Factorization of polynomials over finite fields in *deterministic* polynomial-time

Ivan Boyer

Doctorant sous la direction de Jean-François Mestre
Institut Mathématique de Jussieu

AGCT-13 — C.I.R.M.
March 15, 2011

Algorithmic aspect.

Remark

The deterministic aspect is crucial in this talk : everything becomes "trivial" in probabilistic time. In the same way, assuming G.R.H. would withdraw some of the interest of the following !

Factorization in $\mathbb{F}_p[X]$ – Square roots in $\mathbb{F}_p$.

- There are deterministic algorithms in $\mathbb{F}_p[X]$ (*e.g.* Berlekamp's algorithm) but exponential in $\log p$.
- **No deterministic polynomial-time algorithm is known** for factorization in $\mathbb{F}_p[X]$. Even in degree 2 !
- Easy to decide if $a \in \mathbb{F}_p$ is a square (Legendre symbol, or more generally the g.c.d. with $x^p - x$)
- A lot of literature for square root probabilistic-algorithms, but as for now, we don't know if it's a **P**–problem.
- However, thanks to **Schoof's algorithm**, we can say something in ***deterministic* time**.

Factorization in $\mathbb{F}_p[X]$ – Square roots in $\mathbb{F}_p$.

- There are deterministic algorithms in $\mathbb{F}_p[X]$ (*e.g.* Berlekamp's algorithm) but exponential in $\log p$.
- **No deterministic polynomial-time algorithm is known** for factorization in $\mathbb{F}_p[X]$. Even in degree 2 !
- Easy to decide if $a \in \mathbb{F}_p$ is a square (Legendre symbol, or more generally the g.c.d. with $x^p - x$)
- A lot of literature for square root probabilistic-algorithms, but as for now, we don't know if it's a **P**–problem.
- However, thanks to **Schoof's algorithm**, we can say something in ***deterministic* time**.

Factorization in $\mathbb{F}_p[X]$ – Square roots in $\mathbb{F}_p$.

- There are deterministic algorithms in $\mathbb{F}_p[X]$ (*e.g.* Berlekamp's algorithm) but exponential in $\log p$.
- **No deterministic polynomial-time algorithm is known** for factorization in $\mathbb{F}_p[X]$. Even in degree 2 !
- Easy to decide if $a \in \mathbb{F}_p$ is a square (Legendre symbol, or more generally the g.c.d. with $x^p - x$)
- A lot of literature for square root probabilistic-algorithms, but as for now, we don't know if it's a **P**–problem.
- However, thanks to **Schoof's algorithm**, we can say something in ***deterministic* time**.

Factorization in $\mathbb{F}_p[X]$ – Square roots in $\mathbb{F}_p$.

- There are deterministic algorithms in $\mathbb{F}_p[X]$ (*e.g.* Berlekamp's algorithm) but exponential in $\log p$.
- **No deterministic polynomial-time algorithm is known** for factorization in $\mathbb{F}_p[X]$. Even in degree 2 !
- Easy to decide if $a \in \mathbb{F}_p$ is a square (Legendre symbol, or more generally the g.c.d. with $x^p - x$)
- A lot of literature for square root probabilistic-algorithms, but as for now, we don't know if it's a **P**–problem.
- However, thanks to **Schoof's algorithm**, we can say something in ***deterministic*** **time**.

Factorization in $\mathbb{F}_p[X]$ – Square roots in $\mathbb{F}_p$.

- There are deterministic algorithms in $\mathbb{F}_p[X]$ (*e.g.* Berlekamp's algorithm) but exponential in $\log p$.
- **No deterministic polynomial-time algorithm is known** for factorization in $\mathbb{F}_p[X]$. Even in degree 2 !
- Easy to decide if $a \in \mathbb{F}_p$ is a square (Legendre symbol, or more generally the g.c.d. with $x^p - x$)
- A lot of literature for square root probabilistic-algorithms, but as for now, we don't know if it's a **P**–problem.
- However, thanks to **Schoof's algorithm**, we can say something in ***deterministic* time**.

Schoof's algorithm and square roots.

In his 1985 paper, Schoof showed these two results :

Theorem

Let E be an elliptic curve defined over $\mathbb{F}_p$. There's a deterministic algorithm, polynomial in $\log p$, that counts the number of rational points of E over $\mathbb{F}_p$

Corollary

Let $a \in \mathbb{Z}$ be a fixed integer. There's a deterministic algorithm, polynomial in $\log p$, that finds a square root of $a \mod p$.

Schoof's algorithm and square roots : ideas

1. We assume $p \equiv 1[4]$ (otherwise, $\left(a^{\frac{p+1}{4}}\right)^2 = a$) and so $a < 0$.
2. So a (or $4a$) is a discriminant of a quadratic imaginary field.
3. In constant time (depending "badly" on a) we write the equation of an elliptic curve E_a s.t. :
   - E_a is defined over an extension of $\mathbb{F}_p$ depending only on a.
   - E_a **has complex multiplication by an order of** $\mathbb{Q}[\sqrt{a}]$
4. **The Frobenius** π **belongs to** $\mathrm{End}(E_a)$:

$$\pi = \frac{a + b\sqrt{D}}{2}$$

With $\#E_a$, we know $\mathrm{Tr}(\pi)$ and its norm, so :

$$a^2 - b^2 D \equiv 0[p]$$

and $\frac{a}{b}$ is the wanted square root.

Schoof's algorithm and square roots : ideas

1. We assume $p \equiv 1[4]$ (otherwise, $\left(a^{\frac{p+1}{4}}\right)^2 = a$) and so $a < 0$.
2. So a (or $4a$) is a discriminant of a quadratic imaginary field.
3. In constant time (depending "badly" on a) we write the equation of an elliptic curve E_a s.t. :
   - E_a is defined over an extension of $\mathbb{F}_p$ depending only on a.
   - E_a **has complex multiplication by an order of** $\mathbb{Q}[\sqrt{a}]$
4. **The Frobenius** π **belongs to** $\mathrm{End}(E_a)$:

$$\pi = \frac{a + b\sqrt{D}}{2}$$

With $\#E_a$, we know $\mathrm{Tr}(\pi)$ and its norm, so :

$$a^2 - b^2 D \equiv 0[p]$$

and $\frac{a}{b}$ is the wanted square root.

Schoof's algorithm and square roots : ideas

1. We assume $p \equiv 1[4]$ (otherwise, $\left(a^{\frac{p+1}{4}}\right)^2 = a$) and so $a < 0$.
2. So a (or $4a$) is a discriminant of a quadratic imaginary field.
3. In constant time (depending "badly" on a) we write the equation of an elliptic curve E_a s.t. :
   - E_a is defined over an extension of $\mathbb{F}_p$ depending only on a.
   - E_a **has complex multiplication by an order of** $\mathbb{Q}[\sqrt{a}]$
4. **The Frobenius π belongs to** $\mathrm{End}(E_a)$:

$$\pi = \frac{a + b\sqrt{D}}{2}$$

With $\#E_a$, we know $\mathrm{Tr}(\pi)$ and its norm, so :

$$a^2 - b^2 D \equiv 0[p]$$

and $\frac{a}{b}$ is the wanted square root.

Schoof's algorithm and square roots : ideas

1. We assume $p \equiv 1[4]$ (otherwise, $\left(a^{\frac{p+1}{4}}\right)^2 = a$) and so $a < 0$.
2. So a (or $4a$) is a discriminant of a quadratic imaginary field.
3. In constant time (depending "badly" on a) we write the equation of an elliptic curve E_a s.t. :
   - E_a is defined over an extension of $\mathbb{F}_p$ depending only on a.
   - E_a **has complex multiplication by an order of** $\mathbb{Q}[\sqrt{a}]$
4. **The Frobenius** π **belongs to** $\mathrm{End}(E_a)$:

$$\pi = \frac{a + b\sqrt{D}}{2}$$

With $\#E_a$, we know $\mathrm{Tr}(\pi)$ and its norm, so :

$$a^2 - b^2 D \equiv 0[p]$$

and $\frac{a}{b}$ is the wanted square root.

Generalization of Schoof's result : what we want to do.

- So, if we fix a polynomial of degree 2, we can factorize its reduction over $\mathbb{F}_p$ in *deterministic* polynomial time in $\log p$.
- Now, we want to do the same thing in **higher degree**, with abelian varieties.
- **Cyclotomic polynomials** is a familiy with a lot of interesting properties !
- We can hope in a first time to :
  1. Find their roots in $\mathbb{F}_p$ if they have any.
  2. Factorize them (ie. find the roots in extensions).
  3. Generalize to abelian extensions.

Generalization of Schoof's result : what we want to do.

- So, if we fix a polynomial of degree 2, we can factorize its reduction over $\mathbb{F}_p$ in *deterministic* polynomial time in $\log p$.
- Now, we want to do the same thing in **higher degree**, with abelian varieties.
- **Cyclotomic polynomials** is a familiy with a lot of interesting properties !
- We can hope in a first time to :
  1. Find their roots in $\mathbb{F}_p$ if they have any.
  2. Factorize them (ie. find the roots in extensions).
  3. Generalize to abelian extensions.

Generalization of Schoof's result : what we want to do.

- So, if we fix a polynomial of degree 2, we can factorize its reduction over $\mathbb{F}_p$ in *deterministic* polynomial time in $\log p$.
- Now, we want to do the same thing in **higher degree**, with abelian varieties.
- **Cyclotomic polynomials** is a familiy with a lot of interesting properties !
- We can hope in a first time to :
  1. Find their roots in $\mathbb{F}_p$ if they have any.
  2. Factorize them (ie. find the roots in extensions).
  3. Generalize to abelian extensions.

Generalization of Schoof's result : what we want to do.

- So, if we fix a polynomial of degree 2, we can factorize its reduction over $\mathbb{F}_p$ in *deterministic* polynomial time in $\log p$.
- Now, we want to do the same thing in **higher degree**, with abelian varieties.
- **Cyclotomic polynomials** is a familiy with a lot of interesting properties !
- We can hope in a first time to :
  1. Find their roots in $\mathbb{F}_p$ if they have any.
  2. Factorize them (ie. find the roots in extensions).
  3. Generalize to abelian extensions.

Pila's generalization to Schoof's algorithm.

Pila generalized Schoof's algorithm :

Theorem (Pila, 1989)

Given an abelian variety A over $\mathbb{F}_q$ (with equations for the group law), it's possible to compute the number of $\mathbb{F}_q$–points in polynomial time in $\log q$ *and hence the zeta function of A.*

The easiest way to use this result is when A is a *jacobian* of a curve.
With the Fermat curve, Pila obtained

Theorem

Fixing a prime l and assuming $p \equiv 1[l]$, it's possible to find the roots, in $\mathbb{F}_p$, of $\phi_l(X) = \frac{X^l-1}{X-1}$ in deterministic polynomial-time in $\log p$.

Pila's generalization to Schoof's algorithm.

Pila generalized Schoof's algorithm :

Theorem (Pila, 1989)

Given an abelian variety A over $\mathbb{F}_q$ (with equations for the group law), it's possible to compute the number of $\mathbb{F}_q$–points in polynomial time in $\log q$ and hence the zeta function of A.

The easiest way to use this result is when A is a *jacobian* of a curve.
With the Fermat curve, Pila obtained

Theorem

Fixing a prime l and assuming $p \equiv 1[l]$, it's possible to find the roots, in $\mathbb{F}_p$, of $\phi_l(X) = \frac{X^l-1}{X-1}$ in deterministic polynomial-time in $\log p$.

"Separation" of primes.

Sketch of the proof :

1. The Fermat curve has **complex multiplication by the l^{th}–cyclotomic field $\mathbb{Q}(\zeta_l)$**.
2. (p) totally splits in $\mathbb{Z}[\zeta_l]$ and the ideal (π), generated by the Frobenius, is the product of $\frac{l-1}{2}$ ideals of the shape $(\zeta_l - a)$ (with $\phi_l(a) \equiv 0[p]$).
3. **The action of $\mathrm{Gal}(\mathbb{Q}(\zeta_l)/\mathbb{Q})$ "splits" the primes**, *i.e.* there're never two ideals above (p) dividing exactly the same conjugates of (π).
4. We deduce a root a of ϕ_l, just by calculating some g.c.d.

"Separation" of primes.

Sketch of the proof :

1. The Fermat curve has **complex multiplication by the l^{th}–cyclotomic field $\mathbb{Q}(\zeta_l)$**.
2. (p) totally splits in $\mathbb{Z}[\zeta_l]$ and the ideal (π), generated by the Frobenius, is the product of $\frac{l-1}{2}$ ideals of the shape $(\zeta_l - a)$ (with $\phi_l(a) \equiv 0[p]$).
3. **The action of $\mathrm{Gal}(\mathbb{Q}(\zeta_l)/\mathbb{Q})$ "splits" the primes**, *i.e.* there're never two ideals above (p) dividing exactly the same conjugates of (π).
4. We deduce a root a of ϕ_l, just by calculating some g.c.d.

"Separation" of primes.

Sketch of the proof :

1. The Fermat curve has **complex multiplication by the l^{th}–cyclotomic field** $\mathbb{Q}(\zeta_l)$.
2. (p) totally splits in $\mathbb{Z}[\zeta_l]$ and the ideal (π), generated by the Frobenius, is the product of $\frac{l-1}{2}$ ideals of the shape $(\zeta_l - a)$ (with $\phi_l(a) \equiv 0[p]$).
3. **The action of** $\mathrm{Gal}(\mathbb{Q}(\zeta_l)/\mathbb{Q})$ **"splits" the primes**, *i.e.* there're never two ideals above (p) dividing exactly the same conjugates of (π).
4. We deduce a root a of ϕ_l, just by calculating some g.c.d.

"Separation" of primes.

Sketch of the proof :

1. The Fermat curve has **complex multiplication by the l^{th}–cyclotomic field** $\mathbb{Q}(\zeta_l)$.
2. (p) totally splits in $\mathbb{Z}[\zeta_l]$ and the ideal (π), generated by the Frobenius, is the product of $\frac{l-1}{2}$ ideals of the shape $(\zeta_l - a)$ (with $\phi_l(a) \equiv 0[p]$).
3. **The action of** $\mathrm{Gal}(\mathbb{Q}(\zeta_l)/\mathbb{Q})$ **"splits" the primes**, *i.e.* there're never two ideals above (p) dividing exactly the same conjugates of (π).
4. We deduce a root a of ϕ_l, just by calculating some g.c.d.

Example of separation.

$l = 5$, $p = 11$ and $(F_5) : x^5 + y^5 + z^5$ over $\mathbb{F}_{11}$

The numerator of the zeta function of F_5 can be computed :

$$L(F_5/F_p, \pi) = (\pi^4 + \pi^3 - 9\pi^2 + 11\pi + 121)^3.$$

The number field generated by π is isomorphic to $\mathbb{Q}(\zeta_5)$. For instance,

$$\begin{aligned}
\pi &= -3\zeta_5^3 - \zeta_5^2 + \zeta_5 - 1 \\
\psi_2(\pi) &= \zeta_5^3 + 2\zeta_5^2 - 2\zeta_5 \\
\psi_3(\pi) &= 4\zeta_5^3 + 3\zeta_5^2 + 2\zeta_5 + 2 \\
\psi_4(\pi) &= -2\zeta_5^3 - 4\zeta_5^2 - \zeta_5 - 2
\end{aligned}$$

Example of separation.

$$\boxed{l = 5,\ p = 11 \text{ and } (F_5) : x^5 + y^5 + z^5 \text{ over } \mathbb{F}_{11}}$$

- It remains to compute some g.c.d. : as l is fixed, we can compute all of them if we want.
- Here, we compute for instance the g.c.d. of the polynomials in ζ_5 which give π and $\psi_2(\pi)$.

$$\mathrm{Gcd}_{\mathbb{F}_p}(-3X^3 - X^2 + X - 1, X^3 + 2X^2 - 2X) = X + 6$$

- So, $-6 = 5[11]$ is a 5^{th} primitive root of unity.
- The others are $5^2 = 3[11]$, $5^3 = 4[11]$ and $5^4 = 9[11]$.

Separation of "primes", CM types and simple abelian varieties (1).

- The demonstration of the "separation" uses Jacobi sums, for which l and p prime is important.
- The jacobian of the Fermat curve isn't a simple abelian variety over $\mathbb{F}_p$: we don't need all of it !
- The idea is to use **hyperelliptic curves with complex multiplication by** $\mathbb{Q}(\zeta_l)$.

Proposition

Let l, p to primes s.t. $p \equiv 1[l]$. Then, the jacobian of the curve $y^2 = x^l - 1$ over $\mathbb{F}_p$ is simple and its Frobenius generates $\mathbb{Q}(\zeta_l)$.

Once we have the "separation" property, the mechanism is the same as above.

Separation of "primes", CM types and simple abelian varieties (1).

- The demonstration of the "separation" uses Jacobi sums, for which l and p prime is important.
- The jacobian of the Fermat curve isn't a simple abelian variety over $\mathbb{F}_p$: we don't need all of it !
- The idea is to use **hyperelliptic curves with complex multiplication by $\mathbb{Q}(\zeta_l)$**.

Proposition

Let l, p to primes s.t. $p \equiv 1[l]$. Then, the jacobian of the curve $y^2 = x^l - 1$ over $\mathbb{F}_p$ is simple and its Frobenius generates $\mathbb{Q}(\zeta_l)$.

Once we have the "separation" property, the mechanism is the same as above.

Separation of "primes", CM types and simple abelian varieties (1).

- The demonstration of the "separation" uses Jacobi sums, for which l and p prime is important.
- The jacobian of the Fermat curve isn't a simple abelian variety over $\mathbb{F}_p$: we don't need all of it !
- The idea is to use **hyperelliptic curves with complex multiplication by** $\mathbb{Q}(\zeta_l)$.

Proposition

Let l, p to primes s.t. $p \equiv 1[l]$. Then, the jacobian of the curve $y^2 = x^l - 1$ over $\mathbb{F}_p$ is simple and its Frobenius generates $\mathbb{Q}(\zeta_l)$.

Once we have the "separation" property, the mechanism is the same as above.

Separation of "primes", CM types and simple abelian varieties (2).

- The hyperelliptic curve $y^2 = x^l - 1$ has the automorphism

$$(x, y) \mapsto (\zeta_l x, y)$$

- We find the CM type with its action on a basis of differentials:

$$\left\{ x^i \frac{\mathrm{d}x}{y},\ 0 \leqslant i \leqslant \frac{l-3}{2} \right\}$$

$$[\zeta_l]^* x^i \frac{\mathrm{d}x}{y} = \zeta_l^{i+1} x^i \frac{\mathrm{d}x}{y} =: \psi_{i+1}(\zeta_l) x^i \frac{\mathrm{d}x}{y}$$

and so the CM type is :

$$\Psi = \left\{ \psi_i,\ 1 \leqslant i \leqslant \frac{l-1}{2} \right\}$$

Separation of "primes", CM types and simple abelian varieties (2).

- The hyperelliptic curve $y^2 = x^l - 1$ has the automorphism

$$(x, y) \mapsto (\zeta_l x, y)$$

- We find the CM type with its action on a basis of differentials:

$$\left\{ x^i \frac{\mathrm{d}x}{y},\ 0 \leqslant i \leqslant \frac{l-3}{2} \right\}$$

$$[\zeta_l]^* x^i \frac{\mathrm{d}x}{y} = \zeta_l^{i+1} x^i \frac{\mathrm{d}x}{y} =: \psi_{i+1}(\zeta_l) x^i \frac{\mathrm{d}x}{y}$$

and so the CM type is :

$$\Psi = \left\{ \psi_i,\ 1 \leqslant i \leqslant \frac{l-1}{2} \right\}$$

Separation of "primes", CM types and simple abelian varieties (3).

- An easy computation shows that the CM type Ψ is primitive so the abelian variety is simple.
- The extension $\mathbb{Q}(\zeta_l)/\mathbb{Q}$ is abelian so that $(\mathbb{Q}(\zeta_l), \Psi)$ is *its own reflex*.
- We denote by $\mathfrak{P}$ an ideal above (p), which splits totally $(p \equiv 1[l])$.
- We use a theorem of Shimura to show the existence of $\pi_0 \in \mathbb{Z}[\zeta_l]$ corresponding to the Frobenius (of the reduction mod $\mathfrak{P}$) s.t.

$$(\pi_0) = \prod_{\psi \in \Psi} \psi^{-1}(\mathfrak{P}).$$

Separation of "primes", CM types and simple abelian varieties (3).

- An easy computation shows that the CM type Ψ is primitive so the abelian variety is simple.
- The extension $\mathbb{Q}(\zeta_l)/\mathbb{Q}$ is abelian so that $(\mathbb{Q}(\zeta_l), \Psi)$ is *its own reflex*.
- We denote by $\mathfrak{P}$ an ideal above (p), which splits totally $(p \equiv 1[l])$.
- We use a theorem of Shimura to show the existence of $\pi_0 \in \mathbb{Z}[\zeta_l]$ corresponding to the Frobenius (of the reduction mod $\mathfrak{P}$) s.t.

$$(\pi_0) = \prod_{\psi \in \Psi} \psi^{-1}(\mathfrak{P}).$$

Separation of "primes", CM types and simple abelian varieties (3).

- An easy computation shows that the CM type Ψ is primitive so the abelian variety is simple.
- The extension $\mathbb{Q}(\zeta_l)/\mathbb{Q}$ is abelian so that $(\mathbb{Q}(\zeta_l), \Psi)$ is *its own reflex*.
- We denote by $\mathfrak{P}$ an ideal above (p), which splits totally $(p \equiv 1[l])$.
- We use a theorem of Shimura to show the existence of $\pi_0 \in \mathbb{Z}[\zeta_l]$ corresponding to the Frobenius (of the reduction mod $\mathfrak{P}$) s.t.

$$(\pi_0) = \prod_{\psi \in \Psi} \psi^{-1}(\mathfrak{P}).$$

Separation of "primes", CM types and simple abelian varieties (3).

- An easy computation shows that the CM type Ψ is primitive so the abelian variety is simple.
- The extension $\mathbb{Q}(\zeta_l)/\mathbb{Q}$ is abelian so that $(\mathbb{Q}(\zeta_l), \Psi)$ is *its own reflex*.
- We denote by $\mathfrak{P}$ an ideal above (p), which splits totally $(p \equiv 1[l])$.
- We use a theorem of Shimura to show the existence of $\pi_0 \in \mathbb{Z}[\zeta_l]$ corresponding to the Frobenius (of the reduction mod $\mathfrak{P}$) s.t.

$$(\pi_0) = \prod_{\psi \in \Psi} \psi^{-1}(\mathfrak{P}).$$

Separation of "primes", CM types and simple abelian varieties (4).

Proposition

The "separation" property is equivalent to the fact that the CM type is primitive.

Idea : Two prime ideals $\mathfrak{P}_1$ and $\mathfrak{P}_2$ can't be separated *iff* the automorphism ψ s.t. $\psi(\mathfrak{P}_1) = \mathfrak{P}_2$ stabilize the CM type.

Separation of "primes", CM types and simple abelian varieties (4).

Proposition

The "separation" property is equivalent to the fact that the CM type is primitive.

Idea : Two prime ideals $\mathfrak{P}_1$ and $\mathfrak{P}_2$ can't be separated *iff* the automorphism ψ s.t. $\psi(\mathfrak{P}_1) = \mathfrak{P}_2$ stabilize the CM type.

Generalization.

We have **two different kinds of generalization** of this result, **both of them are needed** for the factorization of polynomials which generate abelian extensions.

1. The first one is to obtain the result for every cyclotomic polynomial ϕ_n, n not necessarily prime, but still with roots in $\mathbb{F}_p$.
2. The second one is to generalize to $\mathbb{F}_{p^r}[X]$ or equivalently to factorize in irreducible factors in $\mathbb{F}_p[X]$.

Generalization.

We have **two different kinds of generalization** of this result, **both of them are needed** for the factorization of polynomials which generate abelian extensions.

1. The first one is to obtain the result for every cyclotomic polynomial ϕ_n, n not necessarily prime, but still with roots in $\mathbb{F}_p$.
2. The second one is to generalize to $\mathbb{F}_{p^r}[X]$ or equivalently to factorize in irreducible factors in $\mathbb{F}_p[X]$.

A generalization to ϕ_n, $p \equiv 1[n]$.

- If $n = ab$ with a, b coprime, then, as $p \equiv 1[a]$ and $p \equiv 1[b]$, we only need to find a^{th} and b^{th} primitive roots of unity
- So we concentrate on ϕ_{l^r} with $p \equiv 1[l^r]$.

Proposition

Let p, l primes and $r \in \mathbb{N}^*$ s.t. $p \equiv 1[l^r]$. Then, the jacobian of the hyperelliptic curve $y^2 = x^n - 1$ isn't simple but contains a subvariety with complex multiplication by $\mathbb{Q}(\zeta_{l^r})$ and primitive CM type :

$$\left\{\psi_i,\ 1 \leqslant i \leqslant \frac{l^n - 1}{2}, i \not\equiv 0[l]\right\}.$$

A generalization to ϕ_n, $p \equiv 1[n]$.

- If $n = ab$ with a, b coprime, then, as $p \equiv 1[a]$ and $p \equiv 1[b]$, we only need to find a^{th} and b^{th} primitive roots of unity
- So we concentrate on ϕ_{l^r} with $p \equiv 1[l^r]$.

Proposition

Let p, l primes and $r \in \mathbb{N}^*$ s.t. $p \equiv 1[l^r]$. Then, the jacobian of the hyperelliptic curve $y^2 = x^n - 1$ isn't simple but contains a subvariety with complex multiplication by $\mathbb{Q}(\zeta_{l^r})$ and primitive CM type :

$$\left\{\psi_i,\ 1 \leqslant i \leqslant \frac{l^n - 1}{2}, i \not\equiv 0[l]\right\}.$$

A generalization to ϕ_n, $p \equiv 1[n]$.

We can in fact find better curves s.t. their jacobians are simple, so the genus is reduced from $\frac{l^r-1}{2}$ to $l^{r-1}\frac{l-1}{2}$

Proposition

Let p, l primes and $r \in \mathbb{N}^*$ s.t. $p \equiv 1[l^r]$. Then, the jacobian of the "superelliptic" curve $y^l = x(x^{l^r-1} - 1)$ has complex multiplication by $\mathbb{Q}(\zeta_{l^r})$ with the primitive CM type :

$$\left\{\psi_{l(i+1)-j},\ 1 \leqslant j \leqslant l-1,\ 0 \leqslant i \leqslant l^{n-2}j - 1\right\}.$$

So this jacobian is simple, with complex multiplication by $\mathbb{Q}(\zeta_l)$.

The second generalization : no condition on p mod l.

This generalization is more difficult and depends on the order of p in $(\mathbb{Z}/lZ)^*$. Some examples :

- $l = 11$, $p = 109$: order 2.
  $L = (t^2 + 109)^5$
- $l = 31$, $p = 149$: order 3.
  $L = t^{30} + 6190t^{27} + 18863049t^{24} + 34431784200t^{21} + 43370374988098t^{18} + 5634555160987122 0t^{15} + 43370374988098 \cdot 149^3 t^{12} + 34431784200 \cdot 149^6 t^9 + 18863049 \cdot 149^9 t^6 + 6190 \cdot 149^{12} t^3 + 149^{15}$.
- $l = 31$, $p = 37$: order 6.
  $L = (t^6 + 37^3)^5$.

Order of p : the odd case.

The above results are quite different :

- In the 1^{st} and 3^{rd} example, p is of even order and the zeta function gives no information in term of complex multiplication.
- In the second one, π^3 generates the subfield of index 3 of $\mathbb{Q}(\zeta_{31})$ and everything works well !

Remark

If we note r the order of $p \in (\mathbb{Z}/l\mathbb{Z})^*$, then ϕ_l hasn't any roots in $\mathbb{F}_p$ but in $\mathbb{F}_{p^r}$. So π no longer commutes with $(x, y) \mapsto (\zeta_l x, y)$ but π^r does.

Order of p : the odd case.

Proposition

If the order r of $p \in (\mathbb{Z}/l\mathbb{Z})^*$ is odd, the same deterministic polynomial-time algorithm works to find the roots of the minimal polynomial of

$$\sum_{i=0}^{r-1} \zeta_l^{p^i}$$

which generates the index r subfield of $\mathbb{Q}(\zeta_l)$. This is equivalent to the factorization of ϕ_l over $\mathbb{F}_p$.

Order of p : the even case – real multiplication curves.

We examine now the situation where p is of order 2.
Here, we can use a result of Tautz, Top and Verberkmoes :

Theorem

Let $l \neq 5$ be a prime and let $g \in \mathbb{Z}[X]$ the minimal polynomial of $-\zeta_l - \zeta_l^{-1}$. The jacobian of the hyperelliptic curve $y^2 = xg(x^2-2)$ has a primitive CM type and complex multiplication by the field $\mathbb{Q}(\zeta_l + \zeta_l^{-1}, i)$.

To use it, we first need :

- $p \equiv 1[4]$ to have complex multiplication by i.
- p of order 2 ($p \equiv -1[l]$).

Then, π commutes with $[\zeta_l + \zeta_l^{-1}]$ and $[i]$ (*i.e.* with the automorphism $(x, y) \mapsto (-x, iy)$).

Order of p : the even case – real multiplication curves.

We examine now the situation where p is of order 2.
Here, we can use a result of Tautz, Top and Verberkmoes :

Theorem

Let $l \neq 5$ be a prime and let $g \in \mathbb{Z}[X]$ the minimal polynomial of $-\zeta_l - \zeta_l^{-1}$. The jacobian of the hyperelliptic curve $y^2 = xg(x^2-2)$ has a primitive CM type and complex multiplication by the field $\mathbb{Q}(\zeta_l + \zeta_l^{-1}, i)$.

To use it, we first need :

- $p \equiv 1[4]$ to have complex multiplication by i.
- p of order 2 ($p \equiv -1[l]$).

Then, π commutes with $[\zeta_l + \zeta_l^{-1}]$ and $[i]$ (*i.e.* with the automorphism $(x, y) \mapsto (-x, iy)$).

An example with p of order 2.

$$\boxed{l = 11,\ p = 109.}$$

- $g = t^5 - t^4 - 4t^3 + 3t^2 + 3t - 1.$
- The curve on $\mathbb{F}_{109}$:
  $y^2 = x(x^{10} + 98x^8 + 44x^6 + 32x^4 + 55x^4 + 98).$

The numerator of its zeta function is :

$$t^{10} - 52t^9 + 1345t^8 - 23248t^7 + 311034t^6 - 3493496t^5 + 311034 \cdot 109t^4 - 23248 \cdot 109^2t^3 + 1345 \cdot 109^3t^2 - 52 \cdot 109^4t + 109^5$$

which generates a field isomorphic to $\mathbb{Q}(\zeta_{11} + \zeta_{11}^{-1}, i)$. It "splits" the primes so we find for instance :

$$-\zeta_{11} - \zeta_{11}^{-1} = 90 \in \mathbb{F}_{109},$$

so $x^2 + 90x + 1$ is an irreducible factor of $x^{11} - 1$.

Order of p : the even case – real multiplication curves.

If the order is 4, π^2 and $[\zeta_l + \zeta_l^{-1}]$ commutes, the jacobian has still complex multiplication but it's no longer simple but isogenous to a product of supersingular varieties. Nevertheless,

Proposition

Let A be the jacobian of $y^2 = x^{4l+1} + x$. Then A has a simple abelian subvariety with complex multiplication by the field $K := \mathbb{Q}(\zeta_{8l} - \zeta_{8l}^{-1})$ and with primitive CM type.

Let p prime of order r : π^r and $\zeta_{8l} - \zeta_{8l}^{-1}$ commutes so $\pi^r \in K$.

Conjecture

Let K_0 be the decomposition field of (p) in K. Then $\mathbb{Q}(\pi^r) = K_0$

With this result, we could positively answer our problem !

Order of p : the even case – real multiplication curves.

If the order is 4, π^2 and $[\zeta_l + \zeta_l^{-1}]$ commutes, the jacobian has still complex multiplication but it's no longer simple but isogenous to a product of supersingular varieties. Nevertheless,

Proposition

Let A be the jacobian of $y^2 = x^{4l+1} + x$. Then A has a simple abelian subvariety with complex multiplication by the field $K := \mathbb{Q}(\zeta_{8l} - \zeta_{8l}^{-1})$ and with primitive CM type.

Let p prime of order r : π^r and $\zeta_{8l} - \zeta_{8l}^{-1}$ commutes so $\pi^r \in K$.

Conjecture

Let K_0 be the decomposition field of (p) in K. Then $\mathbb{Q}(\pi^r) = K_0$

With this result, we could positively answer our problem !

Order of p : the even case – Ad hoc constructions.

We can try to **build directly our abelian variety**, with the appropriate complex multiplication and CM type. For instance :

Goal

Find an abelian variety with complex multiplication by

$$\mathbb{Q}\left(\zeta_{13}^{(4)}, i\right) \quad \text{where } \zeta_{13}^{(4)} := \zeta_{13} + \zeta_{13}^{5} + \zeta_{13}^{8} + \zeta_{13}^{12},$$

and primitive CM type.

With p of order 4 in $(\mathbb{Z}/13\mathbb{Z})^*$, and $p \equiv 1[4]$ (for the complex multiplication by $[i]$), the reduction of such a curve mod p shall give a zeta function which generates the field $\mathbb{Q}\left(\zeta_{13}^{(4)}, i\right)$, with the prime "separation" property.

Order of p : the even case – Ad hoc constructions.

Sketch of the construction

1. First, we compute the ring $\mathcal{O}$ of integers of the CM field, we choose our CM type Ψ, such that our torus with the appropriate complex multiplication is $\mathbb{C}^3/\Psi(\mathcal{O})$.
2. With the different of $\mathcal{O}$ we can find a principal polarization together with a a non-degenerate Riemann form.
3. By computing the theta constants, we can check if we have the jacobian of a curve.
4. The complex multiplication by i implies it's an hyperelliptic curve.
5. Mumford gives formulas between theta constants and the Rosenhain form of the hyperelliptic curve.
6. We finally write "beautiful" equations with `algdep`.

Order of p : the even case – Ad hoc constructions.

Sketch of the construction

1. First, we compute the ring $\mathcal{O}$ of integers of the CM field, we choose our CM type Ψ, such that our torus with the appropriate complex multiplication is $\mathbb{C}^3/\Psi(\mathcal{O})$.
2. With the different of $\mathcal{O}$ we can find a principal polarization together with a a non-degenerate Riemann form.
3. By computing the theta constants, we can check if we have the jacobian of a curve.
4. The complex multiplication by i implies it's an hyperelliptic curve.
5. Mumford gives formulas between theta constants and the Rosenhain form of the hyperelliptic curve.
6. We finally write "beautiful" equations with `algdep`.

Order of p : the even case – Ad hoc constructions.

Sketch of the construction

1. First, we compute the ring $\mathcal{O}$ of integers of the CM field, we choose our CM type Ψ, such that our torus with the appropriate complex multiplication is $\mathbb{C}^3/\Psi(\mathcal{O})$.
2. With the different of $\mathcal{O}$ we can find a principal polarization together with a a non-degenerate Riemann form.
3. By computing the theta constants, we can check if we have the jacobian of a curve.
4. The complex multiplication by i implies it's an hyperelliptic curve.
5. Mumford gives formulas between theta constants and the Rosenhain form of the hyperelliptic curve.
6. We finally write "beautiful" equations with `algdep`.

Order of p : the even case – Ad hoc constructions.

Sketch of the construction

1. First, we compute the ring $\mathcal{O}$ of integers of the CM field, we choose our CM type Ψ, such that our torus with the appropriate complex multiplication is $\mathbb{C}^3/\Psi(\mathcal{O})$.
2. With the different of $\mathcal{O}$ we can find a principal polarization together with a a non-degenerate Riemann form.
3. By computing the theta constants, we can check if we have the jacobian of a curve.
4. The complex multiplication by i implies it's an hyperelliptic curve.
5. Mumford gives formulas between theta constants and the Rosenhain form of the hyperelliptic curve.
6. We finally write "beautiful" equations with `algdep`.

Order of p : the even case – Ad hoc constructions.

Sketch of the construction

1. First, we compute the ring $\mathcal{O}$ of integers of the CM field, we choose our CM type Ψ, such that our torus with the appropriate complex multiplication is $\mathbb{C}^3/\Psi(\mathcal{O})$.
2. With the different of $\mathcal{O}$ we can find a principal polarization together with a a non-degenerate Riemann form.
3. By computing the theta constants, we can check if we have the jacobian of a curve.
4. The complex multiplication by i implies it's an hyperelliptic curve.
5. Mumford gives formulas between theta constants and the Rosenhain form of the hyperelliptic curve.
6. We finally write "beautiful" equations with `algdep`.

Order of p : the even case – Ad hoc constructions.

Sketch of the construction

1. First, we compute the ring $\mathcal{O}$ of integers of the CM field, we choose our CM type Ψ, such that our torus with the appropriate complex multiplication is $\mathbb{C}^3/\Psi(\mathcal{O})$.
2. With the different of $\mathcal{O}$ we can find a principal polarization together with a a non-degenerate Riemann form.
3. By computing the theta constants, we can check if we have the jacobian of a curve.
4. The complex multiplication by i implies it's an hyperelliptic curve.
5. Mumford gives formulas between theta constants and the Rosenhain form of the hyperelliptic curve.
6. We finally write "beautiful" equations with `algdep`.

Ad hoc construction : example of $\mathbb{Q}(\zeta_{13}^{(4)}, i)$.

Up to the precision of the computer, we find a curve defined over the (minimal) number field generated by α with minimal polynomial $t^3 - t^2 + 9t - 1$:

$$y^2 = x\left(x^6 - \frac{\alpha^2 - 2\alpha + 13}{2}x^4 - \frac{\alpha^2 - 12\alpha + 1}{2}x^2 - \alpha^2\right).$$

Modulo 109, its reduction is defined over $\mathbb{F}_{109}$:

$$y^2 = x(x^6 + 75x^4 + 96x^2 + 4).$$

The numerator of the zeta function is :

$$t^6 + 14t^5 - 93t^4 - 3148t^3 - 93 \cdot 109t^2 + 14 \cdot 109^2 t + 109^2,$$

and we check that **it generates the field** $\mathbb{Q}\left(\zeta_{13}^{(4)}, i\right)$.

Ad hoc construction : example of $\mathbb{Q}(\zeta_{13}^{(4)}, i)$.

Up to the precision of the computer, we find a curve defined over the (minimal) number field generated by α with minimal polynomial $t^3 - t^2 + 9t - 1$:

$$y^2 = x\left(x^6 - \frac{\alpha^2 - 2\alpha + 13}{2}x^4 - \frac{\alpha^2 - 12\alpha + 1}{2}x^2 - \alpha^2\right).$$

Modulo 109, its reduction is defined over $\mathbb{F}_{109}$:

$$y^2 = x(x^6 + 75x^4 + 96x^2 + 4).$$

The numerator of the zeta function is :

$$t^6 + 14t^5 - 93t^4 - 3148t^3 - 93 \cdot 109t^2 + 14 \cdot 109^2 t + 109^2,$$

and we check that **it generates the field** $\mathbb{Q}\left(\zeta_{13}^{(4)}, i\right)$.

Determine the endomorphism ring (1).

The construction described above has floating point computations and some denominators are not yet bounded. So :

We have to prove the jacobian has CM by $\mathbb{Q}\left(\zeta_{13}^{(4)}, i\right)$.

Before, we notice the good properties of the equation :

- Its coefficients are integers.
- Its discriminant is a square $(64\alpha^{22})$
- The equation can be factorized : let $\beta = \frac{1}{2}\alpha^2 - \alpha + \frac{1}{2}$:

$$y^2 = x(x^3 + \beta x^2 + (\alpha - \beta)x - \alpha)(x^3 - \beta x^2 + (\alpha - \beta)x + \alpha)$$

- The number field $\mathbb{Q}(\alpha)$ has class number 3 and its Hilbert class field, H, is the extension by $\mathbb{Q}\left(\zeta_{13}^{(4)}\right)$.

Determine the endomorphism ring (1).

The construction described above has floating point computations and some denominators are not yet bounded. So :

We have to prove the jacobian has CM by $\mathbb{Q}\left(\zeta_{13}^{(4)}, i\right)$.

Before, we notice the good properties of the equation :

- Its coefficients are integers.
- Its discriminant is a square $(64\alpha^{22})$
- The equation can be factorized : let $\beta = \frac{1}{2}\alpha^2 - \alpha + \frac{1}{2}$:

$$y^2 = x(x^3 + \beta x^2 + (\alpha - \beta)x - \alpha)(x^3 - \beta x^2 + (\alpha - \beta)x + \alpha)$$

- The number field $\mathbb{Q}(\alpha)$ has class number 3 and its Hilbert class field, H, is the extension by $\mathbb{Q}\left(\zeta_{13}^{(4)}\right)$.

Determine the endomorphism ring (2).

The idea is to find a correspondance on the curve that induce a morphism on the jacobian with minimal polynomial $X^3 + X^2 - 4X + 1$ (a defining polynomial of $\mathbb{Q}\left(\zeta_{13}^{(4)}\right)$) :

- In genus g, it's natural to expect a (n, g)–correspondance.
- We switch back to floating point computations in the jacobian over $\mathbb{C}$.
- We compute a matrix, preserving the lattice, with the good minimal polynomial.
- For $(x, y) \in \mathbb{Z}^* \times \mathbb{C}$, s.t. (x, y) is a point on the curve, we compute the image of $(x, y) - \infty$ with this matrix.
- So, we find 3 x–coordinates, whose symmetric functions must be in the field of definition of the correspondance.
- With sufficient data, we interpolate and find an equation C.

Determine the endomorphism ring (2).

The idea is to find a correspondance on the curve that induce a morphism on the jacobian with minimal polynomial $X^3 + X^2 - 4X + 1$ (a defining polynomial of $\mathbb{Q}\left(\zeta_{13}^{(4)}\right)$) :

- In genus g, it's natural to expect a (n, g)–correspondance.
- We switch back to floating point computations in the jacobian over $\mathbb{C}$.
- We compute a matrix, preserving the lattice, with the good minimal polynomial.
- For $(x, y) \in \mathbb{Z}^* \times \mathbb{C}$, s.t. (x, y) is a point on the curve, we compute the image of $(x, y) - \infty$ with this matrix.
- So, we find 3 x–coordinates, whose symmetric functions must be in the field of definition of the correspondance.
- With sufficient data, we interpolate and find an equation C.

Determine the endomorphism ring (2).

The idea is to find a correspondance on the curve that induce a morphism on the jacobian with minimal polynomial $X^3 + X^2 - 4X + 1$ (a defining polynomial of $\mathbb{Q}\left(\zeta_{13}^{(4)}\right)$) :

- In genus g, it's natural to expect a (n, g)–correspondance.
- We switch back to floating point computations in the jacobian over $\mathbb{C}$.
- We compute a matrix, preserving the lattice, with the good minimal polynomial.
- For $(x, y) \in \mathbb{Z}^* \times \mathbb{C}$, s.t. (x, y) is a point on the curve, we compute the image of $(x, y) - \infty$ with this matrix.
- So, we find 3 x–coordinates, whose symmetric functions must be in the field of definition of the correspondance.
- With sufficient data, we interpolate and find an equation C.

Determine the endomorphism ring (2).

The idea is to find a correspondance on the curve that induce a morphism on the jacobian with minimal polynomial $X^3 + X^2 - 4X + 1$ (a defining polynomial of $\mathbb{Q}\left(\zeta_{13}^{(4)}\right)$) :

- In genus g, it's natural to expect a (n, g)–correspondance.
- We switch back to floating point computations in the jacobian over $\mathbb{C}$.
- We compute a matrix, preserving the lattice, with the good minimal polynomial.
- For $(x, y) \in \mathbb{Z}^* \times \mathbb{C}$, s.t. (x, y) is a point on the curve, we compute the image of $(x, y) - \infty$ with this matrix.
- So, we find 3 x–coordinates, whose symmetric functions must be in the field of definition of the correspondance.
- With sufficient data, we interpolate and find an equation C.

Determine the endomorphism ring (3).

- We actually find a $(8, 3)$–correspondance defined over the Hilbert class field.
- It remains to find an equation for the y–coordinates :

$$yy' \equiv V(x, x')^2 \quad [C].$$

- We do that by *Gröbner basis algorithms* in the field $H(x)$ (so V could be find as a degree 2 polynomial on $H(x)$).
- The correspondance (C, V) induce an endomorphism on the jacobian. We compute its **action on regular differentials**:

$$\mathrm{Tr}\left(\frac{\mathrm{d}x}{y}\right) = \frac{\mathrm{d}x_1}{y_1} + \frac{\mathrm{d}x_2}{y_2} + \frac{\mathrm{d}x_3}{y_3}, \ldots$$

which must be of the shape

$$\left(\alpha + \beta x + \gamma x^2\right)\frac{\mathrm{d}x}{y}, \ldots$$

Determine the endomorphism ring (3).

- We actually find a $(8, 3)$–correspondance defined over the Hilbert class field.
- It remains to find an equation for the y–coordinates :

$$yy' \equiv V(x, x')^2 \quad [C].$$

- We do that by *Gröbner basis algorithms* in the field $H(x)$ (so V could be find as a degree 2 polynomial on $H(x)$).
- The correspondance (C, V) induce an endomorphism on the jacobian. We compute its **action on regular differentials**:

$$\mathrm{Tr}\left(\frac{\mathrm{d}x}{y}\right) = \frac{\mathrm{d}x_1}{y_1} + \frac{\mathrm{d}x_2}{y_2} + \frac{\mathrm{d}x_3}{y_3}, \ldots$$

which must be of the shape

$$\left(\alpha + \beta x + \gamma x^2\right)\frac{\mathrm{d}x}{y}, \ldots$$

The equations ! (1).

Let a generating the Hilbert class field mentioned above :

$$a^9 - a^8 - 2a^7 - a^6 + 5a^5 + a^4 - 5a^3 + 2a^2 + 2a - 1 = 0.$$

$$C = \Big((-10a^8 + 10a^7 + 24a^6 + 16a^5 - 54a^4 - 26a^3 + 40a^2 - 10a - 26)x^7 + (-2a^8 + 4a^7 - 6a^6 + 4a^5 - 2a^4 + 20a^3 - 18a^2 - 16a + 30)x^5 + (8a^8 - 10a^7 + 6a^6 - 24a^5 + 10a^4 - 38a^3 + 52a^2 + 50a - 36)x^3 + (14a^8 - 12a^7 - 36a^6 - 20a^5 + 82a^4 + 52a^3 - 76a^2 - 20a + 18)x\Big)z^3 + \Big(2x^8 + (-6a^7 + 10a^6 + 2a^5 + 4a^4 - 30a^3 + 26a^2 + 16a - 30)x^6 + (19a^8 - 16a^7 - 44a^6 - 26a^5 + 99a^4 + 53a^3 - 100a^2 + 30)x^4 + (-28a^8 + 15a^7 + 70a^6 + 63a^5 - 129a^4 - 120a^3 + 97a^2 + 36a - 27)x^2 - 21a^8 + 8a^7 + 57a^6 + 54a^5 - 95a^4 - 111a^3 + 67a^2 + 47a - 22\Big)z^2 + \Big((-2a^7 - 4a^6 + 6a^5 + 14a^4 + 4a^3 - 24a^2 - 8a + 16)x^7 + (2a^8 + 11a^7 + 17a^6 - 47a^5 - 79a^4 - 12a^3 + 146a^2 + 65a - 63)x^5 + (31a^8 - 18a^7 - 144a^6 - 18a^5 + 271a^4 + 283a^3 - 388a^2 - 204a + 142)x^3 + (-43a^8 + 41a^7 + 56a^6 + 91a^5 - 164a^4 - 23a^3 + 27a^2 - 76a + 37)x\Big)z + \Big((23a^8 - 20a^7 - 46a^6 - 42a^5 + 113a^4 + 53a^3 - 72a^2 - 6a + 14)x^6 + (-94a^8 + 25a^7 + 217a^6 + 291a^5 - 309a^4 - 430a^3 + 88a^2 + 97a - 19)x^4 + (-5a^8 + 145a^7 - 42a^6 - 293a^5 - 442a^4 + 461a^3 + 575a^2 - 118a - 89)x^2 + 61a^8 - 11a^7 - 191a^6 - 167a^5 + 278a^4 + 411a^3 - 236a^2 - 195a + 93\Big)$$

The equations ! (2).

$$V = \Big(\big(x-a+1\big)\big(x+a-1\big)\big(x-2a^8+2a^7+3a^6+3a^5-9a^4-a^3+6a^2-3a\big)\big(x+2a^8-2a^7-3a^6-3a^5+9a^4+a^3-6a^2+3a\big)\big(x^{10}z^2+1/2(-a^8-3a^7+4a^6+8a^5+6a^4-14a^3-6a^2+a-1)x^9z+1/2(31a^8-18a^7-68a^6-64a^5+128a^4+86a^3-104a^2+9a+50)x^8z^2+1/2(-a^8-2a^7+8a^6-3a^4-16a^3+25a^2-2a-15)x^8+1/2(28a^8-34a^7-6a^6-61a^5+75a^4-78a^3+63a^2+134a-66)x^7z+1/2(-76a^8+46a^7+167a^6+159a^5-320a^4-225a^3+240a^2-4a-94)x^6z^2+1/4(63a^8-64a^7-57a^6-121a^5+189a^4-61a^3-17a^2+274a-83)x^6+1/4(51a^8-44a^7-224a^6+8a^5+452a^4+400a^3-694a^2-221a+190)x^5z+1/4(149a^8-48a^7-285a^6-465a^5+403a^4+489a^3-5a^2+46a+13)x^4z^2+1/4(315a^8-252a^7-1020a^6-354a^5+2188a^4+1714a^3-2452a^2-1031a+734)x^4+1/4(-137a^8+134a^7+219a^6+255a^5-615a^4-163a^3+277a^2-134a+41)x^3z+1/4(-85a^8-79a^7+198a^6+506a^5+88a^4-644a^3-462a^2+83a+89)x^2z^2+1/4(-1080a^8+467a^7+2625a^6+2825a^5-4453a^4-4843a^3+2561a^2+1445a-612)x^2+1/4(264a^8+173a^7-643a^6-1385a^5+39a^4+1909a^3+961a^2-341a-212)xz+1/4(119a^8-147a^7-325a^6-55a^5+911a^4+375a^3-961a^2-262a+258)z^2+1/4(-356a^8+500a^7+977a^6+15a^5-2953a^4-983a^3+3227a^2+795a-849)\Big)\Big)/\Big(x\big(x-a^8+a^7+2a^6+2a^5-5a^4-2a^3+2a^2-a\big)\big(x+a^8-a^7-2a^6-2a^5+5a^4+2a^3-2a^2+a\big)\big(x^2+a^8-2a^7-a^6-a^5+6a^4-2a^3-a^2+4a-2\big)^3\Big)$$

The equations ! (3).

The action of the correspondance on the basis of holomorphic differentials

$$\left\{\frac{\mathrm{d}x}{y}, x\frac{\mathrm{d}x}{y}, x^2\frac{\mathrm{d}x}{y}\right\}$$

is given by the matrix

$$\begin{pmatrix} 2a^8-3a^6-5a^5+4a^4+3a^3-5a^2+2 & 0 & -9a^8+2a^7+16a^6+21a^5-25a^4-19a^3+26a^2-12 \\ 0 & \gamma & 0 \\ 3a^8-5a^7-2a^6-2a^5+16a^4-9a^3-7a^2+9a-2 & 0 & -3a^8+a^7+6a^6+7a^5-10a^4-8a^3+9a^2+a-5 \end{pmatrix}$$

were $\gamma = a^8-a^7-3a^6-2a^5+6a^4+5a^3-4a^2-a+2 \in \mathbb{Q}\left(\zeta_{13}^{(4)}\right)$.

Its minimal polynomial is

$$X^3 + X^2 - 4X + 1.$$

Conclusion.

This situation is quite beautiful but there's **no obvious reason** that there's always an **hyperelliptic curve** such that its jacobian has the desired complex multiplication and CM type !

More generally, we can ask

Problem

Can we compute all the equations of an abelian variety with a determined CM field and CM type ? (the time doesn't matter at all !)