p-adic methods in cryptography

Christophe Ritzenthaler

UAB / DTU

Motivation

Discrete logarithm in Jacobians : $\rightsquigarrow$ get a curve over $k = \mathbb{F}_q$ such that $|\mathrm{Jac}(C)(k)|$ contains a big prime factor.
Two strategies :

1. Take random curves and compute quickly $|\mathrm{Jac}(C)(k)|$ $\rightsquigarrow$ l-adics methods, canonical lift, cohomological methods or deformation. If $g \geq 2$: in small characteristics only (classically $q = 2^N$ with N big).
2. We construct a curve over a number field such that the endomorphism ring of its Jacobian is known and with Complex Multiplication (CM). Then one reduces this curve modulo random prime ideals to get good Jacobians : on $\mathbb{F}_p$ with p big.

What is the AGM over $\mathbb{C}$?

Introduced originally over $\mathbb{C}$ to solve elliptic integrals. It is a convergent sequence

$$(a_{n+1}, b_{n+1}) = (\frac{a_n + b_n}{2}, \sqrt{a_n b_n}).$$

$\rightsquigarrow$ fast computation of periods of elliptic curves.

In genus 2, there is a generalization called Borchard's means. It is a special case of the duplication formulae for theta constants.

Remark : **Dupont** are using them to compute periods on genus 2 curves or reciprocally Theta constants.

What is the AGM over the 2-adics (Mestre) ?

1. Input : an ordinary curve $\tilde{C}$ of genus g over $\mathbb{F}_{2^N}$.

What is the AGM over the 2-adics (Mestre) ?

1. Input : an ordinary curve $\tilde{C}$ of genus g over $\mathbb{F}_{2^N}$.
2. Construct a nice lift C over $\mathbb{Q}_{2^N}$.

What is the AGM over the 2-adics (Mestre) ?

1. Input : an ordinary curve $\tilde{C}$ of genus g over $\mathbb{F}_{2^N}$.
2. Construct a nice lift C over $\mathbb{Q}_{2^N}$.
3. Computation of 2-adic numbers $(\vartheta_i^{(0)})_{i=1,\dots 2^g}$ containing enough information on $\mathrm{Jac}(C)$.

What is the AGM over the 2-adics (Mestre) ?

1. Input : an ordinary curve $\tilde{C}$ of genus g over $\mathbb{F}_{2^N}$.
2. Construct a nice lift C over $\mathbb{Q}_{2^N}$.
3. Computation of 2-adic numbers $(\vartheta_i^{(0)})_{i=1,\dots 2^g}$ containing enough information on $\mathrm{Jac}(C)$.
4. Construct a sequence $(\vartheta_i^{(n)}) \in (\mathbb{Q}_{2^N})^{2^g}$ which 'converges' to the canonical lift of $\tilde{C}$.

What is the AGM over the 2-adics (Mestre) ?

1. Input : an ordinary curve $\tilde{C}$ of genus g over $\mathbb{F}_{2^N}$.
2. Construct a nice lift C over $\mathbb{Q}_{2^N}$.
3. Computation of 2-adic numbers $(\vartheta_i^{(0)})_{i=1,\ldots 2^g}$ containing enough information on $\mathrm{Jac}(C)$.
4. Construct a sequence $(\vartheta_i^{(n)}) \in (\mathbb{Q}_{2^N})^{2^g}$ which 'converges' to the canonical lift of $\tilde{C}$.

Why convergence ? 'by hand' for $g = 1$, result of **Carls** in general.

Two different endings

In the point counting (case N big) :

1. For free in the sequence, information on the Frobenius :

   $\mathrm{Norm}_{\mathbb{Q}_q/\mathbb{Q}_2}\left(\vartheta_i^{(n)}/\vartheta_i^{(n+1)}\right)$ converges to $\alpha = \pm\pi_1 \ldots \pi_g$.

Two different endings

In the point counting (case N big) :

1. For free in the sequence, information on the Frobenius :
   $\mathrm{Norm}_{\mathbb{Q}_q/\mathbb{Q}_2}\left(\vartheta_i^{(n)}/\vartheta_i^{(n+1)}\right)$ converges to $\alpha = \pm\pi_1 \dots \pi_g$.
2. Computation of the minimal polynomial P_{sym} of $\alpha + 2^{gN}/\alpha$.

Two different endings

In the point counting (case N big) :

1. For free in the sequence, information on the Frobenius : $\mathrm{Norm}_{\mathbb{Q}_q/\mathbb{Q}_2}\left(\vartheta_i^{(n)}/\vartheta_i^{(n+1)}\right)$ converges to $\alpha = \pm\pi_1 \ldots \pi_g$.
2. Computation of the minimal polynomial P_{sym} of $\alpha + 2^{gN}/\alpha$.
3. Output : the characteristic polynomial of the Frobenius χ_C.

Two different endings

In the point counting (case N big) :

1. For free in the sequence, information on the Frobenius : $\mathsf{Norm}_{\mathbb{Q}_q/\mathbb{Q}_2}\left(\vartheta_i^{(n)}/\vartheta_i^{(n+1)}\right)$ converges to $\alpha = \pm\pi_1 \dots \pi_g$.
2. Computation of the minimal polynomial P_{sym} of $\alpha + 2^{gN}/\alpha$.
3. Output : the characteristic polynomial of the Frobenius χ_C.

In the CM case ($N \leq 10$) :

1. Reconstruction of the curve.

Two different endings

In the point counting (case N big) :

1. For free in the sequence, information on the Frobenius : $\mathrm{Norm}_{\mathbb{Q}_q/\mathbb{Q}_2}\left(\vartheta_i^{(n)}/\vartheta_i^{(n+1)}\right)$ converges to $\alpha = \pm\pi_1 \dots \pi_g$.
2. Computation of the minimal polynomial P_{sym} of $\alpha + 2^{gN}/\alpha$.
3. Output : the characteristic polynomial of the Frobenius χ_C.

In the CM case ($N \leq 10$) :

1. Reconstruction of the curve.
2. Computation of the invariants in $\mathbb{Q}_q$.

Two different endings

In the point counting (case N big) :

1. For free in the sequence, information on the Frobenius : $\mathsf{Norm}_{\mathbb{Q}_q/\mathbb{Q}_2}\left(\vartheta_i^{(n)}/\vartheta_i^{(n+1)}\right)$ converges to $\alpha = \pm\pi_1 \dots \pi_g$.
2. Computation of the minimal polynomial P_{sym} of $\alpha + 2^{gN}/\alpha$.
3. Output : the characteristic polynomial of the Frobenius χ_C.

In the CM case ($N \leq 10$) :

1. Reconstruction of the curve.
2. Computation of the invariants in $\mathbb{Q}_q$.
3. Computation of the minimal polynomials of the invariants.

General features of the AGM methods

- It is based on the canonical lift.

General features of the AGM methods

- It is based on the canonical lift.
  $\rightsquigarrow$ restricted to ordinary abelian varieties.

General features of the AGM methods

- It is based on the canonical lift.
  $\rightsquigarrow$ restricted to ordinary abelian varieties.
  $\rightsquigarrow$ computations in the p-adics require good models to avoid ramified extensions.

General features of the AGM methods

- It is based on the canonical lift.
  $\rightsquigarrow$ restricted to ordinary abelian varieties.
  $\rightsquigarrow$ computations in the p-adics require good models to avoid ramified extensions.
- Use of LLL because

General features of the AGM methods

- It is based on the canonical lift.
  $\rightsquigarrow$ restricted to ordinary abelian varieties.
  $\rightsquigarrow$ computations in the p-adics require good models to avoid ramified extensions.
- Use of LLL because
  one obtains less than the characteristic polynomial ($g \geq 3$).

General features of the AGM methods

- It is based on the canonical lift.
  $\rightsquigarrow$ restricted to ordinary abelian varieties.
  $\rightsquigarrow$ computations in the p-adics require good models to avoid ramified extensions.
- Use of LLL because
  one obtains less than the characteristic polynomial ($g \geq 3$).
  reconstruction of class polynomials from one curve only.

General features of the AGM methods

- It is based on the canonical lift.
  $\rightsquigarrow$ restricted to ordinary abelian varieties.
  $\rightsquigarrow$ computations in the p-adics require good models to avoid ramified extensions.
- Use of LLL because
  one obtains less than the characteristic polynomial ($g \geq 3$).
  reconstruction of class polynomials from one curve only.
- It is based on formulae coming from the complex theory.

General features of the AGM methods

- It is based on the canonical lift.
  $\rightsquigarrow$ restricted to ordinary abelian varieties.
  $\rightsquigarrow$ computations in the p-adics require good models to avoid ramified extensions.
- Use of LLL because
  one obtains less than the characteristic polynomial ($g \geq 3$).
  reconstruction of class polynomials from one curve only.
- It is based on formulae coming from the complex theory.
  $\rightsquigarrow$ general (for every dimension) and elegant.

General features of the AGM methods

- It is based on the canonical lift.
  $\rightsquigarrow$ restricted to ordinary abelian varieties.
  $\rightsquigarrow$ computations in the p-adics require good models to avoid ramified extensions.
- Use of LLL because
  one obtains less than the characteristic polynomial ($g \geq 3$).
  reconstruction of class polynomials from one curve only.
- It is based on formulae coming from the complex theory.
  $\rightsquigarrow$ general (for every dimension) and elegant.
  $\rightsquigarrow$ passing from analogy to a true p-adic theory is hard.

General features of the AGM methods

- It is based on the canonical lift.
  $\leadsto$ restricted to ordinary abelian varieties.
  $\leadsto$ computations in the p-adics require good models to avoid ramified extensions.
- Use of LLL because
  one obtains less than the characteristic polynomial ($g \geq 3$).
  reconstruction of class polynomials from one curve only.
- It is based on formulae coming from the complex theory.
  $\leadsto$ general (for every dimension) and elegant.
  $\leadsto$ passing from analogy to a true p-adic theory is hard.
  $\leadsto$ to link the algebra of the curve with the analytic part (analogs of Thomae's formula) : limited so far to $g = 1, 2, 3$ or hyperelliptic curves.

Complex Multiplication (case of $g = 2$)

Definition : Let $K/\mathbb{Q}$ be an extension of degree 4, with ring of integers $\mathcal{O}_K$. K is a CM field if it is an imaginary quadratic extension of a real quadratic field K_0.

K may be given by $K = \mathbb{Q}(i\sqrt{a + b\sqrt{d}})$ with d and (a, b) square free.

Definition : a type is a couple of two non-conjugate embeddings $\phi_i : K \hookrightarrow \mathbb{C}$.

Restrictions

CM construction : if $I \subset \mathcal{O}_K$ is an ideal, one considers

$$\Phi(I) := \{(\phi_1(\alpha), \phi_2(\alpha)) \subset \mathbb{C}^2, \alpha \in I\}.$$

It is a lattice and $\mathbb{C}^2/\Phi(I)$ is an abelian variety A such that $K \subset \mathrm{End}^0(A)$. We will assume for simplicity :

1. K cyclic or non-Galois $\Rightarrow$ A is absolutely simple.
2. $h_{K_0} = 1$ (i.e K_0 is principal) : A is principally polarized.
3. $K \neq \mathbb{Q}(\zeta_5) \Rightarrow \mu_K = \{\pm 1\}$ (to limit the number of polarizations).
4. $\mathrm{End}(A) = \mathcal{O}_K$ (A is said principal).

Analytic constructions of class polynomials

Van Wamelen and **Weng** for genus 2 curves.

- Construct S the set of isomorphism classes of principal abelian surfaces with CM field K.
  With our assumptions, if K cyclic (resp. non-Galois) then $|S| = h_K$ (resp. $2h_K$).
- Represent each isomorphism class by $\Omega_i \in \mathbb{H}_2$ such that $A_i(\mathbb{C}) \simeq \mathbb{C}^2/(\mathbb{Z}^2 + \Omega_i\mathbb{Z}^2)$.
- For each Ω_i compute the associated theta constants and then the absolute invariants i_1, i_2, i_3.
- Compute $H_n(X) = \prod_S (X - i_n) \in \mathbb{Q}[X]$, $n = 1, 2, 3$.
- Reconstruct the curve with the invariants **(Mestre)**.

Analytic method (end)

- Look for unramified primes p in K ($\Rightarrow$ ordinary reduction) for which the equation $N_{K/K_0}(\pi) = p$ has solutions.

  Remark : The equation has $0, 2$ (K cyclic) or $0, 2, 4$ (K non-Galois) solutions up to conjugacy.

- Proposition : $|\mathrm{Jac}(C)(\mathbb{F}_p)|$ is equal to $f_\pi(1)$ where f_π is the minimal polynomial of one of the solutions.

Canonical lift, AGM and CM

Join work with **Gaudry, Houtmann, Kohel, Weng**.

Let $C/\mathbb{F}_{2^r}$ be an ordinary genus 2 curve whose Jacobian J is absolutely simple. Let $K = \mathrm{End}^0_{\mathbb{F}_{2^r}}(J) = \mathbb{Q}(\pi)$.

Theorem : there exists a p.p. abelian surface (called canonical lift), $J^{\uparrow}/\mathbb{Q}_{2^r}$ which lifts J and such that

$$\mathrm{End}_{\mathbb{Q}_{2^r}}(J^{\uparrow}) = \mathrm{End}_{\mathbb{F}_{2^r}}(J).$$

It can be obtained explicitly by the AGM as a sequence in $\mathbb{Q}_q$ which converges to the invariants associated to $J^{\uparrow}$.

Proposition : $J^{\uparrow} = \mathrm{Jac}(C^{\uparrow})$. The curve $C^{\uparrow}$ is a CM-curve with CM field K. Moreover $J^{\uparrow}$ is principal $\iff$ $\mathrm{End}_{\mathbb{F}_{2^r}}(J) = \mathcal{O}_K$.

Ordinary genus 2 curves

The AGM can be applied to every ordinary hyperelliptic curve for point counting and with restrictions 1-4 for CM constructions.

For genus 2,

$$C/\mathbb{F}_{2^r} : y^2 + v(x)y = u(x)v(x).$$

The polynomial v is square free of degree 3 and u has degree less or equal to 3.

Remark : the Jacobian J of C has four 2-torsion points defined over the extensions generated by the 3 points $(\alpha_i, 0)$ where $v(\alpha_i) = 0$. We denote $k = \mathbb{F}_q$, $q = 2^N$, this extension.

Initialization

One lifts C over $\mathbb{Q}_q$: lift arbitrarily u, v to $U, V \in \mathbb{Q}_q[x]$ and define

$$\mathcal{C}/\mathbb{Q}_q : Y^2 = (2y + V(x))^2 = V(x)(V(x) + 4U(x)).$$

One can factorize the right member

$$\mathcal{C}/\mathbb{Q}_q : Y^2 = \prod_{i=1}^{3}(x - x_i)\prod_{i=1}^{3}(x - (x_i + 4s_i)).$$

Initialization :

$$\begin{aligned} e_1 &= x_1, & e_3 &= x_2, & e_5 &= x_3, \\ e_2 &= x_1 + 4s_1, & e_4 &= x_2 + 4s_2, & e_6 &= x_3 + 4s_3 \end{aligned}$$

Initialization (more)

Thomae's formula give 4 initial invariants :

$$\begin{aligned}
A &= (e_1 - e_3)(e_3 - e_5)(e_5 - e_1)(e_2 - e_4)(e_4 - e_6)(e_6 - e_2) \\
B &= (e_1 - e_3)(e_3 - e_6)(e_6 - e_1)(e_2 - e_4)(e_4 - e_5)(e_5 - e_2) \\
C &= (e_1 - e_4)(e_4 - e_5)(e_5 - e_1)(e_2 - e_3)(e_3 - e_6)(e_6 - e_2) \\
D &= (e_1 - e_4)(e_4 - e_6)(e_6 - e_1)(e_2 - e_3)(e_3 - e_5)(e_5 - e_2)
\end{aligned}$$

Remark : these numbers are 2-adics analogs of

$$\vartheta\left[\begin{smallmatrix}00\\00\end{smallmatrix}\right](0)^4,\ \vartheta\left[\begin{smallmatrix}00\\10\end{smallmatrix}\right](0)^4,\ \vartheta\left[\begin{smallmatrix}00\\01\end{smallmatrix}\right](0)^4,\ \vartheta\left[\begin{smallmatrix}00\\11\end{smallmatrix}\right](0)^4.$$

Then $(A_0, B_0, C_0, D_0) := (1, \sqrt{B/A}, \sqrt{C/A}, \sqrt{D/A})$.

The square root of an element of the form $1 + 8\mathbb{Z}_q$ is the unique element of $\mathbb{Z}_q$ of the form $1 + 4\mathbb{Z}_q$.

Convergence

One uses Borchard's means to get a sequence in $\mathbb{Z}_q$:

$$(A_n, B_n, C_n, D_n) \mapsto (A_{n+1}, B_{n+1}, C_{n+1}, D_{n+1}).$$

These formulae are :

$$A_{n+1} = \frac{A_n + B_n + C_n + D_n}{4} \qquad C_{n+1} = \frac{\sqrt{A_n C_n} + \sqrt{B_n D_n}}{2}$$
$$B_{n+1} = \frac{\sqrt{A_n B_n} + \sqrt{C_n D_n}}{2} \qquad D_{n+1} = \frac{\sqrt{A_n D_n} + \sqrt{B_n C_n}}{2}$$

This sequence converges to the Galois cycle of invariants associated to the canonical lift.

Remark : One may also use Richelot algorithm.

End for point counting

Compute the norm of A_n/A_{n+1} for a sufficiently large $n \rightsquigarrow$ approximation of $\alpha = \pm\pi_1\pi_2$.

Mestre showed that knowing α is sufficient to recover the Frobenius polynomial 'up to a sign' (no LLL needed, no longer true for $g > 2$).

Records : Use of fast norm and Newton lift **(Lercier, Lubicz)**

g	N	Lift	Norm	Total
1	100002	1d 18	1d 16	3d 10
2	32770	7d22	6h	8d4
3	4098	6d8	25mn	6d8

For cryptography ($g = 1, N = 168$) $6.04s$ with **FGH** and $0.08s$ with **Harley**.

Complexity : $O(n^2)$ in time and space.

Back to CM : Reconstruction of the curve

Rosenhain model

$$\mathcal{C} : y^2 = x(x-1)(x-\lambda_1)(x-\lambda_2)(x-\lambda_3)$$

where the λ_i are given by the following expressions :

$$\lambda_1 = -\frac{\vartheta_1^2\vartheta_3^2}{\vartheta_6^2\vartheta_4^2}, \quad \lambda_2 = -\frac{\vartheta_2^2\vartheta_3^2}{\vartheta_6^2\vartheta_5^2}, \quad \lambda_3 = -\frac{\vartheta_2^2\vartheta_1^2}{\vartheta_4^2\vartheta_5^2}$$

ϑ_i are given by ...

Reconstruction (more)

$$\vartheta_1 = \vartheta\left[\begin{smallmatrix}00\\10\end{smallmatrix}\right](0), \quad \vartheta_2 = \vartheta\left[\begin{smallmatrix}00\\11\end{smallmatrix}\right](0), \quad \vartheta_3 = \vartheta\left[\begin{smallmatrix}01\\10\end{smallmatrix}\right](0),$$

$$\vartheta_4 = \vartheta\left[\begin{smallmatrix}10\\00\end{smallmatrix}\right](0), \quad \vartheta_5 = \vartheta\left[\begin{smallmatrix}10\\01\end{smallmatrix}\right](0), \quad \vartheta_6 = \vartheta\left[\begin{smallmatrix}11\\00\end{smallmatrix}\right](0).$$

The (general) duplication formula give these elements from the sequence :

$$\vartheta_1^2 = B_n, \qquad \vartheta_2^2 = D_n,$$

$$\vartheta_3^2 = \frac{\sqrt{A_{n-1}B_{n-1}} - \sqrt{C_{n-1}D_{n-1}}}{2}, \quad \vartheta_4^2 = \frac{A_{n-1} - B_{n-1} + C_{n-1} - D_{n-1}}{4},$$

$$\vartheta_5^2 = \frac{\sqrt{A_{n-1}C_{n-1}} - \sqrt{B_{n-1}D_{n-1}}}{2}, \quad \vartheta_6^2 = \frac{A_{n-1} - B_{n-1} - C_{n-1} + D_{n-1}}{2}.$$

$\rightsquigarrow$ An approximation with precision N of the canonical lift (or of one of its conjugates) after N iterations.

Reconstruction of the invariants

Knowing $\lambda_i \rightsquigarrow I_2, I_4, I_6, I_{10}$ (Igusa invariants) $\rightsquigarrow$ absolute invariants $i_1 = I_2^5/I_{10},\ i_2 = I_2^3 I_4/I_{10},\ i_3 = I_2^2 I_6/I_{10}$.

Knowing these invariants with enough precision one uses LLL : linear relations between $\{1, i_n, i_n^2, \ldots, i_n^{2h_K}\}$ and one gets

$$H_1(i_1) = H_2(i_2) = H_3(i_3) = 0.$$

Moreover one constructs relations

$$L_1(i_1, i_2, i_3) = L_2(i_1, i_2, i_3) = 0.$$

- Relations L_1, L_2 allow to avoid combinatoric problems between the $(2h_K)^3$ roots.
- The H_i may be only factors of class polynomials (not a issue for applications).

The choice of the curve

Let $C/\mathbb{F}_{2^r}$ be an ordinary genus 2 curve.

1. Is χ_π irreducible ?
2. Is $K = \mathbb{Q}(\pi)/\mathbb{Q}$ non-Galois or cyclic ?
3. Is h_K of the right size and $h_{K_0} = 1$? (remark : $r|h_K$.)
4. Is $\mathrm{End}_{\mathbb{F}_{2^k}}(J) = \mathcal{O}_K$?

How to check that ?

We have

$$\mathbb{Z}[\pi] \subset \mathbb{Z}[\pi, \overline{\pi}] \subset \mathrm{End}(J) \subset \mathcal{O}_K.$$

Remark : as $\overline{\pi} = 2^r/\pi$, $[Z[\pi, \overline{\pi}] : Z[\pi]]$ is a power of 2.

Determination of $[O_K : \mathrm{End}(J)]$

let n be an integer, $\alpha : J \to J$ an endomorphism and $\bar{}$ the Rosati involution.

Lemma : Let n be odd (resp. $n = 2^m$). $\alpha(P) = 0$ (resp. $\alpha(P) = 0$ and $\overline{\alpha}(P) = 0$) for all $P \in J[n](\bar{k})$ iff there exists $\beta \in \mathrm{End}(J)$ such that $\alpha = [n]\beta$.

Remark : efficient computations with n-torsion points.

Is the endomorphism ring maximal ?

1. One determines the index of $\mathbb{Z}[\pi, \overline{\pi}]$ in $\mathcal{O}_K$ and (if $\neq 1$) the structure of the extension $\mathcal{O}_K/\mathbb{Z}[\pi, \overline{\pi}]$.
2. Let $f_1(\pi, \overline{\pi})/n_1, \ldots, f_t(\pi, \overline{\pi})/n_t$ be a basis of $\mathcal{O}_K$ over $\mathbb{Z}[\pi, \overline{\pi}]$. For each odd factor l_i (resp. factor 2^{m_i}) of n_i one determines the action of π on $J[l_i](\overline{k})$ (resp. on $J[2^{m_i}](\overline{k})$) and one rejects the curve if the action of $f_i(\pi, \overline{\pi})$ (resp. $f_i(\pi, \overline{\pi})$ or $f_i(\overline{\pi}, \pi)$) on this group is non zero.

An example over $\mathbb{F}_8$

Let $\mathbb{F}_8 = \mathbb{F}_2[\omega]$ with $\omega^3 + \omega + 1 = 0$. Let

$$\begin{aligned} u &= (w^2 + w + 1)x^2 + w^2 x + w^2, \\ v &= x^3 + (w^2 + w + 1)x^2 + x + w + 1. \end{aligned}$$

The Frobenius polynomial is

$$x^4 - 3x^3 + 3x^2 - 24x + 64.$$

It defines an imaginary quadratic extension of $\mathbb{Q}(\sqrt{61})$.
One has $h_K = 3$ (for the other curves over $\mathbb{F}_8$ $h_K = 6$ or 12).

$[\mathcal{O}_K : \mathbb{Z}[\pi]] = 8$ but $\mathbb{Z}[\pi, \overline{\pi}] = \mathcal{O}_K$.

The relations are given by $\ldots$.

Relations

$$2^6 3^{42} i_1^6 - 23449121055031161162885760479530571253 92 i_1^5$$
$$-1126395843903042384561722768451301500394025565862831 56 i_1^4$$
$$-2177415103395854060041246748534717663224784831560700934285483051075 i_1^3$$
$$-1593641994054440870937630653070363836936366222692321471303808012543988702 i_1^2$$
$$-77232882710173372962531506548540432736193603391160944219774880180377797557 2$$
$$+32299720850335379144290409627740329840675572467939277123595091705537581712 5$$
$$43,$$

$$3^{18} i_2^6 + 303458909823080510198053 50 i_2^5$$
$$-2881361916498328939170620773887109083 75 i_2^4$$
$$+75311083251582136774909699089942702936936785265637 5 i_2^3$$
$$-649127309475920539312400482687597914255658885551562830000 i_2^2$$
$$+5120652445919922333588586812287260385399150185276464476808 00000 i_2$$
$$-2427292015515690962866162709711311204495274439003420239222334080 00000,$$

and . . .

$$
\begin{aligned}
&3^{24} i_3^6 + 27437461181384763694011881346 i_3^5 \\
&-352040806049318452655962733807057489240331 i_3^4 \\
&+1178922153334081066484173968480725700444739639422966003 i_3^3 \\
&+5099287909826455148564275585353775058166588909200207226687216 i_3^2 \\
&+228130282826174574878551565831919365949825510821776329730159434 24 i_3 \\
&-19462770713272722403628597313320440103400790281734382852129885861194 5472,
\end{aligned}
$$

$$
\begin{aligned}
&633895738920000 i_1^3 + 8517595035131037 i_1^2 i_2 - 2422318926838275 i_1^2 i_3 \\
&+52888701255649776 0 i_1^2 - 2671415018933342 i_1 i_2^2 + 1010309974499488 2 i_1 i_2 i_3 \\
&+498068270516667479 i_1 i_2 - 31685827189272975 i_1 i_3 + 18498687096353030 60 i_1 \\
&+1100241578433867 4 i_2^3 - 1619524775083390 4 i_2^2 i_3 + 80016484649077407 1 i_2^2 \\
&+2286226402382531 45 i_2 i_3,
\end{aligned}
$$

et.

$$
\begin{aligned}
&5258604005092224 0 i_1^3 + 348046133200631478 i_1^2 i_2 + 197889720810578 10 i_1^2 i_3 \\
&+2623630964591332 9728 i_1^2 - 1611043809046282405 i_1 i_2 i_3 - 3753782789770657910 i_1 i_2 \\
&+151957592539756 4523 i_1 i_3^2 + 2446649956939951033 i_1 i_3 - 1746640058954627936 i_1 \\
&+1153484491100961901 i_2 i_3^2 - 6729087358177501571 i_2 i_3 - 3413986566072687702 i_2 \\
&-158509055831845 9827 i_3^3 - 10377834109186130040 i_3^2 - 12385238120639343570 i_3 ,
\end{aligned}
$$

$$
\begin{aligned}
&14283163413570062 i_1 i_2^2 - 219652172420265 30 i_1 i_2 i_3 - 91100503911673906 i_1 i_2 \\
&+87538195541563 20 i_1 i_3^2 + 741410787750267 0 i_1 i_3 - 85097670432239360 i_1 \\
&+316002807512354 0 i_2^3 - 194154126474081 41 i_2^2 i_3 - 112278555035039 51 i_2^2 \\
&+28513098102060099 i_2 i_3^2 - 101049976189868573 i_2 i_3 - 108901129186080 90 i_3^3 \\
&+428184550411040 40 i_3^2
\end{aligned}
$$

Conclusions

- Record : an example with class number $= 50$ over $\mathbb{F}_{32}$ (precision 65000 bits). The leading coefficient of H_1 is $3^{50} \cdot 11^{156} \cdot 17^{60} \cdot 23^{72} \cdot 41^{24} \cdot 73^{12} \cdot 83^{12} \cdot 181^{48} \cdot 691^{12}$.
- Improvements :
  1. Use more information : one knows the conjugates of the invariants $\rightsquigarrow$ LLL in smaller dimensions.
  2. New strategy : $r \leq 7$: enumerate all the curves $\rightsquigarrow$ quadratic LLL, data base **(Houtmann, Kohel)**.
  3. In the choice of curves : can we detect them quickly ?