Explicit CM in genus 2

David Gruenewald
(University of Sydney)

Joint work with
Reinier Bröker and Kristin Lauter
(Microsoft Research)

Computational Algebra Seminar
The University of Sydney
19th March 2009

Motivation

For elliptic (hyperelliptic) curve cryptography, we need methods to construct an elliptic curve (genus 2 Jacobian) over a finite field having a given number of points (eg. having a very large prime divisor). One such algorithm is the CM method.

CM method for genus 1

Let E be an ordinary elliptic curve over $\mathbb{F}_p$. We have the following well known results:

- $\#E/\mathbb{F}_p = 1 - t + p$, where t is the trace of Frobenius $\pi : (x, y) \mapsto (x^p, y^p)$.
- $\pi^2 - t\pi + p = 0$ with $t^2 - 4p = D < 0$.
- E is the reduction of an elliptic curve over $\mathbb{C}$ having CM by $\mathcal{O} = \mathbb{Z}[\pi]$ (Deuring, 1941).

There are a finite number of isomorphism classes of such curves; when $\mathcal{O}$ is an order in $K = \mathbb{Q}(\sqrt{D})$, the j-invariants of these curves satisfy

$$P_{\mathcal{O}}(j) = 0, \quad P_{\mathcal{O}}(x) \in \mathbb{Z}[x] \text{ monic.}$$

- $H = K(j)$ is the ring class field for $\mathcal{O}$.
- The Galois action of $\mathrm{Gal}(H_{\mathcal{O}}/K) \cong \mathrm{Pic}(\mathcal{O})$ is given by

$$j(\mathbb{C}/\mathcal{O})^{[\mathfrak{a}, H_{\mathcal{O}}/K]} = j(\mathbb{C}/\mathfrak{a}^{-1}).$$

- In the case where $\mathcal{O}$ is the maximal order, $\mathrm{Pic}(\mathcal{O}) = \mathrm{Cl}(K)$ and H is the Hilbert class field of K (the maximal unramified abelian extension of K).

Explicit CM in genus 1!

Computing $P_{\mathcal{O}}$

The polynomial $P_{\mathcal{O}} \in \mathbb{Z}[X]$ can be computed in (at least) three different ways:

- complex arithmetic: use $j : \mathbb{H} \to \mathbb{C}$ given by $j(z) = 1/q + 744 + 196884q + \ldots$ in $q = \exp(2\pi i z)$. *(Enge ('07))*
- p-adic arithmetic: compute the *canonical lift* of an ordinary elliptic curve over $\mathbb{F}_p$. *(Couveignes-Henocq ('02), Bröker ('06))*
- $\mathbb{F}_p$-arithmetic: Chinese remaindering *(Lauter ('04), Belding-Bröker-Enge-Lauter ('08), Sutherland ('08))*.

Aim: Compute the analogue of $P_{\mathcal{O}}$ in genus 2!

Some definitions

Definition: A quartic CM field is an imaginary quadratic extension of a real quadratic field.

Lemma: Let K be a quartic CM field and let L be its Galois closure. Then $\mathrm{Gal}(L/\mathbb{Q}) \cong C_4, C_2 \times C_2, D_4$.

We exclude $\mathrm{Gal}(K/\mathbb{Q}) \cong C_2 \times C_2$ (ensuring that the genus 2 jacobians we construct are simple). Write the 4 embeddings $K \hookrightarrow \mathbb{C}$ as $\{\varphi_1, \varphi_2, \overline{\varphi_1}, \overline{\varphi_2}\}$. The pairs $\Phi = \{\varphi_1, \varphi_2\}$ and $\Phi' = \{\varphi_1, \overline{\varphi_2}\}$ are called CM types. The reflex field of (K, Φ) is

$$K_\Phi = \mathbb{Q}\Big(\sum_{\varphi \in \Phi} \varphi(x) \mid x \in K\Big).$$

The fields K_Φ and $K_{\Phi'}$ are isomorphic subfields of $L \subset \mathbb{C}$.

Leading example

Put $K = \mathbb{Q}[X]/(X^4 + 22X^2 + 73)$. We have $\mathrm{Gal}(L/\mathbb{Q}) = D_4$.

$$
\begin{tikzcd}
 & & L & & \\
\cdot \arrow[urr] & K \arrow[ur] & L^+ \arrow[u] & K_\Phi \arrow[ul] & K_{\Phi'} \arrow[ull] \\
 & K^+ \arrow[ul] \arrow[u] \arrow[ur] & \cdot \arrow[u] & K_\Phi^+ \arrow[ul] \arrow[u] \arrow[ur] & \\
 & & \mathbb{Q} \arrow[ul] \arrow[u] \arrow[ur] & &
\end{tikzcd}
$$

We have $K_\Phi = \mathbb{Q}[X]/(X^4 + 11X^2 + 12)$ and $K^+ = \mathbb{Q}(\sqrt{3})$.

Abelian varieties associated to ideals

For an ideal $I \subseteq \mathcal{O}_K$, the quotient $A_I = \mathbb{C}^2/\Phi(I^{-1})$ is an abelian variety of dimension 2. It has endomorphism ring $\mathcal{O}_K$.
Fact: *We can choose I such that A_I is principally polarized.*

The isomorphism class of the variety A_I is determined by three invariants $j_1(A_I), j_2(A_I), j_3(A_I)$. The Igusa functions j_i are explicitly given functions on the Siegel upper half space

$$\mathbb{H}_2 = \{\tau \in \mathrm{Mat}_{2\times 2}(\mathbb{C}) \mid {}^t\tau = \tau \ , \ \mathrm{Im}(\tau) > 0\} \, .$$

Theorem (weak version): *The field $K_\Phi(j_1(A_I), j_2(A_I), j_3(A_I))$ is a subfield of the Hilbert class field of K_Φ. The polynomial*

$$P_K = \prod_{\{[A/\mathbb{C}] \,|\, \mathrm{End}(A) \cong \mathcal{O}_K\}} (X - j_1(A))$$

has rational coefficients. Similarly for the polynomials Q_K, R_K giving the j_2 and j_3-invariants.

Leading example

We have $\mathrm{Cl}(\mathcal{O}_K) \cong \mathbb{Z}/4\mathbb{Z}$. All four ideal classes are principally polarizable. Take $I = \mathcal{O}_K$ and $A_I = \mathbb{C}^2/\Phi(\mathcal{O}_K)$.
We have $\mathrm{Cl}(\mathcal{O}_{K_\Phi}) \cong \mathbb{Z}/4\mathbb{Z}$ and $\mathrm{Gal}(H(K_\Phi)/K_\Phi) \cong \mathbb{Z}/4\mathbb{Z}$.

$$\begin{tikzcd}
H(K) & & H(K_\Phi) \\
 & & K_\Phi(j_i(A_I)) \arrow[u] \\
K \arrow[uu] & & K_\Phi \arrow[u] \\
 & \mathbb{Q} \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

Computing P_K, Q_K, R_K

The methods for computing P_K, Q_K, R_K are far less developed.

- complex arithmetic: evaluate $j_k : \mathbb{H}_2 \to \mathbb{C}$ to enough precision
- p-adic arithmetic: compute a *canonical lift*, strong condition on the splitting behaviour of the prime p
  ($p = 2$: Gaudry-Houtmann-Kohel-Ritzenthaler-Weng ('05))
  ($p = 3$: Carls-Kohel-Lubicz ('08))
- $\mathbb{F}_p$-arithmetic: Chinese remaindering
  (Eisenträger-Lauter ('05))

All methods have shortcomings. However, computing P_K, Q_K, R_K is the only 'practical' way of constructing cryptographic hyperelliptic curves.

Today's talk: *Understand the Galois action better. This will pave the way for a p-adic method and improve CRT.*

The Galois action for $\mathrm{Gal}(L/\mathbb{Q}) \cong D_4$

The Artin map gives an isomorphism

$$\mathrm{Cl}(\mathcal{O}_{K_\Phi}) \xrightarrow{\sim} \mathrm{Gal}(H(K_\Phi)/K_\Phi).$$

An ideal $\mathfrak{p} \in \mathcal{O}_{K_\Phi}$ yields an ideal in $\mathcal{O}_K$ via the typenorm map

$$N_\Phi(\mathfrak{p}) = N_{L/K}(\mathfrak{p}\mathcal{O}_L).$$

Let $\mathfrak{p} \subset \mathcal{O}_{K_\Phi}$ have norm p. We have $N_\Phi(\mathfrak{p}) \mid (p) \subset \mathcal{O}_K$ and we get a subspace

$$V = \{P \in A_I \mid \forall \alpha \in N_\Phi(\mathfrak{p}) : \alpha(P) = 0\} \subset A[p].$$

This space is 2-dimensional as an $\mathbb{F}_p$-vector space.
The ideal $\mathfrak{p} \in \mathcal{O}_{K_\Phi}$ acts on A_I via

$$A_I \mapsto A_I/V$$

where A_I/V has the induced principal polarization.

Leading example

We have $(3) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3^2 \subset \mathcal{O}_{K_\Phi}$. All ideals have norm 3.

In $\mathcal{O}_K$, we find that $(3) = \widetilde{\mathfrak{p}}_1^2\,\widetilde{\mathfrak{p}}_2^2$. The images under N_Φ are given by

$$
\begin{aligned}
N_\Phi(\mathfrak{p}_1) &= \widetilde{\mathfrak{p}}_1^2 \\
N_\Phi(\mathfrak{p}_2) &= \widetilde{\mathfrak{p}}_2^2 \\
N_\Phi(\mathfrak{p}_3) &= \widetilde{\mathfrak{p}}_1\widetilde{\mathfrak{p}}_2.
\end{aligned}
$$

All three $\mathcal{O}_K$-ideals have norm 9 and divide (p). They yield three different 2-dimensional subspaces of $A_I[p]$.

Towards computing the CM-action

In both genus 1 and 2, the CM-action is given by isogenies.

In genus 1 we can use the curve

$$Y_0(p) = \{(E, L) : L \text{ has index } p \text{ in } E[p]\}$$

parametrizing elliptic curves with a p-isogeny $E \to E/L$ to explicitly compute the CM-action.

[If $N(\mathfrak{a}) = p$ then $E[p] = E[\mathfrak{a}] \oplus E[\bar{\mathfrak{a}}]$ and

$$\mathfrak{a} \longleftrightarrow (\ j(E) \mapsto j(E/E[\mathfrak{a}])\ )$$

defines the isomorphism $\mathrm{Pic}(\mathcal{O}) \cong \mathrm{Gal}(H_{\mathcal{O}}/K)$ **]**

In genus 2, the appropriate analogue is the Siegel modular variety $Y_0^{(2)}(p)$:

$$\{(A,L) : A[p]/L \cong (\mathbb{Z}/p\mathbb{Z})^2,\ L \text{ isotropic}\}.$$

It parametrizes principally polarized abelian surfaces (p.p.a.s.'s) with a (p,p)-isogeny to another p.p.a.s.

A model for $Y_0^{(2)}(p)$ is given by an ideal

$$I_p \subset \mathbb{Z}[X_1, Y_1, Z_1, X_2, Y_2, Z_2].$$

A point

$$\big(j_1(\tau), j_2(\tau), j_3(\tau), j_1(\tau'), j_2(\tau'), j_3(\tau')\big)$$

belongs to $Y_0^{(2)}(p)$ iff it lies in I_p.

Computing the CM-action over finite fields

Setup:

- $A/\mathbb{F}_q$ with endomorphism ring $\mathcal{O}_K$,
- a prime $p \neq q$ such that there is a prime $\mathfrak{p}$ of K_Φ of norm p ,
- the ideal $I_p \subseteq \mathbb{F}_q[X_1, Y_1, Z_1, X_2, Y_2, Z_2]$ describing $Y_0^{(2)}(p)$ over $\mathbb{F}_q$.

Specialize I_p in

$$(X_1, Y_1, Z_1) = (j_1(A), j_2(A), j_3(A)) \in \mathbb{F}_q^3.$$

There are exactly $(p^4 - 1)/(p - 1)$ solutions over $\overline{\mathbb{F}_q}$ of the remaining system of equations.
All solutions are p.p.a.s.'s with endomorphism algebra K. The ones with endomorphism ring $\mathcal{O}_K$ are defined over $\mathbb{F}_q$.

Aside: compare to genus 1

$Y_0(N)$ has a model given by the classical modular polynomial $\phi_N(X,Y)$, having the property that

$$\phi_N(j(\tau), j(N\tau)) = 0.$$

Given $j \in \mathbb{F}_q$ having CM by $\mathcal{O}_K$, the set of solutions to

$$\phi_p(j, Y) = 0,\ Y \in \mathbb{F}_q$$

will contain the isomorphism classes of elliptic curves having endomorphism ring $\mathcal{O}_K$.

The leading example

The prime $q = 1609$ splits as $\pi_1\pi_2\pi_3\pi_4$ in $\mathcal{O}_{K_\Phi}$. It splits completely in H_{K_Φ}.

Bounds on the denonimators (Lauter, Goren) yield that 1609 does not divide the denominators of P_K, Q_K, R_K.

$\Rightarrow$ the polynomials P_K, Q_K, R_K factor completely modulo q.

A random search over $(j_1, j_2, j_3) \in \mathbb{F}_q^3$ yields an abelian surface $A/\mathbb{F}_q$ with

$$(j_1(A), j_2(A), j_3(A)) = (1563, 789, 704)$$

has endomorphism ring $\mathcal{O}_K$.

A practical problem

The ideal I_p is huge. It has only been computed for $p = 2$, it takes 50 Megabytes to store it. Computing I_3 has not yet been undertaken.

Idea: *Use smaller functions to get something reasonable.*

For $x \in \mathbb{Z}^2$, define $\theta_x : \mathbb{H}_2 \to \mathbb{C}$ by

$$\theta_x(\tau) = \sum_{n \in \mathbb{Z}^2} \exp(\pi i n^T \tau n + 2\pi i n^T x).$$

We consider $f_1 = \theta_{(0,0)}$, $f_2 = \theta_{(0,1)}$, $f_3 = \theta_{(1,0)}$ and $f_4 = \theta_{(1,1)}$.

The quotients $f_1/f_4, f_2/f_4, f_3/f_4$ are weakly modular functions for the subgroup $\Gamma(8) \subset \mathrm{Sp}(4, \mathbb{Z})$. Let $\mathrm{Stab}(f)$ be their stabilizer.

The Satake compactification $X(f)$ of the quotient $\mathrm{Stab}(f)\backslash\mathbb{H}_2$ is a projective variety. It has coordinate ring $\mathbb{C}[f_1, f_2, f_3, f_4]$.

Lifting isogenies

Let $p \neq 2$ be prime. A (p,p)-isogeny $A \to A'$ induces an isomorphism

$$A[8] \xrightarrow{\sim} A'[8].$$

On the affine part $Y(f) = \mathrm{Stab}(f)\backslash\mathbb{H}_2$, we get a natural map

$$(A, L) \to (A', L')$$

for every (p,p)-isogeny.

Idea: *Since the f_i's are 'smaller', perhaps we can compute this map for 'large' p.*

The Siegel modular variety $X(f;p)$

$$
\begin{tikzcd}
& X(f;p) \arrow[dl, "s"'] \arrow[ddl, bend right, "F"] \arrow[dr, "t"] \arrow[ddr, bend left, "F'"'] & \\
X(f) \arrow[d, "f_i"] & & X(f) \arrow[d, "f_i"'] \\
\mathbb{P}^3_w & & \mathbb{P}^3_w \\
\mathbb{A}^3 \arrow[u] & & \mathbb{A}^3 \arrow[u]
\end{tikzcd}
$$

Affine points on $X(f;p)$ are triples (A, L, G) with $(A, L) \in X(f)$ and $G \subset A[p]$ isotropic and of dimension 2.
The map t is induced by $A \to A/G$ and s is the forgetful map.

A model for $X(f;p)$

Using the Fourier expansions of the f_i's we can use linear algebra to find a model for $X(f;p)$.
$p = 3$: the defining ideal for $X(f;3)$ has 85 homogeneous degree 6 polynomials (G. '06). One of them is

$$a_1^6 - 7a_1^4c_1^2 + 24a_1^3a_4c_1c_4 - 3a_1^2a_2^4 - 6a_1^2a_2^2c_2^2 + 24a_1^2a_2a_3c_2c_3 - 3a_1^2a_3^4 - 6a_1^2a_3^2c_3^2 + 3a_1^2a_4^4 + 6a_1^2a_4^2c_4^2 - 21a_1^2c_1^4 + 9a_1^2c_2^4 + 9a_1^2c_3^4 - 9a_1^2c_4^4 + 48a_1a_2c_1^3c_2 + 48a_1a_3c_1^3c_3 - 24a_1a_4c_1^3c_4 - a_2^4c_1^2 - 6a_2^2a_3^2a_4^2 + 6a_2^2a_3^2c_4^2 + 6a_2^2a_4^2c_3^2 + 6a_2^2c_1^2c_2^2 + 18a_2^2c_3^2c_4^2 - 24a_2a_3c_1^2c_2c_3 + 48a_2a_4c_1^2c_2c_4 - a_3^4c_1^2 + 6a_3^2a_4^2c_2^2 + 6a_3^2c_1^2c_3^2 + 18a_3^2c_2^2c_4^2 + 48a_3a_4c_1^2c_3c_4 + 5a_4^4c_1^2 - 30a_4^2c_1^2c_4^2 + 18a_4^2c_2^2c_3^2 + 27c_1^6 + 27c_1^2c_2^4 + 27c_1^2c_3^4 - 135c_1^2c_4^4 - 162c_2^2c_3^2c_4^2.$$

- It takes a mere 35Kb to store them
- The coefficients are 8-smooth!
- Computationally friendly

Explicit CM using (3,3)-isogenies

Setup:
- a CM-field K such that there is a prime of norm 3 in K_Φ
- $A/\mathbb{F}_q$ with endomorphism ring $\mathcal{O}_K$
- the ideal $I_3^f \subseteq \mathbb{F}_q[W_1, \ldots, Z_1, W_2, \ldots, Z_2]$ describing $X(f)$ over $\mathbb{F}_q$.

Algorithm:
- Choose a point $(w, x, y, z) \in \mathbb{F}_{q^r}$ on $X(f)$ mapping to $(j_1(A), j_2(A), j_3(A))$. This requires working over an extension of degree $r \leq 24$.
- Specialize I_3^f in $(W_1, X_1, Y_1, Z_1) = (w, x, y, z)$.
- There are exactly 40 solutions over $\bar{\mathbb{F}}_q$ of the remaining system of equations. Map the points defined over $\mathbb{F}_{q^r}$ 'down' to find Igusa triples.
- All solutions are p.p.a.s.'s with endomorphism algebra K. The ones with endomorphism ring $\mathcal{O}_K$ are defined over $\mathbb{F}_q$.

The leading example

Put $\mathbb{F}_{q^4} = \mathbb{F}_q(\alpha) = \mathbb{F}_q[X]/(X^4 + 5X^2 + 1277X + \ 7)$. We choose

$$\begin{aligned} w &= 450\alpha^3 + 100\alpha^2 + 437\alpha + 830 \\ x &= 311\alpha^3 + 1375\alpha^2 + 498\alpha + 817 \\ y &= 738\alpha^3 + 276\alpha^2 + 1004\alpha + 354 \\ z &= 21\alpha^3 + 363\alpha^2 + 1403\alpha + 1310 \end{aligned}$$

lying over $(j_1, j_2, j_3) = (1563, 789, 704) \in \mathbb{F}_q^3$.
Specializing the ideal I_3^f in w, x, y, z yields a system of equations in 4 variables over $\mathbb{F}_{q^4}$.
It has 40 solutions over $\overline{\mathbb{F}_q}$. We only look at solutions over $\mathbb{F}_{q^4}$.

The leading example

Map all 'f-tuples' down to Igusa triples. Over $\mathbb{F}_q$ we find

$$(1563, 789, 704), (587, 1085, 931),$$

$$(961, 509, 36), (1396, 1200, 1520),$$

$$(1350, 1316, 1483), (1310, 1550, 449), (1442, 671, 281).$$

Some of these triples are invariants of p.p.a.v.'s with endomorphism ring $\mathcal{O}_K$, some are not.

We run an 'endomorphism ring check' to decide which ones are roots of $P_K, Q_K, R_K \in \mathbb{F}_q[X]$.

Analyzing the number of 'new' p.p.a.v.'s

Recall: for an $\mathcal{O}_K$-ideal I, the quotient $A_I = \mathbb{C}^2/\Phi(I^{-1})$ is a polarized abelian surface

Question: *Why is there an I such that A_I is principally polarized?*

Answer: A principal polarization is an isomorphism between A_I and its dual $\widehat{A}_I$. For us:

$$\widehat{A}_I = \mathbb{C}^2/\Phi(\bar{I}\mathfrak{D}_K^{-1})$$

with $\mathfrak{D}_K^{-1} = \{x \in K \mid \mathrm{Tr}_{K/\mathbb{Q}}(x\mathcal{O}_K) \subseteq \mathbb{Z}\}$ the inverse different.

If $\pi \in K$ satisfies $\Phi(\pi) \in (i\mathbb{R}_{>0})^2$ and $\pi I\bar{I} = \mathfrak{D}_K^{-1}$, then the map $A_I \to \widehat{A}_I$ given by

$$(z_1, z_2) \mapsto (\varphi_1(\pi)z_1, \varphi_2(\pi)z_2)$$

is an isomorphism. The answer now follows from class field theory.

Analyzing the number of ‘new’ p.p.a.v.’s

Any $\mathcal{O}_K$-ideal $\mathfrak{a}$ naturally acts on A_I via

$$\mathbb{C}^2/\Phi(I^{-1}) \longrightarrow \mathbb{C}^2/\Phi(\mathfrak{a}I^{-1}).$$

The right hand side has a principal polarization if and only if $\mathfrak{a}$ lies in the kernel of

$$\mathrm{Cl}(\mathcal{O}_K) \to \mathrm{Cl}^+(K^+).$$

Writing $\mathfrak{a}\overline{\mathfrak{a}} = \alpha > 0$, the polarization changes from π to $\pi\alpha$.
The group $\mathfrak{C}(K)$ consisting of isomorphism classes of pairs $(\mathfrak{a}, \alpha)$ naturally acts on the p.p.a.s.’s that have CM by $\mathcal{O}_K$. It fits in an exact sequence

$$1 \longrightarrow (\mathcal{O}_{K^+}^*)^+/N_{K/K^+}(\mathcal{O}_K^*) \longrightarrow \mathfrak{C}(K)$$

$$\longrightarrow \mathrm{Cl}(\mathcal{O}_K) \longrightarrow \mathrm{Cl}^+(K^+) \longrightarrow 1.$$

Analyzing the number of 'new' p.p.a.v.'s

We have a natural map $m : \mathcal{O}_{K_\Phi} \to \mathfrak{C}(K)$ given by

$$\mathfrak{p} \longmapsto \left(N_\Phi(\mathfrak{p}), N_{K_\Phi/\mathbb{Q}}(\mathfrak{p})\right).$$

If $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ are the prime ideals of K_Φ of norm p, then the number of (p,p)-isogenous p.p.a.v.'s is

$$|\{m(\mathfrak{p}_1), \ldots, m(\mathfrak{p}_k)\}|.$$

This can be different from k itself!

Example. Take the cyclic field

$$K = \mathbb{Q}[X]/(X^4 + 219X^2 + 10512)$$

with $\mathrm{Cl}(\mathcal{O}_K) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \langle \mathfrak{p}_3, \mathfrak{p}_3' \rangle$. The images $N_\Phi(\mathfrak{p}_3)$, $N_\Phi(\mathfrak{p}_3')$ coincide.

The leading example

We compute

$$1 \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathfrak{C}(K) \longrightarrow \mathbb{Z}/4\mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 1.$$

A close examination yields $\mathfrak{C}(K) \cong \mathbb{Z}/4\mathbb{Z} = \langle g \rangle$.
Under this identification, we have

$$N_\Phi(\mathfrak{p}_1) = g, \quad N_\Phi(\mathfrak{p}_2) = g^{-1}, \quad N_\Phi(\mathfrak{p}_3) = 1.$$

The ideal $\mathfrak{p}_3$ explains why we got the original point $(1563, 789, 704)$ back when we looked at all $(3,3)$-isogenous varieties.

The other 2 ideals yield elements of order 4 in $\mathfrak{C}(K)$.
Note: Under the map to $\mathrm{Cl}(\mathcal{O}_K)$ they have order 2.

The leading example

We compute

$$(1563, 789, 704) \xrightarrow{\mathfrak{p}_1} (1396, 1200, 1520) \xrightarrow{\mathfrak{p}_1}$$
$$(1276, 1484, 7) \xrightarrow{\mathfrak{p}_1} (1350, 1316, 1483) \xrightarrow{\mathfrak{p}_1}$$
$$\xrightarrow{\mathfrak{p}_1} (1563, 789, 704).$$

The polynomial $(X - 1563) \cdot \ldots \cdot (X - 1350) \in \mathbb{F}_q[X]$ divides the degree 8 polynomial P_K.
To find the other degree 4 factor, we do a 2nd random search. In the end, we compute

$$P_K = X^8 + 455X^7 + 410X^6 + 259X^5 + 323X^4$$
$$+153X^3 + 289X^2 + 942X + 416 \mod 1609.$$

The leading example

To compute $P_K \in \mathbb{Q}[X]$ we compute it modulo various primes q and use Chinese remaindering.

The resulting polynomial factors over K_Φ into 2 irreducible quartics.

Over $\mathbb{Q}$, the denominator is 2^{28} and the largest coefficient has 50 decimal digits.

The polynomial P_K is irreducible over $\mathbb{Q}$ and defines the Hilbert class field of K_Φ.

Summary

Our approach works in general, there is no assumption on K.

Right now, we can only compute the CM-action for ideals of norm 2 and norm 3. The norm 5 ideals are computationally out of reach: it is too hard to compute I_5^f.

The map $\mathrm{Cl}(\mathcal{O}_{K_\Phi}) \to \mathfrak{C}(K)$ need not be surjective. This means we have to do several random searches.

Future research:

- Can we efficiently compute I_p^g for primes $p \geq 5$ using modular forms $\{g_i\}$ which have a different level structure?
- Understanding the (p,p)-isogeny graph structure better would speed up the algorithm (some endomorphism ring information is encoded in the graph).