Computing Igusa Class Polynomials

Marco Streng

Universiteit Leiden, Microsoft Research

UW Number Theory and Computation Seminar

Seattle, Sinterklaasavond 2008

Igusa class polynomials

Igusa class polynomials are the genus 2 analogue of the classical Hilbert class polynomial.

Overview:

- The Hilbert class polynomial
  - What is it?
  - Two applications
  - How to compute it?
- What is genus 2?
- Igusa class polynomials
  - What are they?
  - Two applications
  - How to compute them?

Complex multiplication

- An elliptic curve E over a field k (of characteristic $\neq 2$) is a smooth projective curve given by $y^2 = x^3 + ax^2 + bx + c$. It has an algebraic group law.
- Let $\mathrm{End}(E)$ be the ring of algebraic group endomorphisms.
- If k has characteristic 0, then $\mathrm{End}(E)$ is either $\mathbf{Z}$ 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 $\mathbf{C}$ has an endomorphism $(x, y) \mapsto (-x, iy)$, where $i^2 = -1$.
  We call this endomorphism i and notice $i^2 = -1$.
  The endomorphism ring is $\mathrm{End}(E) = \mathbf{Z}[i]$.

Analytic complex multiplication

- Every elliptic curve E over $\mathbf{C}$ is complex analytically isomorphic to $\mathbf{C}/\Lambda$ for some lattice $\Lambda \subset \mathbf{C}$.
- Let $K \subset \mathbf{C}$ be an imaginary quadratic number field. There is a bijection

$$\begin{array}{rcl} \{\text{Elliptic curves over } \mathbf{C} \text{ with CM by } \mathcal{O}_K\}/\cong & \leftrightarrow & \mathrm{Cl}_K \\ \mathbf{C}/\mathfrak{a} & \leftarrow & [\mathfrak{a}], \end{array}$$

where Cl_K is the class group of K.

The j-invariant

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

$$\begin{aligned} \{\text{ elliptic curves}/k\ \}/(\overline{k}\text{-isom.}) &\leftrightarrow k, \\ E &\mapsto \texttt{E.j\_invariant()}, \\ \texttt{EllipticCurve(j)} &\leftarrow j. \end{aligned}$$

- Up to $\overline{k}$-isomorphism, computing E and computing $j(E)$ is the same thing.

The Hilbert class polynomial

Definition

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

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

Examples:

$$\begin{aligned} H_{\mathbf{Q}(i)} &= X - 1728 \\ H_{\mathbf{Q}(\sqrt{-23})} &= X^3 + 3491750X^2 - 5151296875X + 12771880859375 \end{aligned}$$

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 Cl_K (Artin isomorphism).

Theorem

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

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 q be a prime. For any integer t such that $|t| < 2\sqrt{q}$, there exists an elliptic curve $E/\mathbf{F}_q$ with $\#E(\mathbf{F}_q) = q + 1 - t$.
- Let $D = t^2 - 4q$. The polynomial $(H_{\mathbf{Q}(\sqrt{D})} \bmod q) \in \mathbf{F}_q[X]$ splits completely into linear factors, and every zero $j_0 \in \mathbf{F}_q$ is the j-invariant of such an elliptic curve E.
- Computing all curves with j-invariant j_0 is easy, and so is checking which one has group order $q + 1 - t$.
- Conclusion:
  (prime q, $|t| < 2\sqrt{q}$) + $H_{\mathbf{Q}(\sqrt{t^2-4q})} \rightsquigarrow$ EC of order $q+1-t$.

Computing the Hilbert class polynomial

- The Hilbert class polynomial is huge: the degree h_K grows like $|\Delta_K|^{\frac{1}{2}}$, 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, each takes time $O(|\Delta_K|^{1+\epsilon})$, essentially linear in the size of the output.
- MAGMA: `HilbertClassPolynomial(K)`
  NOT Sage: `K.hilbert_class_polynomial()`
- Recent improvements by [BBEL 2008, Sutherland 2008] turned CRT (the underdog) into the record holder: $\Delta_K = -102,197,306,669,747$, $h_K = 2,014,236$.

Part 2: genus 2

Definition

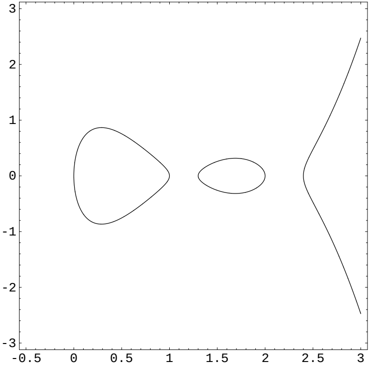
A curve of genus 2 is a smooth geometrically irreducible curve of genus 2.

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.



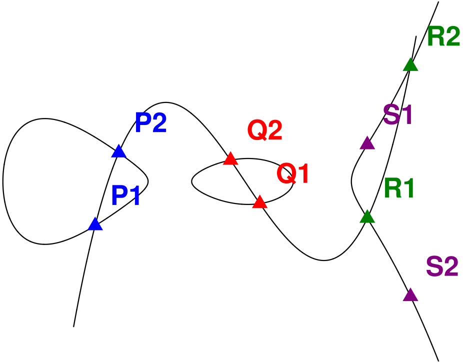
Sage / MAGMA:
`HyperellipticCurve(f)`

How to add points on a curve

- Points on a curve C/k can be added inside the divisor class group
$$\mathrm{Pic}^0(C) = \mathrm{Div}^0(C)/\mathrm{div}(k(C)^*).$$
- For an elliptic curve E, $E(k) \leftrightarrow \mathrm{Pic}^0(E), P \mapsto [P - \infty]$.
- For a curve of genus 2, if we fix a divisor D_0 of degree 2, then for every every divisor $D \in \mathrm{Div}^0(C)$, there are points P_1, P_2 on C such that $[D] = [P_1 + P_2 - D_0]$.

Genus 2 addition law

$$[P_1+P_2-2\infty]+[Q_1+Q_2-2\infty] = -[R_1+R_2-2\infty] = [S_1+S_2-2\infty]$$



Abelian varieties

- The Jacobian $J(C)$ of a curve C/k of genus g is a g-dimensional group variety with $J(C)(k) = \mathrm{Pic}^0(C)$ (if $C(k) \neq \emptyset$).
- The Jacobian is a "principally polarized abelian variety".
- For an elliptic curve E: $J(E) = E$.
- Every principally polarized abelian surface over $\mathbf{C}$ is either the Jacobian of a unique curve $C/\mathbf{C}$ of genus 2 or the (polarized) product of two elliptic curves, but not both.
- Sage: `C.jacobian()`
  MAGMA: `Jacobian(C)`

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 not a product of elliptic curves, hence is the Jacobian of a unique curve of genus 2.

The analogue of the j-invariant

Let k be an algebraically closed field.

- Every elliptic curve over k can be written in Legendre form

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

- Every curve of genus 2 over k can be written in Rosenhain form

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

- Conclusion: 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 k be an algebraically closed field of characteristic different from $2, 3, 5$. (Actually, Igusa's invariants work for any characteristic.)
  - Igusa gives polynomials I_2, I_4, I_6, I_{10} in the coefficients of C.
    MAGMA: `IgusaClebschInvariants(C)`
    not (yet?) in Sage.
  - These give a bijection between the set of isomorphism classes of genus 2 curves over k and k-points $(I_2 : I_4 : I_6 : I_{10})$ in weighted projective space with $I_{10} \neq 0$.
- Mestre's algorithm computes an equation for the curve from the invariants.
  MAGMA: `HyperellipticCurveFromIgusaClebsch(I)`

Igusa class polynomials

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

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

- Points (i_1, i_2, i_3) with $i_1 \neq 0$ correspond bijectively to points $(I_2 : I_4 : I_6 : I_{10})$ with $I_2 I_{10} \neq 0$ and hence to isomorphism classes of curves with $I_2 \neq 0$.

Definition

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

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

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

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

Computing Igusa class polynomials

Analogues of the three algorithms have been developed:

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

But no bounds on the runtime were given:

- algorithms were not explicit enough,
- no rounding error analysis for the complex analytic method,
- no bounds on the denominator,
- no bounds on the absolute values of $i_n(C)$.

In fact, there was not even a proof of correctness of the output.

Computing Igusa class polynomials (2)

- Recently, bounds on the denominator were given [Goren-Lauter 2007], [Goren (unpublished)].
- My work: improve upon Spallek and Van Wamelen and use bounds of Goren and Lauter to get an algorithm with a runtime bound.

Complex analytic method

Basic idea for genus 1:

1. Give a set of representatives of the ideal classes of $\mathcal{O}_K$, each given as $z\mathbf{Z} + \mathbf{Z}$ for $z \in \mathbf{C}$ with $\operatorname{Im} z > 0$.
2. For each, evaluate numerically $j(z) = j(\mathbf{C}/(z\mathbf{Z} + \mathbf{Z})) = q^{-1} + 744 + 196884q + 21493760q^2 + \cdots$, where $q = \exp(2\pi i z)$.
3. Compute $H_K = \prod_z (X - j(z)) \in \mathbf{Z}[X]$.

- Algorithm analysis uses bounds on $\operatorname{Im} z$.

Genus 2, step 1

Enumerating the isomorphism classes.

- Complex principally polarized abelian surfaces over $\mathbf{C}$ are of the form $\mathbf{C}^2/(Z\mathbf{Z}^2 + \mathbf{Z}^2)$, where Z is a period matrix, i.e. a (2×2) complex symmetric matrix with positive definite imaginary part. We call the set $\mathcal{H}_2$ of period matrices matrices the Siegel upper half space.
- A complete set of representatives Z for all isomorphism classes of principally polarized abelian surfaces with CM by $\mathcal{O}_K$ is given by Van Wamelen.

Genus 2, step 2

Evaluating the invariants.

- Recall that $i_1 = I_2^5 I_{10}^{-1}, i_2 = I_2^3 I_4 I_{10}^{-1}$ and $i_3 = I_2^2 I_6 I_{10}^{-1}$.
- Each Igusa invariant $I_{2k}(Z)$ can be given as a polynomial in the theta constants. For $c_1, c_2 \in \{0, \frac{1}{2}\}^2$, let

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

  Moreover,

$$I_{10}(Z) = \prod_{2c_1 . c_2 \in \mathbf{Z}} \theta[c_1, c_2](Z)^2.$$

- We use this to evaluate $i_n(Z)$.
- To get upper bounds on $|i_n(Z)|$, and the required precision for the theta constants, we (only) need to give upper and lower bounds on the theta constants.

Bounding the theta constants (1)

- To be able to bound the theta constants, we move the period matrix Z to a suitable region $\mathcal{F}$ in the upper half space $\mathcal{H}_2$.
- Two period matrices in $\mathcal{H}_2$ correspond to isomorphic principally polarized abelian varieties if and only if they are in the same orbit under the action of the symplectic group $\mathrm{Sp}_4(\mathbf{Z})$.
- Gottschling describes a fundamental domain $\mathcal{F} \subset \mathcal{H}_2$ for the action of $\mathrm{Sp}_4(\mathbf{Z})$ on $\mathcal{H}_2$.
- After step 1, we replace Van Wamelen's period matrices by $\mathrm{Sp}_4(\mathbf{Z})$-equivalent ones in $\mathcal{F}$ using a reduction algorithm. MAGMA: `To2 [Tab]`

Bounding the theta constants (2)

Let

$$Z = \begin{pmatrix} z_1 & z_3 \\ z_3 & z_2 \end{pmatrix} \in \mathcal{F},$$

- There is a constant upper bound on $|\theta[c_1, c_2](Z)|$ that holds for all $Z \in \mathcal{F}$.
- Klingen gives a positive lower bound on $|\theta[c_1, c_2](Z)|$ in terms of upper bounds on $\operatorname{Im} z_1$ and $\operatorname{Im} z_2$ and a lower bound on $|z_3|$.
- The period matrix Z is obtained from Van Wamelen's via a reduction algorithm.
- How to bound its entries? A direct analysis gives bad bounds on $\operatorname{Im} z_1$ and $\operatorname{Im} z_2$.

Bounding the entries of the period matrix (1)

- The lower bound we need on $|z_3|$ is allowed to be weak.
- We know that $z_3 \neq 0$, because otherwise $\mathbf{C}^2/(Z\mathbf{Z}^2 + \mathbf{Z}^2) = \mathbf{C}/(z_1\mathbf{Z} + \mathbf{Z}) \times \mathbf{C}/(z_2\mathbf{Z} + \mathbf{Z})$ is not a Jacobian.
- Therefore, we obtain a lower bound for free from a rounding error analysis.

Bounding the entries of the period matrix (2)

- Trick to bound $\operatorname{Im} z_1$ and $\operatorname{Im} z_2$: certain kinds of bounds on $Z' \in \mathcal{H}_2$ imply uniform bounds on $\operatorname{Im} z_1$ and $\operatorname{Im} z_2$ for all $Z \in \mathrm{Sp}_4(\mathbf{Z})Z'$.
- Compare to: positive upper and lower bounds on $\operatorname{Im} z'$ for $z' \in \mathbf{C}$ together give an upper bound on $\operatorname{Im}((az'+b)(cz'+d)^{-1}) = |cz'+d|^{-2} \operatorname{Im} z'$ for all

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}).$$

- For Z', take an optimal point in the Hilbert upper half space of abelian varieties with real multiplication by $K \cap \mathbf{R}$.
- Z' does not occur in the algorithm, only in the analysis.

Genus 2, step 3

Compute $H_{K,n} = \prod_Z (X - i_n(Z)) \in \mathbf{Q}[X]$.

- To get the correct $\mathbf{Q}$-valued coefficients, use LLL and the appropriate precision obtained from
  - the absolute value bounds above,
  - the denominator bounds of Goren and Lauter, and
  - a rounding error analysis of every step.
- Runtime bound is obtained from the precision bounds and a runtime analysis of every step.

Result

Theorem

The complex analytic method for computing the Igusa class polynomials of a primitive quartic CM field K in which 2 and 3 do not ramify, takes time at most

$$\Delta_K^{7/2+\epsilon} \quad (\Delta_K \to \infty).$$

The size of the output is between

$$\Delta_K^{1/4-\epsilon} \quad \text{and} \quad \Delta_K^{2+\epsilon} \quad (\Delta_K \to \infty).$$

- Ramification assumption comes from Goren's unpublished work and it 'should be' possible to remove them.
- Preprint on my web page `http://www.math.leidenuniv.nl/~streng`