Action of modular correspondences around CM points

Jean-Marc Couveignes and Thierry Henocq

Groupe de Recherche en Informatique et Mathématiques du Mirail*,
Université de Toulouse II, 5 allées Antonio Machado, 31058, Toulouse, France,
couveig, henocq@univ-tlse2.fr,
WWW home page: http://www.univ-tlse2.fr/grimm

Abstract. We study the action of modular correspondences in the p-adic neighborhood of CM points. We deduce and prove two stable and efficient p-adic analytic methods for computing singular values of modular functions. On the way we prove a non trivial lower bound for the density of smooth numbers in imaginary quadratic rings and show that the canonical lift of an elliptic curve over $\mathbb{F}_q$ can be computed in probabilistic time $\ll \exp((\log q)^{\frac{1}{2}+\epsilon})$ under GRH. We also extend the notion of canonical lift to supersingular elliptic curves and show how to compute it in that case.

1 Introduction

Let $X \to X(1)$ be any modular curve seen as a covering of $X(1)$. Let P be a Heegner point on X and let $f \in \bar{\mathbb{Q}}(X)$ be a $\bar{\mathbb{Q}}$-rational function.

For reasonable choices of f, class field theory ensures that $f(P)$ is an algebraic integer. It is a classical algorithmic problem to compute the minimum polynomial of $f(P)$.

The known methods for this rely on complex analytic uniformization of X and provide complex approximations for $f(P)$ and its conjugates f_i. See [5] for a recent general study of this approach.

One then forms and expands the degree h minimal polynomial $\mu(X) = \prod_i (X - f_i)$ the coefficient of which are rational integers.

The difficulty with this method (that appears in quite a range of different contexts) is that it is very hard to control the loss of accuracy while expanding μ.

The only rigorous available evaluations of how many digits are needed are a bit alarming (see [1, Section 7] and [2, Section 9]).

It is thus temptating to look for a p-adic analytic method for computing singular values of modular functions. The reason for that is that the p-adic absolute accuracy is conserved when adding or multiplying two p-adic integers

* The GRIMM is supported by the French Ministry of Research through *Action Concertée Incitative CRYPTOLOGIE*, by the Direction Centrale de la Sécurité des Systèmes d'Information and by the Centre Électronique de L'ARmement.

i.e if one knows a and b up to $O(p^k)$ then one knows $a+b$ and ab up to $O(p^k)$ also.

One may logically look for some p-adic uniformization of X but such an uniformization does not exist in general. In particular it does not exist in the *most important* case of $X = X(1)$.

Instead of that we define and study a representation of the ideal group of an imaginary quadratic order as automorphism group of a p-adic neighborhood of the associated CM points. This representation is quite computational and the CM points are characterized and computed as fixed points of this representation. In this way we also manage to define canonical lifts for supersingular curves.

All this leads to two different proven stable and efficient methods for computing singular values of modular functions.

The reader who is not completely unwilling to read mathematics may also find some intrinsic interest to the p-adic representation itself and to our lemmata.

2 Modular correspondences in the neighborhood of CM points

We refer to [8] for the elementary theory of complex multiplication.

We start with

Definition 1. *Let k be an algebraically closed field and $\mathcal{O}$ the imaginary quadratic order with discriminant $-\Delta$. We denote by $\mathcal{NELL}_\Delta(k)$ the set of isomorphism classes of couples (E,ι) where E is an elliptic curve over k and $\iota : \mathcal{O} \to \mathcal{E}nd(E)$ is a maximal embedding (when E is ordinary ι is an isomorphism). Such a couple is called a normalized elliptic curve. We say that two normalized elliptic curves (E,ι) and (E',ι') are isomorphic if there is an isomorphism $I : E \to E'$ such that $I^{-1}\iota'(X)I = \iota(X)$ for any X in $\mathcal{O}$.*

We denote by $\mathcal{ELL}_\Delta(k)$ the quotient of $\mathcal{NELL}_\Delta(k)$ by the action of complex conjugation. When the characteristic p of k has two primes in the fraction field of $\mathcal{O}$ above it then $\mathcal{ELL}_\Delta(k)$ is the set of isomorphism classes of curves with CM by $\mathcal{O}$.

We now fix an embedding of $\bar{\mathbb{Q}}$ in $\mathbb{C}$. Let $\mathcal{O}$ be a quadratic order with group of units $\{1,-1\}$, class group $\mathcal{C}\ell(\mathcal{O})$, conductor m and discriminant $-\Delta$. Then $\mathcal{ELL}_\Delta(\bar{\mathbb{Q}})$ is the finite set of isomorphism classes of elliptic curves over $\bar{\mathbb{Q}}$ with complex multiplication by $\mathcal{O}$. We may see it as a reduced zero dimensional subvariety in $X(1) = \mathbb{P}^1 - \{\infty\}$, the moduli space of elliptic curves. There is a free faithful action of $\mathcal{C}\ell(\mathcal{O})$ on it.

We fix a prime p and an embedding of $\bar{\mathbb{Q}}$ in $\mathbb{C}_p$ and denote by $\bar{\mathbb{F}}_p$ the residue field of $\mathbb{C}_p$. We assume that p has two primes of $\mathbb{Q}(\sqrt{-\Delta})$ above it. Then $\mathcal{ELL}_\Delta(\bar{\mathbb{Q}})$ splits over $\mathbb{F}_q$ with $q = p^d$ and $d = c\ell(\mathcal{O}')$ where $\mathcal{O}'$ is the order with conductor m' the larger prime to p factor of m. We call $-\Delta'$ the discriminant of $\mathcal{O}'$. We know that reduction modulo p induces a surjection from $\mathcal{ELL}_\Delta(\bar{\mathbb{Q}})$ onto $\mathcal{ELL}_{\Delta'}(\bar{\mathbb{F}}_q)$. This is the set of isomorphism classes of elliptic curves over $\bar{\mathbb{F}}_q$ with

CM by $\mathcal{O}'$. It has cardinality $c\ell(\mathcal{O}')$ and is acted on by $\mathcal{C}\ell(\mathcal{O})$. We also assume that $\mathcal{O}'$ has unit group $\{1,-1\}$.

Let $\mathcal{ELL}^{\circ}_{\Delta}$ be the set of isomorphism classes of elliptic curves over $\mathbb{C}_p$ that reduce modulo p to an elliptic curve in $\mathcal{ELL}_{\Delta'}(\bar{\mathbb{F}}_q)$. Using the modular invariant j this set can be given an analytic structure and is the disjoint union of $c\ell(\mathcal{O}')$ open p-adic disks of radius 1. Every such disk contains $c\ell(\mathcal{O})/c\ell(\mathcal{O}')$ elements in $\mathcal{ELL}_{\Delta}(\bar{\mathbb{Q}})$.

To every point in $\mathcal{ELL}_{\Delta}(\bar{\mathbb{Q}})$ we associate an ideal $\mathfrak{a} \subset \mathcal{O} \subset \bar{\mathbb{Q}} \subset \mathbb{C}$ and a model $E_{\mathfrak{a}} = \mathbb{C}/\mathfrak{a}$ for the corresponding isomorphism class. This way, all the curves $E_{\mathfrak{a}}$ share the same endomorphism ring $\mathcal{O}$. The reductions $E_{\mathfrak{a}} \bmod p$ provide models for the elements in $\mathcal{ELL}_{\Delta'}(\bar{\mathbb{F}}_q)$. Whenever there is no risk of confusion, we shall denote by $\mathfrak{a}$ a point in $\mathcal{ELL}_{\Delta}(\bar{\mathbb{Q}})$ or $\mathcal{ELL}_{\Delta'}(\bar{\mathbb{F}}_q)$.

If $\mathfrak{i}$ is a prime to m ideal in $\mathcal{O}$ we denote by $E_{\mathfrak{a}}[\mathfrak{i}]$ the intersection of kernels of all endomorphisms in $\mathfrak{i}$. Quotienting by this subgroup defines an isogeny $E_{\mathfrak{a}} \to E_{\mathfrak{a}\mathfrak{i}^{-1}}$. If $\mathfrak{b}$ represents the class of $\mathfrak{a}\mathfrak{i}^{-1}$ we set $\mathfrak{i} \bullet \mathfrak{a} = \mathfrak{b}$. If further $\mathfrak{i}$ is prime to p we similarly define an isogeny from the reduction $\bar{E}_{\mathfrak{a}}$ modulo p of $E_{\mathfrak{a}}$.

Thus the group $I(pm)$ of prime to pm ideals of $\mathcal{O}$ acts on both $\mathcal{ELL}_{\Delta}(\bar{\mathbb{Q}})$ and $\mathcal{ELL}_{\Delta'}(\bar{\mathbb{F}}_q)$ and the reduction map is equivariant for these actions.

We now show how this action extends to a continuous action on $\mathcal{ELL}^{\circ}_{\Delta}$. Let x be a point in $\mathcal{ELL}^{\circ}_{\Delta}$. Let $\mathfrak{a}$ be a point in $\mathcal{ELL}_{\Delta}(\bar{\mathbb{Q}})$ which is close to x and let $E_{\mathfrak{a}} = \mathbb{C}/\mathfrak{a}$ be the corresponding elliptic curve. We denote by $D_{\mathfrak{a}}$ the disk in $\mathcal{ELL}^{\circ}_{\Delta}$ that contains $\mathfrak{a}$ and x. Let E_x be a model for x which is close to $E_{\mathfrak{a}}$ i.e. an elliptic curve over $\mathbb{C}_p$ such that $j(E_x) = j(x)$ and E_x and $E_{\mathfrak{a}}$ have equal reductions modulo p (so E_x is the fiber at x in the universal curve over $D_{\mathfrak{a}}$ and this universal curve exists because $D_{\mathfrak{a}}$ does not contain $j = 0$ nor $j = 1728$.) Let $\mathfrak{i}$ be an ideal in $I(pm)$ and set $\mathfrak{b} = \mathfrak{i} \bullet \mathfrak{a}$. Let $E_{\mathfrak{a}}[\mathfrak{i}]$ be the finite subgroup of $E_{\mathfrak{a}}$ defined by $\mathfrak{i}$. Because $\mathfrak{i}$ is prime to p this group 'lifts' to a group scheme over $D_{\mathfrak{a}}$ whose fiber at x defines a subgroup $E_x[\mathfrak{i}]$ of E_x. The quotient of E_x by this group defines a point $y = \mathfrak{i} \bullet x$ in $\mathcal{ELL}^{\circ}_{\Delta}$ which is close to $\mathfrak{b}$.

For every $\mathfrak{i} \in I(pm)$ the map $[\mathfrak{i}] : x \mapsto \mathfrak{i} \bullet x$ is a continuous map on $\mathcal{ELL}^{\circ}_{\Delta}$. Indeed, let $\mathfrak{j}$ be an ideal in $\mathcal{O}$ and α a rational integer such that $\mathfrak{i} = (\alpha)\mathfrak{j}$ and $\mathcal{O}/\mathfrak{j}$ is cyclic of order N. Then $[\mathfrak{i}]$ being the restriction of the level N correspondence is an algebraic map. We recall that the level N correspondence is the divisor on $X(1) \times X(1)$ image of $X_0(N)$ by the map $(E \to E') \mapsto (j(E), j(E'))$. The curve $X_0(N)$ has good reduction modulo p and $\mathfrak{a} \in X_0(N)$ is not p-adically close to any ramification point of j or j'. So $j' - j'(\mathfrak{a})$ is an integral invertible series in $j - j(\mathfrak{a})$ and the radius of convergence of $[\mathfrak{i}]$ is 1. The integer α being inessential we shall assume $\alpha = 1$ and $\mathfrak{i} = \mathfrak{j}$. In that case we say that $\mathfrak{i}$ is *reduced*. The inverse of $[\mathfrak{i}]$ is $[\bar{\mathfrak{i}}]$ given by complex conjugation.

We thus have constructed a morphism ρ from the group $I(pm)$ of prime to pm ideals of $\mathcal{O}$ to the group $\mathrm{Aut}(\mathcal{ELL}^{\circ}_{\Delta})$ of automorphisms of the analytic variety $\mathcal{ELL}^{\circ}_{\Delta}$. The restriction of ρ to the group $P(pm)$ of prime to pm principal ideals of $\mathcal{O}$ defines a morphism (still denoted by ρ)

$$\rho : P(pm) \to \mathrm{Aut}^*(\mathcal{ELL}^{\circ}_{\Delta})$$

to the group of automorphisms that fix $\mathcal{ELL}_\Delta(\bar{\mathbb{Q}})$ (the CM points) and therefore stabilize every disk $D_\mathfrak{a}$.

In order to study this morphism we denote by $\delta_\mathfrak{a} : \mathrm{Aut}^*(\mathcal{ELL}^\circ_\Delta) \to \mathbb{C}_p^*$ the differentiation at the CM point $\mathfrak{a}$.

From lemma 1 below we deduce that $\delta_\mathfrak{a} \circ \rho : P(pm) \to \mathbb{C}_p^*$ is independent of $\mathfrak{a}$, takes values in $\bar{\mathbb{Q}}^*$ and $\delta_\mathfrak{a}(\rho((\mathcal{L}))) = \mathcal{LL}^*$ where $\mathcal{L}^* = \bar{\mathcal{L}}^{-1}$. In particular, the kernel of ρ consists of ideals $(\mathcal{L})$ with $\mathcal{L} \in \mathbb{Q}^*$ prime to pm.

Lemma 1. *Let $\mathcal{O}$ be a quadratic order with group of units $\{1,-1\}$ and conductor m. Let $\mathcal{L} \in \mathcal{O}$ such that $\mathcal{O}/\mathcal{L}$ is cyclic of order N. Let j and j' be the two functions on $X_0(N)$ defined by $j(E \to E') = j(E)$ and $j'(E \to E') = j(E')$. The value of the slope of the tangent $\sigma = \frac{dj'}{dj}$ at all Heegner points with CM by $\mathcal{O}$ and representing multiplication by $\mathcal{L}$ isogenies is $\mathcal{LL}^*$.*

The order $\mathcal{O}$ has discriminant $-\Delta = -m^2D$ and basis $(1, m\frac{\sqrt{-D}-D}{2})$ and $\mathcal{L} = a + bm\frac{\sqrt{-D}-D}{2}$ has norm $N = a^2 - abDm + b^2Km^2$ with $K = D(D+1)/4$. Set $\alpha = m\frac{\sqrt{-D}-D}{2}$ and let c be an integer congruent to a/b modulo N. We have $\alpha^2 + Dm\alpha + Km^2 = 0$. Define the two integers $u = \frac{a-bc}{N}$ and $v = b\frac{c^2-cDm+Km^2}{N}$. Note that b is invertible modulo N because $\mathcal{L}$ is reduced. We look for the Smith normal form of $(\mathcal{L}) \subset \mathcal{O}$. Let $\phi : \mathcal{O} \to \mathbb{Z}$ be the linear form defined by $\phi(x+y\alpha) = x - cy$ that induces an isomorphism $\mathcal{O}/\mathcal{L} \xrightarrow{\phi} \mathbb{Z}/N\mathbb{Z}$. Together with the linear form ψ defined by $\psi(x+y\alpha) = y$ this makes a basis (ϕ, ψ) for the dual of $\mathcal{O}$. A dual basis for $\mathcal{O}$ is $(1, \beta)$ with $\beta = c + \alpha$. A basis for $(\mathcal{L})$ is then (N, β) and this is the Smith normal form. The lattice $\mathcal{L}^*\mathcal{O} = \frac{1}{N}(\mathcal{L})$ admits the two basis $(1, \frac{\beta}{N})$ and $(\mathcal{L}^*, \mathcal{L}^*\beta)$ with transition matrix $\mathcal{M} \in \mathrm{PSL}_2(\mathbb{Z})$

$$\begin{pmatrix} \mathcal{L}^*\beta \\ \mathcal{L}^* \end{pmatrix} = \mathcal{M} \begin{pmatrix} \frac{\beta}{N} \\ 1 \end{pmatrix} = \begin{pmatrix} bc + a - bDm & -v \\ b & u \end{pmatrix} \begin{pmatrix} \frac{\beta}{N} \\ 1 \end{pmatrix}.$$

The class of $\tau = \frac{\beta}{N}$ modulo the action of $\Gamma_0(N)$ on the upper half plane represents the N-isogeny $\mathbb{C}/(1,\tau) \xrightarrow{\times N} \mathbb{C}/(1, N\tau) \xrightarrow{\times \mathcal{L}^*}_{\simeq} \mathbb{C}/(1,\tau)$ which is an endomorphism. So τ is a Heegner point associated to multiplication by $\mathcal{L}$ endomorphism. Since $\frac{dj}{d\tau}$ is a constant times $j\frac{E_6}{E_4}$, the slope $\frac{dj'}{dj}$ is $N\frac{j'}{j}\frac{E_4}{E_4'}\frac{E_6'}{E_6}$ and since $N\tau = \mathcal{M}\tau$ the slope at τ is $N(b\tau + u)^2$ which is easily seen to be independent of c and equal to $\mathcal{LL}^*$. There are $c\ell(\mathcal{O})$ Heegner points of level N with complex multiplication by $\mathcal{O}$ and representing the multiplication by $\mathcal{L}$ isogeny, all defined over the Hilbert class field of $\mathcal{O}$ and conjugated over $\mathbb{Q}(\sqrt{-\Delta})$.

Since $\mathcal{LL}^*$ belongs to the later field, the slope is the same at all such Heegner points. □

We observe that the action of a reduced ideal $\mathfrak{i}$ of norm N on a point $x \in \mathcal{ELL}^\circ_\Delta$ can be computed in time polynomial in N, $\log q$, and almost linear in the p-adic accuracy of x i.e. the number of significant terms in its p-adic expansion. One first reduces to the case N is prime (not essential but simpler).

One then computes the kernel $\bar{E}_{\mathfrak{a}}[\mathrm{i}]$ of the isogeny modulo p thanks to Atkin-Elkies techniques (see [15]). This kernel is then lifted on E_x thanks to Hensel's lemma. The isogeny $E_x \to E_y$ follows using Vélu's formulae [18].

We summarize in

Theorem 1. *Let $\mathcal{O}$ be a quadratic order, p a prime and $\mathcal{O}'$ the smallest p-maximal overorder of $\mathcal{O}$. Assume $\mathcal{O}'$ has group of units $\{1,-1\}$. Let m be the conductor of $\mathcal{O}$. The group $P(pm)$ of prime to pm principal ideals of $\mathcal{O}$ has a modular representation ρ as automorphism group of the p-adic disk with radius 1 in $X(1)$ around any point $\mathfrak{a}$ with CM by $\mathcal{O}$. The differentiation of this representation is just $\mathcal{L} \in P(pm) \mapsto \mathcal{L}\mathcal{L}^*$. The action of $\rho(\mathcal{L})$ on a given point can be computed in time polynomial in N, n, $\log q$ and almost linear in k i.e. $k(\log k)^{O(1)}$ where N is the norm of the bigger prime ideal factor of $\mathcal{L}$, and n is the number of such factors with multiplicities, $\mathbb{F}_q$ is the residue field of $\mathfrak{a}$ and k is the desired accuracy of the result.*

Remark 1. If $\mathcal{O}'$ is $\mathbb{Z}[i]$ (resp. $\mathbb{Z}[\rho]$) then the theorem holds with $\mathcal{L}\mathcal{L}^*$ replaced by $(\mathcal{L}\mathcal{L}^*)^2$ (resp. $(\mathcal{L}\mathcal{L}^*)^3$.)

Remark 2. The $\bullet$ action of principal ideals in $\mathcal{O}'$ (not necessarily principal in $\mathcal{O}$) on the set $\mathcal{E}\mathcal{L}\mathcal{L}_\Delta(\bar{\mathbb{Q}})$ is a Galois action and can be expressed in terms of the Artin map.

3 Computing the canonical lift in all characteristics

In this section we are interested in computing p-adic approximations of the canonical lift of an ordinary elliptic curve over a finite field.

We shall restrict to the case p is prime to the conductor m. So p splits in $\mathcal{O}$. If this is the case the reduction map

$$R : \mathcal{E}\mathcal{L}\mathcal{L}_\Delta(\bar{\mathbb{Q}}) \to \mathcal{E}\mathcal{L}\mathcal{L}_\Delta(\bar{\mathbb{F}}_q)$$

is an equivariant bijection.

We shall prove the

Theorem 2. *Assuming GRH, for any positive ϵ there is an algorithm that computes the inverse of the reduction map R at a given point x in $\mathcal{E}\mathcal{L}\mathcal{L}_\Delta(\bar{\mathbb{F}}_q)$ in probabilistic time*

$$\left[\exp((\log q)^{\frac{1}{2}+\epsilon}) \times \log k\right]^{O(1)} \times k$$

with accuracy k i.e. the error is $O(p^k)$.

In order to prove 2 we give and discuss an algorithm. For fixed ϵ the algorithm goes as follows. We first call E the curve over $\mathbb{F}_q$ associated to the point x. We look for the canonical lift of E.

If the characteristic p of $\mathbb{F}_q$ is less than $2\exp((\log 4q)^{\frac{1}{2}+\epsilon})$ we lift E together with all its conjugates over $\mathbb{F}_p$ using the equations in Lubin and Tate and Serre's

work [16, 11] and/or the cousin algorithm used in Satoh's algorithm [13]. The running time is polynomial in p and the degree d of $\mathbb{F}_q$ over $\mathbb{F}_p$. The result follows.

If $p > 2\exp((\log 4q)^{\frac{1}{2}+\epsilon})$ we make use of smooth isogenies in the spirit of Oesterlé and Mestre's method [12] and Kohel's thesis [6]. We compute the trace t of the Frobenius Φ of E using Schoof's algorithm [14]. Let $-\Delta$ be the discriminant of $\mathbb{Z}[\Phi]$ and let $\mathcal{A}$ be the set of prime to $p\Delta$ integers of the form $a+b\Phi$ with $1 \leq b \leq 2\exp((\log \Delta)^{\frac{1}{2}+\epsilon})$ and $|a + \frac{1}{2}bt| \leq \Delta^{\frac{1}{2}}\exp((\log \Delta)^{\frac{1}{2}+\epsilon})$. Let $B = \lfloor \exp(\sqrt{\log \Delta}) \rfloor$. We say that an integer in $\mathbb{Z}[\Phi]$ is B-smooth iff all its prime factors have norm bounded by B. We assume Δ is big enough to apply lemma 2. Otherwise we may just read the result in a table. We pick random elements in $\mathcal{A}$ with uniform probability until we find one $\mathcal{L}$ which is B-smooth. By lemma 2 we succeed after $\ll \exp(2(\log \Delta)^{\frac{1}{2}} \log\log \Delta)$ attempts with bounded probability. This is the only probabilistic step in the algorithm. We now choose any lift E_1 of E and call j_1 its j invariant and compute $\mathcal{L} \bullet E_1$. This is done step by step, applying successively all prime factors of $\mathcal{L}$. So the running time is polynomial in B. We denote by $\mathcal{L} \bullet j_1$ the j-invariant of $\mathcal{L} \bullet E_1$ and set

$$j_{k+1} = j_k - \frac{\mathcal{L} \bullet j_k - j_k}{\sigma - 1}$$

for $k \geq 1$ where $\sigma = \mathcal{L}\mathcal{L}^*$.

If j_∞ is the j-invariant of the canonical lift we check that $|j_{k+1} - j_\infty| \leq |j_k - j_\infty|^2$. This is just the Newton's tangent method. It is decisive however for this convergence property to hold that $\sigma - 1$ be a p-adic unit. It is a unit indeed otherwise we would have $\mathcal{L} \equiv \bar{\mathcal{L}} \pmod{p}$ so $p|b$ since E is ordinary. But this would contradict our assumption that $p > 2\exp((\log \Delta)^{\frac{1}{2}+\epsilon})$. □

Lemma 2. *Fix an ϵ in $]0, \frac{1}{2}[$. Let Φ be an imaginary quadratic integer and t and q two integers such that $\Phi^2 - t\Phi + q = 0$. Let $-\Delta = t^2 - 4q$ be the discriminant of the order generated by Φ. Let $B = \lfloor \exp(\sqrt{\log \Delta}) \rfloor$. Let $\mathcal{A}$ be the set of prime to $q\Delta$ integers of the form $a + b\Phi$ with $1 \leq b \leq 2\exp((\log \Delta)^{\frac{1}{2}+\epsilon})$ and $|a + \frac{1}{2}bt| \leq \Delta^{\frac{1}{2}}\exp((\log \Delta)^{\frac{1}{2}+\epsilon})$. If GRH holds the proportion of B-smooth elements in $\mathcal{A}$ is $\geq \exp(-2(\log \Delta)^{\frac{1}{2}} \log\log \Delta)$ if Δ is big enough (depending on ϵ).*

We now prove lemma 2. Call $\mathcal{D}$ the set of prime to $p\Delta$ primes in $\mathbb{Z}[\Phi]$ with degree one and norm less than B. Let $\mathcal{B} \subset \mathcal{D}$ be a system of coset representatives for the action of complex conjugation on $\mathcal{D}$ i.e. $\mathcal{D} = \mathcal{B} \cup \bar{\mathcal{B}}$ and $\mathcal{B} \cap \bar{\mathcal{B}} = \emptyset$. Let $\mathcal{O} = \mathbb{Z}[\Phi]$ and $h = c\ell(\mathcal{O}) < \Delta^{\frac{1}{2}} \log \Delta$ by a result of Lenstra and Pomerance [10]. From Lagarias and Odlyzko [7] the size π of $\mathcal{B}$ is at least $\frac{B}{3\log B}$ if Δ is big enough. Set $u = \lfloor \frac{\sqrt{\log \Delta}}{2} + (\log \Delta)^{\epsilon} \rfloor$ and let $\mathcal{S}^u\mathcal{B}$ be the u-th symmetric product of $\mathcal{B}$. Let $\kappa : \mathcal{S}^u\mathcal{B} \to \mathcal{C}\ell(\mathcal{O})$ be defined by $\kappa(\{\mathfrak{p}_1, ..., \mathfrak{p}_u\})$ is the class of the product $\prod_{1 \leq k \leq u} \mathfrak{p}_k$. Let $\mathcal{F} \subset \mathcal{S}^u\mathcal{B} \times \mathcal{S}^u\mathcal{B}$ be the subset of couples (V_1, V_2) such that $V_1 \neq V_2$ and $\kappa(V_1) = \kappa(V_2)$. The average size of fibers of κ is $\geq \lfloor \frac{\pi^u}{u!} \rfloor h^{-1} \geq \lfloor \frac{\pi^u}{u!h} \rfloor - 2$ which is bigger than $\exp(\frac{2\log \Delta^{\frac{1}{2}+\epsilon}}{3})$ when Δ is big enough. The size of

$\mathcal{F}$ is minimum when all fibers have equal cardinality so the size of $\mathcal{F}$ is at least $(\lfloor\frac{\pi^u}{u!h}\rfloor-2)(\lfloor\frac{\pi^u}{u!h}\rfloor-3)h \geq \frac{\pi^{2u}}{2h(u!)^2}$ for Δ big enough. To every couple (V_1,V_2) in $\mathcal{F}$ one associates the product of primes in V_1 together with conjugates of primes in V_2. Let $\mu(V_1,V_2)$ be the unique generator of this ideal of the form $a+b\Phi$ with b positive. We observe that this integer exists because the concerned ideal is principal in $\mathcal{O}$. It has norm $(a+\frac{bt}{2})^2+\frac{\Delta}{4}b^2$ bounded by $\Delta\exp(2(\log\Delta)^{\frac{1}{2}+\epsilon})$ and it is not in $\mathbb{Z}$ because $V_1\neq V_2$. So μ is a map from $\mathcal{F}$ to $\mathcal{A}$. The size of a fiber of μ is bounded by $\binom{2u}{u}$.

So the image of μ which is made of B-smooth elements in $\mathcal{A}$ has size at least $\frac{\pi^{2u}}{2(2u)!h}$. The proportion of B-smooth elements in $\mathcal{A}$ is thus

$$\geq \exp(-\frac{3}{2}(\log\Delta)^{\frac{1}{2}}\log\log\Delta+O((\log\Delta)^{\frac{1}{2}}))$$

which is bigger than $\exp(-2(\log\Delta)^{\frac{1}{2}}\log\log\Delta)$ when Δ is big enough. □

Remark 3. The method of Lubin-Serre-Tate used by Satoh and its variants (especially Mestre's ones using Algebraic Geometrical Means that stresses the underlying dynamical system [3]) use degree p isogenies to compute the canonical lift. We avoid them on the contrary. Firstly because p might be too big and secondly because the slope of a level p correspondence at a CM point is not a p-adic unit. This is not necessarily an inconvenient but it requires a different treatment. Indeed the level p correspondence induces a contracting map on the p-adic neigborhood of CM points that Serre uses to prove the existence and unicity of the canonical lift using the fixed point theorem.

4 Singular values of modular functions

Being able to lift an ordinary elliptic curve we may also lift torsion points on it and this gives a p-adic method for computing p-adic approximations of singular values of any modular function $f\in\bar{\mathbb{Q}}(X)$ at a point P with CM by an order $\mathcal{O}$, provide we are given an ordinary elliptic curve with complex multiplication by $\mathcal{O}$.

This gives a stable and efficient method for computing (ray) class fields.

Indeed, given a negative discriminant $-\Delta$ we first look for the smallest prime to Δ square t^2 such that $t^2+\Delta$ is four times a prime $p=q$. We expect the smallest such t to be quite small (e.g. $(\log\Delta)^{O(1)}$) so that $4q$ is very close to Δ. Even GRH cannot ensure this however.

We then look for an elliptic curve over $\mathbb{F}_q$ with trace t. This is done by choosing random elliptic curves modulo q and requires $q/c\ell(-\Delta)$ trials which is less than $q\Delta^{-\frac{1}{2}+o(1)}$ by Siegel's theorem. Any trial takes time $(\log q)^{O(1)}$ using Schoof's algorithm. This is hopefully $O(\Delta^{\frac{1}{2}+o(1)})$. We then lift this curve using the methods presented above. We thus compute p-adic approximations for all conjugates of an element f in the Hilbert class field of the order with discriminant $-\Delta$ and all this in time $hk^{1+o(1)}\Delta^{o(1)}$ where $h=c\ell(-\Delta)$ is the class number of the order with discriminant $-\Delta$.

If we now want to reconstruct the minimal polynomial of f, we need a bound for the logarithm of coefficients of this polynomial. For reasonable functions (e.g. the modular invariant j see [9, 5.10]) this bound is $O(h^{1+\epsilon})$ so we need accuracy $k = O(h^{1+\epsilon})$ so that the algorithm runs in probabilistic expected time $O(h^{2+\epsilon})$ which is essentially linear in the size of the result and certainly better than the tremendous (but somewhat pessimistic) estimate in [1]. Indeed our method avoids the accuracy problems of the classical one (evaluating modular functions at CM points in the upper half plane). It is compatible with the improvement given by Gee and Stevenhagen in [5] where functions $\eta(Nz)/\eta(z)$ are used (that generalize Weber's functions) together with a rationality criterion deduced from Shimura's reciprocity law.

We now can state the

Theorem 3. *If G.R.H. holds, for any positive ϵ there is an algorithm that computes the Hilbert class polynomial of discriminant $-\Delta$ in probabilistic time $O(\Delta^{1+\epsilon})$.*

The algorithm presented above does not quite prove the theorem since there is no proof that a small enough t exists such that $\Delta + t^2$ is four times a prime.

However, G.R.H. ensures that there exists a principal prime ideal in the Hilbert class field with norm less than a constant times

$$h^2(\log h)^4(\log \Delta)^2(\log\log \Delta)^4$$

which is $O(\Delta(\log \Delta)^8(\log\log \Delta)^4)$ by Lenstra an Pomerance [10].

Therefore there exist $t = \sqrt{\Delta}(\log \Delta)^{4+o(1)}$ and $u = (\log \Delta)^{4+o(1)}$ such that $t^2 + u^2\Delta$ is four times a prime p. Such a pair (t, u) may be found by exhaustive search. The rest of the algorithm goes as above except that in the end we obtain an elliptic curve with CM by an order of discriminant $-u\Delta$. Applying isogenies of degree dividing u we obtain en elliptic curve with CM by the order with discriminant $-\Delta$. □

Remark 4. There is a tentative algorithm for computing CM fields in [2]. This method (Algorithm 3 on page 100) collects information modulo many small primes ℓ by exhaustive search among elliptic curves modulo ℓ for every ℓ. It is overexponential in the class number h however, contrary to the author's claim. The definition field of ordinary elliptic curves used in this method has degree $O(h)$ over $\mathbb{F}_\ell$ and the exhaustive search takes time $O(\ell^h)$ rather than the claimed $O(h^2)$. So this algorithm is worse than any possible one.

It may be possible to turn it into something slightly more sensible by removing step 1 an dealing only with primes with supersingular reductions. Even with this restriction, working with several moduli is not a good idea. See section 5.

5 Canonical lift of supersingular curves

In this section we adapt our ideas to the case of curves with supersingular reduction. We keep the notation of section 2. We assume p has a single prime of

$\mathbb{Q}(\sqrt{-\Delta})$ above it. We assume the order $\mathcal{O}$ with discriminant Δ is maximal. In this case the inertia degree d of p in the Hilbert class field is 1 or 2 and $q = p$ or p^2.

Reduction modulo p of curves with CM by $\mathcal{O}$ needs not be injective. However, let $\mathfrak{A}$ be the quaternion algebra ramified at p and ∞ and for every supersingular curve E modulo p let $i_E : \mathfrak{A} \to \mathcal{E}nd(E) \otimes \mathbb{Q}$ be a fixed isomorphism as in Waterhouse [19]. This way, all endomorphism rings of all supersingular curves are seen as maximal orders inside the same algebra $\mathfrak{A}$. We denote by $\mathcal{E}nd(E)$ the endomorphism ring of E over $\bar{\mathbb{F}}_q$.

Reduction of a normalized curve (E, ι) in $\mathcal{NELL}_\Delta(\bar{\mathbb{Q}})$ thus gives a supersingular curve $\bar{E} = E \mod p$ together with an injection of $\mathcal{O}$ in the maximal order $i_{\bar{E}}(\mathcal{E}nd(\bar{E}))$ of $\mathfrak{A}$.

This is an element of $\mathcal{NELL}_\Delta(\bar{\mathbb{F}}_p)$ the set of isomorphism classes of supersingular curves modulo p normalized with the order $\mathcal{O}$ with discriminant $-\Delta$.

We prove the

Theorem 4. *Let $-\Delta$ be a primitive discriminant and $\mathcal{O}$ the quadratic imaginary maximal order with discriminant $-\Delta$ and p an odd inert prime number in $\mathcal{O}$. The reduction map*

$$R : \mathcal{NELL}_\Delta(\bar{\mathbb{Q}}) \to \mathcal{NELL}_\Delta(\bar{\mathbb{F}}_p)$$

is a bijection.

Its inverse will be called the canonical lift on normalized supersingular curves.

We first observe that the two sets have equal cardinality by one of the many Eichler formulae [4, Proposition 5] and [17, Theorem 2.4.].

We also note that $\mathcal{O}$ has a prime to p element $\mathcal{L}$ such that $\mathcal{L}\mathcal{L}^* \not\equiv 1 \bmod p$. This together with theorem 1 and remark 1 implies that R is injective. □

Remark 5. If p ramifies in $\mathcal{O}$ the reduction map is no longer a bijection. It is a two to one surjection. One may define a pair of canonical lifts at p-adic distance $\frac{1}{2}$ of each other.

Remark 6. The theorem above suggests possible generators for the ring of integers of the Hilbert class field.

As for explicit computation of the canonical lift we observe that results and algorithms in section 2 generalize to the case with supersingular reduction.

Let E be a supersingular elliptic curve. Using the graph method of Oesterlé and Mestre we find in probabilistic time $O(p^{1+\epsilon})$ a basis for a sub-order R' of R with index M bounded by $p^{O(1)}$ and the associated quadratic form.

We now assume $\mathcal{O}$ is a maximal imaginary quadratic order where p stays inert and we look for an embedding of $\mathcal{O}$ into R. Since we do not know R we rather look for an embedding in R' of a sub-order $\mathcal{O}'$ of $\mathcal{O}$ with conductor m dividing M.

This boils down to representing $m^2\Delta$ by a positive definite quadratic form of rank three and discriminant $p^{O(1)}$ and is done in time $(p \log \Delta)^{O(1)}\Delta$ by mere exhaustive search and $(p \log \Delta)^{O(1)}$ heuristically by a random search.

This is a competitive approach for computing singular values of modular functions since we can find a very small (e.g. $(\log \Delta)^{O(1)}$ under GRH) inert prime p in $\mathcal{O}$.

The prime p is indeed very small since 3 is fine for half quadratic orders and 5 is fine for half the remaining ones etc. So the endomorphism rings of all supersingular curves modulo small primes can be precomputed together with their norm forms.

References

1. A.O. Atkin and F. Morain. Elliptic curves and primality proving. *Math. Comp.*, 61:29–68, 1993.
2. J. Chao, O. Nakamura, and K. Sobataka. Construction of secure elliptic cryptosystems using CM tests and liftings. *ASIACRYPT'98*, 1514:95–109, 1998.
3. Jean-François Mestre. Lettre à P. Gaudry et R. Harley, décembre 2000. *Private communication.*
4. M. Eichler. The basis problem for modular forms and the traces of the hecke operators. *Lecture Notes in Math.*, 320, 1973.
5. Alice Gee and Peter Stevenhagen. Generating class fields using Shimura reciprocity. *Lecture Notes in Computer Science*, 1423:441–453, 1998.
6. David Kohel. *Endomorphism rings of elliptic curves over finite fields.* Thesis. University of California at Berkeley, 1996.
7. J. Lagarias and A. Odlyzko. Effective versions of the Chebotarev density theorem. In A. Fröhlich, editor, *Algebraic Number Fields.* Academic Press, 1977.
8. Serge Lang. *Elliptic functions, second edition.* GTM. Springer, 1987.
9. H. W. Lenstra and A. Lenstra. Algorithms in number theory. *Handbook of Theoretical Computer Science, Algorithms and Complexity*, A:673–718, 1990.
10. H. W. Lenstra and C. Pomerance. A rigorous time bound for factoring integers. *Journal of the American Mathematical Society*, 5(3):483–516, 1992.
11. J. Lubin, J.-P. Serre, and J. Tate. Elliptic curves and formal groups. *Lecture notes prepared in connection with the seminars held at the Summer Institute on Algebraic Geometry, Whitney Estate, Woods Hole, Massachusetts, July 6-July 31, 1964*, http://www.ma.utexas.edu/users/voloch/lst.html:1–8, 1964.
12. J.-F. Mestre. La méthode des graphes. exemples et applications. *Proceedings of the international conference on class numbers and fundamental units of algebraic number fields (Katata, 1986)*, pages 217–242, 1986.
13. T. Satoh. The canonical lift of an ordinary elliptic curve over a finite field and its point counting. *J. Ramanujan Math. Soc.*, 15:247–270, 2000.
14. R. Schoof. Elliptic curves over finite fields and the computation of square roots modulo p. *Math. Comp.*, 44:183–211, 1985.
15. R. Schoof. Counting points on elliptic curves over finite fields. *Journal de Théorie des Nombres de Bordeaux*, 7:219–254, 1995.
16. J.-P. Serre. Groupes divisibles (d'après John Tate). *Séminaire Bourbaki*, 10(318):73–86, 1966.
17. Thomas R. Shemanske. Ternary quadratic forms and quaternion algebras. *Journal of Number Theory*, 23:203–209, 1986.

18. J. Vélu. Isogénies entre courbes elliptiques. *Comptes rendus à l'Académie des sciences de Paris*, 273, Série A:238–241, 1971.
19. William C. Waterhouse. Abelian varieties over finite fields. *Ann. scient. Ec. Norm. Sup.*, 2(4):521–560, 1969.

Toulouse, 2002, Saturday January the 12^{th}
Revised, 2002, Saturday March the 30^{th}