THE UNIVERSITY OF WARWICK

Library Declaration and Deposit Agreement

1. STUDENT DETAILS

Please complete the following:

Full name: ……

University ID number: ……

2. THESIS DEPOSIT

2.1 I understand that under my registration at the University, I am required to deposit my thesis with the University in BOTH hard copy and in digital format. The digital version should normally be saved as a single pdf file.

2.2 The hard copy will be housed in the University Library. The digital version will be deposited in the University's Institutional Repository (WRAP). Unless otherwise indicated (see 2.3 below) this will be made openly accessible on the Internet and will be supplied to the British Library to be made available online via its Electronic Theses Online Service (EThOS) service.
[At present, theses submitted for a Master's degree by Research (MA, MSc, LLM, MS or MMedSci) are not being deposited in WRAP and not being made available via EthOS. This may change in future.]

2.3 In exceptional circumstances, the Chair of the Board of Graduate Studies may grant permission for an embargo to be placed on public access to the hard copy thesis for a limited period. It is also possible to apply separately for an embargo on the digital version. (Further information is available in the *Guide to Examinations for Higher Degrees by Research*.)

2.4 *If you are depositing a thesis for a Master's degree by Research, please complete section (a) below. For all other research degrees, please complete both sections (a) and (b) below:*

(a) Hard Copy

I hereby deposit a hard copy of my thesis in the University Library to be made publicly available to readers (please delete as appropriate) EITHER immediately OR after an embargo period of ……..... months/years as agreed by the Chair of the Board of Graduate Studies.

I agree that my thesis may be photocopied. YES / NO (*Please delete as appropriate*)

(b) Digital Copy

I hereby deposit a digital copy of my thesis to be held in WRAP and made available via EThOS.

Please choose one of the following options:

EITHER My thesis can be made publicly available online. YES / NO (*Please delete as appropriate*)

OR My thesis can be made publicly available only after…..[date] (Please give date)
YES / NO (*Please delete as appropriate*)

OR My full thesis cannot be made publicly available online but I am submitting a separately identified additional, abridged version that can be made available online.
YES / NO (*Please delete as appropriate*)

OR My thesis cannot be made publicly available online. YES / NO (*Please delete as appropriate*)

3. GRANTING OF NON-EXCLUSIVE RIGHTS

Whether I deposit my Work personally or through an assistant or other agent, I agree to the following:

Rights granted to the University of Warwick and the British Library and the user of the thesis through this agreement are non-exclusive. I retain all rights in the thesis in its present version or future versions. I agree that the institutional repository administrators and the British Library or their agents may, without changing content, digitise and migrate the thesis to any medium or format for the purpose of future preservation and accessibility.

4. DECLARATIONS

(a) I DECLARE THAT:

- I am the author and owner of the copyright in the thesis and/or I have the authority of the authors and owners of the copyright in the thesis to make this agreement. Reproduction of any part of this thesis for teaching or in academic or other forms of publication is subject to the normal limitations on the use of copyrighted materials and to the proper and full acknowledgement of its source.

- The digital version of the thesis I am supplying is the same version as the final, hard-bound copy submitted in completion of my degree, once any minor corrections have been completed.

- I have exercised reasonable care to ensure that the thesis is original, and does not to the best of my knowledge break any UK law or other Intellectual Property Right, or contain any confidential material.

- I understand that, through the medium of the Internet, files will be available to automated agents, and may be searched and copied by, for example, text mining and plagiarism detection software.

(b) IF I HAVE AGREED (in Section 2 above) TO MAKE MY THESIS PUBLICLY AVAILABLE DIGITALLY, I ALSO DECLARE THAT:

- I grant the University of Warwick and the British Library a licence to make available on the Internet the thesis in digitised format through the Institutional Repository and through the British Library via the EThOS service.

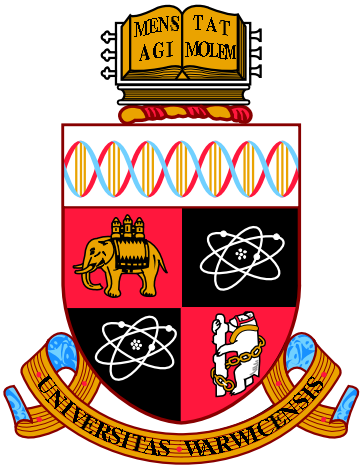
- If my thesis does include any substantial subsidiary material owned by third-party copyright holders, I have sought and obtained permission to include it in any version of my thesis available in digital format and that this permission encompasses the rights that I have granted to the University of Warwick and to the British Library.

5. LEGAL INFRINGEMENTS

I understand that neither the University of Warwick nor the British Library have any obligation to take legal action on behalf of myself, or other rights holders, in the event of infringement of intellectual property rights, breach of contract or of any other right, in the thesis.

Please sign this agreement and return it to the Graduate School Office when you submit your thesis.

Student's signature: .....…… Date: .....



Explicit isogenies of elliptic curves

by

Kiminori Tsukazaki

Thesis

Submitted to the University of Warwick

for the degree of

Doctor of Philosophy

Mathematics Institute

July 2013

THE UNIVERSITY OF
WARWICK

Contents

Acknowledgments

I would like to thank my supervisor Professor John E. Cremona for his valuable guidance and support throughout my Ph.D. period. He has been a great mentor since I started my MSc course under his supervision. I would also like to thank Professor Samir Siksek for his care and guidance and for funding my research. I am grateful to all the members in Warwick Number Theory Group, especially to Alex Bartel, Martin Bright, Haluk Sengun, Jeroen Sijsling and Damiano Testa for their support and useful discussions towards completion of my thesis. I am very thankful to all the staffs in Mathematics Institute for supporting my eight years of student life at Warwick. Furthermore, I would like to thank Mathematics Institute for funding my Ph.D. research.

Thank you very much to my parents, who have continuously supported me during my study in UK. Finally, I would like to give my special thanks to Soma for all her care and support.

Declarations

I hereby declare that all the work in this thesis is my own work, unless otherwise stated. Chapter 2 contains basic background material that can be found in the literature, and Chapter 3, 4 and 5 are entirely my own work, except for the part explicitly indicated otherwise.

Abstract

Let E be an elliptic curve defined over a field K. The main topic of this thesis is to present a method for the explicit computation of all separable K-rational ℓ-isogenies of E and isogenous curves for small primes ℓ. The key tool for this explicit computation is that the modular curve $X_0(\ell)$ parametrises ℓ-isogenies of elliptic curves. In [3], Cremona and Watkins give explicit isogeny formulae for $\ell \in \{2, 3, 5, 7, 13\}$, where the modular curve $X_0(\ell)$ has genus 0. Their formula allow us to compute ℓ-isogenies of E by simply substituting its j-invariant and twisting parameter into the formulae. We extend the work of Cremona and Watkins to the cases $\ell \in \{11, 17, 19, 23, 29, 31, 41, 47, 59, 71\}$, where the genus of $X_0(\ell)$ is greater than 0 but the modular curve $X_0^+(\ell)$ has genus 0.

Chapter 1

Introduction

The main problem we consider in this thesis is the following.

Problem 1.0.1. *Let E be an elliptic curve defined over a field K. For small primes ℓ, compute:*

(1) all separable K-rational ℓ-isogenies of E, up to equivalence.

(2) equations for the isogenous curves.

We say that two isogenies ϕ and ϕ' of an elliptic curve are *equivalent* if $\ker(\phi) = \ker(\phi')$. Moreover, if an isogeny ϕ is separable then $\deg(\phi) = \#\ker(\phi)$. If the characteristic of K is not ℓ then it is well-known that $E[\ell] \cong \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$, which contains $\ell+1$ subgroups of order ℓ. Once we have an order ℓ subgroup $H \subseteq E(\overline{K})$ that is defined over K (i.e. $P \in H$ implies $P^\sigma \in H$ for all $\sigma \in \mathrm{Gal}(\overline{K}/K)$), then there exists a separable K-rational ℓ-isogeny ϕ of E to some elliptic curve E' defined over K. Thus there are at most $\ell + 1$ K-rational ℓ-isogenies of E, up to equivalence.

Vélu [19] gave explicit formulas for ϕ and E' in terms of the coordinates of the points in the kernel H. Later Vélu's formula was modified by Kohel [10]; he introduced the idea of computing ϕ and E' from the associated *kernel polynomial* defined over K, the unique monic polynomial of the smallest degree such that the roots are the x-coordinates of the points in the kernel H. Hence Problem 1.0.1 is reduced to computing the associated kernel polynomials that are defined over K. The rational functions associated to the isogeny can

be computed from the associated kernel polynomial by either `Sage` [15] or `MAGMA` [11].

Cremona and Watkins in their unpublished preprint [3] gave a method for computing kernel polynomials for ℓ-isogenies for $\ell \in \{2, 3, 5, 7, 13\}$, where the modular curve $X_0(\ell)$ has genus 0. The great advantage of their method is that it gives a completely explicit formula for the so-called "generic kernel polynomial", for which we can compute kernel polynomials of a given elliptic curve by simply substituting the j-invariant and a suitable "twisting parameter" of E into the formula. Thus we can compute the generic kernel polynomial once and for all for each ℓ and then specialize to a given curve. Moreover, their method also works over a finite field by first computing in characteristic zero and then reducing.

In Chapter 2, we review the definitions and properties of elliptic curves, isogenies of elliptic curves, modular curves, modular forms and modular functions, which will be required in the later chapters.

In Chapter 3 we give a method called the "Division polynomial factorization method" for computing kernel polynomials for ℓ-isogenies of E. The main advantage of this method is that it works for any prime ℓ and over a field of any characteristic, although it becomes slower for larger ℓ since we need to compute and factorize a polynomial of degree $\frac{\ell^2-1}{2}$. Note that this method is completely algebraic in the sense that it simply involves a factorization of the ℓ-division polynomial of E and does not involve any analytic tools such as modular curves, modular functions and q-expansions.

In Chapter 4 we give the method for computing ℓ-isogenies by using the generic kernel polynomials for $\ell \in \{2, 3, 5, 7, 13\}$ in detail, following Cremona and Watkins [3]. Then in Chapter 5 we extend the method described in Chapter 4 to the cases $\ell \in \{11, 17, 19, 23, 29, 31, 41, 47, 59, 71\}$, where the genus of the modular curve $X_0(\ell)$ is greater than 0 but $X_0^+(\ell)$ has genus 0. The work in Chapter 5 is based on the work of Elkies [7], but the main advantage of our method presented in this thesis is that it works even if the characteristic of the field is sufficiently small, whereas the method of Elkies [7] or Bostan et al [1] requires that the characteristic of the field is sufficiently larger than the degree of isogeny. We will give some illustrative examples for our method, and all the algorithms developed in this thesis are fully implemented in `SAGE`.

Finally, in Appendix A we give tables of data used for the method presented in Chapter 5.

Chapter 2

Background

This chapter contains reviews of the basic material used in the thesis. We refer to the books of Silverman [17], Galbraith [8] and Diamond and Shurman [5] for most of the details and omitted proofs. Throughout this thesis let K denote a field and $\mathrm{char}(K)$ denote the characteristic of K, and let $\overline{K}$ denote the separable closure of K.

2.1 Elliptic curves

An *elliptic curve* E over a field K is a non-singular projective curve of genus 1 with a specified basepoint $\mathcal{O}$ that is defined over K. Using the Riemann-Roch theorem, one can show that every elliptic curve has a plane model given by a *Weierstrass equation*

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \tag{2.1}$$

where $a_1, ..., a_6 \in K$ (see [17, Proposition III.3.1]). Here $\mathcal{O} = [0 : 1 : 0]$ is the basepoint, which we call the *point at infinity* of E. By using the coordinates $x = X/Z$ and $y = Y/Z$, we obtain an affine Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{2.2}$$

In this thesis we will usually assume that an elliptic curve E is given by an affine Weierstrass equation as in (2.2). We also define the following quantities

associated to E:

$$b_2 = a_1^2 + 4a_2, \qquad b_4 = a_1a_3 + 2a_4, \qquad b_6 = a_3^2 + 4a_6,$$
$$b_8 = a_1^2a_6 - a_1a_3a_4 + 4a_2a_6 + a_2a_3^2 - a_4^2.$$

We further define:

$$c_4 = b_2^2 - 24b_4, \qquad c_6 = -b_2^3 + 36b_2b_4 - 216b_6,$$
$$\Delta(E) = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6,$$
$$j(E) = c_4^3/\Delta.$$

We refer to b_2, b_4, b_6 and b_8 as the *b-invariants* and c_4, c_6 as the *c-invariants* of E. The constant $\Delta(E)$ is called the *discriminant* of E, and a Weierstrass equation given by (2.2) is non-singular if and only if $\Delta(E)$ is non-zero. The constant $j(E)$ is called the *j-invariant* of E. It turns out that two elliptic curves E and E' over K are isomorphic over the algebraic closure of K if and only if $j(E) = j(E')$.

Transformations

Let E be an elliptic curve over K given in the form (2.2). If $\mathrm{char}(K) \neq 2$, then applying $(x, y) \mapsto (x, \frac{1}{2}(y - a_1x - a_3))$ gives

$$y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6. \tag{2.3}$$

Further if $\mathrm{char}(K) \neq 3$, then applying $(x, y) \mapsto (\frac{x-3b_2}{36}, \frac{y}{108})$ to (2.3) yields

$$y^2 = x^3 - 27c_4x - 54c_6. \tag{2.4}$$

Twists

Let E be an elliptic curve over K given by the form $y^2 = x^3 + a_2x^2 + a_4x + a_6$ and let $d \in K^\times$. Then the elliptic curve $E^{(d)}$ given by

$$E^{(d)} : y^2 = x^3 + a_2dx^2 + a_4d^2x + a_6d^3$$

is called the *twist of E by d*. Note that $j(E^{(d)}) = j(E)$ and $\Delta(E^{(d)}) = d^6\Delta(E)$.

Elliptic curve with j-invariant j

Given $j \in K \setminus \{0, 1728\}$, we can always construct an elliptic curve with j-invariant j.
(1) If $\mathrm{char}(K) \notin \{2, 3\}$, then the elliptic curve

$$E_j : \ y^2 = x^3 - 3jkx - 2jk^2 \qquad \text{where } k = j - 1728$$

has j-invariant $j(E_j) = j$ and discriminant $\Delta(E_j) = 2^{12}3^6j^2k^3$.
(2) If $\mathrm{char}(K) = 3$, then the elliptic curve

$$y^2 = x^3 - jx^2 + j^3 \tag{2.5}$$

has j-invariant j and discriminant $\Delta = j^5$.
(3) If $\mathrm{char}(K) = 2$, then the elliptic curve

$$y^2 + xy = x^3 + \frac{1}{j} \tag{2.6}$$

has j-invariant j and discriminant $\Delta = \frac{1}{j}$.

In case (1), the curve E_j has bad reduction at 2 and 3. However, we can transform E_j as follows to obtain a curve with j-invariant j and whose discriminant is divisible only by j and k. First apply the transformation $(x, y) \mapsto (x - j, y)$ to E_j to obtain:

$$y^2 = x^3 - 3jx^2 + 2^6 3^4 jx + 2^6 3^3 j(j - 2^7 3^3).$$

Now twist by $\frac{1}{3}$ to obtain

$$E_{g3} : y^2 = x^3 - jx^2 + 2^6 3^2 jx + 2^6 j(j - 2^7 3^3) \tag{2.7}$$

with j-invariant j and discriminant $\Delta = 2^{12}j^2(j - 1728)^3$. Note that E_{g3} has good reduction at 3, and reducing E_{g3} modulo 3 yields the curve (2.5).

Now we twist E_{g3} by $-j$ to obtain:

$$y^2 = x^3 + j^2x^2 + 2^6 3^2 j^3 x - 2^6 j^4(j - 2^7 3^3).$$

Then apply $(x, y) \mapsto (x, y + jx)$ to obtain:

$$y^2 + 2jxy = x^3 + 2^6 3^2 j^3 x - 2^6 j^4 (j - 2^7 3^3).$$

Finally, applying $(x, y) \mapsto ((2j)^2 x, (2j)^3 y)$ yields:

$$E_{g2} = y^2 + xy = x^3 + \frac{2^2 3^2}{j} x - \frac{j - 2^7 3^3}{j^2} \tag{2.8}$$

with j-invariant j and discriminant $\Delta = \frac{(j-1728)^3}{j^4}$. Note that E_{g2} has good reduction at 2 and reducing E_{g2} modulo 2 yields the curve (2.6).

Addition law

Let E be an elliptic curve over K. Let $L \supseteq K$ be a field. We define the set

$$E(L) := \{(x, y) \in L^2 : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6\} \cup \{\mathcal{O}\}.$$

For any two points on $E(L)$, one can define an addition operation $+$, which makes $E(L)$ into an abelian group with identity element $\mathcal{O}$. The addition law can be expressed by rational functions in x and y (see [17, §III.2]).

For a positive integer n and a point $P \in E(\overline{K})$, denote $nP = P + ... + P$ (adding n times). The set

$$E[n] = \{P \in E(\overline{K}) \mid nP = \mathcal{O}\}$$

is a subgroup of $E(\overline{K})$ and is called the *n-torsion* subgroup of E. We have the following theorem.

Theorem 2.1.1. *Let E be an elliptic curve over K and let n be a positive integer.*

(a) If $\mathrm{char}(K) = 0$ *or if* $\mathrm{char}(K)$ *is coprime to n, then*

$$E[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

(b) If $\mathrm{char}(K) = p$*, then*

$$\begin{aligned} \textit{either} \quad & E[p^e] = \{\mathcal{O}\} \qquad \textit{for all } e \in \mathbb{N} \\ \textit{or} \quad & E[p^e] \cong \mathbb{Z}/p^e\mathbb{Z} \qquad \textit{for all } e \in \mathbb{N}. \end{aligned}$$

Proof. See [17, Corollary III.6.4]. □

If $\mathrm{char}(K) = p$, then by the above theorem $E[p] \cong \mathbb{Z}/p\mathbb{Z}$ or $\{\mathcal{O}\}$. E is called *ordinary* if $E[p] \cong \mathbb{Z}/p\mathbb{Z}$, and E is called *supersingular* if $E[p] \cong \{\mathcal{O}\}$.

There is a natural action of the Galois group $\mathrm{Gal}(\overline{K}/K)$ on $E(\overline{K})$. Let $\sigma \in \mathrm{Gal}(\overline{K}/K)$. The action of σ on $P = (x, y) \in E(\overline{K})$ is given by:

$$P^\sigma = (\sigma(x), \sigma(y)) \qquad \text{and} \qquad \mathcal{O}^\sigma = \mathcal{O}.$$

Since the addition on E can be defined by rational functions defined over K, the above Galois action commutes with the addition on E, i.e., $(P + Q)^\sigma = P^\sigma + Q^\sigma$. It follows that $\mathrm{Gal}(\overline{K}/K)$ acts on $E[n]$ for any positive integer n, since if $P \in E[n]$ then $P^\sigma \in E[n]$.

2.2 Isogenies

2.2.1 An overview of isogenies

Let E and E' be elliptic curves defined over a field K. An *isogeny defined over* K or *K-rational isogeny* is a morphism $\phi : E \to E'$ that is defined over K such that $\phi(\mathcal{O}_E) = \mathcal{O}_{E'}$. The *zero isogeny* is the constant morphism $\phi : E \to E'$ such that $\phi(P) = \mathcal{O}_{E'}$ for all $P \in E(\overline{K})$. The *kernel* of an isogeny $\phi : E \to E'$ is

$$\ker(\phi) = \{P \in E(\overline{K}) \mid \phi(P) = \mathcal{O}_{E'}\}.$$

If $\ker(\phi)$ is a cyclic group, then we call ϕ a *cyclic isogeny*. We say that the isogenies $\phi_1, \phi_2 : E \to E'$ are *equivalent* if $\ker(\phi_1) = \ker(\phi_2)$. Otherwise we say that ϕ_1 and ϕ_2 are *inequivalent*. A non-zero isogeny $\phi : E \to E'$ induces an injection of function fields (see [17, §III.4])

$$\phi^* : K(E') \to K(E).$$

The *degree* of an isogeny $\phi : E \to E'$ is

$$\deg(\phi) = [K(E) : \phi^* K(E')],$$

the degree of the field extension $K(E)/\phi^* K(E')$, and the degree of the zero isogeny is 0. We call an isogeny of degree N an *N-isogeny*. An isogeny $\phi : E \to E'$ is called *separable* if the extension $K(E)/\phi^* K(E')$ is separable. If ϕ is separable, then $\#\ker(\phi) = \deg(\phi)$.

It turns out that an isogeny $\phi : E \to E'$ is a homomorphism from E to E', i.e.,

$$\phi(P + Q) = \phi(P) + \phi(Q) \qquad \text{for all } P, Q \in E(\overline{K})$$

(see [17, Theorem III.4.8]). We denote

$$\mathrm{Hom}(E, E') = \{\overline{K}\text{-rational isogenies } \phi : E \to E'\},$$

which is a group under the addition law

$$(\phi_1 + \phi_2)(P) = \phi_1(P) + \phi_2(P)$$

for all $\phi_1, \phi_2 \in \mathrm{Hom}(E, E')$ and $P \in E(\overline{K})$.

Suppose E and E' are given by projective equation as in (2.1). Then a K-rational isogeny $\phi : E \to E'$ is given by the map

$$\phi([X : Y : Z]) = [\phi_0([X : Y : Z]) : \phi_1([X : Y : Z]) : \phi_2([X : Y : Z])]$$

where ϕ_0, ϕ_1, ϕ_2 are homogeneous polynomials of equal degree defined over K (see [14, §III.5]) satisfying the projective equation of E'. If ϕ is an non-zero isogeny, then using the affine coordinates $x = X/Z$ and $y = Y/Z$, ϕ can be expressed in the rational function form:

$$\phi(x, y) = (R_1(x, y), R_2(x, y)), \tag{2.9}$$

where $R_1(x, y) = \frac{\phi_0(x,y,1)}{\phi_2(x,y,1)}$ and $R_2(x, y) = \frac{\phi_1(x,y,1)}{\phi_2(x,y,1)}$, which are rational functions defined over K. In fact, we have the following theorem.

Theorem 2.2.1. *Let* $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ *and* E' :

$y^2 + a'_1xy + a'_3y = x^3 + a'_2x^2 + a'_4x + a'_6$ *be elliptic curves defined over* K*. Let* $\phi : E \to E'$ *be a separable isogeny defined over* K*. Then* ϕ *can be expressed in the rational function form*

$$\phi(x, y) = (r_1(x), cyr'_1(x) + r_2(x)), \tag{2.10}$$

where $r'_1(x) = \frac{dr_1(x)}{dx}$ *is the derivative of the rational function* $r_1(x)$*,* $c \in K^\times$ *is a constant, and* $2r_2(x) = -a'_1r_1(x) - a'_3 + c(a_1x + a_3)r'_1(x)$*.*

Proof. See [8, Theorem 9.7.5]. □

Suppose an isogeny $\phi : E \to E'$ is defined over K and let $H = \ker(\phi)$. Then since ϕ can be expressed by rational functions defined over K, H is *defined over* K, i.e., $P \in H$ implies $P^\sigma \in H$ for all $\sigma \in \mathrm{Gal}(\overline{K}/K)$. Conversely, given a finite subgroup $H \subseteq E(\overline{K})$ that is defined over K one can construct a K-rational isogeny ϕ of E with $\ker(\phi) = H$ as in the following theorem.

Theorem 2.2.2. *Let* E *be an elliptic curve over* K *and let* $H \subseteq E(\overline{K})$ *be a finite subgroup defined over* K*. Then there is a unique elliptic curve* E' *over* K *up to isomorphism over* $\overline{K}$ *and a* K*-rational separable isogeny* $\phi : E \to E'$ *such that* $\ker(\phi) = H$*.*

Proof. See [17, Proposition III.4.12] or [8, Theorem 9.6.19]. □

Hence the existence of a separable K-rational N-isogeny of E is equivalent to the existence of a finite subgroup of $E(\overline{K})$ of order N that is defined over K.

Let $m \in \mathbb{Z}$. The *multiplication by* m map $[m] : E \to E$ is the map defined by

$$[m](P) = \begin{cases} mP & \text{if } m > 0 \\ [-m](-P) & \text{if } m < 0 \\ \mathcal{O} & \text{if } m = 0 \end{cases}$$

for $P \in E(\overline{K})$. Note that $E[m] = \ker([m])$.

Theorem 2.2.3. *Let* $\phi : E \to E'$ *be a non-zero isogeny of degree* m*. Then there is a unique isogeny*

$$\hat{\phi} : E' \to E$$

of degree m such that $\hat{\phi} \circ \phi = [m]$ on E.

Proof. See [17, Theorem III.6.1]. □

The isogeny $\hat{\phi}$ in the above theorem is called the *dual* isogeny of ϕ.

Theorem 2.2.4. *Let*

$$\phi : E_1 \to E_2 \qquad \text{and} \qquad \psi : E_1 \to E_3$$

be non-zero isogenies. Assume that ϕ is separable and $ker(\phi) \subseteq ker(\psi)$. Then there is a unique isogeny

$$\lambda : E_2 \to E_3$$

such that $\psi = \lambda \circ \phi$.

Proof. See [17, Corollary III.4.11]. □

Theorem 2.2.5. *Let E and E' be elliptic curves over K and let $\phi : E \to E'$ be a separable K-rational isogeny. Then*

$$\phi = \phi_1 \circ ... \circ \phi_k \circ [m],$$

where $\phi_1, ..., \phi_k$ are K-rational isogenies of prime degree and m is some integer.

Proof. See [8, Theorem 25.1.2]. □

By the above theorem, in order to construct an isogeny from E to E' it suffices to compute isogenies of prime degree and the multiplication by m map and then compose them. Note that the multiplication by m map can be computed from the division polynomials (see [20, Section 3.2]). Therefore in this thesis we focus on computing isogenies of prime degree.

Throughout the thesis ℓ denotes a prime unless otherwise stated. By Theorem 2.1.1, if $\mathrm{char}(K) \neq \ell$ then $E[\ell] \cong \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$, which has $\ell + 1$ distinct order ℓ subgroups. Let Ω_ℓ denote the collection of order ℓ subgroups of $E[\ell]$. We need the following well-known result.

Theorem 2.2.6. *For a field F consider the group action of $\mathrm{PGL}_2(F)$ on $\mathbb{P}^1(F)$ by linear fractional transformations. Given two sets $\{z_1, z_2, z_3\}$ and $\{z_1', z_2', z_3'\}$ each consisting of three distinct points in $\mathbb{P}^1(F)$, there is a unique $A \in \mathrm{PGL}_2(F)$ such that $Az_i = z_i'$ for $i = 1, 2, 3$.*

Lemma 2.2.7. *Let E be an elliptic curve over K. Then the number of pairwise inequivalent K-rational ℓ-isogenies of E is 0, 1, 2 or $\ell+1$.*

Proof. Let $E[\ell] = \langle P, Q\rangle$. Then $H \in \Omega_\ell$ can be expressed as $\langle aP + bQ\rangle$ for some $a, b \in \mathbb{F}_\ell$, and we can identify H and an element in $\mathbb{P}^1(\mathbb{F}_\ell)$ by the map $\langle aP + bQ\rangle \mapsto [a : b]$. Since $\sigma \in \mathrm{Gal}(\overline{K}/K)$ acts linearly on Ω_ℓ, the action of $\sigma \in \mathrm{Gal}(\overline{K}/K)$ is represented by a matrix in $\mathrm{PGL}_2(\mathbb{F}_\ell)$. Thus by Theorem 2.2.6, the number of points in Ω_ℓ fixed by $\sigma \in \mathrm{Gal}(\overline{K}/K)$ is 0, 1, 2 or $\ell+1$ and the lemma follows. □

2.2.2 Endomorphisms and automorphisms

Let E be an elliptic curve defined over K. We define

$$\mathrm{End}(E) = \mathrm{Hom}(E, E) = \{\overline{K}\text{-rational isogenies } \phi : E \to E\},$$

which is a ring with addition (that comes from addition in $\mathrm{Hom}(E, E)$) and multiplication defined by composition

$$\phi_1 \circ \phi_2(P) = \phi_1(\phi_2(P))$$

for all $\phi_1, \phi_2 \in \mathrm{End}(E)$ and $P \in E(\overline{K})$. $\mathrm{End}(E)$ is called the *endomorphism ring* of E, and an element of $\mathrm{End}(E)$ is called an *endomorphism* of E. For example, the multiplication by m map $[m]$ is an endomorphism of E. Furthermore, there is an induced injective ring homomorphism $[\ ] : \mathbb{Z} \to \mathrm{End}(E)$.

The following is the main theorem on the endomorphism rings.

Theorem 2.2.8. *Let E be an elliptic curve over K. Then there exists an isomorphism $[\ ] : R \xrightarrow{\sim} \mathrm{End}(E)$ where:*

(1) if $\mathrm{char}(K) = 0$, then $R = \mathbb{Z}$ or an order in an imaginary quadratic field.

(2) if $\mathrm{char}(K) \neq 0$:

- *(a) if E is ordinary, then R is an order in an imaginary quadratic field.*
- *(b) if E is supersingular, then R is an order in a quaternion algebra.*

Moreover, in case (1) *we have* $\deg[a] = a^2$ *for all* $a \in \mathbb{Z}$*, and in case* (2a) *we have* $\deg(a) = \mathrm{Norm}_{L/\mathbb{Q}}(a)$ *for all* $a \in R$ *where* $L = R \otimes \mathbb{Q}$*. In case* (2b)*, we have* $\deg(a)$ *is equal to the reduced norm of* a *for all* $a \in R$*.*

Proof. See [17, Theorem III.9.3] and [18, Corollary 1.5]. □

Remark 2.2.9. Suppose that either $\mathrm{char}(K) = 0$ or $\mathrm{char}(K) \neq 0$ and E is ordinary. In this case if $j(E) = 0$ then $\mathrm{End}(E) \cong \mathbb{Z}[\frac{-1+\sqrt{-3}}{2}]$, and if $j(E) = 1728$ then $\mathrm{End}(E) \cong \mathbb{Z}[i]$.

We define

$$\mathrm{Aut}(E) = \{\phi \in \mathrm{End}(E) : \exists\ \phi^{-1} \text{ such that } \phi^{-1} \circ \phi = \mathrm{id}\},$$

the group of units of $\mathrm{End}(E)$. $\mathrm{Aut}(E)$ is called the *automorphism group* of E, and an element of $\mathrm{Aut}(E)$ is called an *automorphism* of E.

Theorem 2.2.10. *Let* E *be an elliptic curve over* K*. Then* $\mathrm{Aut}(E)$ *is a finite group of order:*

$$\begin{array}{ll} 2 & \text{if } j(E) \neq 0, 1728 \\ 4 & \text{if } j(E) = 1728 \text{ and } \mathrm{char}(K) \neq 2, 3 \\ 6 & \text{if } j(E) = 0 \text{ and } \mathrm{char}(K) \neq 2, 3 \\ 12 & \text{if } j(E) = 0 = 1728 \text{ and } \mathrm{char}(K) = 3 \\ 24 & \text{if } j(E) = 0 = 1728 \text{ and } \mathrm{char}(K) = 2. \end{array}$$

Proof. See [17, Theorem III.10.1] □

Remark 2.2.11. Suppose $\mathrm{char}(K) \notin \{2, 3\}$. Then $\mathrm{Aut}(E) \cong \{\pm 1, \frac{\pm 1 \pm \sqrt{-3}}{2}\}$ (sixth roots of unity) if $j(E) = 0$, and $\mathrm{Aut}(E) \cong \{\pm 1, \pm i\}$ (fourth roots of unity) if $j(E) = 1728$.

Action of $\mathrm{Aut}(E)$ on Ω_ℓ

Although the results in this section are well-known, we include proofs since we do not have a suitable reference. Recall that Ω_ℓ denotes the collection of order ℓ subgroups of $E[\ell]$. Then since $\mathrm{Aut}(E)$ acts on the points in $E[n]$, it induces an action on Ω_ℓ. Clearly if $j(E) \notin \{0, 1728\}$ then $\mathrm{Aut}(E) = \{\pm 1\}$ so this action is trivial. However, if $j(E) \in \{0, 1728\}$ then we have the following.

Proposition 2.2.12. *Let K be a field of characteristic not 2, 3 or ℓ. Let E be an elliptic curve over K such that $j(E) \in \{0, 1728\}$. Let $\Omega_\ell^{\mathrm{Aut}(E)}$ denote the set of fixed elements of Ω_ℓ by the action of $\mathrm{Aut}(E)$. Then the following hold.*

(1) (a) If $j(E) = 0$, then

$$|\Omega_\ell^{\mathrm{Aut}(E)}| = \begin{cases} 1 & \text{if } \ell = 3 \\ 2 & \text{if } \ell \equiv 1 \pmod 3 \\ 0 & \text{if } \ell \equiv 2 \pmod 3. \end{cases}$$

(b) If $j(E) = 1728$, then

$$|\Omega_\ell^{\mathrm{Aut}(E)}| = \begin{cases} 1 & \text{if } \ell = 2 \\ 2 & \text{if } \ell \equiv 1 \pmod 4 \\ 0 & \text{if } \ell \equiv 3 \pmod 4. \end{cases}$$

(2) If $H \in \Omega_\ell^{\mathrm{Aut}(E)}$, then $H = \ker(\phi)$ for some $\phi \in \mathrm{End}(E)$. Furthermore, the converse also holds if $\mathrm{End}(E)$ is commutative.

To prove the proposition, we need the following lemmas.

Lemma 2.2.13. *Let E be an elliptic curve over K. If $\mathrm{End}(E)$ is commutative, then for all $\phi \in \mathrm{End}(E)$ and $\alpha \in \mathrm{Aut}(E)$ we have*

$$\alpha(\ker(\phi)) = \ker(\phi).$$

Proof. Since $\mathrm{End}(E)$ is commutative, we have the following:

$$\alpha^{-1}(\ker(\phi)) = \ker(\phi \circ \alpha) = \ker(\alpha \circ \phi) = \ker(\phi).$$

□

Lemma 2.2.14. *Let K be a field of characteristic not 2, 3 or ℓ. Let E be an elliptic curve over K with $j(E) \in \{0, 1728\}$. Then for all $\alpha \in \mathrm{Aut}(E) \setminus \{[\pm 1]\}$, there exists $H \in \Omega_\ell$ such that $\alpha(H) \neq H$.*

Proof. The proof is by contradiction. Suppose that $\alpha(H) = H$ for all $H \in \Omega_\ell$. Then by Theorem 2.2.6 it follows that $\alpha(P) = cP$ for all $P \in E[\ell]$ and some $c \in (\mathbb{Z}/\ell\mathbb{Z})^\times$. Hence $\ker([\ell]) \subseteq \ker(\alpha - c)$, and by Theorem 2.2.4 $\deg[\ell] \mid \deg(\alpha - c)$. By Theorem 2.2.8, ℓ^2 divides $\mathrm{Norm}(\alpha - c) = \alpha\overline{\alpha} - (\alpha + \overline{\alpha})c + c^2$.

If $j(E) = 0$ then $\mathrm{Aut}(E) \cong \{\pm 1, \frac{\pm 1 \pm \sqrt{-3}}{2}\}$ since $\mathrm{char}(K) \notin \{2, 3\}$. Thus ℓ^2 divides $\mathrm{Norm}(\alpha - c) = 1 \pm c + c^2$. We claim that ℓ^2 cannot divide $1 \pm c + c^2$. We may assume that $0 < c < \ell$ since $c \in (\mathbb{Z}/\ell\mathbb{Z})^\times$. Thus it suffices to prove that $\ell^2 \neq 1 \pm c + c^2$ since $1 \pm c + c^2 < 2\ell^2$. Suppose $\ell^2 = 1 \pm c + c^2$ for some $c \in \mathbb{Z}$, then $\sqrt{4\ell^2 - 3} \in \mathbb{Z}$. However, such c does not exist since the equation $x^2 - y^2 = 3$ does not have an integer solution with $x \geq 4$.

If $j(E) = 1728$ then we have $\mathrm{Norm}(\alpha - c) = 1 + c^2$ since $\mathrm{Aut}(E) \cong \{\pm 1, \pm i\}$. Since $c \in (\mathbb{Z}/\ell\mathbb{Z})^\times$, we may assume that $0 < c < \ell$. Then it is clear that ℓ^2 cannot divide $1 + c^2$ for any $0 < c < \ell$. □

Now we prove Proposition 2.2.12.

Proof of Proposition 2.2.12. (1a) Suppose $j(E) = 0$. If $\mathrm{char}(K) = 0$, then $\mathrm{End}(E) \cong \mathbb{Z}[\frac{-1+\sqrt{-3}}{2}]$. By Theorem 2.2.8 the number of inequivalent degree ℓ endomorphisms of E is equal to n, where n is the number of elements in $\mathbb{Z}[\frac{-1+\sqrt{-3}}{2}]$ of norm ℓ, up to multiplication by a unit. Now quadratic reciprocity and the fact that $\mathbb{Q}(\sqrt{-3})$ has class number 1 imply that $n = 1$ if $\ell = 3$, $n = 2$ if $\ell \equiv 1 \pmod 3$ and $n = 0$ if $\ell \equiv 2 \pmod 3$. By Lemma 2.2.13, it follows that

$$|\Omega_\ell^{\mathrm{Aut}(E)}| \geq \begin{cases} 1 & \text{if } \ell = 3, \\ 2 & \text{if } \ell \equiv 1 \pmod 3, \\ 0 & \text{if } \ell \equiv 2 \pmod 3. \end{cases}$$

We can show that this inequality holds even when $\mathrm{char}(K) = p \notin \{2, 3, \ell\}$. Note that in this case we have $\mathrm{End}(E) \supseteq \mathbb{Z}[\frac{-1+\sqrt{-3}}{2}]$, since reducing a degree ℓ endomorphism in characteristic 0 modulo p gives a degree ℓ endomorphism in characteristic p. Moreover, by looking at the kernel polynomial (see section 2.2.3) we can show that the kernel of an endomorphism that corresponds to an element in $\mathbb{Z}[\frac{-1+\sqrt{-3}}{2}]$ is fixed by $\mathrm{Aut}(E)$, thus the above inequality still holds if $\mathrm{char}(K) = p \notin \{2, 3, \ell\}$.

Now we show that the above inequality is in fact equality. Note that Theorem 2.2.6 implies that $|\Omega_\ell^{\mathrm{Aut}(E)}| = 0$, 1, 2 or $\ell + 1$. Let $\Omega_\ell / \mathrm{Aut}(E)$ denote

the set of $\mathrm{Aut}(E)$-orbits of Ω_ℓ. If $\ell = 3$ then $|\Omega_\ell^{\mathrm{Aut}(E)}| = 1$ or 4, since an element of $\Omega_\ell/\mathrm{Aut}(E)$ has size 1 or 3. But $|\Omega_\ell^{\mathrm{Aut}(E)}| \neq 4$ by Lemma 2.2.14, so the result follows. If $\ell \equiv 1 \pmod 3$ then it suffices to prove that $|\Omega_\ell^{\mathrm{Aut}(E)}| \neq \ell+1$, which follows by Lemma 2.2.14. If $\ell \equiv 2 \pmod 3$ then $\ell + 1 = |\Omega_\ell^{\mathrm{Aut}(E)}| + 3 \cdot \#\{\text{orbits of size 3}\}$. Since 3 divides $\ell+1$, it follows that $|\Omega_\ell^{\mathrm{Aut}(E)}| = 0$ or $\ell+1$. But the latter is not possible by Lemma 2.2.14, and hence the result follows. This proves (1a).

(1b) Suppose $j(E) = 1728$. The similar argument as in (1a) shows that

$$|\Omega_\ell^{\mathrm{Aut}(E)}| \geq \begin{cases} 1 & \text{if } \ell = 2, \\ 2 & \text{if } \ell \equiv 1 \pmod 4, \\ 0 & \text{if } \ell \equiv 3 \pmod 4. \end{cases}$$

If $\ell = 2$ then $|\Omega_\ell^{\mathrm{Aut}(E)}|$ is either 1 or 3 since $|\Omega_\ell^{\mathrm{Aut}(E)}| \geq 1$. But the latter is not possible by Lemma 2.2.14. Thus the result follows. If $\ell \equiv 1 \pmod 4$ then it suffices to prove that $|\Omega_\ell^{\mathrm{Aut}(E)}| \neq \ell+1$, which is true by Lemma 2.2.14. If $\ell \equiv 3 \pmod 4$ then since $\mathrm{Aut}(E) \cong \{\pm 1, \pm i\}$, we will show that $[i](H) \neq H$ for all $H \in \Omega_\ell$. Suppose that $[i](H) = H$ for some $H \in \Omega_\ell$. Since $[i] \circ [i] = [-1]$, we have $[i](h) = \lambda h$ for all $h \in H$ where $\lambda \in (\mathbb{Z}/\ell\mathbb{Z})^\times$ such that $\lambda^2 \equiv -1 \pmod \ell$. However, such element does not exist since $\ell \equiv 3 \pmod 4$. Hence the result follows, and this proves (1b).

(2) It follows from the proof of (1). □

Remark 2.2.15. Note that in Proposition 2.2.12, we do need the condition that $\mathrm{End}(E)$ is commutative for the converse to hold. For example, consider the elliptic curve $E : y^2 = x^3 + 1$ over $\overline{\mathbb{F}}_5$ and $\ell = 7$. Since $j(E) = 0$ and $\mathrm{char}(\overline{\mathbb{F}}_5) = 5$, it follows that E is supersingular and hence $\mathrm{End}(E)$ is not commutative. Here although E has eight inequivalent degree 7 endomorphisms, only two of the kernels are fixed by $\mathrm{Aut}(E)$.

2.2.3 Kernel polynomials and division polynomials

Kernel polynomials

In [10] Kohel gives the formula for computing an isogeny from the *kernel polynomial*, the unique monic polynomial of minimal degree such that the

roots are precisely the distinct x-coordinates of the points in the kernel. In contrast to Vélu's formula [19] for computing an isogeny from the coordinates of the points in the kernel, Kohel's formula is more convenient in practice since we only need to work over a field where the kernel polynomial is defined, whereas the coordinates of the points in the kernel may be defined over a higher degree extension. The computation of an isogeny from the kernel polynomial is straight-forward. We illustrate Kohel's formula [10, Section 2.4] for the case where the order of the kernel is odd, 2 or 4. In general, an isogeny of arbitrary degree can be computed by composing isogenies of degree odd, 2 or 4.

Let E be an elliptic curve over K given by $y^2+a_1xy+a_3y = x^3+a_2x^2+a_4x+a_6$. Let $H \subseteq E(\overline{K})$ be a finite subgroup defined over K and assume that the order of H is n, where n is odd, 2 or 4. We define the *kernel polynomial* of H to be

$$\psi_H(x) = \prod_{\pm P=(x_P,y_P)\in H\setminus\{\mathcal{O}\}} (x - x_P),$$

where the product is over one of each pair $\pm P$, which is well-defined since P and $-P$ have the same x-coordinate. If n is odd then the degree of the polynomial $\psi_H(x)$ is $\frac{n-1}{2}$. Otherwise the degree of $\psi_H(x)$ is 1 or 3 if $n = 2$ or 4 respectively. Note that it follows from the definition that $\psi_H(x) \in K[x]$ if and only if H is defined over K. Kohel gives the following formula for a separable isogeny of E with kernel H and the equation for the isogenous curve. The isogeny is given by the rational functions

$$\left(\frac{\phi(x)}{\psi_H(x)^2}, \frac{\omega(x,y)}{\psi_H(x)^3}\right),$$

and as in Vélu's formula [19] the isogenous curve is given by

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + (a_4 - 5t)x + (a_6 - b_2t - 7w),$$

where $\phi(x)$, $\omega(x,y)$, t and w are given according to the following three cases; n is odd, 2 or 4.

Case 1: n odd. In this case, the kernel polynomial ψ_H can be written as

$$\psi(x) = x^d + \sum_{i=1}^{d} (-1)^i s_i x^{d-i},$$

where $d = \frac{n-1}{2}$. $\phi(x)$ is given by

$$\begin{aligned}\phi(x) = (4x^3 + b_2 + 2b_4x + b_6)(\psi'(x)^2 - \psi''(x)\psi(x)) \\ - (6x^2 + b_2x + b_4)\phi'(x)\psi(x) + (nx - 2s_1)\psi(x)^2,\end{aligned}$$

where b_2, b_4 and b_6 are the b-invariants of E. Furthermore, $\omega(x, y)$ is given by

$$\begin{aligned}\omega(x,y) &= \phi'(x)\psi(x)y - \phi(x)\psi'(x)(2y + a_1x + a_3) \\ &+ \Big((a_1x + a_3)(2y + a_1x + a_3)^2(\tilde{\psi}(x)\psi'(x) - \tilde{\tilde{\psi}}(x)\psi(x))) \\ &+ (a_1(2y + a_1x + a_3)^2 - 3(a_1x + a_3)(6x^2 + b_2x + b_6))\tilde{\psi}(x)\psi(x) \\ &+ ((a_1x^3 + 3a_3x^2 + (2a_2a_3 - a_1a_4)x + (a_3a_4 - 2a_1a_6))\psi'(x)^2 \\ &+ (-(3a_1x^2 + 6a_3x + 2a_2a_3 - a_1a_4) + (a_1x + a_3)(Nx - 2s_1))\psi'(x)\psi(x) \\ &+ (a_1s_1 + a_3n)\psi(x)^2\Big)\psi(x),\end{aligned}$$

where

$$\tilde{\psi}(x) = \sum_{i=0}^{n-2} \binom{i+2}{2} s_{i+2}x^i, \qquad \tilde{\tilde{\psi}}(x) = \sum_{i=0}^{n-3} 3\binom{i+3}{2} s_{i+3}x^i.$$

In the equation for the isogenous curve, t and w are given by

$$\begin{aligned}t &= 6(s_1^2 - 2s_2) + b_2s_1 + nb_4, \\ w &= 10(s_1^3 - 3s_1s_2 + 3s_3) + 2b_2(s_1 - 2s_2) + 3b_4s_1 + nb_6.\end{aligned}$$

Case 2: $n = 2$. In this case $\psi_H(x) = x - x_0$, where x_0 is the x-coordinate of the unique non-zero point in H. We define

$$y_0 = \begin{cases} \sqrt{x_0^3 + a_2x_0^2 + a_4x_0 + a_6} & \text{if } \mathrm{char}(K) = 2, \\ -\dfrac{a_1x_0 + a_3}{2} & \text{otherwise.} \end{cases}$$

Note that if $\mathrm{char}(K) = 2$ and assuming that K is perfect, then the square root is unique and defined over K. In the equation for the isogenous curve, t and

w are given by

$$\begin{aligned} t &= 3x_0^2 + 2a_2x_0 + a_4 - a_1y_0, \\ w &= x_0t. \end{aligned}$$

For the isogeny, $\phi(x)$ and $\omega(x, y)$ are given by

$$\begin{aligned} \phi(x) &= (x\psi_H(x) + v)\psi_H(x), \\ \omega(x, y) &= (y\psi_H^2(x) - va_1\psi_H(x) + (y - y_0))\psi_H(x). \end{aligned}$$

Case 3: $n = 4$. In this case $H = E[2]$ and $\psi_H(x) = x^3 + \frac{b_2}{4}x^2 + \frac{b_4}{2}x + \frac{b_6}{4}$. Note that the $\mathrm{char}(K)$ is necessarily not 2, since otherwise the multiplication by 2 map is not separable. For the isogeny, $\phi(x)$ and $\omega(x, y)$ are given by

$$\begin{aligned} \phi(x) &= \psi'^2(x) - 2\psi''(x)\psi(x) + (4x - s_1)\psi^2(x), \\ \omega(x, y) &= \frac{(2y + a_1x + a_3)(\phi'(x)\psi(x) - \phi(x)\psi'(x)) - (a_1\phi(x) + a_3\psi(x))\psi(x)}{2}. \end{aligned}$$

Finally in the equation for the isogenous curve, t and w are given by

$$\begin{aligned} t &= 3(s_1^2 - 2s_2) + \frac{b_2s_1 + 3b_4}{2}, \\ w &= 3(s_1^3 - 3s_1s_2 + 3s_3) + \frac{b_2(s_1^2 - 2s_2) + b_4s_1}{2}. \end{aligned}$$

Although we illustrated the case $n = 4$, in this thesis we will only work with the case where $n = \ell$ is a prime. We will call a polynomial f an *ℓ-kernel polynomial of E* if there exists a subgroup $H \subseteq E(\overline{K})$ of order ℓ such that $f = \psi_H$. Note that the degree of an ℓ-kernel polynomial is $\frac{\ell-1}{2}$ if ℓ is odd, and it is equal to 1 if $\ell = 2$. Since there are $\ell + 1$ distinct subgroups of order ℓ of $E(\overline{K})$, there are precisely $\ell + 1$ distinct ℓ-kernel polynomials of E.

Division polynomials

Let E be an elliptic curve given by $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ and let n be a positive integer. Let b_2, b_4, b_6, b_8 are the b-invariants of E. We define the *n-division polynomial* ψ_n of E by the following recursion:

$$\psi_0 = 0, \qquad \psi_1 = 1, \qquad \psi_2 = 2y + a_1x + a_3,$$
$$\psi_3 = 3x^4 + b_2x_3 + 3b_4x^2 + 3b_6x + b_8,$$
$$\psi_4 = \psi_2(2x^6 + b_2x^5 + 5b_4x^4 + 10b_6x^3 + 10b_8x^2 + (b_2b_8 - b_4b_6)x + b_4b_8 - b_6^2),$$
$$\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^2 \qquad \text{for } m \geq 2,$$
$$\psi_{2m} = \frac{\psi_m}{\psi_2}(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2) \qquad \text{for } m \geq 3.$$

If n is odd then $\psi_n \in \mathbb{Z}[x, a_1, a_2, a_3, a_4, a_6]$ and $\psi_n = \psi_{E[n]}$. If n is even then $\psi_n \in \mathbb{Z}[x, y, a_1, a_2, a_3, a_4, a_6]$. For a prime ℓ, recall that Ω_ℓ denotes the collection of order ℓ subgroups of $E[\ell]$. Since the non-zero points in $E[\ell]$ is the disjoint union of non-zero points in order ℓ subgroups in Ω_ℓ, we have

$$\psi_\ell(x) = \psi_{E[\ell]} = \prod_{H \in \Omega_\ell} \psi_H,$$

the product of all the ℓ-kernel polynomials of E.

2.3 Modular forms and modular curves

In this section we review the basic material on modular forms and modular curves. We refer to [5] for a standard reference.

2.3.1 Modular forms and modular functions

Let $\mathcal{H} = \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}$ be the complex upper half-plane and let $\mathcal{H}^* = \mathcal{H} \cup \mathbb{Q} \cup \{\infty\}$. The group $\mathrm{SL}_2(\mathbb{Z})$ acts on $\mathcal{H}^*$ by the linear fractional transformation:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} z = \frac{az + b}{cz + d} \quad \text{and} \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \infty = \frac{a}{c}$$

where $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ and $z \in \mathbb{C}$. Let N be a positive integer. We define

$$\begin{aligned}
\Gamma(N) &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : a, d \equiv 1 \pmod{N},\ b, c \equiv 0 \pmod{N} \right\}, \\
\Gamma_0(N) &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : c \equiv 0 \pmod{N} \right\}, \\
\Gamma_1(N) &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : a, d \equiv 1 \pmod{N},\ c \equiv 0 \pmod{N} \right\}.
\end{aligned}$$

Definition 2.3.1. A subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$ is a *congruence subgroup* if $\Gamma(N) \subset \Gamma$ for some positive integer N. In this case, Γ is called a *congruence subgroup of level* N.

The groups $\Gamma_0(N)$ and $\Gamma_1(N)$ are congruence subgroups since $\Gamma(N) \subset \Gamma_1(N) \subset \Gamma_0(N) \subset \mathrm{SL}_2(\mathbb{Z})$. We define the *cusps* of a congruence subgroup Γ to be the equivalence classes of $\mathbb{Q} \cup \{\infty\}$ under the above action of Γ on $\mathcal{H}^*$.

Definition 2.3.2. A *modular function for* Γ is a meromorphic function $f : \mathcal{H} \to \mathbb{C}$ such that

(1) $f(Az) = f(z)$ for all $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ and $z \in \mathcal{H}$,

(2) f is meromorphic at the cusps of Γ.

Definition 2.3.3. A *modular form of weight* k *for* Γ is a holomorphic function $f : \mathcal{H} \to \mathbb{C}$ such that

(1) $f(Az) = (cz + d)^k f(z)$ for all $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ and $z \in \mathcal{H}$,

(2) f is holomorphic at the cusps of Γ.

A modular form is called a *cusp form* if it vanishes at all the cusps of Γ. We denote by $M_k(\Gamma)$ and $S_k(\Gamma)$ respectively, the space of modular forms and the space of cusp forms of weight k for Γ.

Eisenstein series, j-function and Dedekind eta function

Let $k > 2$ be an even integer. The *Eisenstein series of weight* k is defined by

$$G_k(\tau) = \sum_{(c,d)\in\mathbb{Z}^2\setminus\{(0,0)\}} \frac{1}{(c\tau + d)^k} \qquad \text{for } \tau \in \mathcal{H}.$$

It turns out that $G_k \in M_k(\mathrm{SL}_2(\mathbb{Z}))$. We further define

$$g_2(\tau) = 60G_4(\tau) \qquad \text{and} \qquad g_3(\tau) = 140G_6(\tau)$$

and define the *modular discriminant* $\Delta : \mathcal{H} \to \mathbb{C}$ by

$$\Delta(\tau) = g_2^3(\tau) - 27g_3^2(\tau).$$

The *j-function* $j : \mathcal{H} \to \mathbb{C}$ is defined by

$$j(\tau) = 1728\frac{g_2^3(\tau)}{\Delta(\tau)},$$

which turns out to be a modular function for $\mathrm{SL}_2(\mathbb{Z})$. One can show that $j(\tau)$ induces an isomorphism $j : \mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}^* \to \mathbb{P}^1(\mathbb{C})$. Note that the function $j(\tau)$ has a simple pole at ∞ and has the Fourier expansion

$$j(q) = \frac{1}{q} + \sum_{n=0}^{\infty} a_n q^n \qquad \text{where } a_n \in \mathbb{Z} \text{ and } q = e^{2\pi i\tau}.$$

The *Dedekind eta function* is defined over the upper half-plane $\mathcal{H}$ by

$$\eta(\tau) = e^{\frac{\pi i\tau}{12}} \prod_{k=1}^{\infty}(1 - e^{2\pi ik\tau}).$$

Note that $\eta(\tau)$ is related to the modular discriminant Δ by

$$\Delta(\tau) = (2\pi)^{12}\eta^{12}(\tau).$$

2.3.2 Modular curves

Let Γ be a congruence subgroup. The *modular curves* $Y(\Gamma)$ and $X(\Gamma)$ are defined as the quotient space of $\mathcal{H}$ and $\mathcal{H}^*$ respectively under the action of Γ:

$$\begin{aligned} Y(\Gamma) &= \Gamma\backslash\mathcal{H} = \{\Gamma\tau \mid \tau \in \mathcal{H}\}, \\ X(\Gamma) &= \Gamma\backslash\mathcal{H}^* = \{\Gamma\tau \mid \tau \in \mathcal{H}^*\}. \end{aligned}$$

We denote the modular curves for $\Gamma_0(N)$ and $\Gamma_1(N)$ by

$$Y_0(N) = \Gamma_0(N)\backslash\mathcal{H}, \qquad X_0(N) = \Gamma_0(N)\backslash\mathcal{H}^*,$$

and

$$Y_1(N) = \Gamma_1(N)\backslash\mathcal{H}, \qquad X_1(N) = \Gamma_1(N)\backslash\mathcal{H}^*.$$

In this thesis we work mainly with $X_0(N)$. By the *cusps of* $X(\Gamma)$ we mean the cusps of Γ. Note that $X_0(\ell)$ has exactly two cusps for a prime ℓ, which we denote by 0 and ∞. One can show that $Y_0(N)$ is a non-compact Riemann surface, and $X_0(N)$ is the compactified Riemann surface of $Y_0(N)$. Since $X_0(N)$ is a compact Riemann surface, $X_0(N)$ is a smooth complex algebraic curve. Furthermore, one can show that $X_0(N)$ can be given the structure of a smooth algebraic curve over $\mathbb{Q}$, which we denote by $X_0(N)_{\mathbb{Q}}$.

The modular curve $X_0(N)$ can be viewed as the moduli space of elliptic curves with extra structure as follows. We define a *modular pair* (E, H) *over* K to be an elliptic curve E over K together with a cyclic subgroup $H \subseteq E(\overline{K})$ of order N defined over K. An isomorphism over K between two modular pairs (E, H) and (E', H') is an isomorphism $\phi : E \to E'$ defined over K such that $\phi(H) = H'$.

Let N be a positive integer. We define

$$\mathrm{Ell}_{0,N}(K) = \{\text{modular pairs } (E, H) \text{ over } K\}/\cong_K,$$

the set of isomorphism classes over K of modular pairs. We have the following theorem.

Theorem 2.3.4. *For any field $K \supseteq \mathbb{Q}$, there is a surjective map*

$$\mathrm{Ell}_{0,N}(K) \longrightarrow X_0(N)_{\mathbb{Q}}(K) \setminus \{\text{cusps}\}.$$

Moreover, this map is bijective if K is algebraically closed.

Proof. See [12, Chapter V. Theorem 2.7]. □

If $K \supseteq \mathbb{Q}$ is not algebraically closed, then we can obtain the following bijection:

$$\mathrm{Ell}'_{0,N}(K) \xrightarrow{\sim} X_0(N)_{\mathbb{Q}}(K) \setminus \{\text{cusps}\},$$

where $\mathrm{Ell}'_{0,N}(K)$ is given by

$$\mathrm{Ell}'_{0,N}(K) = \{\text{modular pairs } (E, H) \text{ over } K\}/\cong_{\overline{K}},$$

the set of isomorphism classes over $\overline{K}$ of modular pairs (see [4, Section 8.2]). Hence we can consider the set of K-rational points $X_0(N)_{\mathbb{Q}}(K)$ for all extensions K of $\mathbb{Q}$. Moreover if p is a prime not dividing N, then the curve $X_0(N)_{\mathbb{Q}}$ has a good reduction at p. Let the reduced curve modulo p be $X_0(N)_{\mathbb{F}_p}$. Thus for a field K of characteristic p, we may also consider the set of K-rational points on $X_0(N)_{\mathbb{F}_p}$ that correspond to modular pairs (E, H) over K up to isomorphism over $\overline{K}$.

Function fields of $X(\Gamma)$

Let Γ be a congruence subgroup. We denote the field of meromorphic functions on the modular curve $X(\Gamma)$ by $\mathbb{C}(X(\Gamma))$. For example, for $X_0(N)$ one can show that

$$\mathbb{C}(X_0(N)) = \mathbb{C}(j, j_N), \quad \text{where } j_N(\tau) = j(N\tau)$$

(see [5, Exercise 7.5.3] for details). Moreover, the curve $X_0(N)_{\mathbb{Q}}$ over $\mathbb{Q}$ can be defined so that the function field $\mathbb{Q}(X_0(N)_{\mathbb{Q}}) = \mathbb{Q}(j, j_N)$. In chapter 4 and 5 we will determine more convenient generators of $\mathbb{Q}(X_0(\ell)_{\mathbb{Q}})$ for several primes ℓ.

Atkin-Lehner involution

Let N be a positive integer. We define the *Atkin-Lehner involution* w_N : $X_0(N) \to X_0(N)$ by

$$w_N = \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}.$$

Note that w_N normalizes $\Gamma_0(N)$ and hence induces an automorphism of $X_0(N)$. Further w_N is an involution on $X_0(N)$ since $w_N^2 = \left(\begin{smallmatrix} N & 0 \\ 0 & N \end{smallmatrix}\right)$ acts trivially on $\mathcal{H}$. We define the quotient curve $X_0^+(N)$ by

$$X_0^+(N) = \langle w_N \rangle \setminus \ X_0(N).$$

For a prime ℓ, we have the following formula for the genus $g(X_0^+(\ell))$ of $X_0^+(\ell)$:

$$g(X_0^+(\ell)) = \frac{1}{2}\big(g(X_0(\ell)) + 1 - H(\ell)\big), \tag{2.11}$$

where $g(X_0(\ell))$ is the genus of $X_0(\ell)$ and

$$H(\ell) = \begin{cases} \frac{1}{2}h(-4\ell) & \text{if } \ell \equiv 1 \pmod 4, \\ \frac{1}{2}\big(h(-\ell) + h(-4\ell)\big) & \text{otherwise,} \end{cases}$$

with $h(D)$ the class number of an order of a quadratic field with discriminant D (see [2]).

By the *cusps of* $X_0^+(N)$ we mean the equivalence classes of the cusps of $X_0(N)$ under the action of $\langle w_N \rangle$. For example, $X_0^+(\ell)$ for a prime ℓ has only one cusp since w_ℓ interchanges the two cusps 0 and ∞ of $X_0(\ell)$.

Furthermore, the action of w_N on $X_0(N)$ induces the action of w_N on a function f on $X_0(N)$ by $w_N(f(\tau)) = f(w_N\tau)$, where w_N acts on τ by the linear fractional transformation. Hence w_N induces an involution on the function field $\mathbb{C}(X_0(N))$ and also on $\mathbb{Q}(X_0(N))$. Recall that $\mathbb{Q}(X_0(N)_{\mathbb{Q}}) = \mathbb{Q}(j, j_N)$. Note that w_N interchanges j and j_N.

The covering map $X_0(\ell) \to X(1)$

Consider the covering map $X_0(\ell) \to X(1)$ for a prime ℓ. One can show that this covering map ramifies only above i, ρ and ∞, where $\rho = \frac{-1+\sqrt{-3}}{2}$. Note

that the j-function $j : \mathcal{H} \to \mathbb{C}$ takes $i \mapsto 1728$ and $\rho \mapsto 0$. The following shows the ramification behavior above i and ρ. Let $e_1(z), ..., e_t(z)$ be the ramification indices above $z \in \{i, \rho\}$. Then it turns out that $\mu = e_1(z) + \cdots + e_t(z)$ where $\mu = [\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(\ell)] = \ell + 1$. If $z = \rho$ then $e_k(z) = 1$ or 3 for $k = 1, ..., t$. Similarly if $z = i$ then $e_k(z) = 1$ or 2 for $k = 1, ..., t$. Let ν_2 denote the number of k for which $e_k(i) = 1$, and ν_3 denote the number of k for which $e_k(\rho) = 1$. By the formulas for ν_2 and ν_3 in [16, Section 1.6] one can show that

$$\nu_2 = \begin{cases} 2 & \text{if } \ell \equiv 1 \pmod 4, \\ 0 & \text{if } \ell \equiv 3 \pmod 4, \\ 1 & \text{if } \ell = 2, \end{cases} \tag{2.12}$$

and

$$\nu_3 = \begin{cases} 2 & \text{if } \ell \equiv 1 \pmod 3, \\ 0 & \text{if } \ell \equiv 2 \pmod 3, \\ 1 & \text{if } \ell = 3. \end{cases} \tag{2.13}$$

Proposition 2.3.5. *The genus $g(X_0(\ell))$ of $X_0(\ell)$ is given by*

$$\begin{aligned} g(X_0(\ell)) &= \frac{1}{12}(\ell + 1 - 3\nu_2 - 4\nu_3) \\ &= \begin{cases} \lfloor \frac{\ell+1}{12} \rfloor - 1 & \textit{if } \ell \equiv 1 \pmod{12}, \\ \lfloor \frac{\ell+1}{12} \rfloor & \textit{otherwise.} \end{cases} \end{aligned}$$

Proof. It follows from [16, Proposition 1.4.0]. □

Chapter 3

Division polynomial factorization method

Let E be an elliptic curve over a field K and let ℓ be a prime. We assume that $\mathrm{char}(K) \neq \ell$ so that $E[\ell]$ is isomorphic to $\mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$. Recall that the ℓ-division polynomial ψ_ℓ of E is the product of all ℓ-kernel polynomials of E. The main aim of this chapter is to compute all K-rational ℓ-kernel polynomials of E by factorizing ψ_ℓ.

If $\ell = 2$ or 3 then an ℓ-kernel polynomial has degree 1, so any linear factor of ψ_ℓ is indeed an ℓ-kernel polynomial of E. For $\ell \geq 5$, the degree of an ℓ-kernel polynomial is $\frac{\ell-1}{2}$. However, it is important to note that a degree $\frac{\ell-1}{2}$ factor of ψ_ℓ is not necessarily an ℓ-kernel polynomial of E.

Thus in this chapter we will develop a method to determine whether a given degree $\frac{\ell-1}{2}$ factor of ψ_ℓ is an ℓ-kernel polynomial or not. Furthermore, given an irreducible factor f of ψ_ℓ such that $\deg(f) < \frac{\ell-1}{2}$, we will give a construction of an ℓ-kernel polynomial from f when it exists. Since it is straight-forward when $\ell = 2$ or 3, we will assume that $\ell \geq 5$ throughout this chapter unless stated otherwise.

3.1 Factorization of ψ_ℓ

We have seen in section 2.2.3 that the kernel polynomial of a K-rational ℓ-isogeny of E is a K-rational degree $\frac{\ell-1}{2}$ factor of ψ_ℓ. However, the converse is not necessarily true. In particular, even an irreducible degree $\frac{\ell-1}{2}$ factor

of ψ_ℓ is not necessarily an ℓ-kernel polynomial of E. The following example illustrates the case where some irreducible degree $\frac{\ell-1}{2}$ factors of ψ_ℓ are not ℓ-kernel polynomials of E.

Example 3.1.1. Let $K = \mathbb{F}_3$ and $\ell = 13$. Let E be the elliptic curve over $\mathbb{F}_3$ given by

$$E : y^2 = x^3 - x.$$

Note that a 13-kernel polynomial of E has degree $\frac{13-1}{2} = 6$. The 13-division polynomial ψ_{13} of E factorizes over $\mathbb{F}_3$ as:

$$\begin{gathered}\psi_{13} = (x^6 + x^4 + x^3 + x^2 - x - 1)(x^6 + x^4 - x^3 + x^2 + x - 1) \\ (x^6 + x^5 + x^3 - x^2 + x - 1)(x^6 + x^5 - x^3 - x^2 - 1) \\ (x^6 + x^5 + x^4 + x^2 - x - 1)(x^6 + x^5 + x^4 + x^3 + x^2 + x - 1) \\ (x^6 + x^5 - x^4 + x^3 + x - 1)(x^6 + x^5 - x^4 - x^3 - 1) \\ (x^6 - x^5 + x^3 - x^2 - 1)(x^6 - x^5 - x^3 - x^2 - x - 1) \\ (x^6 - x^5 + x^4 + x^2 + x - 1)(x^6 - x^5 + x^4 - x^3 + x^2 - x - 1) \\ (x^6 - x^5 - x^4 + x^3 - 1)(x^6 - x^5 - x^4 - x^3 - x - 1),\end{gathered}$$

a product of 14 irreducible polynomials of degree 6. However, only two among them, namely $x^6+x^4+x^3+x^2-x-1$ and $x^6+x^4-x^3+x^2+x-1$, are 13-kernel polynomials of E. In fact, all other 13-kernel polynomials of E are actually defined over $\mathbb{F}_9$. These can be checked by the methods described in section 3.3 and 3.4. Over $\mathbb{F}_9$, ψ_{13} factorizes into a product of 28 irreducible polynomials of degree 3, and all 13-kernel polynomials of E can be obtained by matching those irreducible factors correctly in pairs. We will visit this example again in detail at the end of this chapter.

3.2 Action of endomorphisms on kernel polynomials

Let E be an elliptic curve over K. In this section we develop a method to determine whether a degree $\frac{\ell-1}{2}$ factor of ψ_ℓ is an ℓ-kernel polynomial of E or not. Since $\mathrm{char}(K) \neq \ell$ by assumption, $E[\ell]$ is isomorphic to $\mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$, which contains $\ell + 1$ subgroups of order ℓ. Let $\Omega_\ell = \{H_1, ..., H_{\ell+1}\}$ be the collection of order ℓ subgroups of $E[\ell]$.

Let $\alpha \in \mathrm{End}(E)$ be such that $\deg(\alpha)$ is coprime to ℓ. Then α permutes the points in $E[\ell]$, and thus it induces the permutation $\alpha : \Omega_\ell \to \Omega_\ell$ given by

$$H \longmapsto \alpha(H) := \{\alpha(P) \mid P \in H\}.$$

Remark 3.2.1. Let $m \in \mathbb{Z}$ be coprime to ℓ. Then $[m](H) = H$ for all $H \in \Omega_\ell$. However, note that the permutation $\alpha : \Omega_\ell \to \Omega_\ell$ can be non-trivial if $\mathrm{End}(E)$ is larger than $\mathbb{Z}$ and α is not a multiplication by m map. For example, let E be the elliptic curve over $\mathbb{Q}$ given by $y^2 = x^3 - x$ and let $\alpha \in \mathrm{End}(E)$ be such that $\alpha^2 = [-1]$. Then α acts as an involution on Ω_ℓ if $\ell \equiv 1 \pmod 4$ as in Proposition 2.2.12.

Let Φ_ℓ be the set of all ℓ-kernel polynomials of E and let $\alpha \in \mathrm{End}(E)$ be such that $\deg(\alpha)$ is coprime to ℓ. Then the permutation $\alpha : \Omega_\ell \to \Omega_\ell$ induces the permutation $\alpha : \Phi_\ell \to \Phi_\ell$ given by

$$\psi_H \longmapsto \alpha(\psi_H) := \psi_{\alpha(H)},$$

where ψ_H is the kernel polynomial of H. Note that if $m \in \mathbb{Z}$ is coprime to ℓ, then $[m](\psi_H) = \psi_H$ for all $H \in \Omega_\ell$, since $[m](H) = H$ for all $H \in \Omega_\ell$.

Now we are ready to work with a factor of the ℓ-division polynomial ψ_ℓ. Let f be a factor of ψ_ℓ. We define the equivalence relation on $E[\ell]$ by $P \sim Q$ if and only if $P = \pm Q$, and we denote $E[\ell]/\{\pm 1\}$ to be the set of equivalence classes of $E[\ell]$ under the above equivalence relation. Then f can be written as:

$$f(x) = \prod_{i=1}^{d} (x - x_{P_i})$$

for some $1 \leq d \leq \frac{\ell^2-1}{2}$ and where $P_1, ..., P_d$ are distinct non-zero points in $E[\ell]/\{\pm 1\}$. Let $m \in \mathbb{Z}$ be coprime to ℓ. We define the action of $[m]$ on f by

$$[m](f) = \prod_{i=1}^{d} (x - x_{mP_i}).$$

Note that $[m](f)$ is also a factor of ψ_ℓ of degree d. The following lemma determines whether a degree $\frac{\ell-1}{2}$ factor of ψ_ℓ is an ℓ-kernel polynomial of E or not.

Proposition 3.2.2. *Let f be a degree $\frac{\ell-1}{2}$ factor of ψ_ℓ, and suppose that $a \in \mathbb{Z}$ generates the quotient group $(\mathbb{Z}/\ell\mathbb{Z})^\times/\{\pm 1\}$. Then f is an ℓ-kernel polynomial of E if and only if $[a](f) = f$.*

Proof. Suppose f is an ℓ-kernel polynomial of E. Then $f = \psi_H$ for some $H \in \Omega_\ell$. Clearly a is coprime to ℓ. Thus $[a](\psi_H) = \psi_H$.

Conversely, suppose $[a](f) = f$. We can write $f = \prod_{i=1}^{\frac{\ell-1}{2}}(x - x_{P_i})$ where $P_1, ..., P_{\frac{\ell-1}{2}}$ are distinct non-zero points in $E[\ell]/\{\pm 1\}$. Let $Q = P_1$ and let H be the cyclic group generated by Q. Since $f = [a](f) = \prod_{i=1}^{d}(x - x_{aP_i})$, we see that x_{aQ} is also a root of f. Moreover, x_{a^2Q} is also a root of f since $f = [a]^2(f)$. By continuing this process iteratively, we obtain that x_{a^kQ} is a root of f for all $k = 1, ..., \frac{\ell-1}{2}$. But since a generates $(\mathbb{Z}/\ell\mathbb{Z})^\times/\{\pm 1\}$, we have

$$\prod_{k=1}^{\frac{\ell-1}{2}}(x - x_{a^kQ}) = \prod_{\pm P=(x_P,y_P)\in H\setminus\{\mathcal{O}\}}(x - x_P),$$

which is an ℓ-kernel polynomial of E. □

We will call a generator of the quotient group $(\mathbb{Z}/\ell\mathbb{Z})^\times/\{\pm 1\}$ a *semi-primitive root modulo ℓ*. In the next section we will show that the polynomial $[a](f)$ can be expressed by a rational function in terms of f.

3.3 Kernel polynomial criterion

Let f be a factor of ψ_ℓ and let $m \in \mathbb{Z}$ be coprime to ℓ. Let $r_m = [m]^*x$, which is a rational function in x. Then $f(r_m(x))$ is a rational function in x and can be written as:

$$f(r_m(x)) = \frac{f_1(x)}{f_2(x)},$$

where f_1, f_2 are polynomials with $\gcd(f_1, f_2) = 1$. We define

$$\tau_m(f) = \frac{1}{c} \cdot \gcd(\psi_\ell, f_1),$$

where c is the leading coefficient of $\gcd(\psi_\ell, f_1)$. Hence $\tau_m f$ is a monic polynomial. Note that $\tau_m(f)$ is also a factor of ψ_ℓ.

Proposition 3.3.1. *Let f be a factor of ψ_ℓ and let $m \in \mathbb{Z}$ be coprime to ℓ. Suppose $mn \equiv 1 \pmod{\ell}$. Then $\tau_m(f) = [n](f)$.*

Proof. Write $f = \prod_{i=1}^{d}(x - x_{P_i})$, where d is the degree of f and $P_1, ..., P_d$ are distinct non-zero points in $E[\ell]/\{\pm 1\}$. Since $[n](f) = \prod_{i=1}^{d}(x - x_{nP_i}) = \prod_{i=1}^{d}[n](x - x_{P_i})$, it suffices to show that $\tau_m(x - x_P) = [n](x - x_P)$ for all $P \in E[\ell] \setminus \{\mathcal{O}\}$.

Write $r_m(x) = \frac{u_m(x)}{v_m(x)}$, where u_m, v_m are polynomials with $\gcd(u_m, v_m) = 1$. Then we have

$$r_m(x) - x_P = \frac{u_m(x) - x_P v_m(x)}{v_m(x)},$$

and $u_m(x) - x_P v_m(x) = 0$ if and only if $x = x_{mQ}$ for some point Q on E such that $mQ = \pm P$. Therefore

$$\tau_m(x - x_P) = \frac{1}{c} \cdot \gcd(\psi_\ell, u_m(x) - x_P v_m(x)) = x - x_Q,$$

where c is the leading coefficient of $\gcd(\psi_\ell, u_m(x) - x_P v_m(x))$ and Q is the unique point in $E[\ell]/\{\pm 1\}$ such that $mQ = \pm P$. Thus $x - x_Q = x - x_{nP} = [n](x - x_P)$ and hence the result follows. □

Corollary 3.3.2. *Let f be a degree $\frac{\ell-1}{2}$ factor of ψ_ℓ, and let a be a semi-primitive root modulo ℓ. Then f is an ℓ-kernel polynomial of E if and only if $\tau_a(f) = f$.*

Proof. Follows from Proposition 3.2.2 and 3.3.1. □

The above corollary determines whether a degree $\frac{\ell-1}{2}$ factor of ψ_ℓ is an ℓ-kernel polynomial of E or not. In the next section we will develop a method for construction of an ℓ-kernel polynomial of E from an irreducible factor of ψ_ℓ.

3.4 Computing an ℓ-kernel polynomial from an irreducible factor of ψ_ℓ

In this section, we will develop a method to construct an ℓ-kernel polynomial from an irreducible factor of ψ_ℓ. More precisely, given such a factor h, we give a

criterion for h to be a factor of an ℓ-kernel polynomial f of E and a construction of f from h when it exists. We start with the following proposition.

Proposition 3.4.1. *Let E be an elliptic curve over K and let f be an ℓ-kernel polynomial of E. Suppose f factorizes over a field $L \supseteq K$ as $f = \prod_{i=1}^{n} f_i$ where each f_i is irreducible over L. Then $deg(f_i) = \frac{\ell-1}{2n}$ for all i.*

Proof. Let x_1 be a root of f. Then for any root x_2 of f, there exists $m \in \mathbb{Z}$ with $1 \leq m < \ell$ such that $r_m(x_1) = x_2$. Since E is defined over K, r_m is a rational function in x with coefficients in $K \subseteq L$ and hence $x_2 \in L(x_1)$. By symmetry, the same argument shows that $x_1 \in L(x_2)$. Thus $L(x_1) = L(x_2)$, which implies that all the irreducible factors of f over L have the same degree, and the result follows. □

Since the multiplication by m map $[m]$ maps a factor of a kernel polynomial to another factor of the same kernel polynomial, the above proposition shows that $[m]$ takes an irreducible factor of a kernel polynomial to another irreducible factor of the same kernel polynomial. The following proposition shows how to construct a kernel polynomial f from an irreducible factor of f.

Proposition 3.4.2. *Let E be an elliptic curve over K and let f be an ℓ-kernel polynomial of E. Let h be an irreducible degree d factor of f over a field $L \supseteq K$. If a is a semi-primitive root modulo ℓ, then $f = \prod_{i=1}^{e} \tau_a^i(h)$ where $e = \frac{\ell-1}{2d}$.*

Proof. Let $b \in \mathbb{Z}$ be such that $ab \equiv 1 \pmod{\ell}$. Note that b is also a semi-primitive root modulo ℓ. By Proposition 3.3.1, we have $\prod_{i=1}^{e} \tau_a^i(h) = \prod_{i=1}^{e} [b]^i(h)$. Moreover by Proposition 3.4.1, f has e irreducible factors of degree d over L. Since $[b]$ takes an irreducible factor of f to another irreducible factor of f, it suffices to show that $[b]^i(h)$ are distinct for each $i = 1, ..., e$.

Suppose $[b]^i(h) = [b]^j(h)$ for some i, j with $1 \leq i < j \leq e$. Then there exists an irreducible factor h_0 of f such that $[b]^k(h_0) = h_0$ for some $k < e$. This implies that b does not generate $(\mathbb{Z}/\ell\mathbb{Z})^\times/\{\pm 1\}$, which is a contradiction. Therefore $[b]^i(h)$ are distinct for each $i = 1, ..., e$ and hence $f = \prod_{i=1}^{e} \tau_a^i(h)$ as required. □

By above proposition, one can construct a kernel polynomial from any one of its irreducible factors. Now suppose we are given an irreducible factor of

the ℓ-division polynomial ψ_ℓ. By Proposition 3.4.1, if the degree of h does not divide $\frac{\ell-1}{2}$, then h is not a factor of an ℓ-kernel polynomial of E. Otherwise, the proposition below gives a criterion for whether the given factor is a factor of an ℓ-kernel polynomial of E or not.

Proposition 3.4.3. *Let E be an elliptic curve over K. Let h be an irreducible degree d factor of ψ_ℓ over a field $L \supseteq K$ such that d divides $\frac{\ell-1}{2}$. Let a be a semi-primitive root modulo ℓ and let $e = \frac{\ell-1}{2d}$. Then $\tau_a^e(h) = h$ if and only if h is a factor of an ℓ-kernel polynomial of E.*

Proof. Suppose h is a factor of an ℓ-kernel polynomial f of E. By Proposition 3.4.1, we know that the number of irreducible factors of f over L is e. Since a is a semi-primitive root modulo ℓ, the polynomials $h, \tau_a(h), ..., \tau_a^{e-1}(h)$ are precisely all the distinct irreducible factors of f, as in the proof of proposition 3.4.2. Suppose $\tau_a^e(h) \neq h$. Then there exists an irreducible factor h_0 of f such that $[b]^k(h_0) = h_0$ for some $1 \leq k < e$ where $ab \equiv 1 \pmod{\ell}$. This is a contradiction as in the proof of proposition 3.4.2.

Conversely, suppose that $\tau_a^e(h) = h$. Since h is a factor of ψ_ℓ, we can write h as

$$h(x) = \prod_{i=1}^{d} (x - x_{P_i})$$

where $P_1, ..., P_d \in E[\ell]$. Since $\tau_a^e(h) = h$, we have for any $i = 1, ..., d$,

$$[b]^e(x - x_{P_i}) = (x - x_{P_j}),$$

where b is such that $ab \equiv 1 \pmod{\ell}$ and for some $j \in \{1, ..., d\}$. Next we claim that the set of points $\{[b]^{en}(P_1) \mid n = 1, ..., d\}$ is equal to the set of points $\{P_1, ..., P_d\}$ in $E[\ell]/\{\pm 1\}$. Suppose it is not true. Then there exists a point $P \in \{P_1, ..., P_d\}$ such that $[b]^{ek}(P) = P$ in $E[\ell]/\{\pm 1\}$ for some $1 \leq k < d$. Note that $ek < \frac{\ell-1}{2}$. Since b is a semi-primitive root modulo ℓ, $[b]^n(P) \neq P$ in $E[\ell]/\{\pm 1\}$ for all $1 \leq n < \frac{\ell-1}{2}$, which is a contradiction. Therefore $\{[b]^{en}(P_1) \mid n = 1, ..., d\} = \{P_1, ..., P_d\}$. It implies that $P_1, ..., P_d$ are in the same cyclic subgroup, say $\langle P_1 \rangle$. Hence h is a factor of an ℓ-kernel polynomial of E. □

We have seen that a semi-primitive root modulo ℓ plays an important

role in constructing kernel polynomials. Since the rational function $r_m = [m]^* x$ has degree m^2, for computation it is best to choose the smallest semi-primitive root modulo ℓ. The following lemma gives a criterion for an element of $(\mathbb{Z}/\ell\mathbb{Z})^\times$ to be a semi-primitive root modulo ℓ.

Lemma 3.4.4. *Let $a \in (\mathbb{Z}/\ell\mathbb{Z})^\times$. Denote the order of a by $|a|$.*

(1) *If $\ell \equiv 1 \pmod 4$, then a is a semi-primitive root modulo ℓ if and only if $|a| = \ell - 1$.*

(2) *If $\ell \equiv 3 \pmod 4$, then a is a semi-primitive root modulo ℓ if and only if $|a| \geq \frac{\ell-1}{2}$.*

Proof. First note that if a is a semi-primitive root modulo ℓ then clearly $|a| \geq \frac{\ell-1}{2}$ since the order of the group $(\mathbb{Z}/\ell\mathbb{Z})^\times/\{\pm 1\}$ is $\frac{\ell-1}{2}$. Therefore either $|a| = \ell - 1$ or $\frac{\ell-1}{2}$.

We first prove the statement (1). Suppose $|a| = \ell - 1$. Then since a generates $(\mathbb{Z}/\ell\mathbb{Z})^\times$, it also generates $(\mathbb{Z}/\ell\mathbb{Z})^\times/\{\pm 1\}$, i.e., a is a semi-primitive root modulo ℓ.

Conversely, suppose a is a semi-primitive root modulo ℓ. Then either $|a| = \ell - 1$ or $\frac{\ell-1}{2}$. If $|a| = \ell - 1$, then we are done. Suppose $|a| = \frac{\ell-1}{2}$. Then a is a square, so the group $H = \{a^i \mid i = 1, 2, ..., \frac{\ell-1}{2}\}$ consists of all squares in $(\mathbb{Z}/\ell\mathbb{Z})^\times$. Let $h \in (\mathbb{Z}/\ell\mathbb{Z})^\times \setminus H$. Then since $\ell \equiv 1 \pmod 4$, -1 is a square in $(\mathbb{Z}/\ell\mathbb{Z})^\times$ and hence $-h \notin H$. Thus a cannot generate $(\mathbb{Z}/\ell\mathbb{Z})^\times/\{\pm 1\}$, which contradicts the assumption that a is a semi-primitive root modulo ℓ. Therefore $|a| = \ell - 1$.

Next we prove the statement (2). Suppose a is a semi-primitive root modulo ℓ. Then either $|a| = \ell - 1$ or $\frac{\ell-1}{2}$, so $|a| \geq \frac{\ell-1}{2}$.

Conversely, suppose $|a| \geq \frac{\ell-1}{2}$. If $|a| = \ell - 1$, then we are done. Suppose $|a| = \frac{\ell-1}{2}$. Let $H = \{a^i \mid i = 1, 2, ..., \frac{\ell-1}{2}\}$. Since $\ell \equiv 3 \pmod 4$, -1 is not a square and so $-1 \notin H$. It implies that $H = (\mathbb{Z}/\ell\mathbb{Z})^\times/\{\pm 1\}$, i.e., a generates $(\mathbb{Z}/\ell\mathbb{Z})^\times/\{\pm 1\}$. Therefore a is a semi-primitive root modulo ℓ. □

For most $\ell < 200$, either 2 or 3 is a semi-primitive root modulo ℓ. In fact, 2 is semi-primitive modulo ℓ for

$$\begin{aligned} \ell \;=\; & 3, 5, 7, 11, 13, 19, 23, 29, 37, 47, 53, 59, 61, 67, 71, 79, 83, 101, \\ & 103, 107, 131, 139, 149, 163, 167, 173, 179, 181, 191, 197, 199, \end{aligned}$$

but not for

$$\ell = 17, 31, 41, 43, 73, 89, 97, 109, 113, 127, 137, 151, 157, 193.$$

It turns out that 2 or 3 is a semi-primitive root modulo ℓ for all $\ell < 200$ except for $\ell = 41$, 73, 97, 109, 151, 157, 193. However, for $\ell = 41$, 73, 97, 109, 151, 157, 193, the smallest semi-primitive root modulo ℓ is 6, 5, 5, 6, 5, 5, 5 respectively.

For $\ell < 1000$, the smallest semi-primitive root modulo ℓ is ≤ 6 for all except for 9 out of 167 primes, it is ≤ 13 for all but $\ell = 407$. For $\ell = 407$, the smallest semi-primitive root is 21. Hence the smallest semi-primitive root is not too big for most small primes.

3.5 Algorithm for computing ℓ-kernel polynomials

Let E be an elliptic curve over a field K and let ψ_ℓ be the ℓ-division polynomial of E. Here we summarize the method described in this chapter for constructing K-rational ℓ-kernel polynomials of E by factorizing ψ_ℓ.

Remark 3.5.1. For this algorithm, it is best to take the smallest semi-primitive root modulo ℓ to reduce the computation expense. As ℓ becomes large, computation becomes very expensive since we need to factorize ψ_ℓ which has degree $\frac{\ell^2-1}{2}$. In subsequent chapters, we will develop methods which only require factorization of polynomials of degree $\ell + 1$.

Algorithm 1 Computing K-rational ℓ-kernel polynomials by factoring the ℓ-division polynomial.

Input: E, K, ℓ, a (a semi-primitive root modulo ℓ)
Output: A set of K-rational ℓ-kernel polynomials of E

Compute ψ_ℓ
Factorize ψ_ℓ over K
if $\ell = 2$ or 3 **then**
  Set $\mathcal{K} = \{$linear factors of ψ_ℓ over $K\}$
else
  Set $\mathcal{F} = \{$irreducible factors of ψ_ℓ over K of degree dividing $\frac{\ell-1}{2}\}$
  Set $\mathcal{K} = \emptyset$
  for f in $\mathcal{F}$ **do**
    Let $d = \deg(f)$ and $e = \frac{\ell-1}{2d}$
    Compute $f, \tau_a(f), ..., \tau_a^e(f)$
    if $\tau_a^e(f) = f$ **then**
      Append $\prod_{i=0}^{e-1} \tau_a^i(f)$ to $\mathcal{K}$
    end if
    Delete $\tau_a^i(f)$ from $\mathcal{F}$ for $0 \leq i \leq e-1$
  end for
end if
return $\mathcal{K}$

We give the following two examples that use Algorithm 1.

Example 3.5.2. Let E be the elliptic curve over $\mathbb{Q}(\sqrt{5})$ given by

$$E: \ y^2 + y = x^3 - x^2 - 10x - 20.$$

We will compute all $\mathbb{Q}(\sqrt{5})$-rational 5-kernel polynomials of E. Note that a 5-kernel polynomial of E has degree $\frac{5-1}{2} = 2$. The 5-division polynomial ψ_5 of E factorizes as $\psi_5 = \prod_{i=1}^{8} f_i$ where:

$$\begin{aligned} f_1 &= x - 16, & f_2 &= x - 5, \\ f_3 &= x + \tfrac{1}{2} - \tfrac{11\sqrt{5}}{10}, & f_4 &= \overline{f_3}, \\ f_5 &= x^2 + \tfrac{15-5\sqrt{5}}{2}x + \tfrac{95-41\sqrt{5}}{2}, & f_8 &= \overline{f_5}, \\ f_6 &= x^2 + \tfrac{1-3\sqrt{5}}{2}x + 11 + 2\sqrt{5}, & f_7 &= \overline{f_6}, \end{aligned}$$

where $\overline{h_i}$ denotes the conjugate of h_i.

We can use τ_2 to construct kernel polynomials since 2 is a semi-primitive

root modulo 5. Since $\tau_2(f_1) = f_2$ and $\tau_2^2(f_1) = f_1$, we obtain that

$$f_1 \cdot f_2 = (x - 16)(x - 5) = x^2 - 21x + 80$$

is a 5-kernel polynomial of E. Moreover, since $\tau_2(f_3) = f_4$ and $\tau_2^2(f_3) = f_3$, the polynomial

$$f_3 \cdot f_4 = x^2 + x - \frac{29}{5}$$

is also a 5-kernel polynomial of E.

However, the polynomials f_5, f_6, f_7 and f_8 are not 5-kernel polynomials of E, since they do not satisfy $\tau_2(f_i) = f_i$ even though they are irreducible quadratic factors; τ_2 permutes f_5, f_6 and permutes f_7, f_8. Hence there are two $\mathbb{Q}(\sqrt{5})$-rational 5-kernel polynomials of E, namely $x^2-21x+80$ and $x^2+x-\frac{29}{5}$, which are in fact defined over $\mathbb{Q}$.

Example 3.5.3. This is a revisit of Example 3.1.1. Let E be the elliptic curve over $\mathbb{F}_3$ given by

$$E: \ y^2 = x^3 - x.$$

We will compute all $\mathbb{F}_3$-rational 13-kernel polynomials of E. Note that a 13-kernel polynomial of E has degree $\frac{13-1}{2} = 6$. The 13-division polynomial ψ_{13} of E factorizes as $\psi_{13} = \prod_{i=1}^{14} f_i$ where:

$$\begin{aligned}
&f_1 = x^6 + x^4 + x^3 + x^2 - x - 1, && f_2 = x^6 + x^4 - x^3 + x^2 + x - 1,\\
&f_3 = x^6 + x^5 + x^3 - x^2 + x - 1, && f_4 = x^6 + x^5 - x^3 - x^2 - 1,\\
&f_5 = x^6 + x^5 + x^4 + x^2 - x - 1, && f_6 = x^6 + x^5 + x^4 + x^3 + x^2 + x - 1,\\
&f_7 = x^6 + x^5 - x^4 + x^3 + x - 1, && f_8 = x^6 + x^5 - x^4 - x^3 - 1,\\
&f_9 = x^6 - x^5 + x^3 - x^2 - 1, && f_{10} = x^6 - x^5 - x^3 - x^2 - x - 1,\\
&f_{11} = x^6 - x^5 + x^4 + x^2 + x - 1, && f_{12} = x^6 - x^5 + x^4 - x^3 + x^2 - x - 1,\\
&f_{13} = x^6 - x^5 - x^4 + x^3 - 1, && f_{14} = x^6 - x^5 - x^4 - x^3 - x - 1.
\end{aligned}$$

Note that 2 is a semi-primitive root modulo 13. Since each f_i has degree 6, f_i is a 13-kernel polynomial if and only if $\tau_2(f_i) = f_i$ for each $i = 1, ..., 14$. One can check that

$$\tau_2(f_1) = f_1 \qquad \text{and} \qquad \tau_2(f_2) = f_2,$$

so f_1 and f_2 are 13-kernel polynomials of E. However, for other factors we have:

$$\tau_2(f_3) = f_{14}, \quad \tau_2(f_4) = f_9, \quad \tau_2(f_5) = f_{11},$$
$$\tau_2(f_6) = f_{13}, \quad \tau_2(f_7) = f_{10}, \quad \tau_2(f_8) = f_{12},$$

thus f_i are not 13-kernel polynomials E for $i = 3, ..., 14$. Hence E has two $\mathbb{F}_3$-rational 13-kernel polynomials, namely $f_1 = x^6 + x^4 + x^3 + x^2 - x - 1$ and $f_2 = x^6 + x^4 - x^3 + x^2 + x - 1$.

Now we see what happens over $\mathbb{F}_9$. Over $\mathbb{F}_9$, ψ_{13} factorizes as $\psi_{13} = \prod_{i=1}^{28} h_i$ where h_i are as follows and a denotes an element in $\mathbb{F}_9$ such that $a^2 = -1$:

$$\begin{aligned}
h_1 &= x^3 - x + a + 1, & h_3 &= \overline{h_1},\\
h_2 &= x^3 - x + a - 1, & h_4 &= \overline{h_2},\\
h_5 &= x^3 + (a+1)x^2 + a - 1, & h_{17} &= \overline{h_5},\\
h_6 &= x^3 + (a+1)x^2 + x + a - 1, & h_{18} &= \overline{h_6},\\
h_7 &= x^3 + (a+1)x^2 + (a+1)x - a - 1, & h_{21} &= \overline{h_7},\\
h_8 &= x^3 + (a+1)x^2 + (a-1)x - a + 1, & h_{22} &= \overline{h_8},\\
h_9 &= x^3 + (a+1)x^2 - ax - a - 1, & h_{19} &= \overline{h_9},\\
h_{10} &= x^3 + (a+1)x^2 + (-a-1)x - a + 1, & h_{20} &= \overline{h_{10}},\\
h_{11} &= x^3 + (a-1)x^2 + a + 1, & h_{23} &= \overline{h_{11}},\\
h_{12} &= x^3 + (a-1)x^2 + x + a + 1, & h_{24} &= \overline{h_{12}},\\
h_{13} &= x^3 + (a-1)x^2 + ax - a + 1, & h_{27} &= \overline{h_{13}},\\
h_{14} &= x^3 + (a-1)x^2 + (a-1)x - a - 1, & h_{28} &= \overline{h_{14}},\\
h_{15} &= x^3 + (a-1)x^2 + (-a+1)x - a + 1, & h_{25} &= \overline{h_{15}},\\
h_{16} &= x^3 + (a-1)x^2 + (-a-1)x - a - 1, & h_{26} &= \overline{h_{16}},
\end{aligned}$$

where $\overline{h_i}$ denotes the conjugate of h_i with respect to the conjugation $a \mapsto -a$. By using τ_2, we obtain the following 14 $\mathbb{F}_9$-rational 13-kernel polynomials of E:

$$\begin{aligned}
&h_1 \cdot \tau_2(h_1) = h_1 \cdot h_3 = x^6 + x^4 - x^3 + x^2 + x - 1,\\
&h_2 \cdot \tau_2(h_2) = h_2 \cdot h_4 = x^6 + x^4 + x^3 + x^2 - x - 1,\\
&h_5 \cdot \tau_2(h_5) = h_5 \cdot h_{25} = x^6 + (-a+1)x^4 + ax^3 + (-a-1)x^2 + x + 1,\\
&h_6 \cdot \tau_2(h_6) = h_6 \cdot h_{12} = x^6 - ax^5 + ax^3 + x^2 - ax + 1,\\
&h_7 \cdot \tau_2(h_7) = h_7 \cdot h_{23} = x^6 + (-a+1)x^4 - ax^3 + (-a-1)x^2 - x + 1,\\
&h_8 \cdot \tau_2(h_8) = h_8 \cdot h_{13} = x^6 - ax^5 - ax^4 + x^3 + (a+1)x^2 + x + a,
\end{aligned}$$

$$
\begin{aligned}
h_9 \cdot \tau_2(h_9) = h_9 \cdot h_{16} &= x^6 - ax^5 + ax^4 - x^3 + (-a+1)x^2 - x - a, \\
h_{10} \cdot \tau_2(h_{10}) = h_{10} \cdot h_{28} &= x^6 + (-a+1)x^4 + (-a-1)x^2 - a, \\
h_{11} \cdot \tau_2(h_{11}) = h_{11} \cdot h_{21} &= x^6 + (a+1)x^4 + ax^3 + (a-1)x^2 - x + 1, \\
h_{14} \cdot \tau_2(h_{20}) = h_{14} \cdot h_{20} &= x^6 + (a+1)x^4 + (a-1)x^2 + a, \\
h_{15} \cdot \tau_2(h_{15}) = h_{15} \cdot h_{17} &= x^6 + (a+1)x^4 - ax^3 + (a-1)x^2 + x + 1, \\
h_{18} \cdot \tau_2(h_{18}) = h_{18} \cdot h_{24} &= x^6 + ax^5 - ax^3 + x^2 + ax + 1, \\
h_{19} \cdot \tau_2(h_{19}) = h_{19} \cdot h_{26} &= x^6 + ax^5 - ax^4 - x^3 + (a+1)x^2 - x + a, \\
h_{22} \cdot \tau_2(h_{22}) = h_{22} \cdot h_{27} &= x^6 + ax^5 + ax^4 + x^3 + (-a+1)x^2 + x - a.
\end{aligned}
$$

Chapter 4

Modular Approach: cases where $X_0(\ell)$ has genus 0

Recall from section 2.3.2 that $\mathrm{Ell}'_{0,N}(K)$ denotes the set of pairs (E, H), up to isomorphism over $\overline{K}$, where E is an elliptic curve defined over K and $H \subseteq E(\overline{K})$ is a cyclic subgroup of order N that is defined over K. Then there is a bijection $\mathrm{Ell}'_{0,N}(K) \xrightarrow{\sim} X_0(N)_{\mathbb{Q}}(K) \setminus \{\text{cusps}\}$. Using this moduli interpretation, we compute ℓ-isogenies of an elliptic curve for $\ell \in \{2, 3, 5, 7, 13\}$, following Cremona and Watkins [3]. In this chapter except for section 4.5, we assume that $\mathrm{char}(K) \notin \{2, 3, \ell\}$. In section 4.5 we consider the cases where $\mathrm{char}(K) = 2$ or 3.

4.1 Modular approach

By Proposition 2.3.5, we can see that $X_0(\ell)$ has genus 0 if and only if $\ell \in \{2, 3, 5, 7, 13\}$. When the genus of $X_0(\ell)$ is 0, the function field $\mathbb{C}(X_0(\ell))$ is generated by a single function. For each ℓ, we may choose the generator to be

$$h = \left(\frac{\eta(q)}{\eta(q^\ell)}\right)^{24/(\ell-1)}$$

(see [7, section 4]). The Atkin-Lehner involution w_ℓ takes h to $t := \frac{\ell^{12/(\ell-1)}}{h}$, and thus t is also a generator of $\mathbb{C}(X_0(\ell))$. Using t, the j-function $j : \mathcal{H} \to \mathbb{C}$

can be expressed as $j = F_\ell(t)$ given by the following rational functions:

$$\begin{aligned}
F_2(t) &= \frac{(t+16)^3}{t}, \\
F_3(t) &= \frac{(t+27)(t+3)^3}{t}, \\
F_5(t) &= \frac{(t^2+10t+5)^3}{t}, \\
F_7(t) &= \frac{(t^2+13t+49)(t^2+5t+1)^3}{t}, \\
F_{13}(t) &= \frac{(t^2+5t+13)(t^4+7t^3+20t^2+19t+1)^3}{t}.
\end{aligned}$$

Hence given $j_0 \in K$, each root $t \in K$ of the equation $F_\ell(t) = j_0$ corresponds to a modular pair (E, H) over K such that $j(E) = j_0$.

Since w_ℓ takes t to $h = \frac{\ell^{12/(\ell-1)}}{t}$ and takes j to $j_\ell := j_\ell(\tau) = j(\ell\tau)$, for each ℓ the function j_ℓ can be written as $j_\ell = \tilde{F}_\ell(t)$ where:

$$\begin{aligned}
\tilde{F}_2(t) &= \frac{(t+2^8)^3}{t^2}, \\
\tilde{F}_3(t) &= \frac{(t+27)(t+3^5)^3}{t^3}, \\
\tilde{F}_5(t) &= \frac{(t^2+250t+5^5)^3}{t^5}, \\
\tilde{F}_7(t) &= \frac{(t^2+13t+49)(t^2+245t+7^4)^3}{t^7}, \\
\tilde{F}_{13}(t) &= \frac{(t^2+5t+13)(t^4+247t^3+3380t^2+15379t+13^4)^3}{t^{13}}.
\end{aligned}$$

Since j and j_ℓ can be written as rational functions in t, t generates the function field $\mathbb{Q}(j, j_\ell)$. Moreover, if $t_0 \in K$ satisfies $F_\ell(t_0) = \tilde{F}_\ell(t_0)$, then t_0 corresponds to a degree ℓ endomorphism.

Let $\ell \in \{2, 3, 5, 7, 13\}$. Let $\mathcal{E}(t)$ be an elliptic curve over $\mathbb{Q}(t)$ of the form

$$\mathcal{E}(t) : y^2 = x^3 + a_4(t)x + a_6(t) \qquad \text{such that} \quad j(\mathcal{E}(t)) = F_\ell(t).$$

Such curve does exist since we can always take $\mathcal{E}(t) = E_j$ given by

$$E_j : y^2 = x^3 - 3jkx - 2jk^2,$$

where $j = F_\ell(t)$ and $k = j - 1728$. We will call $\mathcal{E}(t)$ a *universal elliptic curve*. By computation we find that the ℓ-division polynomial of $\mathcal{E}(t)$ has a unique irreducible degree $\frac{\ell-1}{2}$ factor in $\mathbb{Q}(t)[x]$, which we denote by $\Psi_\ell(x,t)$. We call $\Psi_\ell(x,t)$ the *generic ℓ-kernel polynomial* of $\mathcal{E}(t)$.

Given an elliptic curve E over K, for each root $t_0 \in K$ of $j(E) = F_\ell(t)$, if the curve $\mathcal{E}(t_0)$ over K given by

$$\mathcal{E}(t_0) : y^2 = x^3 + a_4(t_0)x + a_6(t_0)$$

is non-singular then $\mathcal{E}(t_0)$ is an elliptic curve with $j(\mathcal{E}(t_0)) = j(E)$. For example, by taking $\mathcal{E}(t) = E_j$ the curve $\mathcal{E}(t_0)$ is non-singular if $j(E) \notin \{0, 1728\}$. In this case the polynomial $\Psi_\ell(x, t_0) \in K[x]$ is an ℓ-kernel polynomial of $\mathcal{E}(t_0)$, and a K-rational ℓ-kernel polynomial of E can be recovered from $\Psi_\ell(x, t_0)$. Thus the main idea of the method is to compute and store $\Psi_\ell(x,t)$ in advance and then specialize to any given elliptic curve. We will give the details in section 4.3.

4.2 Minimal universal elliptic curve

In previous section we saw that the elliptic curve

$$E_j : y^2 = x^3 - 3jkx - 2jk^2, \qquad \text{where } j = F_\ell(t) \text{ and } k = j - 1728,$$

is a universal elliptic curve. In this section we will construct a "minimal" universal elliptic curve from E_j for each $\ell \in \{2, 3, 5, 7, 13\}$, which has the "smallest" coefficients. By *minimal* we mean a curve satisfying Definition 4.2.1. By working with a minimal universal elliptic curve, computation of the generic ℓ-kernel polynomial can be much more efficient and faster.

Definition 4.2.1. Let $\mathcal{E}(t) : y^2 = x^3 + a_4(t)x + a_6(t)$ be a universal elliptic curve. We say that $\mathcal{E}(t)$ is *minimal* if the following conditions hold.

(1) $a_4(t), a_6(t) \in \mathbb{Z}[t]$.

(2) $\nexists\ h \in \mathbb{Z}[t] \setminus \{\pm 1\}$ such that $a_4(t) = h^2 f$ and $a_6(t) = h^3 g$ for some f, $g \in \mathbb{Z}[t]$.

We can obtain a minimal universal elliptic curve from $\mathcal{E}(t) : y^2 = x^3 + a_4(t)x + a_6(t)$ as follows. First we make $\mathcal{E}(t)$ defined over $\mathbb{Z}[t]$ in the same way as making an elliptic curve over $\mathbb{Q}$ integral by clearing the denominators of $a_4(t)$ and $a_6(t)$. Note that the j-invariant does not change by this operation. Once the curve is defined over $\mathbb{Z}[t]$, it is easy to see that there is a unique $h \in \mathbb{Z}[t]$ up to sign, such that the above conditions (1) and (2) hold. Hence we obtain a minimal universal elliptic curve, and note that it is unique up to twist by -1.

We present the table below for a minimal universal elliptic curve $\mathcal{E}(t) : y^2 = x^3 + a_4(t)x + a_6(t)$ for each $\ell \in \{2, 3, 5, 7, 13\}$. The table consists of $a_4(t)$, $a_6(t)$, the discriminant $\Delta(\mathcal{E}(t))$ and the generic kernel polynomial $\Psi_\ell(x, t)$ of $\mathcal{E}(t)$.

Table 4.1: Minimal universal elliptic curves

$\ell = 2 :$
$a_4(t) = -3(t + 16)(t + 64)$ $a_6(t) = -2(t + 64)^2(t - 8)$ $\Delta(\mathcal{E}(t)) = 2^{12}3^6 t(t + 64)^3$ $\Psi_2(x, t) = x + t + 64$
$\ell = 3 :$
$a_4(t) = -3(t + 3)(t + 27)$ $a_6(t) = -2(t + 27)(t^2 + 18t - 27)$ $\Delta(\mathcal{E}(t)) = 2^{12}3^6 t(t + 27)^2$ $\Psi_3(x, t) = x + t + 27$
$\ell = 5 :$
$a_4(t) = -3(t^2 + 10t + 5)(t^2 + 22t + 125)$ $a_6(t) = -2(t^2 + 22t + 125)^2(t^2 + 4t - 1)$ $\Delta(\mathcal{E}(t)) = 2^{12}3^6 t(t^2 + 22t + 125)^3$ $\Psi_5(x, t) = x^2 + 2(t^2 + 22t + 125)x + (t^2 + 22t + 89)(t^2 + 22t + 125)$

$\ell = 7$:
$a_4(t) = -3(t^2+5t+1)(t^2+13t+49)$
$a_6(t) = -2(t^2+13t+49)(t^4+14t^3+63t^2+70t-7)$
$\Delta(\mathcal{E}(t)) = 2^{12}3^6t(t^2+13t+49)^2$
$\Psi_7(x,t) = x^3+3(t^2+13t+49)x^2+3(t^2+13t+33)(t^2+13t+49)x$
$+(t^2+13t+49)(t^4+26t^3+219t^2+778t+881)$
$\ell = 13$:
$a_4(t) = -3(t^2+5t+13)(t^2+6t+13)(t^4+7t^3+20t^2+19t+1)$
$a_6(t) = -2(t^2+5t+13)(t^2+6t+13)^2(t^6+10t^5+46t^4+108t^3$
$+122t^2+38t-1)$
$\Delta(\mathcal{E}(t)) = 2^{12}3^6t(t^2+5t+13)^2(t^2+6t+13)^3$
$\Psi_{13}(x,t) = x^6+6(t^2+5t+13)(t^2+6t+13)x^5+3(t^2+5t+13)$
$(t^2+6t+13)(5t^4+55t^3+260t^2+583t+537)x^4+4(t^2+5t+13)$
$(t^2+6t+13)^2(5t^6+80t^5+560t^4+2214t^3+5128t^2+6568t+3373)x^3$
$+3(t^2+5t+13)^2(t^2+6t+13)^2(5t^8+110t^7+1045t^6+5798t^5$
$+20508t^4+47134t^3+67685t^2+54406t+17581)x^2+6(t^2+5t+13)^2$
$(t^2+6t+13)^3(t^{10}+27t^9+316t^8+2225t^7+10463t^6+34232t^5$
$+78299t^4+122305t^3+122892t^2+69427t+16005)x+(t^2+5t+13)^2$
$(t^2+6t+13)^3(t^{14}+38t^{13}+649t^{12}+6844t^{11}+50216t^{10}$
$+271612t^9+1115174t^8+3520132t^7+8549270t^6+15812476t^5$
$+21764840t^4+21384124t^3+13952929t^2+5282630t+854569)$

4.3 Computing ℓ-isogenies

Let $\ell \in \{2,3,5,7,13\}$ and assume that $\mathrm{char}(K) \notin \{2,3,\ell\}$. Let E be an elliptic curve over K given by $y^2+a_1xy+a_3y = x^3+a_2x^2+a_4x+a_6$. In this section we show how to compute all K-rational ℓ-isogenies of E up to equivalence, by using the minimal universal elliptic curve $\mathcal{E}(t) : y^2 = x^3+a_4(t)x+a_6(t)$ and the generic ℓ-kernel polynomial $\Psi_\ell(x,t)$ of $\mathcal{E}(t)$ given in Table 4.1.

4.3.1 $j(E) \notin \{0, 1728\}$ case

Suppose $j(E) \notin \{0, 1728\}$. In this case the roots of $j(E) = F_\ell(t)$ are distinct since the covering map $X_0(\ell) \to X(1)$ ramifies only above i or ρ, which correspond to the j-invariant 1728 and 0 respectively.

Isogenies from the generic kernel polynomial

Since $\mathrm{char}(K) \neq 2$ or 3, by (2.3) and (2.4) we can transform E to

$$E_w : y^2 = x^3 - 27c_4x - 54c_6. \tag{4.1}$$

Note that c_4 and c_6 are non-zero since $j(E) \notin \{0, 1728\}$. Let

$$T(t) = \frac{a_6(t)}{a_4(t)} \cdot \frac{-27c_4}{-54c_6} = \frac{a_6(t)c_4}{2a_4(t)c_6}.$$

We will call $T(t)$ the *twisting parameter* of $\mathcal{E}(t)$ for $j(E) \notin \{0, 1728\}$. We have the following lemma.

Lemma 4.3.1. *Let $t_0 \in K$ be a root of $j(E) = F_\ell(t)$. Then*

$$(36T(t_0))^{-d} \cdot \Psi_\ell((36x + 3b_2)T(t_0), t_0)$$

is a K-rational ℓ-kernel polynomial of E, where $d = 1$ if $\ell = 2$ and $d = \frac{\ell-1}{2}$ otherwise.

Proof. It is easy to check that the twist of $\mathcal{E}(t_0)$ by $T(t_0)^{-1}$, given by

$$\mathcal{E}^{(T(t_0)^{-1})}(t_0) : y^2 = x^3 + a_4(t_0)xT(t_0)^{-2} + a_6(t_0)T(t_0)^{-3},$$

is equal to E_w. Since $\Psi_\ell(x, t_0)$ is an ℓ-kernel polynomial of $\mathcal{E}(t_0)$ and since a kernel polynomial is monic and has degree d, it follows that $T(t_0)^{-d} \cdot \Psi_\ell((xT(t_0), t_0)$ is an ℓ-kernel polynomial of E_w. Now the result follows from the transformation from E_w to E given in (2.3) and (2.4). The resulting polynomial is clearly K-rational since $T(t_0)$ and b_2 are both in K. □

For each root t_0 of $j(E) = F_\ell(t)$, we can compute a K-rational ℓ-isogeny of E from the ℓ-kernel polynomial obtained from Lemma 4.3.1, by

using Kohel's formula given in section 2.2.3.

4.3.2 $j(E) = 0$ case

In this case the equation $0 = j(E) = F_\ell(t)$ has multiple roots since the covering map $X_0(\ell) \to X(1)$ ramifies above ρ.

For each $\ell \in \{2, 3, 5, 7, 13\}$, the rational function $F_\ell(t)$ is of the form

$$F_\ell(t) = \begin{cases} \frac{e_{0,\ell}(t)h_{0,\ell}^3(t)}{t} & \text{if } \ell = 3 \text{ or } \ell \equiv 1 \pmod 3, \\ \frac{h_{0,\ell}^3(t)}{t} & \text{if } \ell \equiv 2 \pmod 3, \end{cases}$$

where $e_{0,\ell}(t)$, $h_{0,\ell}(t) \in \mathbb{Z}[t]$, $\deg(e_{0,\ell}(t)) = 1$ if $\ell = 3$ and $\deg(e_{0,\ell}(t)) = 2$ if $\ell \equiv 1 \pmod 3$. Note that $e_{0,\ell}(t)$ and $h_{0,\ell}(t)$ have no common root.

The structure of $X_0(\ell)$ as a moduli space and Proposition 2.2.12 imply that a root of $e_{0,\ell}(t) = 0$ corresponds to an order ℓ subgroup of E that is fixed by $\mathrm{Aut}(E)$, while a root of $h_{0,\ell}(t) = 0$ corresponds to an order ℓ subgroup of E that is not fixed by $\mathrm{Aut}(E)$. Hence a root of $e_{0,\ell}(t) = 0$ corresponds to a K-rational degree ℓ endomorphism of E up to equivalence, and a root of $h_{0,\ell}(t) = 0$ corresponds to a K-rational ℓ-isogeny of E up to equivalence that is not an endomorphism.

Endomorphisms

For each $\ell \in \{2, 3, 5, 7, 13\}$, it turns out that if t_0 is a root of $e_{0,\ell}(t) = 0$ then $\mathcal{E}(t_0)$ is singular, where $\mathcal{E}(t)$ is the minimal universal elliptic curve given in Table 4.1. Thus we cannot use the generic ℓ-kernel polynomial $\Psi_\ell(x, t)$ to compute ℓ-kernel polynomials of given E that correspond to endomorphisms up to equivalence. Hence we provide an alternative approach to compute these endomorphisms.

Consider the elliptic curve $\mathcal{E}_0(z) : y^2 = x^3 + z$ over $\mathbb{Q}(z)$. If $\ell = 3$, it turns out that the ℓ-division polynomial of $\mathcal{E}_0(z)$ has a unique linear factor in $\mathbb{Q}(z)[x]$, namely x. From (2.4) it follows that the polynomial

$$36^{-1} \cdot (36x + 3b_2) = x + \frac{b_2}{12}$$

is a kernel polynomial of E.

If $\ell \equiv 1 \pmod 3$ then there are precisely two irreducible degree $\frac{\ell-1}{2}$ factors in $\mathbb{Q}(\sqrt{-3})(z)[x]$, and they are complex conjugates of each other. We denote these two polynomials by $\Psi_{\ell,0}(x,z)$ and $\overline{\Psi}_{\ell,0}(x,z)$. By substituting $z = -54c_6$ and from (2.4), we obtain two kernel polynomials of E that correspond to two inequivalent degree ℓ endomorphisms, given by

$$36^{-d} \cdot \Psi_{\ell,0}((36x + 3b_2), -54c_6),$$
$$36^{-d} \cdot \overline{\Psi}_{\ell,0}((36x + 3b_2), -54c_6).$$

We present the table below for $\Psi_{\ell,0}(x,z)$ for $\ell \in \{3,7,13\}$.

Table 4.2: $\Psi_{\ell,0}(x,z)$ for $\ell \in \{3,7,13\}$

$\ell = 3:$
$\Psi_{3,0}(x,z) = x$
$\ell = 7:$
$\Psi_{7,0}(x,z) = x^3 + \frac{z}{7}(-6\rho - 2)$
$\ell = 13:$
$\Psi_{13,0}(x,z) = x^6 + (-6\rho + 2)x^3 z + \frac{z^2}{13}(-24\rho + 40)$

Non-endomorphisms

Since $j(E) = 0$, we have $c_4 = 0$ and $c_6 \neq 0$. Thus as in (4.1) E can be transformed to

$$E_w : y^2 = x^3 - 54c_6.$$

Let

$$T(t) = \frac{a_6(t)}{-54c_6}.$$

We call $T(t)$ the twisting parameter of $\mathcal{E}(t)$ for $j(E) = 0$. We have the following lemma.

Lemma 4.3.2. *Let $t_0 \in K$ be a root of $h_{0,\ell}(t) = 0$. Let $U \in K$ be such that $U^3 = T(t_0)$. Then*

$$(36U)^{-d} \cdot \Psi_\ell((36x + 3b_2)U, t_0)$$

is a K-rational ℓ-kernel polynomial of E, where $d = 1$ if $\ell = 2$ and $d = \frac{\ell-1}{2}$ otherwise.

Proof. Since $j(\mathcal{E}(t_0)) = j(E) = 0$ and the elliptic curve $\mathcal{E}(t_0)$ is non-singular, $\mathcal{E}(t_0)$ is of the form

$$\mathcal{E}(t_0) : y^2 = x^3 + a_6(t_0).$$

It is easy to check that the twist of $\mathcal{E}(t_0)$ by U^{-1}, given by

$$\mathcal{E}^{(U^{-1})}(t_0) : y^2 = x^3 + a_6(t_0)U^{-3},$$

is equal to E_w. Now the result follows by the same argument as in the proof of Lemma 4.3.1. □

For each root $t_0 \in K$ of $h_{0,\ell}(t) = 0$, there are up to 3 distinct values of U, each giving a distinct kernel polynomial. These three kernel polynomials correspond to one orbit under the action of $\mathrm{Aut}(E)$. For each kernel polynomial, we can compute a K-rational ℓ-isogeny ϕ of E using Kohel's formula given in section 2.2.3.

4.3.3 $j(E) = 1728$ case

In this case the equation $1728 = j(E) = F_\ell(t)$ has multiple roots since the covering map $X_0(\ell) \to X(1)$ ramifies above i.

For each $\ell \in \{2, 3, 5, 7, 13\}$, the rational function $F_\ell(t) - 1728$ is of the form

$$F_\ell(t) - 1728 = \begin{cases} \frac{e_{1728,\ell}(t)h^2_{1728,\ell}(t)}{t} & \text{if } \ell = 2 \text{ or } \ell \equiv 1 \pmod 4 \\ \frac{h^2_{1728,\ell}(t)}{t} & \text{if } \ell \equiv 3 \pmod 4 \end{cases}$$

where $e_{1728,\ell}(t), h_{1728,\ell}(t) \in \mathbb{Z}[t]$. $\deg(e_{1728,\ell}(t)) = 1$ if $\ell = 2$ and $\deg(e_{1728,\ell}(t)) = 2$ if $\ell \equiv 1 \pmod 4$. Note that $e_{1728,\ell}(t)$ and $h_{1728,\ell}(t)$ have no common root.

By the similar argument as in section 4.3.2, a root of $e_{1728,\ell}(t) = 0$ corresponds to a K-rational degree ℓ endomorphism of E up to equivalence, and a root of $h_{1728,\ell}(t) = 0$ corresponds to a K-rational ℓ-isogeny of E up to equivalence that is not an endomorphism.

Endomorphisms

For each $\ell \in \{2, 3, 5, 7, 13\}$, it turns out that if t_0 satisfies $e_{1728,\ell}(t) = 0$ then $\mathcal{E}(t_0)$ is singular, where $\mathcal{E}(t)$ is the minimal universal elliptic curve given in Table 4.1. Thus we cannot use the generic ℓ-kernel polynomial $\Psi_\ell(x, t)$ to compute ℓ-kernel polynomials of given E that correspond to endomorphisms up to equivalence. Hence we provide an alternative approach to compute these endomorphisms.

Consider the elliptic curve $\mathcal{E}_{1728}(z) : y^2 = x^3 + zx$ over $\mathbb{Q}(z)$. If $\ell = 2$, it turns out that the ℓ-division polynomial of $\mathcal{E}_{1728}(z)$ has a unique linear factor in $\mathbb{Q}(z)[x]$, namely x. From (2.4) it follows that the polynomial

$$36^{-1} \cdot (36x + 3b_2) = x + \frac{b_2}{12}$$

is a kernel polynomial of E.

If $\ell \equiv 1 \pmod 4$ then there are precisely two irreducible degree $\frac{\ell-1}{2}$ factors in $\mathbb{Q}(i)(z)[x]$, and they are complex conjugates of each other. We denote these two polynomials by $\Psi_{\ell,1728}(x, z)$ and $\overline{\Psi}_{\ell,1728}(x, z)$. By substituting $z = -27c_4$ and from (2.4), we obtain two kernel polynomials of E that correspond to two degree ℓ endomorphisms, given by

$$36^{-d} \cdot \Psi_{\ell,1728}((36x + 3b_2), -27c_4),$$
$$36^{-d} \cdot \overline{\Psi}_{\ell,1728}((36x + 3b_2), -27c_4).$$

We present the table below for $\Psi_{\ell,1728}(x, z)$ for $\ell \in \{2, 5, 13\}$.

Table 4.3: $\Psi_{\ell,1728}(x,z)$ for $\ell \in \{2,5,13\}$

$\ell = 2:$
$\Psi_{2,1728}(x,z) = x$
$\ell = 5:$
$\Psi_{5,1728}(x,z) = x^2 + \frac{z}{5}(-2i+1)$
$\ell = 13:$
$\Psi_{13,1728}(x,z) = x^6 + (-2i-1)x^4z + (-4i-1)x^2z^2 + \frac{z^3}{13}(-2i-3)$

Non-endomorphisms

Since $j(E) = 1728$, we have $c_4 \neq 0$ and $c_6 = 0$. Thus as in (4.1) E can be transformed to

$$E_w : y^2 = x^3 - 27c_4x.$$

Let

$$T(t) = \frac{a_4(t)}{-27c_4}.$$

We call $T(t)$ the twisting parameter of $\mathcal{E}(t)$ for $j(E) = 1728$. We have the following lemma.

Lemma 4.3.3. *Let $t_0 \in K$ be a root of $h_{1728,\ell}(t) = 0$. Let $U \in K$ be such that $U^2 = T(t_0)$. Then*

$$(36U)^{-d} \cdot \Psi_\ell((36x + 3b_2)U, t_0)$$

is a K-rational ℓ-kernel polynomial of E, where $d = 1$ if $\ell = 2$ and $d = \frac{\ell-1}{2}$ otherwise.

Proof. Since $j(\mathcal{E}(t_0)) = j(E) = 1728$ and the elliptic curve $\mathcal{E}(t_0)$ is non-

singular, $\mathcal{E}(t_0)$ is of the form

$$\mathcal{E}(t_0) : y^2 = x^3 + a_4(t_0)x$$

It is easy to check that the twist of $\mathcal{E}(t_0)$ by U^{-1}, given by

$$\mathcal{E}^{(U^{-1})}(t_0) : y^2 = x^3 + a_4(t_0)xU^{-2}$$

is equal to E_w. Now the result follows by the same argument as in the proof of Lemma 4.3.1. □

For each root $t_0 \in K$ of $h_{1728,\ell}(t) = 0$, there are up to 2 distinct values of U, each giving a distinct kernel polynomial. These two kernel polynomials correspond to one orbit under the action of $\mathrm{Aut}(E)$. For each kernel polynomial, we can compute a K-rational ℓ-isogeny ϕ of E using Kohel's formula given in section 2.2.3.

4.3.4 Algorithm

Let $\ell \in \{2, 3, 5, 7, 13\}$. Let K be a field such that $\mathrm{char}(K) \notin \{2, 3, \ell\}$. Let E be an elliptic curve over K given by

$$E : \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Let $\mathcal{E}(t)$ be the minimal universal elliptic curve

$$\mathcal{E}(t) : y^2 = x^3 + a_4(t)x + a_6(t)$$

and $\Psi_\ell(x, t)$ be the generic ℓ-kernel polynomial of $\mathcal{E}(t)$ given in Table 4.1. Let $\Psi_{\ell,0}(x, z)$ and $\Psi_{\ell,1728}(x, z)$ be the polynomials in Table 4.2 and 4.3 respectively, and let $\overline{\Psi}_{\ell,0}(x, z)$ and $\overline{\Psi}_{\ell,1728}(x, z)$ be complex conjugates of $\Psi_{\ell,0}(x, z)$ and $\Psi_{\ell,1728}(x, z)$ respectively.

We present three algorithms which compute all K-rational ℓ-isogenies of E up to equivalence for the cases $j \notin \{0, 1728\}$, $j = 0$, $j = 1728$ as Algorithm 2, 3 and 4.

Algorithm 2 `isogenies_prime_degree_genus_0`(E, ℓ)

Input: E, ℓ

Output: A set of K-rational ℓ-isogenies of E

Compute $j(E)$
if $j(E) = 0$ **then**
  return `isogenies_prime_degree_genus_0_j0`(E, ℓ)
else if $j(E) = 1728$ **then**
  return `isogenies_prime_degree_genus_0_j1728`(E, ℓ)
else if $j(E) \notin \{0, 1728\}$ **then**
  Let $d = 1$ if $\ell = 2$ and $d = \frac{\ell-1}{2}$ otherwise
  Compute $R_t = \{t_0 \in K \mid j(E) = F_\ell(t_0)\}$
  Compute c_4, c_6, b_2 of E
  Let $T(t) = \frac{a_6(t)c_4}{2a_4(t)c_6}$
  Set $\mathcal{K} = \{(36T(t_0))^{-d} \cdot \Psi_\ell((36x + 3b_2)T(t_0), t_0) \mid t_0 \in R_t\}$
  Set $\mathcal{I} = \emptyset$
  for f in $\mathcal{K}$ **do**
    Compute the isogeny ϕ of E from f `//using Kohel's formula`
    Append ϕ to $\mathcal{I}$
  end for
  return $\mathcal{I}$
end if

Algorithm 3 `isogenies_prime_degree_genus_0_j0`(E, ℓ)

Input: E with $j(E) = 0$, ℓ

Output: A set of K-rational ℓ-isogenies of E

Let $d = 1$ if $\ell = 2$ and $d = \frac{\ell-1}{2}$ otherwise
Compute $R_t = \{t_0 \in K \mid h_{0,\ell}(t_0) = 0\}$
Compute c_6, b_2 of E
Set $\mathcal{K} = \emptyset$
`// For endomorphisms:`
if $\ell = 3$ **then**
    Append $x + \frac{b_2}{12}$ to $\mathcal{K}$
else if $\ell \equiv 1 \pmod 3$ **and** -3 is a square in K **then**
    Append $36^{-d} \cdot \Psi_{\ell,0}((36x + 3b_2), -54c_6)$, $36^{-d} \cdot \overline{\Psi}_{\ell,0}((36x + 3b_2), -54c_6)$ to $\mathcal{K}$
end if
`// For non-endomorphisms:`
for t_0 in R_t **do**
    for $U \in K$ such that $U^3 = \frac{a_6(t_0)}{-54c_6}$ **do**
        Append $(36U)^{-d} \cdot \Psi_\ell((36x + 3b_2)U, t_0)$ to $\mathcal{K}$
    end for
end for
Set $\mathcal{I} = \emptyset$
for f in $\mathcal{K}$ **do**
    Compute the isogeny ϕ of E from f `//using Kohel's formula`
    Append ϕ to $\mathcal{I}$
end for
return $\mathcal{I}$

Algorithm 4 `isogenies_prime_degree_genus_0_j1728`(E, ℓ)

Input: E with $j(E) = 1728$, ℓ

Output: A set of K-rational ℓ-isogenies of E

Let $d = 1$ if $\ell = 2$ and $d = \frac{\ell-1}{2}$ otherwise
Compute $R_t = \{t_0 \in K \mid h_{1728,\ell}(t) = 0\}$
Compute c_4, b_2 of E
Set $\mathcal{K} = \emptyset$
`// For endomorphisms:`
if $\ell = 2$ **then**
    Append $x + \frac{b_2}{12}$ to $\mathcal{K}$
else if $\ell \equiv 1 \pmod 4$ **and** -1 is a square in K **then**
    Append $36^{-d} \cdot \Psi_{\ell,1728}((36x+3b_2), -27c_4)$, $36^{-d} \cdot \overline{\Psi}_{\ell,1728}((36x+3b_2), -27c_4)$ to $\mathcal{K}$
end if
`// For non-endomorphisms:`
for t_0 in R_t **do**
    for $U \in K$ such that $U^2 = \frac{a_4(t_0)}{-27c_4}$ **do**
        Append $(36U)^{-d} \cdot \Psi_\ell((36x + 3b_2)U, t_0)$ to $\mathcal{K}$
    end for
end for
Set $\mathcal{I} = \emptyset$
for f in $\mathcal{K}$ **do**
    Compute the isogeny ϕ of E from f `//using Kohel's formula`
    Append ϕ to $\mathcal{I}$
end for
return $\mathcal{I}$

4.4 Examples

Here we illustrate three examples that use Algorithm 2, 3 and 4.

Example 4.4.1. Let

$$E: \ y^2 + xy = x^3 - x^2 + 1 \quad \text{over } \mathbb{Q}.$$

We will compute all $\mathbb{Q}$-rational 7-isogenies of E up to equivalence. One can check that the only root of the equation $-\frac{9}{5} = j(E) = F_7(t)$ over $\mathbb{Q}$ is $t_0 = -5$. We compute c_4, c_6 and b_2 of E:

$$c_4 = 9, \qquad c_6 = -837, \qquad b_2 = -3.$$

Let $\mathcal{E}(t) : y^2 = x^3 + a_4(t)x + a_6(t)$ be the universal elliptic curve where $a_4(t)$ and $a_6(t)$ are given by

$$\begin{aligned} a_4(t) &= -3(t^2 + 5t + 1)(t^2 + 13t + 49), \\ a_6(t) &= -2(t^2 + 13t + 49)(t^4 + 14t^3 + 63t^2 + 70t - 7). \end{aligned}$$

The generic 7-kernel polynomial of $\mathcal{E}(t)$ is given by

$$\begin{aligned} \Psi_7(x,t) &= x^3 + 3(t^2 + 13t + 49)x^2 + 3(t^2 + 13t + 33)(t^2 + 13t + 49)x \\ &\quad +(t^2 + 13t + 49)(t^4 + 26t^3 + 219t^2 + 778t + 881), \end{aligned}$$

and the twisting parameter is given by $T(t) = \frac{a_6(t)c_4}{2a_4(t)c_6}$.

A kernel polynomial of E is given by

$$(36T(t_0))^{-d} \cdot \Psi_\ell((36x + 3b_2)T(t_0), t_0) = x^3 - 3x^2 + 1.$$

Using Kohel's formula we obtain a 7-isogeny from E to the curve

$$E': \ y^2 + xy = x^3 - x^2 - 225x - 1250 \qquad \text{with } j(E') = -\frac{3^2 \cdot 1201^3}{5^7},$$

and the isogeny is given by $(x, y) \mapsto (r_1(x), yr_1'(x) + r_2(x))$, where

$$r_1(x) = \frac{x^7 - 6x^6 + 54x^5 - 70x^4 - 15x^3 + 72x^2 - 17x + 18}{(x^3 - 3x^2 + 1)^2},$$
$$r_2(x) = \frac{-45x^8 + 108x^7 - 90x^6 - 117x^5 + 270x^4 - 180x^3 + 171x^2 - 9}{(x^3 - 3x^2 + 1)^3}.$$

This is the only $\mathbb{Q}$-rational 7-isogeny of E up to equivalence.

Example 4.4.2. Let $K = \mathbb{Q}(i, \sqrt{5})$ and let

$$E: \ y^2 = x^3 - \sqrt{5}x \quad \text{over } K$$

We will compute all K-rational 5-isogenies of E up to equivalence. Since $j(E) = 1728$ and

$$F_7(t) - 1728 = \frac{(t^2 + 22t + 125)(t^2 + 4t - 1)^2}{t},$$

the roots of $1728 = j(E) = F_7(t)$ over K are $t = -11 \pm 2i$ and $t = -2 \pm \sqrt{5}$. We compute c_4 and b_2 of E:

$$c_4 = 48\sqrt{5}, \qquad b_2 = 0.$$

We use the universal elliptic curve $\mathcal{E}(t) : y^2 = x^3 + a_4(t)x + a_6(t)$ where $a_4(t)$ and $a_6(t)$ are given by

$$\begin{aligned} a_4(t) &= -3(t^2 + 10t + 5)(t^2 + 22t + 125), \\ a_6(t) &= -2(t^2 + 22t + 125)^2(t^2 + 4t - 1). \end{aligned}$$

Its generic kernel polynomial is given by

$$\Psi_5(x, t) = x^2 + 2(t^2 + 22t + 125)x + (t^2 + 22t + 89)(t^2 + 22t + 125),$$

and the twisting parameter is given by $T(t) = \frac{a_4(t)}{-27c_4}$.

The roots $t = -11 \pm 2i$ correspond to two degree 5 endomorphisms of

E up to equivalence. By using

$$\begin{aligned}\Psi_{\ell,1728}(x,z) &= x^2+\frac{z}{5}(-2i+1),\\ \overline{\Psi}_{\ell,1728}(x,z) &= x^2+\frac{z}{5}(2i+1),\end{aligned}$$

we obtain two kernel polynomials of E given by:

$$\begin{aligned}36^{-2}\cdot\Psi_{\ell,1728}((36x+3b_2),-27c_4) &= x^2+\frac{2i\sqrt{5}}{5}-\frac{\sqrt{5}}{5},\\ 36^{-2}\cdot\overline{\Psi}_{\ell,1728}((36x+3b_2),-27c_4) &= x^2-\frac{2i\sqrt{5}}{5}-\frac{\sqrt{5}}{5}.\end{aligned}$$

By using Kohel's formula and post-composing appropriate isomorphism, we obtain two degree 5 endomorphisms of E.

Next consider the root $t_1=-2+\sqrt{5}$. The equation $U^2=\frac{a_4(t_1)}{-27c_4}=1$ has two roots $U=\pm1$ over K. Hence we obtain a kernel polynomial $(36U)^{-d}\cdot\Psi_\ell((36x+3b_2)U,t_1)$ of E for each $U=\pm1$, given by

$$\begin{aligned}f_1 &:= x^2+(5+\sqrt{5})x+5+2\sqrt{5},\\ f_2 &:= x^2-(5+\sqrt{5})x+5+2\sqrt{5}.\end{aligned}$$

By using Kohel's formula and post-composing appropriate isomorphism, f_1 and f_2 both give 5-isogenies of E to the curve

$$E_1':\ y^2=x^3-(600+161\sqrt{5})x+6440+2240\sqrt{5}$$

with $j(E_1')=22015749613248+9845745509376\sqrt{5}$.

For the root $t_2=-2-\sqrt{5}$, The equation $U^2=\frac{a_4(t_2)}{-27c_4}=-1$ has two roots $U=\pm i$ over K. We obtain two kernel polynomials $(36U)^{-d}\cdot\Psi_\ell((36x+3b_2)U,t_2)$, given by

$$\begin{aligned}g_1 &:= x^2+(5-\sqrt{5})ix-5+2\sqrt{5},\\ g_2 &:= x^2-(5-\sqrt{5})ix-5+2\sqrt{5}.\end{aligned}$$

By using Kohel's formula and post-composing appropriate isomorphism, g_1 and g_2 both give 5-isogenies of E to a curve E_2' with $j(E_2')=22015749613248-$

$9845745509376\sqrt{5}$. In total we obtain six K-rational 5-isogenies of E. Here we omit the rational functions for the isogenies since they are too long to list.

Example 4.4.3. Let

$$E:\ y^2+xy+y=x^3-x^2+4x \quad \text{over } \mathbb{F}_7.$$

We will compute all $\mathbb{F}_7$-rational 13-isogenies of E up to equivalence. One can check that the only roots of the equation $3=j(E)=F_{13}(t)$ over $\mathbb{F}_7$ are $t_1=2$ and $t_2=3$. We compute c_4, c_6 and b_2 of E:

$$c_4=3, \qquad c_6=1, \qquad b_2=4.$$

We use the minimal universal elliptic curve $\mathcal{E}(t): y^2=x^3+a_4(t)x+a_6(t)$ and its generic 13-kernel polynomial $\Psi_{13}(x,t)$ given in Table 4.1. The twisting parameter is given by $T(t)=\frac{a_6(t)c_4}{2a_4(t)c_6}$.

For $t_1=2$, a kernel polynomial of E is given by

$$(36T(t_1))^{-6}\cdot\Psi_{13}((36x+3b_2)T(t_1),t_1)=x^6-2x^4+x^3-x^2-2x-2.$$

Using Kohel's formula we obtain a 13-isogeny from E to the curve

$$E':\ y^2+xy+y=x^3-x^2-x+3 \qquad \text{with } j(E')=3.$$

For $t_2=3$, a kernel polynomial of E is given by

$$(36T(t_2))^{-6}\cdot\Psi_{13}((36x+3b_2)T(t_2),t_2)=x^6+x^5-x^4-x^3+x^2+3x-3.$$

Using Kohel's formula we obtain a 13-isogeny from E to the curve

$$E':\ y^2+xy+y=x^3+6x^2+1 \qquad \text{with } j(E')=3.$$

These two are all the $\mathbb{F}_7$-rational 13-isogenies of E up to equivalence.

4.5 Characteristic 2 and 3 case

4.5.1 Ordinary curves in characteristic 3

Let K be a field of characteristic 3, and let E be an elliptic curve over K. Note that E is ordinary if and only if $j(E) \neq 0$ (see [20, section 3.1]). If E is given in the Weierstrass form (2.2) in characteristic 3, then E can be transformed by (2.3) to the curve

$$y^2 = x^3 + b_2x^2 - b_4x + b_6.$$

If $j(E) \neq 0$ then $b_2 \neq 0$, thus applying

$$x \longmapsto x + \frac{b_4}{b_2} \qquad \text{and} \qquad y \longmapsto y \tag{4.2}$$

to the above curve yields

$$y^2 = x^3 + b_2x^2 + \frac{-b_2^2b_4^2 + b_2^3b_6 + b_4^3}{b_2^3}. \tag{4.3}$$

For each $\ell \in \{2, 5, 7, 13\}$, we define a *minimal universal elliptic curve* $\mathcal{E}(t) : y^2 = x^3 + a_4(t)x + a_6(t)$ over $\mathbb{F}_3(t)$ to be a universal elliptic curve satisfying:

(1) $a_2(t), a_6(t) \in \mathbb{F}_3[t]$,

(2) $\nexists\, h \in \mathbb{F}_3[t] \setminus \{\pm 1\}$ such that $h \mid a_2(t)$ and $h^3 \mid a_6(t)$.

We can construct such a curve from the universal elliptic curve

$$y^2 = x^3 - jx^2 + j^2 \qquad \text{where } j = F_\ell(t),$$

by a similar way as in section 4.2. We present a list of minimal universal elliptic curves for each ℓ in Table 4.4. For each $\ell \in \{2, 5, 7, 13\}$, we find by computation that the ℓ-division polynomial of the minimal universal elliptic curve in Table 4.4 has a unique irreducible degree $\frac{\ell-1}{2}$ factor in $\mathbb{Q}(t)[x]$. We denote this factor by $\Psi_\ell(x, t)$ and call it the generic ℓ-kernel polynomial of $\mathcal{E}(t)$. We will compute all K-rational ℓ-isogenies of E up to equivalence by using $\Psi_\ell(x, t)$.

Computing ℓ-isogenies

Let $\ell \in \{2, 5, 7, 13\}$ and let E be an ordinary elliptic curve over K. Note that the roots of $j(E) = F_\ell(t)$ are distinct for each $\ell \in \{2, 5, 7, 13\}$, since the above equation has multiple roots over K if and only if $j(E) = 0$. However E ordinary implies that $j(E) \neq 0$.

Let $\mathcal{E}(t) : y^2 = x^3 + a_2(t)x^2 + a_6(t)$ be a minimal universal elliptic curve, and let $\Psi_\ell(x, t)$ denote the generic kernel polynomial of $\mathcal{E}(t)$. Let

$$T(t) = \frac{a_2(t)}{b_2},$$

and we call $T(t)$ the twisting parameter of $\mathcal{E}(t)$. We have the following lemma.

Lemma 4.5.1. *Let $t_0 \in K$ be a root of $j(E) = F_\ell(t)$. Then*

$$T(t_0)^{-d} \cdot \Psi_\ell \left(\left(x - \frac{b_4}{b_2} \right) T(t_0), t_0 \right)$$

is a K-rational ℓ-kernel polynomial of E, where $d = 1$ if $\ell = 2$ and $d = \frac{\ell-1}{2}$ otherwise.

Proof. It is easy to check that the twist of $\mathcal{E}(t_0)$ by $T(t_0)^{-1}$, given by

$$\mathcal{E}^{(T(t_0)^{-1})}(t_0) : y^2 = x^3 + a_2(t_0)x^2 T(t_0)^{-1} + a_6(t_0)T(t_0)^{-3},$$

is equal to E_w. Now the result follows from the transformation (4.2). □

For each root of $j(E) = F_\ell(t)$, we can compute a K-rational ℓ-isogeny of E from the ℓ-kernel polynomial obtained from Lemma 4.3.1, by using Kohel's formula given in section 2.2.3.

We present the table below for a minimal universal elliptic curve for each $\ell \in \{2, 5, 7, 13\}$. The table consists of $a_4(t)$, $a_6(t)$, the discriminant $\Delta(\mathcal{E}(t))$ and the generic kernel polynomial $\Psi_\ell(x, t)$ of $\mathcal{E}(t)$.

Table 4.4: Minimal universal elliptic curves: for ordinary curves in characteristic 3

$\ell = 2:$
$a_2(t) = t + 1$
$a_6(t) = -t$
$\Delta = t(t+1)^3$
$\Psi_2(x,t) = x + 1$
$\ell = 5:$
$a_2(t) = t^2 + t - 1$
$a_6(t) = -t$
$\Delta = t(t^2+t-1)^3$
$\Psi_5(x,t) = x^2 - (t+1)x + t - 1$
$\ell = 7:$
$a_2(t) = (t-1)(t+1)^2$
$a_6(t) = -t(t-1)$
$\Delta = t(t-1)^4(t+1)^6$
$\Psi_7(x,t) = x^3 - (t-1)(t+1)x^2 + (t-1)^2(t+1)x - (t-1)(t^2+t-1)$
$\ell = 13:$
$a_2(t) = (t-1)^2(t+1)(t^2+1)$
$a_6(t) = -t(t+1)$
$\Delta = t(t-1)^6(t+1)^4(t^2+1)^3$
$\Psi_{13}(x,t) = x^6 - (t-1)(t+1)(t^2+1)x^5$
$+(t-1)(t+1)^2(t^2+1)^2x^4 - t(t+1)(t^7 - t^6 + t^5 + t^4 - t^3 + t^2 - t + 1)x^3$
$+(t-1)(t+1)^2(t^2+1)(t^5 - t^4 + 1)x^2 - (t-1)(t+1)^5(t^2+1)^2x$
$+(t+1)^2(t^7 + t^6 + t^5 - t^4 - t^3 - t + 1)$

Let us look at the following example.

Example 4.5.2. Let

$$E: \ y^2 + xy = x^3 - 1 \quad \text{over } \mathbb{F}_3.$$

We will compute all $\mathbb{F}_3$-rational 5-isogenies of E up to equivalence. One can check that the roots of the equation $1 = j(E) = F_5(t)$ over $\mathbb{F}_3$ are $t_1 = -1$ and

$t_2 = 1$. We compute b_2 and b_4 of E:

$$b_2 = 1, \qquad b_4 = 0.$$

Let $\mathcal{E}(t) : y^2 = x^3 + a_2(t)x^2 + a_6(t)$ be the universal elliptic curve where $a_2(t)$ and $a_6(t)$ are given by

$$a_2(t) = t^2 + t - 1 \qquad \text{and} \qquad a_6(t) = -t.$$

The generic 5-kernel polynomial of $\mathcal{E}(t)$ is given by

$$\Psi_5(x, t) = x^2 - (t + 1)x + t - 1,$$

and the twisting parameter is given by $T(t) = \frac{a_2(t)}{b_2}$.

For the root $t_1 = -1$, a kernel polynomial of E is given by

$$T(t_1)^{-2} \cdot \Psi_5 \left(\left(x - \frac{b_4}{b_2} \right) T(t_1), t_1 \right) = x^2 + x.$$

By using Kohel's formula and post-composing an appropriate isomorphism, we obtain the degree 5 endomorphism of E given by $(x, y) \mapsto (r_1(x), -yr_1'(x) + r_2(x))$, where

$$r_1(x) = \frac{x^5 - x^3 + x^2 + x - 1}{(x^2 + x)^2} \qquad \text{and} \qquad r_2(x) = \frac{-x^7 + x^6 - x^3 + x}{(x^2 + x)^3}.$$

For the root $t_2 = 1$, a kernel polynomial of E is given by

$$T(t_2)^{-2} \cdot \Psi_5 \left(\left(x - \frac{b_4}{b_2} \right) T(t_2), t_2 \right) = x^2 + 1.$$

By using Kohel's formula we obtain another degree 5 endomorphism of E given by $(x, y) \mapsto (r_1(x), yr_1'(x) + r_2(x))$, where

$$r_1(x) = \frac{x^5 - x^3 - x - 1}{(x^2 + 1)^2} \qquad \text{and} \qquad r_2(x) = \frac{x^3 + x^2 - 1}{(x^2 + 1)^3}.$$

These two are all the $\mathbb{F}_3$-rational 5-isogenies of E up to equivalence.

4.5.2 Ordinary curves in characteristic 2

Let K be a field of characteristic 2, and let E be an elliptic curve over K. Note that E is ordinary if and only if $j(E) \neq 0$ (see [20, section 3.1]). If E is given in Weierstrass form (2.2) and $j(E) \neq 0$, then $a_1 \neq 0$. Hence E can be transformed to a curve

$$E_w : y^2 + xy = x^3 + \frac{a_1 a_2 + a_3}{a_1^3} x^2 + \frac{1}{j(E)} \tag{4.4}$$

by the transformation

$$x \longmapsto a_1^2 x + \frac{a_3}{a_1} \qquad \text{and} \qquad y \longmapsto a_1^3 y + \frac{a_1^2 a_4 + a_3^2}{a_1^3} \tag{4.5}$$

(see [17, Appendix A]).

Let $\mathcal{E}(t)$ be the universal elliptic curve over $\mathbb{F}_2(t)$ given by:

$$\mathcal{E}(t) : y^2 + xy = x^3 + \frac{1}{j} \qquad \text{where } j = F_\ell(t).$$

Note that the $\Delta(\mathcal{E}(t)) = t$ for each $\ell \in \{3, 5, 7, 13\}$. For each $\ell \in \{3, 5, 7, 13\}$, we find by computation that the ℓ-division polynomial of $\mathcal{E}(t)$ has a unique irreducible degree $\frac{\ell-1}{2}$ factor in $\mathbb{Q}(t)[x]$. We denote this factor by $\Psi_\ell(x, t)$ and call it the generic ℓ-kernel polynomial of $\mathcal{E}(t)$.

Note that a transformation preserving a curve of the form $y^2 + xy = x^3 + Ax^2 + B$ where $A, B \in K$ is given by (see [17, Appendix A])

$$x \longmapsto x \qquad \text{and} \qquad y \longmapsto y + sx, \qquad \text{where } s \in K.$$

Since a kernel polynomial only depend on x, the kernel polynomials of E_w are same as the kernel polynomials of $\mathcal{E}(t_0) : y^2 + xy = x^3 + 1/F_\ell(t_0)$, where $j(E_w) = j(E) = F_\ell(t_0)$ for some t_0. Hence we compute K-rational ℓ-isogenies of a given elliptic curve as follows.

Computing ℓ-isogenies

Let $\ell \in \{3, 5, 7, 13\}$ and let E be an ordinary elliptic curve over K. Note that the roots of $j(E) = F_\ell(t)$ are distinct for each $\ell \in \{3, 5, 7, 13\}$, since the above

equation has multiple roots over K if and only if $j(E) = 0$. However, $j(E) \neq 0$ since E is ordinary.

For each root $t_0 \in K$ of $j(E) = F_\ell(t)$, the polynomial $\Psi_\ell(x, t_0)$ is an ℓ-kernel polynomial of E_w. From (4.5) it follows that

$$a_1^{\ell-1} \cdot \Psi_\ell\left(\frac{1}{a_1^2}\left(x + \frac{a_3}{a_1}\right), t_0\right)$$

is a K-rational ℓ-kernel polynomial of E. By using Kohel's formula, we obtain a K-rational ℓ-isogeny ϕ of E.

We present the table below for the generic kernel polynomial $\Psi_\ell(x, t)$ of $\mathcal{E}(t)$ above for each $\ell \in \{3, 5, 7, 13\}$. Note that $\Psi_\ell(x, t)$ is well-defined, since $j(E) \neq 0$ implies that $t + 1 \neq 0$ for $\ell = 3$ and 5, $t^2 + t + 1 \neq 0$ for $\ell = 7$, and $(t + 1)(t^2 + t + 1) \neq 0$ for $\ell = 13$.

Table 4.5: The ℓ-generic kernel polynomials for $\mathcal{E}(t)$ for ordinary curves in characteristic 2

$\ell = 3$:
$\Psi_3(x, t) = x + \dfrac{1}{(t+1)}$
$\ell = 5$:
$\Psi_5(x, t) = x^2 + \dfrac{1}{(t+1)}x + \dfrac{1}{(t+1)^3}$
$\ell = 7$:
$\Psi_7(x, t) = x^3 + \dfrac{tx^2}{(t^2+t+1)} + \dfrac{(t+1)x}{(t^2+t+1)^2} + \dfrac{1}{(t^2+t+1)^3}$

$\ell = 13$:
$$\Psi_{13}(x,t) = x^6 + \frac{x^5}{(t+1)} + \frac{t(t^3+t+1)x^4}{(t+1)^3(t^2+t+1)^2} + \frac{tx^3}{(t+1)^3(t^2+t+1)^2} + \frac{(t^4+t^3+1)x^2}{(t+1)^6(t^2+t+1)^4} + \frac{x}{(t+1)^7(t^2+t+1)^4} + \frac{1}{(t+1)^9(t^2+t+1)^6}$$

We give the following example.

Example 4.5.3. Let

$$E: \ y^2 + xy + y = x^3 + x^2 \quad \text{over } \mathbb{F}_2.$$

We will compute all $\mathbb{F}_2$-rational 7-isogenies of E up to equivalence. We find that the only root of the equation $1 = j(E) = F_7(t)$ over $\mathbb{F}_2$ is $t_0 = 1$.

Let

$$\mathcal{E}(t) : y^2 + xy = x^3 + \frac{t}{(t^2+t+1)^4}$$

be the universal elliptic curve. The generic 7-kernel polynomial of $\mathcal{E}(t)$ is given by

$$\Psi_7(x,t) = x^3 + \frac{tx^2}{(t^2+t+1)} + \frac{(t+1)x}{(t^2+t+1)^2} + \frac{1}{(t^2+t+1)^3}.$$

Thus a kernel polynomial of E is given by

$$a_1^6 \cdot \Psi_7\left(\frac{1}{a_1^2}\left(x + \frac{a_3}{a_1}\right), t_0\right) = x^3 + x + 1.$$

By using Kohel's formula and post-composing appropriate isomorphism, we obtain the degree 7 endomorphism of E given by $(x,y) \mapsto (r_1(x), yr_1'(x) + r_2(x))$, where

$$r_1(x) = \frac{x^7 + x^5 + x^4 + x^2 + x}{(x^3+x+1)^2}, \qquad r_2(x) = \frac{x^9 + x^8 + x^6 + x^3 + x^2 + 1}{(x^3+x+1)^3}.$$

This is the only $\mathbb{F}_2$-rational 7-isogeny of E up to equivalence.

4.5.3 Supersingular curves in characteristic 2 and 3

Since a supersingular elliptic curve in characteristic 2 or 3 has a large automorphism group and more isomorphism classes (there are 3 or 7 isomorphism classes in characteristic 2, and there are 4 or 6 isomorphism classes in characteristic 3), the generic kernel polynomial method will be complicated. In this case the division polynomial factorization method would be more desirable to use, since factorization of a polynomial in small characteristic is fast enough to compute.

Chapter 5

Modular Approach: cases where $X_0^+(\ell)$ has genus 0

Let $\mathcal{L}$ denote the set of primes $\{11, 17, 19, 23, 29, 31, 41, 47, 59, 71\}$. These are precisely the primes such that $g(X_0(\ell)) > 0$ and $g(X_0^+(\ell)) = 0$ (see section 5.1 below). In this chapter we extend the method for computing ℓ-isogenies given in Chapter 4 to the cases $\ell \in \mathcal{L}$. We assume throughout the chapter that $\mathrm{char}(K) \neq \ell$.

5.1 Modular Approach

In this section we review the work of Elkies [7] which we will need in later sections. From the genus formulas in Proposition 2.3.5 and (2.11), it follows that $g(X_0(\ell)) > 0$ but $g(X_0^+(\ell)) = 0$ if and only if $\ell \in \mathcal{L}$. For each such ℓ, we can choose a modular function u such that the function field $\mathbb{Q}(X_0^+(\ell))$ is equal to $\mathbb{Q}(u)$. Without loss of generality we may assume that u has a pole only at the cusp of $X_0^+(\ell)$. If $v \in \mathbb{Q}(X_0^+(\ell))$ is such that $w_\ell(v) = -v$, where w_ℓ is the Atkin-Lehner involution, then the function field $\mathbb{Q}(X_0(\ell))$ is generated by u and v. We can choose such v with the property that it has poles only at the cusps of $X_0(\ell)$. Since u and v have poles only at the cusps, there exists a polynomial $f_\ell(u)$ such that $v^2 = f_\ell(u)$, and the degree of $f_\ell(u)$ is $2g + 2$ where $g = g(X_0(\ell))$. Furthermore, suitable choice of u, v (see [7, section 4]) gives $f_\ell(u) \in \mathbb{Q}[u]$. Thus the modular curve $X_0(\ell)_{\mathbb{Q}}$ as a curve over $\mathbb{Q}$ is given by the equation $v^2 = f_\ell(u)$. See Example 5.1.1 for the details of the calculation

(following [7]) for $\ell = 11$ and see [9] for other $\ell \in \mathcal{L}$. In Appendix A we give all 10 polynomials f_ℓ.

Since the j-function j has poles only at the cusps of $X_0(\ell)$, we can write j as a polynomial in u and v. By using the relation $v^2 = f_\ell(u)$, we can write

$$j = \alpha_\ell(u) + v\beta_\ell(u), \tag{5.1}$$

where α_ℓ, $\beta_\ell \in \mathbb{Q}[u]$. To find the polynomials α_ℓ and β_ℓ explicitly, recall the function $j_N(\tau) = j(N\tau)$ from section 2.3.2. Since $w_\ell(j) = j_\ell$ and $w_\ell(v) = -v$, we have

$$j_\ell = \alpha_\ell(u) - v\beta_\ell(u). \tag{5.2}$$

Since $\frac{j+j_\ell}{2} = \alpha_\ell(u)$ and $\frac{j-j_\ell}{2v} = \beta_\ell(u)$, by comparing the q-expansions of u, v, $\frac{j+j_\ell}{2}$ and $\frac{j-j_\ell}{2v}$, we can obtain the polynomials α_ℓ and β_ℓ. Recall from section 2.3.2 that the function field $\mathbb{Q}(X_0(\ell)_\mathbb{Q})$ is equal to $\mathbb{Q}(j, j_\ell)$. Since j and j_ℓ can be written as a polynomial in u and v with coefficients in $\mathbb{Q}$, we have $\mathbb{Q}(j, j_\ell) = \mathbb{Q}(u, v)$.

Example 5.1.1. For $\ell = 11$, we may choose u and v, whose q-expansions are given by:

$$\begin{aligned} u &= q^{-1} + 5 + 17q + 46q^2 + 116q^3 + 252q^4 + O(q^5), \\ v &= -q^{-2} - 2q^{-1} + 12 + 116q + 597q^2 + 2298q^3 + 7616q^4 + O(q^5). \end{aligned}$$

The modular curve $X_0(11)_\mathbb{Q}$ is given by the equation

$$X_0(11)_\mathbb{Q} : \ v^2 = u^4 - 16u^3 + 2u^2 + 12u - 7.$$

Moreover, the j-function j can be written as $j = \alpha_{11}(u) + v\beta_{11}(u)$ where

$$\begin{aligned} \alpha_{11}(u) = \frac{1}{2}(&u^{11} - 55u^{10} + 1188u^9 - 12716u^8 + 69630u^7 - 177408u^6 \\ &+ 133056u^5 + 132066u^4 - 187407u^3 + 40095u^2 + 24300u - 6750), \\ \beta_{11}(u) = \frac{1}{2}&(u-15)(u-6)(u-3)(u-1)u(u^2 - 12u - 9)(u^2 - 10u + 5). \end{aligned}$$

See Appendix A for α_ℓ and β_ℓ for other ℓ.

Finding (u, v) on $X_0(\ell)_{\mathbb{Q}}$ given $j(E)$

Recall that the degree of the covering map $X_0(\ell) \to X(1)$ is $\ell + 1$. Thus given j-invariant $j_0 \in K$, there are at most $\ell + 1$ K-rational points (u, v) on $X_0(\ell)_{\mathbb{Q}}$ satisfying $j_0 = \alpha_\ell(u) + v\beta_\ell(u)$. Each such point corresponds to a modular pair (E, H) defined over K such that $j(E) = j_0$. We will describe how to find all points (u, v) on $X_0(\ell)_{\mathbb{Q}}$ given $j(E)$.

From (5.1) and (5.2), j satisfies the quadratic relation

$$j^2 - P_\ell(u)j + Q_\ell(u) = 0, \tag{5.3}$$

where $P_\ell(u) = j + j_\ell = 2\alpha_\ell(u)$ and $Q_\ell(u) = jj_\ell = \alpha_\ell^2(u) - v^2\beta_\ell^2(u) = \alpha_\ell^2(u) - f_\ell(u)\beta_\ell^2(u)$. By a suitable choice of u and v as in [7, section 4], we have $P_\ell(u)$, $Q_\ell(u) \in \mathbb{Z}[u]$ (see appendix A). Note that since the left hand side of (5.3) has degree $\ell + 1$ as a polynomial in u, there are at most $\ell + 1$ roots in u over K.

Let $u_0 \in K$ be a root of (5.3). If $\beta_\ell(u_0) \neq 0$, then (5.1) gives $v = \frac{j(E) - \alpha_\ell(u_0))}{\beta_\ell(u_0)} \in K$. If $\beta_\ell(u_0) = 0$, then we obtain at most two values of v by solving $v^2 = f_\ell(u_0)$ over K. We obtain at most $\ell + 1$ K-rational points (u, v) on $X_0(\ell)_{\mathbb{Q}}$ satisfying $j(E) = \alpha_\ell(u) + v\beta_\ell(u)$. If $j(E) \notin \{0, 1728\}$ then the covering map $X_0(\ell) \to X(1)$ is unramified, thus there are exactly $\ell + 1$ distinct such points (u, v) on $X_0(\ell)_{\mathbb{Q}}(\overline{K})$ of which the number that are K-rational is 0, 1, 2 or $\ell + 1$.

Remark 5.1.2. Consider a point (u_0, v_0) on $X_0(\ell)_{\mathbb{Q}}$ such that $v_0 = 0$ or $b_\ell(u_0) = 0$. Then since $j(u_0, v_0) = \alpha_\ell(u_0) = j_\ell(u_0, v_0)$, it follows that the point (u_0, v_0) corresponds to some endomorphism.

As in Chapter 4, for each ℓ we construct a *universal elliptic curve* $\mathcal{E}(u, v)$ and *generic ℓ-kernel polynomial* $\Psi_\ell(x, u, v)$ to compute all K-rational ℓ-isogenies of E up to equivalence. For the details of computation of $\Psi_\ell(x, u, v)$, see section 5.3. Let $\mathcal{E}(u, v)$ be an elliptic curve over $\mathbb{Q}(u, v)$ of the form

$$\mathcal{E}(u, v) : y^2 = x^3 + a_4(u, v)x + a_6(u, v),$$

with $a_4(u, v), a_6(u, v) \in \mathbb{Q}(u, v)$, such that $j(\mathcal{E}(u, v)) = \alpha_\ell(u) + v\beta_\ell(u)$. We will call $\mathcal{E}(u, v)$ a *universal elliptic curve*. Such curve does exist since we can

always take $\mathcal{E}(u,v) = E_j$ given by

$$E_j : y^2 = x^3 - 3jkx - 2jk^2,$$

where $j = \alpha_\ell(u) + v\beta_\ell(u)$ and $k = j - 1728$.

Suppose that we are given an elliptic curve E over K. For each K-rational point (u_0, v_0) on $X_0(\ell)_{\mathbb{Q}}$ satisfying $j(E) = \alpha_\ell(u_0) + v_0\beta_\ell(u_0)$, if the curve $\mathcal{E}(u_0, v_0)$ over K given by

$$\mathcal{E}(u_0, v_0) : y^2 = x^3 + a_4(u_0, v_0)x + a_6(u_0, v_0)$$

is non-singular then $\mathcal{E}(u_0, v_0)$ is an elliptic curve with $j(\mathcal{E}(u_0, v_0)) = j(E)$. In this case the polynomial $\Psi_\ell(x, u_0, v_0) \in K[x]$ is an ℓ-kernel polynomial of $\mathcal{E}(u_0, v_0)$, and we can recover a K-rational ℓ-kernel polynomial of E from $\Psi_\ell(x, u_0, v_0)$. The method will be analogous to the one in section 4.3. We compute and store $\Psi_\ell(x, u, v)$ in advance and then specialize to any given elliptic curve. We will give the details in section 5.4.

5.2 Minimal universal elliptic curve

In this section we simplify the universal elliptic curve

$$E_j : y^2 = x^3 - 3jkx - 2jk^2,$$

where $j = \alpha_\ell(u)+v\beta_\ell(u)$ and $k = j-1728$, by studying the divisors of functions j and k. We first define the following.

Definition 5.2.1. Let $\mathcal{E}(u,v) : y^2 = x^3 + a_4(u,v)x + a_6(u,v)$ be a universal elliptic curve. We say that $\mathcal{E}(u,v)$ is *minimal* if the following conditions hold.

(1) $a_4(u,v), a_6(u,v) \in \mathbb{Z}[u,v]$.

(2) $\nexists\ h \in \mathbb{Z}[u,v] \setminus \{\pm 1\}$ such that $a_4(u,v) = h^2 f$ and $a_6(u,v) = h^3 g$ for some $f, g \in \mathbb{Z}[u,v]$.

Elkies [6] constructs a minimal universal elliptic curve by using the Eisenstein series of weight 4 and 6 and a suitable cusp form of weight 2. We

take the following alternative approach by using the divisors to compute the curve obtained by Elkies' method.

Let $\ell \in \mathcal{L}$. Let 0 and ∞ denote the two cusps of $X_0(\ell)$. By (2.12) and (2.13), the divisors of j and k are given by:

$$\mathrm{div}(j) = \begin{cases} 3D_0 + [P_1'] + [P_2'] - \ell[0] - [\infty] & \text{if } \ell \equiv 1 \pmod 3, \\ 3D_0 - \ell[0] - [\infty] & \text{if } \ell \equiv 2 \pmod 3, \end{cases}$$

$$\mathrm{div}(k) = \begin{cases} 2D_{1728} + [Q_1'] + [Q_2'] - \ell[0] - [\infty] & \text{if } \ell \equiv 1 \pmod 4, \\ 2D_{1728} - \ell[0] - [\infty] & \text{if } \ell \equiv 3 \pmod 4, \end{cases}$$

where D_0 and D_{1728} are of the form

$$D_0 = \begin{cases} \sum_{i=1}^{\frac{\ell-1}{3}} [P_i] & \text{if } \ell \equiv 1 \pmod 3, \\ \sum_{i=1}^{\frac{\ell+1}{3}} [P_i] & \text{if } \ell \equiv 2 \pmod 3, \end{cases}$$

$$D_{1728} = \begin{cases} \sum_{i=1}^{\frac{\ell-1}{2}} [Q_i] & \text{if } \ell \equiv 1 \pmod 4, \\ \sum_{i=1}^{\frac{\ell+1}{2}} [Q_i] & \text{if } \ell \equiv 3 \pmod 4. \end{cases}$$

By a theorem of Ogg [13], there is a function h_∞ in $\mathbb{Q}(X_0(\ell)_{\mathbb{Q}})$ such that $\mathrm{div}(h_\infty) = n([0] - [\infty])$, where n is the numerator of $\frac{\ell-1}{12}$.

Furthermore, by using `MAGMA` we find that there is a function h_0 in $\mathbb{Q}(X_0(\ell)_{\mathbb{Q}})$ such that $\mathrm{div}(h_0) = D_0 - \lfloor \frac{\ell+1}{6} \rfloor([0] + [\infty])$. Thus we have

$$\mathrm{div}(j) = \begin{cases} \mathrm{div}(\frac{h_0^3}{h_\infty^d}) + [P_1'] + [P_2'] - [0] - [\infty] & \text{if } \ell \equiv 1 \pmod 3, \\ \mathrm{div}(\frac{h_0^3}{h_\infty^d}) & \text{if } \ell \equiv 2 \pmod 3, \end{cases} \tag{5.4}$$

where d is the denominator of $\frac{\ell+1}{12}$. It follows from (5.4) that there exists a function e_0 in $\mathbb{Q}(X_0(\ell)_{\mathbb{Q}})$ such that $\mathrm{div}(e_0) = [P_1'] + [P_2'] - [0] - [\infty]$ if $\ell \equiv 1 \pmod 3$. Since h_∞, h_0 and e_0 have poles only at the cusps of $X_0(\ell)$, they can be expressed as polynomials in u and v; moreover, we may assume that they are in $\mathbb{Z}[u, v]$. Hence the j-function can be written as

$$j = c\frac{e_0 h_0^3}{h_\infty^d} \tag{5.5}$$

for some $c \in \mathbb{Q}$, where we take $e_0 = 1$ if $\ell \equiv 2 \pmod 3$. For example, for $\ell = 11$ we obtain:

$$c = 2, \qquad e_0 = 1, \qquad h_0 = 61u^2 - 246u + 45 + 60v,$$
$$h_\infty = u^5 - 37u^4 + 459u^3 - 2087u^2 + 2040u + (-u^3 + 29u^2 - 258u + 680)v.$$

Similarly, by using `MAGMA` we find that there is a function h_{1728} in $\mathbb{Q}(X_0(\ell)_{\mathbb{Q}})$ such that $\mathrm{div}(h_{1728}) = D_{1728} - \lfloor \frac{\ell+1}{4} \rfloor([0] + [\infty])$. Thus

$$\mathrm{div}(k) = \begin{cases} \mathrm{div}(\frac{h_{1728}^2}{h_\infty^d}) + [Q_1'] + [Q_2'] - [0] - [\infty] & \text{if } \ell \equiv 1 \pmod 4, \\ \mathrm{div}(\frac{h_{1728}^2}{h_\infty^d}) & \text{if } \ell \equiv 3 \pmod 4. \end{cases} \tag{5.6}$$

It follows from (5.6) that there exists a function e_{1728} in $\mathbb{Q}(X_0(\ell)_{\mathbb{Q}})$ such that $\mathrm{div}(e_{1728}) = [Q_1'] + [Q_2'] - [0] - [\infty]$ if $\ell \equiv 1 \pmod 4$. Since h_{1728} and e_{1728} have poles only at the cusps of $X_0(\ell)$, they can be again expressed as polynomials in u and v, and we may again assume that they are in $\mathbb{Z}[u, v]$. Hence the function k can be written as

$$k = c\frac{e_{1728} h_{1728}^2}{h_\infty^d}, \tag{5.7}$$

where we take $e_{1728} = 1$ if $\ell \equiv 3 \pmod 4$. For example, for $\ell = 11$ we obtain:

$$e_{1728} = 1, \qquad h_{1728} = -7(95u^3 - 819u^2 + 189u + 135) - 18v(37u - 51).$$

From (5.5) and (5.7), we can twist the curve $E_j : y^2 = x^3 - 3jkx - 2jk^2$ to obtain a universal elliptic curve $\mathcal{E}(u, v) : y^2 = x^3 + a_4(u, v) + a_6(u, v)$ where

$$a_4(u, v) = -3e_0 e_{1728} h_0 \qquad \text{and} \qquad a_6(u, v) = -2e_0 e_{1728}^2 h_{1728}.$$

Then $\mathcal{E}(u, v)$ is a minimal universal elliptic curve by construction. For example, for $\ell = 11$ we have

$$a_4(u, v) = -3(61u^2 - 246u + 45 + 60v),$$
$$a_6(u, v) = -2(-7(95u^3 - 819u^2 + 189u + 135) - 18v(37u - 51)).$$

See Appendix A for the table of $a_4(u, v)$ and $a_6(u, v)$ for each $\ell \in \mathcal{L}$.

5.3 Computing generic kernel polynomials

Let $\ell \in \mathcal{L}$ and let $\mathcal{E}(u,v)$ be a universal elliptic curve. To compute the generic ℓ-kernel polynomial $\Psi_\ell(x,u,v)$ of $\mathcal{E}(u,v)$, we need to factorize the ℓ-division polynomial of $\mathcal{E}(u,v)$ and look for an irreducible degree $\frac{\ell-1}{2}$ factor; however, the factorization using the current algorithms (e.g. using `MAGMA`) takes a very long time as ℓ becomes large. For example, for $\ell = 41$ we are not able to factorize the ℓ-division polynomial of degree $\frac{41^2-1}{2} = 840$ in $\mathbb{Q}(u,v)[x]$ using `MAGMA`, even over three weeks. Hence in this section we give an alternative method for computing $\Psi_\ell(x,u,v)$, which is very much faster.

Elkies [7] gave the following idea. Let E and E' be elliptic curves over K given by $E : y^2 = x^3 + Ax + B$ and $E' : y^2 = x^3 + A'x + B'$. Suppose that we have a normalized[1] ℓ-isogeny $\phi : E \to E'$ for a prime ℓ. Let $H = \ker(\phi)$. Let ψ_H be the kernel polynomial of H and write

$$\psi_H(x) = x^d + \sum_{i=1}^{d} s_i x^{d-i}, \qquad \text{where } d = \frac{\ell-1}{2}.$$

The idea of Elkies [7] is that we can recover ψ_H from E, E' and s_1, by using the following recurrence formulas. We give the brief summary of the recurrence here. See [7] for the details.

Recall from chapter 2 that the isogeny $\phi : E \to E'$ can be written as $\phi(x,y) = (r_1(x), cyr_1'(x) + r_2(x))$. Write

$$r_1(x) = x + \sum_{i \geq 1} \frac{c_n}{x_i}.$$

One can show that $c_1 = \frac{A-A'}{5}$ and $c_2 = \frac{B-B'}{7}$. Then for $n \geq 3$ there is the following recurrence relation

$$c_{n+1} = \frac{3\sum_{i=1}^{n-1} c_n c_{n-i} - (2n-1)(n-1)Ac_{n-1} - (2n-2)(n-2)Bc_{n-2}}{(n-1)(2n-5)}.$$

Note that this recursion works only if $n-1$ and $2n-5$ are non-zero in K for

[1] We say that $\phi : E \to E'$ is *normalized* if $\omega_E = \phi^*\omega_{E'}$, where $\omega_E = \frac{dx}{2y+a_1x+a_3}$ and E is given by the general Weierstrass form $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$.

$n \geq 3$. Now let

$$p_n = \sum_{i=1}^{d} x_{P_i}^n \qquad \text{where } d = \frac{\ell - 1}{2}.$$

Note that $p_0 = d$ and $p_1 = s_1$. Then for $n \geq 1$ we have

$$p_{n+1} = \frac{c_n - (4n-2)Ap_{n-1} - (4n-4)Bp_{n-2}}{4n+2}.$$

If $n = 1$ then the recursion is well-defined since $4n-4 = 0$ in this case. Finally, we can compute s_n for $n \geq 2$ from the following relation:

$$s_n = -\frac{1}{n}\sum_{i=1}^{d}(-1)^i p_i s_{d-i}.$$

Note that in order for the above three recursion to work we need the condition that $\mathrm{char}(K) > \ell + 2$.

Now we show how we can compute s_1, given E and E'. Let $\mathbb{C}/\langle 1, \tau\rangle$ be an elliptic curve. Then there is an isomorphism

$$\mathbb{C}/\langle 1, \tau\rangle \longmapsto \mathbb{C}^\times/q^{\mathbb{Z}} \qquad \text{given by } z \longmapsto q_z := e^{2\pi i z},$$

where $q = e^{2\pi i \tau}$. The isogeny $\mathbb{C}/\langle 1, \tau\rangle \to \mathbb{C}/\langle 1, \ell\tau\rangle$ given by $z \mapsto \ell z$ corresponds to the isogeny $q_z \mapsto q_z^\ell$. Elkies [7, section 3] showed that there is a normalized isogeny from $E_q : y^2 = x^3 + a_4 x + a_6$ to $E'_q : y^2 = x^3 + a'_4 x + a'_6$ over $\mathbb{Z}[[q]]$, where

$$a_4 = -\frac{\lambda^{-2}}{48}E_4(q) \qquad \text{and} \qquad a_6 = \frac{\lambda^{-3}}{864}E_6(q),$$

$$a'_4 = -\frac{\ell^2\lambda^{-2}}{48}E_4(q^\ell) \qquad \text{and} \qquad a'_6 = \frac{\ell^3\lambda^{-3}}{864}E_6(q^\ell)$$

for some non-zero element λ in $\mathbb{Z}[[q]]$. Here $E_4(q)$ and $E_6(q)$ are the Eisenstein series of weight 4 and 6 respectively, given by

$$E_4(q) = 1 + 240\sum_{n=1}^{\infty}\sigma_3(n)q^n \qquad \text{and} \qquad E_6(q) = 1 - 504\sum_{n=1}^{\infty}\sigma_5(n)q^n.$$

Let H be the kernel of this isogeny and let $\psi_H(x) = x^d + \sum_{i=1}^{d-1}(-1)^i s_i(q)x^{d-i}$

be the kernel polynomial of H. Furthermore, Elkies showed that

$$s_1(q) = -\ell\lambda_0^{-1}E_2^{(\ell)}(q),$$

where

$$E_2^{(\ell)}(q) = q\frac{d}{dq}\log\frac{\eta(q^\ell)}{\eta(q)} = \frac{\ell-1}{24} + \sum_{n=1}^{\infty}\sigma_1(n)(q^n - \ell q^{\ell n}).$$

For each $\ell \in \mathcal{L}$, by choosing a suitable $\lambda \in S_2(\Gamma_0(\ell))$ we can write each of a_4, a_6, a_4' and a_6' as a polynomial in u and v. Thus given a K-rational point (u_0, v_0) on $X_0(\ell)_{\mathbb{Q}}$, Elkies' idea is to specialize to a curve over K and then use the recurrence to obtain a kernel polynomial. However, this method works only if $\mathrm{char}(K) > \ell + 2$.

Using this idea, we can compute the generic ℓ-kernel polynomial as follows. Consider the minimal universal elliptic curve $\mathcal{E}(u,v) : y^2 = x^3 + a_4(u,v) + a_6(u,v)$ constructed in section 4.2. Then there is a normalized ℓ-isogeny from $\mathcal{E}(u,v)$ to the curve $\mathcal{E}'(u,v) : y^2 = x^3 + a_4'(u,v) + a_6'(u,v)$, where

$$a_4'(u,v) = \ell^2 a_4(u,-v) \qquad \text{and} \qquad a_6'(u,v) = -\ell^3 a_6(u,-v).$$

Let H be the kernel of this isogeny. Then the kernel polynomial of H is the generic ℓ-kernel polynomial $\Psi_\ell(x,u,v) = x^d + \sum_{i=1}^{d} s_i(u,v)x^{d-i}$. Since $\mathcal{E}(u,v)$ and E_q above are isomorphic, it follows that

$$s_1(u,v) = -12\ell\lambda_0^{-1}E_2^{(\ell)}(q).$$

Note that the function $-12\ell\lambda_0^{-1}E_2^{(\ell)}(q)$ can be written as a polynomial in u and v. See Appendix A for the list of $s_1(u,v)$ for each $\ell \in \mathcal{L}$. It turns out that $s_1(u,v) \in \mathbb{Z}[u]$ for each $\ell \in \mathcal{L}$. Since $s_1(u,v) \in \mathbb{Z}[u] \subseteq \mathbb{Q}(u,v)$ and the characteristic of $\mathbb{Q}(u,v)$ is 0, we can compute the generic kernel polynomial of $\mathcal{E}(u,v)$ from s_1 by using the recurrences formula given by Elkies. Computation of $\Psi_\ell(x,u,v)$ for $\ell \in \mathcal{L}$ by the recurrence formulas using `Sage` takes less than 1 second for $\ell \in \{11, 17, 19, 23, 29, 31, 41\}$. For $\ell = 71$, it takes around only 10 seconds, which is much faster than factorizing the ℓ-division polynomial of $\mathcal{E}(u,v)$.

We also remark that for larger ℓ, this generic kernel polynomial $\Psi_\ell(x,u,v)$

of $\mathcal{E}(u,v)$ is extremely large to write down and store. For example, for $\ell = 71$ the size of $\Psi_\ell(x,u,v)$ is 500KB, and the total size of $\Psi_\ell(x,u,v)$ for $\ell \in \mathcal{L}$ is almost 1MB. An additional advantage of the above method is that s_1 is very small (see Appendix A) and recovering $\Psi_\ell(x,u,v)$ from s_1 is fast (and only needs to be computed once for each ℓ).

5.4 Computing ℓ-isogenies

Let $\ell \in \mathcal{L}$ and assume that $\mathrm{char}(K) \notin \{2,3,\ell\}$. Let E be an elliptic curve over K given by $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$. In this section we show how to compute all K-rational ℓ-isogenies of E up to equivalence, by using the minimal universal elliptic curve $\mathcal{E}(u,v) : y^2 = x^3 + a_4(u,v)x + a_6(u,v)$ where $a_4(u,v)$ and $a_6(u,v)$ are given in Appendix A, and the generic ℓ-kernel polynomial $\Psi_\ell(x,u,v)$ of $\mathcal{E}(u,v)$.

5.4.1 $j(E) \notin \{0, 1728\}$ case

Isogenies from the generic kernel polynomial

Suppose $j(E) \notin \{0,1728\}$. Here we use the similar technique to that of section 4.3. Since $\mathrm{char}(K) \notin \{2,3\}$, we can transform E to

$$E_w : y^2 = x^3 - 27c_4x - 54c_6, \tag{5.8}$$

and c_4, c_6 are non-zero since $j(E) \notin \{0,1728\}$. Let

$$T(u,v) = \frac{a_6(u,v)}{a_4(u,v)} \cdot \frac{-27c_4}{-54c_6} = \frac{a_6(u,v)c_4}{2a_4(u,v)c_6},$$

which we call the *twisting parameter* of $\mathcal{E}(u,v)$ for $j(E) \notin \{0,1728\}$.

For each K-rational point (u_0,v_0) on $X_0(\ell)_{\mathbb{Q}}$ satisfying $j(E) = \alpha_\ell(u) + v\beta_\ell(u)$, it follows from Lemma 4.3.1 that

$$(T(u_0,v_0))^{-\frac{\ell-1}{2}} \cdot \Psi_\ell(xT(u_0,v_0),u_0,v_0)$$

is an ℓ-kernel polynomial of E_w, and from the transformation from E_w to E

given in (2.3) and (2.4) implies that

$$(36T(u_0, v_0))^{-\frac{\ell-1}{2}} \cdot \Psi_\ell((36x + 3b_2)T(u_0, v_0), u_0, v_0)$$

is a K-rational ℓ-kernel polynomial of E. By using Kohel's formula, we obtain K-rational ℓ-isogenies of E from these kernel polynomials.

5.4.2 $j(E) = 0$ case

In this case there are repeated solutions (u, v) on $X_0(\ell)_{\mathbb{Q}}$ satisfying $0 = j(E) = \alpha_\ell(u) + v\beta_\ell(u)$ since the covering map $X_0(\ell) \to X(1)$ ramifies above ρ.

Since $j(E) = 0$, the equation (5.3) becomes $Q_\ell(u) = 0$. For each $\ell \in \mathcal{L}$, by computation we find that $Q_\ell(u)$ is of the following form:

$$Q_\ell(u) = \begin{cases} (u - u_e)^2 h_{0,\ell}^3(u) & \text{if } \ell \equiv 1 \pmod 3, \\ h_{0,\ell}^3(u) & \text{if } \ell \equiv 2 \pmod 3, \end{cases}$$

where $h_{0,\ell}(u) \in \mathbb{Z}[u]$. The pairs $(u_e, \pm v_e)$ where $v_e^2 = f_\ell(u_e)$ correspond to two inequivalent degree ℓ endomorphisms, and the points (u, v) on $X_0(\ell)_{\mathbb{Q}}$ satisfying $h_{0,\ell}(u) = 0$ correspond to isogenies of degree ℓ that are non-endomorphisms.

Endomorphisms

For each $\ell \in \mathcal{L}$, the elliptic curve $\mathcal{E}(u_e, \pm v_e)$ is singular. Thus in this case we cannot use the generic ℓ-kernel polynomial $\Psi_\ell(x, u, v)$. Hence as in section 4.3.2, we compute the kernel polynomials of the endomorphisms separately as follows.

Let $\mathcal{E}_0(z) : y^2 = x^3 + z$ be the elliptic curve defined over $\mathbb{Q}(z)$. If $\ell \equiv 1 \pmod 3$ then the ℓ-division polynomial of $\mathcal{E}_0(z)$ has precisely two irreducible degree $\frac{\ell-1}{2}$ factors in $\mathbb{Q}(\sqrt{-3})(z)[x]$, and they are complex conjugates of each other. We denote these two polynomials by $\Psi_{\ell,0}(x, z)$ and $\overline{\Psi}_{\ell,0}(x, z)$. By substituting $z = -54c_6$, we obtain kernel polynomials of the two inequivalent

degree ℓ endomorphisms of E, given by

$$36^{-d} \cdot \Psi_{\ell,0}((36x + 3b_2), -54c_6),$$
$$36^{-d} \cdot \overline{\Psi}_{\ell,0}((36x + 3b_2), -54c_6).$$

Non-endomorphisms

We first find all K-rational points (u, v) on $X_0(\ell)_{\mathbb{Q}}$ satisfying $0 = j(E) = \alpha_\ell(u) + v\beta_\ell(u)$. For each root $u_0 \in K$ of $h_{0,\ell}(u) = 0$, if $\beta_\ell(u_0) \neq 0$, then we obtain $v = -\frac{\alpha_\ell(u_0)}{\beta_\ell(u_0)}$. If $\beta_\ell(u_0) = 0$, then we obtain at most two values of v by solving $v^2 = f_\ell(u_0)$ over K.

Since $j(E) = 0$, we have $c_4 = 0$ and $c_6 \neq 0$. Thus as in (4.1) E can be transformed to

$$E_w : y^2 = x^3 - 54c_6.$$

Let

$$T(u, v) = \frac{a_6(u, v)}{-54c_6}.$$

We call $T(u, v)$ the twisting parameter of $\mathcal{E}(u, v)$ for $j(E) = 0$.

Let (u_0, v_0) be a K-rational point on $X_0(\ell)_{\mathbb{Q}}$ satisfying $0 = j(E) = \alpha_\ell(u) + v\beta_\ell(u)$. Let $U \in K$ be such that $U^3 = T(u_0, v_0)$. Then it follows from Lemma 4.3.2 that

$$(36U)^{-\frac{\ell-1}{2}} \cdot \Psi_\ell((36x + 3b_2)U, u_0, v_0)$$

is a K-rational ℓ-kernel polynomial of E.

Note that there are up to 3 distinct values of U, each giving a distinct kernel polynomial. These three kernel polynomials correspond to one orbit under the action of $\mathrm{Aut}(E)$. For each kernel polynomial, we can compute a K-rational ℓ-isogeny ϕ of E using Kohel's formula given in section 2.2.3.

5.4.3 $j(E) = 1728$ case

In this case there are repeated solutions (u, v) on $X_0(\ell)_{\mathbb{Q}}$ satisfying $1728 = j(E) = \alpha_\ell(u) + v\beta_\ell(u)$ since the covering map $X_0(\ell) \to X(1)$ ramifies above i.

Since $j(E) = 1728$, the equation (5.3) becomes $Q'_\ell(u) := 1728^2 -$

$1728P_\ell(u) + Q_\ell(u) = 0$. For each $\ell \in \mathcal{L}$, by computation we find that $Q'_\ell(u)$ is of the following form:

$$Q'_\ell(u) = \begin{cases} (u-u_e)^2 h^2_{1728,\ell}(u) & \text{if } \ell \equiv 1 \pmod 4, \\ h^2_{1728,\ell}(u) & \text{if } \ell \equiv 3 \pmod 4, \end{cases}$$

where $h_{1728,\ell}(u) \in \mathbb{Z}[u]$. The pairs $(u_e, \pm v_e)$ where $v_e^2 = f_\ell(u_e)$ correspond to two inequivalent degree ℓ endomorphisms, and the points (u, v) on $X_0(\ell)_{\mathbb{Q}}$ satisfying $h_{1728,\ell}(u) = 0$ correspond to isogenies of degree ℓ that are non-endomorphisms.

Endomorphisms

For each $\ell \in \mathcal{L}$, the elliptic curve $\mathcal{E}(u_e, \pm v_e)$ is singular. Thus in this case we cannot use the generic ℓ-kernel polynomial $\Psi_\ell(x, u, v)$. Hence as in section 4.3.3, we will compute the kernel polynomials of the endomorphisms separately as follows.

Let $\mathcal{E}_{1728}(z) : y^2 = x^3 + zx$ be the elliptic curve defined over $\mathbb{Q}(z)$. If $\ell \equiv 1 \pmod 4$ then the ℓ-division polynomial of $\mathcal{E}_{1728}$ has precisely two irreducible degree $\frac{\ell-1}{2}$ factors in $\mathbb{Q}(i)(z)[x]$, and they are complex conjugates of each other. We denote these two polynomials by $\Psi_{\ell,1728}(x, z)$ and $\overline{\Psi}_{\ell,1728}(x, z)$. By substituting $z = -27c_4$ and from (2.4), we obtain kernel polynomials of the two inequivalent degree ℓ endomorphisms of E, given by

$$36^{-d} \cdot \Psi_{\ell,1728}((36x + 3b_2), -27c_4),$$
$$36^{-d} \cdot \overline{\Psi}_{\ell,1728}((36x + 3b_2), -27c_4).$$

Non-endomorphisms

We first find all K-rational points (u, v) on $X_0(\ell)_{\mathbb{Q}}$ satisfying $1728 = j(E) = \alpha_\ell(u) + v\beta_\ell(u)$. For each root $u_0 \in K$ of $h_{1728,\ell}(u) = 0$, if $\beta_\ell(u_0) \neq 0$, then we obtain $v = \frac{1728-\alpha_\ell(u_0)}{\beta_\ell(u_0)}$. If $\beta_\ell(u_0) = 0$, then we obtain at most two values of v by solving $v^2 = f_\ell(u_0)$ over K.

Since $j(E) = 1728$, we have $c_4 \neq 0$ and $c_6 = 0$. Thus as in (4.1) E can be transformed to

$$E_w : y^2 = x^3 - 27c_4 x.$$

Let

$$T(u,v) = \frac{a_4(u,v)}{-27c_4}.$$

We call $T(u,v)$ the twisting parameter of $\mathcal{E}(u,v)$ for $j(E) = 1728$.

Let (u_0, v_0) be a K-rational point on $X_0(\ell)_{\mathbb{Q}}$ satisfying $1728 = j(E) = \alpha_\ell(u) + v\beta_\ell(u)$. Let $U \in K$ be such that $U^2 = T(u_0, v_0)$. Then it follows from Lemma 4.3.3 that

$$(36U)^{-\frac{\ell-1}{2}} \cdot \Psi_\ell((36x + 3b_2)U, u_0, v_0)$$

is a K-rational ℓ-kernel polynomial of E.

Note that there are up to 2 distinct values of U, each giving a distinct kernel polynomial. These two kernel polynomials correspond to one orbit under the action of $\mathrm{Aut}(E)$. For each kernel polynomial, we can compute a K-rational ℓ-isogeny ϕ of E using Kohel's formula given in section 2.2.3.

5.4.4 Algorithm

Let $\ell \in \mathcal{L}$. Let K be a field such that $\mathrm{char}(K) \notin \{2, 3, \ell\}$. Let E be an elliptic curve over K given by

$$E: \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Let $\mathcal{E}(u,v)$ be the minimal universal elliptic curve

$$\mathcal{E}(u,v) : y^2 = x^3 + a_4(u,v)x + a_6(u,v)$$

given in Appendix A and $\Psi_\ell(x,u,v)$ be the generic kernel polynomial of $\mathcal{E}(u,v)$. Let $\Psi_{\ell,0}(x,z)$ and $\Psi_{\ell,1728}(x,z)$ be the polynomials mentioned in section 5.4.2 and 5.4.3 respectively, and let $\overline{\Psi}_{\ell,0}(x,z)$ and $\overline{\Psi}_{\ell,1728}(x,z)$ be complex conjugates of $\Psi_{\ell,0}(x,z)$ and $\Psi_{\ell,1728}(x,z)$ in Appendix A respectively.

We present three algorithms which compute all K-rational ℓ-isogenies of E up to equivalence for the cases $j \notin \{0, 1728\}$, $j = 0$, $j = 1728$ as Algorithm 5, 6 and 7.

Algorithm 5 `isogenies_prime_degree_genus_plus_0`(E, ℓ)

Input: E, ℓ

Output: A set of K-rational ℓ-isogenies of E

Compute $j(E)$
if $j(E) = 0$ **then**
  return `isogenies_prime_degree_genus_plus_0_j0`(E, ℓ)
else if $j(E) = 1728$ **then**
  return `isogenies_prime_degree_genus_plus_0_j1728`(E, ℓ)
else if $j(E) \notin \{0, 1728\}$ **then**
  Let $R_u = \{u_0 \in K \mid j(E)^2 - P_\ell(u_0)j(E) + Q_\ell(u_0) = 0\}$
  Set $R_{u,v} = \emptyset$
  for u_0 in R_u **do**
    if $\beta_\ell(u_0) = 0$ **then**
      Append $(u_0, \pm v_0)$ such that $v_0^2 = f_\ell(u_0)$ and $v_0 \in K$ to $R_{u,v}$
    else
      Append (u_0, v_0) where $v_0 = \frac{j(E) - \alpha_\ell(u_0)}{\beta_\ell(u_0)}$ to $R_{u,v}$
    end if
  end for
  Compute c_4, c_6, b_2 of E
  Let $T(u, v) = \frac{a_6(u,v)c_4}{2a_4(u,v)c_6}$
  Set $\mathcal{K} = \{(36T(u_0, v_0))^{-\frac{\ell-1}{2}} \cdot \Psi_\ell((36x + 3b_2)T(u_0, v_0), u_0, v_0) \mid (u_0, v_0) \in R_{u,v}\}$
  Set $\mathcal{I} = \emptyset$
  for f in $\mathcal{K}$ **do**
    Compute the isogeny ϕ of E from f `//using Kohel's formula`
    Append ϕ to $\mathcal{I}$
  end for
  return $\mathcal{I}$
end if

Algorithm 6 `isogenies_prime_degree_genus_plus_0_j0`(E, ℓ)

Input: E with $j(E) = 0$, ℓ
Output: A set of K-rational ℓ-isogenies of E

Compute $R_u = \{u_0 \in K \mid h_{0,\ell}(u_0) = 0\}$
Compute c_6, b_2 of E
Set $\mathcal{K} = \emptyset$
`// For endomorphisms:`
if $\ell \equiv 1 \pmod 3$ **and** -3 is a square in K **then**
    Append $36^{-\frac{\ell-1}{2}} \cdot \Psi_{\ell,0}((36x+3b_2), -54c_6)$, $36^{-\frac{\ell-1}{2}} \cdot \overline{\Psi}_{\ell,0}((36x+3b_2), -54c_6)$ to $\mathcal{K}$
end if
`// For non-endomorphisms:`
Set $R_{u,v} = \emptyset$
for u_0 in R_u **do**
    if $\beta_\ell(u_0) = 0$ **then**
        Append $(u_0, \pm v_0)$ such that $v_0^2 = f_\ell(u_0)$ and $v_0 \in K$ to $R_{u,v}$
    else
        Append (u_0, v_0) where $v_0 = \frac{-\alpha_\ell(u_0)}{\beta_\ell(u_0)}$ to $R_{u,v}$
    end if
end for
for (u_0, v_0) in $R_{u,v}$ **do**
    for $U \in K$ such that $U^3 = \frac{a_6(u_0,v_0)}{-54c_6}$ **do**
        Append $(36U)^{-\frac{\ell-1}{2}} \cdot \Psi_\ell((36x + 3b_2)U, u_0, v_0)$ to $\mathcal{K}$
    end for
end for
Set $\mathcal{I} = \emptyset$
for f in $\mathcal{K}$ **do**
    Compute the isogeny ϕ of E from f `//using Kohel's formula`
    Append ϕ to $\mathcal{K}$
end for
return $\mathcal{I}$

Algorithm 7 `isogenies_prime_degree_genus_plus_0_j1728`(E, ℓ)

Input: E with $j(E) = 1728$, ℓ

Output: A set of K-rational ℓ-isogenies of E

Compute $R_u = \{u_0 \in K \mid h_{1728,\ell}(u_0) = 0\}$
Compute c_4, b_2 of E
Set $\mathcal{K} = \emptyset$
`// For endomorphisms:`
if $\ell \equiv 1 \pmod 4$ **and** -1 is a square in K **then**
    Append $36^{-\frac{\ell-1}{2}} \cdot \Psi_{\ell,1728}((36x + 3b_2), -27c_4)$, $36^{-\frac{\ell-1}{2}} \cdot \overline{\Psi}_{\ell,1728}((36x + 3b_2), -27c_4)$ to $\mathcal{K}$
end if
`// For non-endomorphisms:`
Set $R_{u,v} = \emptyset$
for u_0 in R_u **do**
    if $\beta_\ell(u_0) = 0$ **then**
        Append $(u_0, \pm v_0)$ such that $v_0^2 = f_\ell(u_0)$ and $v_0 \in K$ to $R_{u,v}$
    else
        Append (u_0, v_0) where $v_0 = \frac{1728 - \alpha_\ell(u_0)}{\beta_\ell(u_0)}$ to $R_{u,v}$
    end if
end for
for (u_0, v_0) in $R_{u,v}$ **do**
    for $U \in K$ such that $U^2 = \frac{a_4(u_0,v_0)}{-27c_4}$ **do**
        Append $(36U)^{-\frac{\ell-1}{2}} \cdot \Psi_\ell((36x + 3b_2)U, u_0, v_0)$ to $\mathcal{K}$
    end for
end for
Set $\mathcal{I} = \emptyset$
for f in $\mathcal{K}$ **do**
    Compute the isogeny ϕ of E from f `//using Kohel's formula`
    Append ϕ to $\mathcal{I}$
end for
return $\mathcal{I}$

5.5 Examples

In this section we illustrate some examples that use Algorithm 5, 6 and 7.

Example 5.5.1. Let

$$E:\ y^2+xy+y=x^3+x^2-30x-76 \quad \text{over } \mathbb{Q}.$$

with $j(E)=-11\cdot 131^3$. We will compute all $\mathbb{Q}$-rational 11-isogenies of E up to equivalence. We find that the only root of the equation $j(E)^2-P_{11}(u)j(E)+Q_{11}(u)=0$ over $\mathbb{Q}$ is $u=-2$. Since $\beta_{11}(-2)=-1124040\neq 0$, we obtain $v=\frac{j(E)-\alpha_{11}(-2)}{\beta_{11}(-2)}=11$. Thus the pair $(u_0,v_0)=(-2,11)$ parametrizes the unique $\mathbb{Q}$-rational 11-isogeny of E up to equivalence. We compute c_4, c_6 and b_2 of E:

$$c_4=1441, \qquad c_6=54703, \qquad b_2=5.$$

Let $\mathcal{E}(u,v): y^2=x^3+a_4(u,v)x+a_6(u,v)$ be the universal elliptic curve where $a_4(u,v)$ and $a_6(u,v)$ are given by

$$\begin{aligned} a_4(u,v) &= -3(61u^2-246u+45+60v),\\ a_6(u,v) &= -2(-7(95u^3-819u^2+189u+135)-18v(37u-51)). \end{aligned}$$

The generic 11-kernel polynomial of $\mathcal{E}(u,v)$ is given by

$$\begin{aligned} &\Psi_{11}(x,u,v)=x^5+(-55u+33)x^4+(216v+994u^2+276u+162)x^3\\ &+[(-4536u-4536)v-8774u^3-7794u^2+38718u-16470]x^2\\ &+[(31752u^2+73872u-185976)v+41453u^4+4452u^3-610578u^2\\ &+580068u+7533]x+[(-842616u^3-2745576u^2+14143896u\\ &-12389112)v-928945u^5+1319331u^4+33434694u^3\\ &-67821354u^2-20437029u+19964151]/11, \end{aligned}$$

and the twisting parameter is given by $T(u,v)=\frac{a_6(u,v)c_4}{2a_4(u,v)c_6}$.

Thus an 11-kernel polynomial of E is given by

$$\begin{aligned} &(36T(u_0,v_0))^{-5}\cdot\Psi_{11}((36x+3b_2)T(u_0,v_0),u_0,v_0)\\ &=x^5+14x^4+63x^3+62x^2-230x-439. \end{aligned}$$

Using Kohel's formula we obtain an 11-isogeny from E to the curve

$$E' : \ y^2 + xy + y = x^3 + x^2 - 305x + 7888 \qquad \text{with } j(E') = -121.$$

This is the only $\mathbb{Q}$-rational 11-isogeny of E up to equivalence. Here we omit the rational functions for the isogenies since they are too long to list.

Example 5.5.2. Let

$$E : \ y^2 = x^3 + x + 4 \quad \text{over } \mathbb{F}_{13}.$$

with $j(E) = 5$. We will compute all $\mathbb{F}_{13}$-rational 71-isogenies of E up to equivalence. Note that this is an example where the method of Bostan et al. [1] cannot be applied since the characteristic of the field is smaller than the degree of isogenies. The roots of the equation $j(E)^2 - P_{71}(u)j(E) + Q_{71}(u) = 0$ over $\mathbb{F}_{13}$ are $u_1 = 5$ and $u_2 = 8$. Since $\beta_{71}(5) = 1 \neq 0$ and $\alpha_{71}(5) = 5$, we obtain $v_1 := \frac{j(E) - \alpha_{71}(5)}{\beta_{71}(5)} = 0$. Similarly, since $\beta_{71}(8) = 1 \neq 0$ and $\alpha_{71}(8) = 5$, we obtain $v_2 := \frac{j(E) - \alpha_{71}(8)}{\beta_{71}(8)} = 0$. Thus $(u_1, v_1) = (5, 0)$ and $(u_2, v_2) = (8, 0)$ parametrize $\mathbb{F}_{13}$-rational 71-isogenies of E up to equivalence. We compute c_4, c_6 and b_2 of E:

$$c_4 = 4, \qquad c_6 = 2, \qquad b_2 = 0.$$

Let $\mathcal{E}(u, v) : y^2 = x^3 + a_4(u, v)x + a_6(u, v)$ be the universal elliptic curve where $a_4(u, v)$ and $a_6(u, v)$ are given in Appendix A. Let $T(u, v) = \frac{a_6(u,v)c_4}{2a_4(u,v)c_6}$ and let $\Psi_{71}(x, u, v)$ be the generic 71-kernel polynomial of $\mathcal{E}(u, v)$.

By using $\Psi_{71}(x, u, v)$ and $T(u, v)$, we obtain the following two 71-kernel polynomials of E:

$$\begin{aligned} & x^{35} + 8x^{34} + 7x^{33} + 4x^{32} + 2x^{31} + 12x^{30} + 6x^{29} + 2x^{28} + 5x^{27} + 5x^{26} \\ & \quad + 6x^{25} + 4x^{24} + 10x^{23} + 9x^{22} + 9x^{21} + 10x^{20} + 10x^{19} + x^{18} + x^{17} \\ & \quad + 12x^{16} + 2x^{15} + 5x^{14} + 3x^{13} + 7x^{12} + 7x^{11} + 3x^{10} + 8x^9 + 6x^8 \\ & \quad + 10x^7 + 2x^6 + 10x^5 + 5x^4 + 2x^3 + 11x + 1 \end{aligned}$$

and

$$x^{35} + x^{34} + 8x^{33} + 9x^{32} + 8x^{31} + x^{30} + 8x^{29} + 10x^{28} + x^{27} + 7x^{26} + 10x^{25} \\ + 9x^{24} + 7x^{23} + 3x^{22} + 5x^{21} + 12x^{20} + 9x^{19} + 5x^{17} + 7x^{16} + 7x^{15} + 7x^{14} \\ + 2x^{12} + x^{10} + 5x^8 + 8x^7 + 4x^6 + 3x^5 + 11x^4 + 11x^3 + 11x^2 + 2x + 5.$$

By Kohel's formula we obtain two 71-isogenies from E, both to the curve

$$E' : \ y^2 = x^3 + 10x + 7 \qquad \text{with } j(E') = 5.$$

Note that although $j(E) = j'(E)$, E is not isomorphic to E' over $\mathbb{F}_{13}$. These two are all the $\mathbb{F}_{13}$-rational 71-isogenies of E up to equivalence. Here we again omit the rational functions for the isogenies since they are too long to list.

5.6 Characteristic 2 and 3 case

5.6.1 Ordinary curves in characteristic 3

In this section we use the similar technique as that of section 4.5.1. The only minor difference to section 4.5.1 is that here we use $\mathcal{E}(u, v)$ for the universal elliptic curve instead of $\mathcal{E}(t)$, and all the argument works as in section 4.5.1. Let K be a field of characteristic 3, and let E be an ordinary elliptic curve over K. If E is given in the Weierstrass form (2.2), then E can be transformed to

$$y^2 = x^3 + b_2x^2 + \frac{-b_2^2b_4^2 + b_2^3b_6 + b_4^3}{b_2^3}. \tag{5.9}$$

Let $\ell \in \mathcal{L}$. Recall the universal elliptic curve

$$y^2 = x^3 - jx^2 + j^2 \qquad \text{where } j = \alpha_\ell(u) + v\beta_\ell(u). \tag{5.10}$$

Moreover, recall from (5.5) that the j-function j is of the form

$$j = c\frac{e_0h_0^3}{h_\infty^d},$$

where d is the denominator of $\frac{\ell+1}{12}$. Thus we can twist the curve (5.10) by $\frac{h_\infty^d}{h_0^2}$ to obtain the simplified universal elliptic curve

$$\mathcal{E}(u,v)_{char3}:\ y^2 = x^3 + a_2(u,v)x^2 + a_6(u,v),$$

where

$$a_2(u,v) = -ce_0h_0 \qquad \text{and} \qquad a_6(u,v) = c^2e_0^2h_\infty^d.$$

Note that $\mathcal{E}(u,v)_{char3}$ can be obtained from the minimal universal elliptic curve $\mathcal{E}(u,v)$ in section 5.4.4 by a sequence of transformations as follows. We first twist $\mathcal{E}(u,v)$ by $\frac{ch_0h_{1728}}{h_\infty^d}$ to obtain the curve $E_j : y^2 = x^3 - 3jkx - 2jk^2$, which follows from section 5.2. Further, we saw in section 2.1 that E_j can be transformed to the curve (2.7), and reducing (2.7) yields the curve (5.10). Finally, twisting (5.10) yields the curve $\mathcal{E}(u,v)_{char3}$ above.

Now recall the generic ℓ-kernel polynomial $\Psi_\ell(x,u,v)$ of $\mathcal{E}(u,v)$. Applying the above transformations to $\Psi_\ell(x,u,v)$ yields a kernel polynomial of $\mathcal{E}(u,v)_{char3}$, say $\Psi_{\ell,char3}(x,u,v)$. We refer to $\Psi_{\ell,char3}(x,u,v)$ as the generic ℓ-kernel polynomial of $\mathcal{E}(u,v)_{char3}$. As in section 4.5.1, we will compute all K-rational ℓ-isogenies of E up to equivalence using $\Psi_{\ell,char3}(x,u,v)$ as follows.

Computing ℓ-isogenies

Let $\ell \in \mathcal{L}$ and let E be an ordinary elliptic curve over K. The equation of the modular curve $X_0(\ell)_{\mathbb{Q}} : v^2 = f_\ell(u)$ can be reduced modulo 3 to obtain the curve

$$X_0(\ell)_{\mathbb{F}_3}:\ v^2 = f_\ell(u), \qquad \text{where } f_\ell(u) \in \mathbb{F}_3(u).$$

We first find all K-rational points (u,v) on $X_0(\ell)_{\mathbb{F}_3}$ satisfying $j(E) = \alpha_\ell(u) + v\beta_\ell(u)$. For each root $u_0 \in K$ of the quadratic equation

$$j(E)^2 - P_\ell(u)j(E) + Q_\ell(u) = 0,$$

if $\beta_\ell(u_0) \neq 0$ then we obtain unique $v = \frac{j(E)-\alpha_\ell(u_0))}{\beta_\ell(u_0)} \in K$. If $\beta_\ell(u_0) = 0$ then we obtain at most two values of v in K by solving $v^2 = f_\ell(u_0)$.

Now let

$$T(u,v) = \frac{a_2(u,v)}{b_2},$$

which we call the twisting parameter of $\mathcal{E}(u,v)$. As in section 4.5.1, we have the following lemma.

Lemma 5.6.1. *Let (u_0, v_0) be a K-rational point on $X_0(\ell)_{\mathbb{F}_3}$ satisfying $j(E) = \alpha_\ell(u) + v\beta_\ell(u)$. Then*

$$T(u_0,v_0)^{-\frac{\ell-1}{2}} \cdot \Psi_{\ell,char3}\left(\left(x - \frac{b_4}{b_2}\right)T(u_0,v_0), u_0, v_0\right)$$

is a K-rational ℓ-kernel polynomial of E.

Proof. It follows from the proof of 4.5.1. □

Once we obtain an ℓ-kernel polynomial by Lemma 4.3.1, we can compute a K-rational ℓ-isogeny of E from the kernel polynomial by using Kohel's formula given in section 2.2.3. We give the following example for $\ell = 11$.

Example 5.6.2. For $\ell = 11$, recall from section 5.2 that the j-function j can be written as

$$j = c\frac{e_0 h_0^3}{h_\infty^d},$$

where

$$c = 2, \qquad e_0 = 1, \qquad h_0 = 61u^2 - 246u + 45 + 60v,$$
$$h_\infty = u^5 - 37u^4 + 459u^3 - 2087u^2 + 2040u + (-u^3 + 29u^2 - 258u + 680)v.$$

Thus we can construct the universal elliptic curve

$$\mathcal{E}(u,v)_{char3} : \ y^2 = x^3 + a_2(u,v)x^2 + a_6(u,v),$$

where

$$a_2(u,v) = -ce_0h_0 = u^2,$$
$$a_6(u,v) = c^2e_0^2h_\infty^d = u^5 - u^4 + u^2 - (u^3 + u^2 + 1)v.$$

The generic 11-kernel polynomial $\Psi_{11,char3}(x,u,v)$ of $\mathcal{E}(u,v)_{char3}$ is given by

$$\begin{aligned}\Psi_{11,char3}(x,u,v) &= x^5 + (2v+u^2)x^4 + (u^2v + (2u^4+2u^3+u^2+2))x^3 \\ &+ ((u^4+2u^3+2u^2+2)v + (2u^6+2u^3))x^2 \\ &+ ((u^6+u^4+u^3+2u^2)v + (2u^8+2u^7+u^3+u^2+2))x \\ &+ (2u^8+2u^7+2u^6+2u^5+u^4+2u^3+1)v + u^{10}+2u^9 \\ &+ u^8+2u^7+u^6+u^5+u^3+u^2.\end{aligned}$$

Now we use $\Psi_{11,char3}(x,u,v)$ to compute all $\mathbb{F}_3$-rational 11-isogenies up to equivalence of the curve

$$E:\ y^2 = x^3+x^2-1 \qquad \text{over } \mathbb{F}_3$$

with $j(E)=1$. We first find all K-rational points (u,v) on $X_0(\ell)_{\mathbb{F}_3}$ satisfying $j(E) = \alpha_\ell(u) + v\beta_\ell(u)$. We find that the only root of the equation $j(E)^2 - P_{11}(u)j(E) + Q_{11}(u) = 0$ over $\mathbb{F}_3$ is $u_0 = -1$. Since $\beta_{11}(u_0) = -1 \neq 0$, we obtain $v_0 := \frac{j(E)-\alpha_{11}(-1)}{\beta_{11}(-1)} = 0$. Thus $(-1,0)$ parametrizes the unique $\mathbb{F}_3$-rational 11-isogeny of E up to equivalence.

The twisting parameter of $\mathcal{E}(u,v)$ is given by

$$T(u,v) = \frac{a_2(u,v)}{b_2} = \frac{u^2}{1} = u^2.$$

Since we compute that $b_4 = 0$, the polynomial

$$T(u_0,v_0)^{-5}\cdot\Psi_{11,char3}\left(\left(x-\frac{b_4}{b_2}\right)T(u_0,v_0),u_0,v_0\right) = x^5+x^4-x+1$$

is an 11-kernel polynomial of E. By using Kohel's formula and post-composing appropriate isomorphism, we obtain an $\mathbb{F}_3$-rational degree 11 endomorphism of E given by $(x,y)\mapsto(r_1(x),-yr_1'(x))$, where

$$r_1(x) = \frac{x^{11}-x^9+x^8+x^7-x^6+x^4+x^3-x^2-1}{(x^5+x^4-x+1)^2}.$$

This is the only $\mathbb{F}_3$-rational 11-isogeny of E up to equivalence.

5.6.2 Ordinary curves in characteristic 2

Recall that the equation of the modular curve $X_0(\ell)_{\mathbb{Q}}$ is given by

$$X_0(\ell)_{\mathbb{Q}} : \ v^2 = f_\ell(u), \qquad \text{where } f_\ell(u) \in \mathbb{Z}[u]. \tag{5.11}$$

However, for each $\ell \in \mathcal{L}$ this hyperelliptic curve becomes singular in characteristic 2, and the j-function j is given by $j = \alpha_\ell(u) + v\beta_\ell(u) \in \frac{1}{2}\mathbb{Z}[u, v]$, so we cannot reduce it modulo 2. We can solve this problem by changing the equation of $X_0(\ell)_{\mathbb{Q}}$ as follows.

By computation we find that the polynomial $f_\ell(u)$ is a square modulo 4 for each $\ell \in \mathcal{L}$. Let $H_\ell(u) \in \mathbb{Z}[u]$ be such that $H_\ell^2(u) \equiv f_\ell(u) \pmod 4$. Moreover, let $F_\ell(u) = \frac{f_\ell(u) - H_\ell^2(u)}{4} \in \mathbb{Z}[u]$. Then the hyperelliptic curve

$$v^2 + H_\ell(u)v = F_\ell(u) \tag{5.12}$$

is non-singular in characteristic 2 and thus we can reduce it modulo 2 to obtain the equation of the modular curve $X_0(\ell)_{\mathbb{F}_2}$. The curve (5.12) is isomorphic to (5.11) over $\mathbb{Q}$ via the isomorphism

$$u \longmapsto u \qquad \text{and} \qquad v \longmapsto 2v + H_\ell(u), \tag{5.13}$$

and the hyperelliptic involution is given by

$$(u, v) \longmapsto (u, -v - H_\ell(u)).$$

Hence the j-function j and the function j_ℓ where $j_\ell(\tau) = j(\ell\tau)$ can be written as

$$\begin{aligned} j &= \tilde{\alpha}_\ell(u) + v\tilde{\beta}_\ell(u), \\ j_\ell &= \tilde{\alpha}_\ell(u) + (-v - H_\ell(u))\tilde{\beta}_\ell(u), \end{aligned}$$

where $\tilde{\alpha}_\ell(u) = \alpha_\ell(u) + H_\ell(u)\beta_\ell(u)$ and $\tilde{\beta}_\ell(u) = 2\beta_\ell(u)$ with $\tilde{\alpha}_\ell(u), \tilde{\beta}_\ell(u) \in \mathbb{Z}[u]$. Note that j still satisfies the quadratic equation (5.3) given by $j^2 - P_\ell(u)j + Q_\ell(u) = 0$ where $P_\ell(u), Q_\ell(u) \in \mathbb{Z}[u]$, since the above isomorphism does not change u.

Thus given an ordinary elliptic curve E over a field K of characteristic 2, we first find the roots of $j(E)^2 - P_\ell(u)j(E) + Q_\ell(u) = 0$ in K. For each root $u_0 \in K$, if $\tilde{\beta}_\ell(u_0) \neq 0$ then we obtain the unique $v = \frac{j(E)-\tilde{\alpha}_\ell(u_0)}{\tilde{\beta}_\ell(u)} \in K$. If $\tilde{\beta}_\ell(u_0) = 0$ then we obtain at most two values of v in K from (5.12).

Let $\mathcal{E}(u, v)$ be the universal elliptic curve over $\mathbb{F}_2(u, v)$ given by

$$\mathcal{E}(u,v)_{char2} : y^2 + xy = x^3 + \frac{1}{j} \qquad \text{where } j = \tilde{\alpha}_\ell(u) + v\tilde{\beta}_\ell(u).$$

Note that $\mathcal{E}(u, v)_{char2}$ can be obtained from the minimal universal elliptic curve $\mathcal{E}(u, v)$ in section 5.4.4 by a sequence of transformations as follows. Since here we are using the modular curve equation (5.12), we first apply the transformation (5.13) to $\mathcal{E}(u, v)$. From section 5.2 it follows that twisting $\mathcal{E}(u, v)$ by $\frac{ch_0h_{1728}}{h_\infty^d}$ gives the curve $E_j : y^2 = x^3 - 3jkx - 2jk^2$. In section 2.1 we saw that E_j can be transformed to the curve (2.8), and reducing (2.8) yields $\mathcal{E}(u, v)_{char2}$.

Now recall the generic ℓ-kernel polynomial $\Psi_\ell(x, u, v)$ of $\mathcal{E}(u, v)$. Applying the above transformations to $\Psi_\ell(x, u, v)$ yields a kernel polynomial of $\mathcal{E}(u, v)_{char2}$, say $\Psi_{\ell,char2}(x, u, v)$. We refer to $\Psi_{\ell,char2}(x, u, v)$ as the generic ℓ-kernel polynomial of $\mathcal{E}(u, v)_{char2}$. Then from section 4.5.2 it follows that for each K-rational point (u_0, v_0) on $X_0(\ell)_{\mathbb{F}_2}$ satisfying $j(E) = \tilde{\alpha}_\ell(u) + v\tilde{\beta}_\ell(u)$, the polynomial

$$a_1^{\ell-1} \cdot \Psi_{\ell,char2}\left(\frac{1}{a_1^2}\left(x + \frac{a_3}{a_1}\right), u_0, v_0\right)$$

is a K-rational ℓ-kernel polynomial of E. We give the following example for $\ell = 11$.

Example 5.6.3. For $\ell = 11$ we may take

$$H_{11}(u) = u^2 + 1 \qquad \text{and} \qquad F_{11}(u) = -4u^3 + 3u - 2.$$

Now we work in characteristic 2. The equation of the modular curve $X_0(11)_{\mathbb{F}_2}$ is given by

$$X_0(11)_{\mathbb{F}_2} : \; v^2 + (u^2 + 1)v = u. \tag{5.14}$$

The j-function j can be written as $j = \tilde{\alpha}_{11}(u) + v\tilde{\beta}_{11}(u)$, where $\tilde{\alpha}_{11}(u) = (u+1)^6(u^5+u^4+u^3+u+1)$ and $\tilde{\beta}_{11}(u) = u^2(u+1)^7$. Moreover, j satisfies the

quadratic equation $j^2 - P_{11}(u)j + Q_{11}(u) = 0$, where $P_{11}(u) = u^2(u+1)^9$ and $Q_{11}(u) = (u+1)^{12}$. Note that if E is ordinary, $j(E) \neq 0$ and thus $u + 1 \neq 0$.

Let $\mathcal{E}(u,v)_{char2}$ be the universal elliptic curve given by

$$\mathcal{E}(u,v)_{char2} : y^2 + xy = x^3 + \frac{1}{j} \qquad \text{where } j = \tilde{\alpha}_{11}(u) + v\tilde{\beta}_{11}(u).$$

The generic 11-kernel polynomial of $\mathcal{E}(u,v)$ is given by

$$\begin{aligned}\Psi_{11,char2}(x,u,v) = x^5 &+ \frac{v+u}{(u+1)^2}x^4 + \frac{v}{(u+1)^2}x^3 + \frac{uv+1}{(u+1)^4}x^2 \\ &+ \frac{u^3(u+1)v + u^3 + u^2 + u}{(u+1)^6}x \\ &+ \frac{(u^6+u^5+u^4+u^3+u)v + u^5 + u^4 + u^2 + u + 1}{(u+1)^8}.\end{aligned}$$

Now we compute all $\mathbb{F}_2$-rational 11-isogenies up to equivalence of the elliptic curve E given by

$$E : \ y^2 + xy = x^3 + 1 \qquad \text{over } \mathbb{F}_2$$

with $j(E) = 1$. The only root of the quadratic equation $j(E)^2 - P_{11}(u)j(E) + Q_{11}(u) = 0$ over $\mathbb{F}_2$ is $u_0 = 0$. Since $\tilde{\beta}_{11}(u_0) = 0$, from (5.14) we obtain $v = 0$ and $v = 1$. Thus $(0,0)$ and $(0,1)$ parametrize $\mathbb{F}_3$-rational 11-isogenies of E up to equivalence.

Since $a_1 = 1$ and $a_3 = 0$, the polynomials

$$\begin{aligned}a_1^{10} \cdot \Psi_{\ell,char2}\left(\frac{1}{a_1^2}\left(x + \frac{a_3}{a_1}\right), 0, 0\right) &= x^5 + x^2 + 1, \\ a_1^{10} \cdot \Psi_{\ell,char2}\left(\frac{1}{a_1^2}\left(x + \frac{a_3}{a_1}\right), 0, 1\right) &= x^5 + x^4 + x^3 + x^2 + 1\end{aligned}$$

are 11-kernel polynomials of E. By using Kohel's formula and post-composing appropriate isomorphism, we can obtain the two degree 11 endomorphism of E given by $(x,y) \mapsto (r_1(x), yr_1'(x) + r_2(x))$, where one of the endomorphisms is given by

$$r_1(x) = \frac{x^{11} + x^7 + x}{(x^5 + x^2 + 1)^2}, \qquad r_2(x) = \frac{x^{13} + x^8 + x^7 + x^6 + x^4}{(x^5 + x^2 + 1)^3},$$

and the other is given by

$$r_1(x) = \frac{x^{11} + x^7 + x^5 + x^3 + x}{(x^5 + x^4 + x^3 + x^2 + 1)^2},$$
$$r_2(x) = \frac{x^{15} + x^{12} + x^{11} + x^9 + x^7 + x^3 + x^2}{(x^5 + x^4 + x^3 + x^2 + 1)^3}.$$

These two endomorphisms are all the $\mathbb{F}_2$-rational 11-isogenies of E up to equivalence.

5.6.3 Supersingular curves in characteristic 2 and 3

As mentioned in section 4.5.3, since a supersingular elliptic curve in characteristic 2 or 3 has a large automorphism group and more isomorphism classes, the generic kernel polynomial method will be complicated. Thus in this case the division polynomial factorization method would be more desirable to use.

Appendix A

Tables

A.1 Formulas

In the following table we give the data used for the computations for ℓ-isogenies for $\ell \in \{11, 17, 19, 23, 29, 31, 41, 47, 59, 71\}$ given in Chapter 5. We first list the q-expansions of the generators u and v such that $\mathbb{C}(X_0(\ell)) = \mathbb{C}(u, v)$ and the equation for the modular curve $X_0(\ell)$. The j-function j can be written as $j = c\frac{e_0 h_0^3}{h_\infty^d} = \alpha_\ell(u) + v\beta_\ell(u)$, and the function $j - 1728$ can be written as $k = c\frac{e_{1728} h_{1728}^2}{h_\infty^d}$, where d is the denominator of $\frac{\ell+1}{12}$. j satisfies the quadratic relation $j^2 - P_\ell(u)j + Q_\ell(u) = 0$, and $j - 1728$ satisfies the quadratic relation $Q'_\ell(u) := (j - 1728)^2 - P_\ell(u)(j - 1728) + Q_\ell(u) = 0$. Then $Q_\ell(u) = e_0^2 h_{0,\ell}^3(u)$ and $Q'_\ell(u) = e_{1728}^2 h_{1728,\ell}^2(u)$. Finally, we denote the generic ℓ-kernel polynomial $\Psi_\ell(x, u, v)$ of the curve $\mathcal{E}(u, v) : y^2 = x^3 + a_4(u, v) + a_6(u, v)$ by $\Psi_\ell(x, u, v) = x^d + \sum_{i=1}^{d} s_i(u, v)x^{d-i}$, and the coefficient s_1 is given in the table below.

Table A.1: $\ell = 11$

u	$q^{-1} + 5 + 17q + 46q^2 + 116q^3 + 252q^4 + O(q^5)$
v	$-q^{-2} - 2q^{-1} + 12 + 116q + 597q^2 + 2298q^3 + 7616q^4 + O(q^5)$
$X_0(11)$	$v^2 = (u + 1)(u^3 - 17u^2 + 19u - 7)$
s_1	$11(5u - 3)$
c	2
e_0	1
e_{1728}	1

h_∞	$(-u^3+29u^2-258u+680)v+u^5-37u^4+459u^3-2087u^2+2040u+1962$
h_0	$61u^2-246u+45+60v$
h_{1728}	$-7(95u^3-819u^2+189u+135)-18v(37u-51)$
$h_{0,11}$	$u^4+228u^3+486u^2-540u+225$
$h_{1728,11}$	$u^6-522u^5-10017u^4+2484u^3-5265u^2+12150u-5103$
P_{11}	$u^{11}-55u^{10}+1188u^9-12716u^8+69630u^7-177408u^6+133056u^5+132066u^4-187407u^3+40095u^2+24300u-6750$
Q_{11}	$(h_{0,11})^3$
a_{11}	$\frac{1}{2}P_{11}$
b_{11}	$\frac{1}{2}(u-15)(u-6)(u-3)(u-1)u(u^2-12u-9)(u^2-10u+5)$

Table A.2: $\ell = 17$

u	$q^{-1}+3+7q+14q^2+29q^3+50q^4+O(q^5)$
v	$-q^{-2}-q^{-1}+6+33q+117q^2+321q^3+830q^4+O(q^5)$
$X_0(17)$	$v^2=u^4-10u^3-3u^2+4u-8$
s_1	$4\cdot 17(u-1)(2u-1)$
c	4
e_0	1
e_{1728}	$u-1$
h_∞	$(-u^2+13u-38)v+u^4-18u^3+89u^2-76u-90$
h_0	$5(29u^3-121u^2+52u+4)+24v(6u-5)$
h_{1728}	$-4(614u^4-4235u^3+1827u^2+698u-1064)-63v(39u^2-82u+20)$
$h_{0,17}$	$u^6+230u^5+497u^4-1216u^3+1352u^2-1120u+400$
$h_{1728,17}$	$u^8-518u^7-11039u^6-1552u^5-11116u^4+35168u^3-54032u^2+27328u-6272$
P_{17}	$u^{17}-51u^{16}+1105u^{15}-13243u^{14}+95659u^{13}-424065u^{12}+1110355u^{11}-1454945u^{10}+73746u^9+2450210u^8-3131026u^7+1104830u^6+1073992u^5-1392232u^4+557600u^3+2720u^2-67200u+16000$
Q_{17}	$(h_{0,17})^3$
a_{17}	$\frac{1}{2}P_{17}$

b_{17}	$\frac{1}{2}(u-10)(u-5)(u-2)(u-1)u(u+1)(u^2-10u+7)(u^2-6u-4)(u^2-4u+2)(u^3-9u^2+8u-4)$
$\Psi_{17,1728}$	$x^8+(-4i+4)x^6z+(4i+6)x^4z^2+(4i+4)x^2z^3+(-4i+1)z^4/17$

Table A.3: $\ell = 19$

u	$q^{-1}+2+6q+10q^2+21q^3+36q^4+O(q^5)$
v	$-q^{-2}+4+18q+74q^2+188q^3+476q^4+O(q^5)$
$X_0(19)$	$v^2=(u+2)(u^3-10u^2+12u-4)$
s_1	$3\cdot 19(u+1)(3u-2)$
c	8
e_0	$u+1$
e_{1728}	1
h_∞	$(-u+6)v+u^3-10u^2+12u+34$
h_0	$181u^3-423u^2-488u+340+60v(3u+1)$
h_{1728}	$-9(381u^5-1496u^4-3323u^3+1246u^2+1772u-560)-14v(245u^3-18u^2-385u-106)$
$h_{0,19}$	$u^6+234u^5+1193u^4+248u^3-536u^2-640u+400$
$h_{1728,19}$	$u^{10}-512u^9-13614u^8-50340u^7-64983u^6+36108u^5+69148u^4-21728u^3-11280u^2+11200u-6272$
P_{19}	$(u+1)(u^6-13u^5+34u^4+58u^3-118u^2-32u+40)(u^{12}-26u^{11}+237u^{10}-768u^9-588u^8+6948u^7-3751u^6-17606u^5+9353u^4+11448u^3-6808u^2-640u+400)$
Q_{19}	$(u+1)^2(h_{0,19})^3$
a_{19}	$\frac{1}{2}P_{19}$
b_{19}	$\frac{1}{2}(u-7)(u-2)(u-1)u(u+1)(u^2-8u-4)(u^2-6u-15)(u^2-5u-5)(u^2-5u+2)(u^2-2u-4)(u^2+u-1)$
$\Psi_{19,0}$	$x^9+(-12\sqrt{-3}-24)x^6z+(-24\sqrt{-3}-24)x^3z^2+(96\sqrt{-3}-224)z^3/19$

Table A.4: $\ell = 23$

u	$q^{-1}+2+4q+7q^2+13q^3+19q^4+O(q^5)$
v	$-q^{-3}-2q^{-2}-q^{-1}+12+67q+228q^2+667q^3+1696q^4+O(q^5)$

$X_0(23)$	$v^2 = (u^3 - u + 1)(u^3 - 8u^2 + 3u - 7)$
s_1	$23(11u^2 - 10u + 3)$
c	2
e_0	1
e_{1728}	1
h_∞	$(-u^8+30u^7-357u^6+2100u^5-5985u^4+5340u^3+7975u^2-12086u-3280)v+u^{11}-34u^{10}+470u^9-3345u^8+12558u^7-20815u^6-3274u^5+49169u^4-36235u^3+1729u^2+9840u-22734$
h_0	$5(53u^4 - 188u^3 + 62u^2 - 12u - 27) + 24v(11u - 5)$
h_{1728}	$-7(869u^6 - 5178u^5 + 3651u^4 - 580u^3 - 2637u^2 + 2430u - 1107) - 36v(169u^3 - 345u^2 + 107u - 15)$
$h_{0,23}$	$u^8+232u^7+732u^6-968u^5+1894u^4-2280u^3+2268u^2-1080u+225$
$h_{1728,23}$	$u^{12}-516u^{11}-11550u^{10}-3076u^9-15105u^8+54456u^7-151460u^6+218520u^5-210033u^4+132300u^3-67230u^2+24300u-5103$
P_{23}	$u^{23}-46u^{22}+920u^{21}-10465u^{20}+74221u^{19}-336927u^{18}+953856u^{17}-1470068u^{16}+336674u^{15}+3209696u^{14}-6447728u^{13}+5423124u^{12}+302266u^{11}-6612454u^{10}+8362616u^9-4877702u^8-116403u^7+2732814u^6-2492280u^5+1115109u^4-170775u^3-83835u^2+48600u-6750$
Q_{23}	$(h_{0,23})^3$
a_{23}	$\frac{1}{2}P_{23}$
b_{23}	$(u-5)(u-3)(u-2)(u-1)u(u+1)(u^2-8u+3)(u^2-6u-9)(u^3-7u^2+3u-5)(u^3-7u^2+7u-3)(u^4-4u^3-1)$

Table A.5: $\ell = 29$

u	$q^{-1} + 1 + 3q + 4q^2 + 7q^3 + 10q^4 + O(q^5)$
v	$-q^{-3} - q^{-2} + 6 + 29q + 85q^2 + 231q^3 + 520q^4 + O(q^5)$
$X_0(29)$	$v^2 = u^6 - 4u^5 - 12u^4 + 2u^3 + 8u^2 + 8u - 7$
s_1	$2 \cdot 29(u + 1)(7u^2 - u - 3)$
c	4
e_0	1
e_{1728}	$u + 1$

h_∞	$(-u^4+11u^3-31u^2-14u+100)v+u^7-13u^6+45u^5+25u^4-269u^3+29u^2+300u+166$
h_0	$421u^5-301u^4-1867u^3-671u^2+627u+405+60v(7u^2+5u-1)$
h_{1728}	$-14(871u^7-1724u^6-7263u^5-1831u^4+4313u^3+3393u^2-918u-675)-9v(1355u^4-28u^3-2307u^2-634u+249)$
$h_{0,29}$	$u^{10}+238u^9+1907u^8+4072u^7+3365u^6-1730u^5-3707u^4-744u^3+459u^2+270u+225$
$h_{1728,29}$	$u^{14}-508u^{13}-15134u^{12}-82634u^{11}-196489u^{10}-143636u^9+80491u^8+233402u^7+141391u^6-59652u^5-136053u^4+1350u^3+40662u^2-972u-5103$
P_{29}	$u^{29}-29u^{28}+319u^{27}-1421u^{26}-580u^{25}+26680u^{24}-53679u^{23}-189399u^{22}+622398u^{21}+853818u^{20}-3427365u^{19}-3592085u^{18}+10954634u^{17}+14041394u^{16}-18871083u^{15}-37142939u^{14}+9216142u^{13}+54103270u^{12}+19207947u^{11}-38397537u^{10}-31795426u^9+9708910u^8+19103721u^7+2357613u^6-5229135u^5-1754181u^4+570024u^3+281880u^2-12150u-6750$
Q_{29}	$(h_{0,29})^3$
a_{29}	$\frac{1}{2}P_{29}$
b_{29}	$(u-3)(u-1)u(u+1)(u+2)(u^2-6u+2)(u^2-5u-5)(u^2-5u+3)(u^2-3u-9)(u^2-u-3)(u^2-u-1)(u^2+u-1)(u^3-4u^2-6u-5)(u^4-2u^3-5u^2-4u-1)$
$\Psi_{29,1728}$	$x^{14}+(-14i+3)x^{12}z+(-20i+73)x^{10}z^2+(-58i+115)x^8z^3+(-56i+59)x^6z^4+(30i+1)x^4z^5+(12i-5)x^2z^6+(2i+5)z^7/29$

Table A.6: $\ell = 31$

u	$q^{-1}+2+3q+3q^2+6q^3+9q^4+O(q^5)$
v	$-q^{-3}-2q^{-2}+8+32q+90q^2+215q^3+464q^4+O(q^5)$
$X_0(31)$	$v^2=(u^3-6u^2-5u-1)(u^3-2u^2-u+3)$
s_1	$3\cdot 31(u-2)(5u^2-6u-3)$
c	8
e_0	$u-2$
e_{1728}	1

h_∞	$(-u^2+10u-24)v+u^5-14u^4+59u^3-57u^2-72u+46$
h_0	$481u^5-2766u^4+3486u^3+1320u^2-2423u-690+120v(4u^2-9u+3)$
h_{1728}	$-9(1655u^8-16522u^7+52005u^6-51168u^5-31099u^4+69638u^3-5709u^2-17436u-1980)-28v(532u^5-3201u^4+6123u^3-3261u^2-1259u+726)$
$h_{0,31}$	$u^{10}+228u^9-192u^8-3192u^7+8630u^6-8064u^5+4884u^4-4200u^3-911u^2+2940u+900$
$h_{1728,31}$	$u^{16}-524u^{15}-7398u^{14}+77436u^{13}-235329u^{12}+308496u^{11}-543420u^{10}+2282040u^9-5204193u^8+5149812u^7-753174u^6-2249748u^5+752113u^4+797704u^3-118440u^2-237600u-52272$
P_{31}	$(u-2)(u^{10}-20u^9+149u^8-495u^7+601u^6+368u^5-1285u^4+357u^3+546u^2-98u-60)(u^{20}-40u^{19}+698u^{18}-6950u^{17}+43203u^{16}-170814u^{15}+406833u^{14}-433212u^{13}-399237u^{12}+1798836u^{11}-1596071u^{10}-1084674u^9+2649985u^8-564454u^7-1445909u^6+621736u^5+367692u^4-137256u^3-53183u^2+2940u+900)$
Q_{31}	$(u-2)^2(h_{0,31})^3$
a_{31}	$\frac{1}{2}P_{31}$
b_{31}	$(u-3)(u-2)(u-1)u(u+1)(u^2-8u+11)(u^2-7u+2)(u^2-5u-2)(u^2-5u+5)(u^2-4u-4)(u^2-4u-1)(u^2-2u-1)(u^2-u-1)(u^3-9u^2+21u-15)(u^4-8u^3+8u^2+12u-9)$
$\Psi_{31,0}$	$x^{15}+(-66\sqrt{-3}+86)x^{12}z+(168\sqrt{-3}+280)x^9z^2+(576\sqrt{-3}+1792)x^6z^3+(384\sqrt{-3}+896)x^3z^4+(-3072\sqrt{-3}-2048)z^5/31$

Table A.7: $\ell = 41$

u	$q^{-1}+1+2q+2q^2+3q^3+4q^4+O(q^5)$
v	$-q^{-4}-2q^{-3}-2q^{-2}+q^{-1}+12+42q+120q^2+283q^3+612q^4+O(q^5)$
$X_0(41)$	$v^2=u^8-4u^7-8u^6+10u^5+20u^4+8u^3-15u^2-20u-8$
s_1	$4\cdot 41(u-1)(5u^3-2u^2-6u-2)$
c	4
e_0	1
e_{1728}	$u-1$

h_∞	$(-u^6+14u^5-66u^4+95u^3+106u^2-286u+20)v+u^{10}-16u^9+88u^8-150u^7-236u^6+832u^5+77u^4-976u^3-452u^2+80u+522$
h_0	$841u^7-2403u^6-1683u^5+4443u^4+2395u^3-1229u^2-1796u-460+120v(7u^3-8u^2-2u+2)$
h_{1728}	$-4(8615u^{10}-34397u^9-23955u^8+105727u^7+51833u^6-79767u^5-94038u^4-4224u^3+42594u^2+20572u+560)-63v(547u^6-1098u^5-675u^4+1212u^3+525u^2-178u-116)$
$h_{0,41}$	$u^{14}+234u^{13}+963u^{12}-1896u^{11}-2659u^{10}-1006u^9+9101u^8+3040u^7-7733u^6-2926u^5+2361u^4-672u^3-184u^2+1120u+400$
$h_{1728,41}$	$u^{20}-512u^{19}-13094u^{18}-25658u^{17}+44779u^{16}+256408u^{15}-74933u^{14}-473006u^{13}-332369u^{12}+236464u^{11}+678355u^{10}+675574u^9-356026u^8-1074148u^7-206215u^6+605400u^5+294756u^4-115776u^3-126992u^2-39872u-6272$
P_{41}	$u^{41}-41u^{40}+738u^{39}-7544u^{38}+46617u^{37}-162483u^{36}+163057u^{35}+1099661u^{34}-4706595u^{33}+3613289u^{32}+20512341u^{31}-49355103u^{30}-24135265u^{29}+193718727u^{28}-61715127u^{27}-462271351u^{26}+261059095u^{25}+879637411u^{24}-421357697u^{23}-1503727029u^{22}+282422801u^{21}+2179745361u^{20}+343522723u^{19}-2400692229u^{18}-1270633050u^{17}+1772593672u^{16}+1832223375u^{15}-605560447u^{14}-1542677562u^{13}-271341362u^{12}+745775322u^{11}+436080674u^{10}-147139488u^9-217030548u^8-31732934u^7+46140990u^6+20985112u^5-1742664u^4-2966432u^3-465760u^2+67200u+16000$
Q_{41}	$(h_{0,41})^3$
a_{41}	$\frac{1}{2}P_{41}$
b_{41}	$(u-5)(u-2)(u-1)u(u+1)(u^2-5u+5)(u^2-3u-7)(u^2-2u-4)(u^2-2u-1)(u^2-u-1)(u^2-2)(u^2+u-1)(u^3-3u^2-5u-2)(u^3-2u^2-2u-1)(u^4-6u^3+5u^2+2u-1)(u^4-5u^3+u^2+4)(u^4-4u^3+2)$
$\Psi_{41,1728}$	$x^{20}+(-12i-22)x^{18}z+(-252i-247)x^{16}z^2+(-176i-424)x^{14}z^3+(464i-254)x^{12}z^4+(1688i-868)x^{10}z^5+(1720i-1190)x^8z^6+(528i-232)x^6z^7+(16i+29)x^4z^8+(20i+10)x^2z^9+(4i+5)z^10/41$

Table A.8: $\ell = 47$

u	$q^{-1} + 1 + q + 2q^2 + 3q^3 + 3q^4 + O(q^5)$
v	$-q^{-5} - 2q^{-4} - 4q^{-3} - 4q^{-2} + 2q^{-1} + 24 + 89q + 236q^2 + 565q^3 + 1218q^4 + O(q^5)$
$X_0(47)$	$v^2 = (u^5 - 5u^4 + 5u^3 - 15u^2 + 6u - 11)(u^5 - u^4 + u^3 + u^2 - 2u + 1)$
s_1	$47(23u^4 - 34u^3 + 47u^2 - 32u + 8)$
c	2
e_0	1
e_{1728}	1
h_∞	$(-u^{18}+32u^{17}-451u^{16}+3670u^{15}-18970u^{14}+64386u^{13}-142259u^{12}+190100u^{11} - 102740u^{10} - 134790u^9 + 397118u^8 - 481050u^7 + 212233u^6 + 205926u^5 - 356850u^4 + 255206u^3 - 1768u^2 - 141184u + 6984)v + u^{23} - 35u^{22} + 548u^{21} - 5064u^{20} + 30701u^{19} - 128502u^{18} + 380807u^{17} - 804478u^{16} + 1181647u^{15} - 1028219u^{14} - 128194u^{13} + 2174401u^{12} - 3944815u^{11} + 3887507u^{10} - 1481829u^9 - 2130163u^8 + 4340198u^7 - 3645695u^6 + 1228720u^5 + 1193720u^4 - 1610664u^3 + 676480u^2 - 55872u - 206350$
h_0	$5(221u^8 - 860u^7 + 1470u^6 - 2316u^5 + 1757u^4 - 1200u^3 + 96u^2 + 272u - 160) + 24v(46u^3 - 51u^2 + 47u - 16)$
h_{1728}	$-(51911u^{12} - 311214u^{11} + 785721u^{10} - 1630156u^9 + 2167161u^8 - 2307006u^7 + 1460351u^6 - 257904u^5 - 754680u^4 + 1054696u^3 - 752640u^2+303168u-59752)-252v(206u^7-619u^6+999u^5-1245u^4+871u^3 - 468u^2 + 96u + 4)$
$h_{0,47}$	$u^{16} + 232u^{15} + 508u^{14} - 1032u^{13} + 7814u^{12} - 17480u^{11} + 43644u^{10} - 76312u^9+120769u^8-152864u^7+163968u^6-143584u^5+102656u^4-57984u^3 + 25024u^2 - 7168u + 1024$
$h_{1728,47}$	$u^{24} - 516u^{23} - 11022u^{22} + 14876u^{21} - 108177u^{20} + 219720u^{19} - 924036u^{18}+2530344u^{17}-7168689u^{16}+16156524u^{15}-32334990u^{14}+55102380u^{13} - 82583999u^{12} + 108299856u^{11} - 125452032u^{10} + 128037264u^9 - 114961824u^8 + 90070656u^7 - 60908352u^6 + 34907136u^5-16548864u^4+6243328u^3-1775616u^2+344064u-34496$

P_{47}	$u^{47} - 47u^{46} + 1034u^{45} - 14194u^{44} + 136864u^{43} - 990431u^{42} + 5617769u^{41} - 25770006u^{40} + 97893151u^{39} - 313468474u^{38} + 856757031u^{37} - 2013138357u^{36} + 4071881378u^{35} - 7040645261u^{34} + 10182603298u^{33} - 11611941072u^{32} + 8435506655u^{31} + 2065827049u^{30} - 20241250112u^{29} + 41879296232u^{28} - 57873890484u^{27} + 57280402355u^{26} - 33364599371u^{25} - 10454018992u^{24} + 59196883097u^{23} - 92028642340u^{22} + 93046207239u^{21} - 60791892299u^{20} + 9942017442u^{19} + 36612252089u^{18} - 60426283952u^{17} + 56657584158u^{16} - 34288012648u^{15} + 8421580132u^{14} + 9100068184u^{13} - 14673798654u^{12} + 11705275552u^{11} - 5945275904u^{10} + 1469334304u^9 + 552981696u^8 - 845669120u^7 + 508021120u^6 - 187217920u^5 + 38598656u^4 - 96256u^3 - 2502656u^2 + 688128u - 65536$
Q_{47}	$(h_{0,47})^3$
a_{47}	$\frac{1}{2}P_{47}$
b_{47}	$(u-4)(u-2)(u-1)u(u+1)(u^2-5u+2)(u^2-2u-1)(u^3-5u^2+5u-7)(u^3-4u^2+3u-4)(u^3-4u^2+3u-1)(u^3-3u^2+2u-4)(u^3-2u^2+2u-2)(u^3+u+1)(u^4-4u^3-2u^2-4)(u^5-5u^4+5u^3-11u^2+6u-4)(u^6-4u^5+2u^4-4u^3-u^2+4u-2)$

Table A.9: $\ell = 59$

u	$q^{-1} + 1 + q + q^2 + 2q^3 + 2q^4 + O(q^5)$
v	$-q^{-6} - 2q^{-5} - 4q^{-4} - 6q^{-3} - 5q^{-2} + 4q^{-1} + 36 + 114q + 291q^2 + 652q^3 + 1356q^4 + O(q^5)$
$X_0(59)$	$v^2 = (u^3 - u^2 - u + 2)(u^9 - 7u^8 + 16u^7 - 21u^6 + 12u^5 - u^4 - 9u^3 + 6u^2 - 4u - 4)$
s_1	$59(29u^5 - 75u^4 + 70u^3 - 5u^2 - 25u + 10)$
c	2
e_0	1
e_{1728}	1

h_∞	$(-u^{23}+37u^{22}-616u^{21}+6069u^{20}-39055u^{19}+170076u^{18}-495775u^{17}+881089u^{16}-537033u^{15}-1541350u^{14}+4481421u^{13}-4596423u^{12}-457055u^{11}+6912466u^{10}-8288040u^9+3173710u^8+3493754u^7-6126974u^6+3753975u^5+66575u^4-1618980u^3+1096775u^2-356875u-97290)v+u^{29}-41u^{28}+767u^{27}-8646u^{26}+65242u^{25}-345346u^{24}+1299200u^{23}-3394428u^{22}+5532057u^{21}-2754549u^{20}-11455781u^{19}+33422064u^{18}-39712945u^{17}+4765791u^{16}+59683258u^{15}-97108805u^{14}+60459413u^{13}+29458008u^{12}-97582565u^{11}+88819755u^{10}-20651425u^9-40904030u^8+51626870u^7-24114790u^6-3594375u^5+12158775u^4-6792025u^3+568250u^2+972900u-304958$
h_0	$1741u^{10}-10326u^9+23113u^8-24254u^7+4200u^6+16806u^5-19051u^4+6906u^3+1281u^2-2948u+820+60v(29u^4-60u^3+42u^2-2u-5)$
h_{1728}	$-(102689u^{15}-923949u^{14}+3395037u^{13}-6767646u^{12}+7137705u^{11}-1410051u^{10}-7059704u^9+10767999u^8-7135101u^7+815998u^6+2659035u^5-2317185u^4+573935u^3+284010u^2-186780u+12880)-126v(815u^9-4077u^8+8092u^7-7639u^6+1800u^5+2865u^4-2762u^3+729u^2+111u-94)$
$h_{0,59}$	$u^{20}+228u^{19}-418u^{18}-2584u^{17}+16417u^{16}-48352u^{15}+100862u^{14}-170700u^{13}+241876u^{12}-267564u^{11}+195830u^{10}-45208u^9-74383u^8+82400u^7-23442u^6-10532u^5+4945u^4+3144u^3-776u^2-1120u+400$
$h_{1728,59}$	$u^{30}-522u^{29}-7917u^{28}+76386u^{27}-307545u^{26}+820932u^{25}-2142548u^{24}+6885156u^{23}-22079883u^{22}+57791950u^{21}-117435843u^{20}+184505958u^{19}-223131606u^{18}+203732586u^{17}-133730439u^{16}+53975742u^{15}+1407345u^{14}-31142904u^{13}+46515140u^{12}-45198360u^{11}+23071443u^{10}+4298322u^9-15343845u^8+8880366u^7-44571u^6-2320908u^5+958668u^4+13312u^3-108240u^2+33600u-6272$

P_{59}	$u^{59} - 59u^{58} + 1652u^{57} - 29205u^{56} + 365800u^{55} - 3452149u^{54} + 25475079u^{53} - 150487052u^{52} + 721829600u^{51} - 2830320860u^{50} + 9059054346u^{49} - 23352309386u^{48} + 46651654354u^{47} - 64236756338u^{46} + 28871590941u^{45} + 134398080099u^{44} - 459184355769u^{43} + 800595050760u^{42} - 748989116551u^{41} - 179519591637u^{40} + 1987950394792u^{39} - 3658171840037u^{38} + 3397583328372u^{37} - 54249978263u^{36} - 5190227733987u^{35} + 8713332734648u^{34} - 6917286294515u^{33} - 315658868113u^{32} + 8512399456274u^{31} - 11643540780203u^{30} + 7131088674129u^{29} + 1742977715620u^{28} - 8488557160148u^{27} + 8772457933356u^{26} - 3589340274442u^{25} - 2342393877496u^{24} + 4920423266916u^{23} - 3566756201696u^{22} + 614906882627u^{21} + 1373184591667u^{20} - 1549365239197u^{19} + 682044179678u^{18} + 121615007703u^{17} - 372641172307u^{16} + 230682514316u^{15} - 33068562195u^{14} - 51342089572u^{13} + 41679530185u^{12} - 10887235780u^{11} - 3953349811u^{10} + 4310971231u^9 - 1262437160u^8 - 170978932u^7 + 241324042u^6 - 60792184u^5 - 5127336u^4 + 5573376u^3 - 783520u^2 - 67200u + 16000$
Q_{59}	$(h_{0,59})^3$
a_{59}	$\frac{1}{2}P_{59}$
b_{59}	$(u-2)(u-1)u(u+1)(u^2-4u-1)(u^2-3u-5)(u^2-3u-2)(u^2-3u+1)(u^2-u-1)(u^3-6u^2+10u-7)(u^3-5u^2+7u-5)(u^3-3u^2+2u-1)(u^3-u^2+1)(u^4-5u^3+4u^2-1)(u^4-4u^3+3u^2+2u-4)(u^4-3u^3-u-1)(u^4-u^3+2u-1)(u^5-6u^4+10u^3-11u^2+8u-4)(u^6-5u^5+5u^4-5u^2+5u-5)$

Table A.10: $\ell = 71$

u	$q^{-1} + 1 + q + q^2 + q^3 + q^4 + O(q^5)$
v	$-q^{-7} - 2q^{-6} - 4q^{-5} - 6q^{-4} - 8q^{-3} - 6q^{-2} + 8q^{-1} + 48 + 147q + 354q^2 + 772q^3 + 1550q^4 + O(q^5)$
$X_0(71)$	$v^2 = (u^7 - 7u^6 + 14u^5 - 11u^4 + 14u^3 - 14u^2 - u - 7)(u^7 - 3u^6 + 2u^5 + u^4 - 2u^3 + 2u^2 - u + 1)$

s_1	$71(35u^6 - 128u^5 + 140u^4 - 70u^3 + 60u^2 - 20u + 3)$
c	2
e_0	1
e_{1728}	1
h_∞	$(-u^{28} + 42u^{27} - 806u^{26} + 9334u^{25} - 72500u^{24} + 396424u^{23} - 1553368u^{22} + 4326410u^{21} - 8160873u^{20} + 8759620u^{19} + 19304u^{18} - 16702602u^{17} + 27869242u^{16} - 22483954u^{15} + 4186685u^{14} + 17823176u^{13} - 31778448u^{12} + 24183078u^{11} - 3392576u^{10} - 9882970u^9 + 13774395u^8 - 10286052u^7 + 1944068u^6 + 2820804u^5 - 2836345u^4 + 893312u^3 - 304857u^2 + 5178u + 254560)v + u^{35} - 47u^{34} + 1022u^{33} - 13619u^{32} + 124132u^{31} - 817352u^{30} + 3998715u^{29} - 14693075u^{28} + 40339679u^{27} - 80418271u^{26} + 106690988u^{25} - 62599465u^{24} - 83567174u^{23} + 272370138u^{22} - 376039968u^{21} + 299347418u^{20} - 40666576u^{19} - 286649771u^{18} + 478017134u^{17} - 413542066u^{16} + 178084164u^{15} + 80660478u^{14} - 247871444u^{13} + 250578745u^{12} - 140527595u^{11} + 26915405u^{10} + 39541134u^9 - 57789935u^8 + 45389940u^7 - 18044877u^6 + 1878151u^5 + 2182861u^4 - 4751823u^3 + 2537833u^2 - 763680u - 242478$
h_0	$2521u^{12} - 20048u^{11} + 60744u^{10} - 91716u^9 + 83912u^8 - 63144u^7 + 34806u^6 - 2528u^5 - 7736u^4 + 8844u^3 - 6008u^2 + 3336u - 855 + 120v(21u^5 - 64u^4 + 56u^3 - 21u^2 + 12u - 2)$
h_{1728}	$-7(25565u^{18} - 306744u^{17} + 1534692u^{16} - 4245086u^{15} + 7365924u^{14} - 8900868u^{13} + 8213555u^{12} - 5570496u^{11} + 1705848u^{10} + 1476740u^9 - 2966568u^8 + 3165576u^7 - 2550405u^6 + 1651128u^5 - 843804u^4 + 371866u^3 - 135612u^2 + 27324u - 4995) - 36v(4971u^11 - 34804u^10 + 94260u^9 - 129897u^8 + 111568u^7 - 79254u^6 + 44433u^5 - 13360u^4 + 2248u^3 + 801u^2 - 748u + 258)$
$h_{0,71}$	$u^{24} + 224u^{23} - 1328u^{22} - 456u^{21} + 25936u^{20} - 115088u^{19} + 319068u^{18} - 714688u^{17} + 1376816u^{16} - 2256088u^{15} + 3130928u^{14} - 3727056u^{13} + 3886438u^{12} - 3629088u^{11} + 3051056u^{10} - 2289208u^9 + 1540528u^8 - 935728u^7 + 501596u^6 - 235776u^5 + 98512u^4 - 33576u^3 + 9936u^2 - 2160u + 225$

$h_{1728,71}$	$u^{36} - 528u^{35} - 4776u^{34} + 119188u^{33} - 836040u^{32} + 3354312u^{31} - 10180254u^{30} + 30268416u^{29} - 96122760u^{28} + 290870292u^{27} - 765646248u^{26} + 1718954424u^{25} - 3321068545u^{24} + 5612654496u^{23} - 8445198288u^{22} + 11482474344u^{21} - 14237874960u^{20} + 16176779856u^{19} - 16897107876u^{18} + 16278213312u^{17} - 14500065744u^{16} + 11961718792u^{15} - 9149462544u^{14} + 6492567792u^{13} - 4273294193u^{12} + 2606941680u^{11} - 1470232968u^{10} + 763563396u^{9} - 363853608u^{8} + 157605480u^{7} - 61336862u^{6} + 21233088u^{5} - 6376104u^{4} + 1592676u^{3} - 327240u^{2} + 48600u - 5103$
P_{71}	$u^{71} - 71u^{70} + 2414u^{69} - 52327u^{68} + 812240u^{67} - 9613968u^{66} + 90223321u^{65} - 689157169u^{64} + 4364552115u^{63} - 23228729413u^{62} + 104923131180u^{61} - 405138280373u^{60} + 1343947848527u^{59} - 3841191816845u^{58} + 9464634765852u^{57} - 20052219750661u^{56} + 36239054778472u^{55} - 54817285755105u^{54} + 66216047255551u^{53} - 54867900326127u^{52} + 5131997859077u^{51} + 87504290135653u^{50} - 205131886553392u^{49} + 304702155703516u^{48} - 330646545417814u^{47} + 241209603962570u^{46} - 36287337331916u^{45} - 230395084854230u^{44} + 466024421705696u^{43} - 576967281819172u^{42} + 512373447321402u^{41} - 289840331821002u^{40} - 111424277668 50u^{39} + 284518400252142u^{38} - 443144048889720u^{37} + 451855980915164u^{36} - 334009986053250u^{35} + 152367877270246u^{34} + 22513210292184u^{33} - 140033523896938u^{32} + 182582147217312u^{31} - 162234735929274u^{30} + 107139839089502u^{29} - 46332664858222u^{28} - 468390635342u^{27} + 25902000374138u^{26} - 32365758791872u^{25} + 27006964902986u^{24} - 17218530732347u^{23} + 8102336330029u^{22} - 1930304898882u^{21} - 1147488305875u^{20} + 2020891913264u^{19} - 1753961304140u^{18} + 1136695427037u^{17} - 585283867605u^{16} + 230566737711u^{15} - 53385529273u^{14} - 11859874932u^{13} + 23635982289u^{12} - 17516526653u^{11} + 9450153463u^{10} - 4089818964u^{9} + 1441975423u^{8} - 399596520u^{7} + 75190491u^{6} - 2486349u^{5} - 4854483u^{4} + 2263977u^{3} - 603855u^{2} + 97200u - 6750$
Q_{71}	$(h_{0,71})^3$
a_{71}	$\frac{1}{2}P_{71}$

b_{71}	$(u-3)(u-2)(u-1)u(u+1)(u^2-5u+5)(u^2-3u+1)(u^2-2u-1)(u^2-u-1)(u^3-5u^2+5u-3)(u^3-4u^2-1)(u^3-2u^2-1)(u^4-6u^3+7u^2+6u-9)(u^4-5u^3+4u^2+u+3)(u^4-5u^3+6u^2-3u+5)(u^4-4u^3+u^2-4u+1)(u^4-4u^3+2u^2-u+1)(u^4-2u^3-3u^2-2u-1)(u^4-2u^3+u-1)(u^6-5u^5+8u^4-7u^3+6u^2-3u+1)(u^8-6u^7+9u^6-2u^5+2u^3-9u^2+2u-1)$

A.2 $X_0(\ell)$ for $\ell = 11, 17, 19$ as an elliptic curve

The modular curve $X_0(\ell)$ for $\ell = 11$, 17, 19 is an elliptic curve since the genus of $X_0(\ell)$ is 1 for these ℓ. Thus there is a standard minimal Weierstrass model of the form (2.2), which we denote by E_ℓ. Also, $X_0(\ell)$ has an equation of the form $C_\ell : v^2 = f_\ell(u)$ where $f_\ell(u)$ is a polynomial of degree 4 in u. Note that both of two cusps of $X_0(\ell)$ are put into the point at infinity of C_ℓ (say "double infinity point" $O^\pm$). We present the tables below for the equations of E_ℓ and $X_0(\ell)$, explicit isomorphisms between them and $\mathbb{Q}$-rational points on C_ℓ and E_ℓ.

Table A.11: $\ell = 11$

Equations of E_{11} and $X_0(11)$
$C_{11} :\ v^2 = u^4 - 16u^3 + 2u^2 + 12u - 7 = (u+1)(u^3 - 17u^2 + 19u - 7)$ $E_{11} :\ y^2 + y = x^3 - x^2 - 10x - 20$
Isomorphisms
$x = \dfrac{5u-6}{u+1}, \qquad y = -\dfrac{u^2+2u+11v+1}{2(u+1)^2}$ $u = -\dfrac{x+6}{x-5}, \qquad v = -\dfrac{11(2y+1)}{(x-5)^2}$
$\mathbb{Q}$-rational points
$C_{11}(\mathbb{Q}) = \{O^\pm, (-1,0), (-2,11), (-2,-11)\}$ $E_{11}(\mathbb{Q}) = \{O, (5,5), (16,-61), (16,60), (5,-6)\}$

The cusps of $X_0(11)$ correspond to O on C with multiplicity 2 and points $(5,5)$, $(5,-6)$ on E.

Table A.12: $\ell = 17$

Equations of E_{17} and $X_0(17)$
$C_{17}: \ v^2 = u^4 - 10u^3 - 3u^2 + 4u - 8$ $E_{17}: \ y^2 + xy + y = x^3 - x^2 - x - 14$
Isomorphisms
$x = \frac{1}{2}(u^2 - 5u + v), \qquad y = \frac{1}{2}(u^3 - 8u^2 + uv + u - 3v)$ $u = -\frac{3x + y}{x - 7}, \qquad v = \frac{2x^3 - 22x^2 - xy - y^2 - 7x - 35y}{(x-7)^2}$
$\mathbb{Q}$-rational points
$C_{17}(\mathbb{Q}) = \{O^{\pm}, (-\frac{3}{2}, \frac{17}{4}), (-\frac{3}{2}, -\frac{17}{4})\}$ $E_{17}(\mathbb{Q}) = \{O, (7, -21), (\frac{11}{4}, -\frac{15}{8}), (7, 13)\}$

The cusps of $X_0(17)$ correspond to O on C with multiplicity 2 and points $(7, -21)$, $(7, 13)$ on E.

Table A.13: $\ell = 19$

Equations of E_{19} and $X_0(19)$
$C_{19}: \ v^2 = u^4 - 8u^3 - 8u^2 + 20u - 8 = (u + 2)(u^3 - 10u^2 + 12u - 4)$ $E_{19}: \ y^2 + y = x^3 + x^2 - 9x - 15$
Isomorphisms
$x = \frac{5u - 9}{u + 2}, \qquad y = -\frac{u^2 + 4u + 19v + 4}{2(u+2)^2}$ $u = -\frac{2x + 9}{x - 5}, \qquad v = -\frac{19(2y + 1)}{(x-5)^2}$

$\mathbb{Q}$-rational points
$C_{19}(\mathbb{Q}) = \{O^{\pm}, (-2, 0)\}$ $E_{19}(\mathbb{Q}) = \{O, (5, -10), (5, 9)\}$

The cusps of $X_0(19)$ correspond to O on C with multiplicity 2 and points $(5, -10)$, $(5, 9)$ on E.

Bibliography

[1] A. Bostan, F. Morain, B. Salvy, and É. Schost. Fast algorithms for computing isogenies between elliptic curves. *Mathematics of Computation*, 77(263):1755–1778, 2008.

[2] Carlos Castano-Bernard. A note on the rational points of $X_0^+(N)$. *arXiv preprint math/0508115*, 2006.

[3] J. E. Cremona and M. Watkins. Computing isogenies of elliptic curves. *preprint*, 2005.

[4] F. Diamond and J. Im. Modular forms and modular curves. In *Seminar on Fermat's Last Theorem, CMS Conference Proceedings 17. American Mathematical Society, Providence, RI*, pages 39–133, 1995.

[5] F. Diamond and J. M. Shurman. *A first course in modular forms*. Springer-Verlag, 2005.

[6] N. D. Elkies. Explicit isogenies. *preprint*, 1991.

[7] N. D. Elkies. Elliptic and modular curves over finite fields and related computational issues. *AMS/IP Studies in Advanced Mathematics*, 7:21–76, 1998.

[8] Steven D. Galbraith. *Mathematics of public key cryptography*. Cambridge University Press, 2012.

[9] J. Gonzalez. Equations of hyperelliptic modular curves. In *Annales de l'institut Fourier*, volume 41, pages 779–795. Institut Fourier, 1991.

[10] D. Kohel. *Endomorphism rings of elliptic curves over finite fields*. PhD thesis, University of California at Berkeley, 1996.

[11] MAGMA. Mathematical software, http://magma.maths.usyd.edu.au/magma/.

[12] J. S. Milne. *Elliptic curves*. BookSurge Publishers, 2006.

[13] A. P. Ogg. Rational points on certain elliptic modular curves. *A talk given in St. Louis on*, 29, 1973.

[14] M. Reid. *Undergraduate algebraic geometry*, volume 12. Cambridge Univ Pr, 1988.

[15] SAGE. Mathematical software, http://sagemath.org/.

[16] G. Shimura. *Introduction to the arithmetic theory of automorphic functions*. Princeton Univ Pr, 1971.

[17] J. H. Silverman. *The arithmetic of elliptic curves, GTM 106*. Springer-Verlag, 1986.

[18] J. H. Silverman. *Advanced topics in the arithmetic of elliptic curves, GTM 151*. Springer-Verlag, 1994.

[19] J. Vélu. Isogénies entre courbes elliptiques. *CR Acad. Sci. Paris Sér. AB*, 273:A238–A241, 1971.

[20] L. C. Washington. *Elliptic curves: number theory and cryptography*. Chapman & Hall, 2008.