Igusa Class Polynomials

Marco Streng

Universiteit Leiden

Genus 2 day, Intercity Number Theory Seminar
Utrecht, April 18th 2008

Overview

- Igusa class polynomials are the genus 2 analogue of the classical Hilbert class polynomial.
- For each notion, I will
    1. tell you what it is,
    2. show two applications
    3. and talk about computing it.

Complex multiplication

The Hilbert class polynomial is a notion from complex multiplication of elliptic curves.

- Let E be an elliptic curve over a field of characteristic 0 and let $\mathrm{End}(E)$ be the ring of algebraic group endomorphisms.
- It is $\mathbb{Z}$ or an order $\mathcal{O}$ in an imaginary quadratic number field. In the second case, we say that E has complex multiplication (CM) by $\mathcal{O}$.
- Example: $E : y^2 = x^3 + x$ over $\mathbb{C}$ has an endomorphism $(x, y) \mapsto (-x, iy)$ with $i^2 = -1$.
  We call this endomorphism i and notice $i^2 = -1$.
  The endomorphism ring is $\mathrm{End}(E) = \mathbb{Z}[i]$.

Complex complex multiplication

- Every elliptic curve E over $\mathbb{C}$ is complex analytically isomorphic to $\mathbb{C}/\Lambda$ for some lattice $\Lambda \subset \mathbb{C}$.
- The algebraic endomorphisms of E correspond to the holomorphic endomorphisms of $\mathbb{C}/\Lambda$ and they are of the form $z \mapsto \alpha z$ with $\alpha\Lambda \subset \Lambda$.
- Let K be an imaginary quadratic number field and $\mathcal{C}_K$ its ideal class group. There is a bijection

$$\begin{array}{rcl} \mathcal{C}_K & \leftrightarrow & \{\text{Elliptic curves over } \mathbb{C} \text{ with CM by } \mathcal{O}_K\}/\cong \\ [\mathfrak{a}] & \mapsto & \mathbb{C}/\mathfrak{a}. \end{array}$$

The j-invariant

- 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.

Definition

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

$$H_K = \prod_{E \in \mathcal{C}_K} (X - j(E)).$$

The Hilbert class polynomial

$$H_K = \prod_{E \in \mathcal{C}_K} (X - j(E)) \in \mathbb{Z}[X].$$

- Why in $\mathbb{Q}[X]$?
  Let $\sigma \in \mathrm{Aut}(\mathbb{C})$ be any ring automorphism of $\mathbb{C}$. The algebraic endomorphism rings of E and ${}^{\sigma}E$ are isomorphic via σ. If $j(E)$ is a root, then so is $j({}^{\sigma}E) = {}^{\sigma}j(E)$. □
- Why in $\mathbb{Z}[X]$?
  Fact: Elliptic curves with complex multiplication have (after suitable base extension) good reduction at every prime $\mathfrak{p}$. Hence $j(E) \bmod \mathfrak{p} = j(E \bmod \mathfrak{p}) \neq \infty$ for all $\mathfrak{p}$, so $j(E)$ is an algebraic integer. □

Application: constructing class fields

Definition

The Hilbert class field $\mathcal{H}_K$ of a field K is the maximal unramified abelian extension of K.

The Galois group $\mathrm{Gal}(\mathcal{H}_K/K)$ is naturally isomorphic to $\mathcal{C}_K$ (Artin isomorphism).

Theorem

Let K be imaginary quadratic. The Hilbert class polynomial H_K is irreducible and normal and its roots generate $\mathcal{H}_K$ over K. The action of $\mathcal{C}_K$ on the roots of H_K is given by $[\mathfrak{a}] \bullet j([\mathfrak{b}]) = j([\mathfrak{a}^{-1}\mathfrak{b}])$.

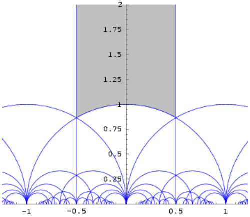
By computing the CM curves and their torsion points, we can also compute the ray class fields of K.

Application: curves of prescribed order

- Let π be an imaginary quadratic integer of prime norm q (a quadratic Weil q-number).
- Suppose that the trace t of π is coprime to q.
- Fact: The Hilbert class polynomial $H_{\mathbb{Q}(\pi)}$ splits into linear factors over $\mathbb{F}_q$; let $j_0 \in \mathbb{F}_q$ be any root.
- Fact: 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 π of trace t) $+\ H_{\mathbb{Q}(\pi)} \rightsquigarrow$ EC of order $q + 1 - t$.

Computing the Hilbert class polynomial

The Hilbert class polynomial is huge: the degree h_K grows like $|\Delta|^{\frac{1}{2}}$, as do the logarithms of the coefficients.



Classical complex analytic method:

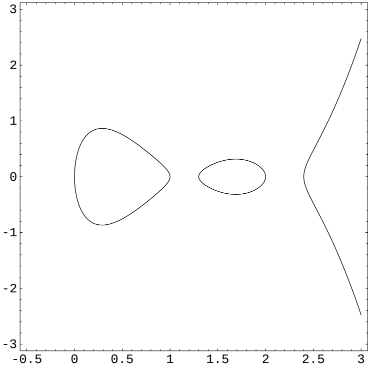
- compute all τ in $\mathcal{F}$ s.t. $\tau\mathbb{Z} + \mathbb{Z}$ is an $\mathcal{O}_K$-ideal,
- evaluate $j(\tau)$ for those τ,
- compute H_K from its roots.

Two other methods:

- p-adic, [Couveignes-Henocq, Bröker]
- Chinese remainder theorem. [CNST,ALV]

Each takes time $\widetilde{O}(|\Delta|)$, essentially linear in the size of the output.

Part 2: genus 2



Definition

A curve of genus 2 is a smooth geometrically irreducible curve of genus 2.

“Definition” (char.$\neq$ 2)

A curve of genus 2 is a smooth projective curve that has an affine model

$$y^2 = f(x), \quad \deg(f) \in \{5, 6\},$$

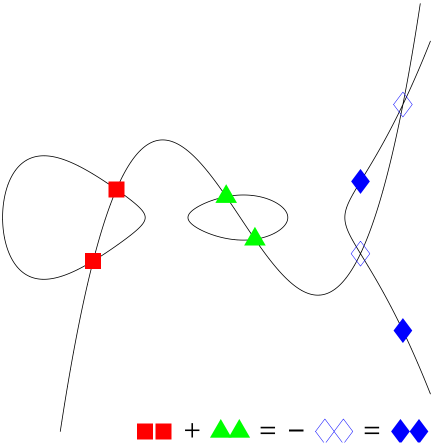
where f has no double roots.

How to add points on a curve

- Let C/k be a curve over a perfect field.
- The group of divisors $\mathrm{Div}(C)$ is the group of Galois invariant elements of the free abelian group on $C(\overline{k})$.
- Let $\mathrm{Div}^0(C)$ be the group of divisors of degree 0.
- Define the divisor $\mathrm{div}(f)$ of a rational function $f \in k(C)^*$ to be the sum of the zeroes/poles with multiplicities. It has degree 0.
- Get a group $\mathrm{Pic}^0(C) = \mathrm{Div}^0(C)/\mathrm{div}(k(C)^*)$.
- For an elliptic curve E: $E(k) \cong \mathrm{Pic}^0(E), P \mapsto [P - O]$.
- For a curve of genus 2, if we fix a divisor D of degree 2, then every class in $\mathrm{Pic}^0(C)$ has a representative $P_1 + P_2 - D$.

Genus 2 addition law

$\{P_1, P_2\} \leftrightarrow [P_1 + P_2 - 2\infty]$, use graphs of cubic polynomials!



Abelian varieties

- An abelian variety (AV) is a smooth projective group variety. (AV of dim. 1 = elliptic curve.)
- We consider abelian varieties together with a "principal polarization". (Every elliptic curve has a unique one.)
- $\mathrm{Pic}^0(C)$ "is" the group of rational points on a principally polarized abelian variety $J(C)$ of dimension $g(C)$, called the Jacobian of C. ($J(E) = E$.)

Complex multiplication

- 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 K of a real quadratic field.
  - It is called primitive if it does not contain an imaginary quadratic subfield.
- Fact: any principally polarized abelian surface with CM by a primitive CM field is the Jacobian of a unique (up to isomorphism) curve of genus 2.

The analogue of the j-invariant

Let $C : y^2 = f(x)$ be a curve of genus 2.

- 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 a 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 $\overline{L}$ and $\overline{L}$-points $(I_2 : I_4 : I_6 : I_{10})$ in weighted projective space with $I_{10} \neq 0$.
- Mestre's algorithm (also implemented in Magma) computes an equation for the curve from the invariants.
  - The curve can be constructed 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

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

- Outside $I_2 = 0$, they define the same space.
- The Jacobian of $C : y^2 = x^5 - 1$ has CM by the ring of integers of $\mathbb{Q}(\zeta_5)$ and corresponds to $I_2 = I_4 = I_6 = 0$. Do there exist other CM curves with $I_2 = 0$?

Igusa class polynomials

Definition

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

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

- By taking one zero i_n^0 of each polynomial $H_{K,n}$, get a 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.
- If $H_{K,1}$ has no double roots, can replace $H_{K,2}$ and $H_{K,3}$ by polynomials $G_{K,2}$ and $G_{K,3}$ such that $G_{K,n}(i_1(C)) = i_n(C)$ for all C with CM by $\mathcal{O}_K$.

Application: computation of class fields.

- In general, CM theory does not generate class fields of the CM field K, but of the reflex field $K^\dagger$.
  - If $K/\mathbb{Q}$ is Galois, then $K^\dagger = K$.
  - If $K = \mathbb{Q}(\sqrt{-a + b\sqrt{d}})$ is a primitive quartic CM field, then $K^\dagger = \mathbb{Q}(\sqrt{-2a + 2\sqrt{d'}})$, where $d' = a^2 - b^2 d$, and $K^{\dagger\dagger} = K$.
- In general, CM theory does not allow you to generate the full Hilbert class field or ray class fields:
  - Which fields can be obtained is described by Shimura.
  - Question: can we use dimension 2 CM as an ingredient for efficient computation of class fields?

Application: prescribed number of points

- Let q be a prime and let π be a quartic Weil q-number (i.e. an algebraic integer with all absolute values $q^{\frac{1}{2}}$) that generates a primitive quartic CM field.
- If the middle coefficient of f^{π} is coprime to q, then

$$\text{(quartic } q\text{-number } \pi) \quad + \quad (H_{\mathbb{Q}(\pi),n})_n$$
$$\downarrow$$
$$\begin{pmatrix} \text{a curve } C/\mathbb{F}_q \text{ of genus 2 with} \\ q+1-\mathrm{Tr}(\pi) \text{ rational points} \\ \text{and } \#\mathrm{Pic}^0(C) = N(\pi-1) \end{pmatrix}.$$

Computing Igusa class polynomials

Analogues of the three algorithms have been developed:

- Complex analytic [Spallek, van Wamelen, Weng]
- p-adic [Gaudry-Houtmann-Kohel-Ritzentaler-Weng]
- Chinese remainder theorem [Eisenträger-Lauter]

But...

- coefficients of Igusa class polynomials are usually not integers and ...
- no bounds on the sizes of $i_n(C)$ were given.

Denominators, why?

- Abelian varieties with CM have potential good reduction.
- But a genus 2 curve C of which the Jacobian has good reduction may have bad reduction!
- In that case, the reduction of C is the union of two intersecting elliptic curves and the reduction of $J(C)$ is a product of those elliptic curves (with product polarization).

Denominators, the "embedding problem"

Let K be a primitive quartic CM field and p a prime number. The following are equivalent: [Goren-Lauter]

1. p occurs in the denominator of $H_{K,n}$ for some n,
2. there exist:
   - a maximal order R in the quaternion algebra $B_{p,\infty}/\mathbb{Q}$,
   - a fractional right R-ideal $\mathfrak{a}$ with left order R' and
   - an embedding of $\mathcal{O}_K$ into the matrix algebra
   $$\begin{pmatrix} R & \mathfrak{a}^{-1} \\ \mathfrak{a} & R' \end{pmatrix}$$
   such that complex conjugation on $\mathcal{O}_K$ coincides with
   $$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \mapsto \begin{pmatrix} \overline{\alpha} & \overline{\beta} N(\mathfrak{a})^{-1} \\ \overline{\gamma} N(\mathfrak{a}) & \overline{\delta} \end{pmatrix}.$$

They also prove that 2. implies $p < c\Delta_K$ for some constant c.

Denominators, a bound

- [Goren-Lauter] bounds the primes in the denominator.
- Recent unpublished results by Eyal Goren bound the order with which they divide the denominator.
- Get a bound on the denominator: $O(d\Delta_K)$, where d is the degree of $H_{K,1}$.

Bounding the absolute values

- Algorithms exist in the sense that if you set your precision “sufficiently high” and know how to compute class groups, then you get an answer.
- No bounds on the output or on “sufficiently high”.
- Fundamental units are used.

To complete the analysis of the complex analytic method:

- enumerate curves in a suitable way to bound them away from $I_{10} = 0$ and $I_k = \infty$,
- analyse the multi-dimensional q-expansions and
- give rounding error analysis.

Result

Theorem (almost)

The complex analytic method takes time at most

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

and the size of the output is at most

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

I have the algorithm, which works at least if the real quadratic subfield has class number one and probably in general. I will write it up this summer.