Igusa class polynomials

Marco Streng

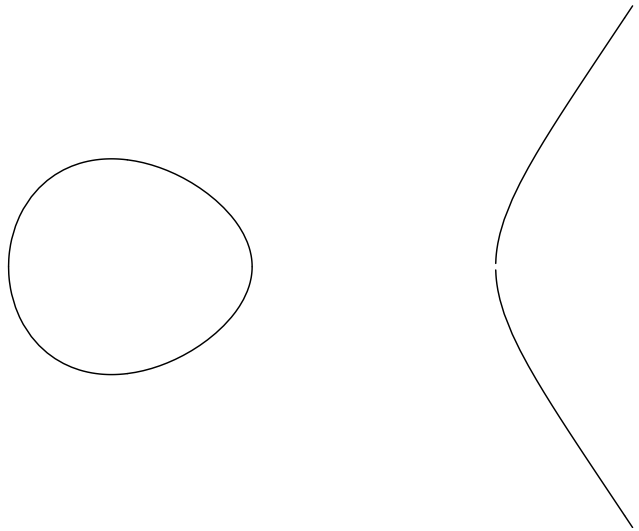
Universiteit Leiden

DIAMANT/EIDMA symposium
Lunteren, November 2009

Elliptic curves

- An *elliptic curve* E/k ($\mathrm{char}(k) \neq 2$) is a smooth projective curve

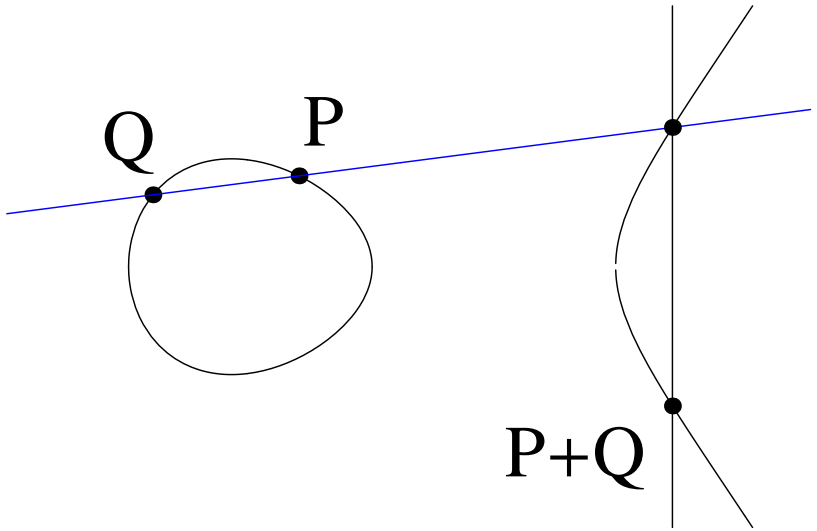
$$y^2 = x^3 + ax^2 + bx + c.$$



Elliptic curves

- An *elliptic curve* E/k ($\mathrm{char}(k) \neq 2$) is a smooth projective curve

$$y^2 = x^3 + ax^2 + bx + c.$$



- $E(k)$ is an abelian group.

Endomorphisms

- $\mathrm{End}(E) = \{(\text{algebraic group}) \text{ morphisms } E \to E\}$
- Examples of elements:
  - For all $n \in \mathbf{Z}$, we have
$$n : P \mapsto P + \cdots + P.$$
  - If $E : y^2 = x^3 + x$ and $i^2 = -1$ in k, then we have
$$i : (x, y) \mapsto (-x, iy).$$
  - 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

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

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

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 $p = \pi\overline{\pi}$ in $\mathcal{O}_K$, then $(H_K \bmod p)$ 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 $= \pi$.
- We get

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

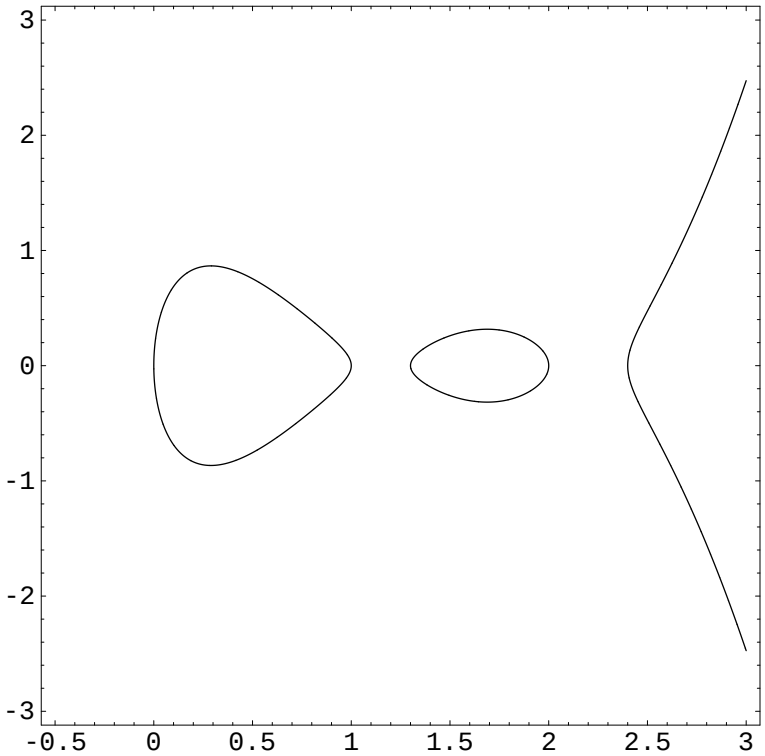
Curves of genus 2

Definition (char.$\neq 2$)

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

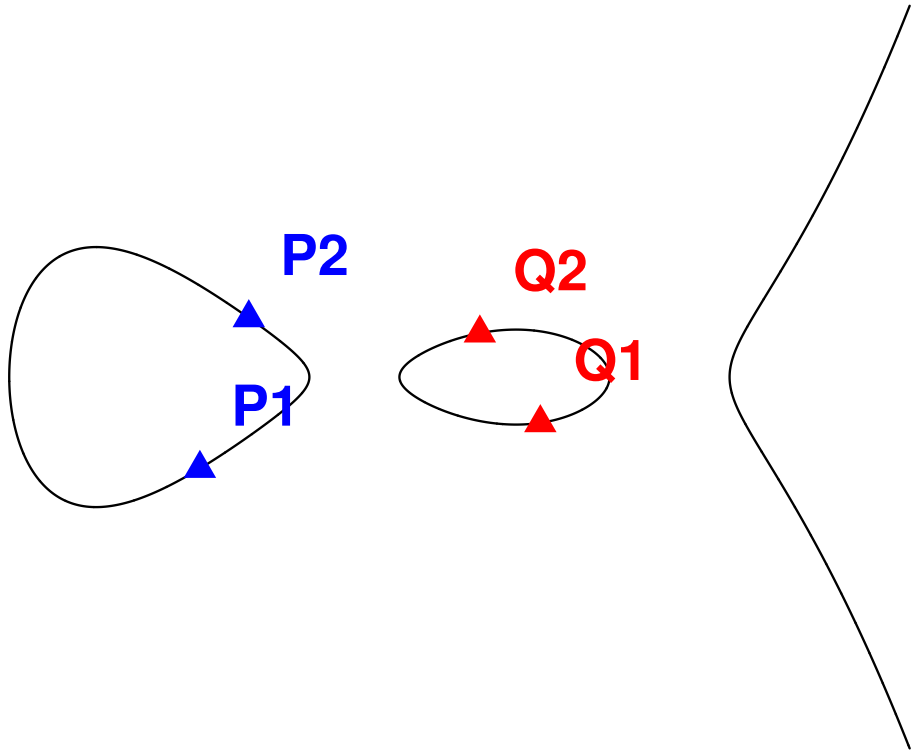
$$y^2 = f(x), \quad \deg(f) \in \{5, 6\},$$

where f has no double roots.



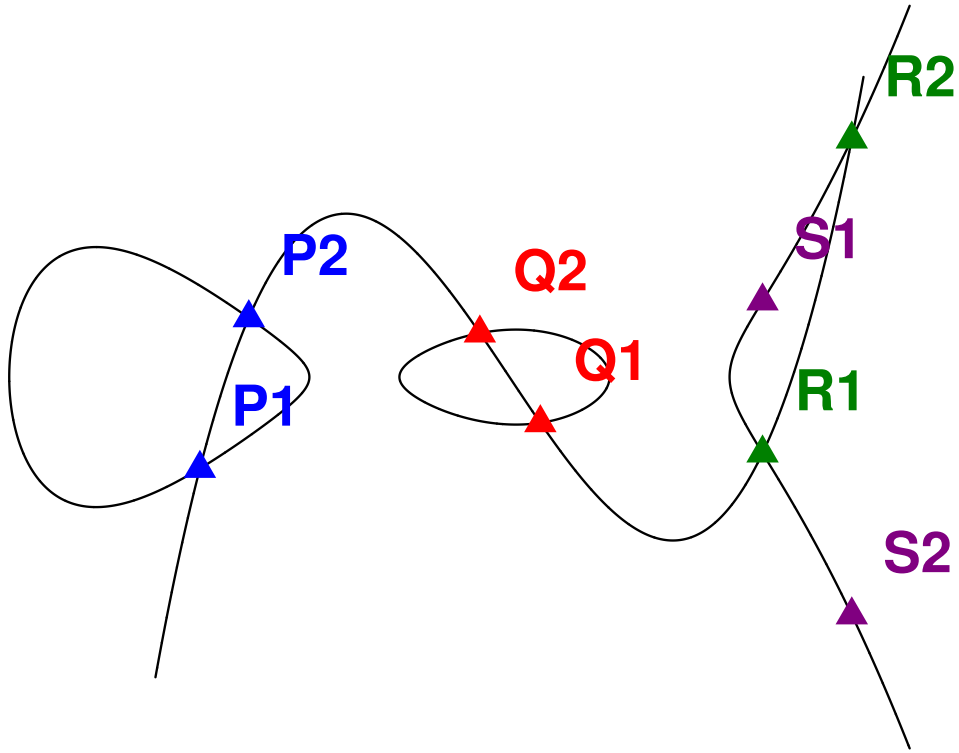
The group law on the Jacobian

Group of (equivalence classes of) pairs of points: the Jacobian.



The group law on the Jacobian

Group of (equivalence classes of) pairs of points: the Jacobian.



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.
- *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 $\mathcal{O}_K$.
- Roots generate class fields. Useful? Efficient?
- If $p = \pi\overline{\pi}$ in $\mathcal{O}_K$, construct curve C with

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

Computing Hilbert class polynomials

We have

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

Write $\mathfrak{a} = \mathbf{Z} + \tau\mathbf{Z}$ and let $q = \exp(2\pi i\tau)$.
We have $j(\mathbf{C}/\mathfrak{a}) = j(q) = q^{-1} + 744 + 196884q + \cdots$.
We compute

$$H_K = \prod_{[\mathfrak{a}] \in \mathcal{CL}_K} (X - j(\mathbf{C}/\mathfrak{a})) \in \mathbf{Z}[X].$$

We have

$$|j(q)| \approx |q|^{-1} = \exp(2\pi \mathrm{Im}(\tau)) \quad \text{and} \quad \sqrt{\frac{3}{4}} \leq \mathrm{Im}(\tau) \leq \frac{1}{2}\sqrt{|D|}.$$

Computing Igusa class polynomials

- Denominators bounded (Goren-Lauter)
- Analogues of $\mathrm{Im}(\tau) \leq \frac{1}{2}\sqrt{|D|}$ and $j(q) \approx q^{-1}$.

Use this and make the algorithm more explicit, get:

Theorem

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

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

The size of the output is between

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