

# Igusa class polynomials

Marco Streng

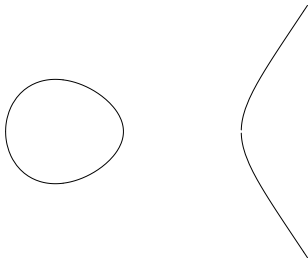
Universiteit Leiden

*DIAMANT/EIDMA symposium*  
Lunteren, November 2009

# Elliptic curves

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

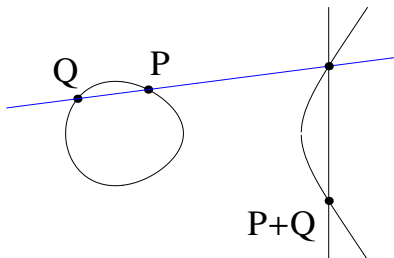
$$y^2 = x^3 + ax^2 + bx + c.$$



# Elliptic curves

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

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



- ▶  $E(k)$  is an abelian group.

# Endomorphisms

- ▶  $\text{End}(E) = \{(\text{algebraic group}) \text{ morphisms } E \rightarrow E\}$
- ▶ 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

$$\text{Frob} : (x, y) \mapsto (x^q, y^q).$$

# The Hilbert class polynomial

The *j-invariant* is

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

$$j(E) = j(F) \iff E \cong_k F$$

## Definition

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

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

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  $p = \pi\bar{\pi}$  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  $\text{Frob} = \pi$ .
- ▶ We get

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

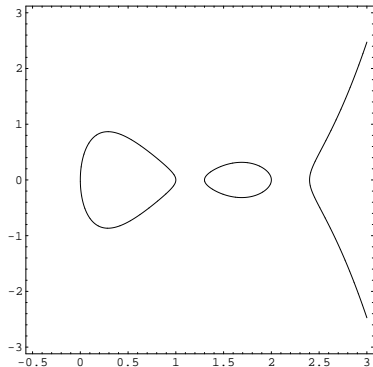
## Curves of genus 2

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

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

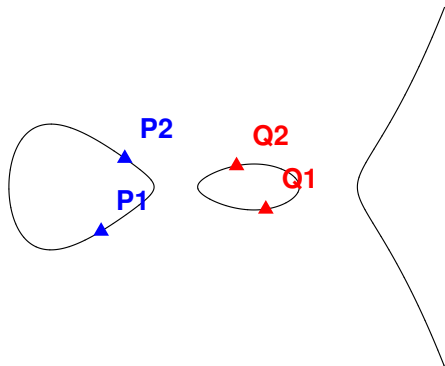
$$y^2 = f(x), \quad \deg(f) \in \{5, 6\},$$

where  $f$  has no double roots.



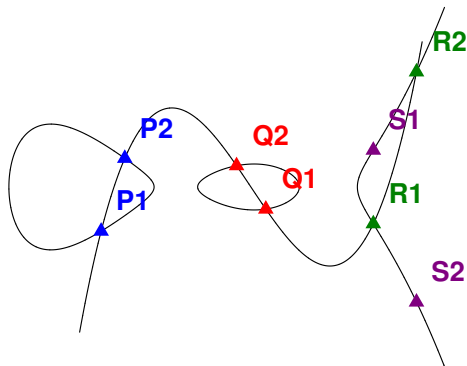
# The group law on the Jacobian

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  $\text{End}(E)$  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  $\text{End}(J(C))$  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  $p = \pi\bar{\pi}$  in  $\mathcal{O}_K$ , construct curve  $C$  with

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

# Computing Hilbert class polynomials

We have

$$\begin{aligned} \mathcal{CL}_K &\longleftrightarrow \frac{\{E/\mathbf{C} : \text{End}(E) \cong \mathcal{O}_K\}}{\cong} \\ [a] &\longmapsto \mathbf{C}/a. \end{aligned}$$

Write  $a = \mathbf{Z} + \tau\mathbf{Z}$  and let  $q = \exp(2\pi i\tau)$ .

We have  $j(\mathbf{C}/a) = j(q) = q^{-1} + 744 + 196884q + \dots$ .

We compute

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

We have

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

# Computing Igusa class polynomials

- ▶ Denominators bounded (Goren-Lauter)
- ▶ Analogues of  $\text{Im}(\tau) \leq \frac{1}{2}\sqrt{|D|}$  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

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

The size of the output is between

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