

# Class invariants in a non-archimedean setting

Reinier Bröker  
Universiteit Leiden



XXIVth Journées Arithmétiques, Marseille  
July 7, 2005

## Topic of today's talk

For an imaginary quadratic number field  $K$ , we can describe the Hilbert class field  $H$  using *complex multiplication*.

Let  $D = \text{disc}(K)$  and define  $\text{Ell}_D(\mathbf{C}) =$   
 $\{\text{elliptic curve } E/\mathbf{C} : \text{End}(E) \cong \mathcal{O}\} / \cong$

### **Theorem.**

We have  $H = K(j(E))$  for  $[E] \in \text{Ell}_D(\mathbf{C})$ .  
Furthermore:

$$f_D = \prod_{[E] \in \text{Ell}_D(\mathbf{C})} (X - j(E)) \in \mathbf{Z}[X].$$

We want to compute  $f_D$  (the *Hilbert class polynomial*) explicitly. It is the minimal polynomial of  $j(E)$  over  $\mathbf{Q}$ .

## The classical algorithm

- list reduced binary quadratic forms  $ax^2 + bxy + cy^2$  of discriminant  $b^2 - 4ac = D$ ;
- compute

$$f_D = \prod_{[a,b,c]} \left( X - j\left(\frac{-b + \sqrt{D}}{2a}\right) \right) \in \mathbf{Z}[X].$$

Here  $j$  is the complex analytic modular function  $\mathbf{H} \rightarrow \mathbf{C}$  with Fourier expansion  $j(\tau) = 1/q + 744 + \dots$  in  $q = \exp(2\pi i\tau)$ .

We compute  $j\left(\frac{-b + \sqrt{D}}{2a}\right)$  with high enough accuracy to be able to round the coefficients of  $f_D$  to the nearest integer.

# Problems

1. We may have *rounding errors* when expanding the product

$$f_D = \prod_{[a,b,c]} \left( X - j\left(\frac{-b + \sqrt{D}}{2a}\right) \right) \in \mathbf{Z}[X].$$

2. The running time is  $O(|D|^{1+o(1)})$ . Even for moderately sized discriminants, the coefficients of  $f_D$  are *huge*.

Example: for  $D = -31$ , we get

$$\begin{aligned} f_{-31} = & X^3 + 39491307X^2 \\ & -58682638134X \\ & +1566028350940383 \in \mathbf{Z}[X]. \end{aligned}$$

## Solution to first problem

- take a prime  $p$  that splits completely in  $H$ , i.e., we have an embedding  $H \hookrightarrow \mathbf{Q}_p$ ;
- put  $\text{Ell}_D(\mathbf{Q}_p) = \{E/\mathbf{Q}_p : \text{End}(E) \cong \mathcal{O}\} / \cong_{\mathbf{Q}_p}$  ;
- we have

$$f_D = \prod_{[E] \in \text{Ell}_D(\mathbf{Q}_p)} (X - j(E)) \in \mathbf{Z}[X];$$

- $\text{Ell}_D(\mathbf{Q}_p)$  is computed via a  $p$ -adic lifting process.
- The classical algorithm only uses the Fourier-expansion of  $j$ ; for the  $p$ -adic algorithm we use more geometry.

**This solves problem 1.**

## Second problem

2. The running time is  $O(|D|^{1+o(1)})$ . Even for moderately sized discriminants, the coefficients of  $f_D$  are *huge*.

Example: for  $D = -31$ , we get

$$\begin{aligned} f_{-31} = & X^3 + 39491307X^2 \\ & - 58682638134X \\ & + 1566028350940383 \in \mathbf{Z}[X]. \end{aligned}$$

The running time can't be helped since the problem is intrinsically exponential.

We can use other functions than  $j$  to save a constant factor in the size of the coefficients of  $f_D$ .

In this talk we focus on  $\gamma_2$ , which yields the polynomial

$$f_{-31}^{\gamma_2} = X^3 + 342X^2 + 837X + 116127.$$

## The function $\gamma_2$

- $j$  has a holomorphic cube root  $\gamma_2 : \mathbf{H} \rightarrow \mathbf{C}$  with integral Fourier expansion;
- $\gamma_2$  is a modular function of level 3;
- write  $\mathcal{O} = \mathbf{Z}[\tau]$  with  $\tau \in \mathbf{H}$ . Then we have  $\gamma_2(\tau) \in H_3$ , with  $H_3$  the ray class field of conductor 3;
- sometimes  $\gamma_2(\tau)$  is a *class invariant*, i.e.,  $\gamma_2(\tau) \in H$ ;
- for  $3 \nmid D$ , we have  $\gamma_2(\tau) \in H$  if  $\tau \in \mathbf{H}$  satisfies  $\tau + \bar{\tau} \equiv 0 \pmod{3}$ ;
- tool for investigating class invariants:  
Shimura reciprocity law (1970).

## Class invariants over $\mathbf{C}$ and over $\mathbf{Q}_p$

- suppose  $3 \nmid D$ . Shimura reciprocity law gives us a list of  $\#\text{Cl}(\mathcal{O})$  points  $\tau_I \in \mathbf{H}$  with

$$f_D^{\gamma_2} = \prod_{[I] \in \text{Cl}(\mathcal{O})} (X - \gamma_2(\tau_I)) \in \mathbf{Z}[X];$$

---

- need a  $p$ -adic substitute for the computation of  $\gamma_2(\tau_I)$  via the  $q$ -expansion of  $\gamma_2$ ;
- for the  $j$ -function we replaced the computation of  $j(\tau)$  via its  $q$ -expansion by a more geometric approach;
- $j$  is an element of the function field of the modular curve  $X(1)$  over  $\mathbf{Q}$ ;
- $\gamma_2$  is an element of the function field of the modular curve  $X(3)$  over  $\mathbf{Q}(\zeta_3)$ .

## Geometric $\gamma_2$

Take an equation  $Y^2 = X^3 + aX + b$  for  $E/\mathbf{Q}_p$ .

Let  $c_1, \dots, c_4 \in \overline{\mathbf{Q}}_p$  be the roots of the 3-division polynomial. Then:

$$\frac{-48a}{2a - 3(c_1c_2 + c_3c_4)}$$

is a cube root of  $j(E)$ .

Value depends on an *ordering* of  $c_1, \dots, c_4$ .  
We get *three* distinct cube roots of  $j$ .

There is no obvious choice for the cube root  $\gamma_2$ .

For  $p \equiv 1 \pmod{3}$ , all three cube roots of  $j$  are defined over  $\mathbf{Q}_p$ .

## Example: $\gamma_2$ and $D = -31$

- work over  $\mathbf{Q}_p$  with  $p = 67 = 6^2 + 31$ ;
- there is a curve  $E_{-31}/\mathbf{Q}_p$  with  $j$ -invariant

$$j(E_{-31}) = 3 + 33p - 16p^2 + O(p^3)$$

and with endomorphism ring  $\mathcal{O} = \mathcal{O}_{-31}$ ;

- we compute  $j(E_{-31})$  with only one-third of the accuracy as we would have done for  $f_{-31}$ ;
- $j(E_{-31})$  has three cube roots in  $\mathbf{Q}_p$ :

$$\eta_1 = 18 + O(p);$$

$$\eta_2 = 53 + O(p);$$

$$\eta_3 = 63 + O(p);$$

- we need to find out which one lies in  $H$ ;

## Action of $\mathcal{O}$ on cube roots of $j$

- a cube root lies in  $H$  if and only if it is invariant under

$$\mathrm{Gal}(H_3/H) \cong (\mathcal{O}/3\mathcal{O})^*/\mathcal{O}^* \cong \mathbf{Z}/4\mathbf{Z} \cong \langle \bar{\alpha} \rangle$$

with  $\alpha = \frac{-1+\sqrt{-31}}{2}$  (we have  $\mathfrak{p}_2^3 = (\alpha)$ );

- choose a Weierstraß equation for  $E_{-31}/\mathbf{Q}_p$ :

$$Y^2 = X^3 + aX + b;$$

- compute the 4 roots  $c_1, \dots, c_4$  of the 3-division polynomial for  $E$  and compute 3-torsion points  $P_i$  with  $x$ -coordinate  $c_i$ ;
- recall: a cube root of  $j(E_{-31})$  is given by

$$\frac{-48a}{2a - 3(c_1c_2 + c_3c_4)};$$

## Action of $\mathcal{O}$ on cube roots of $j$

- for  $I \subseteq \mathcal{O}$  an ideal, there is an isogeny

$$\varphi_I : E_{-31} \rightarrow E_{-31}^I$$

with kernel  $E_{-31}[I] = \bigcap_{f \in I} \ker f$ ;

- algorithmic description of  $\varphi_I$ :
  - ◇ compute a polynomial  $f_I \in \mathbf{Q}_p[X]$  whose roots are the  $x$ -coordinates of  $E_{-31}[I]$  (using Atkin-Elkies techniques);
  - ◇ find an explicit isogeny  $\varphi_I$  using Vélu's formulas;
- we have  $j(E_{-31})^{[I, H/K]} = j(E_{-31}^I)$ ;

## Action of $\mathcal{O}$ on cube roots of $j$

- for  $3 \nmid I$ , we get an isomorphism

$$\varphi_I : E_{-31}[3] \xrightarrow{\sim} E_{-31}^I[3]$$

and hence a natural bijection

$$\varphi_I : \{\eta_1, \eta_2, \eta_3\} \xrightarrow{\sim} \{\text{cube roots of } j(E_{-31}^I)\};$$

- for a cube root

$$\eta = \frac{-48a}{2a - 3(c_1c_2 + c_3c_4)}$$

we have

$$\eta^{[I, H_3/H]} = \varphi_I(\eta) = \frac{-48a'}{2a' - 3(c'_1c'_2 + c'_3c'_4)}$$

with  $c'_i = x(\varphi_I(P_i))$  and  
 $E_{-31}^I : Y^2 = X^3 + a'X + b'$ ;

## Action of $\mathcal{O}$ on cube roots of $j$

- applying this to  $I = \left(\frac{-1+\sqrt{-31}}{2}\right) = \mathfrak{p}_2^3$  we get

$$\begin{aligned}\eta_1 &\xrightarrow{\varphi_I} \eta_1; \\ \eta_2 &\xrightarrow{\varphi_I} \eta_3; \\ \eta_3 &\xrightarrow{\varphi_I} \eta_2.\end{aligned}$$

Hence  $\eta_1 = 18 + O(p)$  is a class invariant.  
(Note:  $\varphi_{\mathfrak{p}_2}$  is just a 2-isogeny in this case.)

---

- we have  $\text{Cl}(\mathcal{O}) \cong \mathbf{Z}/3\mathbf{Z} \cong \langle [\mathfrak{p}_2] \rangle$ ;
- action of  $\mathfrak{p}_2$  on  $\eta_1$  is as before:

$$\eta_1^{[\mathfrak{p}_2, H/K]} = \varphi_{\mathfrak{p}_2}(\eta_1);$$

- we compute the conjugates and expand:

$$\begin{aligned}f_{-31}^{\gamma_2} &= \prod_{i=1}^3 (X - \varphi_{\mathfrak{p}_2}^i(\eta_1)) = \\ &X^3 + 342X^2 + 837X + 116127 \in \mathbf{Z}[X].\end{aligned}$$

## Other functions and larger discriminants

- method works for any modular function  $f$  of level  $N \geq 1$ ;
- writing  $f$  in terms of  $N$ -torsion points is impractical, since  $N$  may be large (e.g. the Weber- $f$  has level 48);
- working with explicit isogenies is impractical if we need prime ideals of large ( $> 30$ ) norm;
- both these problems can be solved by working with *modular equations*;
- current record:  $D \approx -10^{10}$ , using Weber- $f$ .