p-ADIC CLASS INVARIANTS

Reinier Bröker

Abstract. We develop a new p-adic theory of class invariants. Our approach works for virtually any modular function yielding class invariants. The main algorithmic tool are modular polynomials, a concept which we generalize to functions of higher level. The resulting algorithm is very fast in practice.

1. Introduction

Let K be an imaginary quadratic number field. The ring class field $H_{\mathcal{O}}$ of the order $\mathcal{O} \subset K$ of discriminant Δ is an abelian extension of K, and the Artin map gives an isomorphism

$$\mathrm{Gal}(H_{\mathcal{O}}/K) \xrightarrow{\sim} \mathrm{Pic}(\mathcal{O})$$

of its Galois group with the Picard group of the order. In this article we are interested in *explicitly computing* ring class fields. Complex multiplication theory provides us with a means of doing so. It states that we have

$$H_{\mathcal{O}} = K[X]/(P_\Delta^j),$$

where P_Δ^j is the minimal polynomial over $\mathbf{Q}$ of the j-invariant of the complex elliptic curve $\mathbf{C}/\mathcal{O}$. This polynomial is called the *Hilbert class polynomial*. It is a non-trivial fact that P_Δ^j has *integer* coefficients.

The fact that ring class fields are closely linked to j-invariants of elliptic curves has its ramifications outside the context of explicit class field theory. The observation that the roots in $\overline{\mathbf{F}}_p$ of $P_\Delta^j \in \mathbf{F}_p[X]$ are j-invariants of complex elliptic curves with endomorphism ring $\mathcal{O}$ made computing P_Δ^j a key ingredient in the elliptic curve primality proving algorithm [10]. Fast algorithms to compute P_Δ^j are also desirable from a cryptographic point of view. Indeed, computing P_Δ^j allows us to efficiently construct elliptic curves for which the discrete logarithm problem is hard, cf. [5, Chapter 23].

There are three algorithms to compute $P_\Delta^j \in \mathbf{Z}[X]$: a complex analytic [7], a p-adic [2, 6] and a 'multi prime' approach [1, 4]. If GRH holds true, the run time of all

2000 *Mathematics Subject Classification*. Primary 11G15, Secondary 11Y40.

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TeX
version 20070422

three algorithms is $\widetilde{O}(|\Delta|)$, cf. [4]. These three algorithms are efficient in the sense that the bottle neck for each algorithm is the size of the output. We are therefore inherently limited to 'small' discriminants. However, also for small discriminants, the coefficients of P^j_Δ are *huge*. For $\Delta = -23$, we get

$$P^j_{-23} = X^3 + 3491750X^2 - 5151296875X + 12771880859375$$

for instance. History tells us we should be able to do better. In his Lehrbuch der Algebra [19] from 1908, Weber introduces a modular function $\mathfrak{f}$ from the upper half plane $\mathbf{H}$ to $\mathbf{C}$ with the property that $\mathfrak{f}(\omega)$ generates the ring class field of $\mathbf{Z}[\omega]$ for all imaginary quadratic orders $\mathbf{Z}[\omega]$ in which 3 is unramified and 2 splits completely. For $\Delta = -23$, a root of the polynomial

$$P^{\mathfrak{f}}_{-23} = X^3 - X^2 + 1$$

generates the Hilbert class field of $\mathbf{Q}(\sqrt{-23})$. Weber's function $\mathfrak{f}$ is related to the j-function via $(\mathfrak{f}^{24} - 16)^3 - j\mathfrak{f}^{24} = 0$, so computing $P^{\mathfrak{f}}_\Delta$ has the same cryptographic applications as computing P^j_Δ.

Following Weber, we call a function value $f(\omega)$ of a modular function $f : \mathbf{H} \to \mathbf{C}$ a *class invariant* if we have

$$K(f(\omega)) = H_{\mathbf{Z}[\omega]},$$

i.e., if it is generates the ring class field over $K = \mathbf{Q}(\omega)$. The coefficients of the minimal polynomial P^f_Δ of a class invariant are a *constant* factor smaller than the coefficients of P^j_Δ. This means that from a purely asymptotic point of view, there is no advantage in computing P^f_Δ instead of P^j_Δ: the difference in run time is absorbed in the O-constant. The example above shows however that from a more practical point of view, class invariants give a big improvement.

The theory of class invariants is well understood *in the complex analytic setting*. Using complex analytic techniques, it is now a rather mechanical process [17] to decide if $f(\omega)$ is a class invariant, and if so compute its minimal polynomial.

In this article we develop a new *p-adic theory* of class invariants. It is an extension of the p-adic algorithm for the j-function [2], which we briefly recall in Section 2. Our treatment of class invariants is more geometric than the complex analytic one. The main ingredient of our algorithm are *modular polynomials*. These polynomials are well known for the j-function, and we generalize the concept to modular functions of higher level.

In Section 3 we recall the properties of the modular function field and give a 'weak version' of Shimura reciprocity linking modular functions and ring class fields. The geometric approach to class invariants is developed in Sections 4 and 5, the resulting algorithm is stated in Section 6. The algorithm behaves quite well in practice and computer experiments indicate that the p-adic approach is roughly as fast as the complex analytic version. We illustrate the algorithm with a detailed example in Section 7.

2. p-adic algorithm for j-function

In this Section we explain the p-adic algorithm to compute, on input of a discriminant $\Delta < -4$, the Hilbert class polynomial $P_\Delta^j \in \mathbf{Z}[X]$. For more details, proofs and examples, see [2, 6].

As before, let $\mathcal{O} \subset K = \mathbf{Q}(\sqrt{\Delta})$ be the order of discriminant Δ. Let p be a 'small' prime that splits completely in the ring class field $H_\mathcal{O}$. Since a prime splits completely in the ring class field if and only if it splits into principal primes in $\mathcal{O}$, we can find such p by looking for an integer solution to the equation

$$4p = x^2 - \Delta y^2 \tag{2.1}$$

with p prime. Under GRH, we may take p of size $\widetilde{O}(|\Delta|)$ by [2, Lemma 3.1].

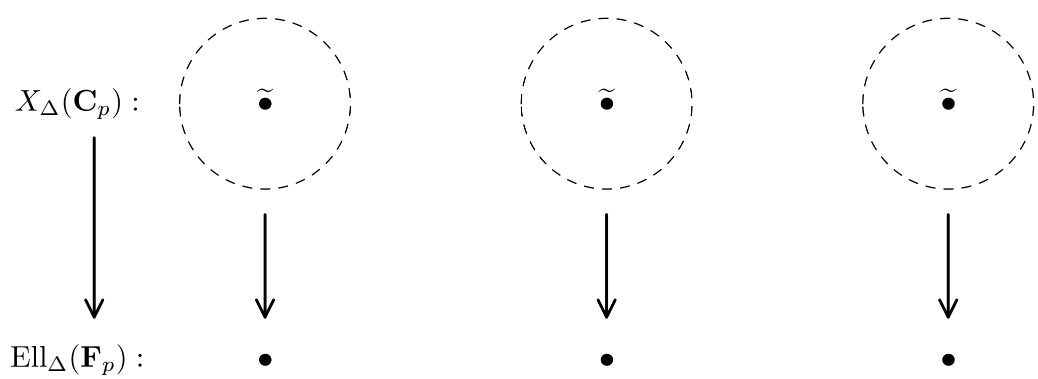
The set

$$\mathrm{Ell}_\Delta(\mathbf{Q}_p) = \{j \in \mathbf{Q}_p \mid \exists E/\mathbf{Q}_p \text{ with } j(E) = j \text{ and } \mathrm{End}(E) = \mathcal{O}\},$$

is a finite set of cardinality $\#\mathrm{Pic}(\mathcal{O})$, and consists of the roots of $P_\Delta^j \in \mathbf{Q}_p[X]$. The set $\mathrm{Ell}_\Delta(\mathbf{F}_p)$ is defined similarly. Its elements are the $\#\mathrm{Pic}(\mathcal{O})$ j-invariants of elliptic curves over $\mathbf{F}_p$ with endomorphism ring $\mathcal{O}$, or equivalently, the roots of $P_\Delta^j \in \mathbf{F}_p[X]$.

We first construct an (ordinary) elliptic curve $\overline{E}/\mathbf{F}_p$ with $j(\overline{E}) \in \mathrm{Ell}_\Delta(\mathbf{F}_p)$. Write $N = p + 1 - x$ with x as in equation 2.1. We try *random* curves over $\mathbf{F}_p$ until we find a curve $\overline{E}$ with N points. The subring $\mathbf{Z}[\mathrm{Frob}] \subseteq \mathcal{O}$ then has index $y \geq 1$. For cryptographic applications, we are mostly interested in the case that $\mathcal{O}$ is the maximal order. If we have $y = 1$ in this case, we know that the curve $\overline{E}$ has endomorphism ring $\mathcal{O}$. For the general case, the equality $\#\overline{E}(\mathbf{F}_p) = N$ does not imply that $\overline{E}$ has endomorphism ring $\mathcal{O}$. We then compute the endomorphism ring $\mathrm{End}(\overline{E})$ using [13] and apply an isogeny of degree dividing $[\mathcal{O}_K : \mathbf{Z}[\mathrm{Frob}]]$ to find an elliptic curve with endomorphism ring $\mathcal{O}$. We refer to [2, Section 3] for details, and fix an elliptic curve $\overline{E}/\mathbf{F}_p$ with $\mathrm{End}(\overline{E}) = \mathcal{O}$ for the remainder of this Section.

We want to lift $j(\overline{E}) \in \mathbf{F}_p$ to $\tilde{\jmath} \in \mathrm{Ell}_\Delta(\mathbf{Q}_p)$. Let $\mathbf{C}_p$ be the completion of an algebraic closure of $\mathbf{Q}_p$, and put $X_\Delta(\mathbf{C}_p) = \{j \in \mathbf{C}_p \mid j \bmod p \in \mathrm{Ell}_\Delta(\mathbf{F}_p)\}$. The set $\mathbf{C}_p$ consists of $\#\mathrm{Pic}(\mathcal{O})$ discs of p-adic radius 1. Each disc contains exactly one element of the set $\mathrm{Ell}_\Delta(\mathbf{Q}_p)$ that we want to compute.



Let $E/\mathbf{Q}_p$ be an elliptic curve with endomorphism ring $\mathcal{O}$. For an ideal $I \subset \mathcal{O}$, there exists an elliptic curve $E^I/\mathbf{Q}_p$ and a separable isogeny $E \to E^I$ which has the subgroup $E[I]$ of I-torsion points as kernel. We obtain a bijection $\rho_I : \mathrm{Ell}_\Delta(\mathbf{Q}_p) \to \mathrm{Ell}_\Delta(\mathbf{Q}_p)$ that sends $j(E)$ to $j(E^I)$. The fundamental idea in [6] is that the map ρ_I has a natural extension to a map

$$\rho_I : X_\Delta(\mathbf{C}_p) \to X_\Delta(\mathbf{C}_p)$$

for ideals I that are coprime to p. For principal ideals I, the map ρ_I is analytic and has the set $\mathrm{Ell}_\Delta(\mathbf{Q}_p)$ as unique fixed points.

To define ρ_I, let $j \in X_\Delta(\mathbf{C}_p)$ and choose an elliptic curve $E/\mathbf{C}_p$ with $j(E) = j$ that has good reduction modulo p. Assume that I is coprime to p, and let $l \in \mathbf{Z}_{>0}$ be its norm. The reduced curve $E'/\mathbf{F}_p$ has endomorphism ring $\mathcal{O}$, and the subgroup $E'[I] \subset E'[l]$ lifts canonically to a subgroup $S \subset E[l]$. We put $\rho_I(j) = j(E/S)$. Note that for $j \in \mathrm{Ell}_\Delta(\mathbf{Q}_p)$ we have $S = E[I]$, so ρ_I is indeed an extension of the map defined on $\mathrm{Ell}_\Delta(\mathbf{Q}_p)$.

One proves [2, Theorem 4.1] that for principal ideals $I = (\alpha) \not\subset \mathbf{Z}$, the map $\rho_\alpha : X_\Delta(\mathbf{C}_p) \to X_\Delta(\mathbf{C}_p)$ is analytic, i.e., it can locally be given by a power series. The derivative in $\tilde{\jmath} \in \mathrm{Ell}_\Delta(\mathbf{Q}_p)$ is given by $\alpha/\overline{\alpha}$, cf. [2, Lemma 4.2]. Here, $\overline{\alpha}$ denotes the complex conjugate of α. If $j_1 \in \mathbf{C}_p$ denotes any integral lift of $j(\overline{E}) \in \mathrm{Ell}_\Delta(\mathbf{F}_p)$, the 'Newton process'

$$j_{k+1} = j_k - \frac{\rho_\alpha(j_k) - j_k}{(\alpha/\overline{\alpha}) - 1} \qquad \text{for } k \in \mathbf{Z}_{\geq 1} \tag{2.1}$$

converges to the canonical lift $\tilde{\jmath} \in \mathrm{Ell}_\Delta(\mathbf{Q}_p)$ if $\alpha/\overline{\alpha} - 1$ is a p-adic unit. For $k = 1$ the computation is performed with two p-adic digits precision, and the precision is doubled in each step. The accuracy required for the computation of P_Δ^j can be explictly bounded [2, Section 7].

The run time of the lifting phase depends heavily on the choice of α. The equality $\rho_{IJ} = \rho_I \rho_J$ shows that we want α to be *smooth*: we can then decompose ρ_α as a series of maps corresponding to the prime divisors of (α). The smoothness properties are 'in practice' a lot better than what can be rigorously proved [6, Lemma 2]. At the end of this Section we give more details on the explicit computation of ρ_α.

Once we have computed the canonical lift with high enough accuracy, we need to compute its conjugates under the action of the Picard group $\mathrm{Pic}(\mathcal{O})$. This can be done using the same techniques as before, since the action of an ideal class $[I] \in \mathrm{Pic}(\mathcal{O})$ is given by

$$j(E) \mapsto j(E^I) = \rho_I(j(E))$$

We compute small generators of the Picard group, and compute the Galois conjugates of $\tilde{\jmath}$. In the end we expand the Hilbert class polynomial

$$P_\Delta^j = \prod_{[I] \in \mathrm{Pic}(\mathcal{O})} (X - \rho_I(\tilde{\jmath})) \in \mathbf{Z}[X].$$

We explain how to explicitly compute the map ρ_I. It suffices to show how to treat the case that I is a prime ideal, and we let $l \neq p$ be its norm. For $j(E) \in \mathrm{Ell}_\Delta(\mathbf{F}_p)$, the isogeny $E \to E^I$ has degree l. Let $\Phi_l(X,Y) \in \mathbf{Z}[X,Y]$ be the classical *modular polynomial* of level l. It is a singular model for the modular curve $X_0(l)$ parametrizing (cyclic) l-isogenies. This means that $j(E^I) \in \mathbf{F}_p$ is a root of $\Phi_l(X, j(E)) \in \mathbf{F}_p[X]$. Under the mild condition that the l-torsion $E[l]$ is not $\mathbf{F}_p$-rational, this polynomial has only *two* roots in $\mathbf{F}_p$ by [2, Theorem 5.1], namely $j(E^I)$ and $j(E^{\overline{I}})$. Choose a root h.

We need to decide if we have $\rho_I(j(E)) = h$ or not. Let $\overline{E}/S$ have j-invariant h, corresponding to a cyclic subgroup $S \subset \overline{E}[l]$ of order l, i.e., S is the kernel of the isogeny $\overline{E} \to \overline{E}/S$. Choosing a Weierstraß equation

$$Y^2 = X^3 + aX + b$$

for $\overline{E}$, the techniques that Elkies used to improve Schoof's original point counting algorithm [15, Sections 7, 8] allow us to compute a polynomial $f_S \in \mathbf{F}_p[X]$ that vanishes exactly on the x-coordinates of the points in S.

Write $I = (l, a + b\pi_p)$ with $\pi_p \in \mathcal{O}$ an element of norm p. Then the group $\overline{E}[I]$ is an eigenspace for the action of Frobenius with eigenvalue $-b/a \in \mathbf{F}_l$. We now test if $(X^p, Y^p) = -b/a \cdot (X,Y)$ holds for the points in S, i.e., we compute both (X^p, Y^p) and $(-c/d) \cdot (X,Y)$ in the ring

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

If they are equal, we have $h = \overline{\rho}_I(j(\overline{E}))$. Otherwise, we need to take the other root of $\Phi_l(j(\overline{E}), X)$.

We have 'decomposed' the map $\overline{\rho}_\alpha : \mathrm{Ell}_\Delta(\mathbf{F}_p) \to \mathrm{Ell}_\Delta(\mathbf{F}_p)$ as a cycle of isogenies. Using modular polynomials, it is a simple matter to lift this cycle of maps

$$j(\overline{E}) \xrightarrow{I_1} j(\overline{E}^{I_1}) \longrightarrow \cdots \xrightarrow{I_n} j(\overline{E}^{(\alpha)}) = j(\overline{E})$$

over $\mathbf{F}_p$ to a 'cycle' $j_k \longrightarrow \ldots \longrightarrow \rho_\alpha(j_k)$ over $\mathbf{Q}_p$. Indeed, we know that $\Phi_l(j_k, X) \in \mathbf{Z}_p[X]$ only has two roots in $\mathbf{Z}_p$, and since we know $j(\overline{E}^I) \in \mathbf{F}_p$, we know which root is $\rho_I(j_k)$. This enables us to compute the map ρ_α on $X_\Delta(\mathbf{C}_p)$.

3. Shimura reciprocity over the ring class field

For an integer $N > 0$, let

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}) \mid a \equiv d \equiv 1 \bmod N, b \equiv c \equiv 0 \bmod N \right\}$$

be the full congruence subgroup of level N. The modular group $\mathrm{SL}_2(\mathbf{Z})$ acts on the complex upper half plane $\mathbf{H}$ and its completion $\overline{\mathbf{H}} = \mathbf{H} \cup \mathbf{P}^1(\mathbf{Q})$ by fractional linear transformations. The quotient $\Gamma(N)\backslash\overline{\mathbf{H}}$ has the structure of a compact Riemann surface, and as such, it is isomorphic to the modular curve $X(N)$ over $\mathbf{C}$.

It is well known that the modular curve $X(N)$ can be defined over the cyclotomic field $\mathbf{Q}(\zeta_N)$, where ζ_N is a primitive Nth root of unity. Let F_N to be the function field of $X(N)$ over $\mathbf{Q}(\zeta_N)$. We have $F_1 = \mathbf{Q}(j)$. Elements of F_N are called *modular functions* of level N. Explicitly, a function $f : \overline{\mathbf{H}} \to \mathbf{C}$ is called modular if it is invariant under $\Gamma(N)$ and if the coefficients of its Fourier expansion – which it has because $\left(\begin{smallmatrix} 1 & N \\ 0 & 1 \end{smallmatrix}\right)$ is an element of $\Gamma(N)$ – lie in $\mathbf{Q}(\zeta_N)$.

Define the function h by

$$h(w,\tau) = -2^7 3^5 \cdot \frac{g_2(\tau)g_3(\tau)}{\Delta(\tau)} \wp(w; \langle 1, \tau\rangle)$$

for $w \in \mathbf{C}$ and $\tau \in \mathbf{H}$. Here, $\wp(\cdot; \langle 1, \tau\rangle)$ is the Weierstraß $\wp$-function associated to the lattice $\mathbf{Z} + \mathbf{Z}\cdot\tau$. For $r, s \in \frac{1}{N}\mathbf{Z}/\mathbf{Z}$, not both 0, define the *Fricke function* $f_{r,s}$ of level N by

$$f_{r,s}(\tau) = h\left(rN + s, \tau\right).$$

The Fourier coefficients of $f_{r,s}$ are contained in $\mathbf{Q}(\zeta_N)$. If we fix τ and let r, s vary over $\frac{1}{N}\mathbf{Z}/\mathbf{Z}$, not both equal to 0, we get the normalized x-coordinates of the N^2-1 non-trivial points of order N of the complex elliptic curve $\mathbf{C}/(\mathbf{Z} + \mathbf{Z}\cdot\tau)$.

Theorem 3.1. *We have*

$$F_N = \mathbf{Q}(j, f_{r,s} \mid r, s \in \tfrac{1}{N}\mathbf{Z}/\mathbf{Z}, \text{not both } 0).$$

Proof. [14, Theorem 6.2 and beginning of Section 6.3].

The extension F_N/F_1 is Galois with group $\mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})/\{\pm 1\}$. This combines the geometric $\mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})/\{\pm 1\}$-action coming from the Galois cover $X(N)_{\mathbf{C}}/X(1)_{\mathbf{C}}$ with the arithmetic $(\mathbf{Z}/N\mathbf{Z})^*$-action coming from $\mathbf{Q}(\zeta_N)/\mathbf{Q}$. Here, $\sigma_d : \zeta_N \mapsto \zeta_N^d$ acts on a modular function $f = \sum_k c_k \cdot q^{k/N}$ via

$$f^{\sigma_d} = \sum_k \sigma_d(c_k) \cdot q^{k/N}. \tag{3.1}$$

Let $\widehat{\mathcal{O}} = \mathcal{O} \otimes_{\mathbf{Z}} \widehat{\mathbf{Z}}$ be the profinite completion of the imaginary quadratic order $\mathcal{O} \subset K$. Class field theory tells us that the Galois group $\mathrm{Gal}(K^{\mathrm{ab}}/H_{\mathcal{O}})$ is given by the exact sequence

$$1 \longrightarrow \mathcal{O}^* \longrightarrow \widehat{\mathcal{O}}^* \xrightarrow{\text{Artin}} \mathrm{Gal}(K^{\mathrm{ab}}/H_{\mathcal{O}}) \longrightarrow 1.$$

We obtain K^{ab} as the union of finite extensions $H_{N,\mathcal{O}}$ corresponding to the finite quotients

$$\widehat{\mathcal{O}}^* \twoheadrightarrow (\widehat{\mathcal{O}}/N\widehat{\mathcal{O}})^* = (\mathcal{O}/N\mathcal{O})^*.$$

The field $H_{N,\mathcal{O}}$ is called the *ray class field of conductor N for the order $\mathcal{O}$*, and the Artin map gives an isomorphism

$$(\mathcal{O}/N\mathcal{O})^*/\mathrm{Im}[\mathcal{O}^*] \xrightarrow{\sim} \mathrm{Gal}(H_{N,\mathcal{O}}/H_{\mathcal{O}}).$$

If $\mathcal{O}$ is the maximal order of K, the field $H_{N,\mathcal{O}}$ is the ray class field of conductor N of K.

Theorem 3.2. *Let $f \in F_N$ be modular of level N, and write $\mathcal{O} = \mathbf{Z}[\omega]$. If $f(\omega)$ is finite, we have $f(\omega) \in H_{N,\mathcal{O}}$.*

Proof. See [14, Chapter 10]. □

Let the notation be as in the Theorem above. Then we have $f(\omega) \in H_{\mathcal{O}} \subseteq H_{N,\mathcal{O}}$ if $f(\omega)$ is a class invariant. To decide if this is the case for a given value $f(\omega)$, we need to know the Galois action of $\mathrm{Gal}(H_{N,\mathcal{O}}/H_{\mathcal{O}})$ on values of modular functions. This is the content of the 'weak' version of Shimura reciprocity, described below.

Shimura reciprocity gives a map $g_\omega : (\mathcal{O}/N\mathcal{O})^* \to \mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$ relating the two exact sequences in the diagram below.

$$\begin{array}{ccccccc} \mathcal{O}^* & \longrightarrow & (\mathcal{O}/N\mathcal{O})^* & \xrightarrow{\text{Artin}} & \mathrm{Gal}(H_{N,\mathcal{O}}/H_{\mathcal{O}}) & \longrightarrow & 1 \\ & & \downarrow g_\omega & & & & \\ \{\pm 1\} & \longrightarrow & \mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z}) & \longrightarrow & \mathrm{Gal}(F_N/\mathbf{Q}(j)) & \longrightarrow & 1. \end{array}$$

If ω has minimal polynomial $X^2 + bX + c \in \mathbf{Z}[X]$, we have

$$g_\omega : \quad x = s\omega + t \longmapsto \begin{pmatrix} t - bs & -cs \\ s & t \end{pmatrix}.$$

The Galois conjugate $f(\omega)^x$ may now be computed via the reciprocity relation

$$(f(\omega))^x = (f^{g_\omega(x^{-1})})(\omega),$$

cf. [16, Theorem 6.31]. If the extension $F_N/\mathbf{Q}(f)$ is Galois, we have the fundamental equivalence

$$(f(\omega))^x = f(\omega) \quad \Longleftrightarrow \quad f^{g_\omega(x)} = f.$$

The implication $\Leftarrow$ is immediate from the reciprocity relation. The other implication requires the hypothesis and an additional argument [16, Proposition 6.33].

We compute generators $x_1, \ldots, x_k$ for $(\mathcal{O}/N\mathcal{O})^*$ and map them to $\mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$ using the map g_ω. The value $f(\omega)$ is contained in the ring class field $H_{\mathcal{O}}$ if and only if $g_\omega(x_1), \ldots, g_\omega(x_k)$ act trivially on f. If we for instance also know that there is an inclusion $\mathbf{Q}(j) \subseteq \mathbf{Q}(f)$, then $f(\omega)$ is also a class invariant if $g_\omega(x_1), \ldots, g_\omega(x_k)$ act trivially on f. We refer to [11] for examples.

4. Class invariants over $\mathbf{Q}_p$

In this Section we extend the p-adic algorithm from Section 2 to work with other modular functions than the j-function. The description we present in this Section is not ideally suited for explicit computations yet, and serves as a stepping stone for the more practical version of Section 5. The modular functions f we will consider are *integral* over $\mathbf{Z}[j]$, so they are given as the zero of some irreducible polynomial $\Psi_f(X, j) \in \mathbf{Z}[j, X]$. All known modular functions yielding class invariants have this property.

As before, let p be prime that splits completely in the ring class field $H_{\mathcal{O}}$ for the order $\mathcal{O}$ of discriminant $\Delta < -4$. For a j-value $j(\tilde{E}) \in \mathrm{Ell}_\Delta(\mathbf{Q}_p)$, the roots of the polynomial $\Psi_f(X, j(\tilde{E})) \in H_{\mathcal{O}}[X]$ lie in the ray class field of conductor $H_{N,\mathcal{O}}$ of conductor N for the order $\mathcal{O}$, cf. Theorem 3.2. If we know that f yields class invariants, for instance by using Shimura reciprocity, we know that some of these roots actually lie in the ring class field $H_{\mathcal{O}}$. We need to decide which ones, and compute the action of the Galois group $\mathrm{Gal}(H_{\mathcal{O}}/K) \cong \mathrm{Pic}(\mathcal{O})$ on such roots.

The key observation is that f is an element of the function field

$$F_N = \mathbf{Q}(j, f_{r,s} \mid r, s \in \tfrac{1}{N}\mathbf{Z}/\mathbf{Z}, \text{ not both } 0)$$

of the modular curve $X(N)$ over $\mathbf{Q}(\zeta_N)$, cf. Theorem 3.1. The Fricke functions $f_{r,s}$ are normalized x-coordinates of N-torsion of points on the elliptic curve $\mathbf{C}/(\mathbf{Z} + \mathbf{Z} \cdot \tau)$, and we can write f as a $\mathbf{Q}$-rational function in j and the functions $f_{r,s}$.

Fix a primitive Nth root of unity $\zeta_N \in \overline{\mathbf{Q}}_p$. For $a \in (\mathbf{Z}/N\mathbf{Z})^*$, let $Y(N)_a$ be the modular curve from parametrizing isomorphism classes of triples

$$(E, P, Q)$$

where $P, Q \in E[N]$ form a basis that maps to ζ_N^a under the Weil pairing e_N. Then f is an element of the function field of $Y(N)_{a,\overline{\mathbf{Q}}_p}$ for every $a \in (\mathbf{Z}/N\mathbf{Z})^*$. Let $x \in \mathbf{Q}_p$ be a root of $\Psi_f(X, j(\tilde{E})) \in \mathbf{Q}_p[X]$. There exist $a \in (\mathbf{Z}/N\mathbf{Z})^*$ and $(\tilde{E}, P, Q) \in Y(N)_a(\overline{\mathbf{Q}}_p)$ with $f(\tilde{E}, P, Q) = x \in \mathbf{Q}_p$.

The group of invertible $\mathcal{O}$-ideals acts on $\mathrm{Ell}_\Delta(\mathbf{Q}_p)$ via $j(E) \mapsto j(E^I)$, and we have $j(\tilde{E})^{[I, H_{\mathcal{O}}/K]} = j(\tilde{E}^I)$. If N is coprime to the norm l of I, the isogeny

$$\varphi_I : \tilde{E} \longrightarrow \tilde{E}^I$$

extends to a natural isomorphism

$$\varphi_I : \tilde{E}[N] \xrightarrow{\sim} \tilde{E}^I[N].$$

A basis $\langle P, Q \rangle$ for $\tilde{E}[N]$ gets mapped to a basis $\langle P^I, Q^I \rangle$ for $\tilde{E}^I[N]$. We compute

$$e_N(P^I, Q^I) = e_N(P, \hat{\varphi}_I(Q^I)) = e_N(P, lQ) = \zeta_N^l$$

and conclude that we have $(\tilde{E}^I, P^I, Q^I) \in Y(N)_{la}(\overline{\mathbf{Q}}_p)$. We have the fundamental equality

$$f(\tilde{E}, P, Q)^{[I, H_{N,\mathcal{O}}/K]} = f(\tilde{E}^I, P^I, Q^I).$$

We can explicitly compute the isogeny φ_I: first we compute the kernel polynomial $g_I \in \mathbf{Q}_p[X]$ corresponding to I using the 'Atkin-Elkies techniques' alluded to in Section 2 and then we compute the isogeny using Vélu's formulas [18]. Hence, we have a way of computing $f(\tilde{E}, P, Q)^{[I, H_{N,\mathcal{O}}/H_{\mathcal{O}}]}$.

A root $x \in \mathbf{Q}_p$ of $\Psi_f(X, j(\tilde{E})) \in \mathbf{Q}_p[X]$ lies in $H_{\mathcal{O}}$ if and only if it is invariant under the action of

$$\mathrm{Gal}(H_{N,\mathcal{O}}/H_{\mathcal{O}}) \cong (\mathcal{O}/N\mathcal{O})^*/\mathcal{O}^*.$$

We write $x = f(\tilde{E}, P, Q)$ for some choice of basis $P, Q \in \tilde{E}[N]$ and test whether $x^{[(y), H_{N,\mathcal{O}}/H_{\mathcal{O}}]} = x$ holds for all generators y of $(\mathcal{O}/N\mathcal{O})^*/\mathcal{O}^*$.

Once we have found that a certain root $x \in \mathbf{Q}_p$ lies in the ring class field $H_{\mathcal{O}}$, we need to compute its conjugates under $\mathrm{Gal}(H_{\mathcal{O}}/K) \cong \mathrm{Pic}(\mathcal{O})$. This proceeds exactly as before, since we have

$$x^{[I, H_{\mathcal{O}}/K]} = f(\tilde{E}, P, Q)^{[I, H_{\mathcal{O}}/K]} = f(\tilde{E}^I, P^I, Q^I) \in \mathbf{Q}_p.$$

All we require is that the norm of I is coprime to the level of f. If the minimal polynomial of x has integer coefficients, we may expand the product

$$P_\Delta^f = \prod_{[I] \in \mathrm{Pic}(\mathcal{O})} \left(X - f(\tilde{E}, P, Q)^{[I, H_{\mathcal{O}}/K]}\right) \in \mathbf{Z}[X].$$

Example. Let $\gamma_2 : \mathbf{H} \to \mathbf{C}$ be the holomorphic cube root of j with integral Fourier expansion. It is a classical fact that γ_2 is modular of level 3. It yields class invariants for all imaginary quadratic orders $\mathcal{O}$ in which 3 is unramified [19, §125].

Let $E : Y^2 = X^3 + aX + b$ be an elliptic curve over $\mathbf{Q}_p$, with $p > 3$. Let $c_1, \ldots, c_4 \in \overline{\mathbf{Q}_p}$ be the roots of the 3-division polynomial of degree $(3^2 - 1)/2 = 4$. Then

$$\frac{-48a}{2a - 3(c_1c_2 + c_3c_4)} \tag{4.1}$$

is a cube root of $j(E)$, as may be checked by using for instance the Fourier expansion of the Fricke functions. Expression 4.1 nicely illustrates that γ_2 is not a function of an elliptic curve alone: also some ordering on the 3-torsion is required. We indeed get three distinct cube roots of $j(E)$. From a geometric point of view, there is no way to single out a root 'corresponding' to γ_2.

We illustrate how we can use this 'geometric γ_2' to compute the polynomial $P_{-31}^{\gamma_2} \in \mathbf{Z}[X]$ for the order $\mathcal{O}$ of discriminant $\Delta = -31$ using p-adic methods. The primes $47 = 4^2 + 31$ and $67 = 6^2 + 31$ both split completely in the Hilbert class field $H = H_{\mathcal{O}}$ of $K = \mathbf{Q}(\sqrt{-31})$. The case $p = 67$ best illustrates our techniques, since $\tilde{\jmath} \in \mathrm{Ell}_\Delta(\mathbf{Q}_p)$ then has 3 cube roots in $\mathbf{Q}_p$.

First we compute a curve $\tilde{E}/\mathbf{Q}_p$ with $\mathrm{End}(\tilde{E}) \cong \mathcal{O}$. The accuracy needed is only one third of the required accuracy for the computation of the Hilbert class polynomial P^j_{-31}. Using the algorithm from Section 2 we find that we may take

$$j(\tilde{E}) = 3 + 33p - 16p^2 + O(p^3) \in \mathbf{Q}_p$$

as j-invariant. The three cube roots of $j(\tilde{E})$ are

$$\begin{aligned}\eta_1 &= 18 + O(p)\\ \eta_2 &= 53 + O(p)\\ \eta_3 &= 63 + O(p).\end{aligned}$$

Only one of them lies in the Hilbert class field H. Indeed, if 2 roots would lie in H, then ζ_3 would be contained in H as well and 3 would ramify in H.

We fix a Weierstraß equation

$$Y^2 = X^3 + aX + b$$

for $\tilde{E}/\mathbf{Q}_p$. Let $c_1, \ldots, c_4 \in \overline{\mathbf{Q}_p}$ be the 4 roots of the 3-division polynomial for $\tilde{E}$. We compute 3-torsion points P_i with x-coordinate c_i. The points P_i are defined over the unramified extension of degree 4 of $\mathbf{Q}_p$.

Let I be an $\mathcal{O}$-ideal that is coprime to 3. The isogeny $\varphi_I : \tilde{E} \to \tilde{E}^I$ extends to a natural isomorphism

$$\varphi_I : \tilde{E}[3] \xrightarrow{\sim} \tilde{E}^I[3].$$

Hence, we get a natural bijection

$$\varphi_I : \{\eta_1, \eta_2, \eta_3\} \xrightarrow{\sim} \{\text{cube roots of } j(\tilde{E}^I)\}.$$

For a cube root

$$\eta = \frac{-48a}{2a - 3(c_1c_2 + c_3c_4)}$$

we have

$$\eta^{[I,H_3/H]} = \frac{-48a'}{2a' - 3(c_1'c_2' + c_3'c_4')}.$$

Here, c_i' is the x-coordinate of $\varphi_I(P_i) \in \tilde{E}^I[3]$ and $\tilde{E}^I$ has Weierstraß equation $Y^2 = X^3 + a'X + b'$. The group $(\mathcal{O}/3\mathcal{O})^*/\mathcal{O}^* \cong \mathbf{Z}/4\mathbf{Z}$ is generated by $\alpha = \frac{-1+\sqrt{-31}}{2}$ of norm 8. We compute $\eta_i^{[I,H_3/H]}$ for $I = (\alpha) = \mathfrak{p}_2^3$ and get

$$\begin{aligned}\eta_1 &\xrightarrow{\varphi_I} \eta_1\\ \eta_2 &\xrightarrow{\varphi_I} \eta_3\\ \eta_3 &\xrightarrow{\varphi_I} \eta_2.\end{aligned}$$

Hence, $\eta_1 = 18 + O(p)$ is a class invariant. Note that $\varphi_{\mathfrak{p}_2}$ is just a 2-isogeny, so we do not actually need the 'Atkin-Elkies' techniques from [15, Sections 7, 8].

Computing the conjugates of $\eta_1 \in H_{\mathcal{O}}$ under $\mathrm{Gal}(H_{\mathcal{O}}/K) \cong \mathrm{Pic}(\mathcal{O})$ proceeds similarly. We have $\mathrm{Pic}(\mathcal{O}) \cong \mathbf{Z}/3\mathbf{Z} \cong \langle [\mathfrak{p}_2] \rangle$ and

$$\eta_1^{[\mathfrak{p}_2, H_{\mathcal{O}}/K]} = \varphi_{\mathfrak{p}_2}(\eta_1).$$

We compute the Galois conjugates of η_1 and expand

$$P_{-31}^{\gamma_2} = \prod_{i=1}^{3} \left(X - \varphi_{\mathfrak{p}_2}^i(\eta_1)\right) = X^3 + 342X^2 + 837X + 116127 \in \mathbf{Z}[X].$$

5. Computing the action of invertible ideals

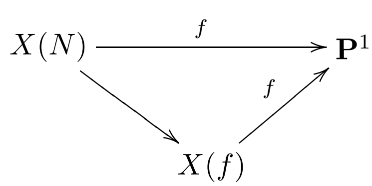
The theory developed in Section 4 is not directly suited for explicit computations. If we are given a modular function f of level N as a Fourier expansion, it is not clear how to write this as a rational function in j and the Fricke functions. Secondly, we have to partially factor the N-division polynomial to use the approach from the previous Section. The degree of this polynomial is roughly N^2, and factoring it annihilates the improvement gained by working with a 'smaller' function f. In this Section we explain how to circumvent these problems.

The crucial observation is that it suffices to compute

$$x^I,$$

where $x \in \mathbf{Q}_p$ is a root of $\Psi_f(X, j(E)) \in \mathbf{Q}_p[X]$ and I is an invertible $\mathcal{O}$-ideal of norm coprime to N. Indeed, if we want to know which root x of $\Psi_f(X, j(E)) \in \mathbf{Q}_p[X]$ is a class invariant, we need to check which root is invariant under the action of $(\mathcal{O}/N\mathcal{O})^*/\mathcal{O}^*$. This amounts to computing x^I, for I the principal ideal generated by one of the generators of $(\mathcal{O}/N\mathcal{O})^*$. Once we know that $x \in \mathbf{Q}_p$ is a class invariant, we need to compute $x^I \in \mathbf{Q}_p$, with I one of the generators of $\mathrm{Pic}(\mathcal{O})$.

Write $\Gamma(f)$ for the stabilizer of f inside $\mathrm{SL}_2(\mathbf{Z})$. We have $\Gamma(N) \subseteq \Gamma(f) \subseteq \mathrm{SL}_2(\mathbf{Z})$, by the assumption that f is modular of level N. Write $X(f)$ for the modular curve corresponding to the congruence subgroup $\Gamma(f)$. The complex points of this curve are $\Gamma(f)\backslash\overline{\mathbf{H}}$. The curve $X(f)$ is a quotient of the modular curve $X(N)$ by a subgroup of $\mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})$, and can be defined over $\mathbf{Q}(\zeta_N)$. We have a commutative diagram



and $f : X(N) \to \mathbf{P}^1$ factors through the quotient $X(f)$. Likewise, there exists a curve $X(f)_a$ for every $a \in (\mathbf{Z}/N\mathbf{Z})^*$ such that f factors through $X(N)_a \to \mathbf{P}^1$. As a complex curve, we have $X(f)_a = X(f)$.

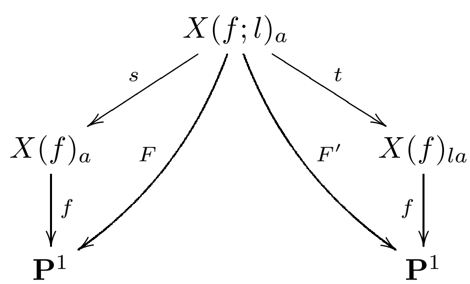
For ease of notation, we simply denote a point on $X(f)_a$ by a triple (E,P,Q) instead of $\overline{(E,P,Q)}$. Here, P,Q form a basis for the N-torsion $E[N]$ of E with $e_N(P,Q)=\zeta_N^a$ for a fixed choice of ζ_N.

Let l be a prime not dividing the level N. Writing $\Gamma(f;l)=\Gamma(f)\cap\Gamma_0(l)$, we have inclusions

$$\Gamma(lN)\subseteq\Gamma(f;l)\subseteq\Gamma(f).$$

Let $X(f;l)$ be the modular curve corresponding to $\Gamma(f;l)$. It can be defined over $\mathbf{Q}(\zeta_{lN})$. Just as we have curves $X(f)_a$, we also have curves $X(f;l)_a$. Points on $X(f;l)_a$ are quadruples (E,P,Q,G), with $(E,P,Q)\in X(f)_a$ and $G\subset E[l]$ a (cyclic) subgroup of order l.

There is a natural map $s: X(f;l)_a\to X(f)_a$ and a natural map $t: X(f;l)_a\to X(f)_{la}$. The map s sends $(E,P,Q,G)\in X(f;l)_a$ to $(E,P,Q)\in X(f)_a$. The map t sends $(E,P,Q,G)\in X(f;l)_a$ to $(E/G,\varphi(P),\varphi(Q))$, where $\varphi: E\to E/G$ has kernel G. The situation is as follows.



(5.1)

Here, F and F' are the composed maps.

Lemma 5.1. *The maps s,t in the diagram above both have degree $l+1$.*

Proof. We will show that the diagram

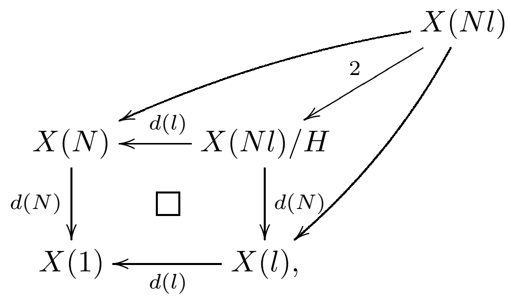
$$\begin{CD} X(f)_a @<{s}<< X(f;l)_a \\ @V{f}VV \square @VVV \\ X(1) @<<< X_0(l) \end{CD}$$

is cartesian in the category of smooth projective curves with surjective maps. As the cover $X_0(l)/X(1)$ has degree $l+1$, this implies that s and t have degree $l+1$. Here, the maps on the 'lower right part' of the square are the forgetful maps. Instead of working over $\mathbf{Q}(\zeta_N)$, we will work over $\mathbf{C}$; the same result then holds over $\mathbf{Q}(\zeta_N)$. We may then omit the subscript a in the diagram. Moreover, it is easier to work with $X(N)/X(1)$ and $X(l)/X(1)$ instead of $X(f)/X(1)$ and $X_0(l)/X(1)$, since in this case we explicitly know the Galois groups.

The fibred product of $X(l)$ and $X(N)$ is almost equal to $X(Nl)$. Indeed, writing $d(k)=\#(\mathrm{SL}_2(\mathbf{Z}/k\mathbf{Z})/\{\pm1\})$, the degree of $X(Nl)/X(1)$ is

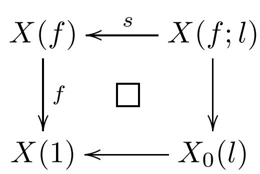
$$\#\mathrm{SL}_2(\mathbf{Z}/Nl\mathbf{Z})/\{\pm1\}=2\cdot d(N)d(l),$$

and we obtain the following diagram



where H is the subgroup $\{1\} \times \{\pm 1\} \subseteq \mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z}) \times \mathrm{SL}_2(\mathbf{Z}/l\mathbf{Z})$. Since we are working over $\mathbf{C}$, we know that the degrees on parallel sides of the square are equal. Hence, the square is cartesian.

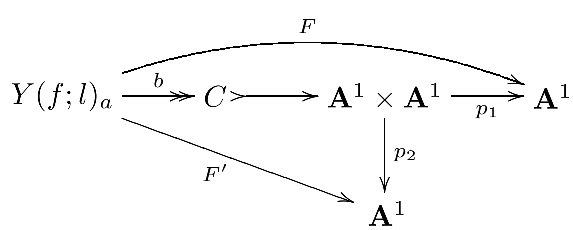
Since we have $\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \in \Gamma_0(l)$, the curve $X(Nl)/H$ is a cover of $X(f;l)$. Hence, the diagram



'fits inside' the bigger cartesian diagram for $X(Nl)/H$. In particular, it is cartesian. Since the degree of $X_0(l)/X(1)$ is $l+1$, the same must hold for $X(f;l)/X(f)$. □

Remark. *The curve* $X_0(l)$ *can be defined over* $\mathbf{Q}$. *The cartesian diagram above shows that* $X(f;l)_a$ *can be defined over* $\mathbf{Q}(\zeta_N)$.

We map $Y(f;l)_a$ to a curve C inside $\mathbf{A}^1 \times \mathbf{A}^1$ as in the diagram below. The map b is defined by $b(x) = (s(x), t(x))$, and the maps p_1, p_2 are the two projection maps.



(5.2)

The function field of C is generated by f and f_l. Here, f_l is as in (3.1) defined by $f_l(\omega) = f^{\sigma_l}(l\omega)$. If f has rational Fourier coefficients, we have $f_l(\omega) = f(l\omega)$. The minimal polynomial Φ_l^f of f_l over $\mathbf{Q}(\zeta_N)(f)$ is called the *modular polynomial* relating f and f_l. The coefficients of Φ_l^f need not be polynomials in f yet, but after multiplying the coefficients by the common denominator, we get a polynomial in $\mathbf{Q}(\zeta_N)[X, Y]$. This polynomial is a model for the curve C. As we have $\deg(F) = \deg(F')$, diagram (5.2) tells us that we have

$$\deg_X(\Phi_l^f) = \deg_Y(\Phi_l^f) = \frac{(l+1)\deg(f)}{\deg(b)}.$$

Remark. *For $f = j$, the modular polynomial Φ_l^j is the 'classical' modular polynomial Φ_l that we used in Section 2.*

Lemma. *If f has rational Fourier expansion, then Φ_l^f has rational coefficients.*

Proof. It suffices to show that $X(f)$ can be defined over $\mathbf{Q}$. Since the algebraic closure of $\mathbf{Q}$ inside $\mathbf{Q}(f,j)$ is $\mathbf{Q}$ itself, the minimal polynomial Ψ_f of f over $\mathbf{Q}(j)$ is absolutely irreducible. The curve defined by $\Psi_f = 0$ is absolutely irreducible and has $\mathbf{Q}(f,j)$ as function field showing that $X(f)$ is defined over $\mathbf{Q}$. □

Computing Φ_l^f is relatively easy if we know the Fourier expansion of f. We have an upper bound

$$\deg(f)(l+1)$$

for the degrees $\deg_X(\Phi_l^f)$ and $\deg_Y(\Phi_l^f)$. By comparing the Fourier coefficients of f and f_l, we can recursively find the coefficients of Φ_l^f. The following lemma often simplifies the computations.

Lemma. *Let f be a modular function, and let l be a prime not dividing the level of f. Suppose that the modular polynomial Φ_l^f has integer coefficients. If f is invariant under the action of either $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbf{Z})$ or $M = \left(\begin{smallmatrix} 0 & -l \\ 1 & 0 \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbf{Q})$, then we have*

$$\Phi_l^f(X,Y) = \Phi_l^f(Y,X),$$

i.e., Φ_l^f is symmetric.

Proof. The proof is similar to the symmetry proof [14, Theorem 5.3] of the classical modular polynomial for the j-function. Assume first that f is invariant under S. If we replace z by $-1/(lz)$ in the equation $\Phi_l^f(f(z), f(lz)) = 0$, we obtain

$$\Phi_l^f(f(-1/(lz)), f(-1/z)) = 0.$$

Using the invariance of f under S, we derive

$$\Phi_l^f(f(lz), f(z)) = 0.$$

Since $\Phi_l^f(X, f)$ is irreducible in $\mathbf{C}[X,Y]$, we see that $\Phi_l^f(f, X)$ is a multiple of $\Phi_l^f(X, f)$. There exists a polynomial $g(X,Y)$ with

$$\Phi_l^f(f, X) = g(X,f)g(f,X)\Phi_l^f(f,X).$$

The Gauß lemma tells us that we have $g(X,Y) \in \mathbf{Z}[X,Y]$ and hence $g(X,Y) = \pm 1$. For $g(X,Y) = -1$, we get $\Phi_l^f(X,Y) = -\Phi_l^f(Y,X)$ and $\Phi_l^f(X,X) = 0$. Then $X - Y$ would be a factor of $\Phi_l^f(X,Y)$. This contradicts the irreducibility. Hence, we have $g(X,Y) = 1$ and Φ_l^f is symmetric.

The other case proceeds similarly, one replaces z by $-1/z$ in the beginning of the proof. □

Let $x \in \mathbf{Q}_p$ be a root of $\Psi_f(X, j(E)) \in \mathbf{Q}_p[X]$ and let I be an invertible $\mathcal{O}$-ideal of prime norm $l \nmid Np$. Let Φ_f^l be the modular polynomial defined above. From the moduli interpretation of $X(f;l)_a$, it is clear that one of the roots of $\Phi_l^f(x, X) \in \overline{\mathbf{Q}}_p[X]$ equals x^I. To see what the other roots are, we look at diagram 5.1. Above $x \in \mathbf{A}^1(\overline{\mathbf{Q}}_p)$ there are $\deg(f)$ distinct points $(E_i, P_i, Q_i) \in Y(f)_a(\overline{\mathbf{Q}}_p)$. Above $(E_i, P_i, Q_i) \in Y(f)_a(\overline{\mathbf{Q}}_p)$, there are $l+1$ points $(E_i, P_i, Q_i, G_j) \in Y(f;l)_a(\overline{\mathbf{Q}}_p)$. Here, G_j ranges over the $l+1$ subgroups of order l of $E_i[l]$. The points (E_i, P_i, Q_i, G_j) all map to $x \in \mathbf{A}^1(\overline{\mathbf{Q}}_p)$ under F. The images under $F' : X(f;l)_a \to \mathbf{A}^1$ are exactly the roots of $\Phi_l^f(x, X)$.

Remark. *The curve $X(f;l)$ is a quotient of $X(lN)$. Since $X(N)$ has good reduction outside N, the curve $X(f;l)$ has good reduction outside lN by [12, Proposition 4.2]. Hence, the description of the roots of $\Phi_l^f(x, X)$ remains valid over $\overline{\mathbf{F}}_p$.*

We need to decide which root of $\Phi_l^f(x, X)$ equals x^I. The first observation is that it suffices to look at the roots in $\mathbf{Q}_p$. Indeed, if x is a class invariant then we automatically have $x \in \mathbf{Q}_p$. If x is not a class invariant, then x^I need not lie in $\mathbf{Q}_p$. But if it does not, we have automatically proven that x is not a class invariant.

Usually, x^I is the only root of $\Phi_l^f(x, X)$ that is also a root of $\Psi_f(X, j(E^I))$. Hence, we test for all roots $\alpha \in \mathbf{Q}_p$ of $\Phi_l^f(x, X)$ whether $\Psi_f(\alpha, j(E^I)) = 0$ holds. If x is a class invariant, we find at least one such α. If we find exactly one root with this property, we have computed x^I.

Lemma 5.2. *Let the notation be as above. Suppose that f has degree 1, and let $x \in \mathbf{Q}_p$ be a class invariant. If the l-torsion of E is not $\mathbf{Q}_p$-rational, there is there is exactly one root $\alpha \in \mathbf{Q}_p$ of both $\Phi_l^f(x, X) \in \mathbf{Q}_p[X]$ and $\Psi_f(X, j(E^I)) \in \mathbf{Q}_p[X]$.*

Proof. Let $(E, P, Q) \in Y(f)_a(\overline{\mathbf{Q}}_p)$ be the unique point of $Y(f)_a$ with $f(E, P, Q) = x \in \mathbf{Q}_p$. Of the $l+1$ points $(E, P, Q, G_i) \in Y(f;l)_a(\overline{\mathbf{Q}}_p)$ lying over $(E, P, Q) \in Y(f)_a(\overline{\mathbf{Q}}_p)$, only for the 2 points having $G_i = E[I]$ or $G_i = E[\overline{I}]$, the value $j(t(E, P, Q, G_i))$ is contained in $\mathbf{Q}_p$, cf. [2, Theorem 5.1]. If both $F'(E, P, Q, E[I])$ and $F'(E, P, Q, E[\overline{I}])$ are roots of $\Phi_l^f(x, X) \in \mathbf{Q}_p[X]$, then we must have $[I] = [\overline{I}] \in \mathrm{Pic}(\mathcal{O})$. Because x is a class invariant, we then have $F'(E, P, Q, E[I]) = F'(E, P, Q, E[\overline{I}])$. □

If we want that the polynomial P_Δ^f has much smaller coefficients than P_Δ^j, we need the degree of f to be small. Many functions that are used in practice, including Weber's function $\mathfrak{f}$ from the introduction, have degree 1. For general f, we cannot prove that there is only one root α as above. In our computations, we have never found an example where this problem occurs.

6. The algorithm

It is of great help that for many class invariants the coefficients of the modular polynomial Φ_l^f are a lot smaller than those of the classical modular polynomial for j. As an example, we consider the Weber function $\mathfrak{f}$ from the introduction. For small primes l the coefficients of the polynomial are really small, like

$$\Phi_5^{\mathfrak{f}}(X,Y) = (X^5 - Y)(X - Y^5) + 5XY.$$

For $l = 13$ it takes at least 2 of these pages to write down the polynomial Φ_l^j, but we have

$$\begin{aligned}\Phi_{13}^{\mathfrak{f}}(X,Y) = &(X^{13} - Y)(X - Y^{13}) + 5 \cdot 13XY \\ &+13(X^2Y^{12} + X^{12}Y^2 + 4X^{10}Y^4 + 4X^{10}Y^4 + 6X^6Y^8 + 6X^8Y^6).\end{aligned}$$

This can be used to give a significant practical speed up of the algorithm. We now give the Algorithm to compute on input $\Delta < -4$ a generating polynomial for the ring class field $H_{\mathcal{O}}$ corresponding to the order of discriminant Δ. Assume that we are given a modular function f that yields class invariants when evaluated at appropriate generators $\omega \in \mathbf{H}$ of the $\mathbf{Z}$-algebra $\mathcal{O} = \mathbf{Z}[\omega]$. We need the Fourier expansion of f and the minimal polynomial $\Psi_f(f, X) \in \mathbf{Z}[j, X]$.

Step 1. Find a prime $p \nmid N$ and an elliptic curve $\overline{E}/\mathbf{F}_p$ with $\mathrm{End}(\overline{E}) \cong \mathcal{O}$. We compute the zeroes $x_1, \ldots, x_k \in \mathbf{F}_p$ of $\Psi_f(X, j(\overline{E})) \in \mathbf{F}_p[X]$.

Step 2. We have to decide which of these zeroes is the reduction of a class invariant. Compute smooth primitive generators $y_1, \ldots, y_t$ of $(\mathcal{O}/N\mathcal{O})^*$.

Write $(y_1) = \alpha_1 \cdot \ldots \cdot \alpha_s$, with $N(\alpha_i) = l_i \in \mathbf{Z}$ prime. Compute the cycle

$$j(E) \xrightarrow{\bar{\rho}_{\alpha_1}} j(\overline{E}^{\alpha_1}) \xrightarrow{\bar{\rho}_{\alpha_2}} \ldots \xrightarrow{\bar{\rho}_{\alpha_t}} j(\overline{E}^{(y_1)}) = j(\overline{E})$$

of j-invariants over $\mathbf{F}_p$ as in Section 2 using the modular polynomials for j. Compute all roots $\eta_i \in \mathbf{F}_p$ of $\Phi_{l_1}^f(x_1, X) \in \mathbf{F}_p[X]$ that also satisfy $\Psi_f(\eta_i, j(\overline{E}^{\alpha_1})) = 0$, where $\Phi_{l_1}^f$ is the modular polynomial for f. In practice, we find either zero or one such root η_i, cf. Section 5. If we find zero roots, then x_1 is not the reduction of a class invariant. If we find one root, we have computed $x_1^{\alpha_1}$.

Continuing like this, we compute a series

$$x_1 \xrightarrow{\bar{\rho}_{\alpha_1}} x_1^{\alpha_1} \xrightarrow{\bar{\rho}_{\alpha_2}} \ldots \xrightarrow{\bar{\rho}_{\alpha_t}} x_1^{(y_1)}.$$

If we have $x_1^{(y_1)} = x_1$, we compute $x_1^{(y_2)}$, etc. If x_1 is invariant under all generators $y_1, \ldots, y_t$ of $(\mathcal{O}/N\mathcal{O})^*$, it is the reduction of a class invariant. Otherwise, we repeat this computation with x_2, etc., until we find a reduction of a class invariant.

Step 3. Say that $x \in \mathbf{F}_p$ is the reduction of a class invariant. We choose a smooth $\mathcal{O}$-ideal $(\alpha) = \alpha_1 \ldots \alpha_u$ for the map ρ_α from Section 2. Here, we require that the norm of α is coprime to the level N.

We compute a cycle

$$j(\overline{E}) \xrightarrow{\bar{\rho}_{\alpha_1}} j(\overline{E}^{\alpha_1}) \xrightarrow{\bar{\rho}_{\alpha_2}} \ldots \xrightarrow{\bar{\rho}_{\alpha_u}} j(\overline{E}^{(\alpha)}) = j(\overline{E}),$$

and using this cycle we compute the corresponding cycle

$$x \xrightarrow{\bar\rho_{\alpha_1}} x^{\alpha_1} \xrightarrow{\bar\rho_{\alpha_2}} \dots \xrightarrow{\bar\rho_{\alpha_u}} x^{\alpha} = x$$

for x, just like we did in Step 2.

Step 4. Lift $\overline{E}/\mathbf{F}_p$ to $E_1/\mathbf{Q}_p$ by lifting the coefficients of the Weierstraß equation for $\overline{E}$ arbitrarily. We use two p-adic digits accuracy in this Step.

Step 5. Lift $x \in \mathbf{F}_p$ to $x_1 \in \mathbf{Z}_p/(p^2)$ as a root of $\Psi_f(X, j(E_1)) \in \mathbf{Z}_p[X]$. It is easy to compute $x_1^{\alpha_1}$. Indeed, we know the reduction $\overline{x_1^{\alpha_1}} = x^{\alpha_1}$ modulo p, hence we know which root of $\Phi_l^f(x_1, X) \in (\mathbf{Z}_p/(p^2))[X]$ to pick. In this way we compute $x_1^{(\alpha)} \in \mathbf{Z}_p/(p^2)$.

We compute $\rho_\alpha(j(E_1))$ as the unique root of $\Psi_f(x_1^{(\alpha)}, X) \in \mathbf{Z}_p[X]$ that reduces to $j(\overline{E})$ modulo p.

Step 6. Update $\rho_\alpha(j(E_1))$ to $j(E_2)$ according to the 'Newton formula' (2.1).

Step 7. Repeat Step 5 with $j(E_1)$ replaced by $j(E_2)$. We now work with four p-adic digits precision. We obtain $j(E_3)$. Continue this iteration process until we have computed the canonical lift $j(\tilde{E})$ with high enough accuracy. We compute the 'canonical lift' $\tilde{x} \in \mathbf{Z}_p$ of x as the root of $\Psi_f(X, j(\tilde{E}))$ reducing to $x \in \mathbf{F}_p$.

Step 8. It remains to compute the conjugates of $\tilde{x}$ under $\mathrm{Pic}(\mathcal{O})$. This is done exactly as before. For an invertible $\mathcal{O}$-ideal I of norm l coprime to N, we compute $j(\overline{E}^I) \in \mathbf{F}_p$ as in Section 2. Knowing $j(\overline{E}^I)$, we compute a root $\beta \in \mathbf{F}_p$ of $\Phi_l^f(x, X) \in \mathbf{F}_p[X]$ that also satisfies $\Psi_f(\beta, j(\overline{E}^I)) = 0$. Just as in Step 2, in practice we only find *one* such β, and we then have $x^I = \beta$.

We know the reduction $\overline{\tilde{x}^I} = \beta$ of $\tilde{x}^I$, and consequently, we know which root of $\Phi_l^f(\tilde{x}, X) \in \mathbf{Z}_p[X]$ is $\tilde{x}^I$.

Step 9. Expand the polynomial

$$P_\Delta^f = \prod_{[I] \in \mathrm{Pic}(\mathcal{O})} (X - \tilde{x}^I) \in \mathbf{Z}_p[X].$$

Remark. *We only need the (large) modular polynomials for j when we are working over $\mathbf{F}_p$. In the lifting process we only need to know the smaller modular polynomials for f.*

7. Example

We illustrate the p-adic algorithm by working with the function

$$f(z) = \frac{\eta(z/5)\eta(z/7)}{\eta(z)\eta(z/35)} \in \mathbf{Z}[[q^{1/35}]],$$

where $\eta(z)$ denotes the Dedekind eta function. More examples can be found in [3, Chapter 7]. Let $\mathcal{O}$ be the order of discriminant $\Delta = -1571$. By [8, Theorem 3], the value $f(\omega)$ is a class invariant for a suitable choice of generator of the $\mathbf{Z}$-algebra $\mathcal{O} = \mathbf{Z}[\omega]$. Furthermore, the polynomial P_Δ^f has integer coefficients, and the size of these coefficients is a factor 24 smaller than for the j-function.

By explicitly computing the conjugates of f over $\mathbf{Q}(j)$, we compute the minimal polynomial Ψ_f of f. In accordance with the example in [9], we find

$$\Psi_f(j, X) = X^{48} + (-j + 708)X^{47} + \ldots + 12X + 1 \in \mathbf{Z}[j, X].$$

The function f generates the function field of $X_0(35)$ over $\mathbf{C}(j)$ and therefore has degree 2. Using linear algebra, we compute some modular polynomials.

$$\begin{aligned}\Phi_2^f &= X^3 + Y^3 - X^2Y^2 + 2(XY^2 + X^2Y) + XY \\ \Phi_3^f &= X^4 + Y^4 - X^3Y^3 + 3(X^2Y^3 + X^3Y^2) + 3(Y^3X + X^3Y) \\ &\quad +6(X^2Y^2) - 3(Y^2X + X^2Y) - XY\end{aligned}$$

The fact that these polynomials have degree $l + 1$ and not $2(l + 1)$ is due to the fact that f is invariant under the Atkin-Lehner involution – the map $b : X(f) \to C$ in diagram (5.2) has degree 2. Since 5 and 7 divide the level 35 of f, we cannot use Φ_5^f and Φ_7^f. We computed all modular polynomials for primes up to 23. This should be seen as a *precomputation*.

The prime $p = 449$ splits completely in the ring class field $H_{\mathcal{O}}$, and the elliptic curve

$$\overline{E} : Y^2 = X^3 + X + 16$$

of j-invariant 383 has endomorphism ring $\mathcal{O}$. The polynomial $\Psi_f(j(\overline{E}), X) \in \mathbf{F}_p[X]$ has the four roots $b_1 = 62$, $b_2 = 130$, $b_3 = 239$ and $b_4 = 358$ in $\mathbf{F}_p$. We know [8, Theorem 3] that each one of them is a reduction of a class invariant. To illustrate our p-adic techniques, we reprove this.

A root $b_i \in \mathbf{F}_p$ is the reduction of a class invariant if it is invariant under the action of the group $(\mathcal{O}/35\mathcal{O})^*/\{\pm 1\} \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/12\mathbf{Z} \times \mathbf{Z}/12\mathbf{Z}$. We take $\{\pi_p, 2\pi_p - 11, 2\pi_p - 19, -\pi_p - 28\}$ as a generating set for $(\mathcal{O}/35\mathcal{O})^*$ where π_p is an element of norm p. We choose this particular set of generators, because the elements have smooth norm (except π_p).

Since b_i is an element of $\mathbf{F}_p$, it is invariant under the action of π_p. The element $\alpha = 2\pi_p - 11$ has order 12 in $(\mathcal{O}/35\mathcal{O})^*$, and the ideal (α) of norm $1587 = 3 \cdot 23^2$ factors as

$$(\alpha) = \mathfrak{p}_3 \cdot \mathfrak{p}_{23}^2 = (3, \pi_p - 1) \cdot (23, \pi_p - 17).$$

We compute the cycle of j-invariants over $\mathbf{F}_p$ for the map $\overline{\rho}_\alpha : \mathrm{Ell}_\Delta(\mathbf{F}_p) \to \mathrm{Ell}_\Delta(\mathbf{F}_p)$:

$$j(\overline{E}) = 383 \xrightarrow{\mathfrak{p}_3} 13 \xrightarrow{\mathfrak{p}_{23}} 24 \xrightarrow{\mathfrak{p}_{23}} 383.$$

The modular polynomial $\Phi_3^f(b_1, X) \in \mathbf{F}_p[X]$ has 2 roots, namely $64, 95 \in \mathbf{F}_p$. We check that 64 satisfies $\Psi_f(13, 64) = 0$, where 13 is the j-invariant of $\overline{E}^{\mathfrak{p}_5}$.

The other root 95 does not satisfy $\Psi_f(13,95)=0$, and we conclude that we have $b_1^{\mathfrak{p}_3}=64\in\mathbf{F}_p$. Continuing like this, we compute

$$b_1 = 62 \xrightarrow{\mathfrak{p}_3} 64 \xrightarrow{\mathfrak{p}_{23}} 34 \xrightarrow{\mathfrak{p}_{23}} 62.$$

The computation for b_2,b_3,b_4 proceeds similarly and they are also invariant under the action of (α). The computation for the other two elements of our generating set is similar. All four elements b_i are invariant under the action of $(\mathcal{O}/35\mathcal{O})^*$, proving that they are reductions of class invariant.

We will work with $b=b_1=62\in\mathbf{F}_p$. For the polynomial P_Δ^j we would have needed 62 p-adic digits accuracy. For P_Δ^f we only need 3 p-adic digits. As element α for the map $\rho_\alpha : X_D(\mathbf{C}_p)\to X_D(\mathbf{C}_p)$ we again take $\alpha=2\pi_p-11$ of norm $3\cdot 23^2$. We lift $\overline{E}/\mathbf{F}_p$ to the curve $E_1/\mathbf{Q}_p$ defined by $Y^2=X^3+X+16$ of j-invariant $j(E_1)=383+224p\in\mathbf{Q}_p$. This leads to the lift $b_1=62+45p\in\mathbf{Q}_p$.

We compute the 'cycle' for $b_1\in\mathbf{Q}_p$ corresponding to the map ρ_α:

$$b_1 = 62+45p \xrightarrow{\mathfrak{p}_3} 64+175p \xrightarrow{\mathfrak{p}_{23}} 34+6p \xrightarrow{\mathfrak{p}_{23}} 62-198p = b_1^{(\alpha)}$$

The degree two polynomial $\Psi_f(X,b_1^{(\alpha)})\in\mathbf{Z}_p[X]$ has roots $131-94p+O(p^2)$ and $383-119p+O(p^2)$. We conclude that we have $\rho_\alpha(j(E_1))=383-119p\in\mathbf{Q}_p$. We update this j-value according to the 'Newton formula' (2.1) and obtain $j(E_2)=383-98p\in\mathbf{Q}_p$. This is the j-invariant of the canonical lift in two p-adic digits accuracy. We compute $\tilde{b}=62-64p+O(p^2)\in\mathbf{Q}_p$. Similarly, we compute $j(E_3)=383-98p+127p^2$ and $\tilde{b}=62-64p+66p^2$. To compute the conjugates of $\tilde{b}$ under $\mathrm{Pic}(\mathcal{O})\cong\mathbf{Z}/17\mathbf{Z}\cong\langle\mathfrak{p}_3\rangle$ we use the modular polynomial Φ_3^f once more. In the end we expand the polynomial

$$P_\Delta^f = \prod_{[I]\in\mathrm{Pic}(\mathcal{O})} (X-\tilde{b}^I)$$

and find

$$\begin{aligned} P_{-1571}^f = {} & X^{17}+21X^{16}+918X^{15}-11046X^{14}+49849X^{13}-115187X^{12} \\ & +112918X^{11}+168294X^{10}-275500X^9+361744X^8-403346X^7 \\ & +181066X^6-10143X^5-3403X^4-4290X^3+1422X^2 \\ & -71X+1\in\mathbf{Z}[X]. \end{aligned}$$

Acknowledgements

I thank Bas Edixhoven 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.

2. R. Bröker, *A p-adic algorithm to compute the Hilbert class polynomial*, Preprint, 2006, available at `http://www.math.ucalgary.ca/~reinier/padidj.pdf`.
3. R. Bröker, *Constructing elliptic curves of prescribed order*, PhD-thesis, Universiteit Leiden, 2006.
4. R. Bröker, A. Enge, K. Lauter, F. Morain, *Computing the Hilbert class polynomial*, In preparation.
5. H. Cohen, G. Frey et al., *Handbook of elliptic and hyperelliptic curve cryptography*, Chapman & Hall, 2006.
6. 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.
7. A. Enge, *The complexity of class polynomial computation via floating point approximations*, Preprint, 2006.
8. A. Enge, R. Schertz, *Constructing elliptic curves over finite fields using double eta-quotients*, J. Théor. Nombres Bordeaux **16** (2004), 555–568.
9. A. Enge, R. Schertz, *Modular curves of composite level*, Acta Arith. **118** (2005), 129–141.
10. 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.
11. A. Gee, P. Stevenhagen, *Generating class fields using Shimura reciprocity*, Algorithmic Number Theory, Springer Lecture Notes in Computer Science, vol. 1423, 1998, pp. 441–453.
12. A. J. de Jong, *Families of curves and alterations*, Ann. Inst. Fourier (Grenoble) **47** (1997), 599–621.
13. D. Kohel, *Endomorphism rings of elliptic curves over finite fields*, PhD-thesis, University of California at Berkeley, 1996.
14. S. Lang, *Elliptic functions*, Springer Graduate Texts in Mathematics, vol. 112, 1987.
15. R. Schoof, *Counting points on elliptic curves over finite fields*, J. Théor. Nombres Bordeaux **7** (1993), 219–254.
16. G. Shimura, *Introduction to the arithmetic theory of automorphic forms*, Princeton University Press, 1971.
17. P. Stevenhagen, *Hilbert's 12th problem, complex multiplication and Shimura reciprocity*, Class field theory – its centenary and prospect, ed. K. Miyake, Adv. studies in pure math., vol. 30, 2001, pp. 161–176.
18. J. Vélu, *Isogénies entre courbes elliptiques*, C. R. Acad. Sci. Paris Sér. A–B **273** (1971), A238–A241.
19. H. Weber, *Lehrbuch der Algebra*, Friedrich Vieweg und Sohn, 1908.

University of Calgary, Department of Mathematics and Statistics, 2500 University Drive NW, Calgary, AB T2N 1N4, Canada
E-mail address: `reinier@math.ucalgary.ca`