. 2] Let D be an imaginary quadratic discriminant and let τ be an integer of $K = \mathbb{Q}(\sqrt{D})$ with characteristic polynomial $X^2 - tX + n$ where $t^2 - 4n = D$.*

Let $\epsilon \in (0, \frac{1}{2})$ and let S be the set of integers $a + b\tau$ with $(a, b) = 1, a + b\tau$ prime to nD, $1 \leq b \leq 2\exp((\log|D|)^{\frac{1}{2}+\epsilon})$ and $n(a + \frac{1}{2}bt) \leq |D|^{\frac{1}{2}}\exp((\log|D|)^{\frac{1}{2}+\epsilon})$. Let $B = \lfloor \exp\sqrt{\log|D|} \rfloor$. Assuming the Generalized Riemann Hypothesis, the proportion of B-smooth elements of S is greater than or equal to $\exp(-2(\log|D|)^{\frac{1}{2}}\log\log|D|$ for D sufficiently large depending on ϵ.

In searching S, we are guaranteed to find a B-smooth element α with norm less than $|D|\exp(2(\log|D|)^{\frac{1}{2}+\epsilon})$. Such an element does not necessarily satisfy the condition that p does not divide b. However, heuristically speaking, there is only a $\frac{1}{p}$ probability that this condition fails, and therefore this gives an estimate on A.

As noted in [5, p.17], an alternative approach to finding a suitable element α is to choose q the smallest split prime in $\mathcal{O}$. Under the Generalized Riemann Hypothesis, the bound on q is $O((\log|D|)^2)$. Letting $(q) = \mathfrak{a}\bar{\mathfrak{a}}$, we have that $\mathfrak{a}^d$ is principal for some d dividing the class number of $\mathcal{O}$. If $\mathfrak{a}^d = (\alpha)$ for α such that $\alpha/\bar{\alpha} - 1$ is invertible, then we may use this α for the map.

In Step 2, we compute a set of left ideal class representatives $\{J_i\}$ of R of norm a power of ℓ using the algorithm found in [44, 9]. Each J_i is given by a basis $\beta_{i,k}$ of four elements of R. Let ℓ^d be the maximum of the norms $n(\beta_{i,k})$. For each J_i, we compute the subgroup of E corresponding to the ideal $i(J_i)$ of $\mathrm{End}(E)$ by checking which points of $E[\ell^d]$ are killed by $i(\beta_{i,k})$ for all k. Then we use Vélu's formulas [41] to compute the isogenous curve $E_i = E/E[J_i]$. This curve is uniquely determined by the condition that the isogeny be *normalized* (see Remark 2.2.1).

For Step 4, we describe the computation of $E^{\mathfrak{a}}[f^{\mathfrak{a}}(\mathfrak{b})]$ given the curve $E^{\mathfrak{a}} = E_i$ and the embedding $f^{\mathfrak{a}} = \varphi_{J_i} i(w) \widehat{\varphi}_{J_i} \otimes (\deg \varphi_{J_i})^{-1}$ where $w = [w_1, ..., w_4] \in \mathcal{A}_{p,\infty}$ is expressed in terms of the basis $\{e_i\}$.

By the choice of $\{J_i\}$, the least common multiple of the denominators of the w_i is ℓ^d for some $0 \leq d \leq h_p$, using Lemma 2.3.8. Therefore $\ell^d i(w)$ is a $\mathbb{Z}$-linear combination of the endomorphisms e_i of E. Write $\mathfrak{b} = (m, c + d\tau)$ with m the norm of $\mathfrak{b}$. Again by choice of J_i, we have that m is relatively prime to $\deg \varphi_{J_i}$. Therefore, we can calculate $E^{\mathfrak{a}}[f^{\mathfrak{a}}(\mathfrak{b})]$ by checking which m-torsion of E_i is killed by the isogeny

$$\ell^d \big(\deg \varphi_{J_i} c + d \cdot \varphi_{J_i} i(w) \widehat{\varphi}_{J_i} \big).$$

We now describe how to compute $\rho_\alpha(j_k)$ in Step 5. Let E_k be a curve reducing to E with j-invariant j_k. To lift $E[f(\mathfrak{a}_1)]$ to E_k, use Hensel's lemma to lift the kernel polynomial $P_1(X)$ to a factor of the ℓ_1-division polynomial of E_k. Use Vélu's formula to compute $j_k^{\mathfrak{a}_1}$, the j-invariant of $E_k^{\mathfrak{a}_1} = E_k / E_k[\mathfrak{a}_1]$. Note that $j_k^{\mathfrak{a}_1} = \rho_{\mathfrak{a}_1}(j_k)$.

In the same way, lifting the polynomials $P_i(X)$ for $i = 2, ..., m$, we compute the cycle of j-invariants

$$j_k \xrightarrow{\mathfrak{b}_1} j_k^{\mathfrak{a}_1} \xrightarrow{\mathfrak{b}_2} j_k^{\mathfrak{a}_2}, ..., \xrightarrow{\mathfrak{b}_m} j_k^{(\alpha)}$$

over F, with computations carried out to 2^{k+1} p-adic digits precision. The resulting $j_k^{(\alpha)}$ is precisely $\rho_\alpha(j_k) + O(p^{2^{k+1}})$.

We remark that for $p = 13$, there is a single isomorphism class of supersingular elliptic curve over $\mathbb{F}_{13}$ and Step 2 is not needed. Furthermore, the computation in Step 4 simplifies to finding which m-torsion is killed by $c + di(w)$.

2.4.2.1 Example

We illustrate Algorithm 2.4.1 by computing the canonical lift of an element of $\mathrm{Emb}_D(\mathbb{F}_{p^2})$ where $D = -56$ and $p = 37$. Let $\mathbb{F}_{p^2} = \mathbb{F}_p[a]$ where a is a root of $X^2+2 = 0$. Let E be the curve $Y^2 = X^3 + 12X + 13$ with j-invariant 8. Let $\{1, i, j, k\}$ be the basis of $\mathcal{A}_{p,\infty}$ with $i^2 = -2, j^2 = j - 5, ij = k$. This basis is also a $\mathbb{Z}$-basis for a maximal order R that is isomorphic to the endomorphism ring $\mathrm{End}(E)$. Writing $\mathcal{O} = \mathbb{Z}[\tau]$, the element $y = [0, 1, 1, -1] \in R$ satisfies $X^2 + 56 = 0$, and as D is fundamental, this determines an optimal embedding $f : \mathcal{O} \to \mathrm{End}(E)$. We now compute the canonical lift of the pair (E, f) to 16 p-adic digits precision.

In Step 1, we choose $\alpha = (5+2\tau)$. The factorization of α is $\mathfrak{a}^4$ where $\mathfrak{a} = (3, 1+\tau)$ is a prime lying over 3.

For Step 2, we use $\ell = 2$. Let J_2 be the left ideal of R with basis $\{2, i + j, 2j, k\}$ and J_3 the ideal with basis $\{1 + j + k, i + k, 2j, 2k\}$. The ideals $J_1 = R, J_2, J_3$ form a set of left R-ideal class representatives. The ideal J_2 defines the 2-isogeny $\varphi_{J_2} : E \to E_2 = E/E[J_2]$ with kernel $\langle(19 + 23a, 0)\rangle$. The curve E_2 has j-invariant $3 - 14a$. The ideal J_3 gives $\varphi_{J_3} : E \to E_3$ with kernel $\langle(19 - 23a, 0)\rangle$ and $j(E_3) = 3 + 14a$. This gives the correspondence of curves and orders: E_1, E_2, E_3 with R, R_2, R_3.

For Step 3, we compute the action of $\alpha = \mathfrak{a}^4$ on $g(\tau) = y$. This has been done in Example 2.3.5.1 and we obtain the sequence

$$\tau \mapsto y_1 \in R, y_2 \in R_2, y_3 \in R_3, y_4 \in R.$$

From Step 2, using the correspondence of E_1, E_2, E_3 with R, R_2, R_3, we count the number of times each order appears in the sequence and obtain

$$H_D \bmod p = (X-8)^2(X^2-6X-6).$$

Now we compute the sequence of kernel polynomials as in Step 4. Let $f = i \circ g$, and compute the kernel $E[f(\mathfrak{a})]$ by checking which 3-torsion points $P \in E[3]$ are killed by $1+f(\tau) \in \mathrm{End}(E)$. This yields the points P with x-coordinate $18 \pm 9a$. Using Vélu's formulas, we confirm that $E^{\mathfrak{a}} \simeq E$.

Similarly, to find $E[f^{\mathfrak{a}}(\mathfrak{a})]$ we check which 3-torsion points $P \in E[3]$ are killed by $1+f^{\mathfrak{a}}(\tau) \in \mathrm{End}(E)$. This yields the points P with x-coordinate $19 \pm 12a$. Note that that $E^{\mathfrak{a}^2}$ has j-invariant $3-14a$, which confirms that $E^{\mathfrak{a}^2} \simeq E_2$.

Now $f^{\mathfrak{a}^2}(\tau) = i_{J_2} \circ g^{\mathfrak{a}^2}(\tau) = i_{J_2}(y_2)$. As there are no denominators in the expression of y_2 in terms of the basis $\{e_i\}$, to find the kernel $E_2[f^{\mathfrak{a}^2}(\mathfrak{a})]$, we check which 3-torsion points $P \in E_2[3]$ are killed by the isogeny

$$2 \cdot c + d \cdot \varphi_{J_2} i(y_2) \widehat{\varphi}_{J_2}.$$

We obtain the points P with x-coordinate $32+8a$. Using Vélu's formulas, we see that $E^{\mathfrak{a}^3} \simeq E_3$.

Lastly, we have $f^{\mathfrak{a}^3}(\tau) = i_{J_3} \circ g^{\mathfrak{a}^3}(\tau) = i_{J_3}(y_3)$. We check which 3-torsion points $P \in E_3[3]$ are killed by the isogeny

$$2 \cdot c + d \cdot \varphi_{J_3} i(y_3) \widehat{\varphi}_{J_3}$$

and obtain the kernel polynomial for $E_3[f^{\mathfrak{a}^3}(\mathfrak{a})]$ as $X + 25a + 11$.

Thus we have a cycle of 3-isogenies

$$(E,f) \to (E^{\mathfrak{a}} = E, f^{\mathfrak{a}}) \to (E^{\mathfrak{a}^2}, f^{\mathfrak{a}^2}) \to (E^{\mathfrak{a}^3}, f^{\mathfrak{a}^3}) \to (E^{\mathfrak{a}^4}, f^{\mathfrak{a}^4}) = (E,f)$$

where each element of the cycle corresponds uniquely to a root of $H_D(X)$.

For Step 5, we choose the curve defined by $Y^2 = X^3 - 210X + 420$ over the unramified extension F of degree 2 of $\mathbb{Q}_p$. Let $F = \mathbb{Q}_p[\tilde{a}]$ where $\tilde{a}$ is the unique lift of $a \in \mathbb{F}_{p^2}$ as a root of $X^2 + 2 = 0$. We lift the cycle of isogenies over $\mathbb{F}_{p^2}$ to F to 2 p-adic digits precision using Hensel's lemma, and obtain $\rho_\alpha(j_0) = 555\tilde{a} - 214 + O(37^2)$. Updating according to the Newton formula, we get $j_1 = 148\tilde{a} - 66 + O(37^2)$. Next we work with 4 p-adic digits precision, lift the cycle of isogenies to get $\rho_\alpha(j_1)$ and update the j-invariant as before.

k	j_k	$\rho_\alpha(j_k)$
0	$8 + O(37^2)$	$555\tilde{a} - 214 + O(37^2)$
1	$148\tilde{a} - 66 + O(37^2)$	$805120\tilde{a} - 733850 + O(37^4)$
2	$37111\tilde{a} + 492774 + O(37^4)$	$3444839480038\tilde{a} + 1323692294659 + O(37^8)$

The value j_3 is $19341378631\tilde{a} + 1272855677534 + O(37^8)$, which is a 37^8 approximation of the canonical lift of (E, f). To confirm this, we use the complex analytic method to compute the polynomial $H_{-56}(X)$, as implemented in MAGMA [9]. We then check that $H_{-56}(j_3)$ has valuation 8, while $H'_{-56}(j_3)$ has valuation one. Therefore, by Hensel's lemma [25, Prop. II.2.2], j_3 lifts uniquely to a root of $H_{-56}(X)$ and is in fact an 8-digit p-adic approximation to the canonical lift of (E, f).

2.5 The Legendre form of an elliptic curve and the case of $p \not\equiv 1 \bmod 12$

2.5.1 Motivation for working with the Legendre form of E

In this section, we present an algorithm which computes the canonical lift of (E, f) in the case of $p \not\equiv 1 \bmod 12$. We begin by explaining the complication that arises when computing the canonical lift in this case.

Let $D < -4$ and let $\mathcal{O}$ be the order of K of discriminant D. Let p be any prime inert with respect to D. Let $\tilde{j}$ be the j-invariant of the canonical lift of a pair (E, f) of $\mathrm{Emb}_D(\mathbb{F}_{p^2})$. There are infinitely many equations of curves $\tilde{E}$ over F reducing to E with j-invariant $\tilde{j}$ and each has complex multiplication by $\mathcal{O}$. Let $\tilde{E}_1$, $\tilde{E}_2$ be two such curves and suppose that the induced embedding $\mathrm{End}(\tilde{E}_1) \hookrightarrow \mathrm{End}(E)$ is f. If h is an isomorphism between E_1 and E_2, then

$$\mathrm{End}(\tilde{E}_2) = \{h\gamma h^{-1} | \gamma \in \mathrm{End}(\tilde{E}_1)\}.$$

As $D < -4$, this isomorphism is unique up to ± 1. The isomorphism h reduces to an automorphism $\bar{h}$ of E and the embedding $\mathrm{End}(\tilde{E}_2) \hookrightarrow \mathrm{End}(E)$ is given by $\bar{h}f(\gamma)\bar{h}^{-1}$ for all $\gamma \in \mathrm{End}(\tilde{E}_1)$. We use $\bar{h}f\bar{h}^{-1}$ to denote this embedding. We have the following commutative diagram:

$$\begin{tikzcd}
\tilde{E}_1 \arrow[r, "h"] \arrow[d] & \tilde{E}_2 \arrow[d] \\
(E, f) \arrow[r, "\bar{h}"] & (E, \bar{h}f\bar{h}^{-1})
\end{tikzcd}$$

If $j(E) \neq 0, 1728$, the automorphism is $\pm\mathrm{Id}$ and $\bar{h}f\bar{h}^{-1} = f$. Thus the embedding $\mathrm{End}(\tilde{E}_2) \hookrightarrow \mathrm{End}(E)$ is also equal to f. In this case, the j-invariant $\tilde{j}$ is sufficient to determine a curve $\tilde{E}$ reducing to E for which the induced embedding is f.

For $j(E) = 0$ or 1728, however, this is not the case. The map $\bar{h}$ may be a non-trivial automorphism of E in which case $\bar{h}f\bar{h}^{-1}$ and f are *not* the same embeddings. This follows from that fact that $\bar{h}$ corresponds to ζ, a primitive sixth, respectively fourth, root of unity in R, the maximal order of $\mathcal{A}_{p,\infty}$ isomorphic to $\mathrm{End}(E)$. Let i be the isomorphism $R \to \mathrm{End}(E)$ and let g denote the embedding $i^{-1} \circ f : \mathcal{O} \hookrightarrow R$. As $D < -4$, the value ζ is not contained in the commutative subfield $g(\mathbb{Q}(\sqrt{D}))$ of R and thus does not commute with $g(\tau)$. Therefore $\bar{h}$ does not commute with the endomorphism $f(\tau)$ and the embeddings are distinct.

For example, let $p \neq 3$ and consider $E/\mathbb{F}_{p^2}$ given by $y^2 = x^3 + x$ with $j(E) = 1728$. Let $\tilde{E}_1$ be the curve given by $y^2 = x^3 + x + B$ where $B \in F$ is such that $j(\tilde{E}_1) = \tilde{j}$, the j-invariant of the canonical lift of (E, f). Let $\tilde{E}_2$ be the curve given by $y^2 = x^3 + x - B$. The isomorphism between them reduces to the non-trivial automorphism $(x, y) \mapsto (-x, iy)$ of E, where i is an element of $\mathbb{F}_{p^2}$ such that $i^2 = -1$. Though both $\tilde{E}_1$ and $\tilde{E}_2$ have j-invariant $\tilde{j}$, exactly one of the curves yields an embedding of endomorphism rings which is equal to f and thus may be properly considered the canonical lift of (E, f).

Therefore, for $j(E) = 0, 1728$, the j-invariant $\tilde{j}$ is not sufficient to determine a curve $\tilde{E}$ reducing to E for which the induced embedding is f. This poses a problem in Step 6 of Algorithm 2.4.1. In the k^{th} iteration, given j_k, we choose a curve E_k with j-invariant j_k which reduces to E. Recall that j_k is the 2^k p-adic digit approximation to $\tilde{j}$. The key assumption is that the curve E_k is a 2^k digit approximation to a curve $\tilde{E}$ for which the induced embedding is f. Therefore, when we lift the kernel of $E[f(\alpha)]$ to a subgroup of E_k and compute the resulting isogeny $E_k \to E_k^{(\alpha)}$, the isogeny is in fact an endomorphism of E_k up to 2^k digits accuracy, and the j-invariant of $E_k^{(\alpha)}$ is in fact the value $\rho_\alpha(j_k)$. Thus when using Newton's method to compute j_{k+1}, we obtain the 2^{k+1} digit approximation to $\tilde{j}$.

If we choose a curve E_k which is *not* an approximation to a curve $\tilde{E}$ for which the induced embedding is f, then the j-invariant of $E_k^{(\alpha)}$ is not necessarily equal to the value $\rho_\alpha(j_k)$. Thus in the case of $j(E) = 0, 1728$, the ambiguity of choice of E_k in Step 6a may lead to incorrect computations. In fact, this ambiguity occurs at any place within the lift of the cycle of isogenies where the curve over $\mathbb{F}_{p^2}$ has j-invariant 0 or 1728.

For this reason, we work with the *Legendre model* of a curve E which takes into consideration the presence of non-trivial automorphisms. These curves are only defined over fields with characteristic not equal to two. Therefore for the remainder of the chapter, we assume $p \neq 2$. For a discussion of the case of $p = 2$, see [33].

2.5.2 The Legendre form of an elliptic curve

Let F be any field of characteristic not equal to two. For $\lambda \in F$, with $\lambda \neq 0, 1$, the curve

$$L_\lambda : y^2 = x(x-1)(x-\lambda)$$

is an elliptic curve in *Legendre form.* A straightforward computation yields that the j-invariant of L_λ is

$$j(L_\lambda) = 2^8 \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda - 1)^2}. \tag{2.8}$$

The two-torsion of L_λ is $L[2] = \{(0,0), (1,0), (\lambda, 0), P_\infty\}$ where P_∞ is the identity of the group $L(\bar{F})$. The following proposition characterizes all curves in Legendre form which are isomorphic to a given curve E. We give the proof here, based on the proof in [38, Sec. III.1], as we refer to it in later arguments.

Proposition 2.5.1 *[38, Prop. III.1.7] Let E be defined over F, with char $F \neq 2$. Then*

1. *E is isomorphic to a curve in Legendre form defined over an extension of F of degree at most six. The isomorphism is defined over an extension of F of degree at most twelve.*

2. *If $j(E) \neq 0, 1728$, there are six distinct values of λ such that $j(L_\lambda) = j(E)$.*

3. *If $j(E) = 0, 1728$ and char $F \neq 3$, there are two, respectively three, distinct values of λ such that $j(L_\lambda) = j(E)$. If char $F = 3$ and $j(E) = 0 = 1728 \bmod 3$, there is only one value λ such that $j(L_\lambda) = j(E)$.*

Proof: Given a curve E with Weierstrass equation $y^2 = f(x)$ over F, let e_1, e_2, e_3 denote the roots of $f(x)$, a degree-3 polynomial. These are the x-coordinates of the 2-torsion of E and they lie in an extension of F of degree at most six. Therefore we can write E as

$$y^2 = (x - e_1)(x - e_2)(x - e_3).$$

The change of coordinates $(x, y) \mapsto (u^2 x + r, u^3 y)$ with $u = \frac{1}{\sqrt{e_2 - e_1}}$ and $r = \frac{-e_1}{e_2 - e_1}$ defines an isomorphism of E to the curve $L : y^2 = x(x-1)(x-\lambda)$ with $\lambda = \frac{e_3 - e_1}{e_2 - e_1}$. The value λ, called the *λ-invariant* of the curve, lies in an extension of F of degree at most six and the isomorphism $E \to L$ is defined over an extension of degree at most twelve. Under this isomorphism, the ordered sequence $\big[(e_1, 0), (e_2, 0), (e_3, 0)\big]$ of non-trivial 2-torsion is sent to $\big[(0, 0), (1, 0), (\lambda, 0)\big]$. Any matrix $M \in \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ acts on the basis $\big((e_1, 0), (e_2, 0)\big)$ of $E[2]$ and gives a permutation $e_1, e_2, e_3 \mapsto e_1', e_2', e_3'$ of the

x-coordinates of the two torsion of E. This defines the curve $L_\mu : y^2 = x(x-1)(x-\mu)$ isomorphic to E with λ-invariant equal to $\mu = \frac{e_3'-e_1'}{e_2'-e_1'}$.

The following chart describes all possible isomorphisms of L_λ to another curve L_μ in Legendre form isomorphic to E. It also gives the corresponding permutation of the x-coordinates of the two-torsion and the matrix $M \in \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ such that μ is the λ-invariant of the curve obtained by the action of M on the basis $\big((e_1, 0), (e_2, 0),\big)$ of $E[2]$. These can be determined from straightforward computations (see also [21, p. 455])

μ	$x \mapsto x'$	0	1	λ	M
λ	x	0	1	μ	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
$\frac{1}{\lambda}$	$\lambda^{-1}x$	0	μ	1	$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$
$1-\lambda$	$-x+1$	1	0	μ	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
$\frac{1}{1-\lambda}$	$\frac{1-x}{1-\lambda}$	μ	0	1	$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$
$\frac{\lambda}{\lambda-1}$	$\frac{\lambda-x}{\lambda-1}$	μ	1	0	$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$
$\frac{\lambda-1}{\lambda}$	$-\lambda^{-1}x+1$	1	μ	0	$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$

Therefore, each μ in the set $S = \{\lambda, \frac{1}{\lambda}, 1-\lambda, \frac{1}{1-\lambda}, \frac{\lambda}{\lambda-1}, \frac{\lambda-1}{\lambda}\}$ defines a curve in Legendre form isomorphic to E defined over an extension of F at most degree 6.

Equating the elements in S, we see that the six values are distinct, with the exception of three cases. If char $F \neq 3$ and $\lambda = -\zeta_3, -\zeta_3^2$, for ζ_3 a primitive third root of unity, there are only two distinct values. If char $F \neq 3$ and $\lambda = -1, 2, \frac{1}{2}$, there are three distinct values. If char $F = 3$ and $\lambda = -1$, then all six values are identical. Using (2.8), we see that the first case corresponds to $j(E) = 0$, the second to $j(E) = 1728$, and the third to $j(E) = 0 = 1728 \bmod 3$. □

Consider an isogeny $\varphi : L_\lambda \to L_\mu$ of two curves in Legendre form, where L_λ and L_μ are not necessarily isomorphic. We say that φ *fixes the two-torsion* if φ sends the ordered sequence $\big[(0,0),(1,0),(\lambda,0)\big]$ to $\big[(0,0),(1,0),(\mu,0)\big]$.

Given $j \in F$, the roots of the polynomial $P_j(X) = 2^8(X^2-X+1)^3 - j \cdot X^2(X-1)^2$ are precisely the elements of

$$S = \{\lambda, \frac{1}{\lambda}, 1-\lambda, \frac{1}{1-\lambda}, \frac{\lambda}{\lambda-1}, \frac{\lambda-1}{\lambda}\}.$$

Note that $F(\mu) = F(\lambda)$ for any $\mu \in S$, since μ is a rational expression in λ. The minimal polynomial of $F(\lambda)$ over F is a factor of $P_j(X)$ of degree one, two, three or six. This follows from the natural action of $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ on the set S of roots of $P_j(X)$, as described in the proof above. Thus if $P_j(X)$ is irreducible, we have that $\mathrm{Gal}(F(\lambda)/F(j))$ is $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \simeq S_3$. The matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ corresponds to the automorphism $\sigma : \lambda \mapsto \frac{1}{\lambda}$ and $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ corresponds to $\tau : \lambda \mapsto \frac{1}{1-\lambda}$ and they do not commute.Therefore, if $F(\lambda)$ is a cyclic extension of $F(j)$ (in particular, if it is a finite field extension or unramified p-adic extension), the polynomial $P_j(X)$ is reducible and the degree of the extension can be at most 3.

2.5.3 The canonical lift of (L, f)

Let $D < -4$, and let p be a prime inert in $K = \mathbb{Q}(\sqrt{D})$ with $p \nmid 2D$. Let $\mathcal{O}$ be the order of K of discriminant D. In this section, we discuss the relationship between curves in Legendre form defined over $\overline{\mathbb{Q}}_p$ with complex multiplication by $\mathcal{O}$ and their reductions modulo $\mathfrak{p}$, a prime above p.

Let F denote the degree two unramified extension of $\mathbb{Q}_p$ and let $\mathrm{Leg}_D(F)$ be the set of normalized elliptic curves L in Legendre form defined over F with endomorphism ring isomorphic to $\mathcal{O}$. Recall from Section 2.3.2 that a "normalized" elliptic curve L is one for which we have chosen the isomorphism $\gamma : \mathcal{O} \xrightarrow{\sim} \mathrm{End}(L)$ such that for any $y \in \mathcal{O}$ and invariant differential ω of L, we have $\omega \circ \gamma(y) = y\omega$, where y is viewed as an element of F under the embedding $H_{\mathcal{O}} \hookrightarrow F$. As in Section 2.3.2, reduction modulo p yields a curve L_p and normalized optimal embedding f. Let $\mathrm{LegEmb}_D(\mathbb{F}_{p^2})$ be the set of pairs (L, f) where L is a supersingular elliptic curve in Legendre form over $\mathbb{F}_{p^2}$ and f is a normalized optimal embedding $f : \mathcal{O}_D \hookrightarrow \mathrm{End}(L)$.

Note that elements of the set $\mathrm{Leg}_D(F)$ represent specific curves, *not* an equivalence class of curves. Similarly, the pair (L, f) in $\mathrm{LegEmb}_D(\mathbb{F}_{p^2})$ represents a specific curve L and a specific embedding f. In contrast to $\mathrm{Emb}_D(\mathbb{F}_{p^2})$, where (L, f) and (L, f') are identified if $f' = h \circ f \circ h^{-1}$ for an automorphism h of L, these are distinct elements of the set $\mathrm{LegEmb}_D(\mathbb{F}_{p^2})$.

Theorem 2.5.2 *Let F denote the degree two unramified extension of $\mathbb{Q}_p$. Let $D < -4$*

and let p be a prime inert in $K = \mathbb{Q}(\sqrt{D})$ with p not dividing $2D$. Let π be the map

$$\begin{array}{rccc} \pi: & \mathrm{Leg}_D(F) & \to & \mathrm{LegEmb}_D(\mathbb{F}_{p^2}) \\ & L & \mapsto & (L_p, f) \end{array}$$

defined by sending a curve L to the pair (L_p, f) where L_p is the reduction of L modulo p and f is the induced embedding of endomorphism rings. Then π is a well-defined bijection.

Proof: Given $L \in \mathrm{Leg}_D(F)$, the reduction map $\mathbb{Z}_F \mapsto \mathbb{F}_{p^2}$ induces a normalized optimal embedding $f : \mathcal{O}_D \to \mathrm{End}(L_p)$, and hence the map is well-defined. By Theorem 2.3.5 we can lift an element (L_p, f) in $\mathrm{Emb}_D(\mathbb{F}_{p^2})$ to a normalized curve $\tilde{E}$ with complex multiplication by $\mathcal{O}$ which reduces to $L : y^2 = x(x-1)(x-\lambda)$ and whose induced embedding is f. As $\tilde{E}$ reduces to L, it must be of the form $y^2 = (x-e_1)(x-e_2)(x-e_3)$ with $e_1, e_2, e_3 \equiv 0, 1, \lambda \bmod p$ respectively. The change of coordinates $(x, y) \mapsto (u^2x + r, u^3y)$ with $u = \frac{1}{\sqrt{e_2 - e_1}}$ and $r = \frac{-e_1}{e_2 - e_1}$ gives an isomorphism from $\tilde{E}$ to the curve $\tilde{L}$ with $\tilde{\lambda} = \frac{e_3 - e_1}{e_2 - e_1} \equiv \lambda \bmod p$. This isomorphism is the identity modulo p, therefore the embedding f is unchanged, and $\tilde{L} \in \mathrm{Leg}_D(F)$ reduces via π to (L, f). Therefore the map is surjective.

It remains to show that the two sets have the same cardinality. We first consider $\mathrm{Leg}_D(F)$. The number of $\bar{F}$-isomorphism classes of curves defined over F with complex multiplication by $\mathcal{O}$ is $h(\mathcal{O})$, the class number of $\mathcal{O}$. Since $D < -4$, the j-invariant of any class is not 0 or 1728 and thus yields six distinct curves in Legendre form. We show in Section 2.7 that all curves in Legendre form isomorphic to a curve E in $\mathrm{Ell}_D(F)$ are defined over F. Thus the cardinality of $\mathrm{Leg}_D(F)$ is $6h(\mathcal{O})$.

Now consider $\mathrm{LegEmb}_D(\mathbb{F}_{p^2})$. As shown in Section 2.3.2, the sets $\mathrm{Emb}_D(\mathbb{F}_{p^2})$ and $\mathrm{Emb}_D(\mathcal{A}_{p,\infty})$ are in bijection. Thus by Proposition 2.3.2, the cardinality of $\mathrm{Emb}_D(\mathbb{F}_{p^2})$ is $h(\mathcal{O})$, the class number of $\mathcal{O}$.

For $j(E) \neq 0, 1728$, there are six distinct curves in Legendre form with j-invariant $j(E)$. Thus each embedding $f : \mathcal{O}_D \hookrightarrow \mathrm{End}(E)$ yields six distinct elements of the set $\mathrm{LegEmb}_D(\mathbb{F}_{p^2})$.

For $j(E) = 0$ and $p \neq 3$, there are two distinct curves in Legendre form. For each curve L, the three automorphisms of L (up to ± 1) yield three distinct isomorphisms from E to L (up to ± 1). Thus for each embedding $f : \mathcal{O}_D \hookrightarrow \mathrm{End}(E)$, there are six distinct elements of $\mathrm{LegEmb}_D(\mathbb{F}_{p^2})$. Similarly, for $j(E) = 1728$ and $p \neq 3$, given an embedding $f : \mathcal{O}_D \hookrightarrow \mathrm{End}(E)$, each of the three curves in Legendre form with j-invariant 1728 has two distinct embeddings. This gives six distinct elements of $\mathrm{LegEmb}_D(\mathbb{F}_{p^2})$. Finally if $p = 3$ and $j(E) = 0 = 1728$, the curve with $\lambda = -1$ has six automorphisms (up to ± 1). Thus for each embedding $f : \mathcal{O}_D \hookrightarrow \mathrm{End}(E)$, there are six distinct elements of $\mathrm{LegEmb}_D(\mathbb{F}_{p^2})$.

As there are $h(\mathcal{O})$ pairs (E, f) where E is an elliptic curve and f is a normalized embedding, the cardinality of $\mathrm{LegEmb}_D(\mathbb{F}_{p^2})$ is $6h(\mathcal{O})$. □

Definition 2.5.3 *The canonical lift $\tilde{L}$ of a pair $(L, f) \in \mathrm{LegEmb}_D(\mathbb{F}_{p^2})$ is the inverse $\pi^{-1}(L, f)$ in $\mathrm{Leg}_D(F)$.*

2.6 The modular function λ of level 2

2.6.1 Brief Introduction to Modular Curves

In this section, we give some facts from the theory of modular curves which will be used in the following sections. Unless otherwise stated, the reference for this material is [15]. Let $\mathcal{H}$ denote the complex upper-half plane. The *prinicipal congruence subgroup of level* N, denoted $\Gamma(N)$, is the subgroup of $SL_2(\mathbb{Z})$ consisting of matrices M such that $M \equiv \mathrm{Id} \bmod N$. More generally, any subgroup Γ of $SL_2(\mathbb{Z})$ containing $\Gamma(N)$ for some N is called a *congruence subgroup of level* N. The *modular curve* $Y(\Gamma)_{\mathbb{C}}$ is defined as $\Gamma\backslash\mathcal{H}$, and $X(\Gamma)$ denotes its compactification as a Riemann surface. A priori, the elements of the "curve" are just cosets. The fact that $X(\Gamma)$ has the structure of an *algebraic curve* comes from a correspondence between non-singular projective curves over $\mathbb{C}$ and transcendental extensions of degree one of $\mathbb{C}$.

For any N, the modular curves $X(N)$ can be described by irreducible non-singular projective models with coefficients in $\mathbb{Z}[\zeta_N]$, where ζ_N is an N^{th} root of unity [22, 32]. Therefore, we may consider $X(N)$ to be defined over an extension of $\mathbb{Q}$ or any field of characteristic p prime to N. In particular, we are interested in $k = \mathbb{Q}_p$ or $\mathbb{F}_p$. We write $X(N)_k$ to indicate that we are working with the modular curve defined over k. For any extension F of k, let $X(N)_k(F)$ denote the F-rational points of $X(N)_k$, and let $Y(N)_k(F)$ denote the F-rational points which are not cusps. We work with both $Y(N)$ and $X(N)$ in what follows.

The points of the affine curve $Y(\Gamma)_{\mathbb{C}}$ correspond to a *moduli space* consisting of equivalence classes of elliptic curves with particular torsion data. Points of $Y(1)$ correspond simply to isomorphism classes $[E]$ of elliptic curves over $\mathbb{C}$. Points of $Y(N)$ correspond to equivalence classes $[E,(P,Q)]$ where E is a curve over $\mathbb{C}$ and (P,Q) is an ordered basis of $E[N]$ such that $e_N(P,Q)=e^{2\pi i/N}$, where e_N is the *Weil pairing* on N-torsion. Two pairs $[E,(P,Q)]$ and $[E',(P',Q')]$ are equivalent if there is an isomorphism $h: E \to E'$ such that $h(P)=P'$ and $h(Q)=Q'$.

In particular, points of $Y(2)$ correspond to equivalence classes $[E,(P,Q)]$ where E is a curve over $\mathbb{C}$ and (P,Q) is an ordered basis of $E[2]$. The Weil-pairing condition is superfluous, as there is a single non-trivial square root of unity. In the next section, we will see that a point $[E,(P,Q)]$ of $Y(2)_{\mathbb{C}}$ corresponds uniquely to a curve in Legendre form over $\mathbb{C}$ isomorphic to E.

For the fields $k=\mathbb{Q},\mathbb{Q}_p$ and $\mathbb{F}_p$, we also have a moduli interpretation of $Y(N)_k$ (with some technical modifications, see [15]). For example, if F is the unramified degree 2 extension of $\mathbb{Q}_p$, the points of $Y(2)_{\mathbb{Q}_p}(F)$ correspond to $\bar{F}$-isomorphism classes $[E,(P,Q)]$ where E is a curve over F and (P,Q) is an ordered basis of $E[2]$ defined over F.

Let $\mathbf{k}$ be an algebraically closed field. The *field of modular functions of* $X(N)_{\mathbf{k}}$, denoted $\mathbf{k}(X(N))$, is the field of rational functions $f: X(N) \to \mathbb{P}^1(\mathbf{k})$. For $\mathbf{k}=\mathbb{C}$, these are functions on the upper half plane which are invariant under $\gamma \in \Gamma(N)$. This field can be described in a purely algebraic way as follows. Assume char $\mathbf{k} \neq 2,3$. Let j be transcendental over $\mathbf{k}$ and let E_j denote the "universal elliptic curve"

$$y^2 = 4x^3 - \frac{27j}{j-1728}x - \frac{27j}{j-1728}.$$

For $j_o \in \mathbf{k}$ with $j_o \neq 0, 1728$, this specializes to an elliptic curve over $\mathbf{k}$ with j-invariant

j_o. Let $x(E_j[N])$ denote the x-coordinates of the N-torsion of this curve. Since the N^{th}-division polynomial has coefficients in $\mathbf{k}(j)$, these are algebraic over $\mathbf{k}(j)$. The field of functions of $X(N)_{\mathbf{k}}$ is $\mathbf{k}(j, x(E_j[N]))$.

We now describe a function λ on $X(2)$ which generates the field of modular functions of $X(2)_{\mathbf{k}}$.

2.6.2 The modular function λ of level 2

In this section, we introduce a function $\lambda : \mathcal{H} \to \mathbb{C}$ which parameterizes the modular curve $Y(2)_{\mathbb{C}}$, assigning to each point $[E,(P,Q)]$ a distinct curve in Legendre form isomorphic to E. Given $E/\mathbb{C}$, choose $\tau \in \mathcal{H}$ such that E is isomorphic to $\mathbb{C}/\Lambda_\tau$ where Λ_τ is the lattice $\mathbb{Z} + \tau\mathbb{Z}$. Let $\wp_\tau(z)$ denote the Weierstrass $\wp$-function associated to Λ_τ. The points of order two of the Riemann surface $\mathbb{C}/\Lambda_\tau$ are $\{\frac{\tau}{2}, \frac{1}{2}, \frac{1+\tau}{2}\}$. Let

$$e_1(\tau) = \wp_\tau(\frac{\tau}{2}), \quad e_2(\tau) = \wp_\tau(\frac{1}{2}), \text{ and } e_3(\tau) = \wp_\tau(\frac{1+\tau}{2}).$$

These are precisely the x-coordinates of the non-trivial two-torsion of E. Define $\lambda : \mathcal{H} \to \mathbb{C}$ as

$$\lambda(\tau) = \frac{e_3(\tau) - e_1(\tau)}{e_2(\tau) - e_1(\tau)}.$$

The following proposition describes the key properties of λ.

Proposition 2.6.1 *[1, Section 7.3.4]*

1. *$\lambda(\tau)$ is analytic on $\mathcal{H}$.*

2. *$\lambda(\tau)$ is $\Gamma(2)$-invariant: $\lambda(\gamma(\tau)) = \lambda(\tau)$ for all $\gamma \in \Gamma(2)$.*

3. λ satisfies the following transformation identities:

$$\lambda(\tau+1) = \frac{\lambda(\tau)}{\lambda(\tau)-1} \text{ and } \lambda(\frac{-1}{\tau}) = 1-\lambda(\tau).$$

At the *cusps* $0, 1, \infty$ of $Y(2)$, the function λ takes the value $1, \infty, 0$ respectively. Furthermore, it can be shown that $\lambda : Y(2) \to \mathbb{C} - \{0, 1\}$ is a one-to-one map [1, Thm 7.7]. Thus $\mathbb{C} - \{0, 1\}$ is a parameter space for the curve $Y(2)$.

Defining $\lambda(0) = 1, \lambda(1) = \infty, \lambda(\infty) = 0$, and using the fact that λ is $\Gamma(2)$-invariant and holomorphic on $\mathcal{H}$, we have that $\lambda : X(2) \to \mathbb{P}^1(\mathbb{C}) = \mathbb{C} \cup \infty$ is *modular function for* $\Gamma(2)$. Thus $X(2)_{\mathbb{C}}(\mathbb{C})$ is in bijection with $\mathbb{P}^1(\mathbb{C})$ via the map λ and the field of functions of $X(2)$ is $\mathbb{C}(\lambda)$.

Let $\mathbf{k}$ be an algebraically closed field not of characteristic two. We define $\lambda : X(2)_{\mathbf{k}} \mapsto \mathbb{P}^1(\mathbf{k})$ analogously to the complex-analytic case. On $Y(2)$, define

$$\lambda([E, (P, Q)]) = \frac{x(P+Q) - x(P)}{x(Q) - x(P)}. \tag{2.9}$$

At the cusps, let $\lambda(0) = 1, \lambda(1) = \infty$ and $\lambda(\infty) = 0$. For L, a curve in Legendre form, we define

$$\lambda(L) := \lambda([L, ((0, 0), (1, 0))]),$$

by abuse of notation. Note the curve L in Legendre form with λ-invariant $\lambda([E, (P, Q)]))$ is isomorphic to E via the change of coordinates in the proof of Proposition 2.5.1, and the ordered basis (P, Q) of $E[2]$ is mapped to the basis $((0, 0), (1, 0))$ of $L[2]$. The fact that λ is well-defined and injective follows from considering the chart in the proof of Proposition 2.5.1.

The map is clearly surjective, since given $\lambda_o \in \mathbf{k}$ with $\lambda_o \neq 0, 1$, the curve $L : y^2 = x(x-1)(x-\lambda_o)$ is mapped via λ to λ_o. Therefore the map $\lambda : X(2)_{\mathbf{k}} \mapsto \mathbb{P}^1(\mathbf{k})$

establishes a bijection with $\mathbb{P}^1(\mathbf{k})$, and the field of functions of $X(2)_{\mathbf{k}}$ is $\mathbf{k}(\lambda)$.

This agrees with definition of the field of modular functions of $X(2)$ as $\mathbf{k}(j, x(E_j[2]))$, where $j : X(1)_{\mathbf{k}}(\mathbf{k}) \to \mathbb{P}^1(\mathbf{k})$ is the (algebraic) j-invariant function for $X(1)$. To see this, we revisit the relationship between the functions λ and j on $X(2)_{\mathbf{k}}$. This is described in [21, p. 461], and we give a more detailed proof here.

Proposition 2.6.2 *Let* $\mathbf{k}$ *be an algebraically closed field, not of characteristic two. Let* j *be transcendental over* $\mathbf{k}$*. Let* λ *be a root of the polynomial* $P_j(X) = 2^8(X^2 - X + 1)^3 - jX^2(X-1)^2$.

1. $\mathbf{k}(j, x(E_j[2])) = \mathbf{k}(\lambda)$.

2. *The map* $J : X(2)_{\mathbf{k}} \mapsto X(1)_{\mathbf{k}}$ *given by*

$$J(\lambda) = 2^8 \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda - 1)^2}$$

is of degree six. For char $\mathbf{k} \neq 3$*, the cover is ramified at* $j = 0, 1728$ *and* ∞ *of degree 3, 2, and 2 respectively. For char* $\mathbf{k} = 3$*, the cover is ramified at* $j = 0$ *and* ∞ *of degree 6 and 2 respectively.*

Proof: Consider the extension of function fields, $\mathbf{k}(\lambda)/\mathbf{k}(j)$. We first show the polynomial $P_j(X)$ is irreducible over $\mathbf{k}(j)$. As there is a single power of j in $P_j(X)$, if $P_j(X)$ factors into two polynomials, we must have that $P_j(X) = A(X)(B(X)+jC(X))$, where A, B, and C are polynomials in $\mathbf{k}[X]$. Thus $A(X)$ must divide both $2^8(X^2-X+1)^3$ and $X^2(X-1)^2$ which implies that $A(X)$ is ± 1 and therefore $P_j(X)$ is irreducible. As each root of $P_j(X)$ is a rational expression in λ, the extension $\mathbf{k}(\lambda)/\mathbf{k}(j)$ is therefore a degree six Galois extension. As discussed in Section 2.5, the Galois group of $\mathbf{k}(\lambda)/\mathbf{k}(j)$

is isomorphic to $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ and generated by the automorphisms $\sigma : \lambda \mapsto \frac{1}{\lambda}$ and $\tau : \lambda \mapsto \frac{1}{1-\lambda}$ of order 2, 3 respectively.

By the same argument as in Section 2.5, the Galois group of $\mathbf{k}(j, x(E_j[2]))/\mathbf{k}(j)$ is isomorphic to $GL_2(\mathbb{Z}/2\mathbb{Z})$ (see also [21, Thm. 4]). Thus it suffices to show λ is in $\mathbf{k}(j, x(E_j[2]))$. The change of coordinates from Proposition 2.5.1 takes E_j to $L : y^2 = x(x-1)(x-\lambda)$ with $\lambda = \frac{e_3-e_2}{e_1-e_2}$, where e_i are some permutation of the x-coordinates of $E_j[2]$. Thus λ is a rational expression in $x(E_j[2])$ and $\lambda \in \mathbf{k}(j, x(E_j[2]))$.

As the discriminant of $P_j(X) \in \mathbf{k}[j][X]$ is $j^4(j-1728)^3$, the only finite points of ramification occur at $j = 0, 1728$. Fix $j_o \in \mathbf{k}$ and let $\mathfrak{p} = (t)$, where $t = (j - j_0) \in \mathbf{k}(j)$ is a uniformizer for j_o. Consider the local field $\mathbf{k}((t))$, with ring of integers $\mathbf{k}[[t]]$. Let $\lambda_o \in \mathbf{k}$ be such that $j(\lambda_o) = j_o$, and let $\mathfrak{P} = (s)$, where $s = \lambda - \lambda_o$ is a uniformizer for λ_o. Since the extension $\mathbf{k}(\lambda)/\mathbf{k}(j)$ is Galois, the ramification degree of the local field extension at j_o is independent of the choice of λ_o. Since $\mathbf{k}((s))$ is a local field extension of $\mathbf{k}((t))$ and both have residue fields $\mathbf{k}$, the ramification degree of $\mathfrak{P}$ is simply the degree of the extension, which is the order of the subgroup of S_3 fixing $\mathfrak{P}$.

Let $j_o = \infty$. The values $0, 1, \infty$ are pre-images of j_o under the map λ. In particular, we see that $\lambda_o = 1$ is only fixed by the subgroup generated by $\sigma : \lambda \mapsto \frac{1}{\lambda}$. Therefore, the ramification degree at $j = \infty$ is 2. Assume char $\mathbf{k} \neq 3$. Let $j_o = 0$ and $\lambda_o = -\zeta_3$. Then $\mathfrak{P} = (\lambda - \lambda_o)$ is fixed only by the subgroup generated by $\tau : \lambda \mapsto \frac{1}{1-\lambda}$.Therefore, the ramification degree at $j = 0$ is 3. Let $j_o = 1728$ and $\lambda_o = -1$. Then $\mathfrak{P} = (\lambda - \lambda_o)$ is fixed only by the subgroup generated by $\sigma : \lambda \mapsto \frac{1}{\lambda}$. Therefore, the ramification degree at $j = 1728$ is 2.

For char $\mathbf{k} = 3$, the only ramification at finite places occurs at $j_o = 0 = 1728$ and $\lambda_o = -1$. The ideal $\mathfrak{P} = (\lambda - \lambda_o)$ is fixed by both τ and σ and therefore the ramifiication degree at $j = 0$ is 6. □

2.7 An action of $Cl(\mathcal{O}_2)$ on $\mathrm{Leg}_D(F)$

Let $\mathcal{O}$ be an order of discriminant $D < -4$ and let $K = \mathbb{Q}(\sqrt{D})$. Let E be a curve with complex multiplication by $\mathcal{O}$. In this section, we describe the minimal extension of K over which the curves in Legendre form isomorphic to E can be defined. In particular, we show that the λ-invariant of a curve in Legendre form with complex multiplication by $\mathcal{O}_K$, the ring of integers of a quadratic imaginary field, generates the *ray class field of* K *of conductor 2*. This is a known result, analogous to the fact that the j-invariant of an elliptic curve with complex multiplication by $\mathcal{O}_K$ generates the *Hilbert class field* H of K. The reference for the class field theory used in this section is [11, Chap. 8].

We also show that all curves in Legendre form with complex multiplication by $\mathcal{O}$ can be defined over F, the degree two unramified extension of $\mathbb{Q}_p$, and define an action of a generalized ideal class group of $\mathcal{O}_K$ on the set $\mathrm{Leg}_D(F)$. This action extends to an action on $\mathrm{LegEmb}_D(\mathbb{F}_{p^2})$ and gives a way to compute the canonical lift of (L, f), as will be described in the next section.

We begin by defining some notation. For $m \in \mathbb{Z}^+$, let $I_m(\mathcal{O}_K)$ denote the set of proper fractional ideals of $\mathcal{O}_K$ relatively prime to $m\mathcal{O}_K$. Let $P_{m,\mathbb{Z}}(\mathcal{O}_K)$ denote the subset of principal ideals (α) such that $\alpha \equiv a \bmod m\mathcal{O}_K$ for some integer a relatively prime to m. Let $P_{m,1}(\mathcal{O}_K)$ denote the subset of principal ideals (α) such that $\alpha \equiv 1 \bmod m\mathcal{O}_K$.

By class field theory, given a fixed algebraic closure of K, there is a unique abelian extension $R_{m,K}$ of K, such that $\mathrm{Gal}(R_{m,K}/K) \simeq I_m(\mathcal{O}_K)/P_{m,1}(\mathcal{O}_K)$ via the *Artin map*. This is called the *ray class field of K of conductor m*.

Let $\mathcal{O}$ be an order of conductor m. The *ring class field of K of conductor m*, denoted $H_{\mathcal{O}}$, is the unique abelian extension of K such that $\mathrm{Gal}(H_{\mathcal{O}}/K) \simeq I_m(\mathcal{O}_K)/P_{m,\mathbb{Z}}(\mathcal{O}_K)$ via the Artin map. The group $I_m(\mathcal{O}_K)/P_{m,\mathbb{Z}}(\mathcal{O}_K)$ is isomorphic to the class group $Cl(\mathcal{O})$ via $\mathfrak{a}_K \mapsto \mathfrak{a}_K \cap \mathcal{O}$. Recall that the class group is the quotient of the group of ideals of $\mathcal{O}$ prime to m by the group of principal ideals of $\mathcal{O}$ prime to m. As $P_{m,1}(\mathcal{O}_K) \subset P_{m,\mathbb{Z}}(\mathcal{O}_K)$, we have that $R_{m,K}$ is an extension of $H_{\mathcal{O}}$.

Let E be a curve in characteristic zero with complex multiplication by $\mathcal{O}$. As shown in Section 2.5, the set of λ-invariants of curves in Legendre form isomorphic to E depends only on the j-invariant of E. Therefore, to determine the λ-invariants associated to $j(E)$, we may work with the "universal curve" E_j defined in Section 2.6.1. The λ-invariant of any curve L in Legendre form isomorphic to E_j is rational expression in the x-coordinates of the two torsion of E_j. Thus λ is an element of the field $K(j(E), x(E_j[2]))$. By the results in [3, 40], the Galois group $\mathrm{Gal}(K(j(E), x(E_j[2]))/K)$ is isomorphic via the Artin map to the quotient of $I_{2m}(\mathcal{O}_K)$ by $P_{2,1}(\mathcal{O})$, the set of principal ideals $\alpha\mathcal{O}_K$ where $\alpha \in \mathcal{O}$ such that $\alpha \equiv 1 \bmod 2\mathcal{O}$ and $\alpha\mathcal{O}_K$ is relatively prime to m, the conductor of $\mathcal{O}$.

We now show that the group $P_{2,1}(\mathcal{O})$ is equal to $P_{2m,\mathbb{Z}}(\mathcal{O}_K)$ and therefore that the ring class field of K of conductor $2m$ is precisely the field $K(j(E), x(E_j[2]))$. Let w be a generator of $\mathcal{O}_K$. If (β) is an ideal of $P_{2m,\mathbb{Z}}(\mathcal{O}_K)$, then $\beta = a + 2mbw$ for some integer a relatively prime to $2m$. Since $\mathcal{O} = \mathbb{Z} + m\mathcal{O}_K$, this implies that $\beta \in \mathcal{O}$ and $\beta \equiv 1 \bmod 2\mathcal{O}$. Furthermore, (β) is relatively prime to m and thus $(\beta) \in P_{2,1}(\mathcal{O})$. For the other containment, let (β) be an ideal of $P_{2,1}(\mathcal{O})$. Since $\beta \equiv 1 \bmod 2\mathcal{O}$, we have $\beta = a + bmw$ with a odd and b even. Therefore $\beta \equiv a \bmod 2m\mathcal{O}_K$. The assumption that (β) is relatively prime to m implies that $(a, m) = 1$ and thus $(\beta) \in P_{2m,\mathbb{Z}}(\mathcal{O}_K)$.

Therefore the ring class field of K of conductor $2m$ is the field $K(j(E), x(E_j[2]))$ and contains the λ-invariant of any curve with complex multiplication by $\mathcal{O}$. We can say more by the following proposition, which follows as in the proof of part 1 of Proposition 2.6.2, using the fact that the Galois group of $\mathbb{Q}(j, x(E_j[2]))$ over $\mathbb{Q}(j)$ is isomorphic to $GL_2(\mathbb{Z}/2\mathbb{Z})$ ([15, Thm. 7.6.3]). An alternate argument is found in [21, p. 460].

Proposition 2.7.1 *Let j be the modular j-invariant function of the curve $X(1)$. The field $\mathbb{Q}(j, x(E_j[2]))$ of modular functions of $X(2)$ is $\mathbb{Q}(\lambda)$, where λ is the modular function from Section 2.6.*

This proposition implies that the λ-invariant of a curve with complex multiplication by $\mathcal{O}$ generates the field $K(j(E), x(E_j[2]))$. In the case of a fundamental discriminant, the groups $P_{2m,1}(\mathcal{O}_K) \subset P_{2m,\mathbb{Z}}(\mathcal{O}_K)$ are equal since the conductor m is 1. Thus the ray class field of K of conductor 2 is the same as the ring class field of conductor 2 and both are equal to $K(\lambda)$ where λ is the λ-invariant of any curve in Legendre form with complex multiplication by $\mathcal{O}_K$.

Let F be the degree two extension of $\mathbb{Q}_p$, where p is a prime not dividing $2D$. We now show that every curve E with complex multiplication by $\mathcal{O}$ is isomorphic to a curve in Legendre form defined over F.

Proposition 2.7.2 *Let $D < -4$ be a discriminant of a quadratic imaginary order and let*

p be inert in $K = \mathbb{Q}(\sqrt{D})$ with $p \nmid 2D$. Let F be the degree two unramified extension of $\mathbb{Q}_p$. For any E with complex multiplication by $\mathcal{O}$ and good reduction modulo p, the curves in Legendre form isomorphic to E are defined over $\mathbb{Z}_F$ and have good reduction modulo p.

Proof: Let E be a curve with complex multiplication by $\mathcal{O}$ and with good reduction modulo p. Any curve L in Legendre form isomorphic to E is given by $\lambda = \frac{e_3 - e_1}{e_2 - e_1}$ where e_1, e_2, e_3 is some ordering of the x-coordinates of $E[2]$. In particular, λ is in $K(j(E), x(E_j[2])$. The fact that p is prime to $2D$ implies that the ideal (p) of K is in $P_{2m,\mathbb{Z}}(\mathcal{O}_K)$, the kernel of the Artin map $I_{2m}(\mathcal{O}_K) \to \mathrm{Gal}(K(j(E), x(E_j[2])/K)$. Therefore (p) splits completely in $K(j(E), x(E_j[2]))$ and the extension field embeds into F. Thus L is defined over F.

As E has good reduction modulo p, the e_i are distinct modulo p. This implies that λ is a p-adic integer and $\lambda \not\equiv 0, 1 \bmod p$. Therefore $\lambda \in \mathbb{Z}_F$ and L has good reduction modulo p. □

By the above proposition, given any j-invariant corresponding to a curve with complex multiplication by $\mathcal{O}$, the six distinct curves in Legendre form with j-invariant j are defined over F. This shows that the cardinality of the set $\mathrm{Leg}_D(F)$ is $6h(\mathcal{O})$, where $h(\mathcal{O})$ is the order of $Cl(\mathcal{O})$, as was claimed in the proof of Theorem 2.5.2.

Let $\mathcal{O}_2$ denote the order of K of conductor $2m$ and let $Cl(\mathcal{O}_2)$ denote its class group. The following commutative diagram relates $Cl(\mathcal{O}_2)$ and $Cl(\mathcal{O})$ with generalized ideal class groups of K:

$$\begin{tikzcd}
I_{2m}(\mathcal{O}_K)/P_{2m,\mathbb{Z}}(\mathcal{O}_K) \arrow[r] \arrow[d] & I_m(\mathcal{O}_K)/P_{m,\mathbb{Z}}(\mathcal{O}_K) \arrow[d] \\
Cl(\mathcal{O}_2) \arrow[r] & Cl(\mathcal{O})
\end{tikzcd}$$

The left and right maps are isomorphisms given by $\mathfrak{a}_K \mapsto \mathfrak{a}_K \cap \mathcal{O}_2$ and $\mathfrak{a}_K \mapsto \mathfrak{a}_K \cap \mathcal{O}$, respectively. The lower horizontal map is the map $\mathfrak{b} \mapsto \mathfrak{b}\mathcal{O}$.

We now define an action of $Cl(\mathcal{O}_2)$ on $\mathrm{Leg}_D(F)$ which is compatible with the action of $Cl(\mathcal{O})$ on the j-invariants of curves in $\mathrm{Ell}_D(F)$ which sends $j(L)$ to $j(E)$ where $E = L/L[\mathfrak{a}]$. Let $L \in \mathrm{Leg}_D(F)$ and let $\mathfrak{a}$ be the image in $Cl(\mathcal{O})$ of an ideal of $Cl(\mathcal{O}_2)$. In particular, $\mathfrak{a}$ is relatively prime to $2\mathcal{O}$. Via the normalized isomorphism $\mathcal{O} \xrightarrow{\sim} \mathrm{End}(L)$, this defines a subgroup $L[\mathfrak{a}] = \bigcap_{\alpha \in \mathfrak{a}} \ker(\alpha)$ and a corresponding isogeny $\varphi_{\mathfrak{a}} : L \to E$. Since $\mathfrak{a}$ is relatively prime to $2\mathcal{O}$, the isogeny $\varphi_{\mathfrak{a}}$ sends $((0,0),(1,0))$ to (P,Q), a basis of $E[2]$. Let

$$\lambda^{\mathfrak{a}} = \lambda([E,(P,Q)]),$$

where λ is the map (2.9) from Section 2.6 and define $L^{\mathfrak{a}}$ to be the curve with Legendre invariant $\lambda^{\mathfrak{a}}$. This gives a well-defined action of $Cl(\mathcal{O}_2)$ on $\mathrm{Leg}_D(F)$, as we show below. Furthermore, as $j(L^{\mathfrak{a}}) = j(L)^{\mathfrak{a}}$, this action is compatible with the action of $Cl(\mathcal{O})$.

Proposition 2.7.3 *The action $L \mapsto L^{\mathfrak{a}}$ is a well-defined free action of $Cl(\mathcal{O}_2)$ on $\mathrm{Leg}_D(F)$. Given $L, L' \in \mathrm{Leg}_D(F)$, there exists $\mathfrak{a} \in Cl(\mathcal{O}_2)$ such that $j(L^{\mathfrak{a}}) = j(L')$.*

Proof: Let (α) be an ideal of $P_{2m,\mathbb{Z}}(\mathcal{O}_K)$. Then $\alpha \equiv a \bmod 2m\mathcal{O}_K$ for some integer a prime to $2m$. Therefore, $\alpha \in \mathcal{O}_2$ and the ideal $\mathfrak{a} = \alpha\mathcal{O}$ is equivalent to 1 modulo $2\mathcal{O}$. The isogeny $\varphi_{\mathfrak{a}} : L \to E$ gives a curve with $j(E) = j(L)$. Let $\lambda^{\mathfrak{a}} = \lambda([E,(P,Q)])$, and let h be the unique isomorphism (up to ±1) $E \to L^{\mathfrak{a}}$ which maps

(P,Q) to $((0,0),(1,0))$. Then $h\varphi_{\mathfrak{a}} : L \to L^{\mathfrak{a}}$ fixes the two-torsion. Let $g : L^{\mathfrak{a}} \to L$ be the unique isomorphism (up to ±1) between the two curves. The map $gh\varphi_{\alpha}$ is an endomorphism of L corresponding to the element $\alpha \in \mathrm{End}(L)$. Since $\alpha \equiv 1 \bmod 2\mathcal{O}$, the endomorphism must fix the two-torsion. Therefore, g must send $((0,0),(1,0))$ to $((0,0),(1,0)) \subset L[2]$. By the chart in the proof of Proposition 2.5.1, an isomorphism between two curves in Legendre form with the same j-invariant which fixes two-torsion must be the identity. Therefore, $L^{\mathfrak{a}} = L$, and the action of $Cl(\mathcal{O}_2)$ is well-defined.

To show the action is free, let $\mathfrak{a}$ be the image in $Cl(\mathcal{O})$ of an ideal of $Cl(\mathcal{O}_2)$ such that $L^{\mathfrak{a}} = L$. We show that $\mathfrak{a} = (\alpha)$ where $\alpha\mathcal{O}_K$ is an ideal of $P_{2m,\mathbb{Z}}(\mathcal{O}_K)$. The action of $\mathfrak{a}$ is compatible with the action of $Cl(\mathcal{O})$ on $\mathrm{Ell}_D(F)$, which sends $j(L)$ to $j(L^{\mathfrak{a}})$ via the isogeny with kernel $L[\mathfrak{a}]$. Therefore, as $j(L^{\mathfrak{a}}) = j(L)$, the ideal $\mathfrak{a}$ must be principal with $\mathfrak{a} = (\alpha)$ for some $\alpha \in \mathcal{O}$. The isomorphism $h : E \to L^{\mathfrak{a}}$ sends (P,Q) to $((0,0),(1,0))$. Since $L^{\mathfrak{a}} = L$, we have that $\alpha = h \circ \varphi_{\mathfrak{a}}$ is an endomorphism of L fixing the two-torsion $L[2]$. This implies that $\alpha \equiv 1 \bmod 2\mathcal{O}$. Letting $\mathcal{O}_K = \mathbb{Z}[w]$, we have that $\alpha = a + bmw$ where b is even and a is odd. Thus $\mathfrak{a}$ is the image of $\alpha\mathcal{O}_2$ in $Cl(\mathcal{O}_2)$ which is by assumption prime to $2m$. Thus a is prime to $2m$. Since $\alpha \equiv a \bmod 2m\mathcal{O}_K$, this shows that $\alpha\mathcal{O}_K$ is in $P_{2m,\mathbb{Z}}(\mathcal{O}_K)$.

The last claim follows from the fact that $Cl(\mathcal{O})$ acts transitively on the set $\mathrm{Ell}_D(F)$, which is precisely the set of j-invariants of curves in $\mathrm{Leg}_D(F)$, and the fact that any ideal class of $Cl(\mathcal{O})$ has a representative relatively prime to (2). □

A straightforward counting argument shows that the action is not transitive. The following exact sequence relates the groups $Cl(\mathcal{O}_2)$ and $Cl(\mathcal{O})$: ([11, Thm. 7.24]):

$$1 \to (\mathcal{O}/2\mathcal{O})^*/(\mathrm{im}(\mathcal{O}^*)(\mathbb{Z}/2\mathbb{Z})^*) \to Cl(\mathcal{O}_2) \to Cl(\mathcal{O}) \to 1 \qquad (2.10)$$

where $\mathrm{im}(\mathcal{O}^*)$ is the image of the unit group $\mathcal{O}^*$ under the map $\mathcal{O} \to \mathcal{O}/2\mathcal{O}$. Let $h(\mathcal{O})$ denote the class number of $\mathcal{O}$. As $(\mathbb{Z}/2\mathbb{Z})^* = 1$ and $\mathrm{im}(\mathcal{O}^*) = 1$, by the above exact sequence, we have that $\#Cl(\mathcal{O}_2) = m \cdot h(\mathcal{O})$ where

$$m = \begin{cases} 1 & (2) \text{ splits in } K \\ 2 & (2) \text{ ramifies in } K \\ 3 & (2) \text{ is inert in } K. \end{cases}$$

As $\mathrm{Leg}_D(F)$ has cardinality $6h(\mathcal{O})$, the action cannot be transitive. In particular, for the case of $m = 1$, there is no $\mathfrak{a} \in Cl(\mathcal{O}_2)$ that sends a curve L in Legendre form to a distinct curve L' in Legendre form with the same j-invariant. Suppose $L' = L^{\mathfrak{a}}$. Then the ideal $\mathfrak{a}$ must be prinicipal, because the action is compatible with that of $Cl(\mathcal{O})$ on $\mathrm{Ell}_D(F)$. Therefore $\mathfrak{a} = (\alpha)$ defines an endomorphism of L fixing the two-torsion, with kernel $L[\alpha]$. By definition of the action, this endomorphism factors through an isogeny between L and $L' = L^{\mathfrak{a}}$ which also fixes the two-torsion. This implies there is an isomorphism between L and L' fixing two-torsion, which implies that $L = L'$, as shown in the proof of Proposition 2.5.1.

The action of $Cl(\mathcal{O}_2)$ on $\mathrm{Leg}_D(F)$ induces an action on $\mathrm{LegEmb}_D(\mathbb{F}_{p^2})$ via Theorem 2.5.2:

$$(L_p, f)^{\mathfrak{a}} = ((L_p)^{\mathfrak{a}}, f^{\mathfrak{a}})$$

where $(L_p)^{\mathfrak{a}} = (L^{\mathfrak{a}})_p$, and $f^{\mathfrak{a}}$ is the action described in Section 2.3.4. For convenience, we reiterate the details here, as the condition of fixing the two-torsion adds a minor technicality. Let $\varphi_{\mathfrak{a}} : L \to E$ be the isogeny with kernel $L[\mathfrak{a}]$. Let $h : E \to L^{\mathfrak{a}}$ be the unique isomorphism (up to ± 1) such that $h\varphi_{\mathfrak{a}}$ fixes the two-torsion, that is, sends the ordered sequence $\big[(0,0),(1,0),(\lambda,0)\big]$ to $\big[(0,0),(1,0),(\lambda^{\mathfrak{a}},0)\big]$. Writing $\mathcal{O} = \mathbb{Z}[\tau]$, let $\beta \in \operatorname{End}(L)$ be the image of τ under the normalized isomorphism $\mathcal{O} \simeq \operatorname{End}(L)$. The normalized isomorphism for $L^{\mathfrak{a}}$ is given by

$$\tau \mapsto h\varphi_{\mathfrak{a}}\beta\widehat{\varphi}_{\mathfrak{a}}h^{-1} \otimes (\deg \varphi_{\mathfrak{a}})^{-1},$$

and $f^{\mathfrak{a}}$ is the composition $\mathcal{O} \simeq \operatorname{End}(L^{\mathfrak{a}}) \hookrightarrow \operatorname{End}(L^{\mathfrak{a}})$.

Remark 2.7.1

In Section 2.3.4, we explicitly computed $f^{\mathfrak{a}}$ using the action of $Cl(\mathcal{O})$ on $\operatorname{Emb}_D(\mathcal{A}_{p,\infty})$. We can use this action to compute $f^{\mathfrak{a}}$ for $\mathfrak{a} \in Cl(\mathcal{O}_2)$, but this only determines the embedding $f^{\mathfrak{a}}$ up to automorphism of $L^{\mathfrak{a}}$. Thus if $j(L_p^{\mathfrak{a}}) = 0$ or 1728, there are three, respectively two, possible candidates for the embedding $f^{\mathfrak{a}}$. To determine which is the correct embedding will require extra computation. This is discussed in Section 2.8.5.

We now proceed to show how the action of $Cl(\mathcal{O}_2)$ is used to compute the canonical lift of $(L, f) \in \operatorname{LegEmb}_D(\mathbb{F}_{p^2})$.

2.8 Computing the canonical lift of $(L, f) \in \operatorname{LegEmb}_D(\mathbb{F}_{p^2})$

In this section, we present an algorithm to compute the canonical lift of $(L, f) \in \operatorname{LegEmb}_D(\mathbb{F}_{p^2})$ for any prime $p \geq 3$. For $p \equiv 1 \bmod 12$, the algorithm is merely a modification of the algorithm in Section 2.4. For $p \not\equiv 1 \bmod 12$, the set of supersingular curves over $\mathbb{F}_{p^2}$ includes a curve with $j = 0$ or 1728, and the algorithm requires a modification of the p-adic analytic map used in the Algorithm 2.4.1.

2.8.1 The map ρ_α for the case of $p \not\equiv 1 \mod 12$

Let $\mathbb{C}_p$ be the completion of an algebraic closure of $\mathbb{Q}_p$. The field $\mathbb{C}_p$ is algebraically closed. Let $\eta = (L_o, f)$ be an element of $\mathrm{LegEmb}_D(\mathbb{F}_{p^2})$, and let $\tilde{L}$ denote its canonical lift. We define a 'disc' above η containing all possible candidates for the λ-invariant of the canonical lift of (L_o, f). These are pairs $(\lambda(L), f)$ with $\lambda(L) \equiv \lambda(L_o)$ modulo $\mathfrak{p}$, where $\mathfrak{p}$ is the prime above p in the smallest extension of $\mathbb{Q}_p$ in which $\lambda(L)$ lies. We denote this disc by

$$X_D(\eta) = \{(\lambda(L), f) \mid \lambda(L) \in \mathbb{C}_p, \lambda(L) \equiv \lambda(L_o) \bmod \mathfrak{p}\}$$

By Theorem 2.5.2, there is exactly one pair in each disc $X_D(\eta)$ such that the induced embedding of endomorphism rings is equal to f, namely $(\lambda(\tilde{L}), f)$. As in Section 2.4, we construct a p-adic analytic map from the set of discs to itself that has these pairs as fixed points and then "zero in" on the canonical lift of η using Newton's method.

Let $\mathfrak{a}$ be an $\mathcal{O}$-ideal of norm N coprime to $2p$. We define a map

$$\rho_{\mathfrak{a}} : \bigcup_{\eta} X_D(\eta) \to \bigcup_{\eta} X_D(\eta)$$

as follows. Let $(\lambda(L), f) \in X_D(\eta)$. The ideal $f(\mathfrak{a})$ of $\mathrm{End}(L_o)$ defines a subgroup $L_o[f(\mathfrak{a})]$ of the N-torsion. Since $(N, p) = 1$, the N-torsion of L_o lifts canonically to $L[N]$ and the subgroup $L_o[f(\mathfrak{a})]$ lifts canonically to a subgroup $L[\mathfrak{a}]$ of L. This defines an isogeny $\varphi_{\mathfrak{a}} : L \to E = L/L[\mathfrak{a}]$. Since $2 \nmid N(\mathfrak{a})$, the map $\varphi_{\mathfrak{a}}$ sends $((0,0), (1,0))$

to a basis (P, Q) of $E[2]$. Thus $[E, (P, Q)]$ is a point of $Y(2)_{\mathbb{Q}_p}$, and we may apply the modular function λ from Section 2.6. Define

$$\rho_{\mathfrak{a}}(\lambda(L), f) = (\lambda([E, (P, Q)]), f^{\mathfrak{a}}),$$

where $f^{\mathfrak{a}}$ is as in Section 2.7. When the map f is clear, we also denote by $\rho_{\mathfrak{a}}$ the induced map on the disc $X_D(\eta)$ restricted to the first coordinate of the pair, which is simply the p-adic disc of radius one around $\lambda(L_o)$.

We now explain the connection of $\rho_{\mathfrak{a}}$ to the action of $Cl(\mathcal{O}_2)$ on $\mathrm{Leg}_D(F)$. If $\tilde{L}$ is the canonical lift of (L_o, f), then $\rho_{\mathfrak{a}}(\lambda(\tilde{L}), f)$ is equal to $(\lambda(\tilde{L}^{\mathfrak{a}}), f^{\mathfrak{a}})$, where $\tilde{L}^{\mathfrak{a}}$ is determined by the action defined in Proposition 2.7.3. This follows from the fact that the induced embedding $\mathrm{End}(\tilde{L}) \simeq \mathcal{O} \hookrightarrow \mathrm{End}(L_o)$ is by definition f. Therefore, the isogeny $\varphi_{\mathfrak{a}}$ defined by the lift of $L_o[f(\mathfrak{a})]$ is precisely the isogeny defined by $\mathfrak{a} \subset \mathrm{End}(\tilde{L})$.

Let $\mathfrak{a}$ be principal with $\mathfrak{a} = (\alpha)$ for $\alpha \equiv 1 \bmod 2$ and norm $N(\alpha)$ coprime to p and m, the conductor of $\mathcal{O}$. Then the isogenous curve $E = \tilde{L}/\tilde{L}[\mathfrak{a}]$ is isomorphic to $\tilde{L}$ and $\lambda([E, (P, Q)])$ equals $\lambda(\tilde{L})$. Furthermore, $f^{\alpha} = f$, and therefore $(\lambda(\tilde{L}), f)$ is fixed by ρ_{α}.

Note, however, that the map $\rho_{\mathfrak{a}}$ is *not* an extension of the action in Proposition 2.7.3. Let $L \in \mathrm{Leg}_D(F)$ with $\lambda(L) \equiv \lambda(L_o) \bmod p$ but such that L is *not* the canonical lift of η. That is, the induced embedding of endomorphism rings is not f. Then the lift of $L_o[f(\mathfrak{a})]$ to L is not *necessarily* equal to the subgroup $L[\mathfrak{a}]$. Therefore, $\rho_{\mathfrak{a}}(\lambda(L), f)$ is not necessarily equal to $(\lambda(L^{\mathfrak{a}}), f^{\mathfrak{a}})$. They may be equal, for example, if the induced embedding is equal to f conjugated by an isogeny which stabilizes the subgroup $L_o[f(\mathfrak{a})]$.

However, if $\mathfrak{a}$ is principal with $\mathfrak{a} = (\alpha)$ where $\alpha/\bar{\alpha} - 1$ is a p-adic unit, then they cannot be not equal. That is, the point $(\lambda(L), f)$ is fixed by ρ_{α} if and only if L is the canonical lift of $\eta = (\lambda(L_o), f)$. Therefore, though the disc $X_D(\eta)$ may contain multiple pairs $(\lambda(L), f)$ with $L \in \mathrm{Leg}_D(F)$, it contains exactly one point fixed by ρ_α. This fact follows from the p-adic analyticity of ρ_α, as we now show.

Let $\alpha \equiv 1 \bmod 2$ with norm N coprime to p and m, the conductor of $\mathcal{O}$. Let $\eta = (L_o, f) \in \mathrm{LegEmb}_D(\mathbb{F}_{p^2})$. Since (α) is prinicipal and $\alpha \equiv 1 \bmod 2$, ρ_α stabilizes $X_D(\eta)$. By abuse of notation, we let $\rho_\alpha : X_D(\eta) \to X_D(\eta)$. denote the corresponding map on λ-invariants and $X_D(\eta)$ denote the p-adic disc of radius one around $\lambda(L_o)$. The proofs of the following statements are found in the next three subsections.

Theorem 2.8.1 *Let $\eta \in \mathrm{LegEmb}_D(\mathbb{F}_{p^2})$ and let $\tilde{\lambda}$ be the λ-invariant of the canonical lift of η. For $\alpha \in \mathcal{O}_K$ with $\alpha \equiv 1 \bmod 2$ and norm $N(\alpha)$ coprime to pm, the map ρ_α is p-adic analytic in the disc $X_D(\eta)$. That is, there exist $a_i \in \mathbb{Z}_F$ such that*

$$\rho_\alpha(\lambda) - \tilde{\lambda} = \sum_{i \geq 1} a_i (\lambda - \tilde{\lambda})^i,$$

for all $\lambda \in X_D(\eta)$.

Proposition 2.8.2 *Let the hypotheses be as in Theorem 2.8.1. The map $\rho_\alpha(\lambda)$ has derivative $\alpha/\bar{\alpha}$ at the point $\lambda = \tilde{\lambda}$.*

As in the case of Section 2.4, for $\bar{\alpha} \not\equiv \alpha \bmod p$, the p-adic analytic map ρ_α has a unique fixed point, namely $\tilde{\lambda}$. The algorithm in Section 2.8.7 to compute the canonical lift uses a variant of Newton's method to converge to $\tilde{\lambda}$.

Proposition 2.8.3 *Let*

$$\lambda_{k+1} = \lambda_k - \frac{\rho_\alpha(\lambda_k) - \lambda_k}{\alpha/\bar{\alpha} - 1}.$$

For any $\lambda_0 \in X_D(\eta)$, the sequence $\{\lambda_k\}$ converges quadratically to $\tilde{\lambda}$. Therefore, the map ρ_α has a unique fixed point in the disc $X_D(\eta)$.

2.8.2 Proof of Theorem 2.8.1

The purpose of this section is to prove Theorem 2.8.1, following the approach found in the proof of [5, Thm. 4.2]. We begin by giving an algebraic-geometric interpretation of ρ_α in terms of functions on modular curves. Let N be odd and consider the modular curve $Y(\Gamma_{2,N})$ defined over $\mathbb{C}$ by the congruence subgroup $\Gamma_{2,N} = \Gamma_0(N) \cap \Gamma(2)$, where $\Gamma_0(N)$ is the subgroup of $SL_2(\mathbb{Z})$ of matrices $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with $c \equiv 0 \bmod N$.

The curve $X(2N)$ has a non-singular projective model over $\mathbb{Z}[\zeta_N]$, thus we can consider it as a curve over $\mathbb{Q}_p(\zeta_N)$. The ζ_N comes from the Weil-pairing condition in the moduli interpretation of $Y(2N)$. Since $\Gamma(2N) \subset \Gamma_{2,N}$, the curve $X(\Gamma_{2,N})$ is a quotient of $X(2N)$ and thus we may also work with $X(\Gamma_{2,N})$ over $\mathbb{Q}_p(\zeta_N)$. Moreover, it can be defined over $\mathbb{Q}_p$, since there is no Weil-pairing condition in the moduli interpretation for $\Gamma_0(N)$. In what follows, we work with the modular curves $X(\Gamma_{2,N})$ and $X(2)$ defined over $\mathbb{Q}_p$, unless otherwise specified, and consider their points over $\mathbb{C}_p$, the completion of an algebraic closure of $\mathbb{Q}_p$.

The points of the affine curve $Y(\Gamma_{2,N})$ correspond to the equivalence classes of triples $[E, G, (P, Q)]$ where E is an elliptic curve over $\mathbb{C}_p$, G is a cyclic order-N subgroup, and (P, Q) is a basis of the 2-torsion. Two triples are equivalent if there is a $\mathbb{C}_p$-isomorphism $h : E \to E'$ such that $h(G) = G', h(P) = P'$ and $h(Q) = Q'$.

We now define two maps $\lambda_1, \lambda_2 : Y(\Gamma_{2,N}) \to \mathbb{C}_p$ as follows. Let π denote the "forgetful" map

$$\begin{array}{rccc} \pi : & Y(\Gamma_{2,N}) & \to & Y(2) \\ & [E, G, (P, Q)] & \mapsto & [E, (P, Q)] \end{array}$$

Given a point $[E, G, (P, Q)]$ of $Y(\Gamma_{2,N})$, let φ_G denote the degree-N isogeny with kernel G. Let $\widehat{G}$ denote the "complementary" subgroup of G, that is, the subgroup of points of $E[N]$ such that $\widehat{G} \oplus G = E[N]$. The *Atkin-Lehner involution* is

$$\begin{array}{rccc} w_N : & Y(\Gamma_{2,N}) & \to & Y(\Gamma_{2,N}) \\ & [E, G, (P, Q)] & \mapsto & [\varphi_G(E), \varphi_G(\widehat{G}), (\varphi_G(P), \varphi_G(Q))] \end{array}$$

and satisfies the property that $w_N^2 = \mathrm{Id}$. This is true by the following facts. The map $\varphi_{\widehat{G}}$ is the map on the curve $\varphi_G(E)$ with kernel $\varphi_G(\widehat{G})$. Therefore it is the dual isogeny to φ_G, and thus $\varphi_{\widehat{G}}\varphi_G = [N]$. Since N is odd, this fixes the two-torsion of E. Note also that the subgroup complementary to $\varphi_G(\widehat{G})$ is mapped by $\varphi_{\widehat{G}}$ to G. Therefore, applying w_N to the point $[\varphi_G(E), \varphi_G(\widehat{G}), (\varphi_G(P), \varphi_G(Q))]$, we get $[E, G, (P, Q)]$. Thus w_N^2 is the identity map.

We define the map $\lambda_1 : Y(\Gamma_{2,N}) \to \mathbb{C}_p$ as $\lambda_1 = \lambda \circ \pi$, where $\lambda : Y(2) \to \mathbb{C}_p$ is the map from Section 2.6. We define the map $\lambda_2 : Y(\Gamma_{2,N}) \to \mathbb{C}_p$ as $\lambda_2 = \lambda_1 \circ w_N$.

The map λ_2 is directly related to ρ_α. Given $\lambda \in X_D(\eta)$, let L over F be the curve $y^2 = x(x-1)(x-\lambda)$. As $L \equiv L_o \bmod p$, we can lift the subgroup $L_o[f(\alpha)]$ uniquely to a subgroup $L[\alpha]$, as described in the previous section. By construction, the value $\rho_\alpha(\lambda)$ is the λ-invariant of the curve L' in Legendre form isomorphic to $L/L[\alpha]$ such that the induced isogeny $L \to L'$ preserves the order of the two-torsion. Thus

$$\rho_\alpha(\lambda) = \lambda_2([L, L[\alpha], ((0,0),(1,0))]).$$

We now have the tools to prove Theorem 2.8.1.

Proof of Thm. 2.8.1: Let $\eta = (L_o, f)$ and let $\tilde{L} \in \mathrm{Leg}_D(F)$ be its canonical lift.

As L_o has all two-torsion defined over $\mathbb{F}_{p^2}$, all endomorphisms of L_o are defined over $\mathbb{F}_{p^2}$ ([46, Thm. 4.1]). Thus the subgroup $L_o[f(\alpha)]$ is defined over $\mathbb{F}_{p^2}$ and its lift $\tilde{L}[\alpha] \subset L[N]$ is defined over F. Therefore, the point $R = [\tilde{L}, \tilde{L}[\alpha], ((0,0),(1,0))]$ is an F-rational point of $Y(\Gamma_{2,N})$. As $\tilde{L}$ is the canonical lift of η, we have that $\lambda_2(R) = \tilde{\lambda}$.

Let $\pi(R) = T$, and let $\mathcal{O}_R$ and $\mathcal{O}_T$ denote the local rings of functions at R and T, respectively. As shown in Section 2.6, the modular function $\lambda : Y(2)(F) \to F - \{0,1\}$ is a bijection. Therefore, $\lambda - \lambda(T)$ is a uniformizer for $\mathcal{O}_T$.

The map $Y(\Gamma(2N)) \to Y(2)$ is unramified above $\lambda \neq 0, 1, \infty$ [21, p. 463], and factors through the map $Y(\Gamma_{2,N}) \to Y(2)$. Therefore the cover $Y(\Gamma_{2,N}) \to Y(2)$ is unramified above $\lambda \neq 0, 1, \infty$. Viewing the maximal ideal $(\lambda - \lambda(T))$ in $\mathcal{O}_R$ and using the fact that $\lambda_1 = \pi \circ \lambda$, this implies that

$$(\lambda - \lambda(T))\mathcal{O}_R = (\lambda_1 - \lambda_1(R)).$$

Therefore the function $\lambda_1 - \lambda_1(R)$ is a uniformizer for the completion $\widehat{\mathcal{O}}_R$ of the local ring at R. Since $Y(\Gamma_{2,N})_F$ is a smooth curve, $\widehat{\mathcal{O}}_R$ is a discrete valuation ring over F. Thus $\widehat{\mathcal{O}}_R \simeq F[[\lambda_1 - \lambda_1(R)]]$.

We now show that $\lambda_2 - \lambda_2(R)$ is also a uniformizer for R. Precomposing with w_N gives

$$(\lambda_2 - \lambda_2(R)) \circ w_N = \lambda_1 \circ w_N^2 - \lambda_2(R) = \lambda_1 - \lambda_1 \circ w_N(R), \tag{2.11}$$

since $w_N^2 = \mathrm{Id}$ and $\lambda_2 = \lambda_1 \circ w_N$. If $\lambda_2 - \lambda_2(R)$ has a zero of order m at R, then (2.11) has a zero of order m at $w_N(R)$, again by the fact that $w_N^2 = \mathrm{Id}$. As (2.11) is a uniformizer for the local ring at $w_N(R)$, we have that $m = 1$, and thus $\lambda_2 - \lambda_2(R)$ is a uniformizer for R in $\widehat{\mathcal{O}}_R$.

The curve $X(2N)$ has good reduction modulo p not dividing N. As $X(\Gamma_{2,N})$ is a quotient of $X(2N)$, the curve $X(\Gamma_{2,N})$ also has good reduction modulo p not dividing N ([12, Prop. 4.2]). Arguing as in [5, p. 10], we now work with the modular curves $X(2)$ and $X(\Gamma_{2,N})$ as schemes over $\mathbb{Z}_p$. As shown in the proof of Proposition 2.7.2, the λ-invariant of $\tilde{L}$, denoted $\tilde{\lambda}$, is in $\mathbb{Z}_F$ and is not equal to 0 or 1 modulo p. Thus $\tilde{L}$ has good reduction modulo p and there is a point R' of $X(\Gamma_{2,N})_{\mathbb{Z}_p}$ which corresponds to R and similarly a point $\bar{R}$ of $X(\Gamma_{2,N})_{\mathbb{F}_p}$ corresponding to R. Similarly, we may consider the points $T', \bar{T}$ of $X(2)_{\mathbb{Z}_p}$, respectively $X(2)_{\mathbb{F}_p}$.

By [21, pp. 460], the function λ generates the field of functions of $X(2)_{\mathbb{F}_p}$, and therefore $\lambda - \lambda_o$ is a uniformizer for $\bar{T}$. The cover $\pi : Y(\Gamma_{2,N})_{\mathbb{F}_p} \longrightarrow Y(2)_{\mathbb{F}_p}$ is unramified above $\lambda \neq 0, 1, \infty$ ([21, p. 463], and so $\lambda_1 = \lambda \circ \pi$ is a uniformizer for $\bar{R}$. Considering $\lambda_2 = \lambda_1 \circ w_N$ as a function $Y(\Gamma_{2,N})_{\mathbb{F}_p} \longrightarrow \overline{\mathbb{F}}_p$, we have that $\lambda_2 - \lambda_o$ is also a uniformizer for $\bar{R}$ by the fact that $w_N^2 = \mathrm{Id}$.

Let $\widehat{\mathcal{O}}_{R'}$ denote the completion of the local ring at R'. Since $\lambda_1 - \tilde{\lambda}$ and $\lambda_2 - \lambda_o$ both reduce to uniformizers modulo p, the ideals $(p, \lambda_1 - \tilde{\lambda})$ and $(p, \lambda_2 - \tilde{\lambda})$ are uniformizers for $\widehat{\mathcal{O}}_{R'}$. By the structure theory of complete local rings, $\widehat{\mathcal{O}}_{R'} \simeq \mathbb{Z}_F[[\lambda_1 - \tilde{\lambda}]]$ [27, Proof of Thm. 29.7]. Therefore, there exist $a_i \in \mathbb{Z}_F$ such that

$$\lambda_2 - \tilde{\lambda} = \sum_{i \geq 1} a_i (\lambda_1 - \tilde{\lambda})^i. \tag{2.12}$$

Given $\lambda \in X_D(\eta)$, let L denote the corresponding curve in Legendre form. Recall that $\rho_\alpha(\lambda) = \lambda_2([L, L[\alpha], ((0,0),(1,0))])$. Therefore

$$\begin{aligned} \rho_\alpha(\lambda) - \tilde{\lambda} &= \lambda_2([L, L[\alpha], ((0,0),(1,0))]) - \tilde{\lambda} \\ &= \textstyle\sum_{i\geq 1} a_i\big(\lambda_1([L, L[\alpha], ((0,0),(1,0))]) - \tilde{\lambda}\big)^i \\ &= \textstyle\sum_{i\geq 1} a_i(\lambda - \tilde{\lambda})^i. \end{aligned}$$

As $a_i \in \mathbb{Z}_F$, this series converges for any $\lambda \in X_D(\eta)$. □

2.8.3 Proof of Proposition 2.8.2

In this section, we prove Proposition 2.8.2 by computing the value $a_1 \in \mathbb{Z}_F$ in the power series (2.12). The proof follows the approach in the proof of [5, Lemma 4.3]. We first show that it is valid to compute the slope in the complex analytic setting. This follows from the fact that the value a_1 may be interpreted as the ratio of differentials of the curve $Y(\Gamma_{2,N})$ evaluated at an F-rational point.

Proof of Prop. 2.8.2 The space of differentials of the curve $Y(\Gamma_{2,N})$ is a one-dimensional vector space over the function field of the curve. As λ_1, λ_2 are functions of $Y(\Gamma_{2,N})$, there exists a function γ on $Y(\Gamma_{2,N})$ such that $\gamma d\lambda_1 = d\lambda_2$. By the power series (2.12), we have that $d\lambda_2 = \big(a_1 + \sum_{i\geq 2} ia_i(\lambda_1 - \tilde{\lambda}))^{i-1}\big)d\lambda_1$. Thus, for the F-rational point $R = [\tilde{L}, \tilde{L}[\alpha], ((0,0),(1,0))]$, we have $\gamma(R) = a_1$.

Since $\tilde{\lambda}$ is integral over $\mathbb{Z}_{(2)}[j(\tilde{L})]$, where $j(\tilde{L})$ is an algebraic integer, we may view $\tilde{\lambda} \in \bar{\mathbb{Q}}$. Thus we may view R as a point in $Y(\Gamma_{2,N})(\mathbb{C})$ and calculate $a_1 = \frac{d\lambda_2}{d\lambda_1}(R)$ from the complex-analytic viewpoint.

By the bijection of the moduli space $Y(\Gamma_{2,N})_{\mathbb{C}}$ with $\Gamma_{2,N}\backslash\mathcal{H}$, given any point P representing $[L, L[\alpha], ((0,0),(1,0))]$, there exists a representative $\tau \in \Gamma_{2,N}\backslash\mathcal{H}$ such that

P corresponds to

$$[\mathbb{C}/\Lambda_\tau, \langle 1/N + \Lambda_\tau \rangle, (\tau/2 + \Lambda_\tau, 1/2 + \Lambda_\tau)].$$

In particular, the kernel of the map α on $\mathbb{C}/\Lambda_\tau$ is $\langle 1/N + \Lambda_\tau \rangle$. Let τ_o be the representative corresponding to the point R.

The map λ_1 on $Y(\Gamma_{2,N})_\mathbb{C}$ is given by $\lambda_1(P) = \lambda(\tau)$. To interpret the map λ_2, note that the complex-analytic map defined by α on L corresponds to

$$\mathbb{C}/\langle 1, \tau \rangle \to \mathbb{C}/\langle 1/N, \tau \rangle \xrightarrow{N} \mathbb{C}/\langle 1, N\tau \rangle, \tag{2.13}$$

where the first map has kernel $\langle 1/N \rangle + \Lambda_\tau$ and the second map is the isomorphism given by rescaling by N. The resulting curve is $\mathbb{C}/\langle 1, N\tau \rangle$ and the map λ_2 is given by $\lambda_2(P) = \lambda(N\tau)$. Letting $\lambda_N(\tau) = \lambda(N\tau)$, we have that

$$\frac{d\lambda_2}{d\lambda_1}(P) = \frac{d\lambda_N}{d\lambda}(\tau).$$

Thus to compute a_1, we want to evaluate at $\tau = \tau_o$.

From Section 2.6, the modular function $j(\tau)$ can be given as a rational expression in $\lambda(\tau)$ via the function J:

$$j(\tau) = J(\lambda(\tau)).$$

Let $j_N(\tau)$ denote the function $j(N\tau)$ and let $J_N(\tau)$ denote the function $J(\lambda_N(\tau))$, which is equal to $j_N(\tau)$. We now show that

$$\frac{d\lambda_N}{d\lambda}(\tau_o) = \frac{dj_N}{dj}(\tau_o).$$

By [5, Lemma 4.3], $\frac{dj_N}{dj}(\tau_o) = \frac{\alpha}{\bar{\alpha}}$, and thus the result follows.

We have

$$\frac{dJ}{d\tau} = \frac{dJ(\lambda(\tau))}{d\tau} = \frac{dJ}{d\lambda}\frac{d\lambda}{d\tau}$$

and

$$\frac{dJ_N}{d\tau} = \frac{dJ(\lambda_N(\tau))}{d\tau} = \frac{dJ_N}{d\lambda_N}\frac{d\lambda_N}{d\tau}.$$

Therefore

$$\frac{dj_N}{dj}(\tau) = \frac{dJ_N}{dJ}(\tau) = \frac{dJ_N}{d\lambda_N}(\tau)(\frac{dJ}{d\lambda}(\tau))^{-1}\frac{d\lambda_N}{d\lambda}(\tau).$$

Since $\frac{dJ_N}{d\lambda_N}(\tau) = \frac{dJ}{d\lambda}(N\tau)$, it suffices to show that $\lambda(N\tau_o) = \lambda(\tau_o)$. Since α is an endomorphism of $\mathbb{C}/\Lambda_{\tau_o}$ with kernel $\langle 1/N\rangle + \Lambda_\tau$, we have $\mathbb{C}/\langle 1, \tau_o\rangle \overset{\alpha}{\to} \mathbb{C}/\langle 1, \tau_o\rangle$. The map (2.13) has the same kernel, thus the image curves are isomorphic via the map α/N:

$$\mathbb{C}/\langle 1, N\tau_o\rangle \overset{\alpha/N}{\to} \mathbb{C}/\langle 1, \tau_o\rangle.$$

Therefore, there exists $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ such that $\alpha\tau_o = a\tau_o + b$ and $\alpha/N = c\tau_o + d$, and $M\tau_o = \frac{a\tau_o+b}{c\tau_o+d} = \frac{\alpha\tau_o}{\alpha/N} = N\tau_o$.

We now show that $M \in \Gamma(2)$. The non-trivial two-torsion of Λ_{τ_o} is $\{1/2 + \Lambda_{\tau_o}, \tau_o/2 + \Lambda_{\tau_o}, (\tau_o + 1)/2 + \Lambda_{\tau_o}\}$. As $\alpha \equiv 1 \bmod 2$, the endomorphism α fixes the two-torsion. Furthermore, since $(N, 2) = 1$, the map $\mathbb{C}/\langle 1, \tau_o\rangle \to \mathbb{C}/\langle 1/N, \tau_o\rangle \overset{N}{\to} \mathbb{C}/\langle 1, N\tau_o\rangle$ also fixes the two-torsion. For example,

$$1/2 + \langle 1, \tau_o\rangle \mapsto 1/2 + \langle \frac{1}{N}, \tau_o\rangle \mapsto N/2 + \langle 1, N\tau_o\rangle = 1/2 + \Lambda_{N\tau_o}.$$

Since neither α nor N permute the two torsion, the isomorphism $\frac{\alpha}{N} = c\tau_o + d$ must also fix the the two-torsion. Thus c is even and d is odd, which implies that $M \in \Gamma(2)$. Since λ is $\Gamma(2)$-invariant, $\lambda(N\tau_o) = \lambda(M\tau_o) = \lambda(\tau_o)$. This completes the proof. □

2.8.4 Proof of Proposition 2.8.3

We now give the proof of Proposition 2.8.3. We assume that $\alpha/\bar{\alpha} - 1$ is a p-adic unit and show that $\{\lambda_k\}$ converges quadratically to $\tilde{\lambda}$ where

$$\lambda_{k+1} = \lambda_k - \frac{\rho_\alpha(\lambda_k) - \lambda_k}{\alpha/\bar{\alpha} - 1}.$$

In particular, this implies that $\tilde{\lambda}$ is the *unique* fixed point in the p-adic disc radius 1 around $\lambda(L_o)$.

Proof of Prop. 2.8.3: Let $a_1 = \alpha/\bar{\alpha}$ and choose $\lambda_0 \in X_D(\eta)$. Then $\lambda_0 \equiv \lambda(L_o) \bmod p$. Let

$$\lambda_{k+1} = \lambda_k - \frac{\rho_\alpha(\lambda_k) - \lambda_k}{a_1 - 1}.$$

Let v_p denote the p-adic valuation of F. We show by induction that for all $k \geq -1$,

$$v_p(\lambda_{k+1} - \tilde{\lambda}) \geq 2^{k+1}.$$

By assumption, $v_p(\lambda_0 - \tilde{\lambda}) \geq 1$, therefore the statement holds for $k = -1$. Assume $v_p(\lambda_k - \tilde{\lambda}) \geq 2^k$. Then

$$\begin{aligned}
\lambda_{k+1} - \tilde{\lambda} &= \lambda_k - \tilde{\lambda} - \big(\rho_\alpha(\lambda_k) - \lambda_k\big)\big(a_1 - 1\big)^{-1} \\
&= (\lambda_k - \tilde{\lambda}) - \big(\tilde{\lambda} + \textstyle\sum_{i\geq 1} a_i(\lambda_k - \tilde{\lambda})^i - \lambda_k\big)\big(a_1 - 1\big)^{-1} \\
&= (\lambda_k - \tilde{\lambda}) - \big((a_1 - 1)(\lambda_k - \tilde{\lambda}) + \textstyle\sum_{i\geq 2} a_i(\lambda_k - \tilde{\lambda})^i\big)\big(a_1 - 1\big)^{-1} \\
&= -\textstyle\sum_{i\geq 2} a_i(a_1 - 1)^{-1}(\lambda_k - \tilde{\lambda})^i
\end{aligned}$$

Thus $v_p(\lambda_{k+1} - \tilde{\lambda}) = v_p(-\sum_{i\geq 2} a_i(a_1 - 1)^{-1}(\lambda_k - \tilde{\lambda})^i) \geq v_p((\lambda_k - \tilde{\lambda})^2) \geq 2^{k+1}$, as desired.

Note that this is essentially Newton's method

$$\lambda_{k+1} = \lambda_k - \frac{\rho_\alpha(\lambda_k) - \lambda_k}{\rho'(\lambda_k) - 1}$$

since $\rho'(\lambda_k) - 1 = \rho'(\tilde{\lambda}) - 1 + O(p^{2^k}) = (a_1 - 1) + O(p^{2^k})$. This completes the proof. □

Corollary 2.8.4 *Let v_p be the p-adic valuation of F and assume $v_p(\lambda_k - \tilde{\lambda}) = 2^k$. Then*

$$v_p(\lambda_{k+1} - \lambda_k) = v_p(\lambda_k - \tilde{\lambda}).$$

Proof: This follows from the definition of ρ_α and λ_{k+1}. Let $a_1 = \alpha/\bar{\alpha}$. Then $v_p(\lambda_{k+1} - \lambda_k) = v_p(\big(\rho_\alpha(\lambda_k) - \lambda_k\big)\big(a_1 - 1\big)^{-1}) = v_p(\rho_\alpha(\lambda_k) - \lambda_k)$, since $a_1 - 1$ is a p-adic unit. □.

2.8.5 An algorithm to compute the action of $Cl(\mathcal{O}_2)$ on $\mathrm{LegEmb}_D(\mathbb{F}_{p^2})$

Let $\mathcal{O}$ be an order of discriminant $D < -4$. Let p be inert in $K = \mathbb{Q}(\sqrt{D})$ with $p \nmid 2D$. In this section, we present an algorithm that computes the action of an ideal $\mathfrak{a} \in Cl(\mathcal{O}_2)$ on a pair (L, f) of the set $\mathrm{LegEmb}_D(\mathbb{F}_{p^2})$ The algorithm returns the curve $L^{\mathfrak{a}}$ and the embedding $f^{\mathfrak{a}}$. In this section, all elliptic curves are supersingular curves in characteristic p.

We fix a maximal order R of $\mathcal{A}_{p,\infty}$ into which $\mathcal{O}$ optimally embeds and a prime ℓ not equal to p. We choose a set of left R-ideal class representatives $\{J_i\}$, each of norm a power of ℓ. As discussed in Section 2.2.2, this is possible because the ℓ-isogeny grapha of supersingular curves over $\overline{\mathbb{F}}_p$ is connected. This determines $\mathrm{Emb}_D(\mathcal{A}_{p,\infty})$, the set of equivalence classes of optimal embeddings $\mathcal{O} \hookrightarrow R_r(J_i)$. As shown in Section 2.3.2, this set is in bijection with $\mathrm{Emb}_D(\mathbb{F}_{p^2})$.

We choose a curve L_1 with $\mathrm{End}(L_1) \simeq R$ and fix an isomorphism $i : \mathcal{A}_{p,\infty} \to \mathrm{End}(L_1) \otimes \mathbb{Q}$ specified by a $\mathbb{Z}$-basis $\{r_i\}$ of R which maps to a $\mathbb{Z}$-basis $\{e_i\}$ of $\mathrm{End}(L_1)$. (For more detail, see A.0.3 in Appendix A and the examples in Appendix B.) For any isogeny $\varphi : L_1 \to E$, we define the isomorphism $i_\varphi : \mathcal{A}_{p,\infty} \to \mathrm{End}(E) \otimes \mathbb{Q}$ by

$$i_\varphi : \alpha \mapsto \varphi i(\alpha)\widehat{\varphi} \otimes (\deg \varphi\ )^{-1}.$$

The left ideals J_i of R define curves $E_i = L_1/L_1[J_i]$ with $R_r(J_i) \simeq \mathrm{End}(E_i)$. As discussed in the remark 2.2.1, we make the choice of isogenous curve E_i such that the isogeny $\varphi_{J_i} : L_1 \to E_i$ is *normalized*. The isogeny φ_{J_i} defines an isomorphism denoted i_{J_i}. Note that the curves E_i are not necessarily in Legendre form.

Fix a pair (L, f) of $\mathrm{LegEmb}_D(\mathbb{F}_{p^2})$ and an ideal $\mathfrak{a}$. The following algorithm computes the unique curve $L^{\mathfrak{a}}$ in Legendre form such that the isogeny $L \to L^{\mathfrak{a}}$ with kernel $L[f(\mathfrak{a})]$ fixes the two-torsion. To compute $f^{\mathfrak{a}}$, we use Algorithm 2.3.1 which returns the value $g^{\mathfrak{a}}(\tau) = w$, an element of $R_r(J_m)$ where $E_m \simeq L^{\mathfrak{a}}$. The value $g^{\mathfrak{a}}(\tau)$ is only determined up to conjugation by units of $R_r(J_m)$. If $j(L^{\mathfrak{a}}) \neq 0, 1728$, the value $g^{\mathfrak{a}}(\tau)$ is uniquely determined. For $j(L^{\mathfrak{a}}) = 0$ or 1728, however, there are three, respectively two, choices of $g^{\mathfrak{a}}(\tau)$, only one of which gives the embedding $f^{\mathfrak{a}}$ into $\mathrm{End}(L^{\mathfrak{a}})$. This ambiguity is addressed in Step 5.

The expression we obtain for $f^{\mathfrak{a}}(\tau)$ gives an endomorphism of the curve $L^{\mathfrak{a}}$ in terms of the basis of endomorphisms $\{e_i\}$ for L_1 and an isogeny $L_1 \to L^{\mathfrak{a}}$. By factoring $L_1 \to L^{\mathfrak{a}}$ through the isogeny $L_1 \to E_m$, we control the denominators in the expression of $f^{\mathfrak{a}}(\tau)$ so that they are at most a power of ℓ. Thus, for any ideal $\mathfrak{a}$ and for any element $\beta \in \mathcal{O}$ with norm prime to ℓ, we can compute the kernel of the endomorphism $f^{\mathfrak{a}}(\beta)$ by computing the kernel of $\ell^d \cdot f^{\mathfrak{a}}(\beta)$ for some d.

Algorithm 2.8.1

INPUT:

- A supersingular curve L in Legendre form with $\mathrm{End}(L) \simeq R_r(J_k)$
- A basis $\{r_i\}$ of R
- The data

  1. $g(\tau) = [y_1, ..., y_4] \in R_r(J_k)$ expressed in terms of the basis $\{r_i\}$ of R
  2. γ, an isomorphism $E_k \to L$

  specifying an optimal embedding $f : \mathcal{O} \hookrightarrow \mathrm{End}(L)$, given by $f(\tau) = i_\varphi \circ g(\tau)$ where $\varphi = \gamma \circ \varphi_{J_k}$

- An ideal $\mathfrak{a}$ of $Cl(\mathcal{O}_2)$ with $\mathfrak{a} = (a, c + d\tau)$ and $n(\mathfrak{a}) = a$ where $(a, \ell) = 1$

OUTPUT:

- The curve $L^{\mathfrak{a}}$
- The data

  1. $g^{\mathfrak{a}}(\tau) = [w_1, ..., w_4] \in R_r(J_m)$ expressed in terms of the basis $\{r_i\}$ of R
  2. γ, an isomorphism $E_m \to L^{\mathfrak{a}}$
  3. δ, an automorphism of $L^{\mathfrak{a}}$

  specifying the embedding $f^{\mathfrak{a}}$ as given by $f^{\mathfrak{a}}(\tau) = i_\varphi \circ g^{\mathfrak{a}}(\tau)$ where $\varphi = \delta \circ \gamma \circ \varphi_{J_m}$

- The polynomial $P(X)$ whose roots are the distinct x-coordinates of the affine points of the kernel $L[f(\mathfrak{a})]$
- The curve $E = L/L[f(\mathfrak{a})]$ and the two-torsion points (P, Q), the image of $((0,0),(1,0))$ under the isogeny $L \xrightarrow{\mathfrak{a}} E$.

The last two outputs are a by-product of the computations $L^{\mathfrak{a}}$ and are used in the algorithm to compute the canonical lift in Section 2.8.7.

1. Using Algorithm 2.3.1, compute $g^{\mathfrak{a}}(\tau) = w \in R_r(J_m)$, with $w = [w_1, ..., w_4]$ in terms of $\{r_i\}$.

2. Compute the subgroup $L[f(\mathfrak{a})]$ by checking which points $Q_i \in L[a]$ are in the kernel of $f(c + d\tau)$. Let $P(X) = \prod_{n=1}^{(a-1)/2}(X - x(Q_i))$, the polynomial whose roots are the x-coordinates of $L[f(\mathfrak{a})]$.

3. Compute $\varphi_{\mathfrak{a}} : L \to E$, the isogeny with kernel $L[f(\mathfrak{a})]$, and (P, Q), the image of $((0,0),(1,0))$ under $\varphi_{\mathfrak{a}}$. Compute

   $$\lambda^{\mathfrak{a}} = \frac{x(P+Q) - x(P)}{x(Q) - x(P)}$$

   and an isomorphism $h : E \to L^{\mathfrak{a}}$ with $(x, y) \mapsto (u^2 x + r, u^3 y)$ for

   $$u = \pm \frac{1}{\sqrt{x(Q) - x(P)}} \text{ and } r = \frac{-x(P)}{x(Q) - x(P)}.$$

   Let $\psi = h\varphi_{\mathfrak{a}} : L \to L^{\mathfrak{a}}$.

4. If $j(L^{\mathfrak{a}}) \neq 0, 1728$, compute the isomorphism $\gamma : E_m \to L^{\mathfrak{a}}$ (unique up to ± 1) and let $\varphi = \gamma \circ \varphi_{J_m}$. Return $L^{\mathfrak{a}}$ and $f^{\mathfrak{a}} = i_{\varphi} \circ g^{\mathfrak{a}}$.

5. If $j(L^{\mathfrak{a}}) = 0$ or 1728, choose an arbitrary isomorphism $\gamma : E_m \to L^{\mathfrak{a}}$. For each automorphism $\delta \in \operatorname{Aut}(L^{\mathfrak{a}})$, let $\varphi = \delta\gamma\varphi_{J_m}$ and determine if
$$i_\varphi(g^{\mathfrak{a}}(\tau))\psi = \psi f(\tau) \tag{2.14}$$
as isogenies $L \to L^{\mathfrak{a}}$. Choose the unique δ (up to ± 1) for which this holds, and return $L^{\mathfrak{a}}$ and $f^{\mathfrak{a}} = i_\varphi \circ g^{\mathfrak{a}}$.

We now give a more detailed description of the algorithm, as well as justification of the fact that Step 5 yields the embedding $f^{\mathfrak{a}}$. In Step 3, we use Vélu's formulas to compute $\varphi_{\mathfrak{a}} : L \to E$. By the proof of Proposition 2.5.1, the curve with λ-invariant $\lambda^{\mathfrak{a}}$ is $L^{\mathfrak{a}}$, the unique curve in Legendre form isomorphic to E such that there exists an isomorphism $E \to L^{\mathfrak{a}}$ sending (P, Q) to $((0, 0), (1, 0))$. Either choice of square root for u is valid, as the automorphism $-\mathrm{Id}$ fixes the two-torsion.

In Steps 4 and 5, the curve E is isomorphic to E_m but not necessarily equal. Since in Step 1, we have computed the value $g^{\mathfrak{a}}(\tau)$ with respect to the set $\operatorname{Emb}_D(\mathcal{A}_{p,\infty})$ which depends on the fixed set $\{E_i\}$ of representatives of isomorphism classes, we factor the isogeny $L_1 \to L^{\mathfrak{a}}$ through E_m. If $p = 3, 5, 7$ or 13, there is a unique isomorphism class of supersingular curves over $\mathbb{F}_{p^2}$. Thus $E_m = L$ and φ_{J_m} is just the identity.

In Step 5, letting $\varphi = \gamma \circ \varphi_{J_m}$, we have that $i_\varphi(g^{\mathfrak{a}}(\tau))\psi = \psi f(\tau)$ up to conjugation by an automorphism $\delta \in \operatorname{Aut}(L^{\mathfrak{a}})$. The goal of Step 5 is to determine the correct δ, up to ± 1.

Let $\phi = i_\varphi(g^{\mathfrak{a}}(\tau))$. For any $\delta, \delta' \in \operatorname{Aut}(L^{\mathfrak{a}})$ with $\delta \neq \pm\delta'$, the endomorphisms $\delta\phi\delta^{-1}$ and $\delta'\phi\delta'^{-1}$ are distinct. Thus there exists some positive integer s, relatively prime to a and ℓ, such that $\delta\phi\delta^{-1}$ and $\delta'\phi\delta'^{-1}$ are not equal on $L^{\mathfrak{a}}[s]$ for all pairs δ, δ' with

$\delta \neq \pm\delta'$.

This implies that there is a unique δ up to ± 1 such that (2.14) holds for points of $L^{\mathfrak{a}}[s]$. We then check each δ until we obtain one for which this is true. As $(s, a \cdot \ell) = 1$, we can do this by checking that

$$a \cdot \delta\big(\varphi_{J_m} i(w) \widehat{\varphi}_{J_m}\big)\delta^{-1} \circ \psi = \ell^d \cdot \big(\psi \circ f(\tau)\big) \tag{2.15}$$

on $L[s]$, where ℓ^d is the maximum of $n(J_m)$ and the denominators of the $\{w_i\}$.

To choose an appropriate s, for each pair of automorphisms with $\delta \neq \pm\delta'$, we compute the difference of $\delta\phi\delta^{-1}$ and $\delta'\phi\delta'^{-1}$ expressed in terms of the basis $\{e_i\}$. For $p \neq 3$ and $j = 1728$, there is two automorphisms up to ± 1, and thus a single difference. For $j = 0$, there are three automorphisms up to ± 1 and thus three differences. If $p = 3$, there are six automorphisms up to ± 1 and thus fifteen differences.

Let m be the smallest absolute value of the numerators of the terms in each of the differences. Choose a positive integer s relatively prime to m, ℓ and a. By the choice of s and the fact that the denominators of the terms contain at most powers of ℓ, the differences are not equal to zero modulo s. Hence the corresponding pairs of endomorphisms are not equivalent on $L^{\mathfrak{a}}[s]$.

This approach gives an upper bound on s, the smallest positive integer such that $\delta\phi\delta^{-1}$ and $\delta'\phi\delta'^{-1}$ are not equal on $L^{\mathfrak{a}}[s]$. The terms of any embedding with respect to the basis are each bounded by $n(\tau)$, the norm of the embedding. Thus the terms in the differences of conjugate endomorphisms are bounded by $2n(\tau)$. For any $s > 2n(\tau)$, the differences are not equal to zero modulo s, and hence the corresponding conjugate endomorphisms are not equivalent on $L^{\mathfrak{a}}[s]$.

There is a better bound on s for large enough $n(\tau)$, as follows. If the differences are zero modulo $r = 2, 3, 5...$ for a sequence of relatively prime integers, then they are zero modulo the product of these primes. For large x, the product of primes less than x is approximately e^x by the Prime Number theorem. More specifically, by [34, Cor. to Thm. 4], for $x \geq 41$,

$$\sum_{p \leq x} \log p > x(1 - 1/(\log x)).$$

Thus solving $x(1 - 1/(\log x)) = \log 2n(\tau)$ for x, we have that the product of primes less than x is greater than $2n(\tau)$. Thus there is a prime $s < x$ such that the differences are not equal to zero modulo s and no pair of conjugate embeddings give endomorphisms which are equal on $L^{\mathfrak{a}}[s]$.

Alternately, we may determine the correct automorphism δ by simply trying primes $r = 2, 3, ...$, coprime to $a \cdot \ell$, in consecutive order, and testing for each δ whether the condition (2.15) holds on $L[r]$. We discard those that fail on any given s until only one δ remains.

For practical implementation, we want to use a small s. For instance, in the case that $s = 2$, the algorithm simplifies, as we know that the isogeny ψ fixes the two-torsion. We present this simplified variant of the algorithm, followed by an example. We then give a characterization, in terms of D and the characteristic polynomial of τ, of the cases when $s = 2$ suffices.

Algorithm 2.8.1, $s = 2$ **Variant**:

The input is the same as in Algorithm 2.8.1, assuming we have chosen the ideal class representatives J_i to have norm a power of $\ell \neq 2$. Steps 1, 2 and 4 remain the same. In Step 3, there is no need to calculate the isomorphism h. Step 5 is replaced by the following step.

Choose an arbitrary isomorphism $\gamma : E_m \to L^{\mathfrak{a}}$. For each $\delta \in \operatorname{Aut}(L^{\mathfrak{a}})$, let $\varphi = \delta\gamma\varphi_{J_m}$. Since the conjugate endomorphisms are not equal on $L^{\mathfrak{a}}[2]$, to check condition (2.14) from Step 7 of Algorithm 2.8.1, it suffices to verify that

$$i_\varphi(g^{\mathfrak{a}}(\tau))\psi \equiv \psi f(\tau) \bmod 2.$$

Since $\psi : L \to L^{\mathfrak{a}}$ fixes the two-torsion $((0,0),(1,0))$, this is equivalent to checking that $i_\varphi(g^{\mathfrak{a}}(\tau))$ and $f(\tau)$ evaluated on the two torsion of $L^{\mathfrak{a}}$ and L, respectively, give the same result. We check this for each $\delta \in \operatorname{Aut}(L^{\mathfrak{a}})/\{\pm 1\}$ until we find one for which this is true. The following example illustrates this variant.

2.8.6 Example

Let $p = 7$ and $D = -23$. We work with $\mathbb{F}_{p^2} = \mathbb{F}_p(a)$ where $a^2 = -2$. The order $\mathcal{O}$ of discriminant D can be written as $\mathbb{Z}[\tau]$ where τ is a root of $X^2 - X + 6 = 0$.

Let L be the curve $y^2 = x(x-1)(x-2)$ with $j(L) = 1728$. We fix a maximal order R with $R \simeq \operatorname{End}(L)$. (See Appendix B for the explicit bases of R and $\operatorname{End}(L)$). As there is a unique conjugacy class of maximal orders of $\mathcal{A}_{7,\infty}$, all embeddings of $\operatorname{Emb}_D(\mathbb{F}_{p^2})$ are embeddings into R.

Let $f : \mathcal{O} \hookrightarrow \operatorname{End}(L)$ be the embedding given by the data $g(\tau) = [0, -1, -1, 1]$, in terms of the basis of R and the isomorphism $i : R \to \operatorname{End}(L)$. Recall that $g(\tau)$ gives an embedding $\mathcal{O} \hookrightarrow R$ and the embedding f is given by the endomorphism $i(g(\tau))$. As D is fundamental, the embedding f is optimal. Furthermore, as $D \equiv 9 \mod 16$, we are able to use the $s = 2$ variant of Algorithm 2.8.1, by Proposition 2.8.5 below.

Given $\mathfrak{a} = (3, 1 + 2\tau)$, an ideal of $\mathcal{O}_K$ relatively prime to 2, we compute the action of $\mathfrak{a}$ on (L, f). In Step 1, we use Algorithm 2.3.1 to compute $g^{\mathfrak{a}}(\tau) = [0, -2, 1, 1] \in R$.

In Step 2, we check which points of $L[3]$ are killed by $1 + 2f(\tau)$. This yields the points with x-coordinate $5a + 5$. Thus $P(X) = X + 2a + 2$ is the kernel polynomial of $L[f(\mathfrak{a})]$.

In Step 3, using Vélu's formulas, we obtain the isogenous curve $E = L/L[f(\mathfrak{a})]$ with $y^2 = x^3 + 4ax$. The images of $(0, 0)$ and $(1, 0)$ under the isogeny are $P = (0, 0)$ and $Q = (5a + 1, 0)$ respectively. The point $P + Q = (2a + 6, 0)$ and we compute $\lambda = 6$. Thus $L^{\mathfrak{a}}$ is the curve given by $y^2 = x(x - 1)(x - 6)$. The isomorphism $(x, y) \mapsto ((a + 4)x, (3a + 3)y)$ sends E to the curve $L^{\mathfrak{a}}$ and the basis (P, Q) to $((0, 0), (1, 0))$.

As $j(L^{\mathfrak{a}}) = 1728$, we go to Step 5. We choose the isomorphism $\gamma : L \to L^{\mathfrak{a}}$ given by $(x, y) \mapsto (x + 6, y)$. The following chart gives the value of the endomorphism $f(\tau)$ of L evaluated on the non-trivial points of $L[2]$. Here P_∞ denotes the identity of the group $L(\mathbb{F}_{p^2})$.

P	$f(\tau)(P)$
$(0, 0)$	$(0, 0)$
$(1, 0)$	P_∞
$(2, 0)$	$(0, 0)$

Similarly, the following chart gives the value of endomorphism $i_\gamma(g^{\mathfrak{a}}(\tau))$ of $L^{\mathfrak{a}}$ evaluated on the non-trivial points of $L^{\mathfrak{a}}[2]$. Here P_∞ denotes the identity of the group $L^{\mathfrak{a}}(\mathbb{F}_{p^2})$.

P	$i_\gamma(g^{\mathfrak{a}}(\tau))(P)$
$(0,0)$	$(0,0)$
$(1,0)$	P_∞
$(6,0)$	$(0,0)$

As they agree, the correct automorphism is $\delta = \mathrm{Id}$ and the embedding $f^{\mathfrak{a}}$ is given by $i_\gamma(g^{\mathfrak{a}}(\tau))$, where $g^{\mathfrak{a}}(\tau) = [0, -2, 1, 1]$ and γ is the isomorphism above.

As a check, we consider the non-trivial automorphism of $L^{\mathfrak{a}}$ given (up to ± 1) by $\delta : (x, y) \to (6x, 2ay)$. Conjugating by δ, we get the embedding $\delta i_\gamma(g^{\mathfrak{a}}(\tau))\delta^{-1}$ and we evaluate it on the non-trivial points of $L^{\mathfrak{a}}[2]$.

P	$\delta(i_\gamma(g^{\mathfrak{a}}(\tau)))\delta^{-1}(P)$
$(0,0)$	$(0,0)$
$(1,0)$	$(0,0)$
$(6,0)$	P_∞

As this doesn't agree with the values of $f(\tau)$ on $L[2]$, this confirms that we have identified the correct embedding automorphism as $\delta = \mathrm{Id}$.

Let L be supersingular curve with $j(L) = 0$ or 1728 such that the order $\mathcal{O}$ of discriminant D embeds in $\mathrm{End}(L)$. The following proposition describes for which discriminants D the endomorphisms corresponding to conjugate embeddings are distinguishable on the 2-torsion of the curve L.

Proposition 2.8.5 *Let L be a supersingular curve in Legendre form over $\mathbb{F}_{p^2}$ with $j(L) =$ 0 or 1728. Let $\mathcal{O} = \mathbb{Z}[\tau]$ be the order of discriminant $D < -4$, and let $T(X) = X^2 -$*

$tX + n$ be the characteristic polynomial of τ. Let ϕ be an element of $\mathrm{End}(L)$ *with characteristic polynomial $T(X)$. Let $\delta \in \mathrm{Aut}(L)$ be any automorphism with $\delta \neq \pm\mathrm{Id}$. Assume $\phi \not\equiv 0 \bmod 2$ and one of the following cases is true*

$$T(X) \equiv \begin{cases} X^2 + X \bmod 2 & \textit{and } j(L^{\mathfrak{a}}) = 0 \textit{ or } 1728 \\ X^2 + X + 1 \bmod 2 & \textit{and } j(L^{\mathfrak{a}}) = 1728 \\ X^2 + 1 \bmod 2 & \textit{and } j(L^{\mathfrak{a}}) = 0. \end{cases}$$

Then $\phi\delta \neq \delta\phi$ on $L[2]$. Furthermore, these are conditions are necessary for $\phi\delta \not\equiv \delta\phi \bmod 2$, except in the last case.

Proof: Let P_0, P_1, P_2 be the non-trivial two-torsion points of L. If $\phi \equiv 0 \bmod 2$, then ϕ kills the two-torsion and thus $\delta\phi \equiv \phi\delta \bmod 2$. Therefore, in order that $\delta\phi \not\equiv \phi\delta \bmod 2$, we must have that $\phi \not\equiv 0 \bmod 2$.

Case 1: If $T(X) \equiv X^2 + X \bmod 2$, then $\phi^2 \equiv \phi$ on $L[2]$ and ϕ kills a point of two-torsion of L. Without loss of generality, let $\phi(P_0) = P_\infty$ and $\phi(P_1) = \phi(P_2) = P_1$.

If $j(L) = 1728$, the non-trivial automorphism δ (up to ± 1) is a permutation of order 2 on the non-trivial points of $L[2]$. Thus δ fixes one non-trivial two-torsion point and permutes the other two. If $\delta(P_0) = P_0$, then $\delta\phi\delta^{-1}(P_2) = P_2$. If $\delta(P_1) = P_1$, then $\delta\phi\delta^{-1}(P_2) = P_\infty$. If $\delta(P_2) = P_2$, then $\delta\phi\delta^{-1}(P_2) = P_0$. In all cases, $\delta\phi\delta^{-1}(P_2)$ is not equal to $\phi(P_2) = P_1$. Therefore $\phi\delta \neq \delta\phi$ on $L[2]$.

If $j(L) = 0$, any non-trivial automorphism δ of L gives a permutation of order 3 and thus does not fix any two-torsion point. We show for each possibility for δ that $\delta\phi\delta^{-1}(P_0) \neq \phi(P_0)$, and therefore $\phi\delta \neq \delta\phi$ on $L[2]$. If $\delta(P_0) = P_1$, then

$\delta\phi\delta^{-1}(P_0) = P_2$. If $\delta(P_0) = P_2$, then $\delta\phi\delta^{-1}(P_0) = P_0$. In both cases, $\delta\phi\delta^{-1}(P_0)$ is not equal to $\phi(P_0) = P_\infty$.

Case 2: Suppose $T(X) \equiv X^2 + X + 1 \bmod 2$. Since $2 \nmid n$, the endomorphism ϕ acts as a permutation on $L[2]$. Writing $[n] = \phi\widehat{\phi}$, we have $\phi^2 + \phi + \phi\widehat{\phi} \equiv 0 \bmod 2$, and thus $\widehat{\phi} \equiv 1 + \phi$ on $L[2]$. If $\phi(P_i) = P_i$ for any i, then $\widehat{\phi}(P_i) = P_\infty$, which is a contradiction. Thus ϕ is a permutation of order 3 on the non-trival points of $L[2]$.

For $j = 0$, the non-trivial automorphisms of L are permutations non-trivial two-torsion of order 3. Therefore δ commutes with ϕ and $\phi\delta \equiv \delta\phi \bmod 2$.

For $j = 1728$, the non-trivial automorphism of L gives an order 2 permutation. Thus ϕ and δ do not commute and $\phi\delta \neq \delta\phi$ on $L[2]$.

Case 3: If $T(X) \equiv X^2 + 1 \bmod 2$, then $\phi^2 \equiv 1$ on $L[2]$. This implies that ϕ is an order 2 permutation of the non-trivial points of $L[2]$. If $j = 0$, then δ is an order 3 permutation of the non-trivial points of $L[2]$. Therefore, $\phi\delta \not\equiv \delta\phi \bmod 2$, as δ and ϕ do not commute.

If $j = 1728$, then δ is an order 2 permutation as well. If δ and ϕ are the same order 2 permutation, then $\delta\phi = \phi\delta$ on $L[2]$. However, if δ and ϕ are not the same permutation, then there exists i such that $\delta\phi\delta^{-1}(P_i) \neq \phi(P_i)$. Thus the condition $T(X) \equiv X^2 + 1 \bmod 2$ and $j(L) = 0$ is sufficient, but not necessary to guarantee $\phi\delta \not\equiv \delta\phi \bmod 2$. $\square$

For D a fundamental discriminant, we may write $\mathcal{O} = \mathbb{Z}[\tau]$ where the characteristic polynomial of τ is

$$T(X) = \begin{cases} X^2 - X + \frac{1-D}{4} & \text{for } D \equiv 1 \bmod 4 \\ X^2 + \frac{D}{4} & \text{for } D \equiv 0 \bmod 4. \end{cases}$$

It is straightforward to verify that

$$D \equiv \begin{cases} 9 \bmod 16 & \text{iff } T(X) \equiv X^2 + X \bmod 2 \text{ and } 4 \nmid n \\ 5 \bmod 8 & \text{iff } T(X) \equiv X^2 + X + 1 \bmod 2 \\ 4 \bmod 8 & \text{iff } T(X) \equiv X^2 + 1 \bmod 2. \end{cases}$$

In particular, this implies that in the case of $D \equiv 9 \bmod 16$, with D a fundamental discriminant, we may always use the $s = 2$ variant of Algorithm 2.8.1, regardless of whether the curves with j-invariant 0 or 1728 are supersingular over $\mathbb{F}_{p^2}$.

2.8.7 An algorithm to compute the canonical lift of (L, f)

We now present the algorithm to compute the canonical lift of the pair (L, f) of the set $\mathrm{LegEmb}_D(\mathbb{F}_{p^2})$ to a specified p-adic accuracy for $p \not\equiv 1 \mod 12$. We use "accuracy" to mean how p-adically close the computed value is to the actual value in terms of the number of p-adic digits to which they agree. We use "precision" to mean the number of p-adic digits which we keep track of in computations. The overall structure of the algorithm is the same as Algorithm 2.4.1 for $p \equiv 1 \bmod 12$. However, some technical details differ as we are working with the Legendre form.

Algorithm 2.8.2

INPUT:

- L, a supersingular curve modulo p with $p \not\equiv 1 \bmod 12$
- A maximal order R of $\mathcal{A}_{p,\infty}$ with $\mathrm{End}(L) \simeq R$ and a basis $\{r_i\}$ of R
- An explicit isomorphism $i : R \to \mathrm{End}(L)$ specified by an identification of bases $\{r_i\}$ of R and $\{e_i\}$ of $\mathrm{End}(L)$
- An optimal embedding $f : \mathcal{O} = \mathbb{Z}[\tau] \hookrightarrow \mathrm{End}(E)$ given by $f(\tau) = y = [y_1, ..., y_4]$ expressed in terms of $\{e_i\}$
- $r \in \mathbb{Z}^+$ such that 2^r is greater than or equal to the desired p-adic accuracy

OUTPUT: The canonical lift $\tilde{\lambda}$ of (L, f) to 2^r p-adic digits accuracy.

1. Choose $\alpha = a + b\tau \in \mathbb{Z}[\tau]$ satisfying the following:

   (a) $\alpha \equiv 1 \bmod 2$

   (b) $\frac{\alpha}{\bar{\alpha}} - 1$ is a p-adic unit

   by searching the set

   $S_A = \{a+b\tau \mid a, b \in \mathbb{Z}, a+b\tau \text{ prime to } D, a \text{ odd}, b \text{ even}, b \not\equiv 0 \bmod p \text{ and } n(a+b\tau) \leq A\}$

   where the bound A is greater than $n(\tau)$. If the set is empty, we increase A until this is not the case. Let $\prod_{i=1}^{m} \mathfrak{b}_i$ be the factorization of α into prime ideals and let $\mathfrak{a}_n = \prod_{i=1}^{n} \mathfrak{b}_i$ for $1 \leq n \leq m$.

2. Choose the smallest prime ℓ relatively prime to $2p \cdot n(\alpha)$. Compute $\{J_i\}$, a set of left R-ideal class representatives, each with norm a power of ℓ. This determines the set $\mathrm{Emb}_D(\mathcal{A}_{p,\infty})$ used in the setup of Algorithm 2.8.1. Compute the corresponding set of elliptic curves $E_i = L/L[i(J_i)]$.

3. Using Algorithm 2.8.1 with input (L, f) and the ideal $\mathfrak{b}_1 = \mathfrak{a}_1$, compute $(L^{\mathfrak{a}_1}, f^{\mathfrak{a}_1})$. Store the following by-products of the computation:

   - $P_1(X)$, the polynomial whose roots are the distinct x-coordinates of the points of the subgroup $L[f(\mathfrak{b}_1)]$
   - $E_{(1)} = L/L[f(\mathfrak{b}_1)]$, the isogenous curve
   - (P_1, Q_1) the image of $((0,0),(1,0))$ under the isogeny $L \to E_{(1)}$.

   Similarly, for $n = 1, ..., m-1$, use Algorithm 2.8.1 with input $(L^{\mathfrak{a}_n}, f^{\mathfrak{a}_n})$ and $\mathfrak{b}_{n+1}$ to compute $(L^{\mathfrak{a}_{n+1}}, f^{\mathfrak{a}_{n+1}})$. Store the polynomial $P_n(X)$ corresponding to the subgroup $L^{\mathfrak{a}_n}[f^{\mathfrak{a}_n}(\mathfrak{b}_{n+1})]$, the isogenous curve $E_{(n)} = L^{\mathfrak{a}_n}/L^{\mathfrak{a}_n}[f^{\mathfrak{a}_n}(\mathfrak{b}_{n+1})]$, and (P_n, Q_n) the image of $((0,0),(1,0))$ under the isogeny $L \to E_{(n)}$. In this way, obtain the cycle of isogenies

$$L \xrightarrow{\mathfrak{b}_1} E_{(1)} \simeq L^{\mathfrak{a}_1} \xrightarrow{\mathfrak{b}_2} E_{(2)} \simeq L^{\mathfrak{a}_2} ... \xrightarrow{\mathfrak{b}_m} E_{(m)} \simeq L^{(\alpha)} = L. \tag{2.16}$$

4. Let λ_0 be an arbitrary lift of $\lambda(L)$ to 2 digits precision.

5. For $k = 0, 1, ..., r-1$, repeat the following four steps. In the k^{th} iteration, work to 2^{k+1} digits precision and obtain λ_{k+1}, which is the value $\tilde{\lambda}$ to 2^{k+1} digit accuracy.

(a) Let L_k be the curve $y^2 = x(x-1)(x-\lambda_k)$ and compute the isogeny

$$L_k \xrightarrow{\mathfrak{b}_1} E_{k,1}$$

with kernel $L_k[\mathfrak{b}_1]$.

(b) Lift the two torsion (P_1, Q_1) of $E_{(1)}$ to $(P_{k,1}, Q_{k,1})$ in $E_{k,1}[2]$. Let

$$\lambda_k^{\mathfrak{a}_1} = \frac{x(P_{k,1}+Q_{k,1}) - x(P_{k,1})}{x(Q_{k,1}) - x(P_{k,1})}.$$

This is $\rho_{\mathfrak{a}_1}(\lambda_k)$ to 2^{k+1} digits accuracy. Let $L_k^{\mathfrak{a}_1}$ be the curve with λ-invariant $\lambda_k^{\mathfrak{a}_1}$.

(c) Lift the remaining $m-1$ isogenies of (2.16) one at a time as in Steps 5a and 5b to obtain the cycle of isogenies

$$L_k \xrightarrow{\mathfrak{b}_1} L_k^{\mathfrak{a}_1} \xrightarrow{\mathfrak{b}_2} L_k^{\mathfrak{a}_2} \ldots \xrightarrow{\mathfrak{b}_m} L_k^{(\alpha)}. \tag{2.17}$$

The λ-invariant of $L_k^{(\alpha)}$ is $\rho_\alpha(\lambda_k)$ to 2^{k+1} digits accuracy.

(d) Compute

$$\lambda_{k+1} = \lambda_k - \frac{\rho_\alpha(\lambda_k) - \lambda_k}{\alpha/\bar{\alpha} - 1}$$

to obtain λ_{k+1}, which is the value $\tilde{\lambda}$ to 2^{k+1} digit accuracy.

6. Return λ_{r-1}, the value $\tilde{\lambda}$ to 2^r digit accuracy.

In Step 1, we want α not only to satisfy the given conditions but to factor into the product of ideals of small norm, as discussed in Algorithm 2.4.1. To find such an α, we fix $A > n(\tau)$ and $B = 20$ and search the set

$$S_A = \{a + b\tau \mid a, b \in \mathbb{Z}, a + b\tau \text{ prime to } D, a \text{ odd}, b \text{ even}, b \not\equiv 0 \bmod p, n(a+b\tau) \leq A\}$$

for elements α such that $n(\alpha)$ is B-smooth. That is, the smallest prime factor of $n(\alpha)$ is less than B. The condition a is odd and b is even ensures that $a + b\tau \equiv 1 \bmod 2$. The condition $b \not\equiv 0 \bmod p$ ensures that $\frac{\alpha}{\bar{\alpha}} - 1$ is a p-adic unit, since $p \nmid D$ implies that $\tau \not\equiv \bar{\tau} \bmod p$. We also may impose the condition $\gcd(a, b) = 1$. If there are no such α we may increase either A, B or both until we find an α satisfying the conditions. (There are more sophisticated sieving methods that could be used to improve the efficiency of this search.)

As discussed in Remark 2.4.1, we can obtain a heuristic upper bound on the size of A needed to find a B-smooth element $\alpha = a + b\tau$ where $B = \lfloor \exp \sqrt{\log |D|} \rfloor$. However, in this algorithm, we also require that a is even and b is odd. Arguing heuristically, this holds for a fourth of the B-smooth elements of the set S defined in Lemma 2.4.1.

In Step 2, we use the algorithm in [44, 9] to compute a set of left ideal class representatives $\{J_i\}$ of R of norm a power of ℓ. Each J_i is given by a basis β_k of four elements of R. For each J_i, we compute the subgroup of L corresponding to the ideal $i(J_i)$ of $\mathrm{End}(E)$ by checking which points of $L[\ell^d]$ are killed by $i(\beta_k)$ for all k. Then we use Vélu's formulas to compute the isogenous curve $E_i = L/L[J_i]$. For $p = 3, 5$ or 7, there is a single isomorphism class of supersingular elliptic curves over $\mathbb{F}_{p^2}$ and Step 2 is not necessary.

Throughout Step 5, the precision for computations in the k^{th} iteration should be 2^{k+1} as we are computing λ_{k+1} to that accuracy. In Step 5a, to compute the isogeny $L_k \xrightarrow{\mathfrak{b}_1} E_{k,1}$ with kernel $L_k[\mathfrak{b}_1]$, we use Hensel's lemma to lift the kernel polynomial $P_1(X)$ to a factor of the N-division polynomial of L_k where N is the norm of $\mathfrak{b}_1$. We use Vélu's formulas to compute $E_{k,1} = L_k/L_k[\mathfrak{b}_1]$.

In Step 5b, to lift (P_1, Q_1) to $(P_{k,1}, Q_{k,1})$ we use Hensel's lemma. Let $y^2 = f(x)$ denote the Weierstrass equation for $E_{k,1}$. We lift the x-coordinates of P_1 and Q_1 to roots of $f(x)$ to obtain the x-coordinates of $P_{k,1}$ and $Q_{k,1}$. As $x(P_{k,1}) \not\equiv x(Q_{k,1}) \bmod p$, no p-adic accuracy is lost in the division required to compute $\lambda_k^{\mathfrak{a}_1}$. Thus this value is equal to $\rho_{\mathfrak{a}_1}(\lambda_k)$ to 2^{k+1} digits accuracy.

For Step 5c, given $\lambda_k^{\mathfrak{a}_{i-1}}$, we compute $\lambda_k^{\mathfrak{a}_i}$ in the same way as in Steps 5a and 5b. In this way, we compute the cycle of λ-invariants

$$\lambda_k \overset{\mathfrak{b}_1}{\to} \lambda_k^{\mathfrak{a}_1} \overset{\mathfrak{b}_2}{\to} \lambda_k^{\mathfrak{a}_2}, ..., \overset{\mathfrak{b}_m}{\to} \lambda_k^{(\alpha)}$$

and $\lambda_k^{(\alpha)}$ is $\rho_\alpha(\lambda_k)$ to 2^{k+1} digits accuracy.

Remark 2.8.1

For calculation purposes, we must determine the correct embedding of $\mathcal{O} = \mathbb{Z}[\tau]$ into F, given by a root of $T(X) = X^2 - tX + n$, the minimal polynomial of τ. This is in order to be able to compute the value $\alpha/\bar{\alpha}$, where $\alpha = a + b\tau$, as an element of F in Step 5d of Algorithm 2.8.2. As f is a normalized embedding, the correct choice of root of $T(X)$ in $\mathbb{F}_{p^2}$ is c such that $f(\tau)^*\omega = c\omega$ for $\omega = \frac{dx}{y}$. Therefore, we can choose one of the two roots c modulo p and verify whether or not this holds. For the correct one, we then lift it to a root of $T(X)$ modulo $p^{2^{k+1}}$.

To check the differential condition, we choose a point P of L not of order 2, and check that

$$\frac{dx \circ f(\tau)}{dx} \frac{1}{(y \circ f(\tau))}(P) = \frac{c}{y(P)}.$$

This requires explicitly obtaining the x-coordinate of the endomorphism $f(\tau)$. For large

D, this coordinate is a ratio of polynomials of large degree. However, we may write $f(\tau) = \sum_{i=1}^{4} b_i e_i$, where e_i are the basis for $\mathrm{End}(L)$. Then by the linearization property of the differential, we have that $f(\tau)^*\omega = \sum_{i=1}^{4} b_i(e_i^*\omega)$, and we check whether

$$\sum_{i=1}^{4} b_i \frac{dx \circ e_i}{dx} \frac{1}{(y \circ e_i)}(P) = \frac{c}{y(P)}.$$

It is feasible to obtain the x-coordinates of the endomorphism e_i as the basis endomorphisms are generally of small degree.

Alternatively, we can choose a root of $T(X)$ in $\mathbb{F}_{p^2}$ arbitrarily. We have a one-half chance of choosing the correct root, and if we choose the incorrect root, we will detect this in the k^{th} iteration where k is such that 2^k is greater than the valuation of $\lambda_0 - \tilde{\lambda}$. In particular, if $a_1 = \alpha/\bar{\alpha}$ and we have chosen the incorrect root, the Newton's method update in Step 5d will use $\bar{a}_1$. Since $\tau \not\equiv \bar{\tau}$ when viewed as elements of $\mathbb{F}_{p^2}$ under the reduction map $\mathcal{O} \to \mathcal{O}/(p) \simeq \mathbb{F}_{p^2}$, we have that $a_1 - 1$ is invertible in F. Therefore $(a_1 - 1)/(\bar{a}_1 - 1)$ is invertible in $\mathbb{Z}_F$. Then

$$\lambda_{k+1} - \lambda_k = (\lambda_k - \tilde{\lambda})\big((a_1 - 1)/(\bar{a}_1 - 1)\big) + \sum_{i \geq 2} a_i(\bar{a}_1 - 1)^{-1}(\lambda_k - \tilde{\lambda})^i$$

and its valuation is thus equal to that of $\lambda_k - \tilde{\lambda}$. As this holds for any k, we see that $\lambda_{k+1} - \lambda_k$ can never have valuation greater than that of the starting valuation of $\lambda_0 - \tilde{\lambda}$. Thus once we reach the end of the k^{th} iteration for k such that 2^k is greater than the valuation of $\lambda_0 - \tilde{\lambda}$, we will detect that we've chosen the incorrect root, since by Corollary 2.8.4, we know we should have that the valuation of $\lambda_{k+1} - \lambda_k$ is at least 2^k. In that case, we choose the conjugate root $\bar{c}$.

We now give a detailed example of Algorithm 2.8.2 for $p = 7$ and $D = -23$.

2.8.7.1 Example

Let $p = 7$ and $D = -23$. We work with $\mathbb{F}_{p^2} = \mathbb{F}_p(a)$ where $a^2 = -2$. We let $F = \mathbb{Q}_p(\tilde{a})$ where $\tilde{a}$ is the unique lift of $a \in \mathbb{F}_{p^2}$ to a root of $X^2 + 2 = 0$. The order $\mathcal{O}$ of discriminant D can be written as $\mathbb{Z}[\tau]$ with τ a root of $X^2 - X + 6 = 0$.

We compute the canonical lift of (L, f) where L is the curve with $\lambda(L) = 2$ and $f(\tau) = [0, -1, -1, 1]$ specifies an optimal embedding of $\mathcal{O} = \mathbb{Z}[\tau]$ into $\mathrm{End}(L)$. We compute the canonical lift $\tilde{\lambda}$ to 16 p-adic digits accuracy.

In Step 1, we choose $\alpha = 1 + 2\tau$ which factors as $(\alpha) = \prod_{i=1}^{3} \mathfrak{a}$ for $\mathfrak{a} = (3, 1 + 2\tau)$. Since $p = 7$, there is a unique class of supersingular elliptic curves and Step 2 is unnecessary. In Step 5, we use the $s = 2$ variant of Algorithm 2.8.1. In Example 2.8.6, we computed the action of $\mathfrak{a}$ on (L, f) and obtained $P_1(X) = X + 2a + 2$ as the kernel polynomial of $L[f(\mathfrak{a})]$. We also computed that $L^{\mathfrak{a}}$ is the curve $y^2 = x(x-1)(x-6)$ and the embedding $f^{\mathfrak{a}}$ is given by $i_\gamma(g^{\mathfrak{a}}(\tau))$ where $g^{\mathfrak{a}}(\tau) = [0, -2, 1, 1]$ and γ is the isomorphism $(x, y) \mapsto (x + 6, y)$.

Similarly, we use Algorithm 2.8.1 with input $(L^{\mathfrak{a}}, f^{\mathfrak{a}})$ and $\mathfrak{a}$. Checking which 3-torsion points of $L^{\mathfrak{a}}$ are killed by $1 + 2 \cdot i_\gamma(g^{\mathfrak{a}}(\tau))$, we see that the kernel of $L^{\mathfrak{a}}[f^{\mathfrak{a}}(\mathfrak{a})]$ is generated by the point with x-coordinate $2a + 4$. Thus $P_2(X) = X + 5a + 3$. We also get that the curve $L^{\mathfrak{a}^2}$ is $y^2 = x(x-1)(x-4)$ and $f^{\mathfrak{a}^2}$ is specified by the isomorphism $\gamma : (x, y) \mapsto (4x, y)$, and the automorphism of $L^{\mathfrak{a}^2}$ $\delta : (x, y) \mapsto (6x + 1, 5ay)$, and $g^{\mathfrak{a}^2}(\tau) = [1, 2, 0, -1]$. Using this, we can determine that the kernel polynomial $P_3(X)$ is $X + a + 5$. Thus Step 3 yields the sequence of kernel polynomials

$$[X + 2a + 2, X + 5a + 3, X + a + 5].$$

We also obtain (P_i, Q_i), the image of the two torsion, for $i = 1, 2, 3$:

$$(1, 5a + 2), (2a + 1, 5a + 6), (a + 1, 4).$$

In Step 4, we choose $\lambda_0 = 9$ as a lift of $\lambda(L) = 2$. In Step 5, to compute $\tilde{\lambda}$ to 16 digits accuracy, we do iterations for $k = 0, 1, 2, 3$. As the value of τ, we use the lift of $3a + 4 \in \mathbb{F}_{p^2}$ to a root of $T(X)$ to 2^{k+1} accuracy. (The value $3a + 4$ is determined by trial and error as discussed in Remark 2.8.1.)

For $k = 0, 1, 2, 3$, we compute the following sequence of isogenies using Steps 5a, b and c.

$$L_k \xrightarrow{\mathfrak{a}} L_k^{\mathfrak{a}} \xrightarrow{\mathfrak{a}} L_k^{\mathfrak{a}^2} \xrightarrow{\mathfrak{a}} L_k^{\mathfrak{a}^3=(\alpha)} \tag{2.18}$$

Let $k = 0$. In Step 5b, we Hensel lift $P_1(X)$ to a factor of the 3-division polynomial of the curve L_0 given by $y^2 = x(x - 1)(x - 9)$. This yields an isogeny to the curve $E_{0,1}$ given by $y^2 = x^3 - 10x^2 + (11\tilde{a} + 3)x + (24\tilde{a} - 22)$. The two torsion (P_1, Q_1) lifts to $((21\tilde{a} - 20, 0), (-16\tilde{a} + 16, 0))$ and we compute $\lambda_0^{\mathfrak{a}} = 14\tilde{a} + 3$.

In Step 5c, we compute the rest of the cycle in the same way to get

$$\lambda_0^{\mathfrak{a}} = 14\tilde{a} + 3,\ \lambda_0^{\mathfrak{a}^2} = 7\tilde{a} + 4,\ \lambda_0^{\mathfrak{a}^3} = -19.$$

The value of $\rho_\alpha(\lambda_0)$ is $-19 + O(7^2)$. For Step 5d, we use the Newton's method update to get $\lambda_1 = -14\tilde{a} - 5 + O(7^2)$.

The results of the other iterations are recorded below.

k	λ_k	$\rho_\alpha(\lambda_k)$
0	$9 + O(7^2)$	$-19 + O(7^2)$
1	$-14\tilde{a} - 5 + O(7^2)$	$-700\tilde{a} - 250 + O(7^4)$
2	$-308\tilde{a} + 975 + O(7^4)$	$-2759057\tilde{a} - 2169529 + O(7^8)$
3	$-1589770\tilde{a} + 2769328 + O(7^8)$	$-8713440653260\tilde{a} - 14503366061721 + O(7^{16})$

The value of λ_4 is $103548953808858\tilde{a} - 11703056327961 + O(7^{16})$.

The following chart gives the j-invariants corresponding to the λ_k as well as the p-adic valuation of the differences between the values in the iterations k and $k-1$. This shows the quadratic convergence of λ_k to $\tilde{\lambda}$.

k	$j(\lambda_k)$	$v_p(\lambda_k - \lambda_{k-1})$	$v_p(j_k - j_{k-1})$
0	$13 + O(7^2)$		
1	$13 + O(7^2)$	1	2
2	$-833\tilde{a} - 673 + O(7^4)$	2	3
3	$-1520666\tilde{a} + 1286263 + O(7^8)$	4	5
4	$70060245474445\tilde{a} + 9359259476181 + O(7^{16})$	8	9

The value λ_4 is the 16 digit approximation to the λ-invariant of the canonical lift $\tilde{L}$ of (L, f). The value j_4 is therefore a 16 digit approximation to the j-invariant of $\tilde{L}$. To confirm this, we compute the polynomial $H_{-23}(X)$ using the complex analytic method as implemented in MAGMA. We then see that $H_{-23}(j_4)$ has valuation 20, while $H'_{-23}(j_4)$ has valuation 4. Therefore, by Hensel's lemma [25, Prop. II.2.2], j_4 lifts uniquely to a root of $H_{-23}(X)$ and is in fact a 20 digit approximation to $\tilde{j}$.

For completeness, we give an algorithm to compute the canonical lift of (L, f) for $p \equiv 1 \bmod 12$. If $p \equiv 1 \bmod 12$, the set of supersingular curves over $\mathbb{F}_{p^2}$ does not include any curve with $j = 0$ or 1728. In this case, we use the algorithm from Section 2.4 to compute the j-invariant of the canonical lift $\tilde{L}$ of (L, f) and choose the root of $P_{j(\tilde{L})}(X)$ which reduces to λ. This will be $\tilde{\lambda}$, the λ-invariant of the canonical lift of (L, f).

Algorithm 2.8.3

INPUT:

- L, a supersingular curve modulo p, where $p \equiv 1 \bmod 12$
- A maximal order R of $\mathcal{A}_{p,\infty}$ with $\mathrm{End}(L) \simeq R$ and a basis $\{r_i\}$ of R
- An explicit isomorphism $i : R \to \mathrm{End}(L)$ specified by an identification of bases $\{r_i\}$ of R and $\{e_i\}$ of $\mathrm{End}(L)$
- An optimal embedding $f : \mathcal{O} = \mathbb{Z}[\tau] \hookrightarrow \mathrm{End}(E)$, given by $f(\tau) = y = [y_1, ..., y_4]$, expressed in terms of $\{e_i\}$
- $r \in \mathbb{Z}^+$ such that 2^r is the desired p-adic accuracy

OUTPUT: The canonical lift $\tilde{\lambda}$ of (L, f) to precision p^{2^r}.

1. Use Algorithm 2.4.1 from Section 2.4 to compute $j(\tilde{L})$, the j-invariant of the canonical lift of (L, f) to precision p^{2^r}.
2. Use Hensel's lemma to lift $\lambda(L)$ to a unique root of $P_{j(\tilde{E})}(X)$ in F to 2^r digits accuracy

Note that we can use Hensel's lemma in Step 2 since $j(L) \neq 0, 1728$ implies that $P_{j(\tilde{E})}(X)$ factors into six distinct linear terms in $\mathbb{F}_{p^2}$.

2.9 A p-adic algorithm to compute H_D for p inert with respect to D

Let $D < -4$ be an imaginary quadratic discriminant. In this section, we give a p-adic algorithm to compute the class polynomial $H_D(X)$ of the order $\mathcal{O}$ of discriminant D. Let p be the smallest prime inert with respect to D. There are two variants of the algorithm, depending on whether or not $p \equiv 1 \bmod 12$.

The algorithm presented in this section is modeled after the p-adic algorithm in [5, Sec. 7] where p is a prime splitting in $\mathcal{O}$. The key step is to compute the canonical lift $\tilde{j}$ of (E, f) to sufficient accuracy. Approximations to the other roots of $H_D(X)$ are then computed using the action of $Cl(\mathcal{O})$ on $\tilde{j}$. In [5], for an ideal $\mathfrak{a} \in Cl(\mathcal{O})$ of prime norm N, the value $\tilde{j}^{\mathfrak{a}}$ is computed by determining the correct root in $\mathbb{F}_p$ of the modular polynomial $\phi_N(\tilde{j}, X) \in \mathbb{F}_p[X]$ and Hensel lifting it to sufficient p-adic accuracy. This is feasible as the polynomial has exactly two distinct roots modulo p.

In the case of p inert, the situation is more delicate as the polynomial $\phi_N(\tilde{j}, X)$ factors completely in $\mathbb{F}_{p^2}[X]$ and is in general not separable. Thus in the following algorithm, we compute the Galois conjugate $\tilde{j}^{\mathfrak{a}}$ by directly applying the map $\rho_{\mathfrak{a}}$ from Section 2.8.1.

Algorithm 2.9.1

INPUT:

- An imaginary quadratic discriminant $D < -4$
- A prime p with $p \equiv 1 \bmod 12$

OUTPUT: The class polynomial $H_D(X) \in \mathbb{Z}[X]$

1. Let $Cl(\mathcal{O}) = \bigoplus_{k=1}^{m} \langle \mathfrak{a}_k \rangle$ be a decomposition of the class group into a direct product of cyclic groups generated by integral prime ideals $\mathfrak{a}_k$ of order h_k and norm ℓ_k not dividing p. Let $\alpha_k = (\mathfrak{a}_k)^{h_k}$.

2. Using Algorithm A.0.2, compute a maximal order R of $\mathcal{A}_{p,\infty}$ into which $\mathcal{O}$ optimally embeds and the embedding $g : \mathcal{O} \hookrightarrow R$ given by $g(\tau) = [w_1, ..., w_4]$ expressed in terms of a basis $\{r_i\}$ for R.

3. Using Algorithm A.0.1, compute the correspondence between the $Gal(\mathbb{F}_{p^2}/\mathbb{F}_p)$-conjugacy classes of supersingular j-invariants over $\mathbb{F}_{p^2}$ and the conjugacy classes of maximal orders of $\mathcal{A}_{p,\infty}$. Select j, a j-invariant in the list corresponding to R.

4. Choose a curve E in Weierstrass form with j-invariant j and fix an isomorphism $i : R \to \mathrm{End}(E)$ using Algorithm A.0.3. Let $f(\tau) = i(g(\tau))$ specify the embedding $f : \mathcal{O} \hookrightarrow \mathrm{End}(E)$.

5. Choose a small prime ℓ relatively prime to $p \cdot \prod \ell_k$. Compute $\{J_i\}$, a set of left R-ideal class representatives, each with norm a prime power of ℓ, and the corresponding set of elliptic curves $E_i = E/E[i(J_i)]$. This determines the set $\mathrm{Emb}_D(\mathcal{A}_{p,\infty})$ used in the set up of Algorithm 2.8.1.

6. Let r be the smallest integer such that 2^r is greater than $\log_p 10 \cdot C + \log_p 2$ where C is the constant (2.1). Use Algorithm 2.4.1 to compute the canonical lift $\tilde{j}$ of (E, f) to 2^r digits accuracy.

7. Working to 2^r digits precision, let $\tilde{E}$ be a curve with j-invariant $\tilde{j}$. Compute $\rho_{\alpha_i}((\tilde{j}, f))$ as in Algorithm 2.4.1 to obtain the set S of pairs of j-invariants and embeddings

$$S = \{(\tilde{j}, f), (\tilde{j}^{\mathfrak{a}_1}, f^{\mathfrak{a}_1}), (\tilde{j}^{\mathfrak{a}_1^2}, f^{\mathfrak{a}_1^2}), ..., (\tilde{j}^{\mathfrak{a}_1^{h_1-1}}, f^{\mathfrak{a}_1^{h_1-1}})\}.$$

The j-invariant $\tilde{j}^{\mathfrak{a}_1^i}$ is the canonical lift of $(E^{\mathfrak{a}_1^i}, f^{\mathfrak{a}_1^i})$ to 2^r digits accuracy.

8. For $k = 2, ..., m$ do the following. For each pair (j, f) in S, compute $\rho_{\alpha_k}(j, f)$ to obtain the pairs $(j^{\mathfrak{a}_k^i}, f^{\mathfrak{a}_k^i})$ for $i = 1, ..., h_k - 1$. At the end of the k^{th} iteration, add these all to the set S, which now contains $h_1 h_2 ... h_k$ pairs. The first coordinate of each pair is a distinct root of $H_D(X)$ computed to 2^r digits accuracy.

9. Working to 2^r digits precision, expand $H_D(X) = \prod_{(j,f)\in S}(X - j)$ and recognize the coefficients as integers between $-p^{2^r}$ and p^{2^r}. Return $H_D(X)$.

For Step 1, there is a bound on the generators of $Cl(\mathcal{O})$. Assuming GRH, the norm of $\mathfrak{a}_i$ is bounded by $O((\log |D|)^2)$ [7, p. 249]. In Step 6, the $\log_p 2$ term in the lower bound on 2^r comes from the fact that the coefficients of $H_D(X)$ have absolute value less than 10^C and thus lie in a range of size $2 \cdot 10^C$.

If there exists k such that $\alpha_k/\bar{\alpha}_k - 1$ is a p-adic unit, then in Step 6 we can compute the canonical lift using the map ρ_{α_k}. Without loss of generality, we may assume $k = 1$. If we compute $\tilde{j}$ to 2^{r+1} digits accuracy, we obtain as a by-product of Algorithm 2.4.1

the pairs $(\tilde{j}^{\mathfrak{a}_1^i}, f^{\mathfrak{a}_1^i})$ where $\tilde{j}^{\mathfrak{a}_1^i}$ is accurate to 2^r digits. Thus this replaces Step 7. However, there is not guaranteed to be such a k in which case we compute the canonical lift in Step 6 by finding an α satisfying the conditions that $\alpha/\bar{\alpha}-1$ is invertible and use the map ρ_α to compute $\tilde{j}$.

The algorithm for $p \not\equiv 1 \bmod 12$ is analogous except that in Steps 6, 7 and 8, we compute $\tilde{\lambda}$, the λ-invariant of the canonical lift of (L, f), and the Galois conjugates of $\tilde{\lambda}$. We then compute $j(\tilde{\lambda}^{\mathfrak{a}})$ for each $\mathfrak{a} \in Cl(\mathcal{O})$ and proceed as in Step 9. In Step 1, we have to use a decomposition of $Cl(\mathcal{O})$ into ideals of odd norm. We can replace Step 7 as described above, provided that $\alpha_k \equiv 1 \bmod 2$. We give the algorithm for completeness.

Algorithm 2.9.2

INPUT:

- An imaginary quadratic discriminant $D < -4$
- A prime p with $p \not\equiv 1 \bmod 12$

OUTPUT: The class polynomial $H_D(X) \in \mathbb{Z}[X]$

1. Let $Cl(\mathcal{O}) = \bigoplus \langle \mathfrak{a}_k \rangle$ be a decomposition of the class group into a direct product of cyclic groups generated by integral prime ideals $\mathfrak{a}_k$ of order h_k and norm ℓ_k prime to $2p$. Let $\alpha_k = (\mathfrak{a}_k)^{h_k}$.
2. Using Algorithm A.0.2, compute a maximal order R of $\mathcal{A}_{p,\infty}$ into which $\mathcal{O}$ optimally embeds and the embedding $g : \mathcal{O} \hookrightarrow R$ given by $g(\tau) = [w_1, ..., w_4]$ expressed in terms of a basis $\{r_i\}$ for R.

3. Using Algorithm A.0.1, compute the correspondence between the $Gal(\mathbb{F}_{p^2}/\mathbb{F}_p)$-conjugacy classes of supersingular j-invariants over $\mathbb{F}_{p^2}$ and the conjugacy classes of maximal orders of $\mathcal{A}_{p,\infty}$. Select j, a j-invariant in the list corresponding to R.

4. Choose a curve L in Legendre form with j-invariant j and fix an isomorphism $i : R \to \mathrm{End}(L)$ using Algorithm A.0.3. Let $f(\tau) = i(g(\tau))$ specify the embedding $f : \mathcal{O} \hookrightarrow \mathrm{End}(L)$.

5. Choose a small prime $\ell \neq 2$ relatively prime to $p \cdot \prod_k \ell_k$. Compute $\{J_i\}$, a set of left R-ideal class representatives, each with norm a prime power of ℓ, and the corresponding set of elliptic curves $E_i = L/L[i(J_i)]$. This determines the set $\mathrm{Emb}_D(\mathcal{A}_{p,\infty})$ used in the set up of Algorithm 2.8.1.

6. Let r be the smallest integer such that 2^r is greater than $\log_p 10 \cdot C + \log_p 2$ where C is the constant (2.1). Use Algorithm 2.8.2 to compute the canonical lift $\tilde{\lambda}$ of (L, f) to 2^r digits accuracy.

7. Working to 2^r digits precision, let $\tilde{L}$ be a curve with λ-invariant $\tilde{\lambda}$. Compute $\rho_{\alpha_i}((\tilde{\lambda}, f))$ as in Algorithm 2.4.1 to obtain the set S of pairs of λ-invariants and embeddings

$$S = \{(\tilde{\lambda}, f), (\tilde{\lambda}^{\mathfrak{a}_1}, f^{\mathfrak{a}_1}), (\tilde{\lambda}^{\mathfrak{a}_1^2}, f^{\mathfrak{a}_1^2}), ..., (\tilde{\lambda}^{\mathfrak{a}_1^{h_1-1}}, f^{\mathfrak{a}_1^{h_1-1}})\}.$$

   The λ-invariant $\tilde{\lambda}^{\mathfrak{a}_1^i}$ is the canonical lift of $(L^{\mathfrak{a}_1^i}, f^{\mathfrak{a}_1^i})$ to 2^r digits accuracy.

8. For $k = 2, ..., m$ do the following. For each pair (λ, f) in S, compute $\rho_{\alpha_k}(\lambda, f)$ to obtain the pairs $(\lambda^{\mathfrak{a}_k^i}, f^{\mathfrak{a}_k^i})$ for $i = 1, ..., h_k - 1$. At the end of the k^{th} iteration,

add these pairs to the set S, which now contains $h_1h_2...h_k$ pairs. The j-invariant of the first coordinate of each pair is a distinct root of $H_D(X)$ computed to 2^r digits accuracy.

9. Working to 2^r digits precision, expand $H_D(X) = \prod_{(\lambda,f)\in S}(X - j(\lambda))$ and recognize the coefficients as integers between $-p^{2^r}$ and p^{2^r}. Return $H_D(X)$.

We remark that in the case of $p = 3, 5, 7, 13$, Steps 3 and 5 of the respective algorithms are not necessary since there is a unique class of supersingular elliptic curves over $\mathbb{F}_{p^2}$.

2.9.1 Example

In this section, we give an example of the algorithm to compute the class polynomial of the order $\mathcal{O}$ of discriminant $D = -4 \cdot 903$. This is the order of conductor two of the field $K = \mathbb{Q}(\sqrt{-903})$. We write it as $\mathcal{O} = \mathbb{Z}[\tau]$ where τ is a root of $T(X) = X^2 + 903$.

The smallest prime inert in K is $p = 5$. As p does not divide D, we may compute $H_D(X)$ 5-adically using Algorithm 2.9.2 since $p \not\equiv 1 \bmod 12$. Steps 3 and 5 of the algorithm are not necessary as there is a unique isomorphism class of supersingular curves over $\mathbb{F}_{p^2}$, namely that with $j = 0$.

The class group of $\mathcal{O}$ is non-cyclic generated by $\mathfrak{a}_1 = (3, 3+\tau)$ and $\mathfrak{a}_2 = (29, 5+\tau)$ of orders 2 and 8, respectively.

The quaternion algebra $\mathcal{A}_{p,\infty}$ for $p = 5$ can be given by $\left(\frac{-2,-5}{\mathbb{Q}}\right)$, where

$$i^2 = -2, j^2 = -5, ij = k, ij = -ji.$$

The single conjugacy class of maximal orders of $\mathcal{A}_{p,\infty}$ has the representative R with basis

$$\{r_1, ..., r_4\} = \{1, 1/2 + i/4 - k/4, 1/2 - 3i/4 - k/4, -1/4i - j/2 - k/4\}.$$

The map $g : \mathcal{O} \to \mathcal{A}_{p,\infty}$ given by $g(\tau) = [-5, -13, 23, 0]$ is an embedding of $\mathcal{O}$ into the order R. As the greatest common divisor of the terms is one, this embedding is optimal.

Let $\mathbb{F}_{p^2} = \mathbb{F}_p(a)$ where a is a root of $X^2 + 2 = 0$. There are two curves in Legendre form with $j = 0$:

$$L : y^2 = x(x - 1)(x - (a + 3))$$

$$L' : y^2 = x(x - 1)(x - (4a + 3)).$$

We choose L and fix an isomorphism $i : R \to \mathrm{End}(E)$ as given in Appendix B. The embedding $f : \mathcal{O} \to \mathrm{End}(E)$ is given by $f(\tau) = i(g(\tau))$.

We compute the constant (2.1) for D and from determine that the necessary p-adic accuracy is 10 digits. Therefore we let $r = 4$ and use Algorithm 2.8.2 to compute $\tilde{\lambda}$ to 16 p-adic digits accuracy.

We note that $\mathfrak{a}_1^2 = (3)$ and $\mathfrak{a}_2^8 = (16900\tau - 475381)$. As $\alpha/\bar{\alpha} - 1$ is not a p-adic unit for either α_1 or α_2, we cannot use either of these values for the map ρ_α when computing the canonical lift. Thus we search the set S_A from Step 1 of Algorithm 2.8.2 for B-smooth elements where $B = 20$ and $A = 20000$.

We find $\alpha = 45 + 5\tau$ of norm $16473 = 3 \cdot 17^2 \cdot 19$. The ideal (α) factors as $\mathfrak{b}_1\mathfrak{b}_2^2\mathfrak{b}_3$ where $\mathfrak{b}_1 = (3, \tau)$, $\mathfrak{b}_2 = (17, 7 + \tau)$, and $\mathfrak{a}_3 = (19, 16 + \tau)$.

The action of $\mathfrak{a}$ on the pair (L, f) yields the sequence of curves

$$L \xrightarrow{\mathfrak{b}_1} L' \xrightarrow{\mathfrak{b}_2} L' \xrightarrow{\mathfrak{b}_2} L \xrightarrow{\mathfrak{b}_3} L$$

with embeddings given by

$$([-5,-13,23,0],\mathrm{Id}),([-17,35,-1,0],\gamma),([11,-1,-21,24],\gamma),([-5,25,-15,12],\mathrm{Id})$$

where $\gamma : L \to L'$ is the isomorphism given by $(4x+1, 3y)$. We also obtain the sequence of kernel polynomials

$$\begin{array}{cc}
P_1 & X+2a+2 \\
P_2 & X^8+(4a+4)X^7+(3a+1)X^6+(2a+1)X^5+(3a+3)X^4+ \\
 & (a+2)X^3+(2a+4)X^2+(3a+1)X+3a+3 \\
P_3 & X^8+(4a+2)X^7+4X^6+(4a+2)X^5+2aX^4+3aX^3+ \\
 & (3a+4)X^2+2aX+4a+4 \\
P_4 & X^9+2X^8+(4a+4)X^7+(a+4)X^6+(2a+2)X^5+3aX^4+ \\
 & 2X^3+3X^2+3X+1
\end{array}$$

and the sequence of two-torsion

$$[(3a+4,3a+2),(a+3,4a+4),(a+3,4a+2),(4a+1,4a)].$$

Let $F = \mathbb{Q}_p(\tilde{a})$ where $\tilde{a}$ is the lift of the root a of $X^2+2=0$. We choose $\lambda_0 = \tilde{a}+8$ as a lift of $\lambda(L) = a+3$. As the value of τ, we use the lift of $2a \in \mathbb{F}_{p^2}$ to a root of $T(X)$ to 2^{k+1} accuracy. Lifting the kernel polynomials and two-torsion data, we compute the canonical lift of (L, f) to 16 p-adic digits precision and obtain $\tilde{\lambda} = -118663765559\tilde{a} - 76293945312 + O(5^{16})$.

We now compute the action of $\mathfrak{a}_1 = (3, \tau+3)$ on $\tilde{\lambda}$ to obtain $\tilde{\lambda}^{\mathfrak{a}_1} = 135182576669\tilde{a} - 76293945312 + O(5^{16})$. The curve $L^{\mathfrak{a}_1}$ in characteristic p is L' and the embedding $f^{\mathfrak{a}_1}$ is specified by $g^{\mathfrak{a}_1}(\tau) = [-17,35,-1,0]$ and the isomorphism $\gamma : L \to L'$. The S in Step 7 of Algorithm 2.9.2 is thus

$$S = \{(\tilde{\lambda}, f), (\tilde{\lambda}^{\mathfrak{a}_1}, f^{\mathfrak{a}_1})\}.$$

We next compute the value ρ_{α_2} of each of the pairs of S to obtain 16 total pairs. For each pair, the j-invariant of the first coordinate is a 16 p-adic digit approximation to a distinct root of $H_D(X)$. Expanding the product and recognizing the coefficients as integers between -5^{16} and 5^{16}, we obtain the polynomial $H_D(X)$ of degree 16. The largest coefficient of $H_D(X)$ is 187 digits.

Chapter 3

A Weil pairing on the p-torsion of ordinary elliptic curves over $K[\epsilon]$

3.1 Introduction

Let E be an elliptic curve over K, an algebraically closed field of characteristic $p > 0$. For n relatively prime to p, the Weil pairing is a bilinear, non-degenerate map

$$e_n : E[n] \times E[n] \to \mu_n(K) \tag{3.1}$$

where $E[n] \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ is the n-torsion subgroup of E and $\mu_n(K)$ is the group of n^{th} roots of unity of K [38]. The Weil pairing is a useful tool in both the theory and application of elliptic curves.

In fact, the Weil pairing may be defined for any n, regardless of the characteristic of K, via a group scheme interpretation, as we briefly mention now. Let S be any scheme. Let $E[n]$ denote the kernel of the multiplication-by-n map on the scheme E. Let μ_n denote the kernel of the multiplication-by-n map on $\mathbb{G}_m$, the group scheme of invertible elements. As explained in [22, pp. 87-89], Cartier duality gives the following isomorphism of group schemes over S:

$$E[n] \xrightarrow{\sim} Hom(E[n], \mu_n). \tag{3.2}$$

Therefore, for any $n \in \mathbb{N}$, and any scheme S, the Weil pairing exists as an isomorphism of group schemes. Let $S = \text{Spec } K$, where K is a field of characteristic p. For n relatively prime to p, this isomorphism is equivalent to the existence and non-degeneracy of the classical Weil pairing (3.1).

For $n = p$, however, if we extend the classical definition to the p-torsion of E, an ordinary elliptic curve, the resulting map e_p is degenerate. This is true for two reasons: K contains no non-trivial p^{th} roots of unity and $E[p] \simeq \mathbb{Z}/p\mathbb{Z}$. Each of these facts implies that $e_p(P, Q) = 1$ for all $P, Q \in E[p](K)$. (Note that the second implies degeneracy since the Weil pairing is bilinear and anti-symmetric).

As the utility of the Weil pairing hinges on its non-degeneracy, we would like to have an explicitly defined non-degenerate Weil pairing on $E[p]$. The purpose of this paper is to concretely develop such a pairing by extending the classical definition to the curve E over the ring of dual numbers $K[\epsilon]$. Through this deformation of K, we have substitutes for the "missing" geometric points of both $E[p]$ and μ_p and thus are able to define a non-degenerate "Weil pairing" on p-torsion. In the process, we demonstrate that the discrete logarithm attacks on p-torsion subgroups of [35] and [36] are essentially Weil-pairing-based attacks, no different than the MOV attacks on n-torsion subgroups for $(n, p) = 1$. (For more on the MOV attack, see [28]).

In section 3.2.1, we give an introduction to elliptic curves over the dual numbers. In sections 3.2.2 and 3.2.3, we recall Miller's algorithm for computing the Weil pairing and Semaev's algorithm for solving the discrete log problem (DLP) on p-subgroups of elliptic curves. In sections 3.3 and 3.4, we define the "Weil pairing on p-torsion," e_p, over the dual numbers, show its direct relation to Semaev's algorithm, and prove that it satisfies the basic properties of the classical Weil pairing. We also describe how e_p can be used to solve the DLP on p-torsion subgroups of an elliptic curve. In section 3.5, we give a simple way to compute the pairing using the algorithm of Rück defined in [35]. In section 3.6, we describe how the map e_p behaves with respect to isogenies of elliptic curves. In the last section, we give another application of elliptic curves over the dual numbers, namely a DLP attack on anomalous curves, analogous to that of Smart in [39].

3.2 Preliminaries

3.2.1 Elliptic Curves over the Dual Numbers

The *ring of dual numbers* of the ring R is $R[x]/(x^2)$, denoted $R[\epsilon]$ with $\epsilon^2 = 0$. Considering elliptic curves over the dual numbers was proposed in [43], where Virat introduced a cryptosystem based on elliptic curves over $\mathbb{F}_q[\epsilon]$, the dual numbers of $\mathbb{F}_q$.

Let K be a field of characteristic $p \neq 0, 2, 3$. Let E be the elliptic curve over K given by the Weierstrass equation $y^2 = x^3 + Ax + B$. Let $\tilde{A} = A + A_1\epsilon$ and $\tilde{B} = B + B_1\epsilon$, for some $A_1, B_1 \in K$. We call the curve $y^2 = x^3 + \tilde{A}x + \tilde{B}$ a *lift of E to* $K[\epsilon]$, and denote it as $\tilde{E}$.

The set of points $\tilde{E}(\bar{K}[\epsilon])$ consists of two sets:

- *Affine Points:* $P = (x_0 + x_1\epsilon : y_0 + y_1\epsilon : 1)$ such that

$$(x_0, y_0) \in E(\overline{K}) \text{ and } (2y_0)y_1 = (3x_0^2 + A)x_1 + A_1x_0 + B_1.$$

- *Points at Infinity:* $\mathcal{O}_k = (k\epsilon : 1 : 0)$ for all $k \in \overline{K}$.

Let Θ denote the set $\{\mathcal{O}_k | k \in \overline{K}\}$ and let P_∞ denote $\mathcal{O}_0$. The standard addition law for elliptic curves may be extended to give an addition law on $\tilde{E}(\bar{K}[\epsilon])$ (see [45], p. 61). An easy calculation shows that

$$\begin{array}{ccc} \overline{K}^{+} & \to & \Theta \\ k & \mapsto & \mathcal{O}_k \end{array}$$

is an isomorphism. Thus, $\tilde{E}(\bar{K}[\epsilon])$ contains the p-torsion subgroup Θ, and there is an exact sequence

$$0 \to \Theta \to \tilde{E}(\bar{K}[\epsilon]) \to E(\overline{K}) \to 0.$$

If $\tilde{A} = A$ and $\tilde{B} = B$, we call $\tilde{E}$ the *canonical lift* of E, since the p-torsion points $E[p]$ remain p-torsion points in $\tilde{E}$. (Though not immediately obvious, this terminology is consistent with the definition of the canonical lift $\tilde{E}$ of an ordinary elliptic curve E to $\overline{\mathbb{Q}}_p$ from Chapter 2. For more on this alternate characterization of the canonical lift, see [8, Thm. 17.29].) For the remainder of the paper (except in Section 3.7), we will assume we are in this situation. In this case, the sequence splits and every point of $\tilde{E}$ may be decomposed as a point of $E(\overline{K})$ and a point of infinity. A straightforward calculation using the addition laws gives the following lemma. (Note that $3x_0^2 + A \neq 0$ for points of order 2, since the curve is non-singular.)

Lemma 3.2.1 *Let $\tilde{P} \in \tilde{E}(\bar{K}[\epsilon])$ with $\tilde{P} = (x_0 + x_1\epsilon : y_0 + y_1\epsilon : 1)$. Then there exists a unique $k \in \overline{K}$ such that $\tilde{P} = P + \mathcal{O}_k$, with $P = (x_0 : y_0 : 1) \in E(\overline{K})$. Furthermore*

$$k = \begin{cases} -\frac{x_1}{2y_0} & \textit{if } y_0 \neq 0 \\ \\ -\frac{y_1}{3x_0^2+A} & \textit{if } y_0 = 0. \end{cases}$$

Note that if $y_0 \neq 0$, the point (x_1, y_1) lies on the line through the origin with slope $\frac{3x_0^2+A}{2y_0}$, which is precisely the tangent space of the elliptic curve point (x_0, y_0). Thus points of $\tilde{E}(\bar{K}[\epsilon])$ may be thought of as points of $E(\overline{K})$ with extra "derivative" information. (In fact, the set of points of $\tilde{E}(\bar{K}[\epsilon])$ may be naturally identified with the tangent bundle of the variety E.)

The canonical lift $\tilde{E}$ has p-torsion $\tilde{E}[p] = E[p] \oplus \Theta$. Furthermore, $\mu_p(\bar{K}[\epsilon])$ has non-trivial p^{th} roots of unity, in particular the subgroup $\{1 + a\epsilon : a \in \overline{K}\}$. Thus we will see that it is possible to define a non-degenerate "Weil pairing" on the p-torsion of $\tilde{E}$. Before we proceed we recall Miller's algorithm for computing the Weil pairing.

3.2.2 Miller's algorithm for computing the Weil pairing

Let $(n, p) = 1$. Let $P, Q \in E[n]$, and let D_P, D_Q be divisors with disjoint support which sum to P, Q respectively. Let f_P, f_Q be functions with divisors nD_P, nD_Q respectively. The Weil pairing is defined as

$$e_n(P, Q) = \frac{f_Q(D_P)}{f_P(D_Q)}.$$

This definition is independent of the choices of divisors by Weil reciprocity. In [30], Miller gives a way to compute the value $f_P(D_Q)$. As this will be the foundation for the definition of the "Weil pairing on p-torsion," we recall the details here.

Let $P, Q \in E[n]$. Choose any two points $T, R \in E(K)$ such that the divisors $D_P = (P+T) - (T)$ and $D_Q = (Q+R) - (R)$ are disjoint. Let f_P be the function with divisor nD_P. Note that this function is unique only up to a non-zero constant. Following [30], in such situations, we choose the unique function with the value 1 at P_∞, which we call the *normalized* function. (Note that since we are calculating the ratio $f_P(Q+R)/f_P(R)$, such constants may in fact be disregarded.)

For $k \in \mathbb{N}$, let f_k denote the (normalized) function with

$$\text{div }(f_k) = k(P+T) - k(T) - (kP+T) + (T).$$

Note that div $(f_1) = 0$, so $f_1 \equiv 1$. Also note that div $(f_P) =$ div (f_n) and div $(f_{i+j}) =$ div $(f_i f_j h_{i,j})$ where

$$\text{div }(h_{i,j}) = -((i+j)P+T) + (iP+T) + (jP+T) - (T).$$

Thus $f_P(Q) = f_n(Q)$ can be calculated recursively by using an addition chain decomposition for n.

An addition chain for a positive integer n is an increasing sequence of integers $S \subset \{1, ..., n\}$ such that for each $k \in S$ with $k > 1$, there exist $i, j \in S$ such that $i + j = k$. Given an addition chain S, an *addition chain decomposition* C of n is a sequence of steps of the form $(k \mapsto i, j)$ with $i+j = k$ and $i, j, k \in S$ which decomposes n into the sum of n ones: $\underbrace{1 + ... + 1}_{n}$. Note that any decomposition will consist of exactly $n - 1$ steps.

Thus, since $f_k(Q) = f_i(Q) f_j(Q) h_{i,j}(Q)$ and $f_1 \equiv 1$, $f_n(Q)$ will be the product of $n - 1$ contributions of the form $h_{i,j}(Q)$. For example, if $n = 11$ and $S = \{1, 2, 4, 8, 10, 11\}$, then one possible decomposition is

$$f_{11} = f_1 f_{10} h_{1,10} = f_1 f_2 f_8 h_{1,10} h_{2,8} = ... = f_1^{11} h_{1,10} h_{2,8} h_{4,4} h_{2,2}^2 h_{1,1}^5.$$

Given an addition chain decomposition C for n, we write $\prod_C h_{i,j}(Q)$ to denote the value $f_n(Q)$. Note that there always exists a decomposition with $O(\log n)$ distinct $h_{i,j}$.

Let $\ell_{i,j}$ denote the line through iP and jP, and let v_i denote the vertical line through

iP. Note that

$$\text{div}\,(\ell_{i,j}) = (iP) + (jP) + (-(i+j)P) - 3P_\infty \text{ and } \text{div}\,(v_i) = (iP) + (-iP) - 2P_\infty.$$

Let τ denote translation by $-T$. Then

$$h_{i,j} = \begin{cases} \frac{\ell_{i,j}}{v_{i+j}} \circ \tau & i+j \neq n, \\ \\ v_i \circ \tau & i+j = n. \end{cases} \tag{3.3}$$

As is remarked in [18], this calculation of $f_P(Q)$ may be interpreted as exponentiation in a generalized jacobian with modulus $(Q+T) - (T)$. The $h_{i,j}$ are simply cocycle values. A good source for this viewpoint is [13].

3.2.3 Semaev's algorithm for solving the DLP on anomalous elliptic curves

Let $K = \mathbb{F}_q$ be a finite field of characteristic p. In [36], Semaev proposed a polynomial time algorithm for solving the DLP on elliptic curves over K which contain a point of order p, using the following map:

$$\begin{array}{rccc} \lambda : & E[p] & \rightarrow & K^+ \\ & P & \mapsto & \frac{f_P'}{f_P}(R) \\ & P_\infty & \mapsto & 0 \end{array}$$

where D_P is any divisor of degree 0 which sums to P, f_P is any function with $\text{div}\,(f_P) = pD_P$, and $R \in E[p]$ with $R \neq P_\infty$. Here f_P' denotes $\frac{d}{dx} f_P$.

To see how this map is used to solve the DLP, consider $P, Q \in E[p]$ with $Q = nP$. Using the standard $\log p$ addition chain decomposition, we can compute $\lambda(P), \lambda(Q)$ in time $O(\log p)$, and then solve $n\lambda(P) = \lambda(Q)$ for $n \in K^+$ by Euclid's algorithm.

Proposition 3.2.2 *(Semaev, [36]) The map λ is well-defined and non-zero for any $R \in E[p]$ with $R \neq P_\infty$. Furthermore, λ is an injective homomorphism with respect to P and is independent of the divisor D_P.*

This is proved explicitly in [36] and in fact, the proof holds for any field K of characteristic $p > 0$ such that $E[p] \subset E(K)$. The proposition also follows from considering the map:

$$\begin{tikzcd}
E[p] \arrow[r] & Pic_K^0(E)[p] \arrow[r] & \Omega_K^h(E) \arrow[r] & \mathcal{L}_{div(dt)} \arrow[r] & K^+ \\
P \arrow[r, mapsto, "\delta"] & D_P \arrow[r, mapsto, "\rho"] & \frac{df_P}{f_P} \arrow[r, mapsto, "\psi"] & \frac{df_P}{dtf_P} \arrow[r, mapsto, "\varphi"] & \frac{df_P}{dtf_P}(R)
\end{tikzcd}$$

where $Pic_K^0(E)$ is the group of divisor classes of E of degree 0, $\Omega_K^h(E)$ are the holomorphic differentials of the one-dimensional $K(C)$-vector space of differentials, $\mathcal{L}_{div(dt)}$ is the one-dimensional K-vector space of functions g with div $(gdt) \geq 0$ and t is a uniformizer for the point R.

This is an injective homomorphism since ρ is an injective homomorphism (see [37]), δ and ψ are isomorphisms, and φ is injective by Riemann-Roch. This is noted in [35], where the attack on the DLP is extended to the p-subgroup of the divisor class group of a curve of arbitrary genus.

The computation method proposed in [36] is a variation on Miller's algorithm. Let T be a point of order two and let $R \in E[p]$. Let f_P be the function with div $(f_P) = D_P = (P+T)-(T)$. As in section 3.2.2, the value of the function λ may be computed by using an addition chain decomposition and summing contributions of the form $\frac{h'_{i,j}}{h_{i,j}}(R)$, where $h_{i,j}$ is as in Section 3.2.2. That is, $\frac{f'_P}{f_P}(R) = \sum_C \frac{h'_{i,j}}{h_{i,j}}(R)$. (We remark that in [36], the function $\frac{v_i v_j}{l_{-i,-j}}$ is used, which is equivalent up to constant since it has the same divisor.)

To compute $h' = \frac{d}{dx}h$, we make use of the invariant differential property $\frac{dx}{y} \circ \tau = \frac{dx}{y}$. Let g be a function expanded in a power series around x. Then $g \circ \tau$ can be expanded in a series around $x \circ \tau$ with the same coefficients, and so

$$\frac{d(g \circ \tau)}{dx} = \frac{d(g \circ \tau)}{d(x \circ \tau)} \frac{d(x \circ \tau)}{dx} = (\frac{dg}{dx} \circ \tau)\frac{y \circ \tau}{y}.$$

Therefore, for $h = \frac{\ell}{v} \circ \tau$, $h'(R) = \frac{y(R+T)}{y(R)}(\frac{\ell}{v})'(R+T)$. (Since T is order 2, translation by T and $-T$ are the same.)

Remark 3.2.1

The choice of the divisor $D_P = (P+T) - (T)$ avoids any possible zeros or undefined values when evaluating the lines through multiples of P at R, which is itself a multiple of P. Note that when $p > 7$, for a fixed point P, it is always possible to choose an $R \in E[p]$ such that the lines in a $\log p$ addition chain decomposition will not have R as a zero. However, since the homomorphism λ is *not* independent of R, in order to have it well-defined it is necessary to choose an evaluation point that works for all P, which explains Semaev's use of a translation point.

As is the case for Miller's algorithm to compute the Weil pairing, this calculation may be interpreted as exponentiation in a generalized jacobian, after a slight modification. Note that if we use the divisor $D_P = (P) - (P_\infty)$, the $h_{i,j}$ are simply ratios of lines through multiples of P, and thus evaluating at $R + T \notin E[p]$ gives well-defined, non-zero values. In this case, we may calculate the value $\frac{f'_P}{f_P}(R+T)$ using exponentiation in a generalized jacobian with modulus $2(R+T)$ for $R \in E[p]$, with T of order 2. The value will differ from the value $\lambda(R)$ by the constant factor $y(R+T)/y(R)$.

3.3 A “Weil pairing” on the p-torsion of $\tilde{E}(\bar{K}[\epsilon])$

Let $\tilde{E}$ denote the canonical lift of $E : y^2 = x^3 + Ax + B$ to $K[\epsilon]$. We define the pairing

$$e_p : \tilde{E}[p] \times \tilde{E}[p] \to \mu_p(\bar{K}[\epsilon])$$

by first defining a bilinear map e on $E[p] \times \Theta$, and then extending it to $\tilde{E}[p]$ in such a way that the necessary properties hold.

Let $P \in E[p]$ and let T be a point of order two. Consider the divisor $D_P = (P+T) - (T)$. Let f_P be the function on E with divisor pD_P, unique up to a non-zero constant. We use the notation of section 3.2.2. Recall that to compute f_P evaluated at a point Q, we choose an addition chain decomposition for p and compute the product of cocycle contributions of the form $h_{i,j}(P)$, where $h_{i,j}$ are ratios of lines translated by T.

Any function in $\overline{K}(E)$ is a well-defined function on the affine points of $\tilde{E}(\bar{K}[\epsilon])$, provided that the denominator is invertible. We will see that this is true for $h_{i,j}$ on certain points of $\tilde{E}$, thereby making the computation of $\prod_C h_{i,j}$ legitimate.

Definition 3.3.1 *Fix $R \in E[p]$ such that $R \neq P_\infty$. Let C be an addition chain decomposition for p. Define the map $e : E[p] \times \Theta \to \mu_p(\bar{K}[\epsilon])$ by*

$$e(P, \mathcal{O}_k) = \begin{cases} \prod_C \frac{h_{i,j}(R)}{h_{i,j}(\mathcal{O}_k+R)} & \textit{if } P, \mathcal{O}_k \neq P_\infty \\ 1 & \textit{if } P = P_\infty \textit{ or } \mathcal{O}_k = P_\infty \end{cases}$$

The proof of the following theorem is given in the next section.

Theorem 3.3.2 *The map e is well-defined and bilinear. It is independent of divisor D_P summing to P, evaluation point $R \in E[p]$ and the addition chain decomposition C of p.*

Furthermore, for any $R \in E(\overline{K})$,

$$e(P, \mathcal{O}_k) = 1 + 2\Big(y\frac{f'_P}{f_P}\Big)(R)k\epsilon,$$

where f_P is the normalized function with divisor pD_P.

We now may define the *Weil pairing on p-torsion.* Extend the map e to

$$e_p : \tilde{E}[p] \times \tilde{E}[p] \to \mu_p(\bar{K}[\epsilon])$$

such that

- $e_p(P, \mathcal{O}_k) = e(P, \mathcal{O}_k)$ for all $P \in E[p]$,
- $e_p(P, Q) = 1$, for all $P, Q \in E[p]$,
- $e_p(\mathcal{O}_k, \mathcal{O}_j) = 1$, for all $j, k \in \overline{K}$,
- e_p is bilinear,
- e_p is anti-symmetric: $e(P, Q) = e(Q, P)^{-1}$.

Theorem 3.3.3 *The map e_p is non-degenerate. That is, if $e_p(P, Q) = 1$ for all $P \in \tilde{E}[p]$, then $Q = P_\infty$, and if $e_p(P, Q) = 1$ for all $Q \in \tilde{E}[p]$, then $P = P_\infty$.*

The proof of this theorem is given in the next section.

Remark 3.3.1

Note that we are defining $e_p(P, \mathcal{O}_k)$ to be the result of Miller's algorithm to compute

$$\frac{f_P(R)}{f_P(\mathcal{O}_k + R)}.$$

This definition can thus be viewed as the analog of the Weil pairing definition for n prime to p:

$$e_n(P,Q) = \frac{f_Q(P+T)}{f_Q(T)} \frac{f_P(R)}{f_P(Q+R)}.$$

Recall that Miller's algorithm computes the value of f_Q as the product of ratios of lines through multiples of the point Q. For $Q = \mathcal{O}_k$, this involves products of lines through points at infinity (which would then be evaluated at affine points of $E(\overline{K})$). Assuming such a line has the form $\ell = 0$ with $\ell(x,y,z) = ax + by + cz$ and $a, b, c \in \bar{K}[\epsilon]$, there is not a unique choice for such a line. For example, any line of the form $a\epsilon x + cz$, for $a \in \overline{K}, c \in \bar{K}[\epsilon]$, passes through all points in Θ. We make the choice of the line $\ell = cz$. When evaluated at affine points, this becomes the constant function c which normalized is just 1. The value of $\frac{f_Q(P+R)}{f_Q(R)}$ for $Q = \mathcal{O}_k$ may therefore naturally be considered to be 1.

We now show how the Weil pairing e_p can be used to solve the DLP on p-subgroups of elliptic curves over $\mathbb{F}_q$. Given $P, Q \in E[p]$ with $Q = nP$, calculate $e_p(P, \mathcal{O}_1) = 1 + a\epsilon$ and $e_p(Q, \mathcal{O}_1) = 1 + b\epsilon$. Since e_p is bilinear, $e_p(Q, \mathcal{O}_1) = e_p(P, \mathcal{O}_1)^n = (1 + a\epsilon)^n = 1 + na\epsilon$. Thus it suffices to solve the equation $b = na$ in $\mathbb{F}_q^+$ for $n \in \mathbb{Z}/p\mathbb{Z}$ by computing the multiplicative inverse of a. By Theorem 3.3.2, for $R \in E[p]$, this process is essentially Semaev's algorithm to solve the DLP in p-subgroups. Therefore, we see that Semaev's algorithm may be interpreted as a Weil-pairing based attack.

3.4 Proof of properties of the pairing

To show that e is well-defined and bilinear, we relate its calculation to the map λ from section 3.2.3. For this, we need the following lemma.

Lemma 3.4.1 *Let $\ell_{i,j}$ denote the line through iP and jP, and let v_i denote the vertical line through iP. Let τ denote translation by $-T$ and let*

$$h_{i,j} = \begin{cases} \frac{\ell_{i,j}}{v_{i+j}} \circ \tau & i+j \neq p, \\ \\ v_i \circ \tau & i+j = p. \end{cases}$$

Let $R \in E[p]$ with $R \neq P_\infty$. Then

$$\frac{h_{i,j}(R)}{h_{i,j}(\mathcal{O}_k + R)} = 1 + 2y(R)\frac{h'_{i,j}}{h_{i,j}}(R)k\epsilon.$$

Proof: We first show that

$$h_{i,j}(\mathcal{O}_k + R) = h_{i,j}(R) - 2y(R)h'_{i,j}(R)\epsilon.$$

We can think of this as analogous to the calculus approximation of $f(x_0 + \epsilon)$ by the value $f(x_0) + f'(x_0)\epsilon$.

Let $S = R + T = (x_0, y_0)$. Assume $i + j \neq p$. Fix i, j and let $h_{i,j} = h = \frac{\ell}{v} \circ \tau$. Since we are evaluating $h_{i,j}$ at affine points, we have $\ell = y - mx - b$ and $v = x - c$ for some $m, b, c \in \overline{K}$.

Since v is a line through a multiple of P, and $S \notin E[p]$, we see that $x_0 - c \neq 0$. Thus $h(R) = \frac{\ell}{v}(S)$ is well-defined. Furthermore, since

$$\mathcal{O}_k + S = (x_0 - 2y_0k\epsilon : y_0 - (3x_0^2 + A)k\epsilon : 1),$$

the denominator of $h(\mathcal{O}_k + R)$ is invertible, and thus the value $h(\mathcal{O}_k + R)$ is well-defined. Then

$$\begin{aligned} h(\mathcal{O}_k + R) &= \frac{\ell}{v}(\mathcal{O}_k + S) \\ &= \Big[(y_0 - mx_0 - b) + (2y_0m - (3x_0^2 + A))k\epsilon\Big]\Big/\Big[(x_0 - c) - 2y_0k\epsilon\Big] \\ &= \Big[(y_0 - mx_0 - b) + (2y_0m - (3x_0^2 + A))k\epsilon\Big]\Big[(x_0 - c)^{-1} + (x_0 - c)^{-2}2y_0k\epsilon\Big] \\ &= h(R) + \Big[(2y_0m - (3x_0^2 + A))(x_0 - c)^{-1} + h(R)(x_0 - c)^{-1}2y_0\Big]k\epsilon. \end{aligned}$$

Recall from section 3.2.3 that $h'(R) = \frac{y(S)}{y(R)}(\frac{\ell}{v})'(S)$. Since $v' = 1$ and $l'(S) = \frac{3x_0^2+A}{2y_0} - m$, we have

$$h'(R) = \frac{1}{2y(R)}\Big((3x_0^2 + A - 2y_0m)(x_0 - c)^{-1} - 2y_0h(R)(x_0 - c)^{-1}\Big)$$

and therefore $h(\mathcal{O}_k + R) = h(R) - 2y(R)h'(R)k\epsilon$.

For $i + j = p$, we have $h = v \circ \tau$ and $h'(R) = \frac{y(S)}{y(R)}$ by the equation in Section 3.2.3. Then

$$h(\mathcal{O}_k + R) = v \circ \tau(\mathcal{O}_k + R) = v(\mathcal{O}_k + S) = (x_0 - c) - 2y_0k\epsilon = h(R) - 2y(R)h'(R)k\epsilon.$$

It remains to show that $h(R) \neq 0$. The fact that $R \in E[p]$ implies that S is not a zero of the line described by ℓ or v. Therefore, in both cases, $h(R) \neq 0$, and thus $\frac{h(\mathcal{O}_k+R)}{h(R)} = 1 - 2y(R)\frac{h'(R)}{h(R)}k\epsilon$. The lemma then follows directly. □

Now we can prove Theorem 3.3.2 and 3.3.3.

Proof (Thm. 3.3.2): Fix $P, \mathcal{O}_k$ and an addition chain decomposition C for p. Note that by Lemma 3.4.1, $e(P, \mathcal{O}_k)$ is well-defined. Let f_P be the function with divisor pD_P for

$D_P = (P+T) - (T)$. Let $R \in E[p]$ with $R \neq P_\infty$. Then $\frac{f'_P(R)}{f_P(R)} = \sum_C \frac{h'_{i,j}}{h_{i,j}}(R)$. We have

$$\begin{aligned} e(P, \mathcal{O}_k) &= \prod_C \frac{h_{i,j}(R)}{h_{i,j}(\mathcal{O}_k + R)} \\ &= \prod_C \Big(1 + 2y(R)\frac{h'_{i,j}}{h_{i,j}}(R)k\epsilon\Big) \\ &= 1 + 2y(R)\Big(\sum_C \frac{h'_{i,j}}{h_{i,j}}(R)\Big)k\epsilon \\ &= 1 + 2y(R)\frac{f'_P(R)}{f_P(R)}k\epsilon. \end{aligned}$$

Note that $\frac{f'_P(R)}{f_P(R)} = \lambda(R)$, where λ is the homomorphism with respect to P from section 3.2.3. Thus since $e(P, \mathcal{O}_k) = 1 + 2(y\frac{f'_P}{f_P})(R)k\epsilon$, the map e is linear in the first coordinate. Furthermore, since $\mathcal{O}_k + \mathcal{O}_j = \mathcal{O}_{k+j}$, we have that e is linear in the second coordinate. Therefore, e is bilinear. Since $\frac{f'_P(R)}{f_P(R)}$ is independent of the divisor for P, as shown in [36], the value of e is independent of choice of the divisor for P. Similarly, since $\frac{f'_P(R)}{f_P(R)}$ is independent of addition chain decomposition, so is the value of e.

As shown in [36], div $(\frac{f'_P}{f_P}) =$ div $(\frac{1}{y})$, thus $y\frac{f'_P}{f_P}$ is a constant function on $E(\overline{K})$. Therefore since $e(P, \mathcal{O}_k) = 1 + 2(y\frac{f'_P}{f_P})(R)k\epsilon$ for $R \in E[p]$, we have for any $R \in E(\overline{K})$ that

$$e(P, \mathcal{O}_k) = 1 + 2\Big(y\frac{f'_P}{f_P}\Big)(R)k\epsilon.$$

Thus, in computing e, we may use any evaluation point R, including P_∞. □

Proof (Thm. 3.3.3): Let $P \in \tilde{E}(\bar{K}[\epsilon])[p]$. We show that if $P \neq P_\infty$, then there exists $Q \in \tilde{E}(\bar{K}[\epsilon])[p]$ such that $e_p(P, Q) \neq 1$. This shows non-degeneracy in the first coordinate, and by the property of anti-symmetry, non-degeneracy in the second coordinate will follow.

By Lemma 3.2.1, P may be written as $P_0 + \mathcal{O}_k$ for $P_0 \in E(\overline{K})$ and $k \in \overline{K}$. If $P_0 \neq P_\infty$, let $Q = \mathcal{O}_1$. Then $e_p(P, Q) = e_p(P_0, \mathcal{O}_1)e_p(\mathcal{O}_k, \mathcal{O}_1) = e_p(P_0, \mathcal{O}_1)$. Let $R \in E[p]$ with $R \neq P_\infty$. By Proposition 3.2.2, $\frac{f'_P}{f_P}(R)$ is non-zero. Therefore, since $e_p(P_0, \mathcal{O}_1) = 1 + 2(y\frac{f'_P}{f_P})(R)\epsilon$ and $R \notin E[2]$, we have that $e_p(P, Q) \neq 1$.

If $P_0 = P_\infty$, then $k \neq 0$, since $P \neq P_\infty$. Let $Q, R \in E[p]$ with $Q, R \neq P_\infty$. Then $e_p(P, Q) = e_p(\mathcal{O}_k, Q) = 1 - 2(y\frac{f'_Q}{f_Q})(R)k\epsilon$. Since $k \neq 0$ and $R \notin E[2]$, we have that $e_p(P, Q) \neq 1$, as desired. □

3.5 Rück's algorithm for solving the DLP on p-torsion

Recall the homomorphism from Section 3.2.3:

$$\begin{tikzcd}
E[p] \arrow[r] & Pic^0_K(E)[p] \arrow[r] & \Omega^h_K(E) \arrow[r] & \mathcal{L}_{div(dt)} \arrow[r] & K^+ \\
P \arrow[r, mapsto, "\delta"] & D_P \arrow[r, mapsto, "\rho"] & \frac{df_P}{f_P} \arrow[r, mapsto, "\psi"] & \frac{df_P}{dtf_P} \arrow[r, mapsto, "\varphi"] & \frac{df_P}{dtf_P}(R)
\end{tikzcd}$$

Choosing the divisor $D_P = (P) - (P_\infty)$ and evaluation point $R = P_\infty$, we may compute the value of $\frac{df_P/dt}{f_P}(R)$ by simply summing the slopes of lines through multiples of P for any addition chain decomposition. This fact is noted in [24], where it is referred to as the "Rück algorithm," and a slight variation is found in [31]. In [35], Rück refers to the result of this algorithm as "the additive version of the Tate pairing." We make this remark explicit by relating the algorithm to the pairing of $E[p]$ and Θ which we've defined.

Proposition 3.5.1 *(Rück, [35]) Let f_P be any function with divisor $p(P) - p(P_\infty)$ and let $t = -\frac{x}{y}$. Let $m_{i,j}$ denote the slope of the line through iP and jP, and let C be an addition* *chain decomposition for p. Then*

$$\frac{df_P/dt}{f_P}(P_\infty) = -\sum_C m_{i,j}.$$

Proof: Consider $\frac{df_P/dt}{f_P}(P_\infty)$. Since $D_P = (P) - (P_\infty)$, this reduces to computing $\frac{dh_{i,j}/dt}{h_{i,j}}$ where $h_{i,j}$ is defined as in section 3.2.3. In particular, we show that

$$\frac{dh_{i,j}/dt}{h_{i,j}} = \begin{cases} -\frac{1}{t} - m_{i,j} + O(t) & \text{if } i+j \neq p, \\ \\ -\frac{2}{t} + O(t) & \text{if } i+j = p \end{cases} \tag{3.4}$$

For $i + j \neq p$,

$$h_{i,j} = \frac{\ell}{v} = \frac{y - mx - b}{x - c} = \frac{1}{t} - m + O(t).$$

Thus

$$\frac{dh/dt}{h} = -\frac{1}{t} - m + O(t).$$

For $i + j = p$, $h_{i,j} = v$. Expanding v around t, we get $v = x - c = \frac{1}{t^2} - c + O(t)$. Thus

$$\frac{dv/dt}{v} = -\frac{2}{t} + O(t),$$

and (3.4) is proved.

Note that using an addition chain decomposition for p to calculate f_P will result in $(p-1)$ terms of the form $h_{i,j}$ with exactly one such that $i + j = p$. Thus the pole contributions of the $h_{i,j}$ total to zero in characteristic p and

$$\frac{df_P/dt}{f_P} = -\frac{p}{t} - \sum_C m_{i,j} + O(t) = -\sum_C m_{i,j} + O(t)$$

Evaluating at P_∞ yields the result. □

Corollary 3.5.2 *Let $m_{i,j}$ be the slope of the line through iP and jP, and let C be an addition chain decomposition for p. Then*

$$e(P, \mathcal{O}_k) = 1 + \Big[\sum_C m_{i,j}\Big]k\epsilon.$$

Proof: By Theorem 3.3.2, the map e is independent of divisor and evaluation point. Thus we may choose the divisor $D_P = (P) - (P_\infty)$ and evaluation point $R = P_\infty$. This means we must calculate

$$e(P, \mathcal{O}_k) = 1 + 2\Big(y\frac{f_P'}{f_P}\Big)(P_\infty)k\epsilon.$$

Since we evaluate at P_∞, we want to expand functions around the uniformizer for P_∞, namely $t = -\frac{x}{y}$. Using the fact that $\frac{dt}{dx} = \frac{x^3+Ax+2B}{2y^3}$, we are looking to compute

$$\frac{df_P/dt}{f_P}\frac{x^3 + Ax + 2B}{y^2}(P_\infty).$$

Recall that x and y have poles at P_∞ of order 2 and 3, respectively. In particular, $x = \frac{1}{t^2} + O(t)$ and $y = -\frac{1}{t^3} + O(t)$ ([38], p. 113). Thus $\frac{x^3+Ax+2B}{y^2} = -1 + O(t)$, and hence this contributes a factor of -1 when we evaluate at P_∞.

Now, by Proposition 3.5.1, $\frac{df_P/dt}{f_P}(P_\infty) = -\sum_C m_{i,j}$, and the result follows. □

3.6 The map e_p and isogenies of $\tilde{E}(K[\epsilon])$

Let $\phi : E_1 \rightarrow E_2$ be an isogeny between curves given by the Weierstrass form $y^2 = x^3 + A_i x + B_i$. Let $\tilde{E}_i$ denote the canonical lift of E_i, as defined in 3.2.1. In this section, we show how to extend ϕ to a homomorphism $\tilde{\phi} : \tilde{E}_1 \rightarrow \tilde{E}_2$ in such a way that the following proposition holds:

Proposition 3.6.1 *For any isogeny $\phi : E_1 \to E_2$,*

$$e_p(\tilde{\phi}(P), \tilde{\phi}(Q)) = e_p(P, Q)^{\deg \phi}.$$

For ease of notation, we assume K is algebraically closed. As $\tilde{E}_i \simeq E_i \oplus \Theta_i$, it suffices to define $\phi : \Theta_1 \to \Theta_2$ and then extend it linearly to a map $\tilde{\phi} : \tilde{E}_1 \to \tilde{E}_2$. Let x_i, y_i denote the coordinate functions of E_i, and let $t_i = -\frac{x_i}{y_i}$ be a uniformizer at $P_\infty^{(i)}$, the point at infinity of E_i. Let $m \in K$ be such that $t_2 \circ \phi = mt_1 + O(t_1^2)$. (To obtain the value m, expand x_1 and y_1 around t_1 and use the fact that x_2 and y_2 are rational functions of x_1 and y_1 to obtain $t_2 \circ \phi$ as a function of t_1.)

Definition 3.6.2 *Given $\phi : E_1 \to E_2$, define $\phi : \Theta_1 \to \Theta_2$ by $\phi(\mathcal{O}_k) = \mathcal{O}_{mk}$.*

First note that $\phi : \Theta_1 \to \Theta_2$ is a homomorphism with respect to this definition. Furthermore, it is compatible with composition of isogenies. That is, if $\phi : E_1 \to E_2$ and $\psi : E_2 \to E_3$, are isogenies, then $(\psi \circ \phi)(\mathcal{O}_k) = \psi(\phi(\mathcal{O}_k))$. This follows from the fact that if $t_2 \circ \phi = m_1 t_1 + O(t_1^2)$ and $t_3 \circ \psi = m_2 t_2 + O(t_2^2)$, then $t_3 \circ (\psi \circ \phi) = (m_1 m_2) t_1 + O(t_1^2)$.

The motivation for this definition is as follows. If ϕ is inseparable, then $\phi = \phi_s \circ \pi^r$, where ϕ_s is separable and the degree of inseparability of ϕ is p^r. The map $\pi : (x : y : z) \mapsto (x^p : y^p : z^p)$ is well-defined on the points of $\tilde{E}(K[\epsilon])$, and clearly $(k\epsilon : 1 : 0) \overset{\pi}{\mapsto} (0 : 1 : 0)$. Thus we should define $\phi(\mathcal{O}_k) = P_\infty^{(2)}$. (Note that this agrees with the idea that Θ is acting as the replacement for the "missing" geometric points of p-torsion, the "kernel of Frobenius.") But if ϕ is inseparable, $m = 0$, since the order of $t_2 \circ \phi$ at $P_\infty^{(1)}$ is equal to the degree of inseparability ([38, pp. 28, 76]). Thus is makes sense to define $\phi(\mathcal{O}_k) = \mathcal{O}_{mk}$.

Now consider ϕ separable. Then $t_2 \circ \phi$ is a uniformizer for $P_\infty^{(1)}$, so $m \neq 0$. Suppose we want $\phi(\mathcal{O}_k) = \mathcal{O}_j$, for some $j \in K$. Since $t_2 \circ \phi(\mathcal{O}_k) = t_2((j\epsilon : 1 : 0)) = -j\epsilon$ and $(mt_1 + O(t_1^2))(\mathcal{O}_k) = -mk\epsilon$, it makes sense to define $j = mk$.

Next we extend the isogeny $\phi : E_1 \to E_2$ to $\tilde{E}(K[\epsilon])$. By Lemma 3.2.1, any point of $\tilde{E}_1(K[\epsilon])$ decomposes uniquely as a point of $E_1(K)$ and Θ. Furthermore, for any $k \in K$ and $P \in E_1(K)$, $\phi(\mathcal{O}_k)$ and $\phi(P)$ are both points of $E_2(K[\epsilon])$, hence their sum is as well. Therefore, the following definition extends ϕ in a well-defined manner to all of $E_1(K[\epsilon])$:

Definition 3.6.3 *Let $\tilde{P} \in \tilde{E}_1(K[\epsilon])$ with $\tilde{P} = P + \mathcal{O}_k$. Define*

$$\tilde{\phi}(\tilde{P}) = \phi(P) + \phi(\mathcal{O}_k). \tag{3.5}$$

Proposition 3.6.4 *Let $P, Q \in \tilde{E}_1(K[\epsilon])$. Then*

$$\tilde{\phi}(P) + \tilde{\phi}(Q) = \tilde{\phi}(P + Q).$$

The proposition follows immediately from Definition (3.6.3) and from the fact that ϕ is a homomorphism on $E_1(K[\epsilon])$ and Θ.

Lemma 3.6.5 *Let $\phi : E_1 \to E_2$ be an isogeny with $t_2 \circ \phi = mt_1 + O(t_1^2)$ for $m \in K$. Then*

$$e(\phi(P), \mathcal{O}_{mk}) = e(P, \mathcal{O}_k)^{\deg \phi}.$$

Proof: If ϕ is inseparable, then the degree of inseparability is $q = p^r$ for some $r > 0$ and thus p divides $\deg \phi$. Furthermore, $m = 0$ since the order of $t_2 \circ \phi$ at $P_\infty^{(1)}$ is the degree of inseparability. So both $e(P, \mathcal{O}_k)^{\deg \phi}$ and $e(\phi(P), \mathcal{O}_k)^m$ equal 1, and the result holds.

Now assume ϕ is separable, which implies that $m \neq 0$. By the proof of Proposition 3.5.2, it suffices to show that

$$m\frac{df_{P_2}/dt_2}{f_{P_2}}(P_\infty^{(2)}) = (\deg\phi)\frac{df_{P_1}/dt_1}{f_{P_1}}(P_\infty^{(1)}).$$

Let $\ker\phi = \{R_1, ...R_s\}$. Since div $(f_{P_2}) = p(P_2) - p(P_\infty)$ and ϕ is separable, div $(f_{P_2} \circ \phi) = \sum_{i=1}^s p(P_1 + R_i) - p(R_i)$. Let $g_i = \frac{l_{-P_1,-R_i}}{v_{P_1}v_{R_i}}$. Then div $(f_{P_2} \circ \phi) = \sum_{i=1}^s p[(P_1) - (P_\infty) +$ div $(g_i)] = \sum_{i=1}^s$ div $(f_{P_1}g_i^p)$. Thus, up to a constant, $f_{P_2} \circ \phi = f_{P_1}^{\deg\phi}(\prod_{i=1}^s g_i)^p$. Since the characteristic of K is p,

$$d(f_{P_2} \circ \phi) = (\deg\phi) f_{P_1}^{\deg\phi - 1}(df_{P_1})(\prod_{i=1}^s g_i)^p.$$

Thus

$$\frac{d(f_{P_2} \circ \phi)}{f_{P_2} \circ \phi} = (\deg\phi)\frac{df_{P_1}}{f_{P_1}}. \tag{3.6}$$

Note that for any function g expanded around t, $\frac{dg}{dt} \circ \phi = \frac{d(g \circ \phi)}{d(t \circ \phi)}$. Using this and (3.6), we have

$$\begin{aligned} m\tfrac{df_{P_2}/dt_2}{f_{P_2}}(P_\infty^{(2)}) &= m\Big(\tfrac{df_{P_2}/dt_2}{f_{P_2}} \circ \phi\Big)(P_\infty^{(1)}) \\ &= m\tfrac{d(f_{P_2}\circ\phi)/d(t_2\circ\phi)}{f_{P_2}\circ\phi}(P_\infty^{(1)}) \\ &= m(\deg\phi)\tfrac{df_{P_1}/d(t_2\circ\phi)}{f_{P_1}}(P_\infty^{(1)}). \end{aligned}$$

From that $\frac{dt_1}{d(t_2\circ\phi)} = m^{-1} + O(t_1)$, we have

$$m\tfrac{df_{P_2}/dt_2}{f_{P_2}}(P_\infty^{(2)}) = (\deg\phi)\tfrac{df_{P_1}/dt_1}{f_{P_1}}(P_\infty^{(1)}),$$

and the lemma is proved. □

The proof of Proposition 3.6.1 is now immediate. From Lemma 3.6.5 and Definition 3.6.3, we have

$$e_p(\tilde{\phi}(P), \tilde{\phi}(\mathcal{O}_k)) \quad = \quad e(\phi(P), \mathcal{O}_{mk}) \quad = \quad e_p(P, \mathcal{O}_k)^{\deg \phi},$$

for $P \in E_1[p]$ and $\mathcal{O}_k \in \Theta$. Thus, since e_p is bilinear and $\tilde{\phi}$ is a homomorphism, the proposition holds.

3.7 Another application of elliptic curves over the dual numbers

We have seen how the extension of the Weil pairing to p-torsion over the dual numbers directly leads to the previously defined maps of [35] and [36]. Though we have not gained any “new” information, we have shown that discrete logarithm attacks on p-torsion subgroups of [35] and [36] may be interpreted as Weil-pairing-based attacks, exactly the same as the MOV attack on prime-to-p torsion subgroups. In this section, we give another example of how looking at elliptic curves over the dual numbers may be a fruitful approach.

The DLP attack of Smart [39] on anomalous elliptic curves involves working in $\tilde{E}(\mathbb{Z}/p^2\mathbb{Z})$ where $\tilde{E}$ is a non-canonical lift of E (meaning p-torsion points of E are no longer p-torsion when lifted to $\tilde{E}$). The attack involves lifting points $P, Q \in E[p]$ with $Q = nP$ to $\tilde{E}(\mathbb{Z}/p^2\mathbb{Z})$, multiplying the points by p, and applying the map $(x, y) \mapsto \frac{x}{y}$. In this way, solving for n such that $nP = Q$ reduces to solving an instance of the DLP in $\mathbb{F}_p^+$. The fact that this map is a homomorphism may be shown via the p-adic elliptic logarithm (see [39], or [45], p. 190).

If we consider $\tilde{E}(\mathbb{F}_p[\epsilon])$ instead, the attack works analogously, and the reasoning behind it is elementary. (In fact, the attack works for $\tilde{E}(K[\epsilon])$, where K is any field of characteristic $p \neq 0, 2, 3$.) Lift P, Q to $\tilde{P}, \tilde{Q} \in \tilde{E}(\mathbb{F}_p[\epsilon])$. The points $\tilde{P}, \tilde{Q}$ may no longer be dependent. However, since $nP = Q \in E(\mathbb{F}_p)$, there exists $R \in \Theta$ such that $n\tilde{P} - \tilde{Q} = R$. Since P, Q are points of p-torsion, $p\tilde{P}, p\tilde{Q} \in \Theta$. Thus we have the following equation in Θ

$$p(n\tilde{P}) - p\tilde{Q} = pR = P_\infty. \tag{3.7}$$

Note that $p\tilde{P}, p\tilde{Q} = P_\infty$ if and only if $\tilde{P}$ and $\tilde{Q}$ are p-torsion points in $\tilde{E}$. Thus if this is not the case, we can translate (3.7) to an instance of the DLP in $\mathbb{F}_p^+$ via the homomorphism $(k\epsilon : 1 : 0) \mapsto k$ and then solve for n.

This version is more efficient, as computations in $\mathbb{F}_p[\epsilon]$ are more straightforward than in $\mathbb{Z}/p^2\mathbb{Z}$. It may present another advantage as well, related to the fact that the DLP attack requires that the lift of the curve over $\mathbb{F}_p$ be non-canonical.

Let $\tilde{E}$ be any lift of the curve $E : y^2 = x^3 + Ax + B$, with j-invariant $j \in \mathbb{F}_p$. Note that $D = 4A^3 + 27B^2 \neq 0$ since E is non-singular. Define $j(\tilde{E})$ as the value $\frac{4\tilde{A}^3}{4\tilde{A}^3 + 27\tilde{B}^2}$. Since $D \neq 0$, the denominator is invertible, and hence $j(\tilde{E}) \in \mathbb{F}_p[\epsilon]$. Let $\tilde{j}$ denote the value $j(\tilde{E})$, and note that $\tilde{j} \equiv j \mod \epsilon$. The following proposition shows that $\tilde{j} \in \mathbb{F}_p$ if and only if the elliptic curve $\tilde{E}$ can be transformed to the "canonical lift" (as defined in Section 3.2.1) by an invertible change of coordinates.

Proposition 3.7.1 *Let E be given by $y^2 = x^3 + Ax + B$. Let $\tilde{E}$ be a lift of E to $\mathbb{F}_p[\epsilon]$ with $\tilde{A} = A + A_1\epsilon, \tilde{B} = B + B_1\epsilon$, for $A_1, B_1 \in \mathbb{F}_p$. Then $\tilde{j} \in \mathbb{F}_p$ if and only if there exists $\mu = 1 + kt$ with $k \in \mathbb{F}_p$ such that $\mu^4 A = \tilde{A}$ and $\mu^6 B = \tilde{B}$. In this case, there exists a change of coordinates $x \mapsto \mu^2 x, y \mapsto \mu^3 y$ taking E to $\tilde{E}$, where E is viewed as an elliptic* *curve over* $\mathbb{F}_p[\epsilon]$.

Proof: Assume there exists $\mu = 1 + kt$, $k \in \mathbb{F}_p$ with $\mu^4 A = \tilde{A}$ and $\mu^6 B = \tilde{B}$. Then $\tilde{j} = \frac{4\tilde{A}^3}{4\tilde{A}^3 + 27\tilde{B}^2} = j$.

For the other implication, assume $\tilde{j} \in \mathbb{F}_p$. Then $\tilde{j} = j$ and a calculation with the ϵ-components yields

$$12A^2 A_1 D = 4A^3(12A^2 A_1 + 56BB_1). \tag{3.8}$$

To find $\mu = 1 + kt$ such that $\mu^4 A = \tilde{A}$ and $\mu^6 B = \tilde{B}$, we solve $4kA = A_1$ and $6kB = B_1$ simultaneously for k. If either A or B is zero this is no problem. If $A, B \neq 0$, choose $k \in \mathbb{F}_p$ such that $4kA = A_1$. Then (3.8) becomes

$$12A^2(4kA)D = 4A^3(12A^2(4kA) + 56BB_1)$$

which simplifies to $6k(D - 4A^3) = 27BB_1$. This implies that $B_1 = 6kB$, as desired. □

Thus if $\tilde{j} \in \mathbb{F}_p$, the p-torsion of E lifts to p-torsion of $\tilde{E}$, and the DLP attack over the dual numbers fails. Calculations suggest that lifts with $\tilde{j} \in \mathbb{F}_p$ are the only lifts of E for which p-torsion lifts to p-torsion. Presuming this, it is easy to avoid a lift to $\mathbb{F}_p[\epsilon]$ for which $\tilde{P}$ and $\tilde{Q}$ are p-torsion simply by choosing a lift with j-invariant $\tilde{j} \notin \mathbb{F}_p$. This differs from the case of lifting to $\mathbb{Z}/p^2\mathbb{Z}$, since (to the author's knowledge) there is no analogously simple way to determine from the j-invariant $\tilde{j} \in \mathbb{Z}/p^2\mathbb{Z}$ whether or not the lift is canonical.

Appendix A

Auxiliary algorithms for computing $H_D(X)$

In this appendix, we give the details of the auxiliary algorithms used in the main algorithms of Chapter 2.

Let $\mathcal{O}$ be an order of discriminant $D < -4$ and let p be a prime inert with respect to D. We fix a maximal order R of $\mathcal{A}_{p,\infty}$ and a set of left R-ideal class representatives $\{J_i\}$. As discussed in Section 2.3.1, this determines the set $\mathrm{Emb}_D(\mathcal{A}_{p,\infty})$ of optimal embeddings of $\mathcal{O}$ into one of the maximal orders $\{R_r(J_i)\}$. The following algorithm, introduced in 2.3.5, computes the action of $Cl(\mathcal{O})$ on the set $\mathrm{Emb}_D(\mathcal{A}_{p,\infty})$. We write $\mathcal{O} = \mathbb{Z}[\tau]$ and fix a $\mathbb{Z}$-basis $\{r_i\}$ for R. All computations in $\mathcal{A}_{p,\infty}$ take place with respect to this basis and the right orders of J_m and J_k are not explicitly computed.

Algorithm 2.3.1

INPUT:

- A basis $\{r_i\}$ for R
- An optimal embedding g given by $g(\tau) = y \in R_r(J_k)$ where $y = [y_1, ..., y_4]$ is in terms of $\{r_i\}$
- An integral ideal $\mathfrak{a} \in Cl(\mathcal{O})$ of norm a with $\mathfrak{a} = (a, c + d\tau)$

OUTPUT:

- The value $g^{\mathfrak{a}}(\tau) = w \in \mathcal{A}_{p,\infty}$, with $w = [w_1, ..., w_4]$ given in terms of $\{r_i\}$
- The left R-ideal class representative J_m such that $g^{\mathfrak{a}}$ is optimal with respect to $R_r(J_m)$

1. Compute the left ideal J of R equal to $J_k g(\mathfrak{a})$.
2. Compute a Minkowski-reduced basis $\{b_i\}$ for J and the set $V = \{v_s\}$ of elements of smallest norm, $n(J)$
3. Starting with $m = 1$, do the following sequence of steps for the left-ideal J_m of R:
    (a) Compute a Minkowski-reduced basis $\{b_{m,i}\}$ of J_m. Check if $n(J_m)n(b_i) = n(b_{m,i})n(J_k)a$ for each i. If so, let $s = 1$ and go to the Step 3b. If not, let $m = m + 1$ and repeat Step 3.
    (b) If $s > \#V$, let $m = m + 1$ and repeat Step 3. Let $x_s = b_{m,1}^{-1} v_s$. For $i = 2, 3, 4$, let $u_i \in \mathcal{A}_{p,\infty}$ be the element such that $b_{m,i}^{-1} b_i = u_i x_s$. Else let $s = s + 1$ and repeat Step 3b.
    (c) Compute the matrix $C = (c_{i,j})$ where $b_{m,i} u_i = \sum_j c_{i,j} b_{m,i}$. If C is invertible over $\mathbb{Z}$, let $x = x_s$ and go to Step 4. Else, let $s = s + 1$ and repeat Step 3b.
4. Return J_m and $w = xyx^{-1}$, expressed in terms of the basis $\{r_i\}$ of R.

In Step 1, let $\{b_{k,i}\}$ denote the $\mathbb{Z}$-basis for J_k. To compute a basis for $J = J_k g(\mathfrak{a})$ we use the LLL-algorithm for linearly dependent lattice vectors ([7, Algorithm 2.6.8]) on the set $\{ab_{k,i}, (c + dy)b_{k,i}\}_{i=1}^{4}$.

In Step 2, we use the Fincke-Pohst algorithm ([7, Algorithm 2.7.7]) to compute a set V of elements of minimal norm. We let b_1 be one of these vectors and compute $\{b_i\}$, a *Minkowski-reduced basis*. This is a basis of J such that b_1 is a shortest vector of the lattice J, the element b_2 is a next shortest vector such that $\{b_1, b_2\}$ extends to a basis of J, and so forth. While there is not necessarily a unique Minkowski-reduced basis, the norms of the elements $n(b_i)$ are unique.

In Step 3, if J_m is right-isomorphic to J, then there exists an $x \in \mathcal{A}_{p,\infty}$, unique up to left multiplication by a unit of $R_r(J_m)$, such that $J_m x = J$. This step is guaranteed to return such an x if J_m and J are left isomorphic. The norm of x is $n(J)/n(J_m) = n(J_k)a/n(J_m)$ which we denote it N.

Compute a Minkowski-reduced basis $\{b_{m,i}\}$ for the ideal J_m. Since the norms of any Minkowski-reduced basis of J are unique, if $J_m x = J$ for some x of norm N, then we must have $n(b_i) = n(b_{m,i})N$ for each i. Furthermore, the element $b_{m,1}x$ must appear in the set V of shortest vectors of J. Therefore, there exists some index s such that $x = b_{m,1}^{-1} v_s$. Thus we consider each $x_s = b_{m,1}^{-1} v_s$ as a candidate for x, and check whether or not $J_m x_s = J$. To do this, we attempt to find an invertible change of bases between $\{b_{m,i} x_s\}$ and $\{b_i\}$.

For $i = 2, 3, 4$, we let u_i be the element such that $b_{m,i}^{-1} b_i = u_i x_s$. Check that $b_{m_i} u_i$ is in J for each i. If so, compute the matrix $C = (c_{i,j})$ where $b_{m,i} u_i = \sum_j c_{i,j} b_{m,j}$. If C is invertible over $\mathbb{Z}$, then this gives a change of basis from $\{b_{m,i}\}$ to $\{b_{m,i} u_i\}$. Using the fact that $b_i = b_{m,i} u_i x_s$, we get that C gives a change of basis from $\{b_{m,i} x_s\}$ to $\{b_i\}$, and thus $J_m x_s = J$. On the other hand, if $J_m x_s = J$, then $\{b_i\}$ and $\{b_{m,i} x_s\}$ are both bases for J and thus the matrix C will be invertible.

We are guaranteed to find J_m such that J_m is right-isomorphic to J via x, since we consider all ideal class representatives for the left R-ideals, and for each of these, we consider all possible candidates for x.

The following algorithm is based on the algorithm in [6] which explicitly establishes the one-to-one correspondence in Theorem 2.2.4 between the $\mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$-conjugacy classes j of supersingular j-invariants and the maximal orders of $\mathcal{A}_{p,\infty}$, up to conjugacy.

Algorithm A.0.1

INPUT: A set $\{R_i\}$ of representatives of the conjugacy classes of maximal orders of the quaternion algebra $\mathcal{A}_{p,\infty}$

OUTPUT: A set $\{j_i\}$ of $\mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$-conjugacy classes of supersingular j-invariants such that for any curve E_i with j-invariant j_i, the ring $\mathrm{End}(E_i)$ is isomorphic to R_i.

We summarize the algorithm found in [6]. The conjugacy classes of maximal orders R_i are uniquely characterized by the set of elements of norm less than B, where the bound B is on the order of $p/12$, ([6, Prop. 3.3]):

$$S_{R_i,B} = \{(t(\alpha), n(\alpha)) |\ \alpha \in R_i \text{ and } n(\alpha) \leq B\}.$$

Therefore, the $\mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$-conjugacy classes of supersingular j-invariants are distinguishable by the set of endomorphisms of $\mathrm{End}(E_i)$ of degree less than B, where E_i is a curve with j-invariant j_i. Thus, to establish the correspondence, for each order R, we compute the set $S_{R_i,B}$ and for each representative j_i, we choose a curve E_i with j-invariant j_i and compute the set

$$S_{j_i,B} = \{(\mathrm{tr}(\alpha), \deg(\alpha)) |\ \alpha \in \mathrm{End}(E_i) \text{ and } \deg(\alpha) \leq B\}.$$

By comparing these sets, we obtain the correspondence. We can also use information about the unit group of R_i to directly identify $j = 0$ and $j = 1728$ with their respective orders. The run-time of the algorithm is $O(p^{5/4})$, thus it is feasible for small primes p. As the p-adic algorithm to compute $H_D(X)$ from Section 2.9 uses the smallest prime p which is inert in K and not dividing D, this is not an issue.

The following algorithm computes an embedding of the order $\mathcal{O}$ of $K = \mathbb{Q}(\sqrt{D})$ of discriminant D into R, a maximal order of $\mathcal{A}_{p,\infty}$. Furthermore, the embedding is optimal with respect to R. Writing $D = m^2\triangle$, for $\triangle$ a fundamental discriminant, we can express $\mathcal{O}$ as $\mathbb{Z}[\tau]$ where τ has characteristic polynomial

$$T(X) = \begin{cases} X^2 - X + \frac{1-D}{4} & D \equiv 1 \bmod 4 \\ X^2 + \frac{D}{4} & D \equiv 0 \bmod 4. \end{cases}$$

The algorithm returns an element w of $\mathcal{A}_{p,\infty}$ with characteristic polynomial $T(X)$ and an order R containing w for which the embedding specified by $g(\tau) = w$ is optimal. The algorithm is guaranteed to succeed as there exist $h(\mathcal{O})$ embeddings of $\mathcal{O}$ into $\mathcal{A}_{p,\infty}$ which are optimal with respect to some maximal order of $\mathcal{A}_{p,\infty}$, by Proposition 2.3.2.

Algorithm A.0.2

INPUT:

- $D < 0$
- A prime p such that p is inert in $K = \mathbb{Q}(\sqrt{D})$ and $p \nmid D$

OUTPUT:

- A maximal order R of $\mathcal{A}_{p,\infty}$ into which $\mathcal{O}$, the order of discriminant D, embeds optimally
- $g(\tau) = [w_1, ..., w_4]$ expressed in terms of a basis $\{r_i\}$ for R

1. Let
$$t, n = \begin{cases} 0, \frac{D}{4} & D \equiv 0 \bmod 4 \\ \\ 1, \frac{1-D}{4} & D \equiv 1 \bmod 4. \end{cases}$$

2. Compute $\{R_k\}_{k=1}^{t_p}$, a set of representatives of the conjugacy classes of maximal orders of $\mathcal{A}_{p,\infty}$.

3. Starting with $k = 1$, repeat the following until a pair R, w is returned.

   (a) Choose a basis $\{r_i\}$ of R_k with $r_4 = 1$. Compute $N(x_1, x_2, x_3, x_4)$, the norm form for $\mathcal{A}_{p,\infty}$ in terms of $\{r_i\}$. Compute $Tr(x_1, x_2, x_3, x_4)$, the trace form in terms of $\{r_i\}$. Let $Q(x_1, x_2, x_3)$ equal $N(x_1, x_2, x_3, x_4) - \frac{1}{4}Tr(x_1, x_2, x_3, x_4)^2$. Let S_k be an empty list.

   (b) Find a triple $(w_1, w_2, w_3) \in \mathbb{Z}^3$ such that $Q(w_1, w_2, w_3) + \frac{1}{4}t^2 = n$ and $(w_1, w_2, w_3) \notin S_k\}$. If none exist, repeat Step 3 with $k = k + 1$. Else, store the 3-tuple the list S_k and go to Step 3.

   (c) Compute the integer $w_4 \in \mathbb{Z}$ such that $Tr(w_1, w_2, w_3, w_4) = t$. Let $w = [w_1, w_2, w_3, w_4]$. This is an element with characteristic polynomial $T(X)$.

   (d) If D is a fundamental discriminant, return R_k and w. Else, for each pair $i, j \in \{1, ..., 4\}$, compute $\gcd(w_i, w_j)$. If there exists a pair with $\gcd$ equal to one, return R_k and w. Else, repeat Step 3b.

For Step 2, we use the characterization of maximal orders of $\mathcal{A}_{p,\infty}$ by ternary quadratic forms to compute representatives of the conjugacy classes of maximal orders of $\mathcal{A}_{p,\infty}$. (See Appendix B and [6] for more detail.)

For Step 3b, we consider the order R as a 4-dimensional lattice with quadratic form $N(x_1, ..., x_4)$. As $r_4 = 1$, the rational part of $N(x_1, ..., x_4)$ is simply $\frac{1}{4}Tr(x_1, ..., x_4)^2$. Thus $Q(x_1, x_2, x_3) + \frac{1}{4}t^2$ is a ternary quadratic form on the sublattice R_t of elements of trace t. This form is positive definite as $\mathcal{A}_{p,\infty}$ is ramified at ∞. We use the Fincke-Pohst algorithm [7, Alg. 2.7.7] to find all vectors of the lattice R_t of norm n. Once we find a solution (w_1, w_2, w_3) in Step 3b, we store in in S and keep note of where the search stopped. Thus, if the solution w in Step 3d is *not* optimal, when we return to Step 3b, we continue the search where we stopped. In this way, we eventually find all solutions to $Q(w_1, w_2, w_3) + t^2 = n$ for a particular maximal order R. If we do this for every maximal order, we are guaranteed to find an optimal embedding of $\mathcal{O}$ into some maximal order of $\mathcal{A}_{p,\infty}$, by Eichler's formula.

In Step 3c, we can find an *integer* w_4 such that $Tr(w_1, ..., w_4) = t$ as follows. By choice of (w_1, w_2, w_3), we have that $N(w_1, w_3, w_3, x_4) - \frac{1}{4}Tr(w_1, w_2, w_3, x_4)^2 = n - \frac{1}{4}t^2$ for any $x_4 \in \mathbb{Z}$. Therefore $Tr(w_1, w_2, w_3, x_4)$ and t have the same parity for any $x_4 \in \mathbb{Z}$. Letting $x_4 = 0$, we solve for $w_4 \in \mathbb{Z}$ such that $Tr(w_1, w_2, w_3, 0) - t$ equals $-2w_4$. Then $Tr(w_1, ..., w_4) = t$.

In Step 3d, we check that the embedding given by $\tau \mapsto [w_1, w_2, w_3, w_4]$ is optimal with respect to R. This is automatically true if D is a fundamental discriminant. Otherwise, it is true if only if there exist $i, j \in \{1, ..., 4\}$ such that $\gcd(w_i, w_j) = 1$ by Proposition 2.3.1. We can give a rough estimate on the probability that the element w gives an optimal embedding.

Let $\mathcal{O}'$ be an order containing $\mathcal{O}$. Every optimal embedding of $\mathcal{O}'$ into a maximal order of $\mathcal{A}_{p,\infty}$ corresponds to a non-optimal embedding of $\mathcal{O}$ into the same order. There are $h(\mathcal{O}')$ such embeddings, each given by an element of $\mathcal{A}_{p,\infty}$ with characteristic polynomial $T(X)$. An element of $\mathcal{A}_{p,\infty}$ may lie in more than one maximal order, and thus it may correspond to more than one embedding of $\mathcal{O}'$ into a maximal order of $\mathcal{A}_{p,\infty}$. Therefore, there are at most

$$\sum_{\mathcal{O}\subset\mathcal{O}'\subset\mathcal{O}_k} h(\mathcal{O}')$$

elements of the union $\bigcup_k R_k$ which have characteristic polynomial $T(X)$. Of these, at most $h(\mathcal{O})$ elements give optimal embeddings of $\mathcal{O}$ into some maximal order.

In Step 3, we enumerate all possible elements with characteristic polynomial $T(X)$ contained in one of the maximal orders R_k, with possible repetition if an element is contained in more than one maximal order. If d is the number of divisors of the conductor m of $\mathcal{O}$ in $\mathcal{O}_K$, then the probability we get an element corresponding to an optimal embedding is *roughly*

$$\frac{h(\mathcal{O})}{\sum_{\mathcal{O}\subset\mathcal{O}'\subset\mathcal{O}_k} h(\mathcal{O}')} > \frac{h(\mathcal{O})}{dh(\mathcal{O})} = \frac{1}{d}.$$

In particular, this says that if R_k contains $\mathcal{O}$ optimally, it is likely we will find an optimal embedding after d repetitions of Steps b-d. This heuristic assumes that elements corresponding to non-optimal and optimal embeddings are equally distributed. It also does not take into account the fact that the type number t_p and class number h_p of $\mathcal{A}_{p,\infty}$ may not be equal. That is, for a fixed maximal order R, and a set of left ideal classes J_i, a conjugacy class of a maximal order may be represented twice on the list $\{R_r(J_i\})$, which is of size h_p. These orders correspond precisely to the supersingular curves defined over $\mathbb{F}_{p^2}$ but not over $\mathbb{F}_p$, and embeddings into these conjugate orders are counted separately in the formula for $h(\mathcal{O})$.

We now give an algorithm to compute an explicit basis of endomorphisms for a supersingular elliptic curve E, given a basis $\{r_i\}$ of a maximal order R of $\mathcal{A}_{p,\infty}$ with $\mathrm{End}(E) \simeq R$. For one way to determine such a basis $\{r_i\}$, see the remark which follows this algorithm. For an alternate construction of an explicit basis of endomorphisms, see [33] or the algorithm in [23].

To specify a basis $\{e_1\}$ for the quaternion algebra $\mathrm{End}(E) \otimes \mathbb{Q}$, it suffices to specify the characteristic polynomials for each e_i and the relations $e_1e_2, e_2e_1, e_1e_3, e_3e_1, e_2e_3, e_3e_2$. Therefore we search for a set of endomorphisms of E satisfying the characteristic polynomials of the r_i and the relations $r_1r_2, r_2r_1, r_1r_3, r_3r_1, r_2r_3, r_3r_2$, expressed in terms of the basis $\{1, r_1, r_2, r_3\}$.

$$\begin{array}{lllllllll} r_1^2 & = & [n_1, t_1, 0, 0] & r_2^2 & = & [n_2, 0, t_2, 0] & r_3^2 & = & [n_3, 0, 0, t_3] \\ r_1r_2 & = & \dots & r_2r_1 & = & \dots & r_2r_3 & = & \dots \\ r_3r_2 & = & \dots & r_3r_1 & = & \dots & r_1r_3 & = & \dots \end{array} \tag{A.1}$$

Any two distinct bases of R satisfying the relations corresponds to an automorphism of $\mathcal{A}_{p,\infty}$, which by the theorem of Skolem-Noether, implies that one is the conjugate of the other by an element x. As $xRx^{-1} = R$, we have that the element x is in the normalizer of R, $\mathrm{Normalizer}(R)$. Furthermore, conjugation of a basis by any non-trivial x in $\mathrm{Normalizer}(R)$ gives another basis satisfying the same relations. Thus there are $\#(\mathrm{Normalizer}(R)/\mathbb{Q}^*)$ distinct bases satisfying a given set of relations.

By [42, Ex. III.5.4], for R a maximal order of $\mathcal{A}_{p,\infty}$, the group $\mathrm{Normalizer}(R)/\mathbb{Q}^*$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^m R^*$ with $m = 0$ or 1. Using the connection with supersingular curves, we have that the only endomorphisms of E which are in $\mathrm{Normalizer}(\mathrm{End}(E))$

are those whose kernels are stabilized by every $\alpha \in \mathrm{End}(E)$ [26, Thm. 13.3.10]. Such endomorphisms must either be in the center of $\mathrm{End}(E)$ or they must have no kernel. Therefore the only elements of $\mathrm{Normalizer}(\mathrm{End}(E))/\mathbb{Q}^*$ are either automorphisms or powers of the Frobenius element. For a supersingular curve defined over $\mathbb{F}_p$, the Frobenius element π_p is an endomorphism and does not commute with $\mathrm{End}(E)$ ([46]). Furthermore, as E is supersingular, we have $\pi_p^2 = [p]$. Thus $m = 1$. For a supersingular curve E not defined over $\mathbb{F}_p$, we have $m = 0$, since the Frobenius endomorphism is $\pi_p^2 = [p]$ which commutes with all endomorphisms of E. Thus the number of distinct bases of $\mathrm{End}(E)$ satisfying a given set of relations is

$$N = \begin{cases} 2|\#\mathrm{Aut}(E)/\{\pm 1\}| & j(E) \in \mathbb{F}_p \\ \\ |\#\mathrm{Aut}(E)/\{\pm 1\}| & j(E) \in \mathbb{F}_{p^2}. \end{cases}$$

Algorithm A.0.3

INPUT:

- The relations (A.1) for a basis $\{r_i\}$ of a maximal order R of $\mathcal{A}_{p,\infty}$, with $r_4 = \mathrm{Id}$
- An elliptic curve E with $\mathrm{End}(E) \simeq R$

OUTPUT: A set B of all bases $\{e_i\}$ of endomorphisms of E satisfying the relations (A.1)

1. Work over an extension of $\mathbb{F}_{p^2}$ of degree at least 2. Let P be a random point not of order 2.

2. Factor the n_1-division polynomial of E. For each factor $F(x)$, use Vélu's formulas to compute the j-invariant of the isogenous curve E'. If $j(E') = j(E)$, compute the explicit isogeny $\varphi : E \to E'$ and an isomorphism $\gamma : E' \to E$. For $\delta \in \mathrm{Aut}(E)$,

include $\delta\gamma\varphi$ in the set B_1. For each $\phi \in B_1$, test if ϕ satisfies the relation $r_1^2 = t_1r_1 + n_1$ on P. If not, discard ϕ from B_1. These are all the candidates for the endomorphism e_1.

3. Factor the n_2-division polynomial of E. For each factor $F(x)$, use Vélu's formulas to compute the j-invariant of the isogenous curve E'. If $j(E') = j(E)$, compute the explicit isogeny $\varphi : E \to E'$ and an isomorphism $\gamma : E' \to E$. For $\delta \in \mathrm{Aut}(E)$, include $\delta\gamma\varphi$ in the set B_2. For each $\phi \in B_2$, test if ϕ satisfies the relation $r_2^2 = t_2r_2 + n_2$ on P. If not, discard ϕ from B_2. These are candidates for the endomorphism e_2.

4. For each $\phi_1 \in B_1$, do the following:

   (a) For each $\phi_2 \in B_2$,

      i. Let $r_1 = \phi_1$ and $r_2 = \phi_2$ and determine ϕ_3 uniquely using one of the relations in (A.1).

      ii. Check that the remaining six relations are satisfied on the point P. If not, discard ϕ_2 and go back to step 4a. Else, store the tuple $(\phi_1, \phi_2, \phi_3, 1)$ in the set B of possible bases for $\mathrm{End}(E)$.

5. If $\#B = N$, return B. Else choose another random point P, and for each tuple in B, check that the nine relations are satisfied on the point P, discarding those that fail. Then repeat Step 5.

Remark A.0.1

Given a curve E, we may use the algorithm of Cerviño [6] to find the ternary quadratic form associated to the maximal order R such that $\mathrm{End}(E) \simeq R$. That is, we use the explicit bijection between the classes of ternary quadratic forms of discriminant $-p$ and the conjugacy classes of maximal orders of $\mathcal{A}_{p,\infty}$ [4]. The coefficients of the form $f = a_{11}x_1^2 + a_{22}x_2^2 + a_{33}x_3^2 + a_{12}x_1x_2 + a_{13}x_1x_3 + a_{23}x_2x_3$ determine a $\mathbb{Z}$-basis for a maximal order R_f of $\mathcal{A}_{p,\infty}$. Letting (i, j, k) equal $(1, 2, 3), (2, 3, 1)$, and $(3, 1, 2)$ (all even permutations of $1, 2$ and 3) we get a set of nine relations which uniquely determine R_f:

$$\begin{aligned} r_i^2 &= a_{jk}r_i - a_{jj}a_{kk} \\ r_ir_j &= a_{kk}a_{ij} - a_{kk}r_k \\ r_jr_i &= a_{1k}r_1 + a_{2k}r_2 + a_{3k}r_3 - a_{ik}a_{jk}. \end{aligned} \tag{A.2}$$

We represent the form f by the matrix of coefficients

$$M_f = \begin{pmatrix} a_{11} & a_{22} & a_{33} \\ a_{23} & a_{13} & a_{12} \end{pmatrix}$$

Tables for the classes of ternary quadratic forms of discriminant $-p$ up to $p = 1000$ are found in [4].

Appendix B

Explicit Bases of $\mathrm{End}(E)$ for $E/\mathbb{F}_{p^2}$ with $p = 3, 5, 7, 13$ and 37

In this Appendix, we give explicit bases for the endomorphism rings of a representative of the unique class of supersingular curves over $\mathbb{F}_{p^2}$ for $p = 3, 5, 7$ and 13. In this case, we use MAGMA to compute a representative R of the maximal order of $\mathcal{A}_{p,\infty}$ and a Minkowski-reduced basis $\{r_i\}$. We then use Algorithm A.0.3 from Appendix A to compute the bases.

We also give the basis for the endomorphism ring of a curve E with j-invariant 8 over $\mathbb{F}_{p^2}$ where $p = 37$, from the example from Section 2.4. See the example or Algorithm A.0.1 for how to determine which maximal order R of $\mathcal{A}_{p,\infty}$ is isomorphic to $\mathrm{End}(E)$.

Let E be a curve over $\mathbb{F}_{p^2}$. Given a subgroup G_N of $E[N]$ of order N, we let E/G_N denote the unique curve (up to automorphism) such that the isogeny $E \to E/G_N$ with kernel G_N is *normalized* (see 2.2.1). This curve can be computed using Vélu's formulas [41]. We record an endomorphism of E with kernel G_N as a pair $(P(X), (u, r))$ where $P(X)$ is the polynomial whose roots are the x-coordinates of the points of G_N and (u, r) defines the isomorphism $h : E/G_N \to E$ given by $(x, y) \to (u^2x + r, u^3y)$.

B.1 $\quad p = 3$

The quaternion algebra $\mathcal{A}_{p,\infty}$ for $p = 3$ can be given by $\left(\frac{-1,-3}{\mathbb{Q}}\right)$, where

$$i^2 = -1, j^2 = -3, ij = k, ij = -ji.$$

The single conjugacy class of maximal orders of $\mathcal{A}_{p,\infty}$ has the representative R with basis of elements of norm one

$$\{r_1, ..., r_4\} = \{(1+j)/2, -(i-k)/2, -i, 1\}.$$

The basis relations are given by the following tuples of coefficients of $1, r_1, r_2, r_3$:

$$\begin{array}{rclrclrcl} r_1^2 & = & [-1,0,0,0] & r_2^2 & = & [-1,0,1,0] & r_3^2 & = & [-1,0,0,0] \\ r_1r_2 & = & [0,1,0,-1] & r_2r_1 & = & [0,0,0,1] & r_2r_3 & = & [0,-1,0,1] \\ r_3r_2 & = & [0,0,-1,0] & r_3r_1 & = & [0,1,0,0] & r_1r_3 & = & [-1,0,1,0]. \end{array}$$

The curve $L : y^2 = x(x-1)(x+1)$ has $j(E) = 0$. Let $\mathbb{F}_{p^2} = \mathbb{F}_p[a]$ where a is a root of $x^2+1 = 0$. The basis for $\mathrm{End}(L)$ is given by $\{e_1, .., e_4\}$ where

	$P(X)$	u	r
e_1	1	$2a$	2
e_2	1	a	0

$e_2 = -e_3 \circ e_1$, and $e_4 = \mathrm{Id}$. The map $i : r_i \mapsto e_i$ is an isomorphism $R \to \mathrm{End}(L)$.

B.2 $p = 5$

The quaternion algebra $\mathcal{A}_{p,\infty}$ for $p = 5$ can be given by $\left(\frac{-2,-5}{\mathbb{Q}}\right)$, where

$$i^2 = -2, j^2 = -5, ij = k, ij = -ji.$$

The single conjugacy class of maximal orders of $\mathcal{A}_{p,\infty}$ has the representative R with basis

$$\{r_1, r_2, r_3, r_4\} = \{1/2 + i/4 - k/4, 1/2 - 3i/4 - k/4, -i/4 - j/2 - k/4, 1\}.$$

The basis relations are given by the following tuples of coefficients of $1, r_1, r_2, r_3$:

$$\begin{array}{rclrclrcl}
r_1^2 & = & [-1,1,0,0] & r_2^2 & = & [-2,0,1,0] & r_3^2 & = & [-2,0,0,0] \\
r_1r_2 & = & [-1,1,1,-1] & r_2r_1 & = & [0,0,0,1] & r_2r_3 & = & [0,-2,0,1] \\
r_3r_2 & = & [-2,2,0,0] & r_3r_1 & = & [0,0,-1,1] & r_1r_3 & = & [-1,0,1,0].
\end{array}$$

Let $\mathbb{F}_{p^2} = \mathbb{F}_p[a]$ where a is a root of $x^2 + 2 = 0$. The curve $L : y^2 = x(x-1)(x-(a+3))$ has $j(E) = 0$. The basis for $\mathrm{End}(L)$ is given by $\{e_1, .., e_4\}$ where

	$P(X)$	u	r
e_1	1	$a+3$	1
e_2	$X+4$	$a+4$	$2a+3$

$e_3 = e_2 \circ e_1$, and $e_4 = \mathrm{Id}$. The map $i : r_i \mapsto e_i$ is an isomorphism $R \to \mathrm{End}(L)$.

B.3 $p = 7$

The quaternion algebra $\mathcal{A}_{p,\infty}$ for $p = 7$ can be given by $\left(\frac{-1,-7}{\mathbb{Q}}\right)$, where

$$i^2 = -1, j^2 = -7, ij = k, ij = -ji.$$

The single conjugacy class of maximal orders of $\mathcal{A}_{p,\infty}$ has the representative R with basis

$$\{r_1, r_2, r_3, r_4\} = \{i, (i+k)/2, (1+j)/2, 1\}.$$

The basis relations are given by the following tuples of coefficients of $1, r_1, r_2, r_3$:

$$\begin{array}{rclrclrcl}
r_1^2 & = & [-1,0,0,0] & r_2^2 & = & [-2,0,0,0] & r_3^2 & = & [-2,0,0,1] \\
r_1r_2 & = & [0,0,0,-1] & r_2r_1 & = & [-1,0,0,1] & r_2r_3 & = & [0,-2,1,0] \\
r_3r_2 & = & [0,2,0,0] & r_3r_1 & = & [0,1,-1,0] & r_1r_3 & = & [0,0,1,0].
\end{array}$$

The curve $L : y^2 = x(x-1)(x-2)$ has $j(E) = 1728$. Let $\mathbb{F}_{p^2} = \mathbb{F}_p[a]$ where a is a root of $x^2 + 2 = 0$. The basis for $\mathrm{End}(L)$ is given by $\{e_1, .., e_4\}$ where

	$P(X)$	u	r
e_1	1	$5a$	2
e_2	$X+5$	$3a$	1

$e_3 = -e_1 \circ e_2$, and $e_4 = \mathrm{Id}$. The map $i : r_i \mapsto e_i$ is an isomorphism $R \to \mathrm{End}(L)$.

B.4 $p = 13$

The quaternion algebra $\mathcal{A}_{p,\infty}$ for $p = 13$ can be given by $\left(\frac{-2,-13}{\mathbb{Q}}\right)$, where

$$i^2 = -2, j^2 = -13, ij = k, ij = -ji.$$

The single conjugacy class of maximal orders of $\mathcal{A}_{p,\infty}$ has the representative R with basis

$$\{r_1, ..., r_4\} = \{1/2 - i/4 + k/4, -i, 1/2 - i/2 - j/2, 1\}.$$

The basis relations are given by the following tuples of coefficients of $1, r_1, r_2, r_3$:

$$\begin{array}{rclrclrcl} r_1^2 &=& [-2,1,0,0] & r_2^2 &=& [-2,0,0,0] & r_3^2 &=& [-4,0,0,1] \\ r_1r_2 &=& [-1,0,0,1] & r_2r_1 &=& [0,0,1,-1] & r_2r_3 &=& [-2,2,0,0] \\ r_3r_2 &=& [0,-2,1,0] & r_3r_1 &=& [0,0,2,0] & r_1r_3 &=& [-1,1,2,1]. \end{array}$$

The curve $E : y^2 = x^3 + 10x + 6$ has $j(E) = 5$. Let $\mathbb{F}_{p^2} = \mathbb{F}_p[a]$ where a is a root of $x^2 + 2 = 0$. The basis for $\mathrm{End}(E)$ is given by $\{e_1, .., e_4\}$ where

	$P(X)$	u	r
e_1	$X + 4a + 4$	$5a + 10$	0
e_2	$X+5$	$7a$	0

$e_3 = \mathrm{Id} + e_1 \circ e_2$, and $e_4 = \mathrm{Id}$. The map $i : r_i \mapsto e_i$ is an isomorphism $R \to \mathrm{End}(E)$.

B.5 $p = 37$

The quaternion algebra $\mathcal{A}_{p,\infty}$ for $p = 37$ can be given by $\left(\frac{-2,-37}{\mathbb{Q}}\right)$, where

$$i^2 = -2, j^2 = -37, ij = k, ij = -ji.$$

The maximal order R of $\mathcal{A}_{p,\infty}$ with basis

$$\{r_1, ..., r_4\} = \{i, 1/2 - i/4 + k/4, -1/2 + i/2 + j/2, 1\}$$

is isomorphic to $\mathrm{End}(E)$ where $j(E) = 8$. The basis relations are given by the following tuples of coefficients of $1, r_1, r_2, r_3$:

$$\begin{array}{rclrclrcl}
r_1^2 &=& [-2,0,0,0] & r_2^2 &=& [-5,0,1,0] & r_3^2 &=& [-10,0,0,-1] \\
r_1r_2 &=& [0,1,0,-1] & r_2r_1 &=& [1,0,0,1] & r_2r_3 &=& [1,-5,-1,1] \\
r_3r_2 &=& [0,5,0,0] & r_3r_1 &=& [0,-1,-2,0] & r_1r_3 &=& [-2,0,2,0].
\end{array}$$

Let $\mathbb{F}_{p^2} = \mathbb{F}_p[a]$ where a is a root of $x^2 + 2 = 0$. The curve $E : y^2 = x^3 + 12x + 13$ has $j(E) = 8$. The basis for $\mathrm{End}(E)$ is given by $\{e_1, .., e_4\}$ where

	$P(X)$	u
e_2	$X + 1$	$19a$
e_3	$X^2 + (8a + 29)X + (4a + 23)$	$24a + 26$

$e_3 = e_1 \circ e_2$, and $e_4 = \mathrm{Id}$. The map $i : r_i \mapsto e_i$ is an isomorphism $R \to \mathrm{End}(E)$.

Bibliography

[1] L. Ahlfors. *Complex analysis*. McGraw-Hill, 3rd edition, 1979.

[2] J. Belding, R. Bröker, A. Enge, and K. Lauter. Computing Hilbert class polynomials. To appear in proceedings of *ANTS VIII*, 2007.

[3] W. Bley. Konstruktion von Ganzheitsbasen in abelschen Körpererweiterungen von imaginär- quadratischen Zahlk ?orpern. *J. Number Theory*, 46(3):334–371, 1994.

[4] H. Brandt and O. Intrau. Tabellen reduzirter positiver ternärer quadratischer formen. *Abh. der Sächsischen Akad. der Wissenschaften zu Leipzig*, 45, 1958.

[5] R. Bröker. A p-adic algorithm to compute the Hilbert class polynomial. To appear in *Math. Comp.*, 2007.

[6] J. M. Cerviño. Supersingular elliptic curves and maximal quaternionic orders. In *Math. Institut G-A-Univ. Göttingen*, pages 53–60, 2004.

[7] H. Cohen. *A course in computational algebraic number theory*. GTM 138. Springer-Verlag, New York, 3rd edition, 1996.

[8] H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen, and F. Vercauteren. *Handbook of elliptic and hyperelliptic curve cryptography*. Discrete mathematics and its applications. Chapman & Hall, 2006.

[9] MAGMA computer algebra system. *MAGMA documentation*. University of Sydney, 2008.

[10] J.-M. Couveignes and T. Henocq. Action of modular correspondences around CM points. In C. Fieker and D. Kohel, editors, *ANTS-V*, volume 2369 of *LNCS*, pages 234–243. Springer-Verlag, 2002.

[11] D. A. Cox. *Primes of the form $x^2 + ny^2$*. John Wiley & Sons, 1989.

[12] A.J. de Jong. Families of curves and alterations. *Ann. Inst. Fourier*, 47:599–621, 1997.

[13] I. Dechêne. Arithmetic in generalized jacobians. In *ANTS-VII*, volume 4076 of *Lecture Notes in Computer Science*, pages 421–435, 2006.

[14] M. Deuring. Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. *Abh Math. Sem. Univ. Hamburg*, 14:197–272, 1941.

[15] F. Diamond and J. Shurman. *A first course in modular forms*. GTM 228. Springer-Verlag, New York, 1st edition, 2005.

[16] M. Eichler. The basis problem for modular forms and the traces of the hecke operators. *Lecture Notes in Math., Springer*, (320):75–152, 1973.

[17] A. Enge. The complexity of class polynomial computation via floating point approximations. HAL-INRIA 1040 and ArXiv cs.CC/0601104, INRIA, 2006.

[18] G. Frey and H. Rück. A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves. *Mathematics of Computation*, 62(206):865–874, 1994.

[19] B. H. Gross. Heights and special values of l-series. In *CMS Proceedings, AMS*, volume 7, pages 115–187, 1986.

[20] B. H. Gross and D. B. Zagier. On singular moduli. *J. Reine Angew. Math.*, 355(2):191–220, 1985.

[21] J. Igusa. Fibre systems of jacobian varieties iii. *American Journal of Mathematics*, 81(2):453–476, 1959.

[22] N. Katz and B. Mazur. *Arithmetic moduli of elliptic curves*. AM 108. Princeton University Press, 1985.

[23] D. Kohel. *Endomorphism rings of elliptic curves over finite fields*. PhD thesis, University of California at Berkeley, 1996.

[24] N. Kunihiro and K. Koyama. Two discrete log algorithms for super-anomalous elliptic curves and their applications. *IEICE Trans. Fundamentals*, E83-A(1):10–16, 2000.

[25] S. Lang. *Algebraic number theory*. Addison-Wesley, 1st edition, 1970.

[26] S. Lang. *Elliptic functions*. GTM 112. Springer-Verlag, New York, 2nd edition, 1987.

[27] H. Matsumura. *Commutative ring theory*, volume 112 of *Cambridge Studies in advanced mathematics*. Cambridge University Press, 1986.

[28] A. J. Menezes, T. Okamoto, and S.A. Vanstone. Reducing elliptic curve logarithms to logarithms in a finite field. *IEEE Trans. Inform. Theory*, 39:1639–1646, 1993.

[29] J.-F. Mestre. Sur la méthode des graphes, exemples et applications. *Proceedings of the international conference on class numbers and fundamental units of algebraic number fields*, pages 217–242, 1986.

[30] V. Miller. The Weil pairing, and its efficient calculation. *Journal of Cryptology*, 17:235–261, 2004.

[31] D.Y. Pei and Y.F. Zhu. An algorithm for dlp on anomalous elliptic curves over $\mathbb{F}_p$. *Science in China, Series A, Math, physics, astronomy*, 45(6):773–777, 2002.

[32] M. Rapoport and P. Deligne. Les schémas de modules de courbes elliptiques. *LNM Springer*, 249:143–316, 1972.

[33] E. Riboulet-Deyris. *Calculs despaces de modules par déformations en égales et inégales caractéristiques*. PhD thesis, Université Paul Sabatier, Toulouse III, 2004.

[34] J. B. Rosser and L. Schoenfeld. Approximate formulas for some functions of prime numbers. *Illinois J. Math.*, 6:64–94, 1962.

[35] H. Rück. On the discrete logarithm in the divisor class group of curves. *Mathematics of Computation*, 68(226):805–806, 1999.

[36] I.A. Semaev. Evaluation of discrete logarithms in a group of p-torsion points of an elliptic curve in characteristic p. *Mathematics of Computation*, 67(221):353–356, 1998.

[37] J-P. Serre. *Sur la topologie des variétés algébriques en caractéristique p.* Springer-Verlag, 1986.

[38] J. Silverman. *The arithmetic of elliptic curves.* GTM 106. Springer-Verlag, 1986.

[39] N. Smart. The discrete logarithm problem on elliptic curves of trace one. *Journal of Cryptology*, 12:193–196, 1999.

[40] H. Söhngen. Zur komplexen Multiplikation. *Math. Ann.*, 111:302–328, 1935.

[41] J. Vélu. Isogénies entre courbes elliptiques. *C. R. Acad. Sci. Paris, Sér A*, 273:238–241, 1971.

[42] M.-F. Vignéras. *Arithmétique des algèbres de quaternions.* LNM 800. Springer-Verlag, New York, 1980.

[43] M. Virat. A cryptosystem “à la” ElGamal on an elliptic curve over $K[\epsilon]$. In *Proceedings of Western European workshop on research in cryptography*, pages 32–44, 2005.

[44] J. Voight. Algorithms for quaternion algebras. In preparation, 2008.

[45] L.C. Washington. *Elliptic curves: number theory and cryptography*. Discrete math and its applications. Chapman & Hall/CRC, 2003.

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