Igusa Class Polynomials

Marco Streng

Universiteit Leiden,
supported by the Leiden University Fund (LUF)

Joint Mathematics Meetings, San Diego, January 2008

Overview

- Igusa class polynomials are the genus 2 analogue of the classical Hilbert class polynomials.
- This talk: explain what they are.
- Talks by Freeman and Lauter following this talk: bounding the running time of algorithms that compute them.

Complex Multiplication

- Let E be an elliptic curve over a field of characteristic 0. Its endomorphism ring is either $\mathbb{Z}$ or an order $\mathcal{O}$ in an imaginary quadratic number field.
- In the second case, we say that E has complex multiplication (CM) by $\mathcal{O}$.
- Every elliptic curve over $\mathbb{C}$ is complex analytically isomorphic to $\mathbb{C}/\Lambda$ for some lattice $\Lambda \subset \mathbb{C}$.
- Let K be an imaginary quadratic number field. Every elliptic curve over $\mathbb{C}$ with CM by $\mathcal{O}_K$ is isomorphic to $\mathbb{C}/\mathfrak{a}$ for an ideal $\mathfrak{a}$ of $\mathcal{O}_K$.
- This gives a bijection between the set of isomorphism classes of elliptic curves over $\mathbb{C}$ with CM by $\mathcal{O}_K$ and the ideal class group $\mathcal{C}_K$ of K.

The Hilbert Class Polynomial

- The j-invariant is a rational function in the coefficients of the (Weierstrass) equation of an elliptic curve.
- For any field L, there is a bijection

$$\{\text{ elliptic curves over } L\ \}/(\overline{L}\text{-isom.}) \leftrightarrow L,$$

  given by the j-invariant.
- Up to $\overline{L}$-isomorphism, computing E and computing $j(E)$ is the same thing.
- The Hilbert Class Polynomial of an imaginary quadratic number field K is defined by

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

Application: constructing class fields

- Definition: the Hilbert class field of a field K is the maximal unramified abelian extension of K.
- Its Galois group over K is naturally isomorphic to the class group of K (Artin isomorphism).
- If K is imaginary quadratic, then the Hilbert class field of K is generated over K by the roots of $H_K(X)$. The Artin isomorphism corresponds to the action $\mathfrak{a} \cdot j(\mathbb{C}/\mathfrak{b}) = j(\mathbb{C}/\mathfrak{a}^{-1}\mathfrak{b})$.
- By computing the CM curves and their torsion points, we can also compute ray class fields of K.

Application: curves with prescribed number of points

- Let π be an imaginary quadratic integer of prime power norm q (a quadratic Weil q-number) and suppose that the trace t of π is coprime to q.
- The polynomial $H_{\mathbb{Q}(\pi)}(X)$ splits into linear factors over $\mathbb{F}_q$; let $j_0 \in \mathbb{F}_q$ be any root.
- There exists an ordinary elliptic curve $E/\mathbb{F}_q$ with $j(E) = j_0$ and $\#E(\mathbb{F}_q) = q + 1 - t$.
- Over $\overline{\mathbb{F}_q}$, all curves with j-invariant j_0 are isomorphic; over $\mathbb{F}_q$, there are at most 6 and it is easy to select the right one.
- Conclusion: (q-number of trace t) $+$ (class polynomial) $\rightsquigarrow$ (elliptic curve with $q + 1 - t$ points).
- See talk 4 (Stevenhagen) for more detail and for genus two.

Computing Hilbert class polynomials

- The coefficients are integers (because CM curves have potential good reduction).
- There are methods to compute the polynomial:
  - analytic,
  - p-adic, [Couveignes-Henocq, Bröker]
  - Chinese remainder theorem. [Chao-Nakamura-Sobataka-Tsujii, Agashe-Lauter-Venkatesan]
- The Hilbert class polynomial is huge: the logarithms of the coefficients are of size $\sqrt{|\Delta|}$, just like the degree of $H_K(X)$ (which is the class number of K).
- The complexity of all these methods is $\widetilde{O}(|\Delta|)$, essentially linear in the output.

Part 2: Genus 2

- An abelian variety (AV) is a smooth projective group variety.
- An elliptic curve (dim. 1 AV) has CM if its endomorphism ring is an order in an imaginary quadratic number field.
- An abelian surface (dim. 2 AV) has CM if its endomorphism ring is an order in a CM field of degree 4.
- A CM field of degree 4 is a totally imaginary quadratic extension of a real quadratic field.

Jacobians

- We consider abelian varieties together with a principal polarization. Every elliptic curve has a unique principal polarization.
- The Jacobian $J(C)$ of a curve C of genus g is a principally polarized abelian variety of dimension g.
- Weil: a principally polarized abelian surface over an algebraically closed field is one of the following:
  1. a product of two elliptic curves, or
  2. the Jacobian of a smooth irreducible curve of genus two, which (by Torelli's theorem) is unique up to isomorphism.
- Products of elliptic curves do not have CM.
- So instead of CM abelian surfaces, we study curves C of genus two such that $J(C)$ has CM.

Curves of genus 2

- Every curve of genus 2 is hyperelliptic, i.e. (in characteristic $\neq 2$)

$$C : y^2 = f(x), \quad \deg(f) = 6.$$

- Over algebraically closed fields, we can write it in Rosenhain form

$$C : y^2 = x(x-1)(x-\lambda_1)(x-\lambda_2)(x-\lambda_3).$$

- Compare this to Legendre form for elliptic curves

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

  The "family" of elliptic curves is one-dimensional, that of curves of genus 2 is three-dimensional.

Igusa invariants

- Igusa gave a genus 2 analogue of the j-invariant.
  - Let L be an algebraically closed field of characteristic different from 2. (Actually, Igusa's invariants work for any characteristic.)
  - Igusa gives polynomials I_2, I_4, I_6, I_{10} in the coefficients of f.
  - These give a bijection between the set of isomorphism classes of genus two curves over L and points $(I_2 : I_4 : I_6 : I_{10})$ in weighted projective space satisfying $I_{10} \neq 0$.
- Mestre's algorithm (also implemented in Magma) computes an equation for the curve from the invariants.
  - The curve can be defined over a field of degree at most 2 over any field containing the invariants.

Absolute invariants

- One simplifies by looking at the so-called absolute Igusa invariants

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

- If I_2 is non-zero, then these completely determine the $\overline{L}$-isomorphism class of the curve. Otherwise, build in a case distinction (as in [Cardona-Quer]).
- Do there exist CM curves C with $I_2(C) = 0$?

Igusa class polynomials

- The Igusa class polynomials are the polynomials

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

  of degree $d \leq 2h$.
  - By taking one zero i_n^0 of each polynomial $H_{K,n}$, one finds the point (i_1^0, i_2^0, i_3^0) and hence an isomorphism class of curve.
  - The polynomials thus specify d^3 isomorphism classes and the d classes with CM by $\mathcal{O}_K$ are among them.
  - Interpolation formulae can be used to specify which. [Gaudry-Houtmann-Kohel-Ritzenthaler-Weng 2006]
- Can consider the same applications as in the elliptic case.

Computing Igusa class polynomials

- Coefficients usually do not lie in $\mathbb{Z}$, but denominators have recently been bounded by Goren-Lauter and Goren, see talk 3.
- Analogues of the three algorithms have been developed, but there is no complexity bound yet.
- We study the complex analytic method and will give the first proven asymptotic bounds on the size of the output and the complexity of the three algorithms, such as:

Computing Igusa class polynomials

We (Freeman-Lauter-S) will prove:

Theorem

The complex analytic method takes time at most

$$\widetilde{O}(h^3\Delta^2) \leq \widetilde{O}(\Delta^{7/2})$$

and the size of the output is at most

$$\widetilde{O}(h^2\Delta) \leq \widetilde{O}(\Delta^2).$$

See next talk!