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

The class polynomial $H_K$ of a quadratic imaginary field
Definitions and Notation
Computing $H_K(X)$

$p$-adic method for computing $H_K$
The Canonical Lift
The Supersingular Case: $p$ inert in $K$

A $p$-adic algorithm to compute the canonical lift for $p$ inert in $K$
The case of $j = 0, 1728$
The Legendre form of an elliptic curve
The $p$-adic analytic map $\rho_\alpha$
Example of algorithm, $p = 7, D = -23$

Algorithms to compute $H_K(X)$
$p$-adic algorithm for $p$ inert in $K$
Comparison of Algorithms
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 $\mathbb{C}$
- $\text{End}(E)$, the ring of endomorphisms $E \to E$
- $j(E)$, the $j$-invariant of $E$ (classifies $E$ up to isomorphism)

**Definition**

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

**Fact**

$j(E)$ is an algebraic integer.
The class polynomial \( H_K \) of a quadratic imaginary field

\( p \)-adic method for computing \( H_K \)

A \( p \)-adic algorithm to compute the canonical lift for \( p \) inert in \( K \)

Algorithms to compute \( H_K(X) \)

### Definitions and Notation

### Computing \( H_K(X) \)

#### Algorithms to compute \( H_K(X) \)

#### Definitions and Notation

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

**Definition**

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

**Fact**

*There is a transitive and free action of $\text{Cl}(\mathcal{O}_K)$ on the set of $j$-invariants of curves with CM by $\mathcal{O}_K$.***
Example: $D = -23$

- $\mathcal{O}_K = \mathbb{Z}[\tau]$ where $\tau$ is a root of $X^2 - X + 6$
- $\text{Cl}(\mathcal{O}_K) = \langle a \rangle$ is order 3 where
  \[ a = (3, 1 + 2\tau) \]

and

\[ a^3 = (1 + 2\tau) \]

The action of $a$ gives

\[ E_1 = \mathbb{C}/a^2 \longrightarrow E_2 = \mathbb{C}/a \longrightarrow E_3 = \mathbb{C}/\mathcal{O}_K \longrightarrow \mathbb{C}/a^{-1} \approx E_1 \]

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

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

Time to expand:

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

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

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

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

\[
\begin{align*}
  j(\mathcal{O}_K) &= -3493225.6999699... \\
  j(a) &= 737.84998496668... - 1764.018938612i \\
  j(a^2) &= 737.84998496668... + 1764.018938612i 
\end{align*}
\]

...to sufficient accuracy.
Complex analytic method, con’t.

3. Expand

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

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-Henocq (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 $\text{Cl}(\mathcal{O}_K)$ on $\tilde{j}$:

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

to obtain the other roots.
3. Expand

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

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 $\mathfrak{p}$
- $E_\mathfrak{p}$, the reduction of $E$

**Fact**

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

$$f : \text{End}(E) \simeq \mathcal{O}_K \hookrightarrow \text{End}(E_\mathfrak{p})$$
The class polynomial $H_K$ of a quadratic imaginary field
$p$-adic method for computing $H_K$
A $p$-adic algorithm to compute the canonical lift for $p$ inert in $K$
Algorithms to compute $H_K(X)$

The Canonical Lift
The Supersingular Case: $p$ inert in $K$

The canonical lift of $(E_p, f)$

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

**Definition**
The *canonical lift* of $(E_p, f)$ is the curve $\tilde{E}$ defined over $H_{\mathcal{O}_K}$ such that
- $E_p \equiv \tilde{E} \mod p$
- $\text{End}(\tilde{E}) \hookrightarrow \text{End}(E_p)$ is precisely $f$.

By the *Deuring Lifting Theorem*, the curve $\tilde{E}$ exists and is unique up to isomorphism.
Outline of $p$-adic method (Couv.-Hen.)

- $\tilde{E}$, the canonical lift of $(E_p, f)$
- $D_j$, 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 $(\alpha) \in Cl(\mathcal{O}_K)$,
   \[\rho_\alpha : D_{\tilde{j}} \rightarrow D_{\tilde{j}}\]
   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 $D_j$ 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)

**Key:** Computing action of $Cl(\mathcal{O}_K)$ modulo $p$ and lifting to char 0
Case 1: $p$ splits principally in $K$

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

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

\[
\tilde{E}/\mathbb{Q}_p \leftrightarrow E_p/\mathbb{F}_p \\
\text{End}(\tilde{E}) \simeq O_K \quad \text{End}(E_p) \simeq O_K
\]
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 $\mathbb{F}_p^2$
- $\text{End}(E_p)$ is a maximal order in the quaternion algebra $\mathcal{A}_{p,\infty}$
- $f$ is an embedding: $f : \text{End}(E) \hookrightarrow \text{End}(E_p)$

There is a one-to-one correspondence:

\[
\begin{align*}
\tilde{E}/F & \leftrightarrow E_p/\mathbb{F}_p^2 \\
\text{End}(\tilde{E}) & \simeq \mathcal{O}_K \\
f : \mathcal{O}_K & \hookrightarrow \text{End}(E_p)
\end{align*}
\]

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 $j(E_p) = 1728 = 6$.

- $A_{p, \infty} = \mathbb{Q}[i, j, k]$ with
  \[
i^2 = -1, j^2 = -7, ij = k, ij = -ji.
  \]

- $\text{End}(E_p) \cong \mathbb{Z}[i, (i + k)/2, (1 + j)/2]$

- $\text{Aut}(E_p) \cong \{ \pm 1, \pm i \}$

If $p$ is inert in $K$, $E$ with CM by $\mathcal{O}_K$ reduces mod $p$ to $\cong E_p$ and there is an embedding $\mathcal{O}_K \hookrightarrow \text{End}(E_p)$. 
Example: $p = 7, D = -23$

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

\[
\begin{align*}
f_1 : \quad \tau & \mapsto 1/2 - 3i/2 + j/2 - k/2 \\
f_2 : \quad \tau & \mapsto 1/2 - 3i/2 + j/2 + k/2 \\
f_3 : \quad \tau & \mapsto 1/2 + 2i - j/2
\end{align*}
\]

up to conjugation by units of $\text{End}(E_p)$.

- 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 $\rho_\alpha$ uses the action of $Cl(\mathcal{O}_K)$ on pairs

  $$(E_p, f) \mapsto (E_p^\alpha, f^\alpha)$$

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

  $\varphi : E_p \longrightarrow E_p/E_p[a]$. 

- $f^\alpha(\tau)$ is $\varphi \cdot \tau \cdot \varphi^{-1}$
Main difference in the supersingular case, I

**Difficulty:** Unwieldy to explicitly compute $f \mapsto f^a$

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

- Determine right-isomorphism of left ideal classes of maximal order $R \simeq \text{End}(E_p)$:

  **Eg:** $p = 7$

  \[
  R^a \simeq Rx
  \]

  \[
  f^a(\tau) = x \cdot \tau \cdot x^{-1}
  \]

- “Translate" back to $\text{End}(E_p)$ 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 \((E_p, f)\)
- \( \tilde{E}_1 \), a canonical lift of \((E_p, f)\)
- \( \tilde{E}_2 \), another curve with \( j \)-invariant \( \tilde{j} \) reducing to \( E_p \)

\[
\begin{array}{ccc}
\tilde{E}_1 & \xrightarrow{h} & \tilde{E}_2 \\
\downarrow & & \downarrow \\
(E_p, f) & \xrightarrow{\tilde{h}} & (E_p, \tilde{h}f\tilde{h}^{-1})
\end{array}
\]

**Note:** \( \tilde{h} \) is an automorphism of \( E_p \).
The class polynomial $H_K$ of a quadratic imaginary field
$p$-adic method for computing $H_K$
A $p$-adic algorithm to compute the canonical lift for $p$ inert in $K$
Algorithms to compute $H_K(X)$

The case of $j = 0, 1728$
The Legendre form of an elliptic curve
The $p$-adic analytic map $ρ_α$
Example of algorithm, $p = 7, D = −23$

$j(E_p) = 0$ or $1728$

- The automorphism $\bar{h}$ may be non-trivial.
- Then $\bar{h}f\bar{h}^{-1}$ and $f$ are not the same embeddings.
- $\tilde{E}_2$ 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 $p \not\equiv 1 \mod 12$, then curves over $\mathbb{F}_p^2$ with $j = 0$ and/or $1728$ are supersingular.
Example: $p = 7, D = -23$

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

\[ \tilde{E}_1 : y^2 = x^3 + Ax + B \]  \[ \tilde{E}_2 : y^2 = x^3 + Ax - B \]

($x, y$)  $\mapsto$  $(-x, iy)$

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

**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 $\pm 1$)

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

sending $(P, Q)$ to $(0, 0), (1, 0)$. 
The modular function $\lambda$

- $E$, 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 $\lambda$ is

$$\lambda : Y(2) \longrightarrow \mathbb{K}$$

$$[E, (P, Q)] \mapsto \lambda$$

where

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

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

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

<table>
<thead>
<tr>
<th>$j(E)$</th>
<th>$N$</th>
<th>$A$</th>
<th>char $K$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\neq 0, 1728$</td>
<td>6</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>1728</td>
<td>3</td>
<td>2</td>
<td>$K \neq 3$</td>
</tr>
<tr>
<td>0</td>
<td>2</td>
<td>3</td>
<td>$K \neq 3$</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>6</td>
<td>$K = 3$</td>
</tr>
</tbody>
</table>

For each equivalence class of embeddings $\mathcal{O}_K \hookrightarrow \text{End}(E_p)$, there are $N \cdot A = 6$ distinct pairs $(L_p, f)$ with $L_p$ isomorphic to $E$ and $f$ an embedding into $\text{End}(L_p)$. 
The class polynomial $H_K$ of a quadratic imaginary field $p$-adic method for computing $H_K$
A $p$-adic algorithm to compute the canonical lift for $p$ inert in $K$
Algorithms to compute $H_K(X)$

The case of $j = 0, 1728$
The Legendre form of an elliptic curve
The $p$-adic analytic map $\rho_\alpha$
Example of algorithm, $p = 7, D = -23$

Upshot:

There is a one-to-one correspondence:

\[
\tilde{L}/F \leftrightarrow L_p/F_p^2
\]

End($\tilde{L}$) $\simeq \mathcal{O}_K$

$f : \mathcal{O}_K \hookrightarrow \text{End}(L_p)$

Definition

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

Note: The curve $\tilde{L}$ is \textit{unique}.

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

Action of $\text{Cl}_2(\mathcal{O}_K)$ on CM curves in Legendre form

- $l_2(\mathcal{O}_K)$, the group of ideals of $\mathcal{O}_K$ prime to (2).
- $P_{2,1}(\mathcal{O}_K)$, principal ideals $(\alpha)$ with $\alpha \equiv 1 \mod 2\mathcal{O}_K$
- $\text{Cl}_2(\mathcal{O}_K) = l_2(\mathcal{O}_K)/P_{2,1}(\mathcal{O}_K)$

**Definition**

The *ray class field of $K$ of conductor 2* is the unique abelian extension $R$ with $\text{Gal}(R/K) \cong \text{Cl}_2(\mathcal{O}_K)$ via the Artin map.
The $\lambda$-invariant of a curve with CM by $\mathcal{O}_K$

Fact

The $\lambda$-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 $\mathcal{O}_K$. 

The case of $j = 0, 1728$

The Legendre form of an elliptic curve

The $p$-adic analytic map $\rho_\alpha$

Example of algorithm, $p = 7, D = -23$
Action of $Cl_2(O_K)$ on CM curves in Legendre form

- $\alpha$, an ideal of $O_K$ prime to $(2)$
- $L$, curve over $F$ with $\text{End}(L) \simeq O_K$

The subgroup

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

defines an isogeny

$$L \longrightarrow E = L/L[\alpha].$$
Action of $\text{Cl}_2(\mathcal{O}_K)$ on CM curves in Legendre form, con’t

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

\[
\begin{align*}
L & \xrightarrow{\alpha} E = L/L[\alpha] \xrightarrow{\sim} L^\alpha \\
((0, 0), (1, 0)) & \mapsto (P, Q) \mapsto ((0, 0), (1, 0))
\end{align*}
\]

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

\[L^\alpha = L.\]
**Action of $\text{Cl}_2(\mathcal{O}_K)$ modulo $p$**

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

$$
\begin{array}{cccc}
\sim & \quad \sim \\
\downarrow & \quad \downarrow & \quad \downarrow \\
(L_p, f) & E_p = L_p/L_p[f(\alpha)] & (\tilde{L})^a & (L_p^a, f^a)
\end{array}
$$

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

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

- $(\tilde{L})^a$ is the canonical lift of $(L_p^a, f^a)$. 
Lifting the action to non-CM curves

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

$$L \leftarrow \circlearrowright \ L[a]$$

$$L_p \leftarrow \circlearrowright \ L_p[f(a)]$$

This determines an isogeny

$$L \xrightarrow{\alpha} E = L/L[a] \xrightarrow{\sim} L^a$$

and we define

$$\rho_a(\lambda(L)) := \lambda(L^a).$$
The map $\rho_\alpha$

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

$$
\begin{array}{c}
\tilde{L} \\
\downarrow \\
L_p
\end{array} \xrightarrow{\alpha} \begin{array}{c}
\tilde{L}/\tilde{L}[\alpha] \\
\downarrow \\
L_p/L_p[\alpha]
\end{array} \simeq \begin{array}{c}
\tilde{L} \\
L_p
\end{array}
$$

So

$$\rho_\alpha(\tilde{\lambda}) = \tilde{\lambda}.$$
The class polynomial $H_K$ of a quadratic imaginary field
$p$-adic method for computing $H_K$
A $p$-adic algorithm to compute the canonical lift for $p$ inert in $K$
Algorithms to compute $H_K(X)$

The case of $j = 0, 1728$
The Legendre form of an elliptic curve
The $p$-adic analytic map $\rho_\alpha$
Example of algorithm, $p = 7, D = -23$

The map $\rho_\alpha$

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 $\alpha \equiv 1 \mod 2$ 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 $\rho_{\alpha}$

**Theorem**

1. The map $\rho_{\alpha}$ 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 $\rho_{\alpha}$ 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:** $\lambda_{k+1}$ is a $2^{k+1}$ digit approximation to $\tilde{\lambda}$.  

The class polynomial $H_K$ of a quadratic imaginary field

A $p$-adic method for computing $H_K$

A $p$-adic algorithm to compute the canonical lift for $p$ inert in $K$

Algorithms to compute $H_K(X)$

The case of $j = 0, 1728$

The Legendre form of an elliptic curve

The $p$-adic analytic map $\rho_\alpha$

Example of algorithm, $p = 7, D = -23$
Algorithm to compute $\tilde{\lambda}$

**Input:**
- $L_p$, a supersingular curve defined over $\mathbb{F}_p^2$
- $f : \mathcal{O}_K \hookrightarrow \text{End}(L_p)$, 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 $\tau$ is a root of $X^2 - X + 6$
- $L_p$ is the curve $y^2 = x(x - 1)(x - 2)$ with $\lambda = 2$
- $f : \mathcal{O}_K \hookrightarrow \text{End}(L_p)$ 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 $\alpha$

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

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

$$(\alpha) = a^3 \text{ for } a = (3, 1 + 2\tau).$$
Step 1: Action of \((\alpha)\) in characteristic \(p\)

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

\[
\begin{align*}
L_p & \xrightarrow{\alpha} L_p^a & L_p^{a^2} & \xrightarrow{\alpha} L_p^{(\alpha)} = L_p \\
 f & \xrightarrow{\alpha} f^a & f^{a^2} & \xrightarrow{\alpha} f^\alpha = f
\end{align*}
\]

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

\[
L_p[f(\alpha)], \quad L_p^a[f^a(\alpha)], \quad L_p^{a^2}[f^{a^2}(\alpha)]
\]

which we lift to characteristic zero to compute \(\rho_\alpha\).
**Eg \( p = 7, D = -23 \): Action in characteristic \( p \)**

Compute the action of \( \alpha \) factor by factor:

\[
L_p \xrightarrow{a} L_p^{a} \xrightarrow{a} L_p^{a^2} \xrightarrow{a} L_p^{(\alpha)} = L_p
\]

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

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 $\lambda_k$, a $2^k$ digit approximation to $\tilde{\lambda}$, let
  
  $$L_k : y^2 = x(x - 1)(x - \lambda_k).$$

- Lift the action of $\alpha$

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

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

- Compute

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

  This is $\tilde{\lambda}$ to $2^{k+1}$ $p$-adic digits accuracy.
Eg \( p = 7, D = -23 \): Lifting action to compute \( \rho_\alpha \)

- Choose \( \lambda_0 = 9 \) in \( D_\lambda \) and let \( L_0 \) be the curve
  \[
y^2 = x(x - 1)(x - 9).
  \]

- Lift the kernels one-by-one to get
  \[
  L_0 \xrightarrow{a} L_0^a \xrightarrow{a} L_0^{a^2} \xrightarrow{a} L_0^{(\alpha)}
  \]

- 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 $a$.

<table>
<thead>
<tr>
<th>$k$</th>
<th>$\lambda_k$</th>
<th>$\rho_\alpha(\lambda_k)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>$9 + O(7^2)$</td>
<td>$-19 + O(7^2)$</td>
</tr>
<tr>
<td>1</td>
<td>$-14\tilde{a} - 5 + O(7^2)$</td>
<td>$-700\tilde{a} - 250 + O(7^4)$</td>
</tr>
<tr>
<td>2</td>
<td>$-308\tilde{a} + 975 + O(7^4)$</td>
<td>$-2759057\tilde{a} - 2169529 + O(7^8)$</td>
</tr>
</tbody>
</table>

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 $H_K(X)$

2. Choose a curve $L_p$ such that $\mathcal{O}_K \hookrightarrow \text{End}(L_p)$ via some $f$.
3. Compute the $\lambda$-invariant $\tilde{\lambda}$ of the canonical lift of $(L_p, f)$ to sufficient accuracy using Algorithm 1.
4. For each $\alpha \in \text{Cl}(\mathcal{O}_K)$, compute the action on $\tilde{\lambda}$ using $\rho_\alpha$:
   \[
   \tilde{\lambda} \mapsto \tilde{\lambda}^\alpha
   \]
5. Use $j$ function to obtain the roots $\tilde{j}^\alpha$.
6. Expand
   \[
   \prod_{\alpha \in \text{Cl}(\mathcal{O}_K)} (X - \tilde{j}^\alpha)
   \]
   and recognize coefficients as integers.
Algorithm to compute $H_K(X)$

Key computational steps to analyze/improve:

- Matching $\text{End}(E_p)$ with maximal order $R$ (Cervino, $O(p^{5/2})$)
- Computing an embedding $\mathcal{O}_K \hookrightarrow R$ (norm $O(|D|)$)
- Computing $f \mapsto f^a$ (ideal class isomorphisms in $R$)
- Given $f(a)$, 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 $f \mapsto f^a$
  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

$$H_D(X) \mod p.$$  

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)
- 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)
  \[ O(|D| \log |D|^{??}) \]

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

- Improved CRT Method (2009)
  \[ O(|D| \log |D|^{5+\epsilon}) \]
The class polynomial $H_K$ of a quadratic imaginary field

$p$-adic method for computing $H_K$

A $p$-adic algorithm to compute the canonical lift for $p$ inert in $K$

Algorithms to compute $H_K(X)$

$p$-adic algorithm for $p$ inert in $K$

Comparison of Algorithms

Thank you to...

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