Canonical and Quasi-canonical lifts of elliptic curves

Andy Ramirez-Cote

McGill University, Montreal

August, 2020

A thesis submitted to McGill University in partial fulfillment of the requirements of the degree of

Master of Mathematics

Abstract

We give a brief overview of the problem of lifting elliptic curves, and of the classical theory of complex multiplication. We then concretize the results of B. Gross [3] on lifting endomorphism of formal groups from characteristic p to characteristic 0 by applying them to elliptic curves, with a view toward developing explicit numerical methods to compute the lift of the j-invariants with reduction in $\mathbb{F}_p$. Chapter 1 and Chapter 2.1 are review of well-known results, while the results of Chapter 2.2 and Chapter 3 have been derived independently except where otherwise mentioned.

Abrégé

Nous présentons sommairement le problème de relèvement pour les courbes elliptiques et la théorie de la multiplication complexes. Par la suite, nous appliquons les résultats de B. Gross [3] sur le relèvement d'endomorphismes de groupes formels de caractéristique p en caractéristique 0 au courbes elliptiques. Notre but est de développer des méthodes numériques explicites pour calculer le le relèvement des j-invariants de courbes elliptiques. Le chapitre 1 et le chapitre 2.1 présentes des résultats déja connus dans la littérature, tandis que les résultats des chapitre 2.2 et 3 ont été trouvé de manière indépendante, sauf lorsque qu'il en est indiqué autrement.

Acknowledgements

I would like to thank Professor Henri Darmon for his guidance and his helpful suggestions.

Table of Contents

Abstract i

Abrégé ii

Acknowledgements iii

List of Tables v

1 Introduction **1**

1.1 Background on lifting 1

1.2 Complex Multiplication 4

2 Canonical lifts **9**

2.1 Lifting curves over $\mathbb{F}_q - \mathbb{F}_{p^2}$ 9

2.2 The case of $\mathbb{F}_p$ 11

2.2.1 Endomorphism of degree p 11

2.2.2 Numerical applications 15

2.2.3 Endomorphism of degree l, and endomorphism of arbibtrary degree 18

3 Code and Numerical results **20**

Conclusion 28

List of Tables

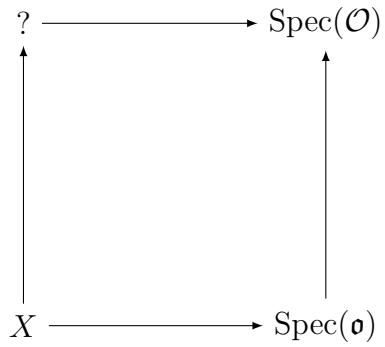
3.1 Lifts of Frobenius in characteristic 5 27
3.2 Lift of the ordinary Frobenius in characteristic 7 27

Chapter 1

Introduction

1.1 Background on lifting

Let L be a local field with ring of integer $(\mathcal{O}, \mathfrak{m})$, and denote the corresponding residue field by $\mathfrak{o}$. Any abelian scheme over $\mathcal{O}$ with good reduction gives rise to a corresponding scheme over $\mathfrak{o}$ in the obvious manner. The question of lifting an abelian scheme $X \mapsto \mathrm{Spec}(\mathfrak{o})$ amounts to the converse: Can we complete the cartesian diagram



and if so, can we complete it uniquely? An important result of Serre-Tate, summarized in a 1964 seminar (for which complete proofs were published by Messing [5] and Drinfeld [2]), goes a long way to answering this question on a theoretical level:

Theorem 1 *[7] Let R be an Artinian local ring with residue field k. Then there is an equivalence of categories $C_1 \longmapsto C_2$ where*

C_1 is the category whose objects are abelian schemes over R and whose morphisms are regular group homomorphism.

C_2 is the category whose objects are pairs (Φ, X) with Φ an abelian scheme over k and X is a p-divisible group lifting $\Phi[p^\infty] := \varinjlim \Phi[p^n]$, and whose morphisms are pairs of regular group homomorphisms compatible with the inclusions $\Phi[p^n] \subset \Phi$.

Here $\Phi[p^n]$ is the group scheme $\ker(p^n : \Phi \longmapsto \Phi)$ and $\Phi[p^\infty]$ the ind-group scheme corresponding to the inclusions $\Phi[p^n] \mapsto \Phi[p^{n+1}]$. While the theorem is ostensibly only about Artinian rings, by passing to the limit we can generalize to complete local Noetherian rings, at the cost of having what may only be formal abelian schemes.

To use this theorem, we need more explicit descriptions of the objects of the category C_2. There are two extreme cases, which we summarize below [7].

1) Φ has the maximal number of p-torsion points. Then $\Phi[p]$ is a sum of an étale k-group of the form $(\mathbb{Z}/p\mathbb{Z})^n$ twisted by a Galois action and infinitesimal k-group whose functor of points has the form $R \rightsquigarrow \{r \in R | r^n = 1\}$ twisted by a Galois action. In fact, when k is perfect we can decompose $\Phi[p^\infty] = \Phi[p^\infty]_{\acute{e}t} + \Phi[p^\infty]_{inf}$ in a canonical fashion. The étale part has a unique lift by Hensel's lemma, and the infinitesimal part has a unique lift by Cartier duality. Combined this gives a canonical lifting of $\Phi[p^\infty]$ to Artinian local rings R ; the limit over R gives rises to an actual abelian scheme and partially inverts the reduction functor. In particular, if $E \longrightarrow \mathrm{Spec}(\mathfrak{o})$ is an ordinary elliptic curve, it has a canonical lift $\tilde{E} \longrightarrow \mathrm{Spec}(\mathcal{O})$ whose p-divisible group splits as a sum of an étale group and a connected group.

2) Φ has no p-torsion points. In this case, the ind-object Φ is to be understood as the formal group of Φ^*, and the theorem says that lifting Φ amounts to lifting its formal group. This is the case of interest when we want to lift a supersingular elliptic curve $E \mapsto \mathrm{Spec}(\mathfrak{o})$

We also note that a canonical lift corresponds to a lift on the level of abelian variety [7].

Gross [3] investigated the structure of quasi-canonical lifts of formal groups in more detail, which we summarize below: Let K be a local field complete with respect to a

discrete valuation, let A be its ring of integers, let π be a uniformiser of A and let $k := A/$. We assume that k is finite of characteristic p. Furthermore, assume that L/K is a separable quadratic extension. Now, let G be a formal A-module of height 2 over k, and note that the endomorphism ring $End_A(G)$ is isomorphic to a maximal order in a quaternion algebra over F. A formal A-module is a pair (G, g) where G is a commutative formal group of dimension 1 over k and $g : A \longmapsto End_k(G)$ is a homomorphism corresponding to reduction modulo π on the tangent spaces. Fix an embedding $\alpha : \mathcal{O} \hookrightarrow End_A(G)$ of the ring of integers of L such that the induced action on $\mathrm{Lie}(G)$ is compatible with reduction modulo $\mathfrak{m}$. This gives G the structure of a formal $\mathcal{O}$-module. Finally, let M/L be the completion of the maximal unramified extension of L, let W be its ring of integers and let $\mathfrak{m}$ be the maximal ideal of W.

Theorem 2 *There is a formal $\mathcal{O}$-module $\underline{G}$ over W which reduces to $G \mod \mathfrak{m}$. Moreover, $\underline{G}$ is unique up to W-isomorphism.*

Proof: From the work of Lubin and Tate, there exist a formal $\mathcal{O}$-module $\underline{G}$ of height 1. $\underline{G}$ must then become isomorphic to G over $W/\mathfrak{m}W$ because the latter is separably closed. Moreover, $\underline{G}$ is the unique lifting since height 1 formal modules have a trivial deformation space [4]. □

We call $\underline{G}$ a canonical lifting of the pair (G, α). This is consistent with the usage above as, in light of Theorem 2, the choice of an embedding $\alpha : \mathcal{O} \hookrightarrow End(G)$ trivialise the formal moduli space. Note that as $\underline{G}$ is a height 1 $\mathcal{O}$-module, $End_W(\underline{G}) = \mathcal{O}$. The work of Gross also gives a very useful explicit description of the endomorphism over the intermediate Artinian local rings $W/\mathfrak{m}^n W$, which will be used to ensure that we can construct the canonical lifting stepwise.

Theorem 3 *(Gross [3]) Let $R_n = End_{W/\mathfrak{m}^n W}(\underline{G})$. Then*
1) We have a system of compatible injections $R_n \hookrightarrow R_{n-1} \hookrightarrow R_{n-2} \hookrightarrow ... \hookrightarrow R_0$

2) $R_n = \mathcal{O} + \mathfrak{m}^n R_0$

3) R_0 *is a maximal order in a quaternion algebra*

A third result of Gross's 1986 article will be useful for our purpose. The ring R_0 has many subrings isomorphic to non-maximal orders in an imaginary quadratic field, and it is natural to ask whether these too can be lifted. For some $\ell \neq p$, let T be the Tate module at ℓ of $\underline{G}$ over M, and let $T \subset T' \subset T \otimes_{\mathcal{O}} L$ be an A-module with $[T' : T] < \infty$. Then T' gives rise to a formal A-module $\underline{G'}$ isogenous to $\underline{G}$ over $\bar{M}$. In fact, there is an explicit formula due to Serre that can be found in Gross's article which gives such an isogeny. This isogeny is rational over the integers W' of the finite extension M' corresponding to $Stab(T') \subset Gal(\bar{M}|M)$. The ring $\mathcal{O}' := End_{W'}(\underline{G'})$ is an order in $\mathcal{O}$, and consists of the endomorphisms fixing the A-module T'. As $A \subset \mathcal{O}'$, we deduce that $\mathcal{O}' = A + \mathfrak{m}^s\mathcal{O}$ for some uniquely determined $s \geq 0$. The case $s = 0$ is that of the canonical lift, and for $s \geq 1$, we say that $\underline{G'}$ is a quasi-canonical lift of level s.

Theorem 4 *(Gross 1986)*

1) There exist quasi-canonical lifts of all levels

2) The lifts of level s are rational over W'*, and* $Gal(M'|M)$ *acts simply transitively on them.*

Note that 1) implies the existence of lifts for any subring of rank 2 in $End_A(G)$, since they are contained in a maximal subring of rank 2. Moreover, 2) implies that the (potentially formal) moduli of lifts of level s is finite, so both usages of the term 'quasi-canonical' are consistent.

1.2 Complex Multiplication

Elliptic curves that arise as lifts have special number theoretic properties which are explained by the theory of complex multiplication (CM), so we give a brief review of the parts of the theory that are relevant. All results in this section are adapted from [9]. While it may seem strange to use complex analytic methods to study something that is a priori

only p-adic, the fact that elliptic curves having exceptional endomorphism correspond to specific algebraic points in a moduli space defined over $Spec(\mathbb{Z})$ implies that a lift as above corresponds abstractly to a curve of the form $E_{\mathbb{Q}_p} := E \times_K Spec(\mathbb{Q}_q)$ for a finite extension K of $\mathbb{Q}$ embedded into a finite extension $\mathbb{Q}_q$ of $\mathbb{Q}_p$. Consequently, we can apply the theory of complex multiplication to $E_{\mathbb{C}}$ to gain insight into our curve.

The main result concerning CM curves that interest us is the following:

Theorem 5 *Let $E/\mathbb{C}$ be an elliptic curve with CM by the ring of integers R_K of an imaginary quadratic field $K/\mathbb{Q}$. Then*
1) $j(E)$ is an algebraic integer.
2) $(K(j(E))|K)$ is the maximal abelian unramified extension of K

We fix some notation: Let $\mathcal{ELL}(R) := \frac{\{\text{Elliptic curves } E/\mathbb{C} \text{ with } End(E) \simeq R\}}{\{\text{Isomorphisms over } \mathbb{C}\}}$ and let $\mathcal{CL}(R)$ be the class group of R. K denotes an imaginary quadratic field, while R_K denote its ring of integers. Given a lattice $\Lambda \subset \mathbb{C}$, we denote the corresponding complex elliptic curve by $E_\Lambda \cong \mathbb{C}/\Lambda$, and identify its endomorphism ring with $\{\alpha \in \mathbb{C} | \alpha\Lambda \subset \Lambda\}$. The basic results that we'll need are the following:

Proposition 6 *Let $\Lambda \subset \mathbb{C}$ be a lattice such that $E_\Lambda \in \mathcal{ELL}(R_K)$ and let $\mathfrak{a}, \mathfrak{b}$ be nonzero fractional ideals in R_K. Then*
(i) $\mathfrak{a}\Lambda$ is a lattice such that $E_{\mathfrak{a}\Lambda} \in \mathcal{ELL}(R_K)$.
(ii) $E_{\mathfrak{a}\Lambda} \simeq E_{\mathfrak{b}\Lambda}$ if and only if $[\mathfrak{a}] = [\mathfrak{b}]$ in $\mathcal{CL}(R_K)$.
(iii) $\mathcal{CL}(R_K)$ acts simply transitively on $\mathcal{ELL}(R_K)$

Proof: (i) By assumption, $R_K\Lambda = \Lambda$. Choosing $d, d' \in \mathbb{Z}$ such that $dR_K \subset \mathfrak{a} \subset \frac{1}{d'}R_K$, which we can do by the definition of a fractional ideal, and multiplying by our lattice, we get that $d\Lambda \subset \mathfrak{a}\Lambda \subset \frac{1}{d'}\Lambda$, establishing that $\mathfrak{a}\Lambda$ is indeed a lattice. Moreover, given $\alpha \in \mathbb{C}$, we deduce from the group structure on the set of fractional ideals of R_K that

$$\alpha\mathfrak{a}\Lambda \subset \mathfrak{a}\Lambda \iff \mathfrak{a}^{-1}\alpha\mathfrak{a}\Lambda \subset \mathfrak{a}^{-1}\mathfrak{a}\Lambda \iff \alpha\Lambda \subset \Lambda \iff \alpha \in R_K$$

(ii) Say $E_{\mathfrak{a}\Lambda} \simeq E_{\mathfrak{b}\Lambda}$. Then we have $\mathfrak{a}\Lambda = c\mathfrak{b}\Lambda$ for some $c \in \mathbb{C}^*$. Multiplying by $\mathfrak{a}^{-1}$ and $c^{-1}\mathfrak{b}^{-1}$, we see that both $\mathfrak{a}c^{-1}\mathfrak{b}^{-1}$ and its inverse map Λ into itself, hence both are contained in $End(E_{\mathfrak{a}}) \simeq R_K$. We conclude that $\mathfrak{a} = c\mathfrak{b} \iff [\mathfrak{a}] = [\mathfrak{b}]$.

(iii) Now, define the action $\mathcal{CL}(R_K) \curvearrowright \mathcal{ELL}(R_K)$ by $[\mathfrak{a}] * E_\Lambda = E_{\mathfrak{a}^{-1}\Lambda}$. By (ii), the stabilizer of any isomorphism class is trivial, so it remains to show that this action is transitive. Given two isomorphism classes, take two representatives $E_{\Lambda_1}, E_{\Lambda_2}$. Choose $\lambda_i \in \Lambda_i - \{0\}$ and define $\mathfrak{a}_i := \frac{1}{\lambda_i}\Lambda_i$. Then $\mathfrak{a}_i \subset K$ is a finitely generated R_K-module, hence a fractional ideal, and $\frac{\lambda_2}{\lambda_1}\mathfrak{a}_2\mathfrak{a}_1^{-1}\Lambda_1 = \Lambda_2$. As a result, $[\mathfrak{a}_1\mathfrak{a}_2^{-1}] * E_{\Lambda_1} \simeq E_{\Lambda_2}$. $\square$

Proposition 7 *Let $E/\mathbb{C}$ be an elliptic curve.*

(i) If $\sigma \in Aut(\mathbb{C})$, then $End(E^\sigma) \simeq End(E)$.

(ii) If E has CM by R_K, then $[\mathbb{Q}(j(E)) : \mathbb{Q}] \leq h_K$ and therefore $j(E) \in \bar{\mathbb{Q}}$.

(iii) $\mathcal{ELL}(R_K) := \frac{\{\text{Elliptic curves } E/\bar{\mathbb{Q}} \text{ with } End(E) \simeq R_K\}}{\{\text{Isomorphisms over } \bar{\mathbb{Q}}\}}$

Proof: (i) Since σ is compatible with isomorphisms between Weierstrass models, it is clear that if $\phi \in End(E)$ then $\phi^\sigma \in End(E^\sigma)$.

(ii) Thinking of E^σ as being obtained from a Weierstrass model of E by letting σ act on the coefficients, we see that $j(E^\sigma) = j(E)^\sigma$. On the other hand by (i) $E^\sigma \in \mathcal{ELL}(R_K)$ and j uniquely determines the isomorphism class of an elliptic curve over $\mathbb{C}$, so by Proposition 6 $j(E)^\sigma$ takes on at most h_K values as σ ranges over $Aut(\mathbb{C})$. Thus $[\mathbb{Q}(j(E)) : \mathbb{Q}] \leq h_K$.

(iii) By the previous part, any isomorphism class in $\mathcal{ELL}(R_K)$ is represented by a curve defined over $\bar{\mathbb{Q}}$, so the natural map $\{\text{Elliptic curves } E/\bar{\mathbb{Q}} \text{ with } End(E) \simeq R_K\} \longmapsto \mathcal{ELL}(R_K)$ surjects. Since $\bar{\mathbb{Q}}$ is algebraically closed, two elliptic curves over $\bar{\mathbb{Q}}$ are $\mathbb{C}$-isomorphic if and only if they are $\bar{\mathbb{Q}}$-isomorphic [8]. $\square$

By Proposition 7(iii), $G(\bar{K}|K)$ acts naturally on $\mathcal{ELL}(R_K)$, and thus by fixing a curve $E \in \mathcal{ELL}(R_K)$ we obtain a well-defined map $\phi : G(\bar{K}|K) \longmapsto \mathcal{CL}(R_K)$ uniquely characterized by $\phi(\sigma) = [\mathfrak{a}] \iff [\mathfrak{a}] * E \simeq E^\sigma$. This is actually a group homomorphism, which turns out to be independent of our choice of E.

As noted in Theorem 5, a bit more is true. Namely, for a CM curve E, $j(E)$ is actually an integral element of $\bar{\mathbb{Q}}$. Below we present a conceptual proof of this fact that relies

on ℓ-adic techniques, but we note that the minimal polynomial of $j(E)$ can be explicitly constructed, using for examples complex analytic methods and modular forms.

Proposition 8 *Let L be a number field and E/L be an elliptic curve with CM. Then E has potentially good reduction at every prime v of L, and $j(E)$ is an algebraic integer.*

Proof: We want to apply the following corollary to the criterion of Néron-Ogg-Shafarevitch: E/L has potentially good reduction if and only if there exists some $\ell \neq \mathrm{char}(L)$ such that the action of the inertia group $I(\bar{L}_v|L_v)$ on the Tate module $T_\ell(E)$ factors through a finite quotient [8]. In other words, we need to show that the image of $I(\bar{L}_v|L_v) \hookrightarrow Aut(T_\ell(E))$ is finite for some prime $\ell \neq p$. The target is abelian, and by local class field theory we have a compatible isomorphism $I(L_v^{ab}|L_v) \simeq R_v^*$, so it suffices to show that the image of the latter is finite. But we have a diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & R_{v,1}^* & \longrightarrow & R_v^* & \longrightarrow & R_v/\mathfrak{m}_v^* & \longrightarrow & 0 \\ & & & & \downarrow & & & & \\ 0 & \longrightarrow & GL_2(\mathbb{Z}_l)_1 & \longrightarrow & Aut(T_\ell(E)) & \longrightarrow & GL_2(\mathbb{Z}/l\mathbb{Z}) & \longrightarrow & 0 \end{array}$$

Since $R_{v,1}^* \simeq \hat{\mathbb{G}}_m(\mathfrak{m}_v)$ is a pro-p-group while $GL_2(\mathbb{Z}_l)_1$ is a pro-ℓ-group, $\ell \neq p$ implies that the image of the first is disjoint from the image of the second, hence $\#im(R_{v,1}^*) \leq \#GL_2(\mathbb{Z}/l\mathbb{Z}) < +\infty$. But $R_v/\mathfrak{m}_v$ is also finite, hence $im(R_v^* \mapsto Aut(T_\ell(E))$ must also be finite, as desired.

Now, if we take an equation for E with coefficients in $\mathbb{Q}(j(E))$, we see that E has potentially good reduction at every prime, hence by [9] $j(E)$ is an algebraic integer. $\square$

To explain why $j(E)$ generates the Hilbert class field, we'll need some notation and terminology from global class field theory. Given a finite abelian extension $(L|K)$, for any unramified prime $\mathfrak{p} \in Spec(R_K)$ we denote the corresponding Frobenius element by $\sigma_\mathfrak{p} \in G(L|K)$. If $\mathfrak{c} \subset R_K$ is an ideal divisible by all primes of R_K which ramify in R_L, we define $I(\mathfrak{c}) := \{\text{fractional ideal of } K \text{relatively prime to } \mathfrak{c}\}$. We define the Artin symbol by

$$(\tfrac{L/K}{\cdot}) : I(\mathfrak{c}) \longmapsto G(L|K) : \mathfrak{a} \longmapsto (\tfrac{L/K}{\mathfrak{a}}) := \Pi \sigma_{\mathfrak{p}}^{v_{\mathfrak{p}}(\mathfrak{a})}$$

with the product taken over the primes of R_K (note that only finitely many terms are nontrivial). We will take for granted the technical result that there exist a finite set of primes $S \subset Spec(\mathbb{Z})$ such that if $p \notin S$ splits in R_K, say as $(p) = \mathfrak{p}\mathfrak{p}'$, then $\phi(\sigma_{\mathfrak{p}}) = [\mathfrak{p}]$. We break down the proof that $(K(j(E))|K)$ is the maximal unramified abelian extension of K into 3 steps.

Proposition 9 *Let $(L|K)$ be the finite extension corresponding to the kernel of $G(\bar{K}|K) \longrightarrow \mathcal{CL}(R_K)$ (i) $L = K(j(E))$ is an abelian extension of K*
(ii) L is an unramified extension
(iii) $[L : K] = h_K$

Proof: (i) Since $\mathcal{CL}(R_K)$ acts simply transitively, the definition of ϕ yields
$\ker \phi = \{\sigma \in G(\bar{K}|K) | \phi(\sigma) * E = E\} = \{\sigma \in G(\bar{K}|K) | E = E^{\sigma}\} = \{\sigma \in G(\bar{K}|K) | j(E) = j(E)^{\sigma}\} = G(\bar{K}|K(j(E))$. Hence, $L = K(j(E))$ by elementary Galois theory. Moreover, $(L|K)$ is abelian as $G(L|K) \hookrightarrow \mathcal{CL}(R_K)$ is injective.

(ii) Consider the map $I(\mathfrak{c}_{L/K}) \longmapsto G(L|K) \longmapsto \mathcal{CL}(R_K)$ obtained by composing the Artin symbol with ϕ. For any fractional ideal $[\mathfrak{a}]$, by Dirichlet theorem on arithmetic progression we can find some prime ideal $\mathfrak{p} \notin S$ such that $[\mathfrak{p}]$ is in the same ideal class as $[\mathfrak{a}]$. Using the technical result mentioned above, we then have for some $\alpha \cong 1 \mod \mathfrak{c}_{L/K}$ that

$$\phi((\frac{L/K}{\mathfrak{a}})) = \phi((\frac{L/K}{\alpha\mathfrak{p}})) = \phi((\frac{L/K}{\mathfrak{p}})) = [\mathfrak{p}] = [\mathfrak{a}]$$

But ϕ is injective, so $\frac{L/K}{\cdot}$ vanishing on all principal ideal. It follows that $\mathfrak{c}_{L/K} = (1)$, but every prime that ramifies in $(L|K)$ divides the conductor, so $(L|K)$ must actually be unramified.

(iii) It is clear that the map $I(\mathfrak{c}_{L/K}) = I(1) \longmapsto \mathcal{CL}(R_K)$ is surjective, thus $[L : K] = h_K$.
□

Chapter 2

Canonical lifts

2.1 Lifting curves over $\mathbb{F}_q - \mathbb{F}_{p^2}$

The existence of a canonical lift in this case is a classical [1] (p. 424), and so our approach is based on the following result, which reduces the problem of finding a canonical lift of an elliptic curve $\bar{E}$ over $\mathbb{F}_q$ to the problem of finding a curve E reducing to $\bar{E}$ and a lift $E \mapsto E^\sigma$ of the Frobenius morphism.

Theorem 10 *(Serre, Tate) Let q be a fixed power of p, let $\bar{j} \in \mathbb{F}_q - \mathbb{F}_{p^2}$, let $\mathbb{Q}_q$ be the unramified extension of $\mathbb{Q}_p$ with residue field $\mathbb{F}_q$ and let $\sigma : \mathbb{Q}_q \longmapsto \mathbb{Q}_q$ be the Frobenius endomorphism. Then there exist a $\tilde{j} \in \mathbb{Q}_q$ above $\bar{j}$ corresponding to a canonical lift $E_{\tilde{j}}$ of $E_{\bar{j}}$, and this $\tilde{j}$ is uniquely characterised by being a solution to $\Phi_p(\tilde{j}, \sigma\tilde{j}) = 0$ where Φ_p is the p-th classical modular polynomial.*

With this theorem, what remains to be done is to find an effective method to find the corresponding points on the modular curve $X_0(p)$. For this, we use a standard iterative method closely related to Newton's method [1] (Ch. 12), which will be amenable to generalization.

Let j denote a canonical lift and say we have an estimate $j_N \equiv j \mod p^N$. Denoting the p-th classical modular polynomial by $\Phi_p(y, z)$, and letting $\delta_N = \frac{j - j_N}{p^N}$, we take the Taylor expansion of Φ_p about $(j, \sigma j)$ to find

$$0 \equiv \Phi_p(j_N, \sigma j_N) + p^N(\Delta_y \delta_N + \Delta_z \sigma \delta_N) \mod p^{2N}$$
$$0 \equiv \frac{\Phi_p(j_N, \sigma j_N)}{p^N} + \Delta_y \delta_N + \Delta_z \sigma \delta_N \mod p^N$$

where $\Delta_y := \partial_y(\Phi_p)|_{(j_N, \sigma j_N)}$ and $\Delta_z := \partial_z(\Phi_p)|_{(j_N, \sigma j_N)}$ are the partial derivatives.

If $v_p(\Delta_y) > v_p(\Delta_z)$ and $v_p(\Phi(j_N, \sigma j_N)) \geq v_p(\Delta_z) + N$, dividing the entire equation by $p^{v_p(\Delta_z)}$ gives an Artin-Schreier equation i.e an equation of the form $\alpha\sigma(x) + \beta x + \gamma = 0$, with $\alpha \in \mathbb{Z}_q^\times$ and $\beta, \gamma \in \mathbb{Z}_q$. If we can find an integral solution δ', setting $x_{2N - v_p(\Delta_z)} = x_N + p^N \delta'$, we get $\Phi(x_{2N-v_p(\Delta_z)}, \sigma x_{2N-v_p(\Delta_z)}) \equiv 0 \mod p^{2N}$. Moreover, if $N > v_p(\Delta_z)$, the updated partial derivatives will still satisfy the conditions on their valuation above, so we can iterate this process to approximate j to an arbitrary precision p^M using $O(log(M))$ recursive calls.

We now investigate when an Artin-Schreier equation has a solution over $\mathbb{Z}_q$. To do this, we leverage the simple fact the Frobenius of an unramified extension of degree d satisfies $\sigma^d = \text{id}$. Note that without loss of generality we can take $\alpha = 1$ and then rewrite the equation as $\sigma(x) + a_1 x + b_1 = 0$. Applying σ to both side, we can use recursion to write $\sigma^k(x) = a_k x + b_k$ for $a_k, b_k \in \mathbb{Z}_q$. Then $x = \sigma^d(x) = a_d x + b_d$, so if $a_d \neq 1$, or equivalently $Nm_{\mathbb{Q}_p}^{\mathbb{Q}_q}(a_1) \neq 1$, the unique solution in $\mathbb{Q}_q$ is $x = \frac{b_d}{1 - a_d}$. In addition, this solution is integral if and only if $1 - a_d \in \mathbb{Z}_q^\times$, which is definitely the case when $v(a_1) > 0$. Thus, what remains is to find an efficient algorithm to solve Artin-Schreier equations.

A solution to this problem is given by the Lercier–Lubicz algorithm, an implementation of which can be found in Chapter 3. It is based on repeated squaring. Namely, since the Frobenius is an endomorphism, we have the formula

$$\sigma^{n+k}(x) = \sigma^k(a_n)\sigma^k(x) + \sigma^k(b_n)$$

from which we easily deduce that

$$a_{n+k} = \sigma^k(a_n),\ b_{n+k} = \sigma_k(b_n) + \sigma^k(a_n) b_k$$

Consequently, we can compute a_d, b_d using $O(log(d))$ recursive calls, each of which involves $O(1)$ additions, multiplications, and applications of a Frobenius endomorphism.

While the time complexity of these three operations depend on low-level implementation details concerning, for example, how p-adic values are represented, in all efficient implementation the time complexity will be $O(poly(N))$ for some polynomial of small degree.

In light of the explanation above, we conclude the following more constructive version of Theorem 10

Theorem 11 *Let $\bar{j} \in \mathbb{F}_{p^d} - \mathbb{F}_{p^2}$ and let $\tilde{j} \in \mathbb{Q}_{p^d}$ above $\bar{j}$ be the j-invariant of the canonical lift. Then there exist an algorithm with time complexity $O(poly(N)log(d))$ that takes as input $(\bar{j}, N)$ and returns as output a p-adic integer j_N such that $v_p(\tilde{j} - j_N) \geq N$.*

2.2 The case of $\mathbb{F}_p$

2.2.1 Endomorphism of degree p

We use the following classical results concerning modular curves:

1. $\Phi_p(x, y) \equiv (x^p - y)(y^p - x) \mod p$
2. $\deg(\Phi_p(x, x)) = 2p$

From these, we see that over $\overline{\mathbb{Q}_p^{alg}}$, $\Phi_p(x, x)$ has precisely two roots with multiplicity congruent modulo $\mathfrak{m}$ to a residue class r $\in \{0, 1, ..., p-1\}$. Let $p_r(x) \in \bar{\mathbb{Q}_p^{alg}}[x]$ be the quadratic polynomial whose roots are the roots of $\Phi_p(x, x)$ congruent to r.

Lemma 12 *Let F be a formal group over a local field K of characteristic 0 with uniformiser π, and assume $v_\pi(a) = 0$. Then the equation $[a]x^2 + [b]x = [\pi]$, where products denote compositions of power series, has a solution in $\mathcal{O}_K[[T]]$ of height 1 if and only if $v_\pi(b) = 0$.*

Proof: Recall that $[a] = aT + O(T^2)$, and likewise for $[b]$. Therefore, if the desired power series $S = \sum_{n=1}^{\infty} c_n T^n$ exists, by comparing the first term we get that $c_1(ac_1 + b) = \pi$. As S has height 1, $v_\pi(c_1) = 1$ so $\frac{c_1}{\pi}(ac_1 + b) = 1 \implies v_\pi(ac_1 + b) = 0$, hence the condition $v_\pi(b) =$

0 is clearly necessary. In fact, it is equivalent to the existence of an approximate solution to order $O(T^2)$.

To see that it suffices, assume that we can solve for $c_1, ..., c_{n-1}$. Then the only possibility for c_n is

$$c_n = (ac_1 + b)^{-1} * ([p][n+1] - \sum_{k\in\mathbb{N},|j|=n+1} c_k(d_{j_1}...d_{j_k}))$$

where $[\pi][j]$ is the jth coefficent of $[p]$ and d_j is jth coefficent of $[a]S + [b]$. This is well-defined since $(ac_1 + b)$ is a unit and all the terms which occur on the RHS are uniquely determined by $c_1, ..., c_{n-1}$. Taking the limit, we obtain the desired solution S. □

Theorem 13 *1. The factorization $\Phi_p(x, x) = \Pi_{r\in\mathbb{F}_p} p_r(x)$ can be realized over $\mathbb{Q}_p$*

2. $p_r(x)$ splits over $\mathbb{Q}_p[x]$ if and only if the curve $E(r)/\mathbb{F}_p$ has a canonical lift over $\mathbb{Q}_p$ if and only if $E(r)/\mathbb{F}_p$ is ordinary. In this case $p_r(x)$ has a double root and the lift is unique. Otherwise, $p_r(x)$ has two distinct roots which lie in the ramified extension of degree 2.

Proof: Given r $\in \{0, 1, ..., p-1\}$, $\Phi(x - r, x - r)$ has precisely two roots in $\mathfrak{m}$, and all other roots are units. Thus, this polynomial has Newton slopes $(i, i, 0, .., 0)$ for some $i \in \mathbb{Q}_{>0}$. Consequently, $\Phi(x - r, x - r)$ factors in $\mathbb{Q}_p[x]$ as $f(x)g(x)$ for some quadratic polynomial f whose roots are nonunits [6]. Shifting by $x \mapsto x + r$, we get that $\Phi_p(x, x) = p_r(x)g(x + r)$. Repeating this for all residue classes, $\Phi_p(x, x) = h(x)\Pi_{r\in\mathbb{F}_p} p_r(x)$ for some $h(x) \in \mathbb{Q}_p[x]$, but $\Phi_p(x, x)$ and $\Pi_{r\in\mathbb{F}_p} p_r(x)$ are both monic polynomial of degree 2p, which proves 1.

Let $(E(\tilde{r})/K)$ be a lift of $(E(r), \sigma)$ with deg(σ) = p. Without loss of generality we can assume that K is a smallest field over which such an elliptic curve exists. Then $K = \mathbb{Q}_p$ if and only if $p_r(x)$ splits in $\mathbb{Q}_p[x]$. On the other hand, denoting the formal group of an elliptic curve E by F_E, we have a commutative diagram

$$\begin{array}{ccc} End_K(E(\tilde{r})) & \longrightarrow & End_K(F_{E(\tilde{r})}) \\ \downarrow & & \downarrow \\ End_{\mathbb{F}_p}(E(r)) & = & End_{\mathbb{F}_p}(F_{E(r)}) \end{array}$$

As the bottom row is a natural identification, both rings in the top row correspond to the same order in $End_{\mathbb{F}_p}(E(r))$. Moreover, by the proof of Lemma 12 the endomorphism σ of formal groups is defined over K. If σ has minimal polynomial $x^2 + bx + c$, then by our choice of σ,

$$v_p(deg(c)) = 2$$

so $\tilde{\sigma}^2 + [b]\tilde{\sigma} = [c'][p]$ where $[c']$ is a unit. Thus by Lemma 12 the lift of Frobenius for the formal group can be defined over $\mathbb{Q}_p$ if and only if $v_p(b) = 0$. But $E(r)$ is supersingular if and only if b is divisible by p [8].

Say $j_0, j_1 \in \mathbb{Q}_p$ are the two roots of $p_r(x)$. Assume that $v_p(j_0 - j_1) = k \in \mathbb{N}$. Since the second partial derivative of $\Phi_p(x, x)$ evaluated at j_0, j_1 is a unit, we can expand $\Phi_p(x, x)$ to second order about j_0, j_1 to get

$$(\partial_x \Phi_p \mid_{x=j_0})(j_1 - j_0) + (\partial_x^2 \Phi_p \mid_{x=j_0})(j_1 - j_0)^2 + O(p^{2k+1})$$
$$(\partial_x \Phi_p \mid_{x=j_1})(j_0 - j_1) + (\partial_x^2 \Phi_p \mid_{x=j_1})(j_0 - j_1)^2 + O(p^{2k+1})$$

On the other hand, by expanding the partial derivative about j_0, the second line becomes

$$(\partial_x \Phi_p(x, x) \mid_{x=j_0})(j_0 - j_1) + (\partial_x^2 \Phi_p(x, x) \mid_{x=j_1})(j_1 - j_0)^2 - (\partial_x^2 \Phi_p(x, x) \mid_{x=j_0})(j_1 - j_0)^2$$
$$\equiv (\partial_x \Phi_p(x, x) \mid_{x=j_0})(j_0 - j_1) \mod p^{2k+1}$$

and adding this together, we get that

$$(\partial_x^2\ \Phi_p(x,x)\mid_{x=j_1})(j_1-j_0)^2 \equiv 0 \mod p^{2k+1}$$

which is absurd. It follows that $v_p(j_0 - j_1) = \infty$ i.e. that $j_0 = j_1$. Finally, if $p_r(x)$ does not split, it is irreducible, hence separable. It must also generate the unique ramified extension of degree 2 since the Frobenius endomorphism acts trivially on its roots. □

As it turns out, $\Phi_p(x, y)$ also controls the structure of the set of quasi-canonical lifts when the corresponding orders have index p. Fix an order $\mathcal{O}$, not necessarily maximal, and let γ denote a quasi-canonical lift.For any $j \in \mathbb{Q}_p^{alg}$, let $\mathcal{I}(j) := \{j' \in \mathbb{Q}_p^{alg} | \Phi(j, j') = 0\}, \mathcal{L}_n = \{j \in \mathbb{Q}_p^{alg} | End(j(E)) = \mathbb{Z} + p^n\mathcal{O}\}$. Let $K_0 = \mathbb{Q}_p[\gamma]$ and we define K_n to be its totally ramified abelian extension of degree p^n.

Theorem 14 *Every $j \in \mathcal{L}_n$ is in contained in $\mathcal{I}(j')$ for precisely one $j' \in \mathcal{L}_n$. If $\mathbb{Q}_p[\gamma]$ is ramified, $(K_{n-1}(j)|K_{n-1})$ is a totally ramified extension of degree p. Otherwise, $K_0(j)$ is the maximal tamely ramified extension.*

Proof: Because each quasi-canonical lift of level n is p-isogenous to a quasi-canonical lift of level n-1 [3], $\cup_{j\in\mathcal{L}_n} I(j) - \mathcal{L}_{n-1} \supset \mathcal{L}_{n+1}$. From the congruence $\Phi(x, y) \cong (x^p - y)(y^p - x) \mod p$ we see that the roots of $\Phi(x, j')$ lie in a totally ramified extension of $K_0(j')$. By induction, one of these roots lie in a proper subextension of K_{n-1}, hence the remaining roots must be congruent to one of the roots of $x^p - j'$. We easily deduce from this that if $j' \notin \mathbb{Q}_p$ then $\frac{\Phi(x+a,j')}{(x+a-j'')}$ is Eisenstein of degree p for some $a \in \mathbb{Q}_p$. Thus $K_{n-1}(j) = K_n$, and in particular all conjugates of $E(j)$ are p-isogenous to $E(j')$. But conjugates of $E(j)$ are also quasi-canonical lifts. Indeed, the isomorphism $End(E(j)) \equiv End(E(\sigma j))$ induced by the action of $Gal(K_n|K_0)$ on coefficient commutes with reduction mod π_n, and is trivial mod π_n. Thus,

$$p^n \leq \#\mathcal{L}_n \leq \#\cup_{j\in\mathcal{L}_n} I(j) - \mathcal{L}_{n-1} \leq p * p^{n-1}$$

Finally, if $\gamma \in \mathbb{Q}_p$, then $\frac{\Phi(x,\gamma)}{(x-\gamma)^2}$ is a polynomial over $\mathbb{Q}_p$ of degree $p - 1$ congruent to $x^{p-1} - 1$, so its roots correspond to the tamely ramified part of $\mathbb{Q}_p^{alg}$. Since $gcd(p, p-1) = 1$, we see that the valuations of the roots of the centered polynomial $\frac{\Phi(x+a,j')}{(x+a-j')}$ satisfy $\langle v(j + a)\rangle = \langle v(j' + a)\rangle$. Therefore $K_0(j) = K_0(j')$. □

Corollary 15 *Let j be a quasi-canonical lift of Frobenius of level $n > 1$. Then the extension $\mathbb{Q}_p[j]/\mathbb{Q}_p$ is abelian and corresponds to μ_{p-1} if $E(j)$ reduces to an ordinary elliptic curve, and corresponds to $\{\pm 1\}U^{(1)}/U^{(n)}$ if $E(j)$ reduces to a supersingular elliptic curve.*

2.2.2 Numerical applications

Theorem 13 reduces the problem of computing canonical lifts to that of finding a root of a polynomial in $\mathbb{Q}_p(\sqrt{p})$. Hence, in the supersingular case, we can proceed in an algorithmic fashion as follows: Let $K = \mathbb{Q}_p(\sqrt{p})$ be a ramified extension of degree two, let $E(r)$ be the supersingular elliptic curve over $\mathbb{F}_p$ with j-invariant $r \in \mathbb{F}_p$ and let j_0, j_1 the two distinct roots of $p_r(x)$ in K. Given $j \in \mathfrak{O}_K$ such that $v_\pi(j_0 - j) > v_\pi(j_1 - j) > 0$, j_0 can be computed by applying Hensel's lemma to $\Phi_p(x, x)$. Indeed, writing $f := \Phi_p(x, x)$ as a product and its derivative as a sum of products, it is clear that $v_p(f(j_0)) > 2v_p(f'(j_0))$ so that the conditions of the general univariate Hensel's lemma are satisfied. The precision doubles at each step, so to find a root to precision N we need $O(log(N))$ steps assuming unit cost for arithmetic operations.

In the ordinary case, Hensel's lemma cannot be applied directly to $\Phi_p(x, x)$ to find an ordinary j-invariant *j*. But *j* is also a root of the derivative of $\Phi_p(x, x)$, and one might hope that it has lower multiplicity, since this is true for a generic polynomial. The derivative of the modular polynomial is of the form $2(x^p - x)(px^{p-1} - 1) + O(p)$, and since the Newton slopes increase monotonically the last $2p - 1 - p = p - 1$ slopes must be greater than 1. That is, $\partial_x f$has at most p integral roots. But every lifted j-invariant is an approximate root of $\partial_x f$. Consequently, distinct integral roots of $\partial_x f$lie in distinct residue class, so if j is the lift of an ordinary elliptic curve, j is a root of $\partial_x f$and $\partial_x^2 f(j) \neq 0$. Hence we can apply Hensel's lemma to $\partial_x f$to obtain the canonical lift. In general, there is a robust version of the Newton-Hensel root-finding method that handles the case where some roots may have multiplicity > 1.

The reason this works is that if $(x - r)^k | f, (x - r)^{k-1} | f'$ so h has only simple roots, which are also roots of f. By looking at the degree, it is clear that h is not constant,

Algorithm 1 Newton-Hensel, robust

```
1: procedure NH-R
2:     Roots = []
3:     for deg(f) ≥ 1 do
4:         f' ← Differentiate(f)
5:         g ← GCD(f, f')
6:         h ← f/g
7:         for i in {1, ...deg(h)} do
8:             r ← Hensel(f, r_i).
9:             Add r to Roots
10:            f ← Divide(f, (x − r))
11:    Return Roots
```

so every iteration of the outer loops find new roots of f. Computing the gcd can be done efficiently with, say, Euclid's algorithm, and likewise polynomial division can be done using long division, so for polynomials of fixed degree this robust version still runs in time $O(poly(N))$. This algorithm also illustrate a significant advantage of working over p-adic fields. Namely, polynomial division is numerically stable in the sense that if $r + O(p^N)$ is an approximate root of f, performing long division of f by $r + O(p^N)$ gives a polynomial whose roots are approximate roots of order $O(p^N)$. This contrasts with the case of archimedean fields, where polynomials with very close coefficients can have roots that are very far apart.

If f has distinct but very close roots, Algorithm 1 will still find the roots when given a sufficiently good approximation, but finding such an approximation by trial and error might be infeasible. We can use the ideas in the preceding algorithm to improve the naive version of Algorithm 1 when a polynomial has multiple close roots so that we merely need an initial value which has a neighborhood containing only one root.

Lemma 16 *Say we are given f with an approximate root r $r_0 + O(p^N)$ and with true roots $r_1, ..., r_n$ $r_o + O(p^M)$ for $M < N$. Let M' be the optimal such M. Take some $s \neq r$ congruent to $r_0, ..., r_n \mod p^M$. Then for $N < (n+1)M + v(n)$, the Newton-Hensel algorithm applied to $g := \frac{f}{(x-s)^n}$ has faster convergence to r_0, and for larger values of N it is equivalent to the Newton-Hensel algorithm applied to f*

Writing $f(r) = \Pi(r - r_i)$, we see that

$$v(f(r)) = N + nM'$$
$$v(f'(r)) = nM' + v(deg(f))$$

The rational function $g := \frac{f}{(x-s)^n}$ then also vanishes at r_0 and $v(g(r)) = N + n(M' - M)$. The valuation of its derivative $g'(r) = \frac{f'(r)}{(r-s)^n} - \frac{nf(r)}{(r-s)^{n+1}}$ tends to $v(f'(r)) - nv(r - s)$ as $r \mapsto r_0$. Indeed,

$$v(\frac{f'}{(r-s)^n}) = n(M' - M) + v(deg(f))$$
$$v(\frac{f}{(r-s)^{n+1}}) = N - M + n(M' - M) + v(n)$$

The first value is constant while the second is $O(N)$. Therefore, $v(\frac{f(r)}{f'(r)^2}) \leq v(\frac{g(r)}{g'(r)}^2)$, and this inequality is strict for $N \leq (n+1)M + v(n)$. $\square$

The description of $\mathcal{L}_n$ given by Theorem 14 suggests that an algorithm of the form could be used to recursively compute all quasi-canonical lifts of a supersingular elliptic

Algorithm 2 A hypothetical algorithm for quasi-canonical lifts of Frobenius

```
1: procedure QCL
2:     I(j') ←QCL(n − 1)
3:     for j' in I(j') do
4:         j ← Root(Φ(j', x)).
5:         if v_p(j) = n then
6:             Add j, ζj, ...ζ^{p−1}j to I(j)
       .
7:     Return I(j)
```

curve up to some level n using Root as a black-box subroutine which returns a root of minimal valuation. Unfortunately, while the realization of the wildly ramified extension of K_0 as a tower $K_0 \subset K_1 \subset ... \subset K_n \subset ...$ generated by j-invariant is arguably pleasing, this theoretical insight concerning the fields K_n strongly suggests that even finding a single element of $\mathcal{L}$ cannot be done efficiently. Indeed, any numerical implementation

would need $O([K_n : K_0]) = O(p^n)$ space just to store j to fixed precision, and the cost of arithmetic operation similarly increase exponentially as $n \to \infty$.

2.2.3 Endomorphism of degree *l*, and endomorphism of arbibtrary degree

Since the moduli of elliptic curves that have an isogeny of degree ℓ is defined over $\mathbb{Q}$, the j-invariant of these elliptic curves can be found in p-adic fields by finding the roots of a suitable modular polynomial as in the ℓ-adic case. In practice, this can easily be done using Algorithm 1 and Lemma 16 if needed. On a theoretical level, we can deduce results related to the theory of complex multiplication.

Theorem 17 *Say α generates a Dedekind domain in the endomorphism ring of a supersingular elliptic curve over $\mathbb{F}_\ell$. Let γ be the j-invariant of the corresponding canonical lift. For every prime p the extension $\mathbb{Q}_p[\alpha, \gamma]/\mathbb{Q}_p[\alpha]$ is trivial.*

Let K be a Galois closure of the extension $(\mathbb{Q}_p[\alpha, \gamma]|\mathbb{Q}_p[\alpha])$. For any $a \in \mathbb{Q}_p[\alpha]$, consider the symbol $\sigma = (a, K|\mathbb{Q})$. By uniqueness of the canonical lift its action on γ is uniquely determined by $[\alpha] \longmapsto [\alpha^\sigma]$ which is uniquely determined by $\alpha \longmapsto \alpha^\sigma$. In particular all norms of $\mathbb{Q}[\alpha]$ act trivially, so the result follows from the functoriality of the local Artin symbol. □

Combined with Theorem 14, we can deduce a well-known generalization of Theorem 5 using only p-adic methods.

Corollary 18 *The extension $\mathbb{Q}[\alpha, \gamma]/\mathbb{Q}[\alpha] := H/K$ of global fields is the ring class field of $\mathbb{Z}[\alpha]$*

An example: The polynomial Φ_5 splits over $\mathbb{Q}_7[x]$, and in fact over $\mathbb{Z}[x]$, into

$$(x + 884736)^2(x - 287496)^2(x - 1728)^2(x + 32768)^2(x^2 - 1264000x - 681472000)$$

Note that the roots $1728, -32768, 287496$ reduce to $1728 \cong_7 0$, which correspond to the unique supersingular elliptic curve over $\bar{\mathbb{F}}_7$, hence all of these roots correspond to a quasi-canonical lift. The polynomial Φ_3 splits completely over $\mathbb{Q}_7[x]$, and in fact over $\mathbb{Z}[x]$, into

$$x(x-54000)(x-8000)^2(x+32768)^2$$

so the roots corresponding to a quasi-canonical lift are $8000, -32768$.

Finally, recall that by Galois theory, an isogeny $E \mapsto E'$ of degree $l_1 l_2$ factors as a composite $E \mapsto E'' \mapsto E'$ of degree l_1, l_2 in at least two distinct ways. Thus, we can realize $\Phi_{l_1 l_2, red}$ as a subscheme of $X_0(l_1) \cap X_0(l_2) \subset \mathbb{P}^2$ with the same underlying space. Moreover, in general we can factor an isogeny as a composite of cyclic isogenies, so in the general case, to find a canonical lift of degree coprime to the characteristic of the residue field it suffices to solve a system of equation

$$\begin{aligned}
\Phi_{l_1}(x_1, x_2) &= 0 \\
\Phi_{l_2}(x_2, x_3) &= 0 \\
&\dots \\
\Phi_{l_n}(x_n, x_1) &= 0
\end{aligned}$$

Since the solutions correspond to singular points, the determinant of $J := (\partial_{x_i} \Phi_{l_j})_{(ij)}$ also vanishes at these points. However, every point in a generic intersection occur with multiplicity 1. Because p-adic balls of arbitrarily small radius are Zariski dense in $\mathbb{A}^N_{\mathbb{Q}_p}$, we may perform an arbitrarily small perturbation ϵ of the coefficents occuring in $*$ to obtain a nonsingular system of equation whose solution are arbitrarily close to those of the original one. Indeed, a solution x to the original system is an approximate solution of order $O(\epsilon)$ to the second system, and the perturbed Jacobian is of order $\Omega(\epsilon)$, so there exist a point in $B(x, \epsilon)$ such that the condition of the multivariate Hensel lemma are satisfied. $\square$

Chapter 3

Code and Numerical results

In this chapter we compile some examples of quasi-canonical lifts for small primes. For all the examples, $b := \sqrt{p}$ will denote a generator of the quadratic ramified extension $\mathbb{Q}_p/\mathbb{Q}$. The SAGE code used to generate these j-invariants is listed below, and can be used to fully automatically handle the case of endomorphism of degree p in characteristic p. To find minimal polynomials of traces and norms, we use PARI's algdep method. While there is no guarantee that this method will find the true minimal polynomials, we can and did check for overfitting by verifying that the output of the method is stable as the precision of the input is increased.

```
import numpy as np
from sage.libs.pari.convert_sage import gen_to_sage
from sage.schemes.elliptic_curves.ell_finite_field import is_j_supersingular

class CLParam:
    def __init__(self, p, f, e, prec):
      """
      Wrapper class for the background parameters.
      INPUT:
      p: Residue characteristic of the p-adic field
      f: Degree of the maximal unramified subextension over the base p-adic
   field
```

```
    e: Degree of the ramified subextension. Must be either 1 or 2, depending on whether p     is a square root in the relevant field.
    prec: Working precision for the p-adic field.
    OUTPUT: Wrapper class.
    """
      self.p = p
      self.f = f
      self.e = e
      self.prec = prec
      L.<z> = Qp(p, prec = prec, names = 'z')[]
      self.pol_ring = L
      self.indeterminate = self.pol_ring.gen()
      self.unr = Qq(p^f, prec = prec, names = 't')
      self.var_unr = self.unr.gen()
      self.Frob = self.unr.frobenius_endomorphism()
      K.<a> = self.unr[]
      self.unr_pol = K

      if e > 1:
          R.<b> = Qp(p , prec = prec, names = 'b').ext(self.indeterminate^e-p)
          self.rm = R
          self.var_rm = self.rm.gen()

      #Stores modular polynomial phi_p and its first partial derivatives in memory
      pol_mod = pari.polmodular(p)
      R.<x,y> = QQ[]
      self.pol_mod = gen_to_sage(pol_mod, {'x': x, 'y': y})
      self.partial_x = derivative(self.pol_mod,x)
      self.partial_y = derivative(self.pol_mod,y)
      self.diag = self.pol_mod(z,z)
      self.g = self.diag.differentiate()
      self.h = self.g.differentiate()
```

```
43
44      def Frob_lift(self,x,k):
45          """
46          Wrapper to call the (lift to char = 0 of) Frobenius multiple times
47          INPUT
48          x : Element of the field K specified above. A polynomial expression in
        the generator a
49          k : Number of times the Frobenius map is applied to k
50          OUTPUT
51          The k-th power of the Frobenius map applied to x
52          """
53          if k <= self.f:
54              if k == 0:
55                  return x
56              if k == 1:
57                  return self.Frob(x)
58              else:
59                  return self.Frob(self.Frob_lift(x,k-1))
60          else:
61              return self.Frob(self.Frob_lift(x,k%self.f-1))
62
63      def asroot1(self,a,b,k):
64          """
65          Returns elements a_1, b_1 s.t Frob^k(x) ~= a_1*x+b_1 for
66          a hypothetical solution to an Artin-Schreier equation.
67          INPUT
68          a, b: coefficient of Artin-Schreir equation
69          k : Power of the Frobenius map
70          OUTPUT
71          Integral elements a_1, b_1
72          """
73          if k == 1:
74              a_1 = a
75              b_1 = b
```

```
76          else:
77              l = np.floor(k/2)
78              a_0, b_0 = self.asroot1(a,b,l)
79              a_frob = self.Frob_lift(a_0,l)
80              b_frob = self.Frob_lift(b_0,l)
81              a_1 = a_0*a_frob
82              b_1 = b_0*a_frob + b_frob
83
84              if k%2 == 1:
85                  b_1 = b*self.Frob_lift(a_1,1) + self.Frob_lift(b_1,1)
86                  a_1 = a*self.Frob_lift(a_1,1)
87          return a_1, b_1
88
89      def asroot2(self,alpha,beta,gamma):
90          """
91          Wrapper for solving general a Artin-Schreier equation alpha*Frob(x)+
    beta*x+gamma = 0
92          """
93          a_n, b_n = self.asroot1(-1*beta/alpha,-1*gamma/alpha,self.f)
94          return b_n/(1-a_n)
95
96      def Hensel(self,pol,dpol,root, N):
97          """
98          Applies Hensel's lemma to lift a root of an univariate polynomial
99          INPUT:
100         pol: Polynomial whose root is to be lifted
101         dpol: derivative of pol
102         root: Approximate root
103         N: Desired precision
104         """
105         if N <= 1:
106             return root
107         else:
108             M = np.ceil((N)/2)
```

```
109             M = int(M)
110             x_1 = self.Hensel(pol,dpol, root, M)
111             if pol(x_1).valuation() - 2*dpol(x_1).valuation() <= 0:
112                 print("Further iterations will not converge")
113                 return x_1
114             x_2 = x_1 - pol(x_1)/dpol(x_1)
115             return x_2
116 
117     def exponentiate(self,n):
118         """
119         Don't ask
120         """
121         if n == 1:
122             return self.p
123         else:
124             x = self.p
125             if x%2 == 1:
126                 x = self.p
127             return exponentiate(self.p,floor(n/2))^2*x
128 
129     def Canonical_lift(self,x_0, N):
130         """
131         (Generalized) Newton lift. The technique works for equations of the
    form f(x,Frob(x))=0 in general, but
132         here f is hardcoded as a modular polynomial
133         INPUT:
134         x_0: Initial guess
135         N: Desired precision (limited by the precision given at the start of
    the program)
136         OUTPUT:
137         A solution to phi(x,Frob(x)) over the p-adic
138         """
139         if self.f == 1:
140             x_2 = self.Canonical_lift_f1(x_0,N)
```

```
            return x_2
        if N <= 1:
            print(x_0)
            return x_0
        else:
            M = int(np.ceil(N/2))
            x_1 = self.Canonical_lift(x_0,M)
            y_1 = self.Frob(x_1)
            ev = self.pol_mod(x_1,y_1)
            dx = self.partial_x(x_1,y_1)
            dy = self.partial_y(x_1,y_1)
            var = self.asroot2(dy,dx,ev/self.exponentiate(M))
            x_2 = x_1+(var*self.exponentiate(M))
        return x_2

    def Canonical_lift_f1(self, x_0,N):
        """
        (Generalized) Newton lift. Deals with the case where x_0 lies in a quadratic extension of Qp. If the
        lifts of the supersingular values hasn't been computed yet, this will do so before lifting x_0
        INPUT:
        x_0: Initial guess
        N: Desired precision (limited by the precision given at the start of the program)
        OUTPUT:
        A solution to phi(x,x) over the p-adic
        """
        ss = is_j_supersingular(GF(self.p)(x_0))
        if N == 1:
            return x_0, ss

        else:
            #Iterative procedure
```

```
            x_1 , ss = self.Canonical_lift_f1(x_0,N-1)
            if ss:
                x_2 = x_1 - self.diag(x_1)/self.g(x_1)
            else:
                x_2 = x_1 - self.g(x_1)/self.h(x_1)
            return x_2, ss


def Euclid(pol, root, degree):
    temp = pol.coefficients()[::-1]
    factor = [temp[0]]
    var = 0
    for i in range(1,len(temp)-1):
        var = temp[i] + root*factor[i-1]
        factor.append(var)

    factor = factor[::-1]
    var = 0
    f = 0
    for i in factor:
        f = f + i*x^(var)
        var += 1

    return f
```

In characteristic 5, we obtain the results tabulated below. Note that the only lift that does not lie in $\mathbb{Q}_5$ is the supersingular one, as expected from the general theory developped in Chapter 2.

Input seed	p-adic lift	Supersingular	Trace	Norm
$5 * b$	$b^3 + b^6 + O(b^7)$	True	$x - 1264000$	x - 681472000
$1 + 5 * b$	$1 + 4 * b^2 + 4 * b^4 + 4 * b^6 + O(b^7)$	True	$x - 574992$	$x - 82653950016$
$2 + 5 * b$	$2 + b^2 + 4 * b^4 + 2 * b^6 + O(b^7)$	False	$x + 65536$	$x - 1073741824$
$3 + 5 * b$	$3 + 4 * b^4 + 3 * b^6 + O(b^7)$	False	$x - 3456$	$x - 2985984$
$4 + 5 * b$	$4 + 2 * b^2 + 2 * b^6 + O(b^7)$	False	$x + 1769472$	$x - 782757789696$

Table 3.1: Lifts of Frobenius in characteristic 5

In characteristic 7, the results for the ordinary lifts are tabulated below. The lift for the supersingular value $6 \in \mathbb{F}_p$ is found to be $6+4*b+4*b^2+4*b^4+b^5+5*b^6+O(b^{10})$, and while it is easily computed to arbitrary precision, PARI's algdep method seems to be sensitive to our choice of generator for the quadratic ramified extension. Nonetheless, when these approximate lifts are substituted back in the relevant modular polynomial, the resulting value is approximately zero and shrinks as the precision is increased, as expected.

Input seed	p-adic lift	Supersingular	Trace	Norm
b	$0 + O(10)$	False	x - 0	x - 0
$1 + b$	$1 + b^2 + 4 * b^4 + 3 * b^6 + O(b^7)$	False	$x + 1769472$	$x - 782757789696$
$2 + b$	$2+3*b^4+3*b^6+O(b^7)$	False	$x - 108000$	$x - 2916000000$
$3 + b$	$3+3*b^2+6*b^4+O(b^7)$	False	$x + 24576000$	$x - 150994944000000$
$4 + b$	$4+6*b^2+5*b^4+5*b^6+O(b^7)$	False	$x^2 - 9669888x + 58680557568$	$x^2 - 23347343204352x + 215212989780710129664$
$5 + b$	$5 + 2 * b^2 + b^4 + 6 * b^6 + O(b^7)$	False	$x^2 - 9669888x + 58680557568$	$x^2 - 23347343204352x + 215212989780710129664$

Table 3.2: Lift of the ordinary Frobenius in characteristic 7

Conclusion

In conclusion, the results of Chapter 2 give a complete theoretical solution to the problem of finding quasi-canonical lifts of curves in $\mathbb{F}_p$. It would be interesting to see if the analogy with the theory of complex multiplication could be pushed further. A large part of this theoretical solution has been successfully implemented as shown in the code and examples given in Chapter 3. Nonetheless, from a numerical perspective, it remains to extend those results by fully implementing the algorithms described and by extending them to the case of curves over $\mathbb{F}_{p^2}$.

Bibliography

[1] COHEN, H., FREY, G., AVANZI, R., DOCHE, C., LANGE, T., NGUYEN, K., AND VERCAUTEREN, F. *Handbook of Elliptic and Hyperelliptic Curve Cryptography*, 1 ed. Discrete mathematics and its applications. Chapman & Hall/CRC, 2006.

[2] DRINFEL'D, V. Coverings of p-adic symmetric domains.

[3] GROSS, B. H. On canonical and quasi-canonical liftings. *Inventiones Mathematicae 84*, 2 (1986), 321–326.

[4] LUBIN, J., AND TATE, J. Formal moduli for one-parameter formal lie groups. *Bulletin de la Société Mathématique de France 94* (1966), 49–59.

[5] MESSING, W. *The crystals associated to Barsotti-Tate groups: with applications to Abelian schemes*. Lecture notes in mathematics, 264. Springer-Verlag, 1972.

[6] NEUKIRCH, J. *Algebraic Number Theory*, 1 ed. Grundlehren der mathematischen Wissenschaften 322. Springer-Verlag Berlin Heidelberg, 1999.

[7] SERRE, J.-P., AND TATE, J. Seminar at woods hole institute for algebraic geometry, 1964.

[8] SILVERMAN, J. H. *The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics 106. Springer New York, 1986.

[9] SILVERMAN, J. H. *Advanced Topics in the Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics. Springer, 1999.