Computing the Hilbert Class Polynomial Using p-adic Lifting

Juliana V. Belding

Department of Mathematics
Harvard University

S.T.A.G.E. at MIT
May 11, 2009

Outline

Complex Multiplication

- K, a quadratic imaginary field of discriminant $D < 0$.
- $\mathcal{O}_K$, the ring of integers of K
- E, an elliptic curve over $\mathbb{C}$
- $\mathrm{End}(E)$, the ring of endomorphisms $E \longrightarrow E$
- $j(E)$, the j-invariant of E (classifies E up to isomorphism)

Definition

If $\mathrm{End}(E) \simeq \mathcal{O}_K$, then E has *complex multiplication (CM) by* $\mathcal{O}_K$.

Fact

$j(E)$ is an algebraic integer.

The Hilbert class polynomial of K

Goal: Compute the *Hilbert class polynomial of* K, the polynomial $H_K(X) \in \mathbb{Z}[X]$ whose roots are exactly the j-invariants of curves with CM by $\mathcal{O}_K$.

- **Cryptography:** $H_K(X)$ can be used to construct elliptic curves with a prescribed number of points over a finite field.
- **Explicit Class Field Theory:** $H_K(X)$ is a minimal polynomial of the *Hilbert class field of* K, the maximal abelian unramified extension of K.

The Hilbert class field of K

- $I(\mathcal{O}_K)$, the group of ideals of $\mathcal{O}_K$
- $P(\mathcal{O}_K)$, the subgroup of principal ideals.
- $Cl(\mathcal{O}_K) = I(\mathcal{O}_K)/P(\mathcal{O}_K)$ is the *class group of K*
- $h_K = \#Cl(\mathcal{O}_K)$

Definition

The *Hilbert class field $H_{\mathcal{O}_K}$ of K* is the algebraic extension of K with $\mathrm{Gal}(H_{\mathcal{O}_K}/K) \simeq Cl(\mathcal{O}_K)$ via the *Artin map*.

Fact

There is a transitive and free action of $Cl(\mathcal{O}_K)$ on the set of j-invariants of curves with CM by $\mathcal{O}_K$.

Example: $D = -23$

- $\mathcal{O}_K = \mathbb{Z}[\tau]$ where τ is a root of $X^2 - X + 6$
- $Cl(\mathcal{O}_K) = \langle \mathfrak{a} \rangle$ is order 3 where

$$\mathfrak{a} = (3, 1 + 2\tau)$$

and

$$\mathfrak{a}^3 = (1 + 2\tau)$$

The action of $\mathfrak{a}$ gives

$$E_1 = \mathbb{C}/\mathfrak{a}^2 \longrightarrow E_2 = \mathbb{C}/\mathfrak{a} \longrightarrow E_3 = \mathbb{C}/\mathcal{O}_K \longrightarrow \mathbb{C}/\mathfrak{a}^{-1} \simeq E_1$$

The j-invariant of each curve is a root of $H_{-23}(X)$:

$$X^3 + 3491750X^2 - 5151296875X + 12771880859375$$

How “big" is H_K?

- Degree of $H_K(X)$ is $h_K = \tilde{O}(\sqrt{|D|})$
- Coefficients of $H_K(X)$ are integers $\leq C = \tilde{O}(\sqrt{|D|})$ decimal digits.
- So $\tilde{O}(|D|)$ to write down and store $H_K(X)$

General approach: Compute roots j_i to C digits accuracy and expand

$$\prod_{i=1}^{h_K}(X - j_i)$$

Time to expand:

$$O(|D| \log |D|^{3+\epsilon})$$

Complex analytic algorithm

1. View each ideal as a lattice $\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$

$$\mathcal{O}_K = \mathbb{Z} + \tau\mathbb{Z}, \quad \mathfrak{a} = 3\mathbb{Z} + (1+2\tau)\mathbb{Z}, \quad \mathfrak{a}^2 = 9\mathbb{Z} + (4+8\tau)\mathbb{Z}$$

2. Use the function $j(z) : \mathcal{H} \longrightarrow \mathbb{C}$ to compute $j_i = j(\omega_1/\omega_2)$:

$$\begin{aligned} j(\mathcal{O}_K) &= -3493225.6999699... \\ j(\mathfrak{a}) &= 737.84998496668... - 1764.018938612i \\ j(\mathfrak{a}^2) &= 737.84998496668... + 1764.018938612i \end{aligned}$$

to sufficient accuracy.

Complex analytic method, con't.

3. Expand

$$\prod_{i=1}^{h_K}(X - j_i)$$

and recognize coefficients as integers:

$$X^3 + 3491750X^2 - 5151296875X + 12771880859375$$

Complex analytic method, con't.

- Complex Analytic Method (Enge, 2006) has

$$O(|D| \log |D|^{5+\epsilon})$$

  This is deterministic but...
- **Drawback:** Round-off error when multiplying/adding in $\mathbb{C}$
- **Fact:** No round-off error when multiplying or adding p-adic integers...
- Couveignes-Henoqc (2002): Compute roots p-adically.

p-adic Method

1. Compute a single root $\tilde{j}$ of $H_K(X)$ to sufficient accuracy.
2. Compute the action of $Cl(\mathcal{O}_K)$ on $\tilde{j}$:

$$\tilde{j} \mapsto \tilde{j}^{\mathfrak{a}}$$

   to obtain the other roots.
3. Expand

$$\prod_{\mathfrak{a} \in Cl(\mathcal{O}_K)} (X - \tilde{j}^{\mathfrak{a}})$$

   and recognize coefficients as integers.

Q: How to compute $\tilde{j}$?

Complex multiplication in characteristic p

- $\mathfrak{p}$, a prime above p in the field $H_{\mathcal{O}_K}$
- E, a curve with CM by $\mathcal{O}_K$ and good reduction modulo $\mathfrak{p}$
- E_p, the reduction of E

Fact

Reduction modulo $\mathfrak{p}$ induces an embedding

$$f : \mathrm{End}(E) \simeq \mathcal{O}_K \hookrightarrow \mathrm{End}(E_p)$$

The canonical lift of (E_p, f)

- E_p, a curve over $\bar{\mathbb{F}}_p$
- $f : \mathcal{O}_K \hookrightarrow \mathrm{End}(E_p)$, an embedding

Definition

The *canonical lift* of (E_p, f) is the curve $\widetilde{E}$ defined over $H_{\mathcal{O}_K}$ such that

- $E_p \equiv \widetilde{E} \bmod \mathfrak{p}$
- $\mathrm{End}(\widetilde{E}) \hookrightarrow \mathrm{End}(E_p)$ is precisely f.

By the *Deuring Lifting Theorem*, the curve $\widetilde{E}$ exists and is unique up to isomorphism.

Outline of p-adic method (Couv.-Hen.)

- $\widetilde{E}$, the canonical lift of (E_p, f)
- $D_{\tilde{j}}$, open p-adic disc radius one in $\mathbb{C}_p$ centered at $\tilde{j}$

1. Define a ***p*-adic analytic map** with $\tilde{j}$ as a fixed point:
   For $(\alpha) \in Cl(\mathcal{O}_K)$,
   $$\rho_\alpha : D_{\tilde{j}} \longrightarrow D_{\tilde{j}}$$
   depends on the **action of** $Cl(\mathcal{O}_K)$ **on CM points.**
2. Use **Newton's method** to compute the unique root of
   $$\rho_\alpha(X) - X$$
   in $D_{\tilde{j}}$ to sufficient accuracy.

Two cases for p-adic method

Case 1: p splits principally in K

- The smallest such prime p is at least $|D|/4$
- Bröker (2006) Runtime: $O(|D| \log |D|^{6+\epsilon})$ (under GRH)

Case 2: p inert in K

- Smallest such prime p is $< O((\log |D|)^2)$ (under GRH)
- B. (2008) Runtime: ???

Key: Computing action of $Cl(\mathcal{O}_K)$ modulo p and lifting to char 0

Case 1: p splits principally in K

- $H_{\mathcal{O}_K}$ embeds into $\mathbb{Q}_p$
- E_p is *ordinary* and defined over $\mathbb{F}_p$
- $\mathrm{End}(E_p) \simeq \mathcal{O}_K$
- f is an *isomorphism*: $f : \mathrm{End}(E) \xrightarrow{\sim} \mathrm{End}(E_p)$

There is a one-to-one correspondence: (up to $\simeq$ of curves)

$$\begin{array}{ccc} \widetilde{E}/\mathbb{Q}_p & \leftrightarrow & E_p/\mathbb{F}_p \\ \mathrm{End}(\widetilde{E}) \simeq \mathcal{O}_K & & \mathrm{End}(E_p) \simeq \mathcal{O}_K \end{array}$$

Case 2: p is inert in K

- $H_{\mathcal{O}_K}$ embeds into F, the degree 2 unramified extn. of $\mathbb{Q}_p$
- E_p is *supersingular* and defined over $\mathbb{F}_{p^2}$
- $\mathrm{End}(E_p)$ is a *maximal order* in the quaternion algebra $\mathcal{A}_{p,\infty}$
- f is an *embedding*: $f : \mathrm{End}(E) \hookrightarrow \mathrm{End}(E_p)$

There is a one-to-one correspondence:

$$\begin{array}{ccc} \widetilde{E}/F & \leftrightarrow & E_p/\mathbb{F}_{p^2} \\ \mathrm{End}(\widetilde{E}) \simeq \mathcal{O}_K & & f : \mathcal{O}_K \hookrightarrow \mathrm{End}(E_p) \end{array}$$

up to isomorphism of curves and up to conjugation of embeddings by automorphisms.

Example: $p = 7$

- There is a unique class of supersingular curves E_p over $\mathbb{F}_{p^2}$:
$$y^2 = x^3 + x$$
with $j(E_p) = 1728 = 6$.
- $\mathcal{A}_{p,\infty} = \mathbb{Q}[i, j, k]$ with
$$i^2 = -1, j^2 = -7, ij = k, ij = -ji.$$
- $\mathrm{End}(E_p) \simeq \mathbb{Z}[i, (i + k)/2, (1 + j)/2]$
- $\mathrm{Aut}(E_p) \simeq \{\pm 1, \pm i\}$

If p is inert in K, E with CM by $\mathcal{O}_K$ reduces mod p to $\simeq E_p$ and there is an embedding $\mathcal{O}_K \hookrightarrow \mathrm{End}(E_p)$.

Example: $p = 7, D = -23$

- $\mathcal{O}_K = \mathbb{Z}[\tau]$ where τ is a root of $X^2 - X + 6$
- $\mathcal{O}_K$ embeds into $\mathrm{End}(E_p)$ in three ways

$$\begin{aligned} f_1 : \quad \tau &\mapsto \quad 1/2 - 3i/2 + j/2 - k/2 \\ f_2 : \quad \tau &\mapsto \quad 1/2 - 3i/2 + j/2 + k/2 \\ f_3 : \quad \tau &\mapsto \quad 1/2 + 2i - j/2 \end{aligned}$$

  up to conjugation by units of $\mathrm{End}(E_p)$.
- Each pair (E_p, f_i) corresponds uniquely to root of $H_{-23}(X)$:

$$X^3 + 3491750X^2 - 5151296875X + 12771880859375$$

Main difference in the supersingular case, I

In both cases,

- The map ρ_α uses the action of $Cl(\mathcal{O}_K)$ on *pairs*

$$(E_p, f) \mapsto (E_p^{\mathfrak{a}}, f^{\mathfrak{a}})$$

- The subgroup $E_p[\mathfrak{a}] := \bigcap_{\alpha \in \mathfrak{a}} \ker(\alpha)$ defines an *isogeny*

$$\varphi : E_p \longrightarrow E_p / E_p[\mathfrak{a}].$$

- $f^{\mathfrak{a}}(\tau)$ is $\varphi \cdot \tau \cdot \varphi^{-1}$

Main difference in the supersingular case, I

Difficulty: Unwieldy to explicitly compute $f \mapsto f^{\mathfrak{a}}$

Solution: Compute the action in the quaternion algebra $\mathcal{A}_{p,\infty}$

- Determine right-isomorphism of left ideal classes of maximal order $R \simeq \mathrm{End}(E_p)$:
  Eg: $p = 7$

$$R\mathfrak{a} \simeq Rx$$

$$f^{\mathfrak{a}}(\tau) = x \cdot \tau \cdot x^{-1}$$

- “Translate" back to $\mathrm{End}(E_p)$ using basis of small degrees endomorphisms

Main difference in the supersingular case, II

- The curves with $j = 0, 1728$ may be supersingular.
- **Difficulty:** $\tilde{j}$ not sufficient to determine canonical lift of (E_p, f) due to extra automorphisms.
- **Solution:** Use *Legendre form* of an elliptic curve:

$$y^2 = x(x-1)(x-\lambda).$$

The issue for $j = 0, 1728$

- $\tilde{j}$, the j-invariant of the canonical lift of (E_p, f)
- $\widetilde{E}_1$, a canonical lift of (E_p, f)
- $\widetilde{E}_2$, another curve with j-invariant $\tilde{j}$ reducing to E_p

$$\begin{array}{ccc} \widetilde{E}_1 & \xrightarrow{h} & \widetilde{E}_2 \\ \downarrow & & \downarrow \\ (E_p, f) & \xrightarrow{\bar{h}} & (E_p, \bar{h} f \bar{h}^{-1}) \end{array}$$

Note: $\bar{h}$ is an automorphism of E_p.

$j(E_p) = 0$ or 1728

- The automorphism $\bar{h}$ may be non-trivial.
- Then $\bar{h}f\bar{h}^{-1}$ and f are **not** the same embeddings.
- $\widetilde{E}_2$ is **not** a canonical lift of (E_p, f)
- **Upshot:** The j-invariant $\tilde{j}$ not sufficient to determine a canonical lift of (E_p, f).

Note: If $p \not\equiv 1 \bmod 12$, then curves over $\mathbb{F}_{p^2}$ with $j = 0$ and/or 1728 are supersingular.

Example: $p = 7, D = -23$

- $E_p : y^2 = x^3 + x$
- $f : \mathcal{O}_K \hookrightarrow \mathrm{End}(E_p)$

$$\begin{array}{ccc} \widetilde{E}_1 : y^2 = x^3 + Ax + B & \xrightarrow{h} & \widetilde{E}_2 : y^2 = x^3 + Ax - B \\ (x, y) & \mapsto & (-x, iy) \end{array}$$

- Exactly one of $\widetilde{E}_1, \widetilde{E}_2$ is a canonical lift of (E_p, f).
- Determining which one is key to computing action, i.e. ρ_α

Solution: Work with an equation for E which removes the ambiguity of extra automorphisms.

The Legendre form of an elliptic curve

Definition

Let $\mathbb{K}$ be any field not of characteristic two. For $\lambda \in \mathbb{K}$, with $\lambda \neq 0, 1$, the curve

$$L : y^2 = x(x-1)(x-\lambda)$$

is an elliptic curve in *Legendre form*.

- $j(L) = 2^8 \frac{(\lambda^2-\lambda+1)^3}{\lambda^2(\lambda-1)^2}$
- The two-torsion of L is $L[2] = \{(0,0), (1,0), (\lambda, 0), P_\infty\}$

The Legendre form and two-torsion

- E, any curve over $\mathbb{K}$
- (P, Q), an ordered basis of $E[2]$

Let

$$\lambda = \frac{x(P+Q) - x(P)}{x(Q) - x(P)}.$$

There is a unique isomorphism (up to ± 1)

$$E \longrightarrow L : y^2 = x(x-1)(x-\lambda)$$

sending (P, Q) to $(0, 0), (1, 0)$.

The modular function λ

- E, any curve over $\mathbb{K}$
- (P, Q), an ordered basis of $E[2]$

The *moduli space* $Y(2)$ consists of equivalence classes

$$[E, (P, Q)]$$

The modular function λ is

$$\begin{array}{cccc} \lambda : & Y(2) & \longrightarrow & \mathbb{K} \\ & [E, (P, Q)] & \mapsto & \lambda \end{array}$$

where

$$\lambda = \frac{x(P+Q) - x(P)}{x(Q) - x(P)}.$$

The Legendre form

The map $\lambda \mapsto j$ is degree six.

- $N = \#$ distinct curves in Legendre form isomorphic to E
- $A = \#\mathrm{Aut}(E)/\{\pm 1\}$

$j(E)$	N	A	
$\neq 0, 1728$	6	1	
1728	3	2	char $\mathbb{K} \neq 3$
0	2	3	char $\mathbb{K} \neq 3$
0	1	6	char $\mathbb{K} = 3$

For each equivalence class of embeddings $\mathcal{O}_K \hookrightarrow \mathrm{End}(E_p)$, there are $N \cdot A = 6$ distinct pairs (L_p, f) with L_p isomorphic to E and f an embedding into $\mathrm{End}(L_p)$.

Upshot:

There is a one-to-one correspondence:

$$\begin{array}{ccc} \widetilde{L}/F & \leftrightarrow & L_p/\mathbb{F}_{p^2} \\ \mathrm{End}(\widetilde{L}) \simeq \mathcal{O}_K & & f : \mathcal{O}_K \hookrightarrow \mathrm{End}(L_p) \end{array}$$

Definition

The *canonical lift of* (L_p, f) is the curve $\widetilde{L}$ reducing to L_p with induced embedding $f : \mathrm{End}(\widetilde{L}) \hookrightarrow \mathrm{End}(L_p)$.

Note: The curve $\widetilde{L}$ is *unique*.

Idea: Compute canonical lift $\tilde{\lambda}$ of (L_p, f), then compute $\tilde{j}$.

Action of $Cl_2(\mathcal{O}_K)$ on CM curves in Legendre form

- $I_2(\mathcal{O}_K)$, the group of ideals of $\mathcal{O}_K$ prime to (2).
- $P_{2,1}(\mathcal{O}_K)$, principal ideals (α) with $\alpha \equiv 1 \bmod 2\mathcal{O}_K$
- $Cl_2(\mathcal{O}_K) = I_2(\mathcal{O}_K)/P_{2,1}(\mathcal{O}_K)$

Definition

The *ray class field of K of conductor* 2 is the unique abelian extension R with $\mathrm{Gal}(R/K) \simeq Cl_2(\mathcal{O}_K)$ via the Artin map.

The λ-invariant of a curve with CM by $\mathcal{O}_K$

Fact

The λ-invariant of a curve with CM by $\mathcal{O}_K$ generates the ray class field R of conductor 2 over K:

$$R = K(\lambda).$$

Key: Use action of $Cl_2(\mathcal{O}_K)$ on the set of curves in Legendre form with CM by $\mathcal{O}_K$.

Action of $Cl_2(\mathcal{O}_K)$ on CM curves in Legendre form

- $\mathfrak{a}$, an ideal of $\mathcal{O}_K$ prime to (2)
- L, curve over F with $\mathrm{End}(L) \simeq \mathcal{O}_K$

The subgroup

$$L[\mathfrak{a}] := \bigcap_{\alpha \in \mathfrak{a}} \ker(\alpha).$$

defines an *isogeny*

$$L \longrightarrow E = L/L[\mathfrak{a}].$$

Action of $Cl_2(\mathcal{O}_K)$ on CM curves in Legendre form, con't

Define $L^{\mathfrak{a}}$ to be the curve with $\lambda = \lambda([E, (P, Q)])$.

$$\begin{array}{ccccc} L & \xrightarrow{\mathfrak{a}} & E = L/L[\mathfrak{a}] & \xrightarrow{\sim} & L^{\mathfrak{a}} \\ ((0,0),(1,0)) & \mapsto & (P, Q) & \mapsto & ((0,0),(1,0)) \end{array}$$

Note: If $\mathfrak{a} = (\alpha)$ is principal with $\alpha \equiv 1 \bmod 2$, then α is an *endomorphism of L* which *fixes the two-torsion*. Thus

$$L^{\alpha} = L.$$

Action of $Cl_2(\mathcal{O}_K)$ modulo p

Let $\widetilde{L}$ be the canonical lift of (L_p, f).

$$\begin{tikzcd}
\widetilde{L} \arrow[r, "\mathfrak{a}"] \arrow[d] & E = \widetilde{L}/\widetilde{L}[\mathfrak{a}] \arrow[r, "\sim"] \arrow[d] & (\widetilde{L})^{\mathfrak{a}} \arrow[d] \\
(L_p, f) \arrow[r, "\mathfrak{a}"] & E_p = L_p/L_p[f(\mathfrak{a})] \arrow[r, "\sim"] & (L_p^{\mathfrak{a}}, f^{\mathfrak{a}})
\end{tikzcd}$$

- The kernel of the isogeny of L_p is determined by f

$$L_p[f(\mathfrak{a})] := \bigcap_{\alpha \in \mathfrak{a}} \ker f(\alpha).$$

- $(\widetilde{L})^{\mathfrak{a}}$ is the canonical lift of $(L_p^{\mathfrak{a}}, f^{\mathfrak{a}})$.

Lifting the action to non-CM curves

For *any* lift L/F of L_p, the kernel $L_p[f(\mathfrak{a})]$ lifts uniquely

$$\begin{array}{ccc} L & \xleftarrow{\supset} & L[\mathfrak{a}] \\ \uparrow & & \uparrow \\ L_p & \xleftarrow{\supset} & L_p[f(\mathfrak{a})] \end{array}$$

This determines an isogeny

$$\begin{array}{ccccc} L & \xrightarrow{\mathfrak{a}} & E = L/L[\mathfrak{a}] & \xrightarrow{\sim} & L^{\mathfrak{a}} \\ ((0,0),(1,0)) & \mapsto & (P,Q) & \mapsto & ((0,0),(1,0)) \end{array}$$

and we define

$$\rho_{\mathfrak{a}}(\lambda(L)) := \lambda(L^{\mathfrak{a}}).$$

The map ρ_α

If $\mathfrak{a} = (\alpha)$ is in $P_{2,1}(\mathcal{O}_K)$ and $\widetilde{L}$ is a canonical lift of (L_p, f) then $\widetilde{L}[\mathfrak{a}]$ is the kernel of an *endomorphism* of $\widetilde{L}$ fixing $\tilde{L}[2]$:

$$\begin{array}{ccc} \widetilde{L} & \xrightarrow{\alpha} & \widetilde{L}/\widetilde{L}[\alpha] \simeq \widetilde{L} \\ \downarrow & & \downarrow \\ L_p & \xrightarrow{\alpha} & L_p/L_p[\alpha] \simeq L_p \end{array}$$

So

$$\rho_\alpha(\tilde{\lambda}) = \tilde{\lambda}.$$

The map ρ_α

Upshot

Lifting the action of $Cl_2(\mathcal{O}_K)$ in characteristic p defines a map

$$\rho_\alpha : D_{\tilde{\lambda}} \longrightarrow D_{\tilde{\lambda}}$$

where

- $\alpha \in \mathcal{O}_K$ with $\alpha \equiv 1 \bmod 2$ and norm prime to p
- $D_{\tilde{\lambda}}$, open p-adic disc radius one around $\tilde{\lambda}$ ($D_{\tilde{\lambda}} = D_{\lambda_p}$)
- $\tilde{\lambda}$ is a fixed point

The map ρ_α

Theorem

1. *The map ρ_α is p-adic analytic in the disc $D_{\tilde{\lambda}}$. That is, there exist p-adic integers a_i such that*

$$\rho_\alpha(\lambda) - \tilde{\lambda} = \sum_{i \geq 1} a_i (\lambda - \tilde{\lambda})^i,$$

for all $\lambda \in D_{\tilde{\lambda}}$.

2. *The derivative of ρ_α at the point $\lambda = \tilde{\lambda}$ is $\alpha/\bar{\alpha}$.*

So we can use Newton's method...

Newton's method

- Assume $\alpha/\bar{\alpha} - 1$ is a p-adic unit
- Choose $\lambda_0 \in D_{\tilde{\lambda}}$, a one digit approx. to $\tilde{\lambda}$

Let

$$\lambda_{k+1} = \lambda_k - \frac{\rho_\alpha(\lambda_k) - \lambda_k}{\alpha/\bar{\alpha} - 1}.$$

The sequence $\{\lambda_k\}$ converges quadratically to $\tilde{\lambda}$.

Note: λ_{k+1} is a 2^{k+1} digit approximation to $\tilde{\lambda}$.

Algorithm to compute $\tilde{\lambda}$

Input:

- L_p, a supersingular curve defined over $\mathbb{F}_{p^2}$
- $f : \mathcal{O}_K \hookrightarrow \mathrm{End}(L_p)$, an embedding
- r such that 2^r is the desired accuracy for $\tilde{\lambda}$

Output: the 2^r digit approximation to $\tilde{\lambda}$

The j-invariant of the canonical lift of (L_p, f) is

$$\tilde{j} = 2^8 \frac{(\tilde{\lambda}^2 - \tilde{\lambda} + 1)^3}{\tilde{\lambda}^2(\tilde{\lambda} - 1)^2}.$$

to 2^r digits accuracy.

Eg $p = 7, D = -23$

Input:

- $K = \mathbb{Q}(\sqrt{D})$
- $\mathcal{O}_K = \mathbb{Z}[\tau]$ where τ is a root of $X^2 - X + 6$
- L_p is the curve $y^2 = x(x-1)(x-2)$ with $\lambda = 2$
- $f : \mathcal{O}_K \hookrightarrow \mathrm{End}(L_p)$ is $f(\tau) = 1/2 - 3i/2 + j/2 - k/2$

Output: the canonical lift $\tilde{\lambda}$ of (L_p, f) to 8 p-adic digits accuracy.

Step 0: Choosing α

- Choose α in $\mathcal{O}_K$ with
  - $\alpha \equiv 1 \bmod 2\mathcal{O}_K$
  - $\alpha/\bar{\alpha} - 1$ a p-adic unit
  - Norm of α prime to p
- Factor (α) into prime ideals.

For $D = -23$, choose $\alpha = (1 + 2\tau)$ where

$$(\alpha) = \mathfrak{a}^3 \text{ for } \mathfrak{a} = (3, 1 + 2\tau).$$

Step 1: Action of (α) in characteristic p

Compute the action of (α) factor by factor in characteristic p:

$$\begin{array}{ccccccc} L_p & \xrightarrow{\mathfrak{a}} & L_p^{\mathfrak{a}} & \xrightarrow{\mathfrak{a}} & L_p^{\mathfrak{a}^2} & \xrightarrow{\mathfrak{a}} & L_p^{(\alpha)} = L_p \\ f & & f^{\mathfrak{a}} & & f^{\mathfrak{a}^2} & & f^{\alpha} = f \end{array}$$

We must compute the action on the embeddings as well.
This gives a sequence of subgroups

$$L_p[f(\mathfrak{a})], \qquad L_p^{\mathfrak{a}}[f^{\mathfrak{a}}(\mathfrak{a})], \qquad L_p^{\mathfrak{a}^2}[f^{\mathfrak{a}^2}(\mathfrak{a})]$$

which we lift to characteristic zero to compute ρ_α.

Eg $p = 7, D = -23$: Action in characteristic p

Compute the action of α factor by factor:

$$\begin{array}{ccccccc} L_p & \xrightarrow{\mathfrak{a}} & L_p^{\mathfrak{a}} & \xrightarrow{\mathfrak{a}} & L_p^{\mathfrak{a}^2} & \xrightarrow{\mathfrak{a}} & L_p^{(\alpha)} = L_p \\ f & & f^{\mathfrak{a}} & & f^{\mathfrak{a}^2} & & f^{\alpha} = f \end{array}$$

- $L_p^{\mathfrak{a}}$ has $\lambda = 6$, $f^{\mathfrak{a}}(\tau) = 1/2 - 3i/2 + j/2 + k/2$
- $L_p^{\mathfrak{a}^2}$ has $\lambda = 4$, $f^{\mathfrak{a}^2}(\tau) = 1/2 + 2i - j/2$

The kernels are given by the 3-torsion points with

$$x = 5a + 5, \quad x = 5a + 3, \quad x = a + 5.$$

where $a^2 = -2$ in $\mathbb{F}_{p^2}$.

Step 2: Lifting the action to curves over F

- Given λ_k, a 2^k digit approximation to $\tilde{\lambda}$, let

$$L_k : y^2 = x(x-1)(x-\lambda_k).$$

- Lift the action of α

$$L_k \xrightarrow{\mathfrak{a}} L_k^{\mathfrak{a}} \xrightarrow{\mathfrak{a}} L_k^{\mathfrak{a}^2} \xrightarrow{\mathfrak{a}} L_k^{(\alpha)}$$

  to get $\rho_\alpha(\lambda_k) = \lambda(L_k^{(\alpha)})$.

- Compute

$$\lambda_{k+1} = \lambda_k - \frac{\rho_\alpha(\lambda_k) - \lambda_k}{\alpha/\bar{\alpha} - 1}.$$

  This is $\tilde{\lambda}$ to 2^{k+1} p-adic digits accuracy.

Eg $p = 7, D = -23$: Lifting action to compute ρ_α

- Choose $\lambda_0 = 9$ in $D_{\tilde{\lambda}}$ and let L_0 be the curve

$$y^2 = x(x-1)(x-9).$$

- Lift the kernels one-by-one to get

$$L_0 \xrightarrow{\mathfrak{a}} L_0^{\mathfrak{a}} \xrightarrow{\mathfrak{a}} L_0^{\mathfrak{a}^2} \xrightarrow{\mathfrak{a}} L_0^{(\alpha)}$$

- Compute

$$\rho_\alpha(\lambda_0) = \lambda(L_0^{(\alpha)}) = -19 + O(7^2).$$

- Use Newton's Method to get

$$\lambda_1 = -14\tilde{a} - 5 + O(7^2)$$

Eg $p = 7, D = -23$: Newton's method

Let $F = \mathbb{Q}_p(\tilde{a})$ where $\tilde{a}$ is the lift of a.

k	λ_k	$\rho_\alpha(\lambda_k)$
0	$9 + O(7^2)$	$-19 + O(7^2)$
1	$-14\tilde{a} - 5 + O(7^2)$	$-700\tilde{a} - 250 + O(7^4)$
2	$-308\tilde{a} + 975 + O(7^4)$	$-2759057\tilde{a} - 2169529 + O(7^8)$

We get 8 digit p-adic approximations to $\tilde{\lambda}$ and $\tilde{j}$ resp.:

$$\lambda_3 = -1589770\tilde{a} + 2769328 + O(7^8)$$

$$j(\lambda_3) = -1520666\tilde{a} + 1286263 + O(7^8)$$

Algorithm to compute $H_K(X)$

1. Choose smallest inert prime p in K.
2. Choose a curve L_p such that $\mathcal{O}_K \hookrightarrow \mathrm{End}(L_p)$ via some f.
3. Compute the λ-invariant $\tilde{\lambda}$ of the canonical lift of (L_p, f) to sufficient accuracy using Algorithm 1.
4. For each $\mathfrak{a} \in Cl(\mathcal{O}_K)$, compute the action on $\tilde{\lambda}$ using $\rho_{\mathfrak{a}}$:

$$\tilde{\lambda} \mapsto \tilde{\lambda}^{\mathfrak{a}}$$

5. Use j function to obtain the roots $\tilde{j}^{\mathfrak{a}}$.
6. Expand

$$\prod_{\mathfrak{a} \in Cl(\mathcal{O}_K)} (X - \tilde{j}^{\mathfrak{a}})$$

and recognize coefficients as integers.

Algorithm to compute $H_K(X)$

Key computational steps to analyze/improve:

- Matching $\mathrm{End}(E_p)$ with maximal order R (Cervino, $O(p^{5/2})$)
- Computing an embedding $\mathcal{O}_K \hookrightarrow R$ (norm $O(|D|)$)
- Computing $f \mapsto f^{\mathfrak{a}}$ (ideal class isomorphisms in R)
- Given $f(\mathfrak{a})$, computing kernel polynomial (naive search)
- Hensel lift of kernel polynomial to $\mathbb{Q}_{p^2}[X]$ to precision 2^k

An algorithm to compute $H_K(X)$ mod p for p inert in K

- The action
$$f \mapsto f^{\mathfrak{a}}$$
moves between different *maximal orders* of $\mathcal{A}_{p,\infty}$.
- Match each maximal order of $\mathcal{A}_{p,\infty}$ with a class of supersingular elliptic curves over $\mathbb{F}_{p^2}$.
- $\#$ embeddings into an order $=$ multiplicity of the j-invariant
- This gives
$$H_D(X) \bmod p.$$

Used in the Chinese Remainder Theorem algorithm to compute $H_D(X)$

Current State of Methods

- Complex Analytic Method (Enge, 2006)
- Ordinary p-adic Method (Bröker, 2006)
- Inert p-adic Method (B. 2008, Riboulet, 2004, $p = 2$)
- Chinese Remainder Theorem Method (BBEL, 2008)
- Improved CRT Method (Sutherland, 2009)

Comparison of Methods (under GRH)

- CAM (assuming no round-off error)

$$O(|D| \log |D|^3 \log\log |D|^3)$$

- Ordinary p-adic Method (2008)

$$O(|D| \log |D|^{6+\epsilon})$$

- Inert p-adic Method (2008)

$$O(|D| \log |D|^{???})$$

- Chinese Remainder Theorem Method (2008)

$$O(|D| \log |D|^{7+\epsilon})$$

- Improved CRT Method (2009)

$$O(|D| \log |D|^5 \log\log |D|^4)$$

Thank you to...

- STAGE at MIT
- Dr. Larry Washington and Dr. Reinier Bröker