Computing Igusa Class Polynomials

Marco Streng

Universiteit Leiden

Explicit Methods in Number Theory
Oberwolfach, July 2009
The Hilbert class polynomial

Definition

The Hilbert class polynomial $H_K$ of an imaginary quadratic number field $K$ is

$$H_K = \prod \left( X - j(E) \right) \in \mathbb{Z}[X].$$

\{E/C : \text{End}(E) \cong \mathcal{O}_K \}

Applications:

1. $K[X]/H_K = \text{Hilbert class field of } K$
2. Elliptic curves over $\mathbb{F}_p$:
The Hilbert class polynomial

Definition

The Hilbert class polynomial $H_K$ of an imaginary quadratic number field $K$ is

$$H_K = \prod_{\{E/C : \text{End}(E) \cong \mathcal{O}_K\}} (X - j(E)) \in \mathbb{Z}[X].$$

Applications:

1. $K[X]/H_K = \text{Hilbert class field of } K$

2. Elliptic curves over $\mathbb{F}_p$: if $\pi \in \mathcal{O}_K, \pi \bar{\pi} = p$, then

   $(H_K \mod p)$ is a product of linear factors and

   for any root $j_0 \in \mathbb{F}_p$, exists $E$ with $j(E) = j_0$ and

   $$\#E(\mathbb{F}_p) = p + 1 - \text{tr}(\pi)$$
1. Bijection

\[ \text{Cl}_K \leftrightarrow \{ E/\mathbb{C} \text{ with CM by } \mathcal{O}_K \}/ \cong \]

\[ [a] \mapsto \mathbb{C}/a, \]

\[ \alpha = z \mathbb{Z} + \mathbb{Z} \text{ with } z \text{ in fund. domain:} \]

\[ \text{Im} z > 0, |\text{Re} z| \leq \frac{1}{2}, |z| \geq 1 \]
Algorithm (sketch)

1. Bijection

\[ \text{Cl}_K \leftrightarrow \{ E/\mathbb{C} \text{ with CM by } \mathcal{O}_K \}/ \cong \]

\[ [a] \mapsto \mathbb{C}/a, \]

\[ a = z\mathbb{Z} + \mathbb{Z} \text{ with } z \text{ in fund. domain:} \]

\[ \text{Im} z > 0, |\text{Re} z| \leq \frac{1}{2}, |z| \geq 1 \]

2. \( j(a) = q^{-1} + 744 + 196884q + 21493760q^2 + \cdots \) \((q = e^{2\pi i z})\)

(or smarter approximation)

3. Compute \( H_K = \prod_z (X - j(z)) \in \mathbb{Z}[X] \)
The Hilbert class polynomial is huge: the degree $h_K$ grows like $|D|^{1/2}$, as do the logarithms of the coefficients.

Three algorithms:

- Complex analytic method,
- $p$-adic, [Couveignes-Henocq 2002, Bröker 2006]
- Chinese remainder theorem. [CNST 1998, ALV 2004]
The Hilbert class polynomial is huge: the degree \( h_K \) grows like \( |D|^{1/2} \), as do the logarithms of the coefficients.

Three algorithms:
- Complex analytic method,
- \( p \)-adic, [Couveignes-Henocq 2002, Bröker 2006]
- Chinese remainder theorem. [CNST 1998, ALV 2004]

Under GRH or heuristics, all \( O(|D|^{1+\epsilon}) \).

[BBEL 2008, Sutherland 2009] turned CRT (the underdog) into the record holder: \(-D > 4 \cdot 10^{12}, h_K = 5,000,000\).
Complex multiplication

- An elliptic curve has CM if $\text{End}(E) \cong \mathcal{O}_K$ with $K$ imaginary quadratic.
- A curve of genus 2 has CM if $\text{End}(J(C)) \cong \mathcal{O}_K$ with $K$ a CM field of degree 4.
Complex multiplication

- An elliptic curve has CM if $\text{End}(E) \cong \mathcal{O}_K$ with $K$ imaginary quadratic.
- A curve of genus 2 has CM if $\text{End}(J(C)) \cong \mathcal{O}_K$ with $K$ a CM field of degree 4.
- A CM field is $K_0(\sqrt{r})$ with $K_0$ totally real and $r \in K_0$, $r \ll 0$.
- $K$ is primitive if it does not contain an imaginary quadratic subfield.
Igusa invariants

For

\[ C : y^2 = f(x) = a_6 \prod_{i=1}^{6} (x - \alpha_i), \]

let \((ij) = (\alpha_i - \alpha_j)\) and

\[
I_2 = a_6^2 \sum_{15} (12)^2 (34)^2 (56)^2,
\]

\[
I_4 = a_6^4 \sum_{10} (12)^2 (23)^2 (31)^2 (45)^2 (56)^2 (64)^2,
\]

\[
I_6 = a_6^6 \sum_{60} (12)^2 (23)^2 (31)^2 (45)^2 (56)^2 (64)^2 (14)^2 (25)^2 (36)^2,
\]

\[
I_{10} = a_6^{10} \prod_{i<j} (ij)^2 = \text{discr.}(f) \neq 0.
\]

Bijection between set of genus-2 curves and points in a weighted projective 3-space.
Igusa class polynomials

Simplification: $i_1 = \frac{l_2^5}{l_{10}}$, $i_2 = \frac{l_2^3 l_4}{l_{10}}$ and $i_3 = \frac{l_2^2 l_6}{l_{10}}$.

Definition

The Igusa class polynomials of a primitive quartic CM field $K$ are the polynomials

$$H_{K,n}(X) = \prod_{\{C/C : \text{End}(J(C)) \cong \mathcal{O}_K\} / \cong} (X - i_n(C)) \in \mathbb{Q}[X], \quad n \in \{1, 2, 3\}.$$  

Applications:

- Class fields
- Curves over finite fields
Algorithms

2. 2-adic [GHKRW 2002]
Algorithms

2. 2-adic [GHKRW 2002]

No bounds on the runtime:
- not explicit enough,
- no rounding error analysis for algorithm 1,
- no bound on denominator,
- no bound on absolute values of $i_n(C)$.

Recently, bounds on the denominator were given [Goren-Lauter 2007], [Goren (unpublished)], [Yang (special cases 2007)].
Step 1: Enumerate $\cong$-classes

\[ K \otimes \mathbb{R} \cong_{\text{R-alg.}} \mathbb{C}^2 \]

For $\Phi$ an isomorphism and $a \subset \mathcal{O}_K$, get lattice $\Lambda = \Phi(a) \subset \mathbb{C}^2$ and $\text{End}(\mathbb{C}^2/\Lambda) = \mathcal{O}_K$

Also need a principal polarization, so

\[ \{(\Phi, a, \xi)\} \sim \leftrightarrow \frac{\{C/\mathcal{C} \text{ with } CM \text{ by } \mathcal{O}_K\}}{\mathbb{R}} \]
Step 1: Enumerate $\cong$-classes

$$K \otimes \mathbb{R} \cong_{\mathbb{R}-\text{alg.}} \mathbb{C}^2$$

- For $\Phi$ an isomorphism and $a \subset \mathcal{O}_K$, get lattice $\Lambda = \Phi(a) \subset \mathbb{C}^2$ and $\text{End}(\mathbb{C}^2/\Lambda) = \mathcal{O}_K$
- Also need a principal polarization, so

$$\{(\Phi, a, \xi)\} \sim \leftrightarrow \{\mathbb{C}/\mathbb{C} \text{ with CM by } \mathcal{O}_K\}$$

- symplectic basis gives $\Lambda = \mathbb{Z}\mathbb{Z}^2 + \mathbb{Z}^2$ with $\mathbb{Z} = \mathbb{Z}^t, \text{Im}\mathbb{Z} > 0$
Step 2: Reduction

- Z is unique up to action of $\text{Sp}_4(\mathbb{Z})$ given by $MZ = (AZ + B)(CZ + D)^{-1}$.

- $\text{Sp}_4(\mathbb{Z})$-reduce $Z = (z_{jk})$, $z_{jk} = x_{jk} + iy_{jk}$:
  1. $\text{Im}Z$ reduced: $0 \leq 2y_{12} \leq y_{11} \leq y_{22}$
  2. $|x_{jk}| \leq \frac{1}{2}$
  3. $|\det CZ + D| \geq 1$ for $M \in \text{Sp}_4(\mathbb{Z})$. 
Step 3: Igusa invariants

- Thomae’s formulae gives an equation for $C$, given $Z$, in terms of $\theta$-constants.
  For $c_1, c_2 \in \{0, \frac{1}{2}\}^2$, let
  
  $$\theta[c_1, c_2](Z) = \sum_{v \in \mathbb{Z}^2} \exp(\pi i (v + c_1)Z(v + c_1)^t + 2\pi i (v + c_1)c_2^t).$$

- Write out, get
  
  $$j_n(Z) = \frac{\text{pol. in } \theta's}{(\prod \text{all } \theta's \neq 0)^*}$$

- Compute $H_{K,n} \in \mathbb{Q}[X]$.
  
  Have $\theta < 2$ for reduced $Z$, so need lower bound on $\theta$.  

Marco Streng
Computing Igusa Class Polynomials
Bounding $\theta$

Let $Z = (z_{jk})$ be reduced and write $z_{jk} = x_{jk} + iy_{jk}$.

- $|\theta[c](Z)| < 2.$
- lower bounds on $|\theta[c](Z)|$ in terms of
  1. upper bound on $y_{22}$ and
  2. (weak) lower bound on $|z_{12}|$.
- We know $C^2/(ZZ^2 + Z^2) \neq \prod_{j=1}^2 C/(z_{jj}Z + Z)$, so $z_3 \neq 0$, hence bound 2 follows from error analysis.
Bounding the period matrix

- Genus 1: given positive upper and lower bounds on $\text{Im } z'$ for $z' \in \mathbb{C}$, get upper bound on

$$\text{Im } Az' = \frac{\text{Im } z'}{|cz' + d|^2}$$

independent of $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z})$.

- Similar results for genus 2, so look for good $Z'$, only in proof.
Bounding the period matrix

- Genus 1: given positive upper and lower bounds on $\text{Im} \ z'$ for $z' \in \mathbb{C}$, get upper bound on

$$\text{Im} \ Az' = \frac{\text{Im} \ z'}{|cz' + d|^2}$$

independent of $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z})$.

- Similar results for genus 2, so look for good $Z'$, only in proof.

- We find $Z'$ by taking $a = zb + b^{-1}$ with $b \subset K_0$ and $z \in K$.

- Bounds we need = upper and lower bounds on $N_{K/Q}(b^2(z - \overline{z})\mathcal{O}_K)$

- Lower bounds: pick $z, b$ to maximize, use Minkowski’s convex body theorem.

- Upper bound from CM by $K = K_0(\sqrt{r})$. 
Result

Theorem

Can compute the Igusa class polynomials of primitive quartic CM fields $K$ in time

$$\tilde{O}(D_1^{7/2}D_0^{11/2}),$$

where $D_0 = D(K_0), D = D(K) = D_1D_0^2$ and $2, 3 \nmid D$.

The size of the output is between

$$\text{cst.}(D_1D_0)^{1/2-\epsilon} \quad \text{and} \quad \tilde{O}(D_1^2D_0^3)$$

- Ramification assumptions come from Goren’s unpublished work and it ‘should be’ possible to remove them.

- Preprint on Arxiv and on my web page

http://www.math.leidenuniv.nl/~streng