Igusa class polynomials

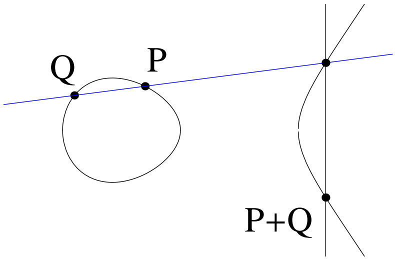
Marco Streng

THE UNIVERSITY OF WARWICK

Number Theory Seminar
Nottingham
11 May 2011

Elliptic curves

- An *elliptic curve* E/k ($\mathrm{char}(k) \neq 2$) is a smooth projective curve
$$y^2 = x^3 + ax^2 + bx + c.$$



- E is a commutative algebraic group

Endomorphisms

- $\mathrm{End}(E) =$ (ring of algebraic group morphisms $E \to E$)
  - $(\phi + \psi)(P) = \phi(P) + \psi(P)$
  - $(\phi\psi)(P) = \phi(\psi(P))$
- Examples:
  - $\mathbf{Z} \subset \mathrm{End}(E)$ with $n : P \mapsto P + \cdots + P$.
    For "most" E's in characteristic 0, have $\mathrm{End}(E) = \mathbf{Z}$.
  - If $E : y^2 = x^3 + x$ and $i^2 = -1$ in k, then we have
    $$i : (x, y) \mapsto (-x, iy),$$
    and $\mathbf{Z}[i] \subset \mathrm{End}(E)$.
  - If $\#k = q$, we have
    $$\mathrm{Frob} : (x, y) \mapsto (x^q, y^q).$$

The Hilbert class polynomial

The *j-invariant* is

$$j(E) = \frac{2^8 3^3 b^3}{2^2 b^3 + 3^3 c^2} \quad \text{for} \quad E : y^2 = x^3 + bx + c.$$

$$j(E) = j(F) \iff E \cong_{\overline{k}} F$$

Definition

Let K be an imaginary quadratic number field. Its Hilbert class polynomial is

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

Application 1: roots generate the Hilbert class field of K over K.

Application 2: make elliptic curves with prescribed order over $\mathbf{F}_p$.

Curves with prescribed order

- If $p = \pi\overline{\pi}$ for $\pi \in \mathcal{O}_K$, then (H_K mod p) splits into linear factors.
- Let $j_0 \in \mathbf{F}_p$ be a root and let $E_0/\mathbf{F}_p$ have $j(E_0) = j_0$.
- Then a twist E of E_0 has "Frob $= \pi$".
  Reason:
  - E_0 is the reduction of some $\widetilde{E}$ with $\mathrm{End}(\widetilde{E}) = \mathcal{O}_K$
  - CM theory $\Longrightarrow$ Frob $\in \mathcal{O}_K$ and $N(\mathrm{Frob}) = p$.
- We get

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

Computing Hilbert class polynomials (1)

- Any E is complex analytically $\mathbf{C}/\Lambda$ for a lattice Λ
- Endomorphisms induce $\mathbf{C}$-linear maps $\alpha : \mathbf{C} \to \mathbf{C}$ with $\alpha(\Lambda) \subset \Lambda$
- If $\mathrm{End}(E) \cong \mathcal{O}_K$, then $\Lambda = c\mathfrak{a}$ for an ideal $\mathfrak{a} \subset \mathcal{O}_K$ and $c \in \mathbf{C}^*$.
- We get

$$\begin{array}{ccc} \mathrm{Cl}_K & \longleftrightarrow & \dfrac{\{E/\mathbf{C} : \mathrm{End}(E) \cong \mathcal{O}_K\}}{\cong} \\ [\mathfrak{a}] & \longmapsto & \mathbf{C}/\mathfrak{a}. \end{array}$$

Computing Hilbert class polynomials (2)

- Write $\mathfrak{a} = \tau\mathbf{Z} + \mathbf{Z}$ and let $q = \exp(2\pi i\tau)$.
- Let $\theta_0 = 1 + 2\sum_{n=1}^{\infty} q^{\frac{1}{2}n^2}$ and $\theta_1 = 1 + 2\sum_{n=1}^{\infty}(-1)^n q^{\frac{1}{2}n^2}$. Then
$$j(z) = 256\frac{(\theta_0^8 - \theta_0^4\theta_1^4 + \theta_1^8)^3}{\theta_0^8\theta_1^8(\theta_0^4 - \theta_1^4)^2}$$
- Compute
$$H_K = \prod_{[\mathfrak{a}]\in\mathcal{CL}_K} (X - j(\mathbf{C}/\mathfrak{a})) \in \mathbf{Z}[X].$$
- Other algorithms:
  - p-adic, [Couveignes-Henocq 2002, Bröker 2006]
  - Chinese remainder theorem. [Chao-Nakamura-Sobataka-Tsujii 1998, Agashe-Lauter-Venkatesan 2004]

Performance

- The Hilbert class polynomial is huge: the degree h_K grows like $|D|^{\frac{1}{2}}$, as do the logarithms of the coefficients.
- Example: for $K = \mathbf{Q}(\sqrt{-101})$, get

$$\begin{aligned}
H_K =\, & X^{14} - 26523162922592872254376679 68X^{13} - 1365996687301280729477925915809419014840 32X^{12} \\
& -18914753547800938220605525785297549126598228285849 6X^{11} - 261816917979673221354141821 37\backslash \\
& 36079615091619955384077799915 52X^{10} - 11938851150588269566222488021842096539844729124 87\backslash \\
& 39406654201659392X^{9} - 19970076081487858762907119018999559036025406760107290495924627270\backslash \\
& 795264X^{8} + 70524492551600286857708450126047595357088538427268967051429368624924170649 6X^{7} \\
& -33872799529198964844915900102578375435327831844475016592225474796536885894184960X^{6} \\
& -2896474067779984860686947109556011057884959990693925971654663930124666762752216268 8X^{5} \\
& -225668200685134628791028483185000419030568870544024367727924246520982009875909034010214 4X^{4} \\
& -200298571407255942413741032535199918038466280292881148988363030841251201350298522427064\backslash \\
& 320X^{3} + 47260057763554643848267927603680487900953998656856813562449899690387453644049 3\backslash \\
& 770310317768704X^{2} + 130938563560495587536701299947027165858686450832805101450845834339\backslash \\
& 0877415208257790347777713111 04X - 1594321005753707552829297243529545040400813484400170\backslash \\
& 06382564760342197351665472136478486380891078656
\end{aligned}$$

Performance

- The Hilbert class polynomial is huge: the degree h_K grows like $|D|^{\frac{1}{2}}$, as do the logarithms of the coefficients.
- Example: for $K = \mathbf{Q}(\sqrt{-101})$, get

$$
\begin{aligned}
H_K = {} & X^{14} - 2652316292259287225437667968X^{13} - 1365996687301280729477925915809419014840 32X^{12} \\
& - 18914753547800938220605525785297549126598228285 8496X^{11} - 2618169179796732213541418 2137\backslash \\
& 3607961509161995538407779991552X^{10} - 11938851150588269566222488021842096539844 72912487\backslash \\
& 39406654201659392X^{9} \\
& + \quad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
& - 1594321005753707552829297243529545040400813484400170063825647603421973516654721364\backslash \\
& 78486380891078656
\end{aligned}
$$

- Under GRH or heuristics, all three *quasi-linear* $O(|D|^{1+\epsilon})$.
- CRT (the underdog) is now the record holder: constructed a large finite field elliptic curve with $-D > 10^{15}$, $h_K > 10^{7}$. [Belding-Bröker-Enge-Lauter 2008, Sutherland 2009]

Curves of genus 2

Definition

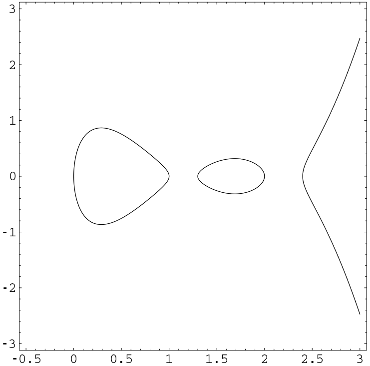
A curve of genus 2 is a smooth geometrically irreducible curve of which the genus is 2.

"Definition" (char. $\neq 2$)

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

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

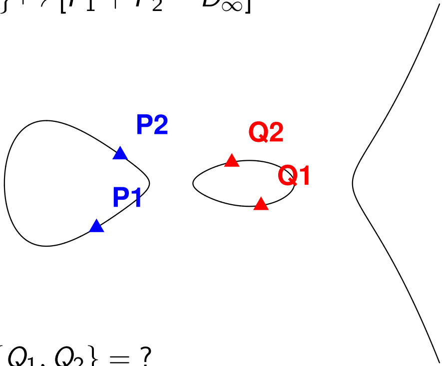
where f has no double roots.



The group law on the Jacobian

The Jacobian: group of equivalence classes of pairs of points.

- More precisely, divisor class group $\mathrm{Pic}^0(C)$
  $\{P_1, P_2\} \mapsto [P_1 + P_2 - D_\infty]$

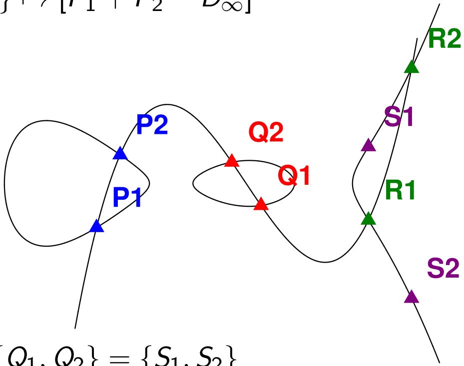


$\{P_1, P_2\} + \{Q_1, Q_2\} = ?$

The group law on the Jacobian

The Jacobian: group of equivalence classes of pairs of points.

- More precisely, divisor class group $\mathrm{Pic}^0(C)$
  $\{P_1, P_2\} \mapsto [P_1 + P_2 - D_\infty]$



$\{P_1, P_2\} + \{Q_1, Q_2\} = \{S_1, S_2\}$

Igusa class polynomials

- Elliptic curves E have CM if $\mathrm{End}(E)$ is an order in an imaginary quadratic field $K = \mathbf{Q}(\sqrt{r})$ with $r \in \mathbf{Q}$ negative.
- Curves C of genus 2 have CM if $\mathrm{End}(J(C))$ is an order in a *CM field K of degree 4*, i.e. $K = K_0(\sqrt{r})$ with K_0 real quadratic and $r \in K_0$ totally negative.
- Assume K contains no imaginary quadratic field.
- *Igusa's invariants* i_1, i_2, i_3 are the genus-2 analogue of j
- The *Igusa class polynomials* of a quartic CM field K are a set of polynomials of which the roots are the Igusa invariants of curves C of genus 2 with CM by $\mathcal{O}_K$.

Applications

- Roots generate class fields.
  - not of K, but of its "reflex field" (no problem)
  - not the full Hilbert class field (but we know which field)
  - useful? efficient? (work in progress!)
- If $p = \pi\overline{\pi}$ in $\mathcal{O}_K$, construct curve C with

$$\#J(C)(\mathbf{F}_p) = N(\pi - 1) \quad \text{and} \quad \#C(\mathbf{F}_p) = p + 1 - \operatorname{tr}(\pi).$$

Algorithms

1. Complex analytic [Spallek 1994, Van Wamelen 1999]
2. p-adic [Gaudry-Houtmann-Kohel-Ritzenthaler-Weng 2002, Carls-Kohel-Lubicz 2008]
3. Chinese remainder theorem [Eisenträger-Lauter 2005]

None of these had running time bounds:

- denominators
- not known how to bound $|i_n(C)|$.
- algorithms not explicit enough
- no rounding error analysis for alg. 1 (not even for genus 1!!)

Denominators

- CM elliptic curves have "potential good reduction", hence $j(E) \in \overline{\mathbf{Z}}$, hence Hilbert class polynomials are in $\mathbf{Z}[X]$
- CM abelian varieties (such as $J(C)$) also have potential good reduction, but may have

$$(J(C) \bmod \mathfrak{p}) = E_1 \times E_2 \quad \text{and} \quad (C \bmod \mathfrak{p}) = E_1 \cup E_2.$$

- In that case, $\exists \iota : \mathcal{O}_K \to \mathrm{End}(E_1 \times E_2)$ and E_1 and E_2 are isogenous supersingular elliptic curves.
- Can bound denominators by studying the "embedding problem" [Goren-Lauter 2007], [Goren-Lauter 2011]

Step 1: Enumerating $\cong$-classes

- $K \otimes \mathbf{R} \cong_{\mathbf{R}-\mathrm{alg.}} \mathbf{C}^2$
- For Φ an isomorphism and $\mathfrak{a} \subset \mathcal{O}_K$, get a lattice $\Lambda = \Phi(\mathfrak{a}) \subset \mathbf{C}^2$ and $\mathrm{End}(\mathbf{C}^2/\Lambda) = \mathcal{O}_K$.
- Also need a polarization, given by $\xi \in K^*$ with $\xi\mathfrak{a}\overline{\mathfrak{a}}\mathcal{D}_{K/\mathbf{Q}} = \mathcal{O}_K$, and $\Phi(\xi) \in i\mathbf{R}^2_{>0}$.
- Then

$$\frac{\{(\Phi, \mathfrak{a}, \xi)\}}{\sim} \quad \longleftrightarrow \quad \frac{\{C/\mathbf{C} : \mathrm{End}(J(C)) \cong \mathcal{O}_K\}}{\cong}.$$

- Symplectic basis gives $\Lambda = \tau\mathbf{Z}^2 + \mathbf{Z}^2$ with $\tau \in \mathrm{Mat}_2(\mathbf{C})$ symmetric with pos. def. imaginary part.

Step 2: Reduction (elliptic case)

For $E = \mathbf{C}/(\tau\mathbf{Z} + \mathbf{Z})$, the number τ is unique up to

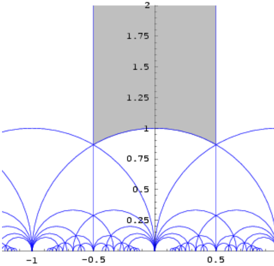
$\mathrm{SL}_2(\mathbf{Z})$

acting via

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \tau = (a\tau + b)(c\tau + d)^{-1}.$$

We make τ reduced:

1. $|\mathrm{Re}\,\tau| \leq 1/2$,
2. $|\ \tau\ \ \ \ | \geq 1$



Step 2: Reduction (elliptic case)

For $E = \mathbf{C}/(\tau\mathbf{Z} + \mathbf{Z})$, the number τ is unique up to

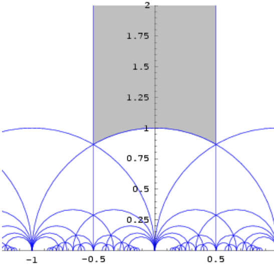
$$\mathrm{SL}_2(\mathbf{Z}) = \{M \in \mathrm{GL}_2(\mathbf{Z}) : M^{\mathrm{t}} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} M = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\},$$

acting via

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \tau = (a\tau + b)(c\tau + d)^{-1}.$$

We make τ reduced:

1. $|\mathrm{Re}\,\tau| \leq 1/2$,
2. $|c\tau + d| \geq 1$ for all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z})$



Step 2: Reduction

For $J(C) = \mathbf{C}^2/(\tau\mathbf{Z}^2 + \mathbf{Z}^2)$, the matrix τ is unique up to

$$\mathrm{Sp}_4(\mathbf{Z}) = \{M \in \mathrm{GL}_4(\mathbf{Z}) : M^{\mathrm{t}} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} M = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\},$$

acting via

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \tau = (a\tau + b)(c\tau + d)^{-1}.$$

We make τ reduced:

1. entries of $\mathrm{Re}\,\tau$ have absolute value $\leq 1/2$,
2. $|\det(c\tau + d)| \geq 1$ for all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Sp}_4(\mathbf{Z})$,
3. $\mathrm{Im}\,\tau = \begin{pmatrix} y_1 & y_3 \\ y_3 & y_2 \end{pmatrix}$ is reduced: $0 \leq 2y_3 \leq y_1 \leq y_2$.

Step 3: Numerical evaluation

- Thomae's formula [1870] gives an equation for C, given τ, in terms of the ten even theta constants

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

with $c_1, c_2 \in \{0, \frac{1}{2}\}^2$, $2 c_1 c_2^{\mathrm{t}} \in \mathbf{Z}$.

- Write out, get [Bolza 1887, Igusa 1967]

$$i_k(\tau) = \frac{\text{pol. in } \theta\text{'s}}{\prod \theta^4}, \qquad \text{e.g.} \qquad i_2(\tau) = \frac{(\sum \theta^8)^5}{\prod \theta^4}.$$

- Evaluate Igusa class polynomials numerically.

Bounds on Igusa invariants

- For running time bound, need upper bound on

$$|i_k| = \frac{|\text{pol. in } \theta\text{'s}|}{\prod |\theta|^4}.$$

- Have $|\theta(\tau)| < 2$ for reduced τ, so only need lower bound on $|\theta(\tau)|$.
- Got a bound in terms of
  1. upper bound on entries of $\operatorname{Im}\tau$,
  2. lower bound on $|\tau_{12}|$ (allowed to be weak)
- Part 2 for free from detailed analysis of our construction of τ.

Bound on $\operatorname{Im} \tau$ (elliptic case)

- For elliptic curves, we have

$$\tau = \frac{-b + \sqrt{D}}{2a}$$

  with a, $b \in \mathbf{Z}$, hence $\operatorname{Im} \tau \leq \frac{1}{2}\sqrt{|D|}$.
- For genus 2, it is not that simple.

Bound on $\operatorname{Im}\tau$

- Bound $\operatorname{Im}\tau$ by proving existence of alternative τ' and relating it to τ via $A \in \mathrm{Sp}_4(\mathbf{Z})$.
- Elliptic curves: if $\tau = A\tau'$ and $\tau' = x + yi$, then

$$\begin{aligned}\operatorname{Im}\tau = \frac{\operatorname{Im}\tau'}{|c\tau' + d|^2} &= \frac{y}{(cx+d)^2 + (cy)^2} \\ &\leq \begin{cases} y & \text{if } c = 0 \\ y^{-1} & \text{if } c \neq 0 \end{cases} \\ &\leq \max\{y, y^{-1}\}\end{aligned}$$

  Similar results for genus 2.
- To get τ', write $\mathfrak{a} = z\mathfrak{b} + \mathfrak{b}^{-1}$ and maximize $N_{K/\mathbf{Q}}(\mathfrak{b}^2(z - \overline{z})\mathcal{O}_K)$.
  (related to fundamental domains for $\mathrm{SL}_2(\mathcal{O}_{K_0})$).

Result

Theorem

Algorithm computes the Igusa class polynomials of K in time less than

$$\text{cst.}(D_1^{7/2} D_0^{11/2})^{1+\epsilon},$$

where $D_0 = \operatorname{disc} K_0$ and $D_1 D_0^2 = \operatorname{disc} K$. The bit size of the output is between

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

Bottlenecks:

1. quasi-quadratic time theta evaluation (quasi-linear method not proven [Dupont 2006])
2. denominator bounds not optimal (special cases/conjectures [Bruinier-Yang 2006, Yang (preprint)])

What's next?

$g = 1$: In practice, one does not use j, but uses "smaller functions" such as $\sqrt[3]{j}$, Weber functions, and (double) eta quotients.

$g = 2$: Still stuck with Igusa's invariants.

$g = 1$: Useful tool: explicit version of Shimura's reciprocity law, relating Galois action of $\widehat{K}^*$ on values of modular functions to the action of $\mathrm{GL}_2(\widehat{\mathbf{Q}})$ on the modular functions themselves.

$g = 2$: I have been making Shimura's reciprocity law for $g = 2$ more explicit and have some ideas for "smaller functions".

The "embedding problem" (Goren-Lauter)

Given a quartic CM field K (not containing an imag. quadr. field). What are the primes p such that the following exist?

- a maximal order R in the quaternion algebra $B_{p,\infty}/\mathbf{Q}$,
- 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

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \mapsto \begin{pmatrix} \overline{\alpha} & \overline{\gamma} N(\mathfrak{a})^{-1} \\ \overline{\beta} N(\mathfrak{a}) & \overline{\delta} \end{pmatrix}.$$

Partial answer: we know the splitting behaviour of p in the normal closure of K and we know $p < c \cdot \mathrm{disc} K$. [GL 2006]