MATHEMATICS OF COMPUTATION
Volume 77, Number 264, October 2008, Pages 2417–2435
S 0025-5718(08)02091-7
Article electronically published on April 23, 2008

A p-ADIC ALGORITHM TO COMPUTE THE HILBERT CLASS POLYNOMIAL

REINIER BRÖKER

Abstract. Classically, the Hilbert class polynomial $P_\Delta \in \mathbf{Z}[X]$ of an imaginary quadratic discriminant Δ is computed using complex analytic techniques. In 2002, Couveignes and Henocq suggested a p-adic algorithm to compute P_Δ. Unlike the complex analytic method, it does not suffer from problems caused by rounding errors. In this paper we give a detailed description of the algorithm in the paper by Couveignes and Henocq, and our careful study of the complexity shows that, if the Generalized Riemann Hypothesis holds true, the expected runtime of the p-adic algorithm is $O(|\Delta|(\log|\Delta|)^{8+\varepsilon})$ instead of $O(|\Delta|^{1+\varepsilon})$. We illustrate the algorithm by computing the polynomial P_{-639} using a 643-adic algorithm.

1. Introduction

The *Hilbert class polynomial* P_Δ is the minimal polynomial over $\mathbf{Q}$ of the modular j-value $j(\mathcal{O}_\Delta)$ for the imaginary quadratic order $\mathcal{O}_\Delta$. It is a polynomial with *integer* coefficients. The polynomials P_Δ generate the ring class fields of imaginary quadratic fields. More precisely, the ring class field $H_\mathcal{O}$ for the order $\mathcal{O} = \mathcal{O}_\Delta \subset \mathbf{Q}(\sqrt{\Delta}) = K$ of discriminant Δ is given by $H_\mathcal{O} = K[X]/(P_\Delta)$. In case $\mathcal{O}$ is the maximal order of K, the ring class field $H_\mathcal{O}$ is also known as the *Hilbert class field*.

Such a canonical family of generators of ring class fields is quite rare, and is only known for imaginary quadratic fields K and for $\mathbf{Q}$, where it is provided by the theorem of Kronecker-Weber. The compositium of the ring class fields for all orders $\mathcal{O} \subset K$, together with the roots of unity, gives us a large part of the maximal abelian extension K^{ab} of K. More precisely, the field

$$K' = \mathbf{Q}^{\mathrm{ab}} \cdot \bigcup_{\substack{\mathcal{O}\subset K \\ \text{order}}} H_\mathcal{O}$$

is a subfield of K^{ab}, and the Galois group $\mathrm{Gal}(K^{\mathrm{ab}}/K')$ is a product of groups of order 2; cf. [22, Section 3].

In this article we focus on a method to *explicitly compute* $P_\Delta \in \mathbf{Z}[X]$. This gives us a means of computing abelian extensions of imaginary quadratic fields, and the observation that the roots in $\overline{\mathbf{F}}_p$ of $P_\Delta \in \mathbf{F}_p[X]$ are j-invariants of elliptic curves with endomorphism ring $\mathcal{O}_\Delta$ has had its impact outside the context of explicit class field theory. It is a key ingredient in the elliptic curve primality proving algorithm [9], and an important step in this algorithm is to compute P_Δ. Fast algorithms to compute P_Δ are also desirable from a cryptographic point of view.

Received by the editor November 10, 2006 and, in revised form, June 27, 2007.
2000 *Mathematics Subject Classification.* Primary 11G15.

Indeed, computing P_Δ allows us to efficiently construct elliptic curves for which the discrete logarithm problem is hard; cf. [4, Chapter 23].

There is a classical algorithm [3, Section 7.6] to compute $P_\Delta \in \mathbf{Z}[X]$. One computes the set S_Δ of reduced primitive positive definite quadratic forms $[a,b,c] = aX^2 + bXY + cY^2$ of discriminant $b^2 - 4ac = \Delta$, and evaluates P_Δ as

$$P_\Delta = \prod_{[a,b,c]\in S_\Delta} \left(X - j(\frac{-b+\sqrt{\Delta}}{2a}) \right) \in \mathbf{Z}[X]. \tag{1.1}$$

Here, we approximate the values $j(\frac{-b+\sqrt{\Delta}}{2a}) \in \mathbf{C}$ with high enough accuracy to ensure that we can 'recognize' the coefficients of the product as integers. Working in this *archimedean setting* has the disadvantage that rounding errors may occur in expanding the product (1.1), and this has prevented a rigorous *runtime analysis* of this algorithm. We expect [8] the runtime to be $\widetilde{O}(|\Delta|)$, where we use the $\widetilde{O}$-notation to indicate that the factors that are of logarithmic order in the main term have been disregarded.

In 2002, Couveignes and Henocq suggested [5] a p-adic algorithm to compute P_Δ. Note that a p-adic algorithm automatically circumvents the problem of rounding errors. The main result of [5] is the following theorem.

Theorem 1.1 (Couveignes-Henocq)**.** *The algorithm suggested in* [5] *computes, on input of a discriminant $\Delta < 0$, the Hilbert class polynomial $P_\Delta \in \mathbf{Z}[X]$. If GRH holds true, the algorithm has an an expected runtime $O(|\Delta|^{1+\varepsilon})$ for every $\varepsilon > 0$.*

In this article, we study in detail the algorithm suggested in [5], we give proofs for the statements implicitly used in [5] to prove Theorem 1.1, we provide a better runtime analysis of the p-adic algorithm and we explain how to implement it. This yields the following result.

Theorem 1.2. *The algorithm presented in this paper returns, on input of a discriminant $\Delta < 0$, the Hilbert class polynomial $P_\Delta \in \mathbf{Z}[X]$. If GRH holds true, the algorithm has an an expected runtime $O(|\Delta|(\log|\Delta|)^{8+\varepsilon})$ for every $\varepsilon > 0$.*

In Section 2 we recall the basis statements of complex multiplication theory that we need for our algorithm. The algorithm itself is presented in Sections 3–7, and we analyse its runtime in Section 7. The algoritm is illustrated by means of a detailed example in Section 8.

2. Complex multiplication

The p-adic algorithm uses more geometry than the complex analytic algorithm. In this section we give the main results of complex multiplication (CM) theory from a 'geometric point of view'. Throughout this section, K is an imaginary quadratic number field and $\mathcal{O} = \mathcal{O}_\Delta \subset K$ is an order in K.

Let F be a field for which there exists an elliptic curve E/F with endomorphism ring $\mathrm{End}_F(E) \cong \mathcal{O}$. We write $\mathcal{O} = \mathbf{Z}[\alpha]$ for some $\alpha \in \mathcal{O}$. The minimal polynomial $f^\alpha_{\mathbf{Z}}$ of α splits in $F[X]$. We fix a root of $f^\alpha_{\mathbf{Z}} \in F[X]$, and view F as an $\mathcal{O}$-algebra. There are two isomorphisms $\mathcal{O} \xrightarrow{\sim} \mathrm{End}_F(E)$. We will always consider the *normalized* isomorphism, i.e., the unique isomorphism φ with $\varphi(\alpha)^*\omega = \alpha\omega$ for all $\alpha \in \mathcal{O}$ and all invariant differentials $\omega \in \Omega_E$. Such a pair (E, φ) is called a *normalized elliptic curve*. Two normalized elliptic curves (E, φ) and (E', φ') are said to be isomorphic if there exists an isomorphism $\tau : E \to E'$ of elliptic curves with $\tau^{-1}\varphi'(\alpha)\tau = \varphi(\alpha)$ for all $\alpha \in \mathcal{O}$. As there will hardly be any risk of confusion, we will usually write E instead of (E, φ) and just speak of an elliptic curve instead of a normalized one.

Define the set

$$\mathrm{Ell}_\Delta(F) = \{j(E) \in F \mid \text{ there exists an elliptic curve } E/F \text{ with } \mathrm{End}_F(E) = \mathcal{O}\}$$

of j-invariants of elliptic curves over F with endomorphism ring $\mathcal{O}$. This set can be empty, as the example $F = \mathbf{Q}$ shows. In the cases that will be of interest to us, it will be a finite set of cardinality $h(\Delta)$, the class number of $\mathcal{O}$.

Let $I \subseteq \mathrm{End}_F(E)$ be an ideal with norm $N(I)$ coprime to $\mathrm{char}(F)$ and define

$$E[I] = \{P \in E(\overline{F}) \,|\, \forall \alpha \in I : \alpha(P) = 0\},$$

the group of I-torsion points of E. There exist an elliptic curve E^I and a separable isogeny $\phi : E \to E^I$ with $\mathrm{Ker}(\phi) = E[I]$ by [24, Proposition 3.4.12]. The curve E^I is unique up to F-isomorphism. We get a quotient map $E \to E^I$ for every ideal $I \subset \mathcal{O}$ coprime to $\mathrm{char}(F)$. The definition of E^I does depend on the choice of an isomorphism $\mathcal{O} \xrightarrow{\sim} \mathrm{End}_F(E)$.

Now let $F = \mathbf{C}$ be the field of complex numbers. A complex elliptic curve with endomorphism ring $\mathcal{O} \subset \mathbf{C}$ is isomorphic to a curve $E_\mathfrak{a} = \mathbf{C}/\mathfrak{a}$ for an invertible $\mathcal{O}$-ideal $\mathfrak{a}$. For an invertible $\mathcal{O}$-ideal I, the isogeny

$$\begin{aligned} \mathbf{C}/\mathfrak{a} &\to \mathbf{C}/(I^{-1}\mathfrak{a}), \\ z &\mapsto z \end{aligned}$$

has kernel $E_\mathfrak{a}[I]$. We have $E_\mathfrak{a}^I \cong E_{I^{-1}\mathfrak{a}}$, and the curve $E_\mathfrak{a}^I$ has endomorphism ring $\mathcal{O}$. The map $\rho_I : \mathrm{Ell}_\Delta(\mathbf{C}) \to \mathrm{Ell}_\Delta(\mathbf{C})$ that sends $j(E)$ to $j(E^I)$ is well-defined. Its inverse is given by $\rho_{\overline{I}}$, where $\overline{I}$ denotes the complex conjugate of I. The map ρ_I gives an action of the group $\mathcal{I}(\mathcal{O})$ of invertible fractional $\mathcal{O}$-ideals on the set $\mathrm{Ell}_\Delta(\mathbf{C})$.

Let $\mathfrak{a}, \mathfrak{b} \subset \mathcal{O}$ be two invertible $\mathcal{O}$-ideals, viewed at lattices in $\mathbf{C}$. The complex elliptic curves $E_\mathfrak{a} = \mathbf{C}/\mathfrak{a}$ and $E_\mathfrak{b} = \mathbf{C}/\mathfrak{b}$ are isomorphic if and only if the lattices $\mathfrak{a}$ and $\mathfrak{b}$ are homothetic. In other words: we have $j(\mathbf{C}/\mathfrak{a}) = j(\mathbf{C}/\mathfrak{b})$ if and only if the equality $[\mathfrak{a}] = [\mathfrak{b}]$ holds in the Picard group $\mathrm{Pic}(\mathcal{O})$. The action of $\mathcal{I}(\mathcal{O})$ given by the map $\rho_I : \mathrm{Ell}_\Delta(\mathbf{C}) \to \mathrm{Ell}_\Delta(\mathbf{C})$ factors through the quotient map $\mathcal{I}(\mathcal{O}) \twoheadrightarrow \mathrm{Pic}(\mathcal{O})$, and we get an action of $\mathrm{Pic}(\mathcal{O})$ on $\mathrm{Ell}_\Delta(\mathbf{C})$. This action is simply transitive. The transitivity follows from the equality $\rho_{\mathfrak{b}^{-1}\mathfrak{a}}(j(\mathbf{C}/\mathfrak{a})) = j(\mathbf{C}/\mathfrak{b})$. It is clear that the action is free. We have made $\mathrm{Ell}_\Delta(\mathbf{C})$ into a principal homogeneous $\mathrm{Pic}(\mathcal{O})$-space, or $\mathrm{Pic}(\mathcal{O})$-torsor. In particular, $\mathrm{Ell}_\Delta(\mathbf{C})$ is a *finite* set of cardinality $h(\Delta)$, and we have

$$\mathrm{Ell}_\Delta(\mathbf{C}) = \{j(\mathbf{C}/\mathfrak{a}_i) \mid [\mathfrak{a}_i] \in \mathrm{Pic}(\mathcal{O})\}.$$

The main theorem [14, Section 10.3] of CM-theory states that the ring class field $H_\mathcal{O}$ for the order $\mathcal{O} \subset \mathbf{Q}(\sqrt{\Delta}) = K$ is given by $H_\mathcal{O} = K(j(\mathbf{C}/\mathcal{O}))$. Furthermore, for $E = \mathbf{C}/\mathcal{O}$ the Galois action of an ideal class $[\mathfrak{a}] \in \mathrm{Pic}(\mathcal{O})$ on $j(E)$ is given by

$$j(E)^{[\mathfrak{a}, H_\mathcal{O}/K]} = j(E^\mathfrak{a}).$$

The minimal polynomial P_Δ over $\mathbf{Q}$ of $j(\mathbf{C}/\mathcal{O})$ has integer coefficients by [23, Section 2.6], and we have

$$P_\Delta = \prod_{j \in \mathrm{Ell}_\Delta(F)} (X - j) = \prod_{[I] \in \mathrm{Pic}(\mathcal{O})} \big(X - j(E^I)\big) \tag{2.1}$$

for any field F in which we can embed the ring class field $H_{\mathcal{O}}$. Here E/F is an elliptic curve with endomorphism ring $\mathcal{O}$.

We will use $F = \mathbf{Q}_p$, where p is a prime that splits completely in the ring class field $H_{\mathcal{O}}$. Chebotarev's density theorem [18, Theorem VII.13.4] tells us that there are infinitely many such p. Fix a prime $p \geq 5$ for the remainder of this section that splits completely in $H_{\mathcal{O}}$.

As an element $j \in \mathrm{Ell}_{\Delta}(\mathbf{Q}_p)$ is integral, we obtain a natural bijection

$$\mu : \mathrm{Ell}_{\Delta}(\mathbf{Q}_p) \to \mathrm{Ell}_{\Delta}(\mathbf{F}_p).$$

If $\overline{E}/\mathbf{F}_p$ is an ordinary elliptic curve with endomorphism ring $\mathcal{O}$, the value $\tilde{\jmath} = \mu^{-1}(j(\overline{E})) \in \mathbf{Q}_p$ is called the *canonical lift* of $j(\overline{E}) \in \mathbf{F}_p$. An elliptic curve with j-invariant $\tilde{\jmath} \in \mathbf{Q}_p$ has endomorphism ring $\mathcal{O}$.

The outline of the p-adic algorithm is as follows. First we find a 'small' splitting prime p and an elliptic curve $\overline{E}/\mathbf{F}_p$ with endomorphism ring $\mathcal{O}$. We explain this step in Section 3. Next we lift $j(\overline{E}) \in \mathbf{F}_p$ to its canonical lift $\tilde{\jmath} \in \mathbf{Q}_p$. This is the hardest step of the algorithm and is explained in Sections 4–7. Finally, we explain in Section 7 how to compute the conjugates of the canonical lift under the action of the group $\mathrm{Pic}(\mathcal{O})$. The analysis of the various steps of the algorithm will yield Theorem 1.2.

3. A small splitting prime

Fix a discriminant $\Delta < -4$, and let $\mathcal{O} = \mathcal{O}_{\Delta}$ be the order of discriminant Δ. In this section we explain how to find a 'small' prime p that splits completely in the ring class field $H_{\mathcal{O}}$, and how to find an elliptic curve $\overline{E}/\mathbf{F}_p$ with endomorphism ring $\mathcal{O}$.

The Picard group $\mathrm{Pic}(\mathcal{O})$ is isomorphic to the Galois group $\mathrm{Gal}(H_{\mathcal{O}}/K)$ via the Artin map, and a prime $p \nmid \Delta$ splits completely in $H_{\mathcal{O}}$ if and only if (p) splits into two principal ideals in $\mathcal{O}$, i.e., if and only if we can solve the equation

$$4p = t^2 - u^2\Delta \tag{3.1}$$

in integers t, u. From this we see that we have a lower bound $p \geq |\Delta|/4$ on p. In order to find a prime p that splits completely in $H_{\mathcal{O}}$ we can first take $u = 1$ in equation (3.1). We let t range over $1, 2, \ldots, B(\Delta)$ and test whether $\frac{t^2-u^2\Delta}{4}$ is prime. Here $B(\Delta)$ is some upper bound, depending on Δ. If we do not find a solution to equation (3.1) with $u = 1$, we try $u = 2, 3, \ldots$, etc. However, for $\Delta \equiv 0 \bmod 4$, we take t even to ensure that $\frac{t^2-u^2\Delta}{4}$ is an integer. For $\Delta \equiv 1 \bmod 4$, the integers t and u should have the same parity.

Lemma 3.1. *If GRH holds true, there exists an effectively computable constant $c \in \mathbf{R}_{>0}$ such that for every $\Delta < 0$ there exists a prime $p \in \mathbf{Z}$ that splits completely in $H_{\mathcal{O}}$ and that satisfies*

$$p \leq c \cdot |\Delta|(\log|\Delta|)^4.$$

Proof. The effective Chebotarev density theorem, which requires the assumption of GRH, states that there is an effectively computable constant $c \in \mathbf{R}_{>0}$ such that for every $\Delta < 0$ there exists a prime p that splits completely in $H_{\mathcal{O}}$ and that satisfies

$$p \leq c \cdot (\log|\mathrm{disc}(H_{\mathcal{O}}/\mathbf{Q})|)^2,$$

where $\mathrm{disc}(H_{\mathcal{O}}/\mathbf{Q})$ is the discriminant of $H_{\mathcal{O}}/\mathbf{Q}$. We will compute the discriminant $\mathrm{disc}(H_{\mathcal{O}}/\mathbf{Q})$ via the relation

$$\mathrm{disc}(H_{\mathcal{O}}/\mathbf{Q}) = N_{K/\mathbf{Q}}(\mathrm{disc}(H_{\mathcal{O}}/K)) \cdot \mathrm{disc}(K/\mathbf{Q})^{[H_{\mathcal{O}}:K]},$$

with $K = \mathbf{Q}(\sqrt{\Delta})$. Write $\Delta = f^2 D$ with $D = \mathrm{disc}(K)$. Then $H_{\mathcal{O}}/K$ is an abelian extension of a conductor dividing f and degree $h(\Delta)$. From the conductor discriminant formula [18, Theorem VII.11.9] we see that the $\mathcal{O}_K$-ideal $\mathrm{disc}(H_{\mathcal{O}}/K)$ is a divisor of $f^{h(\Delta)}$. We have $N_{K/\mathbf{Q}}(f^{h(\Delta)}) = f^{2h(\Delta)}$ and we estimate

$$\mathrm{disc}(H_{\mathcal{O}}/\mathbf{Q}) \leq f^{2h(\Delta)} \cdot |D|^{h(\Delta)} = |\Delta|^{h(\Delta)}.$$

Using the upper bound $h(\Delta) \leq \sqrt{|\Delta|} \log|\Delta|$ from [16, Section 2], we conclude

$$\mathrm{disc}(H_{\mathcal{O}}/\mathbf{Q}) \leq |\Delta|^{\sqrt{|\Delta|}\log|\Delta|}. \qquad \square$$

Fix a solution (p, t, u), with p prime and $t \neq 0$, to equation (3.1). In the remainder of this section we present and analyse a simple Algorithm for finding an ordinary elliptic curve $\overline{E}/\mathbf{F}_p$ with endomorphism ring $\mathrm{End}_{\mathbf{F}_p}(\overline{E}) = \mathcal{O}$.

By [20, Theorem 4.6] there exists an elliptic curve $E/\mathbf{F}_p$ whose Frobenius morphism $F_p : E \to E$ has trace t. The subring $\mathbf{Z}[F_p] \subseteq \mathcal{O}$ has index $u \geq 1$. We find such a curve E by trying *random* curves over $\mathbf{F}_p$ until we hit a curve with the correct number of points. More precisely, we pick a random element $b \in \mathbf{F}_p^* \setminus \{\frac{-27}{4}\}$ and test whether the curve $E_b : Y^2 = X^3 + bX - b$ or its quadratic twist has trace of Frobenius t. As 'early abort strategy' we test whether the point $(1,1) \in E_b(\mathbf{F}_p)$ is annihilated by $p + 1 \pm t$.

Once we have found a curve $E/\mathbf{F}_p$ with a trace of Frobenius t, we compute its endomorphism ring using Kohel's algorithm [12]. If E has endomorphism ring $\mathcal{O}$, we return E and halt. Otherwise, we compute another random curve with trace of Frobenius t and test whether this curve has endomorphism ring $\mathcal{O}$, etc., until we find a desired curve with endomorphism ring $\mathcal{O}$.

Remark. If $E/\mathbf{F}_p$ has trace of Frobenius t and endomorphism ring $\mathcal{O}_{\Delta'}$ of discriminant $\Delta' \neq \Delta$, there is another method to find a curve with endomorphism ring $\mathcal{O}$. Let g be the index of $\mathbf{Z}[F_p]$ in $\mathcal{O}_{\Delta'}$. We first apply an isogeny of degree g starting at E to obtain a curve with endomorphism ring $\mathbf{Z}[F_p]$, and then we apply an isogeny of degree u to find a curve with the desired endomorphism ring. This method is fast if both g and u are 'small'.

Remark. In the examples we have computed, we often have $u = 1$. If Δ is fundamental, finding a curve with trace t is then the same as finding a curve with endomorphism ring $\mathcal{O}$, and there is no need to apply Kohel's algorithm.

We continue with the analysis of the algorithm. We assume that we have $p = O(|\Delta|(\log|\Delta|)^4)$, $|t| \leq \sqrt{p}$ and $u = O((\log|\Delta|)^2)$, where the constants in the O-symbols come from Lemma 3.1.

The number of $\mathbf{F}_p$-isomorphism classes of elliptic curves with trace of Frobenius t equals $H(t^2 - 4p)$ by [20, Theorem 4.6], where H denotes the Kronecker class number. From [15, Proposition 1.8] we derive that, if GRH holds true, we have

$$H(t^2 - 4p) \geq c \cdot \sqrt{|\Delta|}(\log|\Delta|)^3$$

for some effectively computable constant $c \in \mathbf{R}_{>0}$ which is independent of Δ. It is here that we need the assumption $|t| \leq \sqrt{p}$ to ensure that $|t^2 - 4p|$ is not too small.

We conclude that we may expect to find a curve $E/\mathbf{F}_p$ with trace of Frobenius t after $\widetilde{O}(|\Delta|^{1/2})$ tries. Computing the endomorphism ring of E takes time $\widetilde{O}(|\Delta|^{1/3})$ using Kohel's algorithm [12]. Also here we need to assume GRH.

The fraction

$$\frac{\#\{E/\mathbf{F}_p \mid \mathrm{End}_{\mathbf{F}_p}(E) = \mathcal{O} = \mathcal{O}_\Delta\}/_{\cong_{\mathbf{F}_p}}}{\#\{E/\mathbf{F}_p \mid \mathrm{End}_{\mathbf{F}_p}(E) \supseteq \mathcal{O}_{u^2\Delta}\}/_{\cong_{\mathbf{F}_p}}}$$

of elliptic curves with trace of Frobenius t and endomorphism ring $\mathcal{O}$ equals $n = h(\Delta)/H(u^2\Delta) \in \mathbf{Q}$. From the formulas given in [15, Section 1.6] for the Kronecker class number we derive

$$n \geq \left(\frac{\varphi(f)}{f}\right)^2 \cdot \frac{1}{u},$$

where φ denotes the Euler-φ function and f is the index of $\mathcal{O}_{u^2\Delta}$ in its maximal overorder. Theorem 328 in [11] gives that $\liminf_{f\to\infty} \frac{\varphi(f)\log\log f}{f}$ is finite. Combining this with the estimate $u = O((\log|\Delta|)^2)$, we derive the lower bound

$$n \geq c_\varepsilon \cdot \frac{1}{(\log|\Delta|)^{2+\varepsilon}}$$

for some effectively computable constant c_ε, depending on ε.

Theorem 3.2. *The Algorithm presented in this section returns, on input of a discriminant $\Delta < -4$, a prime number p and an elliptic curve over $\mathbf{F}_p$ with endomorphism ring $\mathcal{O} = \mathcal{O}_\Delta$. If GRH holds true, the expected runtime is $\widetilde{O}(|\Delta|^{1/2})$.*

4. Computing the canonical lift

Let $p \geq 5$ be a prime that splits completely in the ring class field $H_\mathcal{O}$ of the order $\mathcal{O} = \mathcal{O}_\Delta$ of discriminant $\Delta < -4$. Fix an ordinary elliptic curve $\overline{E}/\mathbf{F}_p$ with endomorphism ring $\mathcal{O}$. In Sections 4–7 we give an algorithm to compute the canonical lift $\tilde{\jmath} = j(\widetilde{E}) \in \mathbf{Q}_p$ of $j(\overline{E}) \in \mathbf{F}_p$. The runtime analysis in Section 7 will yield the following theorem.

Theorem 4.1. *There exists an algorithm which has as input*

◇ *a prime $p \geq 5$,*
◇ *an ordinary j-invariant $j \in \mathbf{F}_p$,*
◇ *a positive integer k,*

and as output the canonical lift $\tilde{\jmath} \in \mathbf{Q}_p$ of $j \in \mathbf{F}_p$ in k-digit accuracy. If GRH holds true, the expected runtime of this algorithm is for every $\varepsilon > 0$ bounded by

$$c_\varepsilon \left(\exp((\log p)^{1/2+\varepsilon}) \times \log k\right)^4 \times k$$

for some effectively computable constant $c_\varepsilon > 0$.

Let $I \subset \mathcal{O}$ be an invertible $\mathcal{O}$-ideal. As in Section 2 we have a map

$$\rho_I : \mathrm{Ell}_\Delta(\mathbf{Q}_p) \to \mathrm{Ell}_\Delta(\mathbf{Q}_p)$$

that maps $j(\widetilde{E})$ to $j(\widetilde{E}^I)$. Here, the isogeny $\widetilde{E} \to \widetilde{E}^I$ has the group $\widetilde{E}[I]$ of I-torsion points as a kernel. The inverse of ρ_I is given by $\rho_{\overline{I}}$, where $\overline{I}$ is the complex conjugate of I, and the map ρ_I is bijective.

For the remainder of this section we assume that the ideal $I \subset \mathcal{O}$ is coprime to p. We then obtain a bijection $\overline{\rho}_I : \mathrm{Ell}_\Delta(\mathbf{F}_p) \to \mathrm{Ell}_\Delta(\mathbf{F}_p)$ that sends $j(\overline{E})$ to $j(\overline{E}^I)$, and we have a commutative diagram

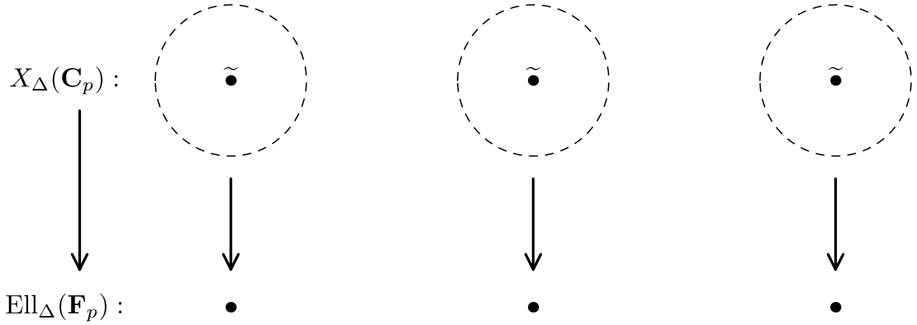
$$\begin{tikzcd}
j(\widetilde{E}) \arrow[r, "\rho_I"] \arrow[d] & j(\widetilde{E}^I) \arrow[d] \\
j(\overline{E}) \arrow[r, "\overline{\rho}_I"] & j(\overline{E}^I).
\end{tikzcd}$$

The map ρ_I induces a transitive and free action of the Picard group $\mathrm{Pic}(\mathcal{O})$ on $\mathrm{Ell}_\Delta(\mathbf{Q}_p)$; cf. Section 2. Similarly, we have an action of $\mathrm{Pic}(\mathcal{O})$ on $\mathrm{Ell}_\Delta(\mathbf{F}_p)$. The action of $\mathrm{Pic}(\mathcal{O})$ on $\mathrm{Ell}_\Delta(\mathbf{Q}_p)$ and $\mathrm{Ell}_\Delta(\mathbf{F}_p)$ is compatible with reducing modulo p.

Let $\mathbf{C}_p$ be the completion of an algebraic closure of $\mathbf{Q}_p$. It is well known that $\mathbf{C}_p$ is itself algebraically closed. Define

$$X_\Delta(\mathbf{C}_p) = \{j \in \mathbf{C}_p \,|\, \overline{\jmath} \in \mathrm{Ell}_\Delta(\mathbf{F}_p)\} \subset \mathbf{C}_p.$$

The set $X_\Delta(\mathbf{C}_p)$ consists of $h(\Delta)$ open discs of p-adic radius 1 around the CM-points $\mathrm{Ell}_\Delta(\mathbf{Q}_p)$. Every disc contains exactly one element of $\mathrm{Ell}_\Delta(\mathbf{Q}_p)$.


$X_\Delta(\mathbf{C}_p)$:
$\mathrm{Ell}_\Delta(\mathbf{F}_p)$:

The picture visualises the situation. The elements of the set $\mathrm{Ell}_\Delta(\mathbf{F}_p)$ are denoted by thick points. The set $X_\Delta(\mathbf{C}_p)$ is denoted by a series of open discs, one above each point in $\mathrm{Ell}_\Delta(\mathbf{F}_p)$. Just as we denoted the canonical lift of $j(\overline{E}) \in \mathbf{F}_p$ by $j(\widetilde{E})$, we place a tilde above a thick point to denote the elements of $\mathrm{Ell}_\Delta(\mathbf{Q}_p)$.

The fundamental idea in [5] is that the map $\rho_I : \mathrm{Ell}_\Delta(\mathbf{Q}_p) \to \mathrm{Ell}_\Delta(\mathbf{Q}_p)$ has a natural extension to a map $\rho_I : X_\Delta(\mathbf{C}_p) \to X_\Delta(\mathbf{C}_p)$, which we proceed to define. Let $N \in \mathbf{Z}_{>0}$ be the norm of I, which we assumed to be coprime to p. Take an arbitrary element $j \in X_\Delta(\mathbf{C}_p)$, and write $\overline{\jmath} \in \mathbf{F}_p$ for its reduction modulo p. Pick a curve $\overline{E}/\mathbf{F}_p$ with j-invariant $j(\overline{E}) = \overline{\jmath}$, and take any curve $E/\mathbf{C}_p$ with $j(E) = j \in \mathbf{C}_p$ that reduces to $\overline{E}/\mathbf{F}_p$. We have a natural isomorphism

$$\eta : E[N] \xrightarrow{\sim} \overline{E}[N]$$

by the assumption that N is coprime to p. The subgroup $\overline{E}[I] \subset \overline{E}[N]$ has a well defined inverse image under η. We denote $\eta^{-1}(\overline{E}[I])$ by $E[I]$. The group $E[I]$ is a subgroup of order N of $E[N]$, and it provides a lift of $\overline{E}[I]$ to a *group scheme* over the p-adic disc in $X_\Delta(\mathbf{C}_p)$ lying over $\overline{\jmath} \in \mathrm{Ell}_\Delta(\mathbf{F}_p)$. We define $\rho_I(j) = j(E^I)$. The j-invariant $j(E^I)$ is independent of the choice of E, and therefore ρ_I is well-defined.

For $j \in \mathrm{Ell}_\Delta(\mathbf{Q}_p)$ we now have two definitions of ρ_I: one in terms of a Galois action and one in terms of a group scheme. A moment's reflection shows however that these two definitions coincide.

Remark. For two invertible $\mathcal{O}$-ideals I, J that are coprime to p, we have $\rho_{IJ} = \rho_I \rho_J$. Furthermore, if J is contained in $\mathbf{Z}$, we have $\rho_J = \mathrm{id}$.

The map ρ_I has a geometric interpretation. After possibly multiplying with a principal fractional ideal, we assume that $\mathcal{O}/I$ is cyclic. Again, let N be the norm of I. We map the modular curve $Y_0(N)_{\mathbf{C}_p}$ inside $\mathbf{A}^1_{\mathbf{C}_p} \times \mathbf{A}^1_{\mathbf{C}_p}$:

$$\begin{tikzcd}
Y_0(N)(\mathbf{C}_p) \arrow[r, two heads] & C(\mathbf{C}_p) \arrow[r, tail] & \mathbf{A}^1(\mathbf{C}_p) \times \mathbf{A}^1(\mathbf{C}_p) \arrow[r, "p_1"] \arrow[ddd, "p_2"] & \mathbf{A}^1(\mathbf{C}_p) \\
\cup & & & \\
(E,G) \arrow[r, mapsto] & (j(E), j(E/G)) & & \\
& & \mathbf{A}^1(\mathbf{C}_p). &
\end{tikzcd}$$

The maps p_1, p_2 are the normal projection maps. The curve C is defined by $\Phi_N = 0$, with Φ_N the classical modular polynomial. Take a j-invariant $j(E) \in X_\Delta(\mathbf{C}_p)$. The fiber $p_1^{-1}(j(E)) \subset C(\mathbf{C}_p)$ above $j(E)$ consists of the points $(j(E), j(E/G_i))$, with G_i ranging over the $\psi(N)$ cyclic subgroups of order N of $E[N]$. We have $\rho_I(j(E)) = j(E^I) = p_2(j(E), j(E^I))$.

In other words, we have chosen two functions $j_1, j_2 : Y_0(N)_{\mathbf{C}_p} \to \mathbf{A}^1_{\mathbf{C}_p}$. They are defined by $j_1((E,G)) = j(E)$ and $j_2((E,G)) = j(E/G)$. For $j(E) \in X_\Delta(\mathbf{C}_p)$, we have $\rho_I(j(E)) = j_2((E, E[I]))$. We will often write $j_1(E)$ instead of $j_1((E,G))$ if there cannot be any confusion about which subgroup $G \subset E[N]$ we mean. Likewise for j_2.

Now let $I \subset \mathcal{O}$ be a *principal* ideal, and let $\alpha \in \mathcal{O}$ be a generator. We keep the assumption that p does not divide the norm of I, and we write ρ_α to denote the map $\rho_{(\alpha)}$.

Theorem 4.2. *Let $(\alpha) \subset \mathcal{O}$ be a principal ideal such that $\mathcal{O}/(\alpha)$ is cyclic as an abelian group. Assume that (α) is coprime to p. Then the map $\rho_\alpha : X_\Delta(\mathbf{C}_p) \to X_\Delta(\mathbf{C}_p)$ is analytic, i.e., it can be given locally by a power series.*

Proof. Take an elliptic curve $E/\mathbf{Q}_p$ with $j(E) \in \mathrm{Ell}_\Delta(\mathbf{Q}_p)$, such that E has good reduction modulo p. We define $P = (E, E[(\alpha)]) \in Y_0(N)(\mathbf{C}_p)$. The point P lies on the diagonal if we map $Y_0(N)_{\mathbf{C}_p}$ into $\mathbf{A}^1_{\mathbf{C}_p} \times \mathbf{A}^1_{\mathbf{C}_p}$, i.e., we have

$$j_1(E) = j_2(E).$$

The curve E is defined over $\mathbf{Q}_p$, and since the prime p splits in $\mathcal{O}$ we have $\alpha \in \mathbf{Q}_p$. This shows that $E[(\alpha)]$ is defined over $\mathbf{Q}_p$ and we have

$$P = (E, E[(\alpha)]) \in Y_0(N)(\mathbf{Q}_p).$$

The assumption $\Delta < -4$ yields that $j(E) \in \mathbf{C}_p$ has positive p-adic distance to $0, 1728 \in \mathbf{C}_p$. Now consider the local ring $\mathcal{O}_{Y_0(N)_{\mathbf{Q}_p}, P}$ and its completion $\widehat{\mathcal{O}}_{Y_0(N)_{\mathbf{Q}_p}, P}$ at the point P. Since $Y_0(N)_{\mathbf{Q}_p}$ is a smooth curve, $\widehat{\mathcal{O}}_{Y_0(N)_{\mathbf{Q}_p}, P}$ is a complete discrete valuation ring over $\mathbf{Q}_p$. Since $j_1(E)$ and $j_2(E)$ are not equal to one of the ramification points $j = 0, 1728$ of the cover $Y_0(N)_{\mathbf{Q}_p}/\mathbf{A}^1_{\mathbf{Q}_p}$, the functions $j_1 - j_1(E)$ and $j_2 - j_2(E)$ are uniformising parameters for $\widehat{\mathcal{O}}_{Y_0(N)_{\mathbf{Q}_p}, P}$.

The isomorphism $\widehat{\mathcal{O}}_{Y_0(N)_{\mathbf{Q}_p},P} \cong \mathbf{Q}_p[[j_1 - j_1(E)]]$ shows that we can express $j_2 - j_2(E)$ as a formal power series in $j_1 - j_1(E)$:

$$j_2 - j_2(E) = \sum_{i \geq 1} c_i (j_1 - j_1(E))^i \qquad \text{with } c_i \in \mathbf{Q}_p.$$

The theorem follows if we prove that the coefficients c_i of this power series lie in $\mathbf{Z}_p$.

As in [6, Section 9.3], we consider the modular curve $X_0(N)_{\mathbf{Q}_p}$ as a scheme over $\mathrm{Spec}(\mathbf{Q}_p)$. The diagram

$$\begin{tikzcd}
X_0(N)_{\mathbf{Q}_p} \arrow[r, tail] \arrow[d] & X_0(N)_{\mathbf{F}_p} \arrow[d] & X_0(N)_{\mathbf{F}_p} \arrow[l, tail] \arrow[d] \\
\mathrm{Spec}(\mathbf{Q}_p) \arrow[r, tail] \arrow[u, bend right, "P"'] & \mathrm{Spec}(\mathbf{Z}_p) \arrow[u, bend right, "P'"'] & \mathrm{Spec}(\mathbf{F}_p) \arrow[l, tail] \arrow[u, bend right, "\bar{P}"']
\end{tikzcd}$$

explains the situation. We view the point P as a section $\mathrm{Spec}(\mathbf{Q}_p) \to X_0(N)_{\mathbf{Q}_p}$. As $X_0(N)_{\mathbf{Z}_p}$ is proper over $\mathrm{Spec}(\mathbf{Z}_p)$, there exists a unique section $P' : \mathrm{Spec}(\mathbf{Z}_p) \to X_0(N)_{\mathbf{Z}_p}$ making the left square commutative. The existence of $\overline{P} : \mathrm{Spec}(\mathbf{F}_p) \to X_0(N)_{\mathbf{F}_p}$ is automatic from the existence of the section P'.

Since we assumed $p \nmid N$, the curve $X_0(N)_{\mathbf{F}_p}$ is smooth over $\mathrm{Spec}(\mathbf{F}_p)$. We have $j_1(\overline{E}) = j_2(\overline{E}) \neq 0, 1728 \in \mathbf{F}_p$, and the functions $j_1 - j_1(E)$ and $j_2 - j_2(E)$ remain uniformising parameters for the complete discrete valuation ring $\widehat{\mathcal{O}}_{X_0(N)_{\mathbf{F}_p},\bar{P}}$ over $\mathbf{F}_p$. We get $(p, j_1 - j_1(E))$ and $(p, j_2 - j_2(E))$ as parameters for $\mathcal{O}_{X_0(N)_{\mathbf{Z}_p},\bar{P}}$, and the ring $\mathcal{O}_{X_0(N)_{\mathbf{Z}_p},\bar{P}}$ is a 2-dimensional regular local ring. Exactly as in the proof of [17, Theorem 29.7], we get an isomorphism

$$\widehat{\mathcal{O}}_{X_0(N)_{\mathbf{Z}_p},\bar{P}} \cong \mathbf{Z}_p[[j_1 - j_1(E)]]. \qquad \square$$

The map ρ_α fixes the CM-points $\mathrm{Ell}_\Delta(\mathbf{Q}_p)$ and therefore stabilizes every disc. We have constructed an analytic map that has the CM-points as *fixed points*. We will use a kind of Newton iteration to converge to the canonical lift $\tilde{j} \in \mathbf{Q}_p$ of $j(\overline{E}) \in \mathbf{F}_p$ starting from a j-invariant $j(E_1) \in \mathbf{C}_p$ that reduces to $j(\overline{E})$ modulo p. The following lemma gives the derivative of ρ_α in a CM-point, i.e., the first coefficient c_1 in the power series above.

Lemma 4.3. *Let $(\alpha) \subset \mathcal{O}$ be a principal ideal such that $\mathcal{O}/(\alpha)$ is cyclic as an abelian group. Assume that (α) is coprime to p. Then the derivative of ρ_α in $j(\widetilde{E}) \in \mathrm{Ell}_\Delta(\mathbf{Q}_p)$ is given by $\alpha\overline{\alpha}^{-1}$, where $\overline{\alpha}$ is the complex conjugate of α.*

Proof. This is lemma 1 in [5]. The proof there is rooted in a complex analytic setting. The lemma can also be proven completely geometrically; see [7, Proposition 3.3.2]. For convenience, we give the (slightly modified) proof from [5]. The main difference with the proof in [5] is that we have removed the explicit computation of normal forms of ideals.

Let N be the norm of the principal $\mathcal{O}$-ideal (α). We take a curve $E_{\overline{\mathbf{Q}}}$ defined over $\overline{\mathbf{Q}}$ with $j(E_{\overline{\mathbf{Q}}}) = j(E) \in \mathrm{Ell}_\Delta(\mathbf{Q}_p)$. This gives a point $P_{\overline{\mathbf{Q}}} = (E_{\overline{\mathbf{Q}}}, E_{\overline{\mathbf{Q}}}[(\alpha)]) \in Y_0(N)(\overline{\mathbf{Q}})$. After a base change to $\mathbf{C}$, we get a point $P \in Y_0(N)(\mathbf{C})$. We will work with the modular curve $Y_0(N)_{\mathbf{C}}$ over $\mathbf{C}$. The diagram

$$\begin{tikzcd}
Y_0(N)(\mathbf{C}) \arrow[r, two heads] \arrow[rrr, bend left, "j_1"] \arrow[rrd, "j_2"'] & C(\mathbf{C}) \arrow[r, tail] & \mathbf{A}^1(\mathbf{C}) \times \mathbf{A}^1(\mathbf{C}) \arrow[r] \arrow[d] & \mathbf{A}^1(\mathbf{C}) \\
 & & \mathbf{A}^1(\mathbf{C}) &
\end{tikzcd}$$

gives the two functions $j_1, j_2 : Y_0(N)_{\mathbf{C}} \to \mathbf{A}^1_{\mathbf{C}}$ that we have chosen, i.e., we have $j_1((E,G)) = j(E)$ and $j_2((E,G)) = j(E/G)$. For $(E,G) = (E_\tau, \langle 1/N \rangle)$ we have $j_1(E) = j(\tau)$ and $j_2((E_\tau), \langle 1/N \rangle) = j(N\tau)$. Let $F = \mathbf{C}(j_1, j_2)$ be the function field of $Y_0(N)_{\mathbf{C}}$ and let $\Omega_{F/\mathbf{C}}$ be its module of Kähler differentials. The module $\Omega_{F/\mathbf{C}}$ has dimension 1 as a vector space over F. Hence, there is an element $\sigma \in F$ with $\sigma \mathrm{d}j_1 = \mathrm{d}j_2$. We map $Y_0(N)_{\mathbf{C}}$ to the curve C inside $\mathbf{A}^1_{\mathbf{C}} \times \mathbf{A}^1_{\mathbf{C}}$. The function value $\sigma((E, E[(\alpha)])) \in \mathbf{C}$ is the slope of the tangent line at $(j_1(E), j_2(E)) \in C$ at the branch of (E,G). We have $c_1 = \sigma(P)$.

View $Y_0(N)(\mathbf{C})$ as the quotient $\Gamma_0(N)\backslash\mathbf{H}$ and choose a representative $\tau \in \mathbf{H}$ of $P \in Y_0(N)(\mathbf{C})$. Defining $j_N(z) = j(Nz)$, we can compute c_1 as

$$c_1 = \frac{\mathrm{d}j_N}{\mathrm{d}j}(\tau).$$

Let $j' = \frac{\mathrm{d}j}{\mathrm{d}\tau}$ be the derivative of the j-function and let $G_i(\tau)$ be the i-th Eisenstein series attached to the lattice $\langle 1, \tau \rangle$.

Claim. There exists a constant $c \in \mathbf{C}$ with

$$\frac{j'}{j} = c\frac{G_6}{G_4}.$$

Proof of the Claim. The j-function has a triple zero at ζ_3, and has no other zeroes in the standard fundamental domain of $\mathrm{SL}_2(\mathbf{Z})\backslash\mathbf{H}$. The quotient j'/j is a rational modular form of weight 2, with a simple pole at ζ_3.

The quotient G_6/G_4 is a modular form of weight 2 and has a simple pole at ζ_3. There exists a constant $c \in \mathbf{C}$ such that $j'/j - cG_6/G_4$ has no poles on the upper half plane $\mathbf{H}$. We see that $j'/j - cG_6/G_4$ is a modular function of weight 2 which is everywhere holomorphic, including infinity. It is therefore equal to zero, which proves our claim.

We derive $\frac{\mathrm{d}j}{\mathrm{d}\tau}(\tau) = cG_6(\tau)j(\tau)/G_4(\tau)$ and $\frac{\mathrm{d}j_N}{\mathrm{d}\tau}(\tau) = N\frac{\mathrm{d}j}{\mathrm{d}\tau}(N\tau)$, i.e., we have

$$c_1 = \frac{\mathrm{d}j_N}{\mathrm{d}\tau}\frac{\mathrm{d}\tau}{\mathrm{d}j}(\tau) = N\frac{j(N\tau)}{j(\tau)} \cdot \frac{(G_6/G_4)(N\tau)}{(G_6/G_4)(\tau)}.$$

The curve $E_\tau = \mathbf{C}/\langle 1, \tau \rangle$ has endomorphism ring $\mathcal{O}$ and we have a commutative diagram

$$\begin{tikzcd}
\mathbf{C}/\langle 1, \tau \rangle \arrow[rr, "\times N"] \arrow[dr, "\times \alpha"] & & \mathbf{C}/\langle 1, N\tau \rangle \arrow[dl, "\sim"', "\times \frac{\alpha}{N}"] \\
 & \mathbf{C}/\langle 1, \tau \rangle, &
\end{tikzcd}$$

since α is an endomorphism of E_τ. We see that we have $\frac{\alpha}{N}\langle 1, N\tau\rangle = \langle 1, \tau\rangle$, i.e., we get $\alpha\tau = a\tau + b$, $\alpha/N = c\tau + d$ with $\binom{a\,b}{c\,d} \in \mathrm{SL}_2(\mathbf{Z})$. Using the relation $N\tau = (a\tau + b)/(c\tau + d)$, we compute

$$c_1 = N\frac{(G_6/G_4)(N\tau)}{(G_6/G_4)(\tau)} = N(c\tau + d)^2 = \frac{\alpha^2}{N} = \frac{\alpha}{\overline{\alpha}}. \qquad \square$$

To compute the j-invariant of the canonical lift $\widetilde{E}/\mathbf{Q}_p$, we look for a fixed point of ρ_α, i.e., for a zero of the function $\rho_\alpha - \mathrm{id}$. We use a Newton iteration process to converge to a zero of $\rho_\alpha - \mathrm{id}$. Pick an elliptic curve $E_1/\mathbf{C}_p$ that reduces to $\overline{E}/\mathbf{F}_p$ modulo p. Assume that we have $\alpha/\overline{\alpha} - 1 \in \mathbf{Z}_p^*$ and consider the following iteration process:

$$j(E_{k+1}) = j(E_k) - \frac{\rho_\alpha(j(E_k)) - j(E_k)}{(\alpha/\overline{\alpha}) - 1} \qquad \text{for } k \in \mathbf{Z}_{\geq 1}.$$

This computation is carried out with 2-digit precision for $k = 1$, and the precision is doubled in each iteration step. This process is a modified version of Newton iteration. For classical Newton iteration we would need $\rho'_\alpha(j(E_k)) - 1$ in the denominator instead of $(\alpha/\overline{\alpha}) - 1 = \rho'_\alpha(j(\widetilde{E})) - 1$. We are working with bounded precision in each step and we have to check that

$$(*) \qquad \frac{\rho_\alpha(j(E_k)) - j(E_k)}{\rho'_\alpha(j(\widetilde{E})) - 1} = \frac{\rho_\alpha(j(E_k)) - j(E_k)}{\rho'_\alpha(j(E_k)) - 1} \in \mathbf{Z}_p/(p^{2^k})$$

holds in the k-th iteration step. For $k = 1$, we have $j(E_1) = j(\widetilde{E}) \bmod p$, and therefore also $\rho'_\alpha(j(E_1)) = \rho'_\alpha(j(\widetilde{E})) \bmod p$. As $\rho_\alpha(j(E_1)) - j(E_1)$ is divisible by p, we see that $(*)$ holds for $k = 1$, i.e., modulo p^2. Now suppose $k > 1$. With induction we see that $j(E_k) = j(\widetilde{E}) \bmod p^{2^{k-1}}$ holds and $\rho_\alpha(j(E_k)) - j(E_k)$ is divisible by $p^{2^{k-1}}$. We conclude that equality $(*)$ holds for all $k \in \mathbf{Z}_{\geq 1}$, and that for $\alpha/\overline{\alpha} - 1 \in \mathbf{Z}_p^*$, the process above converges to the canonical lift $\tilde{\jmath} = j(\widetilde{E}) \in \mathbf{Q}_p$.

5. Computing the kernel polynomial

The description of the algorithm in Section 4 is not yet suited for explicit computations, and in this section we explain how to compute, given a degree one prime ideal $\mathfrak{l} \subset \mathcal{O}$ of norm l with $l \nmid p\Delta$ and an ordinary elliptic curve $\overline{E}/\mathbf{F}_p$ with $\mathrm{End}(\overline{E}) = \mathcal{O}$, the value $\overline{\rho}_\mathfrak{l}(j(\overline{E})) \in \mathbf{F}_p$. We will have to make some extra conditions on $\mathfrak{l}$ in this section. In Section 7 we prove that there are enough 'smooth' $\alpha \in \mathcal{O}$ such that all prime ideals $\mathfrak{l}_i$ dividing (α) satisfy our conditions.

Let $\widetilde{\mathcal{O}}$ be the order of discriminant $t^2 - 4p$, where t is the trace of the Frobenius morphism of $\overline{E}$.

Theorem 5.1. *Let $\overline{E}/\mathbf{F}_p$, $\mathfrak{l}$ and $\widetilde{\mathcal{O}}$ be as above. Then we have*

$$\Phi_l(j(\overline{E}), \overline{\rho}_\mathfrak{l}(j(\overline{E}))) = 0,$$

where Φ_l denotes the classical l-th modular polynomial. If the order $\widetilde{\mathcal{O}}$ is maximal at l, then the polynomial

$$\Phi_l(j(\overline{E}), X) \in \mathbf{F}_p[X]$$

has exactly 2 roots in $\mathbf{F}_p$.

Proof. The first statement in the theorem follows immediately from the properties of the modular polynomial. Indeed, for any algebraically closed field $k = \bar{k}$ of characteristic $\mathrm{char}(k) \neq l$ and for any $j \in k$, the roots of $\Phi_l(j, X) \in k[X]$ are exactly the j-invariants of curves that are l-isogenous to a curve with j-invariant j. We know that $\overline{\rho}_{\mathfrak{l}}(j(\overline{E}))$ is contained in $\mathbf{F}_p$, and the first result follows.

By assumption, the order $\mathcal{O}$ is maximal at l. By [2, Corollary 5.12] or [12, Proposition 23] there are two possibilities for the number of roots of $\Phi_l(j(\overline{E}), X) \in \mathbf{F}_p[X]$. If the index $[\mathcal{O} : \widetilde{\mathcal{O}}]$ is divisible by l, there are $l + 1$ roots, and there are $\left(\frac{\Delta}{l}\right) + 1 = 2$ roots otherwise. The second result follows. □

Assume that $\widetilde{\mathcal{O}}$ is maximal at l, and fix a root $h \in \mathbf{F}_p$ of $\Phi_l(j(\overline{E}), X) \in \mathbf{F}_p[X]$. We either have $h = \overline{\rho}_{\mathfrak{l}}(j(\overline{E}))$ or $h = \overline{\rho}_{\overline{\mathfrak{l}}}(j(\overline{E}))$, where $\overline{\mathfrak{l}}$ is the complex conjugate of $\mathfrak{l}$, and in the remainder of this section we explain how to find out which case we are in.

Let $\overline{E}/C$ have j-invariant h, corresponding to a cyclic subgroup $C \subset \overline{E}[l]$ of order l, i.e., C is the kernel of the isogeny $\overline{E} \to \overline{E}/C$. The techniques that Elkies used to improve Schoof's original point counting algorithm [19, Sections 7, 8] allow us to compute, given $h \in \mathbf{F}_p$, a polynomial $f_C \in \mathbf{F}_p[X]$ that vanishes exactly on the x-coordinates of the points in C. We refer to [19] for the algorithm to compute $f_C \in \mathbf{F}_p[X]$. In order to apply this algorithm we need to assume that

$$|\Delta| \leq 4l^2$$

holds.

Write $\mathfrak{l} = (l, c + d\pi_p)$, with $l \nmid d$. Here, $\pi_p \in \mathcal{O}$ is the image of the Frobenius $F_p \in \mathrm{End}(\overline{E})$ under the fixed isomorphism $\mathrm{End}(\overline{E}) \xrightarrow{\sim} \mathcal{O}$.

The Frobenius acts on $\mathfrak{l} \subset \overline{E}[l]$ as multiplying by $-c/d \in \mathbf{F}_l$. We test if

$$(X^p, Y^p) = (-c/d) \cdot (X, Y) \tag{5.1}$$

holds for the points in C, i.e., we compute both (X^p, Y^p) and $(-c/d) \cdot (X, Y)$ in the ring

$$\mathbf{F}_p[X, Y]/(f_C(X), Y^2 - X^3 - aX - b).$$

Note that the $\cdot$ means repeated adding *on the curve*, and $(-c/d) \cdot (X, Y)$ can be computed by employing division polynomials.

If equality (5.1) holds, we have $h = \overline{\rho}_{\mathfrak{l}}(j(\overline{E}))$. Otherwise, the unique other zero of

$$\gcd(X^p - X, \Phi_l(j(\overline{E}), X)) \in \mathbf{F}_p[X]$$

equals $\overline{\rho}_{\mathfrak{l}}(j(\overline{E})) \in \mathbf{F}_p$.

6. Algorithm for computing the canonical lift

In this section we give the algorithm to compute the canonical lift $\tilde{\jmath} \in \mathbf{Q}_p$ of an ordinary j-invariant $j(\overline{E}) \neq 0, 1728 \in \mathbf{F}_p$ of an elliptic curve $\overline{E}$ with endomorphism ring $\mathrm{End}(\overline{E}) = \mathcal{O} = \mathcal{O}_\Delta$. We can choose the element $\alpha \in \mathcal{O}$ that we use for the map $\rho_\alpha : X_\Delta(\mathbf{C}_p) \to X_\Delta(\mathbf{C}_p)$ ourselves. We recall the conditions that α should satisfy.

1. α is contained in $\mathbf{Z}[F_p] \cong \widetilde{\mathcal{O}}$,
2. α is primitive,
3. $\alpha/\overline{\alpha} - 1$ is a p-adic unit,
4. for any prime divisor l of $N(\alpha)$, we have $l \nmid [\mathcal{O} : \widetilde{\mathcal{O}}]$,
5. for any prime divisor l of $N(\alpha)$, we have $l < \sqrt{-\Delta/4}$.

The input of the algorithm below consists of an ordinary curve $\overline{E}/\mathbf{F}_p$ with j-invariant $j(\overline{E}) \neq 0, 1728 \in \mathbf{F}_p$, an element $\alpha \in \mathcal{O} \setminus \mathbf{Z}$ satisfying the conditions above, together with the factorization $(\alpha) = \prod_i \mathfrak{l}_i$ into prime ideals, and a positive integer k. The output is the canonical lift $\tilde{\jmath} = j(\widetilde{E}) \in \mathbf{Q}_p$ in k-digit accuracy.

Step 1. As in Section 5, compute the polynomial $\overline{f}_{\mathfrak{l}_1} \in \mathbf{F}_p[X]$ corresponding to the subgroup $\overline{E}[\mathfrak{l}_1] \subset \overline{E}[l_1]$. In the same way, we compute a cycle of isogenies

$$(*) \qquad \overline{E} \xrightarrow{\mathfrak{l}_1} \overline{E}^{\mathfrak{l}_1} \longrightarrow \cdots \xrightarrow{\mathfrak{l}_n} \overline{E}^{(\alpha)} \cong \overline{E}$$

over $\mathbf{F}_p$. The isomorphism $\overline{E}^{(\alpha)} \cong \overline{E}$ follows from the fact that principal ideals act trivially. This is a good check for our computations so far.

Step 2. Choose an arbitrary lift $E_1/\mathbf{Q}_p$, in two p-adic digits precision, of $\overline{E}/\mathbf{F}_p$.

Step 3. Lift the cycle $(*)$ of isogenies over $\mathbf{F}_p$ to a 'cycle' of isogenies over $\mathbf{Q}_p$ in the following way. For $l = l_1$, we lift $j(\overline{E}^{\mathfrak{l}_1}) \in \mathbf{F}_p$ to $\mathbf{Z}_p$ as a root of $\Phi_l(j(E_1), X) \in \mathbf{Z}_p[X]$ to $h \in \mathbf{Z}_p$. Here Φ_l is the l-th modular polynomial. We use Hensel's lemma for this lifting process. Hensel requires that $\frac{\mathrm{d}}{\mathrm{d}X}\Phi_l(j(\overline{E}), X)$ is non-zero when evaluated in $X = j(\overline{E}^{\mathfrak{l}_1}) \in \mathbf{F}_p$. This requirement is satisfied by assumption 5. We have $h = \rho_{\mathfrak{l}}(j(E_1))$. In the same way, we compute the 'cycle' of j-invariants

$$j(E_1) \xrightarrow{\rho_{\mathfrak{l}_1}} j(E_1)^{\mathfrak{l}_1} \longrightarrow \cdots \xrightarrow{\rho_{\mathfrak{l}_n}} j(E_1)^{(\alpha)}$$

over $\mathbf{Q}_p$. This computation is carried out with two p-adic digit precision.

Step 4. Update $j(E_1)$ according to the Newton formula

$$j(E_{k+1}) = j(E_k) - \frac{\rho_\alpha(j(E_k)) - j(E_k)}{(\alpha/\bar{\alpha}) - 1} \qquad \text{for } k \in \mathbf{Z}_{\geq 1}$$

to find $j(E_2) \in \mathbf{Z}_p$. The value $j(E_2)$ is the two digit approximation of the canonical lift $j(\widetilde{E})$.

Step 5. Lift the cycle $(*)$ to a 'cycle' of j-invariants

$$j(E_2) \xrightarrow{\rho_{\mathfrak{l}_1}} j(E_2)^{\mathfrak{l}_1} \longrightarrow \cdots \xrightarrow{\rho_{\mathfrak{l}_n}} j(E_2)^{(\alpha)}$$

over $\mathbf{Q}_p$. This computation is carried out with four p-adic digit precision. Update $j(E_2)$ according to the Newton formula above. The value $j(E_3)$ is the four digit approximation of the canonical lift $j(\widetilde{E})$.

Step 6. Repeat Step 5 with E_2 replaced by E_k with $k = 3, 4$, etc. until we have computed $j(\widetilde{E}) \in \mathbf{Z}_p$ with the desired precision. The precision is doubled in each iteration step.

Remark. There is a different way to lift the cycle $(*)$ of isogenies in Step 3. The polynomial $\overline{f}_{\mathfrak{l}}$ has a unique Hensel lift to a factor $f_{\mathfrak{l}} \in \mathbf{Z}_p[X]$ of the l-th division polynomial Ψ_l of E_1. This lift is the algorithmic version of the group scheme from Section 4: every choice of E_1 gives us a subgroup $E_1[\mathfrak{l}] \subset E_1[l]$. Computing the isogenous curve $E_1^{\mathfrak{l}}$ is now easy, since we can apply 'Vélu's formulas' [25]. This approach has the disadvantage that lifting $\overline{f}_{\mathfrak{l}} \in \mathbf{F}_p[X]$ to $f_{\mathfrak{l}} \in \mathbf{Z}_p[X]$ is rather 'expensive'. Indeed, the polynomial $\overline{f}_{\mathfrak{l}}$ has degree $(l-1)/2$ for $l > 2$. In our approach in Step 3, we only perform a simple Hensel lift of a zero of a polynomial of degree $l + 1$.

The runtime of this algorithm depends heavily on the primes l_i, i.e., on the smoothness properties of (α). In computing the canonical lift of $\overline{E}/\mathbf{F}_p$, we have the freedom to choose $\alpha \in \mathcal{O}$ ourselves. Subject to the 5 conditions from the beginning of this section, we want (α) to be *smooth*, i.e., the norm $N(\alpha)$ should be smooth.

Write $\alpha = c + d\pi_p$, with $\gcd(c, d) = 1$ and with $d \neq 0$. Here $\pi_p \in \mathbf{Z}[\pi_p] = \widetilde{\mathcal{O}}$ is an element of norm p. Condition 3 is satisfied precisely when p does not divide $2d\pi_p$. We conclude that $\alpha/\overline{\alpha} - 1$ will be a p-adic unit for $p > d$.

The following lemma guarantees that there are enough smooth elements α satisfying our conditions.

Lemma 6.1. *Let $\varepsilon \in (0, 1/2)$ be a real number and let π_p be imaginary quadratic with minimal polynomial $\pi_p^2 - t\pi_p + p = 0$. Put $t^2 - 4p = \widetilde{\Delta}$ and $B = \lfloor \exp(\sqrt{\log|\widetilde{\Delta}|}) \rfloor$. Let A_ε be the set of $c + d\pi_p \in \mathbf{Z}[\pi_p]$ with $c \in \mathbf{Z}$ and $1 \leq d \leq 2\exp((\log|\widetilde{\Delta}|)^{1/2+\varepsilon})$ satisfying the properties*

- ◇ $|c + \frac{1}{2}dt| \leq |\widetilde{\Delta}|^{1/2}\exp((\log|\widetilde{\Delta}|)^{1/2+\varepsilon})$,
- ◇ *c and d are coprime,*
- ◇ *$c + d\pi_p$ and $p\widetilde{\Delta}$ are coprime. If GRH holds true, the fraction of B-smooth elements in A_ε is at least*

$$\exp(-2(\log|\widetilde{\Delta}|)^{1/2}\log\log|\widetilde{\Delta}|)$$

for $|\widetilde{\Delta}|$ large enough, depending on ε.

Proof. This is lemma 2 in [5]. □

An element $\alpha \in \mathbf{Z}[\pi_p]$ satisfying the conditions of Lemma 6.1 automatically satisfies the 5 conditions from the beginning of this section.

We find a suitable α by sieving in the set

$$S = \{c + d\pi_p : c, d \in \mathbf{Z}, d \neq 0, (c, d) = 1, c + d\pi_p \text{ and } p\widetilde{\Delta} \text{ are coprime}\},$$

where $\widetilde{\Delta}$ is the discriminant of $\widetilde{\mathcal{O}}$.

Proof of Theorem 4.1. Fix a real number $\varepsilon \in (0, 1/2)$. We sieve for a smooth element $\alpha \in \mathbf{Z}[\pi_p] \setminus \mathbf{Z}$. Next we apply the Algorithm from this section, with this principal ideal (α), to compute the j-invariant of the canonical lift in k-digit accuracy.

It remains to analyse the runtime of the Algorithm. Searching in

$$\{c + d\pi_p : c, d \in \mathbf{Z}, d \neq 0, (c, d) = 1, c + d\pi_p \text{ and } p\widetilde{\Delta} \text{ are coprime}\}$$

for a suitable B-smooth element α takes probabilistic time $O(\exp(\sqrt{\log p}\log\log p)^4)$ by Lemma 6.1, with $B = \lfloor \exp(\sqrt{\log p}) \rfloor$. Here, we used the estimate

$$|\widetilde{\Delta}| \leq 4p.$$

In the first step of the Algorithm we compute the cycle of isogenies over $\mathbf{F}_p$ corresponding to the map ρ_α. We only have to perform 'simple' tasks in this step, like computing a modular polynomial, Euclidean division, computing a root of $\Phi_l(j(\overline{E}), X) \in \mathbf{F}_p[X]$, etc. We compute the cycle in time $O((B^2(\log p)^3)^{1+o(1)})$.

In Steps 3, 5 and 6 we lift the cycle to a 'cycle' of isogenies over $\mathbf{Z}_p$. Fix an integer $n \in \mathbf{Z}_{>0}$ and assume that we have computed the cycle over $\mathbf{Z}_p/(p^{2^n})$. Lifting the cycle to $\mathbf{Z}_p/(p^{2^{n+1}})$ boils down to evaluating the modular polynomial and some Hensel lifts. We can lift the cycle in time $O(B^2 2^{n+1}(\log p)^2)$.

Combining the sieving step, the computation of the cycle over $\mathbf{F}_p$ and the lifting process, we see that the expected runtime is $O(B^{4+\varepsilon}(\log p)^{3+\varepsilon}k\log k)$, which proves the theorem. □

Remark. Instead of sieving for a smooth element $\alpha \in S$, we can also pick the smallest prime l that splits in the order $\widetilde{\mathcal{O}}$ of discriminant $\widetilde{\Delta}$. Write $(l) = \mathfrak{l}\bar{\mathfrak{l}}$ and let n be the order of $\mathfrak{l} \in \operatorname{Pic}(\widetilde{\mathcal{O}})$. Now let α be a generator of the principal ideal $\mathfrak{l}^n$. If GRH holds true, the Bach bound yields that l is of size $O((\log|\widetilde{\Delta}|)^2)$, but unfortunately we do not have any guarantee that $\alpha/\overline{\alpha} - 1$ is a p-adic unit. In practice this condition never poses a problem. Computing the canonical lift $\tilde{\jmath}$ may take a lot more time, however. Indeed, as class groups are 'often' cyclic it might very well be that $[\mathfrak{l}] \in \operatorname{Pic}(\mathcal{O})$ generates the Picard group. The length of the cycle of isogenies over $\mathbf{F}_p$ then becomes $\widetilde{O}(|\Delta|^{1/2})$ instead of $O((\log|\widetilde{\Delta}|)^{1+o(1)})$ for the sieving method.

7. Computing the Hilbert class polynomial

Once we have computed one element $j \in \operatorname{Ell}_\Delta(\mathbf{Q}_p)$ with high enough accuracy, it is an easy matter to compute its conjugates under the action of the Picard group $\operatorname{Pic}(\mathcal{O})$. Namely, let $l = \mathfrak{l}\bar{\mathfrak{l}}$ be a prime that splits in $\mathcal{O}$. The conjugates of $j \in \operatorname{Ell}_\Delta(\mathbf{Q}_p)$ under the action of $[\mathfrak{l}], [\bar{\mathfrak{l}}] \in \operatorname{Pic}(\mathcal{O})$ are the 2 roots of $\Phi_l(j, X) \in \mathbf{Z}_p[X]$. If GRH holds true, we can compute a set of primes S generating $\operatorname{Pic}(\mathcal{O})$ with the property that the largest element of S does not exceed the Bach bound $O((\log|\Delta|)^2)$.

The logarithmic height of the zeroes of $P_\Delta \in \mathbf{C}[X]$ is well known. Let S_Δ be the set of reduced primitive positive definite quadratic forms $[a,b,c] = aX^2+bXY+cY^2$ of discriminant $b^2 - 4ac = \Delta$. Recall that a form $[a,b,c]$ is said to be *reduced* if we have $|b| \leq a \leq c$ and moreover $b \geq 0$ if one of the inequalities is an equality. The largest coefficient of P_Δ has logarithmic height bounded by

$$2h(\Delta) + \frac{\pi\sqrt{|\Delta|}}{\log 10} \sum_{[a,b,c]\in S_\Delta} \frac{1}{a},$$

where $h(\Delta)$ is the class number of $\mathcal{O} = \mathcal{O}_\Delta$; cf. [1].

Algorithm (Non-archimedean algorithm)**.**

Input: a discriminant $\Delta < -4$. Output: the Hilbert class polynomial $P_\Delta \in \mathbf{Z}[X]$.

1. *Apply the algorithm from Section 3 to find a prime p and an ordinary elliptic curve $\overline{E}/\mathbf{F}_p$ with* $\operatorname{End}(\overline{E}) = \mathcal{O}_\Delta$.

2. *Put* $k \leftarrow \left\lceil \left(\frac{\pi\sqrt{|\Delta|}}{\log p} \sum_{[a,b,c]\in S_\Delta} \frac{1}{a}\right) + \log_p\binom{h}{\lfloor h/2\rfloor} \right\rceil$, *with* $h = h(\Delta)$.

3. *Compute the canonical lift $\tilde{\jmath} \in \mathbf{Q}_p$ of $j(\overline{E}) \in \mathbf{F}_p$ up to k p-adic digit accuracy using the algorithm from Section 6.*

4. *Compute a complete set C of conjugates of $\tilde{\jmath}$ under the action of* $\operatorname{Pic}(\mathcal{O})$ *in k p-adic digits accuracy.*

5. *Put* $P_\Delta = \prod_{j\in C}(X - j) \in (\mathbf{Z}_p/(p^k))[X]$.

6. *Lift the coefficients of P_Δ from $\mathbf{Z}_p/(p^k) = \mathbf{Z}/(p^k)$ to $\mathbf{Z}$, where we take the representative between $-p^k/2$ and $p^k/2$. Return $P_\Delta \in \mathbf{Z}[X]$.*

Theorem 7.1. *If GRH holds true, then the non-archimedean algorithm has an expected runtime $O(|\Delta|(\log|\Delta|)^{8+\varepsilon})$ for every $\varepsilon > 0$.*

Proof. The runtime of Step 1 is $\widetilde{O}(|\Delta|^{1/2})$. To estimate the runtime of Step 3, we apply Theorem 4.1 with the k from Step 2. We have $k = O(\sqrt{|\Delta|}(\log|\Delta|)^2)$ by [21, Lemma 2.2], and we can compute the j-invariant of the canonical lift of $\overline{E}$ with high enough accuracy in time $O(|\Delta|^{1/2+o(1)})$. Computing one conjugate with k-digit accuracy in Step 4 takes time $O(|\Delta|^{1/2}(\log|\Delta|)^{7+o(1)})$; the bottleneck is evaluating a modular polynomial $\Phi_l(X, Y)$ of degree $O((\log|\Delta|)^2)$ in $X = j(\widetilde{E})$. Using the estimate $h(\Delta) \leq \sqrt{|\Delta|}\log|\Delta|$, we can compute all conjugates in time $O(|\Delta|(\log|\Delta|)^{8+o(1)})$. This dominates the time needed for the 'divide-and-conquer' algorithm, as in [10, Section 10.1], to compute the polynomial in Step 5. □

► **Implementation details**

We give some tricks to speed up an implementation of the non-archimedean algorithm. First of all, it is a good idea to precompute a reasonable amount of modular polynomials. Experience has shown that computing the first 25 polynomials, i.e., for primes up to 100, suffices for discriminants down to -10^{12}.

One can save some time in computing the cycles of isogenies over $\mathbf{F}_p$. Let $\overline{E}/\mathbf{F}_p$ be an elliptic curve with $\mathrm{End}(\overline{E}) = \mathcal{O}$ and let $\mathfrak{l} \subset \mathcal{O}$ be of norm $l \neq p$. After we have computed a root $h \in \mathbf{F}_p$ of $\Phi_l(j(\overline{E}), X) \in \mathbf{F}_p[X]$ we have to check if h equals $\overline{\rho}_{\mathfrak{l}}(j(\overline{E}))$ and not $\overline{\rho}_{\overline{\mathfrak{l}}}(j(\overline{E}))$. In many cases this check can be performed very easily. Namely, suppose that $\mathfrak{l}^2$ divides (α), i.e., we have to compute the map $\overline{\rho}_{\mathfrak{l}}$ twice. The first time we apply the check proposed at the end of Section 5. The j-invariant $\overline{\rho}_{\mathfrak{l}^2}(j(\overline{E})) \in \mathbf{F}_p$ can now be computed more easily. Namely, we compute the 2 roots in $\mathbf{F}_p$ of $\Phi_l(\overline{\rho}_{\mathfrak{l}}(j(\overline{E})), X) \in \mathbf{F}_p[X]$ and note that one of these roots has to be the j-invariant of $\overline{E}$, and hence we know right away which root is $\overline{\rho}_{\mathfrak{l}^2}(j(\overline{E}))$.

Finally, the upper bound

$$k = \Big(\frac{\pi\sqrt{|\Delta|}}{\log p}\sum_{[a,b,c]\in S_\Delta}\frac{1}{a}\Big) + \log_p\binom{h}{\lfloor h/2\rfloor}$$

for the required precision is somewhat pessimistic. Practical experience has shown that for discriminants down to -10^{12} it suffices to work with

$$k = \frac{\pi\sqrt{|\Delta|}}{\log p}\sum_{[a,b,c]\in S_\Delta}\frac{1}{a} + 10$$

p-adic digits. This is a significant speed up in the practical performance of the algorithm.

8. Example

We illustrate the non-archimedean algorithm by computing the Hilbert class polynomial P_Δ for $\Delta = -639 = -3^2 \cdot 71$. First we find a finite field $\mathbf{F}_p$ and an elliptic curve $\overline{E}/\mathbf{F}_p$ with endomorphism ring $\mathcal{O} = \mathcal{O}_\Delta$.

We apply the algorithm from Section 2. As we have $\Delta \equiv 1 \bmod 8$, the equation $4p = t^2 - \Delta$ has no solutions with p prime. The smallest integer $t > 0$ for which $(t^2 - 4\Delta)/4$ is prime is $t = 4$, leading to $p = 643$. We fix p for the rest of this section. We apply the naïve algorithm and look for a curve with $p + 1 \pm t$ points. We find that the curve $\overline{E}/\mathbf{F}_p$ defined by

$$Y^2 = X^3 + 89X - 89$$

of j-invariant $j(\overline{E}) = 295 \in \mathbf{F}_p$ has trace of Frobenius 4.

Let $\mathcal{O}_K$ be the maximal order of $K = \mathbf{Q}(\sqrt{\Delta})$. We have inclusions

$$\mathbf{Z}[F_p] \overset{2}{\subset} \mathcal{O} \overset{3}{\subset} \mathcal{O}_K,$$

and we have to compute the endomorphism ring of $\overline{E}$. The 2-division polynomial $X^3+89X-89 \in \mathbf{F}_p[X]$ splits completely, showing that $\overline{E}$ has CM by $\mathcal{O}$. The prime 3 splits in $\mathcal{O}_K$. If $\overline{E}$ has CM by $\mathcal{O}_K$, the modular polynomial $\Phi_3(j(\overline{E}), X) \in \mathbf{F}_p[X]$ has 4 roots in $\mathbf{F}_p$ as the proof of Theorem 5.1 shows. We compute

$$\gcd(\Phi_3(j(\overline{E}), X), X^p - X) = X - 429 \in \mathbf{F}_p[X]$$

and conclude that $\overline{E}$ does not have CM by $\mathcal{O}_K$, and therefore has endomorphism ring $\mathcal{O}$. We need to compute the canonical lift $\widetilde{E}/\mathbf{Q}_p$ up to k p-adic digit accuracy, with

$$k \approx \frac{\pi\sqrt{|\Delta|}}{\log p} \sum_{[a,b,c]\in S_\Delta} \frac{1}{a}.$$

The Picard group $\mathrm{Pic}(\mathcal{O})$ has order 14, and representing the elements as binary quadratic forms as in Section 7, we find $k \approx 44$. We will compute $j(\widetilde{E}) \in \mathbf{Q}_p$ up to 45 p-adic digit precision.

As a smooth element $\alpha \in \mathcal{O} \setminus \mathbf{Z}$ for the map $\rho_\alpha : X_\Delta(\mathbf{C}_p) \to X_\Delta(\mathbf{C}_p)$ we will use $\alpha = \pi_p - 108$ of norm $11875 = 5^4 \cdot 19$. Here, $\pi_p = \frac{4+\sqrt{\Delta}}{2}$ is an element of norm p. We factor

$$(\alpha) = \mathfrak{p}_5^4 \cdot \mathfrak{p}_{19} = (5, \pi_p - 3)^4 \cdot (19, \pi_p - 13).$$

We compute the action of the prime ideal $\mathfrak{p}_5$ on $j(\overline{E}) \in \mathbf{F}_p$. If we evaluate the modular polynomial $\Phi_5(X, Y) \in \mathbf{F}_p[X, Y]$ in $X = j(\overline{E}) = 295$ we get a polynomial that has 2 roots in $\mathbf{F}_p$, namely 449 and 532. From this we deduce that $\mathfrak{p}_5$ sends $j(\overline{E})$ to one of these roots. We do not know which one yet.

Let $\overline{E}/C$ have j-invariant $449 \in \mathbf{F}_p$, corresponding to a cyclic subgroup $C \subset \overline{E}[5]$. We either have $C = \overline{E}[\mathfrak{p}_5]$ or $C = \overline{E}[\overline{\mathfrak{p}}_5]$. Using the method from Section 5, we compute the Weierstraß equation

$$Y^2 = X^3 + 390X + 466$$

for $\overline{E}/C$. We get the x-coordinates of the points in C as zeroes of

$$\overline{f}_C = X^2 + 614X + 471 \in \mathbf{F}_p[X].$$

The eigenvalue for the action of Frobenius on the torsion $\overline{E}[\mathfrak{p}_5]$ is $3 \in \mathbf{F}_5$. We now check whether

$$(X^p, Y^p) = 3 \cdot (X, Y)$$

holds for the points in C, i.e., we compute both (X^p, Y^p) and $3 \cdot (X, Y)$ in the ring

$$\mathbf{F}_p[X, Y]/(\overline{f}_C, Y^2 - X^3 - 89X + 89).$$

Here, the $\cdot$ means adding *on the curve*. It turns out that (X^p, Y^p) and $3 \cdot (X, Y)$ are the same. We deduce that we have $j(\overline{E})^{\mathfrak{p}_5} = 449 \in \mathbf{F}_p$.

The action of $\mathfrak{p}_5$ on the j-invariant $449 \in \mathbf{F}_p$ is now easier to compute. The polynomial $\Phi_5(449, X) \in \mathbf{F}_p[X]$ has 2 roots in $\mathbf{F}_p$, but one of these roots corresponds to the action of $\overline{\mathfrak{p}}_5$ and is therefore equal to $j(\overline{E})$. We pick the other root $73 \in \mathbf{F}_p$. If we compute the entire cycle of j-invariants over $\mathbf{F}_p$, we get

$$295 \xrightarrow{\mathfrak{p}_5} 449 \xrightarrow{\mathfrak{p}_5} 73 \xrightarrow{\mathfrak{p}_5} 55 \xrightarrow{\mathfrak{p}_5} 328 \xrightarrow{\mathfrak{p}_{19}} 295.$$

We knew beforehand that this cycle is closed, since we know that (α) acts trivially on $j(\overline{E})$.

We now lift $\overline{E}/\mathbf{F}_p$ to $E_1/\mathbf{Q}_p$ by lifting the coefficients of its Weierstraß equation arbitrarily. The polynomial $\Phi_5(j(E_1), X) \in \mathbf{Z}_p[X]$ has exactly 2 roots, one of which reduces to $449 \in \mathbf{F}_p$. Taking the lift $E_1/\mathbf{Q}_p$ defined by $Y^2 = X^3 + 89X - 89$ of j-invariant $295 - 233p + O(p^2) \in \mathbf{Q}_p$, we compute the 'cycle'

$$j(E_1) \xrightarrow{\mathfrak{p}_5} -194+296p \xrightarrow{\mathfrak{p}_5} 73-236p \xrightarrow{\mathfrak{p}_5} 55+155p \xrightarrow{\mathfrak{p}_5} -315+131p \xrightarrow{\mathfrak{p}_{19}} 295-236p$$

over $\mathbf{Q}_p$. We update $j(E_1)$ according to the 'Newton formula'

$$j(E_{k+1}) = j(E_k) - \frac{\rho_\alpha(j(E_k)) - j(E_k)}{(\alpha/\overline{\alpha}) - 1} \qquad \text{for } k \in \mathbf{Z}_{\geq 1}$$

and find that $j(E_2) = 295 - 155p$ is the two digit approximation of the j-invariant of the canonical lift $\widetilde{E}/\mathbf{Q}_p$.

Starting from $j(E_2)$, we now lift the cycle to four p-adic digit precision, compute $j(E_3)$ from this, and so on. We obtain

$$\begin{aligned}
j(\widetilde{E}) &= 295 + O(p) \\
&= 295 - 155p + O(p^2) \\
&= 295 - 155p + 195p^2 + 287p^3 + O(p^4) \\
&= 295 - 155p + 195p^2 + 287p^3 - 153p^4 + 245p^5 + 272p^6 + 298p^7 + O(p^8) \\
&= 295 - 155p + 195p^2 + 287p^3 - 153p^4 + 245p^5 + 272p^6 + 298p^7 - 277p^8 \\
&\qquad + 170p^9 - 123p^{10} - 86p^{11} - 165p^{12} - 115p^{13} + 195p^{14} + 56p^{15} + O(p^{16}).
\end{aligned}$$

We continue this process until we have computed the canonical lift in 45 p-adic digit accuracy.

Next, we compute the conjugates of $j(\widetilde{E})$ under $\mathrm{Gal}(H_{\mathcal{O}}/K) \cong \mathrm{Pic}(\mathcal{O})$. The Picard group $\mathrm{Pic}(\mathcal{O})$ is cyclic of order 14 and is generated by a prime of norm 5. We compute the conjugates of $j(\widetilde{E})$ by employing the modular polynomial Φ_5: the roots of $\Phi_5(j(\widetilde{E}), X) \in \mathbf{Z}_p[X]$ give us the conjugates $j(\widetilde{E})^{\mathfrak{p}_5}$ and $j(\widetilde{E})^{\overline{\mathfrak{p}}_5}$, etc. In the end we expand the degree 14 polynomial

$$P_{-639} = \prod_{[I] \in \mathrm{Pic}(\mathcal{O})} (X - j(\widetilde{E})^I) \in \mathbf{Z}[X].$$

The polynomial P_{-639} has coefficients up to 126 decimal digits.

Acknowledgements

I thank Jean-Marc Couveignes, Bas Edixhoven, Thierry Henocq and Peter Stevenhagen for helpful discussions.

References

1. A. Agashe, K. Lauter, R. Venkatesan, *Constructing elliptic curves with a known number of points over a prime field*, High Primes and Misdemeanours: lectures in honour of the 60th birthday of H. C. Williams, Fields Institute Communications Series, vol. 41, 2004, pp. 1–17. MR2075643 (2005m:11112)
2. R. Bröker, *Constructing elliptic curves of prescribed order*, Ph.D. thesis, Universiteit Leiden, 2006.
3. H. Cohen, *A course in computational algebraic number theory*, Springer Graduate Texts in Mathematics, vol. 138, 1993. MR1228206 (94i:11105)

4. H. Cohen, G. Frey et al., *Handbook of elliptic and hyperelliptic curve cryptography*, Chapman & Hall, 2006. MR2162716 (2007f:14020)
5. J.-M. Couveignes, T. Henocq, *Action of modular correspondences around CM-points*, Algorithmic Number Theory Symposium V, Springer Lecture Notes in Computer Science, vol. 2369, 2002, pp. 234–243. MR2041087 (2005b:11077)
6. F. Diamond, J. Im, *Modular forms and modular curves*, Seminar on Fermat's last theorem, CMS conference proceedings, vol. 17, 1995, pp. 39–133. MR1357209 (97g:11044)
7. S. J. Edixhoven, *Stable models of modular curves and applications*, Ph.D. thesis, Universiteit Utrecht, 1989.
8. A. Enge, *The complexity of class polynomial computation via floating point approximations*, Preprint, 2006.
9. J. Franke, T. Kleinjung, F. Morain, T. Wirth, *Proving the primality of very large numbers with fastECPP*, Algorithmic Number Theory Symposium VI, Springer Lecture Notes in Computer Science, vol. 3076, 2004, pp. 194–207. MR2137354 (2006a:11172)
10. J. von zur Gathen, J. Gerhard, *Modern computer algebra*, Cambridge University Press, 1999. MR1689167 (2000j:68205)
11. G. H. Hardy, E. M. Wright, *An introduction to the theory of numbers*, Oxford University Press, 1938. MR0067125 (16:673c)
12. D. Kohel, *Endomorphism rings of elliptic curves over finite fields*, Ph.D. thesis, University of California at Berkeley, 1996.
13. J. C. Lagarias, A. M. Odlyzko, *Effective versions of the Chebotarev density theorem*, Algebraic Number Fields, ed. A. Fröhlich, Academic Press, 1977, pp. 409–465. MR0447191 (56:5506)
14. S. Lang, *Elliptic functions*, Springer Graduate Texts in Mathematics, vol. 112, 1987. MR890960 (88c:11028)
15. H. W. Lenstra, Jr., *Factoring integers with elliptic curves*, Ann. of Math. (2) **126** (1987), 649–673. MR916721 (89g:11125)
16. H. W. Lenstra, Jr., C. Pomerance, *A rigorous time bound for factoring integers*, J. Amer. Math. Soc. **5** (1992), 483–516. MR1137100 (92m:11145)
17. H. Matsumura, *Commutative ring theory*, Cambridge Studies in Advanced Mathematics, vol. 8, 1986. MR879273 (88h:13001)
18. J. Neukirch, *Algebraic number theory*, Springer, Grundlehren der mathematischen Wissenschaften, vol. 322, 1999. MR1697859 (2000m:11104)
19. R. Schoof, *Counting points on elliptic curves over finite fields*, J. Théor. Nombres Bordeaux **7** (1993), 219–254. MR1413578 (97i:11070)
20. R. Schoof, *Nonsingular plane cubic curves over finite fields*, J. Combin. Theory Ser. A **46** (1987), 183–211. MR914657 (88k:14013)
21. R. Schoof, *The exponents of the groups of points of the reductions of an elliptic curve*, Arithmetic Algebraic Geometry, ed. G. van der Geer, 1991. MR1085266 (91j:11043)
22. J.-P. Serre, *Complex multiplication*, Algebraic Number Theory, ed. J. W. S. Cassels & A. Fröhlich, Academic Press, 1967. MR0244199 (39:5516)
23. J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Springer Graduate Texts in Mathematics, vol. 151, 1994. MR1312368 (96b:11074)
24. J. H. Silverman, *The arithmetic of elliptic curves*, Springer Gruadate Texts in Mathematics, vol. 106, 1986. MR817210 (87g:11070)
25. J. Vélu, *Isogénies entre courbes elliptiques*, C. R. Acad. Sci. Paris Sér. A–B **273** (1971), A238–A241.

Department of Mathematics and Statistics, University of Calgary, 2500 University Drive NW, Calgary, AB T2N 1N4, Canada

Current address: Microsoft Research, One Microsoft Way, Redmond, Washington 98052

E-mail address: `reinier@math.leidenuniv.nl`