Constructing cryptographic curves with complex multiplication

Reinier Bröker

Microsoft Research

Fields Institute
May 2009

Curves and crypto

Curve cryptography comes in 2 flavours:

- *standard*: we want curves of prime order;
- *pairing-based*: we want 'pairing friendly curves'.

We are limited to (Jacobians of) genus 1 and genus 2 curves.

In this talk we'll focus mostly on finding elliptic curves and abelian surfaces of prime order.

Elliptic curves of prime order

For cryptography, we need

$$N = \#E(\mathbf{F}_p) \approx 10^{60}$$

prime. By Hasse's theorem, this means $p \approx 10^{60}$.

Four questions:

- given p, N, find $E/\mathbf{F}_p$ with $\#E(\mathbf{F}_p) = N$
- given p, find $E/\mathbf{F}_p$ of prime order
- given N, find p and $E/\mathbf{F}_p$ with $\#E(\mathbf{F}_p) = N$
- given k, find p and $E/\mathbf{F}_p$ with $\#E(\mathbf{F}_p) \approx 10^k$ prime

Prescribing p

For given N, a curve E with $\#E(\mathbf{F}_p) = N$ exists *if and only if*

$$N \in [p+1-2\sqrt{p}, p+1+2\sqrt{p}].$$

To find E, we should count the number of points on *randomly* selected curves: this is *faster* than using 'CM-techniques'.

Run time I: $\widetilde{O}(\sqrt{p})$. (*probabilistic*)

If we only insist that E has prime order, then the run time drops significantly. Reason: there are many primes, but only one N ...

Run time II: $O((\log p)^5)$. (*heuristic*)

Stay tuned for a faster solution to problem 2.

Prescribing the group order

Efficient constructions for the other 2 problems rely on *complex multiplication techniques*.

Any elliptic curve $E/\mathbf{F}_p$ has a Frobenius morphism

$$\mathrm{Frob}(x, y) = (x^p, y^p)$$

that satisfies

$$\mathrm{Frob}^2 - t\mathrm{Frob} + p = 0 \in \mathrm{End}(E).$$

The ring $\mathbf{Z}[\mathrm{Frob}]$ is isomorphic to the imaginary quadratic order $\mathcal{O}_D$ of discriminant $D = t^2 - 4p < 0$.

We will assume $t \neq 0$. The curve E is then *ordinary* and the index $[\mathrm{End}(E) : \mathbf{Z}[\mathrm{Frob}]]$ is *finite*.

Complex multiplication constructions

The morphism $\mathrm{Frob} : E \to E$ corresponds to an element $\pi \in \mathcal{O}_D$ of *norm* p and *trace* t.

If $E/\mathbf{F}_p$ has endomorphism algebra $\mathbf{Q}(\sqrt{t^2-4p})$ then it has

$$N = \#\mathrm{Ker}(1-\mathrm{Frob}) = \mathrm{Norm}(1-\pi) = p+1\pm t$$

points.

We see: constructing curves of prescribed order is 'the same' as constructing curves with prescribed endomorphism algebra.

Curves with given endomorphism ring

Over $\mathbf{C}$, the j-invariants of the elliptic curves with endomorphism ring $\mathcal{O}_D$ are roots of the *Hilbert class polynomial*

$$P_D = \prod_{[I] \in \mathrm{Pic}(\mathcal{O}_D)} (X - j(I)) \in \mathbf{Z}[X].$$

This polynomial has degree roughly $\sqrt{|D|}$ and coefficients of $\sqrt{|D|}$ bits.

If $p = \pi\overline{\pi}$ splits into principal primes in $\mathcal{O}_D$, then P_D factors into linear factors over $\mathbf{F}_p$.

The roots of $P_D \in \mathbf{F}_p[X]$ are j-invariants of curves with $p+1-t = N$ points.

Curve construction

If $\mathcal{O}_D$ contains an element π with

$$\mathrm{Norm}(1-\pi) = N \text{ (prime)} \qquad \text{and} \qquad \mathrm{Norm}(\pi) = p \text{ (prime)}$$

then we can use $P_D \in \mathbf{F}_p[X]$ to find a curve with N points.

Observation: the condition on D is symmetric in π in $1-\pi$. Hence: prescribing N or prescribing p is ‘the same’.

Theorem. (Atkin-Morain-Bröker-Stevenhagen)
An elliptic curve of prime order $\approx 10^k$ can be constructed in heuristic time $\widetilde{O}(k^3)$.

The method where N is prescribed can be generalized to non-prime N to yield a run time $O(2^{\omega(N)}(\log N)^{4+o(1)})$.

The main tool

The fastest way to compute the Hilbert class polynomial P_D is the *CRT-approach*.

Three-stage-conception:

- Agashe, Lauter, Venkatesan (2004): $O(|D|^{3/2})$
- Belding, Bröker, Enge, Lauter (2008): $O(|D|^{1+o(1)})$
- Sutherland (2009): $O(|D|^{1+o(1)})$. Smaller 'lower order term' and a *huge* practical speed up.

We saw yesterday: $D \approx -10^{14}$ is now feasible if we use smaller functions.

A key concept in the CRT-approach

The CRT-approach computes $P_D \in \mathbf{F}_p[X]$ for many, smartly chosen primes p.

To compute $P_D \bmod p$, we find one root by a random search and apply the *Galois action* of $\mathrm{Pic}(\mathcal{O}_D)$ to find the other roots.

A prime $\mathcal{O}_D$-ideal L of norm l acts on a root $j(E)$ via

$$j(E) \mapsto j(E/E[L]),$$

i.e., via an 'l-isogeny'. We can use the *modular polynomial* of level l to compute this action.

An extension to *abelian surfaces* should use the same technique!

How about genus 2?

Main Philosophy. Everything for elliptic curves can be generalized to (principally polarized) abelian surfaces.

We again want to construct abelian surfaces $A/\mathbf{F}_p$ of prime order N.

By Hasse-Weil, we have $N \approx p^2$.

Basic questions:

- given p, find $A/\mathbf{F}_p$ of prime order
- given N, find a finite field $\mathbf{F}_p$ and $A/\mathbf{F}_p$ with $\#A(\mathbf{F}_p) = N$
- given k, find a finite field $\mathbf{F}_p$ and $A/\mathbf{F}_p$ with $\#A(\mathbf{F}_p) \approx 10^k$ prime.

Bad news for first question

The generalization of Schoof's point counting algorithm to abelian surfaces is polynomial time.

We can find an abelian surface over $\mathbf{F}_p$ of prime order in heuristic polynomial time.

However: that is only theory. *In practice* point counting is slow!

Point counting has been improved a lot recently, but it is not yet practical in the cryptographic range.

Question. *How about the CM-approach?*

CM-theory for genus 2

Just as for elliptic curves, we want to construct an abelian surface with prescribed *endomorphism algebra* K.

In the case that interests us, K is a degree 4 CM-field: a quadratic imaginary extension of a totally real field.

With $K = \mathbf{Q}(\pi)$ and $p = \pi\overline{\pi}$, an abelian surface with endomorphism algebra K and Frobenius π has

$$N = \mathrm{Norm}(1 - \pi)$$

points over $\mathbf{F}_p$.

The analogue of the Hilbert class polynomial is the *Igusa class polynomials*. We get *three* polynomials for every field K.

Bad news, part II

A straightforward generalization of the elliptic curve construction does not work!

Theorem. (Howe, Lauter, Stevenhagen) *The CM-method does not allow a polynomial time algorithm to construct, on input of a prime N, a field $\mathbf{F}_p$ and an abelian surface $A/\mathbf{F}_p$ with $\#A(\mathbf{F}_p) = N$.*

The 'reason' is that there are not enough degree 4 CM-fields.

Sidenote. It does often allow for a fast algorithm to compute genus 2 curves of given order. Perhaps not useful for cryptography…

Natural question. Can we tweak the CM-approach for elliptic curves so that it does generalize?

Back to genus 1

An alternative approach to constructing an elliptic curve of prime order $\approx 10^k$ is as follows.

- fix a negative discriminant $D = 5 \bmod 8$
- find a prime $p \approx 10^k$ that factors as $p = \pi\overline{\pi} \in \mathcal{O}_D$
- if $\mathrm{Norm}(1-\pi)$ is prime, construct the curve over $\mathbf{F}_p$. Else, find the next prime p.

The heuristic run time is $\widetilde{O}(k^4)$, due to the many primality tests.

However: the order $\mathcal{O}_D$ is fixed now. This slower approach *does* generalize!

Remainder of talk. *How to compute the Igusa class polynomials?*

CM-theory for genus 2, the math

Let K be an imaginary quadratic extension of a real quadratic field, and let L be its Galois closure.

Lemma. *We have* $\mathrm{Gal}(L/\mathbf{Q}) \cong C_4, C_2 \times C_2, D_4$.

The 4 embeddings $K \hookrightarrow \mathbf{C}$ naturally come in 2 pairs $\Phi = \{\varphi_1, \varphi_2\}$ and $\Phi' = \{\varphi_1, \overline{\varphi}_2\}$. We exclude $\mathrm{Gal}(K/\mathbf{Q}) \cong C_2 \times C_2$.

The *reflex field* of (K, Φ) is

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

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

Leading example

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

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

We have $K_\Phi = \mathbf{Q}[X]/(X^4 + 172X^3 + 7840X^2 + 11904X + 340992)$ and $K^+ = \mathbf{Q}(\sqrt{3})$.

Abelian surfaces associated to ideals

For an ideal $I \subseteq \mathcal{O}_K$, the quotient $A_I = \mathbf{C}^2/\Phi(I)$ is an abelian surface. 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.

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*

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

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

Igusa class polynomials

Theorem. (Shimura) *The Igusa class polynomials P_K, Q_K, R_K all have degree*

$$\varepsilon \frac{\#\mathrm{Pic}(\mathcal{O}_K)}{\#\mathrm{Pic}^+(\mathcal{O}_{K^+})} \#((\mathcal{O}_{K^+}^*)^+/N_{K/K^+}(\mathcal{O}_K^*))$$

with $\varepsilon \in \{1, 2\}$ depending on whether K is Galois or not.

The polynomials P_K, Q_K, R_K have *rational* coefficients. Their denominators have only recently been bounded (Goren, Lauter).

The Igusa polynomials are typically not irreducible over $\mathbf{Q}$.

Computing P_K, Q_K, R_K

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

- complex arithmetic: not for every K *(Spallek ('94), Streng ('08))*
- 2-adic arithmetic: compute a *canonical lift*, strong condition on the splitting behaviour of the prime 2 *(Kohel-Ritzenthaler-Weng-Houtmann-Gaudry ('05))*
- $\mathbf{F}_p$-arithmetic: Chinese remaindering *(Eisenträger-Lauter ('05))*

Remainder of talk. *How far are we from using the Galois action in a CRT-approach?*

Leading example

We have $\mathrm{Cl}(\mathcal{O}_K) \cong \mathbf{Z}/4\mathbf{Z}$. Of the 4 ideal classes, ideals I from only 2 classes yield p.p.a.s.'s A_I. We take $I = \mathcal{O}_K$ and $A_I = \mathbf{C}^2/\Phi(\mathcal{O}_K)$.

We have $\mathrm{Cl}(\mathcal{O}_{K_\Phi}) \cong \mathbf{Z}/4\mathbf{Z}$ and $\mathrm{Gal}(H(K_\Phi)/K_\Phi) \cong \mathbf{Z}/4\mathbf{Z}$.

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

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

The Artin map gives an isomorphism $\mathrm{Cl}(\mathcal{O}_{K_\Phi}) \xrightarrow{\sim} \mathrm{Gal}(H(K_\Phi)/K_\Phi)$.

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

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

of $A[p]$. This space is 2-dimensional as $\mathbf{F}_p$-vector space.

The ideal $\mathfrak{p} \subset \mathcal{O}_{K_\Phi}$ 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 compute $(3) = \widetilde{\mathfrak{p}}_1^2 \, \widetilde{\mathfrak{p}}_2^2$.

The images under N_Φ are given by

$$N_\Phi(\mathfrak{p}_1) = \widetilde{\mathfrak{p}}_1^2 \qquad N_\Phi(\mathfrak{p}_2) = \widetilde{\mathfrak{p}}_2^2 \qquad N_\Phi(\mathfrak{p}_3) = \widetilde{\mathfrak{p}}_1 \widetilde{\mathfrak{p}}_2.$$

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

Both in dimension 1 ($[K : \mathbf{Q}] = 2$) and dimension 2, the CM-action is given by *isogenies*.

In genus 1 we can use the curve $Y_0(p)$ parametrizing elliptic curves with a p-isogeny to explicitly compute the CM-action.

The Siegel modular variety $Y_0^{(2)}(p)$ is the 'correct analogue' of $Y_0(p)$. Points on $Y_0^{(2)}(p)$ are p.p.a.s.'s together with an *isotropic* (p,p)-isogeny.

Bröker, Lauter (preprint, '08): investigate explicit models for $Y_0^{(2)}(p)$.

A model for $Y_0^{(2)}(p)$ is given by an ideal $I_p \subset \mathbf{Z}[X_1, Y_1, Z_1, X_2, Y_2, Z_2]$. A point

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

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

Computing the CM-action over finite fields

Setup:

- $A/\mathbf{F}_q$ 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 $I_p \subseteq \mathbf{F}_q[X_1, Y_1, Z_1, X_2, Y_2, Z_2]$ describing $Y_0^{(2)}(p)$ over $\mathbf{F}_q$.

Specialize I_p in $(X_1, Y_1, Z_1) = (j_1(A), j_2(A), j_3(A)) \in \mathbf{F}_q^3$. There are exactly $(p^4 - 1)/(p - 1)$ solutions over $\overline{\mathbf{F}}_q$ 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 $\mathbf{F}_q$.

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}.

The denominator bounds yield that 1609 does *not* divide the denominators of P_K, Q_K, R_K.

The polynomials P_K, Q_K, R_K factor completely modulo q.

A random search over $(j_1, j_2, j_3) \in \mathbf{F}_q^3$ yields that $A/\mathbf{F}_q$ 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 $x \in \mathbf{Z}^2$, define $\theta_x : \mathbf{H}_2 \to \mathbf{C}$ by

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

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 $\Gamma(8) \subset \mathrm{Sp}(4, \mathbf{Z})$. Let $\mathrm{Stab}(f)$ be their stabilizer.

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

A ‘smaller’ function

The functions f_i are Siegel modular forms of level 8. Affine points on $X(f)$ can be viewed as tuples (A, L) with A a p.p.a.s. and L a level-8 structure.

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 $Y(f) = \mathrm{Stab}(f)\backslash\mathbf{H}_2$, 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 $X(f;p)$

$$
\begin{tikzcd}
 & & X(f;p) \arrow[dll, "s"'] \arrow[drr, "t"] \arrow[ddll, bend right=20, "F"] \arrow[ddrr, bend left=20, "F'"'] & & \\
X(f) \arrow[d, "f_i"] & & & & X(f) \arrow[d, "f_i"'] \\
\mathbf{P}^3_w & & & & \mathbf{P}^3_w \\
\mathbf{A}^3 \arrow[u] & & & & \mathbf{A}^3 \arrow[u]
\end{tikzcd}
$$

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 $X(f;p)$.

For $p = 3$ this is 'easy'. We find 85 homogeneous degree 6 polynomials describing $X(f;3)$.

One of them is

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

Computing the CM-action over finite fields, II

Setup:

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

Choose a point (w, x, y, z) on $X(f)$ mapping to $(j_1(A), j_2(A), j_3(A))$. This requires working over a degree 24 extension.

Specialize I_3^f in $(W_1, X_1, Y_1, Z_1) = (w, x, y, z)$. There are exactly 40 solutions over $\overline{\mathbf{F}}_q$ of the remaining system of equations. Map them 'down' to find 40 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 $\mathbf{F}_q$.

The leading example

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

We choose

$$w = 450\alpha^3 + 100\alpha^2 + 437\alpha + 830$$

$$x = 311\alpha^3 + 1375\alpha^2 + 498\alpha + 817$$

$$y = 738\alpha^3 + 276\alpha^2 + 1004\alpha + 354$$

$$z = 21\alpha^3 + 363\alpha^2 + 1403\alpha + 1310$$

lying over $(j_1(A), j_2(A), j_3(A)) = (1563, 789, 704) \in \mathbf{F}_q^3$.

Specializing the ideal I_3^f in w, x, y, z yields a system of equations in 4 variables over $\mathbf{F}_{q^4}$. It has 40 solutions over $\overline{\mathbf{F}}_q$. We only look at solutions over $\mathbf{F}_{q^{24}}$.

The leading example

We map all 'f-tuples' down to Igusa triples. Over $\mathbf{F}_q$ 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.s.'s with endomorphism ring $\mathcal{O}_K$, some are not.

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

The leading example

We compute

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

$$(1350, 1316, 1483) \xrightarrow{\mathfrak{p}_1} (1563, 789, 704).$$

The polynomial $(X - 1563) \cdot \ldots \cdot (X - 1350) \in \mathbf{F}_q[X]$ 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

$$P_K = X^8 + 455X^7 + 410X^6 + 259X^5 + 323X^4$$

$$+153X^3 + 289X^2 + 942X + 416 \bmod 1609.$$

The leading example

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

The resulting polynomial factors over K_Φ into 2 irreducible quartics.

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

The polynomial P_K defines the Hilbert class field of K_Φ.

What remains to be done

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: the naive way of computing I_5^f takes too long.

Questions.

- how much trickery is there to speed up the computation of I_5^f?
- are there even smaller functions out there?
- does it help to work inside weighted projective space?

$$\vdots$$

- *how to compute isogenies between abelian surfaces?*