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

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

Applications:

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

The Hilbert class polynomial

Definition

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

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

Applications:

1. $K[X]/H_K =$ Hilbert class field of K
2. Elliptic curves over $\mathbf{F}_p$: if $\pi \in \mathcal{O}_K, \pi\overline{\pi} = p$, then $(H_K \bmod p)$ is a product of linear factors and for any root $j_0 \in \mathbf{F}_p$, exists E with $j(E) = j_0$ and

$$\#E(\mathbf{F}_p) = p + 1 - \mathrm{tr}(\pi)$$

Algorithm (sketch)

1. Bijection

$$\begin{aligned} \mathrm{Cl}_K &\leftrightarrow \{E/\mathbf{C} \text{ with CM by } \mathcal{O}_K\}/\cong \\ [\mathfrak{a}] &\mapsto \mathbf{C}/\mathfrak{a}, \end{aligned}$$

$\mathfrak{a} = z\mathbf{Z} + \mathbf{Z}$ with z in fund. domain:
$\mathrm{Im} z > 0, |\mathrm{Re} z| \leq \frac{1}{2}, |z| \geq 1$

Algorithm (sketch)

1. Bijection

$$\begin{aligned} \mathrm{Cl}_K &\leftrightarrow \{E/\mathbf{C} \text{ with CM by } \mathcal{O}_K\}/\cong \\ [\mathfrak{a}] &\mapsto \mathbf{C}/\mathfrak{a}, \end{aligned}$$

   $\mathfrak{a} = z\mathbf{Z} + \mathbf{Z}$ with z in fund. domain:
   $\mathrm{Im} z > 0, |\mathrm{Re} z| \leq \frac{1}{2}, |z| \geq 1$
2. $j(\mathfrak{a}) = q^{-1} + 744 + 196884q + 21493760q^2 + \cdots \quad (q = e^{2\pi i z})$
   (or smarter approximation)
3. Compute $H_K = \prod_z (X - j(z)) \in \mathbf{Z}[X]$

Algorithms

- The Hilbert class polynomial is huge: the degree h_K grows like $|D|^{\frac{1}{2}}$, 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]

Algorithms

- The Hilbert class polynomial is huge: the degree h_K grows like $|D|^{\frac{1}{2}}$, 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 $\mathrm{End}(E) \cong \mathcal{O}_K$ with K imaginary quadratic.
- A curve of genus 2 has CM if $\mathrm{End}(J(C)) \cong \mathcal{O}_K$ with K a CM field of degree 4.

Complex multiplication

- An elliptic curve has CM if $\mathrm{End}(E) \cong \mathcal{O}_K$ with K imaginary quadratic.
- A curve of genus 2 has CM if $\mathrm{End}(J(C)) \cong \mathcal{O}_K$ with K a CM field of degree 4.
- A CM field is $K_0(\sqrt{r})$ with K_0 totally real and $r \in K_0$, $r << 0$.
- 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

$$\begin{aligned}
I_2 &= a_6^2 \sum_{15} (12)^2 (34)^2 (56)^2, \\
I_4 &= a_6^4 \sum_{10} (12)^2 (23)^2 (31)^2 (45)^2 (56)^2 (64)^2, \\
I_6 &= a_6^6 \sum_{60} (12)^2 (23)^2 (31)^2 (45)^2 (56)^2 (64)^2 (14)^2 (25)^2 (36)^2, \\
I_{10} &= a_6^{10} \prod_{i<j} (ij)^2 \quad = \text{discr.}(f) \neq 0.
\end{aligned}$$

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

Igusa class polynomials

Simplification: $i_1 = \frac{I_2^5}{I_{10}}$, $i_2 = \frac{I_2^3 I_4}{I_{10}}$ and $i_3 = \frac{I_2^2 I_6}{I_{10}}$.

Definition

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

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

Applications:

- Class fields
- Curves over finite fields

Algorithms

1. Complex analytic [Spallek 1994, Van Wamelen 1999]
2. 2-adic [GHKRW 2002]
3. Chinese remainder theorem [Eisenträger-Lauter 2005]

Algorithms

1. Complex analytic [Spallek 1994, Van Wamelen 1999]
2. 2-adic [GHKRW 2002]
3. Chinese remainder theorem [Eisenträger-Lauter 2005]

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

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

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

$$\frac{\{(\Phi, \mathfrak{a}, \xi)\}}{\sim} \quad \longleftrightarrow \quad \frac{\{C/\mathbf{C} \text{ with CM by } \mathcal{O}_K\}}{\cong}$$

Step 1: Enumerate $\cong$-classes

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

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

$$\frac{\{(\Phi, \mathfrak{a}, \xi)\}}{\sim} \quad \longleftrightarrow \quad \frac{\{C/\mathbf{C} \text{ with CM by } \mathcal{O}_K\}}{\cong}$$

- symplectic basis gives $\Lambda = Z\mathbf{Z}^2 + \mathbf{Z}^2$ with $Z = Z^{\mathrm{t}}, \mathrm{Im}Z > 0$

Step 2: Reduction

- Z is unique up to action of

$$\mathrm{Sp}_4(\mathbf{Z}) = \left\{ M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathrm{GL}_4(\mathbf{Z}) : \begin{array}{c} A^{\mathrm{t}}D - C^{\mathrm{t}}B = 1 \\ A^{\mathrm{t}}C, D^{\mathrm{t}}B \text{ symmetric} \end{array} \right\},$$

  given by $MZ = (AZ + B)(CZ + D)^{-1}$.
- $\mathrm{Sp}_4(\mathbf{Z})$-reduce $Z = (z_{jk})$, $z_{jk} = x_{jk} + iy_{jk}$:
  1. $\mathrm{Im}Z$ 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 $M \in \mathrm{Sp}_4(\mathbf{Z})$.

Step 3: Igusa invariants

- Thomae's formulae gives an equation for C, given Z, in terms of θ-constants.
  For $c_1, c_2 \in \{0, \frac{1}{2}\}^2$, let

$$\theta[c_1, c_2](Z) = \sum_{v \in \mathbf{Z}^2} \exp(\pi i (v + c_1) Z (v + c_1)^{\mathrm{t}} + 2\pi i (v + c_1) {c_2}^{\mathrm{t}}).$$

- Write out, get

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

- Compute $H_{K,n} \in \mathbf{Q}[X]$.

Have $\theta < 2$ for reduced Z, so need lower bound on θ.

Bounding θ

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 $\mathbf{C}^2/(Z\mathbf{Z}^2 + \mathbf{Z}^2) \neq \prod_{j=1}^{2} \mathbf{C}/(z_{jj}\mathbf{Z} + \mathbf{Z})$, 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 $\operatorname{Im} z'$ for $z' \in \mathbf{C}$, get upper bound on

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

  independent of $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z})$.
- 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 $\operatorname{Im} z'$ for $z' \in \mathbf{C}$, get upper bound on

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

  independent of $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z})$.
- Similar results for genus 2, so look for good Z', only in proof.
- We find Z' by taking $\mathfrak{a} = z\mathfrak{b} + \mathfrak{b}^{-1}$ with $\mathfrak{b} \subset K_0$ and $z \in K$.
- Bounds we need = upper and lower bounds on $N_{K/\mathbf{Q}}(\mathfrak{b}^2(z - \overline{z})\mathcal{O}_K)$
- Lower bounds: pick $z, \mathfrak{b}$ 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

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

where $D_0 = D(K_0)$, $D = D(K) = D_1 D_0^2$ and $2, 3 \nmid D$.
The size of the output is between

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

- 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`