

p -adic class invariants

Reinier Bröker
University of Calgary

Québec-Vermont Number Theory Seminar
February 2007

Explicit class field theory

Abelian extensions of a number field K are described by *class field theory*.

It is a classical problem to ‘explicitly compute’ these extensions.

Theorem. *Every finite abelian extension of $K = \mathbf{Q}$ is contained in a cyclotomic extension.*

Only for \mathbf{Q} and for imaginary quadratic K , there is a satisfactory answer.

We will focus on the ring class fields of imaginary quadratic fields.

CM-theory

- Let K be an imaginary quadratic field, and $\mathcal{O} = \mathcal{O}_\Delta$ an order in K .
- The ring class field $H_{\mathcal{O}}$ for \mathcal{O} is an abelian extension of K with Galois group isomorphic to $\text{Pic}(\mathcal{O})$ via the Artin map.

Theorem. *We have*

$$H_{\mathcal{O}} = K(j(\mathbf{C}/\mathcal{O}))$$

and the Galois action of $\text{Gal}(H_{\mathcal{O}}/K) \cong \text{Pic}(\mathcal{O})$ is given by

$$j(\mathbf{C}/\mathcal{O})^{[\mathfrak{a}, H_{\mathcal{O}}/K]} = j(\mathbf{C}/\mathfrak{a}).$$

Furthermore: the minimal polynomial P_Δ of $j(\mathbf{C}/\mathcal{O})$ over \mathbf{Q} has integer coefficients.

Classical algorithm to compute P_Δ

- List reduced binary quadratic forms $aX^2 + bXY + cY^2$ of discriminant $b^2 - 4ac = \Delta$.
- Compute

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

Here j is the complex analytic modular function $\mathbf{H} \rightarrow \mathbf{C}$ with Fourier expansion $j(z) = 1/q + 744 + 196884q + \dots$ in $q = \exp(2\pi iz)$.

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

Today. p -adic algorithm to compute P_Δ for $\Delta < -4$.

The fundamental action

- L field, E/L elliptic curve with $\text{End}_L(E) \cong \mathcal{O} \stackrel{\text{def}}{=} \mathcal{O}_\Delta$.
- For $I \subset \text{End}_L(E)$ an ideal, coprime to $\text{char}(L)$, put

$$E[I] \stackrel{\text{def}}{=} \{P \in E(\overline{L}) \mid \forall \alpha \in I : \alpha(P) = 0\}.$$

- There is a curve E^I/L and an isogeny $E \rightarrow E^I$ with kernel $E[I]$.
- Put $\text{Ell}_\Delta(L) \stackrel{\text{def}}{=} \{j \in L \mid \exists E/L : j(E) = j, \text{End}_L(E) = \mathcal{O}\}$.
- The Picard group $\text{Pic}(\mathcal{O})$ acts on $\text{Ell}_\Delta(L)$ via

$$j(E) \rightarrow j(E^I).$$

The Hilbert class polynomial

- Recall: for E/\mathbf{C} with $\text{End}(E) = \mathcal{O}$, we have $j(E) \in H_{\mathcal{O}}$
- We have $P_{\Delta} = \prod_{j \in \text{Ell}_{\Delta}(H)} (X - j) = \prod_{\mathfrak{a} \in \text{Pic}(\mathcal{O})} (X - j(\mathbf{C}/\mathcal{O})^{\mathfrak{a}}) \in \mathbf{Z}[X]$

Take a prime p that splits completely in $H_{\mathcal{O}}$, i.e., we have $H_{\mathcal{O}} \hookrightarrow \mathbf{Q}_p$.

- $P_{\Delta} = \prod_{j \in \text{Ell}_{\Delta}(\mathbf{Q}_p)} (X - j) \in \mathbf{Z}[X]$
- $P_{\Delta} \bmod p = \prod_{j \in \text{Ell}_{\Delta}(\mathbf{F}_p)} (X - j) \in \mathbf{F}_p[X]$

Size of p

Need a small prime p splitting completely in $H_{\mathcal{O}}$.

Class field theory: p splits in $H_{\mathcal{O}} \iff p$ splits in principal ideals in \mathcal{O} .

Find p by looking for solution to $t^2 - Du^2 = 4p$ for $t, u = 0, 1, 2, \dots$

Lemma. *(Under GRH) The smallest splitting prime p satisfies*

$$p = O(|D|(\log |D|)^4).$$

Proof requires the bound $\text{disc}(H/\mathbf{Q}) \leq |D|^{h(D)} \leq |D|^{\sqrt{|D|} \log |D|}$.

Requires work for non-fundamental D .

Finding a curve of prescribed endomorphism ring

We have $t^2 - 4p = Du^2$, with $u = [\mathcal{O} : \mathbf{Z}[F_p]] \in \mathbf{Z}_{\geq 1}$.

The curve we are looking for has $p + 1 \pm t$ points. Only count points on curves E with $(p + 1 \pm t)P = 0$ for random point $P \in E(\mathbf{F}_p)$.

For $u = 1$, we are done. However: $D \equiv 1 \pmod{8} \implies u$ is even.

Lemma. *If $[\mathcal{O} : \mathbf{Z}[F_p]] = 2$, then: $\text{End}(E) = \mathcal{O} \iff E[2]$ is defined over \mathbf{F}_p . For $E[2](\mathbf{F}_p) = \{0, P\}$, the curve $E/\langle P \rangle$ has endomorphism ring \mathcal{O} .*

‘In practice’: always have $u = 1, 2$.

For theoretical analysis: compute $\text{End}(E)$ using Kohel’s algorithm, remove the conductor u using Fouquet-Morain’s algorithm.

The canonical lift

We have $j(\overline{E}) \in \text{Ell}_\Delta(\mathbf{F}_p)$.

Elements of $\text{Ell}_\Delta(\mathbf{Q}_p)$ are integral: lie in \mathbf{Z}_p .

Unique $j(\tilde{E}) \in \text{Ell}_\Delta(\mathbf{Q}_p)$ with $j(\tilde{E}) \bmod p = j(\overline{E})$ is called the *canonical lift* of $j(\overline{E})$.

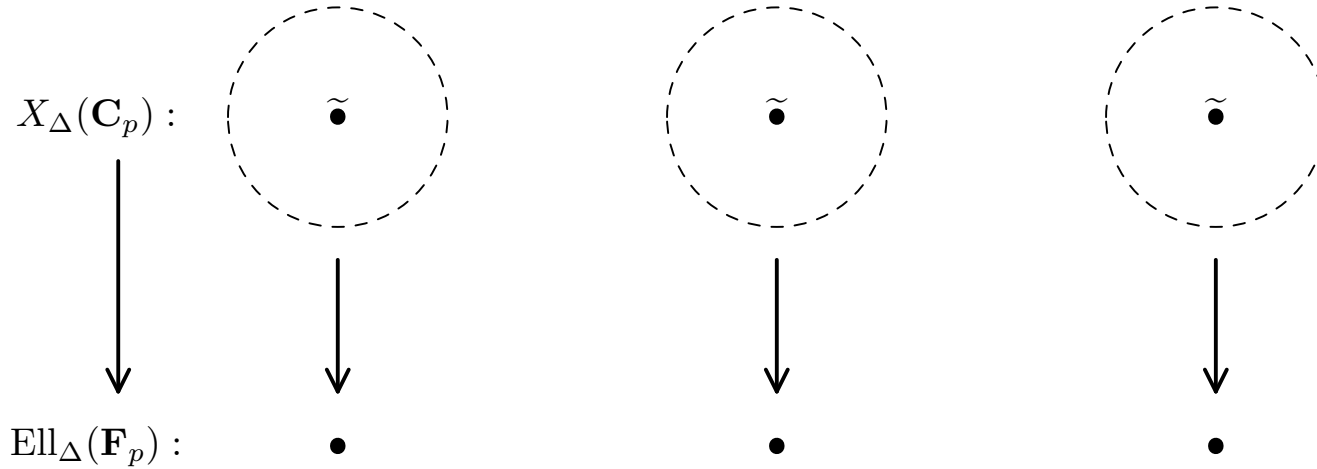
We need to compute $j(\tilde{E}) \in \mathbf{Z}_p$ with high enough accuracy.

We have:

$$P_\Delta = \prod_{[\mathfrak{a}] \in \text{Pic}(\mathcal{O})} (X - j(\tilde{E})^{\mathfrak{a}}) \in \mathbf{Z}[X].$$

Computing the canonical lift

Put $X_\Delta(\mathbf{C}_p) \stackrel{\text{def}}{=} \{j \in \mathbf{C}_p \mid \bar{j} \in \text{Ell}_\Delta(\mathbf{F}_p)\} \supset \text{Ell}_\Delta(\mathbf{Q}_p)$.



For $I \subset \mathcal{O}$ of norm N , coprime to p , define

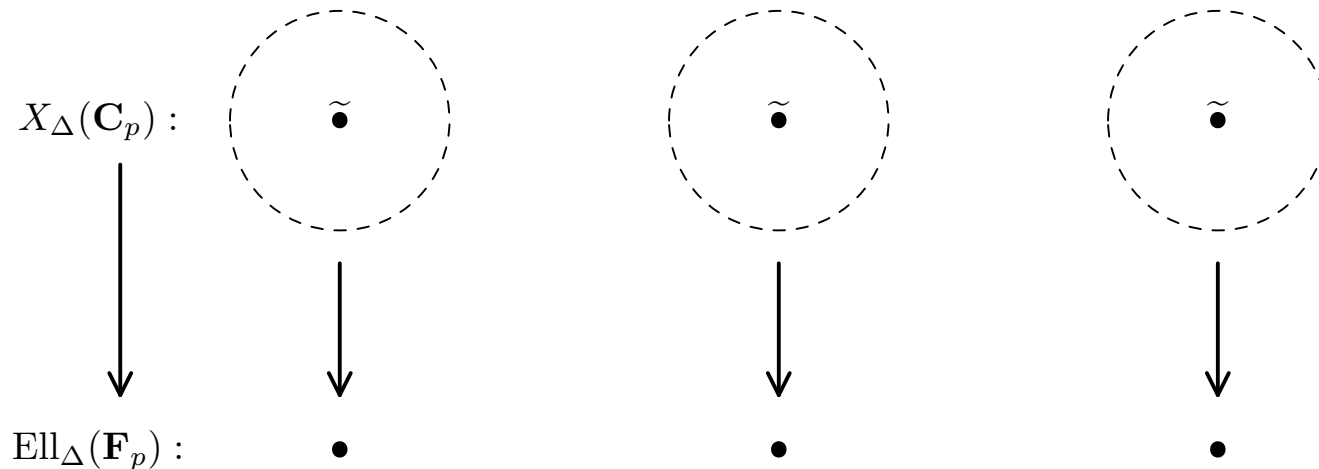
$$\begin{aligned} \rho_I : \text{Ell}_\Delta(\mathbf{Q}_p) &\rightarrow \text{Ell}_\Delta(\mathbf{Q}_p) \\ j(E) &\mapsto j(E^I). \end{aligned}$$

Couveignes-Henocq: ρ_I has a natural extension to

$$\rho_I : X_\Delta(\mathbf{C}_p) \rightarrow X_\Delta(\mathbf{C}_p).$$

Definition of ρ_I

- For $j \in X_\Delta(\mathbf{C}_p)$, take a curve E/\mathbf{C}_p with $j(E) = j$ that has good reduction mod p . Write \overline{E} for its reduction.
- We have a natural isomorphism $\varphi : E[N] \xrightarrow{\sim} \overline{E}[N]$.
- Put $\rho_I(j) \stackrel{\text{def}}{=} j(E/\varphi^{-1}(\overline{E}[I]))$.



Computing the canonical lift

Restrict to *principal* ideals $I = (\alpha)$. The map ρ_α then has $\text{Ell}_\Delta(\mathbf{Q}_p)$ as unique *fixed points*.

Theorem. *If $\mathcal{O}/(\alpha)$ is cyclic as abelian group, then $\rho_\alpha : X_\Delta(\mathbf{C}_p) \rightarrow X_\Delta(\mathbf{C}_p)$ is analytic, i.e., it can locally be given by a power series.*

Sketch of proof. We have maps

$$j, \rho_\alpha : X_\Delta(\mathbf{C}_p) \rightarrow X_\Delta(\mathbf{C}_p) \subset \mathbf{C}_p.$$

At $P = (\tilde{E}, \tilde{E}[(\alpha)])$, the ring $\hat{\mathcal{O}}_{Y_0(N)_{\mathbf{Q}_p, P}}$ is a complete DVR over \mathbf{Q}_p .

Uniformizers: $j - j(\tilde{E})$ and $\rho_\alpha - \rho_\alpha(j(\tilde{E}))$.

Some geometry gives

$$\rho_\alpha - \rho_\alpha(j(\tilde{E})) = \sum_{i \geq 1} c_i (j - j(\tilde{E}))^i, \quad c_i \in \mathbf{Z}_p.$$

Computing the canonical lift

Lift $j \in \text{Ell}_\Delta(\mathbf{F}_p)$ randomly to $j_1 \in X_\Delta(\mathbf{C}_p)$.

We use ‘Newton iteration’ to converge to the *fixed point* $\tilde{j} \in \text{Ell}_\Delta(\mathbf{Q}_p)$ of the analytic map $\rho_\alpha : X_\Delta(\mathbf{C}_p) \rightarrow X_\Delta(\mathbf{C}_p)$.

Theorem. *The derivative of ρ_α in $\tilde{j} \in \text{Ell}_\Delta(\mathbf{Q}_p)$ is given by $\alpha/\bar{\alpha}$.*

For $\alpha/\bar{\alpha} - 1 \in \mathbf{Z}_p^*$, the process

$$\dot{j}_{k+1} = \dot{j}_k - \frac{\rho_\alpha(\dot{j}_k) - \dot{j}_k}{\alpha/\bar{\alpha} - 1} \quad \text{for } k \in \mathbf{Z}_{\geq 1}$$

converges to $\tilde{j} \in \text{Ell}_\Delta(\mathbf{Q}_p)$.

Computing P_Δ

Step 1. Find a small prime p that splits completely in $H_{\mathcal{O}}$.

Step 2. Find a curve $\overline{E}/\mathbf{F}_p$ with $\text{End}(\overline{E}) = \mathcal{O}$.

Step 3. Find a suitable smooth $\alpha \in \mathcal{O}$ to use in Step 4.

Step 4. Lift $j(\overline{E}) \in \mathbf{F}_p$ to its canonical lift $j(\tilde{E}) \in \mathbf{Q}_p$ with high enough accuracy.

Step 5. Compute the conjugates of $j(\tilde{E})$ under the action of $\text{Pic}(\mathcal{O})$.

Step 6. Expand $P_\Delta = \prod_{[I] \in \text{Pic}(\mathcal{O})} (X - j(\tilde{E})^I) \in \mathbf{Z}[X]$.

Example: $D = -639 = -3^2 \cdot 71$

We have $D \equiv 1 \pmod{8}$, so no solutions to $4p = t^2 - D$.

Smallest $t > 0$ with $(t^2 - D)/4$ prime is $t = 4$, yields $p = 643$.

Test if curves $E_a : Y^2 = X^3 + aX - a$ with $a \in \mathbf{F}_p$ have $p + 1 \pm t$ points. Reason: $P = (1, 1) \in E_a(\mathbf{F}_p)$ comes ‘for free’.

The curve

$$\overline{E} : Y^2 = X^3 + 89X - 89 \quad \text{with} \quad j(\overline{E}) = 295$$

has $p + 1 - t = 640 = 2^7 \cdot 5$ points.

Computing the endomorphism ring

We have

$$\mathbf{Z}[F_p] \stackrel{2}{\subset} \mathcal{O}_\Delta \stackrel{3}{\subset} \mathcal{O}_{\max},$$

and we need to compute $\text{End}(\overline{E})$.

The polynomial $X^3 - 89X - 89 \in \mathbf{F}_p[X]$ splits over \mathbf{F}_p . We derive: $\mathcal{O}_\Delta \subseteq \text{End}(\overline{E})$.

Prime 3 splits in \mathcal{O}_{\max} , so $\text{End}(\overline{E}) = \mathcal{O}_{\max} \implies$ at least two 3-isogenies defined over \mathbf{F}_p .

Modular polynomial $\Phi_3(X, Y) \in \mathbf{F}_p[X, Y]$ parametrizes 3 isogenies. Compute: $\gcd(\Phi_3(X, j(\overline{E})), X^p - X) = X - 429 \in \mathbf{F}_p[X]$.

Conclude: $\overline{E}/\mathbf{F}_p$ with $j(\overline{E}) = 295$ has $\text{End}(\overline{E}) = \mathcal{O}_\Delta$.

Setting the parameters

Need to compute $j(\tilde{E}) \in \mathbf{Z}_p$ with

$$k = \frac{\pi \sqrt{|D|}}{\log p} \sum_{[a,b,c] \in \text{Pic}(\mathcal{O})} \frac{1}{a} \approx 44$$

p -adic digits precision. To be safe, we take 45 digits.

As smooth element $\alpha \in \mathcal{O} \setminus \mathbf{Z}$ for $\rho_\alpha : X_\Delta(\mathbf{C}_p) \rightarrow X_\Delta(\mathbf{C}_p)$ we take

$$\alpha = \pi_p - 108, \text{ with } \pi_p = \frac{4 + \sqrt{|D|}}{2}, \text{ of norm } N(\alpha) = 11874 = 5^4 \cdot 19.$$

Factor

$$(\alpha) = \mathfrak{p}_5^4 \mathfrak{p}_{19} = (5, \pi_p - 3)^4 \cdot (19, \pi_p - 13).$$

Computing $\bar{\rho}_\alpha$

Compute $\bar{\rho}_\alpha : \text{Ell}_\Delta(\mathbf{F}_p) \rightarrow \text{Ell}_\Delta(\mathbf{F}_p)$ one prime ideal at a time.

The j -invariant $j(\bar{E}^{\mathfrak{p}_5})$ is a root of $\Phi_5(X, j(\bar{E}))$. This polynomial has two roots: 449 and 532.

Can prove: under ‘harmless conditions’ it always has two roots.

We *guess* $j(\bar{E}^{\mathfrak{p}_5}) = 449$. Use ‘Atkin-Elkies techniques’ to compute the subgroup $C \subset \bar{E}[5]$ with $j(E/C) = 449$.

The x -coordinates of points in C are roots of

$$\bar{f}_C = X^2 + 614X + 471 \in \mathbf{F}_p[X].$$

Checking $j(\overline{E}^{\mathfrak{p}_5}) = 449$

We have $\mathfrak{p}_5 = (5, \pi_p - 3)$.

Need to test

$$(x^p, y^p) = 3 \cdot (x, y) \quad (x, y) \in C \subset \overline{E}[5].$$

Compute (X^p, Y^p) and $3 \cdot (X, Y)$ in the ring

$$\mathbf{F}_p[X, Y]/(\overline{f}_C, Y^2 - X^3 - 89X + 89).$$

They are the same, hence:

$$\overline{\rho}_{\mathfrak{p}_5}(j(\overline{E})) = j(\overline{E}^{\mathfrak{p}_5}) = 449 \in \mathbf{F}_p.$$

Computing $\bar{\rho}_\alpha$

The value $\bar{\rho}_{\mathfrak{p}_5}(j(\bar{E}^{\mathfrak{p}_5})) = \bar{\rho}_{\mathfrak{p}_5}(449)$ is easier to compute.

The polynomial $\Phi_5(X, 449)$ has two roots in \mathbf{F}_p : 73 and $295 = j(\bar{E})$.

No surprise: $\mathfrak{p}_5 \bar{\mathfrak{p}}_5 = (5)$ and $j(\bar{E}^{(5)}) = j(\bar{E})$.

Cycle for $(\alpha) = \mathfrak{p}_5^4 \mathfrak{p}_{19}$ becomes

$$295 \xrightarrow{\mathfrak{p}_5} 449 \xrightarrow{\mathfrak{p}_5} 73 \xrightarrow{\mathfrak{p}_5} 55 \xrightarrow{\mathfrak{p}_5} 328 \xrightarrow{\mathfrak{p}_{19}} 295.$$

Cycle is closed because $(\alpha) \subseteq \mathcal{O}_\Delta = \text{End}(\bar{E})$.

Lifting the cycle to \mathbf{Q}_p

Take arbitrary lift of $\overline{E}/\mathbf{F}_p$ to \mathbf{Q}_p . We take

$$E_1 : Y^2 = X^3 - 89X + 89 \quad \text{with} \quad j(E_1) = 295 - 233p \in \mathbf{Z}_p.$$

‘Theoretical description’: lift $\overline{f}_C \in \mathbf{F}_p[X]$ to $f_C \in \mathbf{Z}_p[X]$ as factor of 5-division polynomial for E_1 .

Polynomial f_C ‘codes’ the subgroup $E_1[\mathfrak{p}_5] \subset E_1[5]$. Can use Vélu’s formulas to compute $E_1/E_1[\mathfrak{p}_5]$. Then take j -invariant. All mod p^2 .

Observation: only interested in $j(E_1/E_1[\mathfrak{p}_5])$, a root of $\Phi_5(X, j(E_1))$.

We know $j(E_1/[\mathfrak{p}_5]) \bmod p$, so we know which root to pick.

Enormous speed-up in practical performance.

Lifting the cycle to \mathbf{Q}_p

We lift

$$295 \xrightarrow{\mathfrak{p}_5} 449 \xrightarrow{\mathfrak{p}_5} 73 \xrightarrow{\mathfrak{p}_5} 55 \xrightarrow{\mathfrak{p}_5} 328 \xrightarrow{\mathfrak{p}_{19}} 295$$

over \mathbf{F}_p to

$$\begin{aligned} 295 - 233p &\xrightarrow{\mathfrak{p}_5} -194 + 296p \xrightarrow{\mathfrak{p}_5} 73 - 236p \xrightarrow{\mathfrak{p}_5} 55 + 155p \\ &\xrightarrow{\mathfrak{p}_5} -315 + 131p \xrightarrow{\mathfrak{p}_{19}} 295 - 236p \end{aligned}$$

over \mathbf{Q}_p . Computations are done mod p^2 .

Cycle not closed because $(\alpha) \notin \text{End}(E_1) = \mathbf{Z}$.

We have $\rho_\alpha(j(E_1)) = 295 - 236 \pmod{p^2}$.

Newton

Next step: compute $\alpha/\bar{\alpha} \in \mathbf{Z}_p/(p^2)$. We know the minimal polynomial of α , so use Hensel.

Practical speed up: use Horner's rule. Gives the derivative needed for Hensel for free.

Then update $j(E_1) \in \mathbf{Z}_p$ according to Newton's formula

$$j(E_{k+1}) = j(E_k) - \frac{\rho_\alpha(j(E_k)) - j(E_k)}{(\alpha/\bar{\alpha}) - 1} \quad \text{for } k \in \mathbf{Z}_{\geq 1}.$$

We have $j(E_2) = 295 - 155p + O(p^2) = j(\tilde{E}) \pmod{p^2}$.

Next few cycles

We update the ‘cycle’ over $\mathbf{Z}_p/(p^2)$ to a ‘cycle’ over $\mathbf{Z}_p/(p^4)$, etc.

Precision is doubled in each step.

Use the information modulo p^k for the computation mod p^{2k} .

We get:

$$\begin{aligned} j(\tilde{E}) &= 295 + O(p) \\ &= 295 - 155p + O(p^2) \\ &= 295 - 155p + 195p^2 + 287p^3 + O(p^4) \\ &= 295 - 155p + 195p^2 + 287p^3 - 153p^4 + 245p^5 + 272p^6 \\ &\quad + 298p^7 + O(p^8). \\ &= 295 - 155p + 195p^2 + 287p^3 - 153p^4 + 245p^5 + 272p^6 \\ &\quad + 298p^7 - 277p^8 + 170p^9 - 123p^{10} - 86p^{11} - 165p^{12} \\ &\quad - 115p^{13} + 195p^{14} + 56p^{15} + O(p^{16}). \end{aligned}$$

Computing the conjugates

Recall: $\text{Pic}(\mathcal{O})$ acts on $\text{Ell}_\Delta(\mathbf{Q}_p)$ via

$$j(E) \mapsto j(E^I) \quad [I] \in \text{Pic}(\mathcal{O}).$$

Action is transitive and free.

Under GRH, we have *small* generators of $\text{Pic}(\mathcal{O})$. Proven bound $O((\log |D|)^2)$ is even pessimistic ‘in practice’.

For I of norm l , we have

$$\Phi_l(j(E), j(E^I)) = 0 \in \mathbf{Q}_p.$$

This observation suffices to find other elements of $\text{Ell}_\Delta(\mathbf{Q}_p)$.

Conjugates in the example

We have $\text{Pic}(\mathcal{O}) \cong \mathbf{Z}/14\mathbf{Z} \cong \langle \mathfrak{p}_5 \rangle$.

Expand

$$P_{-639} = \prod_{[I] \in \text{Pic}(\mathcal{O})} (X - j(\tilde{E})^I) \in \mathbf{Z}[X].$$

Polynomial has coefficients up to 126 decimal digits:

$$\begin{aligned} P_{-639}(0) = & 1721051509821005661717426130583703669328143 \\ & 1233506629561471642040639130300833400407189 \\ & 58275994891098076959831873615798485563169. \end{aligned}$$

Problem

The coefficients of P_Δ are *huge*.

Coefficients grow exponentially in size for $|\Delta| \rightarrow \infty$ and for ‘small’ Δ , they are *massive*.

Example:

$$P_{-23} = X^3 + 3491750X^2 - 5151296875X + 12771880859375 \in \mathbf{Z}[X].$$

Growth rate cannot be helped, but the polynomial $X^3 - X^2 + 1$ also generates $H_{\mathcal{O}_{-23}}$.

Question: how to find/compute such a ‘small’ polynomial?

Modular functions

A function $f : \mathbf{H} \rightarrow \mathbf{C}$ is *modular* of level $N \in \mathbf{Z}_{\geq 1}$ if

- ◇ $\Gamma(N) \stackrel{\text{def}}{=} \text{Ker}(\text{SL}_2(\mathbf{Z}) \rightarrow \text{SL}_2(\mathbf{Z}/N\mathbf{Z}))$ stabilizes f
- ◇ f is meromorphic on $\overline{\mathbf{H}} = \mathbf{H} \cup \mathbf{P}^1(\mathbf{Q})$.

A modular function has a Fourier expansion in $q^{1/N}$.

Examples.

$$j(z) = q^{-1} + 744 + 196884q + 21493760q^2 + \dots \quad (N = 1)$$

$$\gamma_2(z) = q^{-1/3} + 248q^{2/3} + 4124q^{5/3} + \dots \quad (N = 3, \gamma_2^3 = j)$$

$$f(z) = \zeta_{48}^{-1} \cdot \frac{\eta(\frac{z+1}{2})}{\eta(z)} = q^{1/24} + q^{25/24} + 3q^{49/24} + \dots \quad (N = 48)$$

The modular function field

- $F_N = \{ \text{modular functions of level } N \text{ over } \mathbf{Q}(\zeta_N) \}$ forms a field
- $F_1 = \mathbf{Q}(j)$
- $\mathcal{F} = \bigcup_{N \geq 1} F_N$ is Galois extension of F_1
- the sequence $1 \longrightarrow \{\pm 1\} \longrightarrow \mathrm{GL}_2(\widehat{\mathbf{Z}}) \longrightarrow \mathrm{Gal}(\mathcal{F}/F_1) \longrightarrow 1$ is exact.

Theorem. Write $\mathcal{O} = \mathbf{Z}[\theta]$ with $\theta \in \mathbf{H}$ and let $H_{\mathcal{O},N}$ be the ray class field of conductor N for \mathcal{O} . Then:

$$H_{\mathcal{O},N} = K(\{f(\theta) : f \in F_N \text{ and } f(\theta) \neq \infty\}).$$

In particular: $H_{\mathcal{O},1} = H_{\mathcal{O}} = K(j(\theta))$.

Class invariants

The value $f(\theta)$ is called a *class invariant* if we have

$$K(f(\theta)) = H_{\mathcal{O}}.$$

Tool for investigation: *Shimura reciprocity*. It gives the action of $\text{Gal}(K_{\text{ab}}/H_{\mathcal{O}})$ on $f(\theta)$ via

$$\begin{array}{ccccccc} 1 & \longrightarrow & \mathcal{O}^* & \longrightarrow & \widehat{\mathcal{O}}^* & \xrightarrow{\text{Artin}} & \text{Gal}(K_{\text{ab}}/H_{\mathcal{O}}) \longrightarrow 1 \\ & & & & \downarrow g_{\theta} & & \\ 1 & \longrightarrow & \{\pm 1\} & \longrightarrow & \text{GL}_2(\widehat{\mathbf{Z}}) & \longrightarrow & \text{Gal}(\mathcal{F}/\mathbf{Q}(j)) \longrightarrow 1. \end{array}$$

If $\mathcal{F}/\mathbf{Q}(f)$ is Galois, we have

$$(f(\theta))^x = f(\theta) \iff f^{g_{\theta}(x)} = f.$$

Class invariants, examples

In this talk, we focus on 2 examples.

1. Suppose $3 \nmid \Delta$, and write $\mathcal{O} = \mathbf{Z}[\theta]$ with $\theta + \bar{\theta} \equiv 0 \pmod{3}$. Then $\gamma_2(\theta)$ is a class invariant.
2. Suppose $3 \nmid \Delta$ and $\Delta \equiv 1 \pmod{8}$. Then \mathfrak{f} yields class invariants for appropriate $\theta \in \mathcal{O}$.

In both cases, the minimal polynomial P_{Δ}^f of $f(\theta)$ over \mathbf{Q} has *integer* coefficients.

For $f = \gamma_2$ its coefficients are a factor 3 smaller than for $P_{\Delta} = P_{\Delta}^j$, for \mathfrak{f} a factor 72.

Computing conjugates

‘Extended’ Shimura reciprocity gives the conjugates of $f(\theta)$ under $\text{Gal}(H_{\mathcal{O}}/K) \cong \text{Pic}(\mathcal{O})$ via

$$\begin{array}{ccccccc}
 1 & \longrightarrow & K^* & \longrightarrow & \widehat{K}^* & \xrightarrow{\text{Artin}} & \text{Gal}(K_{\text{ab}}/K) \longrightarrow 1 \\
 & & & & \downarrow g_{\theta} & & \\
 1 & \longrightarrow & \mathbf{Q}^* & \longrightarrow & \text{GL}_2(\widehat{\mathbf{Q}}) & \longrightarrow & \text{Aut}(\mathcal{F}) \longrightarrow 1.
 \end{array}$$

We have

$$(f(\theta))^x = (f^{g_{\theta}(x^{-1})})(\theta).$$

We can compute the minimal polynomial P_{Δ}^f of $f(\theta)$ using *complex analytic means*.

Example: $P_{-71}^f = X^7 - X^6 - X^5 + X^4 - X^3 - X^2 + 2X + 1 \in \mathbf{Z}[X]$.

p -adic class invariants

Recall: we can compute

$$\text{Ell}_\Delta(\mathbf{Q}_p) = \{\tilde{j} \in \mathbf{Q}_p \mid \exists E/\mathbf{Q}_p : j(E) = \tilde{j}, \text{End}_{\mathbf{Q}_p}(E) = \mathcal{O}\}.$$

Let $\Psi_f(X, j)$ be the minimal polynomial of f over $\mathbf{C}(j)$.

Assumption: $\Psi_f(X, j) \in \mathbf{Z}[X, j]$.

If f yields class invariants, one root of $\Psi_f(X, \tilde{j}) \in \mathbf{Q}_p[X]$ lies in $H_{\mathcal{O}} \hookrightarrow \mathbf{Q}_p$.

We need to figure out which one.

Geometric description of f

We have

$$F_N = \mathbf{Q}(\zeta_N)(X(N)) = \mathbf{Q}(j, g_{r,s} \mid r, s \in \frac{1}{N}\mathbf{Z}/\mathbf{Z}, \text{ not both } 0).$$

Functions $g_{r,s}$ are normalized x -coordinates of N -torsion points of an elliptic curve with j -invariant j . Name: *Fricke functions*.

In principle, we can write $f \in F_N$ as a rational function in j and the Fricke functions.

So: $f \in F_N$ is a function of

- ◇ a curve E
- ◇ a basis P, Q for the N -torsion $E[N]$.

Galois action on roots

Write a root $r \in \mathbf{Q}_p$ of $\Psi_f(X, \tilde{j}) \in \mathbf{Q}_p[X]$ as

$$r = f(\tilde{E}, P, Q) \quad \text{with } P, Q \in \tilde{E}[N].$$

The root r lies in $H_{\mathcal{O}}$ if and only if

$$\forall \sigma \in \text{Gal}(H_{N, \mathcal{O}}/H_{\mathcal{O}}) \cong (\mathcal{O}/N\mathcal{O})^*/\mathcal{O}^* : \quad \sigma(r) = r.$$

For an ideal $I \subset \mathcal{O}$, coprime to N , the isogeny $\varphi_I : \tilde{E} \rightarrow \tilde{E}^I$ induces an isomorphism

$$\varphi_I : \tilde{E}[N] \xrightarrow{\sim} \tilde{E}^I[N].$$

Key observation. We have $r^{[[I], H_{N, \mathcal{O}}/H_{\mathcal{O}}]} = f(\varphi_I(\tilde{E}), \varphi_I(P), \varphi_I(Q))$.

What can we compute?

- which root of $r \in \mathbf{Q}_p$ of $\Psi_f(X, \tilde{j}) \in \mathbf{Q}_p[X]$ is a class invariant
- the conjugates of a class invariant $r \in \mathbf{Q}_p$ under $\text{Pic}(\mathcal{O})$, same technique: the Galois action is given by isogenies!
- the minimal polynomial

$$P_{\Delta}^f = \prod_{[\mathfrak{a}] \in \text{Pic}(\mathcal{O})} (X - r^{[\mathfrak{a}, H_{\mathcal{O}}/K]}) \in \mathcal{O}[X] \quad (\text{or } \mathbf{Z}[X]).$$

Example: γ_2

Choose an equation $Y^2 = X^3 + aX + b$ for \tilde{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 $j(\tilde{E})$.

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 γ_2 ’.

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

Example: γ_2 and $\Delta = -31$

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

$$j(\tilde{E}_{-31}) = 3 + 33p - 16p^2 + O(p^3)$$

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

- we compute $j(\tilde{E}_{-31})$ with only one-third of the accuracy as we would have done for $P_{-31} = P_{-31}^j$
- $j(\tilde{E}_{-31})$ has three cube roots in \mathbf{Q}_p :

$$\eta_1 = 18 + O(p) \quad \eta_2 = 53 + O(p) \quad \eta_3 = 63 + O(p)$$

- we need to find out which one lies in $H_{\mathcal{O}}$.

Action of \mathcal{O} on cube roots of $j(\tilde{E})$

- a cube root lies in $H_{\mathcal{O}}$ if and only if it is invariant under

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

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

- choose a Weierstraß equation $Y^2 = X^3 + aX + b$ for $\tilde{E}_{-31}/\mathbf{Q}_p$
- compute the 4 roots c_1, \dots, c_4 of the 3-division polynomial for \tilde{E} and compute 3-torsion points P_i with x -coordinate c_i
- recall: a cube root of $j(\tilde{E}_{-31})$ is given by

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

Action of \mathcal{O} on cube roots of $j(\tilde{E})$

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

$$\varphi_I : \tilde{E}_{-31} \rightarrow \tilde{E}_{-31}^I$$

with kernel $\tilde{E}_{-31}[I] = \bigcap_{g \in I} \text{Ker } g$

- algorithmic description of φ_I :

- ◇ compute a polynomial $f_I \in \mathbf{Q}_p[X]$ whose roots are the x -coordinates of $\tilde{E}_{-31}[I]$ (using Atkin-Elkies techniques)

- ◇ find an explicit isogeny φ_I using Vélu's formulas

- we have $j(\tilde{E}_{-31})^{[[I], H_{\mathcal{O}}/K]} = j(\tilde{E}_{-31}^I)$

Action of \mathcal{O} on cube roots of $j(\tilde{E})$

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

$$\varphi_I : \tilde{E}_{-31}[3] \xrightarrow{\sim} \tilde{E}_{-31}^I[3]$$

and hence a natural bijection

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

- for a cube root $\eta = \frac{-48a}{2a - 3(c_1c_2 + c_3c_4)}$ we have

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

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

Action of \mathcal{O} on cube roots of $j(\tilde{E})$

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

$$\eta_1 \xrightarrow{\varphi_I} \eta_1 \quad \eta_2 \xrightarrow{\varphi_I} \eta_3 \quad \eta_3 \xrightarrow{\varphi_I} \eta_2$$

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 $\text{Pic}(\mathcal{O}) \cong \mathbf{Z}/3\mathbf{Z} \cong \langle [\mathfrak{p}_2] \rangle$
- action of \mathfrak{p}_2 on η_1 is as before: $\eta_1^{[\mathfrak{p}_2, H/K]} = \varphi_{\mathfrak{p}_2}(\eta_1)$
- we compute the conjugates and expand:

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

Practical problem

This method works for any function f .

However: how to write f as function in j and Fricke functions? And: we might have to factor the N -division polynomial of degree $O(N^2)$.

For $f = \mathfrak{f}$ of level $N = 48$ this approach is not practical.

Solution. All we need to know is

$$r^I$$

for an ‘ f -value’ r and an ideal $I \subseteq \mathcal{O}$.

The curve $X(f) = \text{Stab}_{\text{SL}_2(\mathbf{z})}(f) \backslash \overline{\mathbf{H}}$ is a quotient of $X(N)$.

$$\begin{array}{ccc}
 X(N) & \xrightarrow{f} & \mathbf{P}^1 \\
 & \searrow & \nearrow f \\
 & X(f) &
 \end{array}$$

Write $X(f; l) = (\text{Stab}_{\text{SL}_2(\mathbf{z})}(f) \cap \Gamma_0(l)) \backslash \overline{\mathbf{H}}$ for $l \nmid N$ prime.

$$\begin{array}{ccccc}
 & & X(f; l) & & \\
 & \swarrow s & & \searrow t & \\
 X(f) & & & & X(f) \\
 \downarrow f & \nearrow F & & \searrow F' & \downarrow f \\
 \mathbf{P}^1 & & & & \mathbf{P}^1
 \end{array}$$

Computing r^I

Assume that f has integer Fourier coefficients.

Let Φ_f^l be the minimal polynomial of $f(lz)$ over $\mathbf{Q}(f)$.

Then Φ_f^l is an affine model for $X(f; l)$.

The value $r^I \in \mathbf{Q}_p$ is a root of $\Phi_f^l(r, X) \in \mathbf{Q}_p[X]$.

‘Usually’, there is only one root of both $\Phi_f^l(r, X)$ and $\Psi_f(X, j(\tilde{E})^I)$.

This root is r^I .

For $\deg f = 1$, we can *prove* there is only one such root.

This **solves** the ‘practical problem’!

Example: \mathfrak{f}

We have $\Psi_{\mathfrak{f}} = (X^{24} - 16)^3 - jX^{24} \in \mathbf{Z}[j, X]$.

Models for $X(\mathfrak{f}; 5)$ and $X(\mathfrak{f}; 7)$:

$$\Phi_{\mathfrak{f}}^5(X, Y) = (X^5 - Y)(X - Y^5) + 5XY \in \mathbf{Z}[X, Y]$$

$$\Phi_{\mathfrak{f}}^7(X, Y) = (X^7 - Y)(X - Y^7) + 7(XY - X^4Y^4) \in \mathbf{Z}[X, Y]$$

Can prove: all polynomials for \mathfrak{f} are symmetric, and have integer coefficients.

Note: the coefficients are *much* smaller than for the ‘classical’ modular polynomials.

Example: f and $\Delta = -71$

- take $p = 107$ and

$$\overline{E}/\mathbf{F}_p : Y^2 = X^3 + 91X + 16$$

of j -invariant $19 \in \mathbf{F}_p$

- the polynomial $\Psi_f(X, 19) \in \mathbf{F}_p[X]$ has two roots in \mathbf{F}_p : 26 and 81. Take $r = 26$.
- $\text{Pic}(\mathcal{O}) \cong \mathbf{Z}/7\mathbf{Z} \cong \langle [\mathfrak{p}_5] \rangle$;

For this *small* discriminant we only need one p -adic digit accuracy.
No need to apply map ρ_α .

Example: f and $\Delta = -71$

- the polynomial $\Phi_f^5(X, r) \in \mathbf{F}_p[X]$ has two roots in \mathbf{F}_p : 56 and 59
- we compute $j(\overline{E})^{\mathfrak{p}_5} = 77 \in \mathbf{F}_p$, and have

$$r^{\mathfrak{p}_5} = 56 \in \mathbf{F}_p$$

We compute $r^{\mathfrak{p}_5^i}$ for $1 \leq i \leq 7$ and expand

$$P_{-71}^f = \prod_{1 \leq i \leq 7} (X - r^{\mathfrak{p}_5^i}) =$$

$$X^7 - X^6 - X^5 + X^4 - X^3 - X^2 + 2X + 1 \in \mathbf{Z}[X].$$

Larger discriminants

- p -adic approach works for any modular function f
- with a few tricks, it is just as fast as the complex analytic method
- ‘world record’: $\Delta \approx -10^{11}$
- problem becomes *memory*, not run time!