Fast computation of hyperelliptic curve isogenies in odd characteristic

Elie Eid

FAST COMPUTATION OF HYPERELLIPTIC CURVE ISOGENIES IN ODD CHARACTERISTIC

ÉLIE EID

Abstract. Let p be an odd prime number and $g \geq 2$ be an integer. We present an algorithm for computing explicit rational representations of isogenies between Jacobians of hyperelliptic curves of genus g over an extension K of the field of p-adic numbers $\mathbb{Q}_p$. It relies on an efficient resolution, with a logarithmic loss of p-adic precision, of a first order system of differential equations.

1. Introduction

After exploring elliptic curves in cryptography and their isogenies, and interest has been raised to their generalizations. Researchers began to inspect principally polarized abelian varieties, especially Jacobians of genus two and three curves and compute isogenies between them [CR15, CE15, Mil19, Tia20]. Their main interest was to calculate the number of points of these varieties over finite fields [GS12, LL06, BGG+17] and more recently to instantiate isogeny-based cryptography schemes [FT19, CS20]. In this work, we concentrate on the problem of computing explicitly isogenies between Jacobians of hyperelliptic curves over finite fields of odd characteristic, this will be a generalization to [CE15] and [Mil19].

A separable isogeny between Jacobians of hyperelliptic curves of genus g defined over a field k is characterized by its so called rational representation (see Section 2.2 for the definition); it is a compact writing of the isogeny and can be expressed by $2g$ rational fractions defined over a finite extension of k. These rational fractions are related. In fields of characteristic different from 2, they can be determined by computing an approximation of the solution $X(t) \in k[\![t]\!]^g$ of a first order non-linear system of differential equations of the form

$$H\left(X(t)\right) \cdot X'(t) = G(t) \tag{1}$$

where $H : k[\![t]\!]^g \to M_g(k[\![t]\!])$ is a well chosen map and $G(t) \in k[\![t]\!]^g$. This approach is a generalization of the elliptic curves case [LV16] for which Equation (1) is solved in dimension one.

Equation (1) was first introduced in [CE15] for genus two curves defined over finite fields of odd characteristic and solved in [KPR20] using a well-designed algorithm based on a Newton iteration; this allowed them to compute $X(t)$ modulo $t^{O(\ell)}$ in the case of an (ℓ, ℓ)-isogeny for a cost of $\tilde{O}(\ell)$ operations in k then recover the rational fractions that defines the rational representation of the isogeny. This approach does not work when the characteristic of k is positive and small compared to ℓ, in which case divisions by p occur and an error can be raised while doing the computations. We take on this issue similarly as in the elliptic curve case ([LS08, CEL20]) by lifting the problem to the p-adics. We will always suppose that the lifted Jacobians are also Jacobians for some hyperelliptic curves. It is relevant to assume this, even though it is not the generic case when g is greater than 3 [OS86], since it allows us to compute efficiently the rational representation of the multiplication by an integer which in this case the lifting can be done arbitrarily. After this process, we need to analyze the loss of p-adic precision in order to solve

Equation (1) without having a numerical instability. We extend the result of [LV16], by proving that the number of lost digits when computing an approximation of the solution of Equation (1) modulo $t^{O(g\ell)}$, stays within $O\left(\log_p(g\ell)\right)$. Our main theorem is the following.

Theorem. *Let p be a prime number. Let K be a finite extension of $\mathbb{Q}_p$ and $\mathcal{O}_K$ be its ring of integers. There exists an algorithm that takes as input:*

- *three positive integers n,g and N,*
- *a map $H\colon \mathcal{O}_K[\![t]\!]^g \to M_g(\mathcal{O}_K[\![t]\!])$ such that $H(0) \in GL_g(\mathcal{O}_K)$,*
- *a vector $G(t) \in \mathcal{O}_K[\![t]\!]^g$,*

and, assuming that the differential equation

$$H(X(t)) \cdot X'(t) = G(t)$$

admits a unique solution in $(t\mathcal{O}_K[\![t]\!])^g$, outputs an approximation of this solution modulo (p^N, t^{n+1}) for a cost $\tilde{O}(g^\omega n)$, where $\omega \in [2,3[$ is the exponent of matrix multiplication, at precision $O(p^M)$ with $M = \max(N,3) + \lfloor \log_p(n) \rfloor$ if $p = 2$, $M = \max(N,2) + \lfloor \log_p(n) \rfloor$ if $p = 3$ and $M = N + \lfloor \log_p(n) \rfloor$ otherwise.

One can do a bit better for $p = 2$ and 3 if we follow the same strategy as [LV16], in this case M is equal to $\max(N,2) + \lfloor \log_p(n) \rfloor$ if $p = 2$ and $N + \lfloor \log_p(n) \rfloor$ otherwise. For the sake of simplicity, we will not prove this here.

Note that this technique does not allow to compute isogenies in characteristic two for several reasons. First, the general equation of a hyperelliptic curve in characteristic two does not have the same form as in odd characteristic. Moreover, the map H includes square roots of polynomials which implies that solving Equation (1) will require to extract square roots at some point. However, it is well known that extracting square roots in an extension of $\mathbb{Q}_2$ is an unstable operation. Still, it is quite interesting to solve Equation (1) for $p = 2$ with the assumptions that we made in the main theorem, even thought this approach does not lead to the computation of isogenies between Jacobians of hyperelliptic curves.

2. Jacobians of curves and their isogenies

Throughout this section, the letter k refers to a fixed field of characteristic different from two. Let $\bar{k}$ be a fixed algebraic closure of k. In Section 2.1, we briefly recall some basic elements about principally polarized abelian varieties and $(\ell,\dots,\ell)$-isogenies between them; the notion of rational representation is discussed in Section 2.2. Finally, for a given rational representation, we construct a system of differential equations that we associate with it.

2.1. $(\ell,\cdots,\ell)$-isogenies between abelian varieties.

Let A be an abelian variety of dimension g over k and $A^\vee$ be its dual. To a fixed line bundle $\mathcal{L}$ on A, we associate the morphism $\lambda_{\mathcal{L}}$ defined as follows

$$\begin{array}{rccc} \lambda_{\mathcal{L}} : & A & \longrightarrow & A^\vee \\ & x & \longmapsto & t_x^*\mathcal{L} \otimes \mathcal{L}^{-1} \end{array}$$

where t_x denotes the translation by x and $t_x^*\mathcal{L}$ is the pullback of $\mathcal{L}$ by t_x.

We recall from [Mil86] that *a polarization* λ of A is an isogeny $\lambda : A \longrightarrow A^\vee$, that is a surjective homomorphism of abelian varieties of finite kernel, such that over $\bar{k}$, λ is of the form $\lambda_{\mathcal{L}}$ for some ample line bundle $\mathcal{L}$ on $A_{\bar{k}} := A \otimes \mathrm{Spec}(\bar{k})$. When the degree of a polarization λ of A is equal to 1, we say that λ is a *principal polarization* and the pair (A,λ) is a *principally polarized abelian*

variety. We assume in the rest of this subsection that we are given a principally polarized abelian variety (A, λ). The *Rosati involution* on the ring $\mathrm{End}(A)$ of endomorphsims of A corresponding to the polarization λ is the map

$$\begin{array}{ccc} \mathrm{End}(A) & \longrightarrow & \mathrm{End}(A) \\ \alpha & \longmapsto & \lambda^{-1} \circ \alpha^{\vee} \circ \lambda. \end{array}$$

The Rosati involution is crucial for the study of the division algebra $\mathrm{End}(A) \otimes \mathbb{Q}$, but for our purpose, we only state the following result.

Proposition 1. [Mil86, Proposition 14.2] *For every $\alpha \in End(A)$ fixed by the Rosati involution, there exists, up to algebraic equivalence, a unique line bundle $\mathcal{L}_A^{\alpha}$ on A such that $\lambda_{\mathcal{L}_A^{\alpha}} = \lambda \circ \alpha$.*

In particular, taking α to be the identity endomorphism denoted "1", there exists a unique line bundle $\mathcal{L}_A^1$ such that $\lambda_{\mathcal{L}_A^1} = \lambda$.
Using Proposition 1, we give the definition of an $(\ell, \dots, \ell)$-isogeny.

Definition 2. *Let (A_1, λ_1) and (A_2, λ_2) be two principally polarized abelian varieties of dimension g over k and $\ell \in \mathbb{N}^*$. An $(\ell, \dots, \ell)$-isogeny I between A_1 and A_2 is an isogeny $I : A_1 \longrightarrow A_2$ such that*

$$I^* \mathcal{L}_{A_2}^1 = \mathcal{L}_{A_1}^{\ell},$$

where $\mathcal{L}_{A_1}^{\ell}$ is the unique line bundle on A_1 associated with the multiplication by ℓ map.

We now suppose that A is the Jacobian of a genus g curve C over k. We will always make the assumption that there is at least one k-rational point on C. Let r be a positive integer and fix $P \in C$. We define $C^{(r)}$ to be the symmetric power of C and $j_P^{(r)}$ to be the map

$$\begin{array}{ccc} C^{(r)} & \xrightarrow{j_P^{(r)}} & A \simeq J(C) \\ (P_1, \dots, P_r) & \longmapsto & [P_1 + \cdots P_r - rP]. \end{array}$$

If $r = 1$ then the map $j_P^{(1)}$ is called the *Jacobi map* with origin P.
We write $j^{(r)}$ for the map $j_P^{(r)}$. The image of $j^{(r)}$ is a closed subvariety of A which can be also written as r summands of $j^{(1)}(C)$. Let Θ be the image of $j^{(g)}$, it is a divisor on A and when P is replaced by another point, Θ is replaced by a translate. We call Θ the theta divisor associated to A.

Remark 3. If A is the Jacobian of a curve C and Θ its theta divisor, then $\mathcal{L}_A^1 = \mathcal{L}(\Theta)$, where $\mathcal{L}(\Theta)$ is the sheaf associated to the divisor Θ.

Using Remark 3, Definition 2 for Jacobian varieties gives the following

Proposition 4. *Let $\ell \in \mathbb{N}^*$, A_1 and A_2 be the Jacobians of two algebraic curves over k and Θ_1 and Θ_2 be the theta divisors associated to A_1 and A_2 respectively. If an isogeny $I : A_1 \longrightarrow A_2$ is an $(\ell, \dots, \ell)$-isogeny then $I^*\Theta_2$ is algebraically equivalent to $\ell\Theta_1$.*

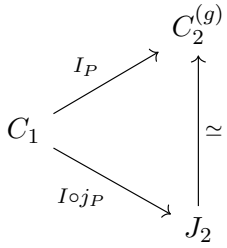
Proof. For all $x \in A_1$, the theorem of squares [Mil86, Theorem 5.5] gives the following relation

$$t_{\ell x}^* \mathcal{L}_{A_1}^1 \otimes \left(\mathcal{L}_{A_1}^1\right)^{-1} = t_x^* \left(\mathcal{L}_{A_1}^1\right)^{\otimes \ell} \otimes \left(\left(\mathcal{L}_{A_1}^1\right)^{\otimes \ell}\right)^{-1}.$$

By Proposition 1, the line bundle $\mathcal{L}_{A_1}^{\ell}$ is algebraically equivalent to $\left(\mathcal{L}_{A_1}^1\right)^{\otimes \ell}$, therefore $I^*\mathcal{L}_{A_2}^1$ and $\left(\mathcal{L}_{A_1}^1\right)^{\otimes \ell}$ are algebraically equivalent. By Remark 3, $I^*\mathcal{L}_{A_2}^1$ corresponds to $I^*\Theta_2$ and $\left(\mathcal{L}_{A_1}^1\right)^{\otimes \ell}$ corresponds to $\ell\Theta_1$. □

2.2. **Rational representation of an isogeny between Jacobians of hyperelliptic curves.** We focus on computing an isogeny between Jacobians of hyperelliptic curves. Let C_1 (resp. C_2) be a genus g hyperelliptic curve over k, J_1 (resp. J_2) be its associated Jacobian and Θ_1 (resp. Θ_2) be its theta divisor. We suppose that there exists a separable isogeny $I : J_1 \longrightarrow J_2$. For $P \in C_1$, let $j_P : C_1 \longrightarrow J_1$ be the Jacobi map with origin P. Generalizing [KPR20, Proposition 4.1] gives the following proposition

Proposition 5. *The morphism $I \circ j_P$ induces a unique morphism $I_P : C_1 \longrightarrow C_2^{(g)}$ such that the following diagram commutes*



We assume that C_1 (resp. C_2) is given by the following singular model

$$v^2 = f_1(u) \quad (\text{resp. } y^2 = f_2(x))$$

where f_1 (resp. f_2) is a polynomial of degree $2g+1$ or $2g+2$. Set $Q = (u, v) \in C_1$ and $I_P(Q) = \{(x_1, y_1), \ldots, (x_g, y_g)\}$. We use the Mumford's coordinates to represent the element $I_P(Q)$: it is given by a pair of polynomials $(U(X), V(X))$ such that

$$U(X) = X^g + \sigma_1 X^{g-1} + \cdots + \sigma_g$$

where

$$\sigma_i = (-1)^i \sum_{1 \leq j_1 < j_2 < \cdots < j_i \leq g} x_{j_1} x_{j_2} \cdots x_{j_i}$$

and

$$V(X) = \rho_1 X^{g-1} + \cdots + \rho_g = \sum_{j=0}^{g-1} y_j \left(\prod_{i=0, i \neq j}^{g-1} \frac{X - x_i}{x_j - x_i} \right).$$

The tuple $(\sigma_1, \cdots, \sigma_g, \rho_1, \cdots, \rho_g)$ consists of rational fractions in u and v and it is called the *rational representation* of I.

Remark 6. Since $I_P(u, -v) = -I_P(u, v)$, the functions $\sigma_1, \ldots, \sigma_g$ can be seen as rational fractions in u and have the same degree bounded by $\deg(\sigma_1)/2$. Moreover, the functions $\rho_1/v, \ldots, \rho_g/v$ can also be expressed as rational fractions in u of degrees bounded by $\deg(\rho_1)+3, \ldots, \deg(\rho_g)+3$ respectively.

In order to determine the isogeny I, it suffices to compute its rational representation (because I is a group homomorphism), so we need to have some bounds on the degree of the rational functions $\sigma_1, \ldots, \sigma_g, \rho_1/v, \ldots, \rho_g/v$. In the case of an $(\ell, \ldots, \ell)$-isogeny, we adapt the proof of [CE15, § 6.1] in order to obtain bounds in terms of ℓ and g.

Lemma 7. *Let $i \in \{1, \ldots, g\}$. The pole divisor of σ_i seen as function on J_2 is algebraically equivalent to $2\Theta_2$. The pole divisor of ρ_i seen as function on J_2 is algebraically equivalent to $(2i+1)\Theta_2$ if $\deg(f_2) = 2g+1$, and $(2i+2)\Theta_2$ otherwise.*

Proof. This is a generalization of [KPR20, Lemma 4.25]. Note that if $\deg(f_2) = 2g+1$, then σ_i has a pole of order one along the divisor $\{(R_1, \dots, R_{g-1}, \infty)\,; R_i \in C_2\}$ which is algebraically equivalent to $2\Theta_2$. □

Lemma 8. [Mat59, Appendix] *The divisor $j_P(C_1)$ of J_1 is algebraically equivalent to $\dfrac{\Theta_1^{g-1}}{(g-1)!}$ where Θ_1^{g-1} denotes the $g-1$ times self intersection of the divisor Θ_1.*

Proposition 9. *Let ℓ be a non-zero positive integer and $i \in \{1, \dots, g\}$. If I is an $(\ell, \dots, \ell)$-isogeny, then the degree of σ_i seen as a function on C_1 is bounded by $2g\ell$. The degree of ρ_i seen as a function on C_1 is bounded by $(2i+1)g\ell$ if $\deg(f_2) = 2g+1$, and $(2i+2)g\ell$ otherwise.*

Proof. The degrees of $\sigma_1, \dots, \sigma_g, \rho_1, \dots, \rho_g$ are obtained by computing the intersection of $j_P(C)$ with their pole divisors. By Lemma 7, it suffices to show that

$$j_P(C) \cdot \Theta_2 = \ell g.$$

Since I is an $(\ell, \dots, \ell)$-isogeny, Proposition 4 gives that $I^*\Theta_2$ is algebraically equivalent to $\ell\Theta_1$. Moreover,

$$I^*\big(I_P(C)\big) = \big(|\ker(I)|\big)\, j_P(C) = l^g j_P(C).$$

Using Lemma 8, we obtain

$$I^*\big(I_P(C)\big) \cdot I^*\Theta_2 = g l^{g+1}.$$

As

$$I^*\big(I_P(C)\big) \cdot I^*\Theta_2 = \deg(I)\,\big(I_P(C) \cdot \Theta_2\big) = l^g (I_P(C) \cdot \Theta_2),$$

the result follows. □

2.3. **Associated differential equation.** We assume that $\mathrm{char}(k) \neq 2$. We generalize [CE15, § 6.2] by constructing a differential system modeling the map $F_P = I \circ j_P$ of Proposition 5. The map F_P is a morphism of varieties, it acts naturally on the spaces of holomorphic differentials $H^0(J_2, \Omega^1_{J_2})$ and $H^0(C_1, \Omega^1_{C_1})$ associated to J_2 and C_1 respectively, this action gives a map

$$F_P^* \,:\, H^0(J_2, \Omega^1_{J_2}) \longrightarrow H^0(C_1, \Omega^1_{C_1}).$$

A basis of $H^0(C_1, \Omega^1_{C_1})$ is given by

$$B_1 = \left\{ u^i \frac{du}{v}\,; i \in \{0, \dots, g-1\} \right\}.$$

The Jacobi map of C_2 induces an isomorphism between the spaces of holomorphic differentials associated to C_2 and J_2, so $H^0(J_2, \Omega^1_{J_2})$ is of dimension g, it can be identified with the space $H^0(C_2^g, \Omega^1_{C_2^g})^{S_n}$ (here the symmetric group S_n acts naturally on the space $H^0(C_2^g, \Omega^1_{C_2^g})$). With this identification, a basis of $H^0(J_2, \Omega^1_{J_2})$ is chosen to be equal to

$$B_2 = \left\{ \sum_{j=1}^{g} x_j^i \frac{dx_j}{y_j}\,;\, i \in \{0, \dots, g-1\} \right\}.$$

Let $(m_{ij})_{0 \leq i,j \leq g} \in \mathrm{GL}_g(\bar{k})$ be the matrix of F_P^* with respect of these two bases, we call it the *normalization matrix*. Let $Q = (u_Q, v_Q) \in C_1$ be a non-Weierstrass point different from P and $I_P(Q) = \{R_1, \dots, R_g\}$ such that $I_P(Q)$ contains g distinct points and does not contain neither a point at infinity nor a Weierstrass point. The points R_i may be defined over an extension k' of

k of degree equal to $O(g)$. Let t be a formal parameter of C_1 at Q, then we have the following diagram

$$\begin{array}{ccc} Spec\big(k'[\![t]\!]\big) & \xrightarrow{t\mapsto (R_i(t))_i} & C_2^g \\ \downarrow & & \downarrow \\ C_1 & \xrightarrow{I_P} & C_2^{(g)} \end{array}$$

This gives the differential system

$$\begin{cases} \dfrac{dx_1}{y_1} + \cdots + \dfrac{dx_g}{y_g} = \big(m_{11} + m_{12}\cdot u + \ldots + m_{1g}\cdot u^{g-1}\big)\dfrac{du}{v}, \\ \dfrac{x_1\cdot dx_1}{y_1} + \cdots + \dfrac{x_g\cdot dx_g}{y_g} = \big(m_{21} + m_{22}\cdot u + \ldots + m_{2g}\cdot u^{g-1}\big)\dfrac{du}{v}, \\ \qquad\vdots \qquad\qquad\qquad\qquad\qquad\qquad \vdots \\ \dfrac{x_1^{g-1}\cdot dx_1}{y_1} + \cdots + \dfrac{x_g^{g-1}\cdot dx_g}{y_g} = \big(m_{g1} + m_{g2}\cdot u + \ldots + m_{gg}\cdot u^{g-1}\big)\dfrac{du}{v}, \\ y_1^2 = f_2(x_1), \quad \cdots \quad , y_g^2 = f_2(x_g)\,. \end{cases} \tag{2}$$

Equation (2) has been initially constructed and solved in [CE15] for $g = 2$. In this case, the normalization matrix and the initial condition $(x_1(0), x_2(0))$ are computed using algebraic theta functions. In a more practical way, we refer to [KPR20] for an easy computation of the initial condition $(x_1(0), x_2(0))$ of Equation (2) and for solving the differential system using a Newton iteration. However, in this case, the normalization matrix is determined by differentiating modular equations. There is a slight difference in Equation (2) between the two cases, especially $x_1(0)$ and $x_2(0)$ are different in the first, and equal in the second. Let H be the g-squared matrix defined by

$$H(x_1, \ldots x_g) = \left(x_j^{i-1}\frac{1}{y_j}\right)_{1\le i,j\le g}.$$

We suppose that $g = 2$. If the initial condition $(x_1(0), x_2(0))$ of Equation (2) satisfies $x_1(0) \neq x_2(0)$, then the matrix $H(x_1(0), x_2(0))$ is invertible in $M_2(k)$. Otherwise, its determinant is equal to zero.

More generally, we prove that with the assumptions that we made on $Q, R_1, R_2, \ldots R_{g-1}$ and R_g, the matrix $H(x_1(0), \ldots, x_g(0))$ is invertible in $M_g(k)$. Let t be a formal parameter, $Q(t)$ the formal point on C_1 $(k[\![t]\!])$ that corresponds to $t = u - u_Q$ and $\{R_1(t), \ldots, R_g(t)\}$ the image of $Q(t)$ by I_P, then Equation (2) becomes

$$H(X(t))\cdot X'(t) = G(t) \tag{3}$$

where $X(t) = (x_1(t), \ldots, x_g(t))$ and $G(t) = v^{-1}\left(\sum_{i=1}^{g} m_{ij}u^{i-1}\right)_{1\le j\le g}$. Thus we have the following proposition

Proposition 10. *The matrix $H(X(t))$ is invertible in $M_g(k[\![t]\!])$.*

Proof. The matrix $H(X(t))$ is sort of a generalization of the Vandermonde matrix, its determinant is given by

$$\det\left(H(X(t))\right) = \frac{\prod_{1\leq i<j\leq g}\left(x_j(t)-x_i(t)\right)}{\prod_{i=1}^{g} y_i(t)}$$

which is invertible in $M_g(k[\![t]\!])$ because $x_i(0) \neq x_j(0)$ for all $i, j \in \{1, \ldots, g\}$ such that $i \neq j$. □

3. Fast resolution of systems of p-adic differential equations

In this section, we give a proof of the main theorem by solving efficiently the nonlinear system of differential equations (1) in an extension of $\mathbb{Q}_p$ for all prime numbers p even though it is not useful for computing isogenies for $p = 2$. In Section 3.1, we introduce the computational model that we use in our algorithm exposed in Section 3.2 and the proof of its correctness is presented in Section 3.3.

Throughout this section the letter p refers to a fixed prime number and K corresponds to a fixed finite extension of $\mathbb{Q}_p$. We denote by υ_p the unique normalized extension to K of the p-adic valuation. We denote by $\mathcal{O}_K$ the ring of integers of K, $\pi \in \mathcal{O}_K$ a fixed uniformizer of K and e the ramification index of the extension $K/\mathbb{Q}_p$. We naturally extend the valuation υ_p to quotients of $\mathcal{O}_K$, the resultant valuation is also denoted by υ_p.

3.1. Computational model.

From an algorithmic point of view, p-adic numbers behave like real numbers: they are defined as infinite sequences of digits that cannot be handled by computers. It is thus necessary to work with truncations. For this reason, several computational models were suggested to tackle these issues (see [Car17] for more details). In this paper, we use the fixed point arithmetic model at precision $O(p^M)$, where $M \in \mathbb{N}^*$, to do computations in K. More precisely, an element in K is represented by an interval of the form $a + O(p^M)$ with $a \in \mathcal{O}_K/\pi^{eM}\mathcal{O}_K$. We define basic arithmetic operations on intervals in an elementary way

$$\begin{aligned}\left(x + O(p^M)\right) \pm \left(y + O(p^M)\right) &= (x \pm y) + O(p^M)\,,\\ \left(x + O(p^M)\right) \times \left(y + O(p^M)\right) &= xy + O(p^M)\,.\end{aligned}$$

For divisions we make the following assumption: for $x, y \in \mathcal{O}_K/\pi^{eM}\mathcal{O}_K$, the division of $x+O(p^M)$ by $y + O(p^M)$ raises an error if $\upsilon_p(y) > \upsilon_p(x)$, returns $0 + O(p^M)$ if $x = 0$ in $\mathcal{O}_K/\pi^{eM}\mathcal{O}_K$ and returns any representative $z + O(p^M)$ with the property $x = yz$ in $\mathcal{O}_K/\pi^{eM}\mathcal{O}_K$ otherwise.

Matrix computation. We extend the notion of intervals to the K-vector space $M_{n,m}(K)$: an element in $M_{n,m}(K)$ of the form $A + O(p^M)$ represents a matrix $\left(a_{ij} + O(p^M)\right)_{ij}$ with $A = (a_{ij}) \in M_{n,m}\left(\mathcal{O}_K/\pi^{eM}\mathcal{O}_K\right)$. Operations in $M_{n,m}(K)$ are defined from those in K:

$$\begin{aligned}\left(A + O(p^M)\right) \pm \left(B + O(p^M)\right) &= (A \pm B) + O(p^M),\\ \left(A + O(p^M)\right) \cdot \left(B + O(p^M)\right) &= (A \cdot B) + O(p^M).\end{aligned}$$

For inversions, we use standard Gaussian elimination.

Lemma 11. [Vac15, Proposition 1.2.4 and Théorème 1.2.6] *Let A be an invertible matrix in $M_n(\mathcal{O}_K)$ with entries known up to precision $O(p^M)$. The Gauss-Jordan algorithm computes the inverse A^{-1} of A with entries known with the same precision as those of A using $O(n^3)$ operations in K.*

3.2. **The algorithm.** Let g be a positive integer, $K[\![t]\!]$ be the ring of formal series over K in t. We denote by $M_g(k)$ the ring of square matrices of size g over a field k. Let $\mathrm{f} = \big(f_{ij}\big)_{i,j} \in M_g(K[\![t]\!])$ and H_f be the map defined by

$$\begin{array}{ccc} \big(tK[\![t]\!]\big)^g & \xrightarrow{\quad H_\mathrm{f} \quad} & M_g(K[\![t]\!]) \\ \big(x_1(t), \ldots, x_g(t)\big) & \longmapsto & \Big(f_{ij}\big(x_i(t)\big)\Big)_{ij}. \end{array}$$

Given $\mathrm{f} \in M_g(K[\![t]\!])$ and $G = (G_1, \ldots, G_g) \in K[\![t]\!]^g$, we consider the following differential equation in $X = (x_1, \ldots, x_g)$,

$$H_\mathrm{f} \circ X \cdot X' = G. \tag{4}$$

We will always look for solutions of (4) in $\big(tK[\![t]\!]\big)^g$ in order to ensure that $H_\mathrm{f} \circ X$ is well defined. We further assume that $H_\mathrm{f}(0)$ is invertible in $M_g(K)$.

Remark 12. Up to a change of variables, the differential system (3) fulfills all the assumptions of Equation (4).

The next proposition guarantees the existence and the uniqueness of a solution of the differential equation (4).

Proposition 13. *Assuming that $H_\mathrm{f}(0)$ is invertible in $M_g(K)$, the system of differential equations (4) admits a unique solution in $K[\![t]\!]^g$.*

Proof. We are looking for a vector $X(t) = \sum_{n=1}^{\infty} X_n t^n$ that satisfies Equation (4). Since $X(0) = 0$ and $H_\mathrm{f}(0)$ is invertible in $K[\![t]\!]^g$, then $H_\mathrm{f}\big(X(t)\big)$ is invertible in $M_g(K[\![t]\!])$. So Equation (4) can be written as

$$X'(t) = \big(H_\mathrm{f}(X(t))\big)^{-1} \cdot G(t). \tag{5}$$

Equation (5) applied to 0, gives the non-zero vector X_1. Taking the n-derivative of Equation (5) with respect to t and applying the result to 0, we observe that the coefficient X_n only appears on the hand left side of the result, so each component of X_n is a polynomial in the components of the X_i's for $i < n$ with coefficients in K. Therefore, the coefficients X_n exist and are all uniquely determined. □

We construct the solution of Equation (4) using a Newton scheme. We recall that for $Y = (y_1, \ldots, y_g) \in K[\![t]\!]^g$, the differential of H_f with respect to Y is the function

$$\begin{array}{rccc} dH_\mathrm{f}(Y) : & K[\![t]\!]^g & \longrightarrow & M_g(K[\![t]\!]) \\ & h & \longmapsto & dH_\mathrm{f}(Y)(h) = \Big(f'_{ij}\left(y_i\right) \cdot h_i\Big)_{1 \le i,j \le g}. \end{array} \tag{6}$$

We fix $m \in \mathbb{N}$ and we consider an approximation X_m of X modulo t^m. We want to find a vector $h \in (t^m\, K[\![t]\!])^g$, such that $X_m + h$ is a better approximation of X. We compute

$$H_\mathrm{f}\left(X_m + h\right) = H_\mathrm{f}\left(X_m\right) + dH_\mathrm{f}(X_m)(h) \pmod{t^{2m}}.$$

Therefore we obtain the following relation

$$\begin{aligned} H_\mathrm{f}\left(X_m + h\right) \cdot \left(X_m + h\right)' - G = \\ H_\mathrm{f}\left(X_m\right) \cdot X'_m + H_\mathrm{f}\left(X_m\right) \cdot h' + dH_\mathrm{f}(X_m)(h) \cdot X'_m - G \pmod{t^{2m-1}}. \end{aligned}$$

So we look for h such that

$$H_\mathrm{f}\left(X_m\right) \cdot h' + dH_\mathrm{f}(X_m)(h) \cdot X'_m = -H_\mathrm{f}\left(X_m\right) \cdot X'_m + G \pmod{t^{2m-1}}. \tag{7}$$

It is easy to see that the left hand side of Equation (7) is equal to $\left(\left(H_{\mathrm{f}}\left(X_m\right)\cdot h\right)'\right.$, therefore integrating each component of Equation (7) and multiplying the result by $\left(H_{\mathrm{f}}\left(X_m\right)\right)^{-1}$ gives the following expression for h

$$h = \left(H_{\mathrm{f}}\left(X_m\right)\right)^{-1} \int \left(G - H_{\mathrm{f}}\left(X_m\right)\cdot X_m'\right)\, dt \pmod{t^{2m}}, \tag{8}$$

where $\int Y dt$, for $Y \in K[\![t]\!]^g$, denotes the unique vector $I \in K[\![t]\!]^g$ such that $I' = Y$ and $I(0) = 0$.
This formula defines a Newton operator for computing an approximation of the solution of Equation (4). Reversing the above calculations leads to the following proposition.

Proposition 14. *We assume that $H_{\mathrm{f}}(0)$ is invertible in $M_g(K)$. Let $m > 0$ be an integer, $n = 2m$ and $X_m \in K[\![t]\!]^g$ a solution of Equation (4) mod t^m. Then,*

$$X_n = X_m + \left(H_{\mathrm{f}}\left(X_m\right)\right)^{-1} \int \left(G - H_{\mathrm{f}}\left(X_m\right)\cdot X_m'\right)\, dt$$

is a solution of Equation (4) mod t^{n+1}.

It is straightforward to turn Proposition 14 into an algorithm that solves the nonlinear system (4). We make a small optimization by integrating the computation of $H_{\mathrm{f}}(X)^{-1}$ in the Newton scheme.

Algorithm 1: Differential Equation Solver

`DiffSolve` (G, f, n, g)
- **Input :** $G, \mathrm{f} \mod t^n$ such that $H_{\mathrm{f}}(0)$ is invertible in $M_g(K)$.
- **Output:** The solution X of Equation (4) $\mod t^{n+1}$, $H_{\mathrm{f}}\left(X\right) \mod t^{\lceil n/2 \rceil}$
- **if** $n = 0$ **then**
  - **return** $0 \mod t$, $H_{\mathrm{f}}(0)^{-1} \mod t$
- $m := \lceil \frac{n-1}{2} \rceil$;
- $X_m, H_m :=$ `DiffSolve`(G, f, m, g);
- $H_n := 2H_m - H_m \cdot H_{\mathrm{f}}(X) \cdot H_m \mod t^{m+1}$
- **return** $X_m + H_n \int (G - H_{\mathrm{f}}\left(X_m\right)\cdot X_m')\, dt \mod t^{n+1}$

According to Proposition 14, Algorithm 1 runs correctly when its entries are given with an infinite p-adic precision; however it could stop working if we use the fixed point arithmetic model. The next theorem guarantees its correctness in this type of models.

Theorem 15. *Let $n, g \in \mathbb{N}$, $N \in \frac{1}{e}\mathbb{Z}^*, G \in \mathcal{O}_K[\![t]\!]^g$ and $\mathrm{f} \in M_g(\mathcal{O}_K[\![t]\!])$. We assume that $H_{\mathrm{f}}(0)$ is invertible in $M_g(\mathcal{O}_K)$ and that the components of the solution of Equation (4) have coefficients in $\mathcal{O}_K$. When the procedure* `DiffSolve` *runs with fixed point arithmetic at precision $O(p^M)$, with $M = \max(N, 3) + \lfloor \log_p(n) \rfloor$ if $p = 2$, $M = \max(N, 2) + \lfloor \log_p(n) \rfloor$ if $p = 3$ and $M = N + \lfloor \log_p(n) \rfloor$ otherwise. All the computations are done in $\mathcal{O}_K$ and the result is correct at precision $O(p^N)$.*

We give a proof of Theorem 15 at the end of Section 3.3. Right now, we concentrate on the complexity of Algorithm 1. Let $\mathrm{MM}(g, n)$ be the number of arithmetical operations required to compute the product of two $g \times g$ matrices containing polynomials of degree n with coefficients

in K and $\mathrm{M}(n) := \mathrm{MM}(1,n)$, therefore $\mathrm{M}(n)$ is the number of arithmetical operations required to compute the product of two polynomials of degree n. According to [BCG+17, Chapter 8], the two functions $\mathrm{M}(.)$ and $\mathrm{MM}(g,.)$ are related by the following formula

$$\mathrm{MM}(g,n) = O\left(g^{\omega}\mathrm{M}(n)\right), \tag{9}$$

where $\omega \in [2,3[$ is the exponent of matrix multiplication. Furthermore, we denote by $\mathrm{C}_H(n)$ the algebraic complexity for computing $H \circ X \mod t^n$ for any map $H : K[\![t]\!]^g \to M_g(K[\![t]\!])$. We assume that $\mathrm{M}(n)$ and $\mathrm{C}_H(n)$ satisfy the superadditivity hypothesis

$$\begin{array}{rcl} \mathrm{M}(n_1+n_2) & \geq & \mathrm{M}(n_1)+\mathrm{M}(n_2), \\ \mathrm{C}_H(n_1+n_2) & \geq & \mathrm{C}_H(n_1)+\mathrm{C}_H(n_2), \quad \forall n_1,n_2 \in \mathbb{N}. \end{array} \tag{10}$$

For instance, when H is given by a matrix $(f_{ij})_{i,j}$ such that f_{ij} is an univariate polynomial of degree d for every $i,j \in \{1,\ldots,g\}$, then $\mathrm{C}_H(n) = O\left(g^2 d\mathrm{M}(n)\right)$.

Remark 16. In the situation of Equation (2), the map H includes univariate rational fractions of radicals of degree $O(g)$; in this case, we compute $y_1^2,\ldots,y_g^2 \mod t^n$, we use a Newton scheme to compute $y_1^{-1},\ldots,y_g^{-1} \mod t^n$, then we compute $x_i y_i^{-1}, x_i^2 y_i^{-1}, \ldots x_i^{g-1} y_i^{-1} \mod t^n$ for $i = 1,\ldots,g$. The algebraic complexity $\mathrm{C}_H(n)$ is therefore equal to $\mathrm{C}_H(n) = O\left(g^2\mathrm{M}(n)\right)$.

Proposition 17. *Algorithm 1 performs* $O\left(\mathrm{MM}(g,n) + \mathrm{C}_{H_{\mathrm{f}}}(n)\right)$ *operations in* K.

Proof. The complexity of computing $H_{\mathrm{f}}(0)^{-1}$ is at most $O(g^{\omega})$ operations in K. Let D denote the algebraic complexity of Algorithm 1, then we have the following relation

$$\mathrm{D}(n) \leq \mathrm{D}\left(\left\lceil \frac{n-1}{2} \right\rceil\right) + O\left(\mathrm{MM}(g,n) + \mathrm{C}_{H_{\mathrm{f}}}(n)\right).$$

Noticing that g is fixed and using Eqs. (9) and (10), we find $\mathrm{D}(n) = O\left(\mathrm{MM}(g,n) + \mathrm{C}_{H_{\mathrm{f}}}(n)\right)$ and the result is proved. □

Corollary 18. *When performed with fixed point arithmetic at precision* $O(p^M)$*, the bit complexity of Algorithm 1 is* $O\left(\left(\mathrm{MM}(g,n) + \mathrm{C}_{H_{\mathrm{f}}}(n)\right) \cdot \mathrm{A}(K;M)\right)$ *where* $\mathrm{A}(K;M)$ *denotes an upper bound on the bit complexity of the arithmetic operations in* $\mathcal{O}_K/\pi^{eM}\mathcal{O}_K$.

3.3. **Precision analysis.** The goal of this subsection is to prove Theorem 15. The proof relies on the the theory of "differential precision" developed in [CRV14, CRV15]. We follow the same strategy of [CEL20, LV16].

Let g be a fixed positive integer. We study the solution X of Equation (4) when G varies, with the assumption $H_{\mathrm{f}}(0)$ is invertible in $M_g(\mathcal{O}_K)$. Proposition 13 showed that Equation (4) has a unique solution $X(G) \in K[\![t]\!]^g$. Moreover, if we examine the proof of Proposition 13, we see that the $n+1$ first coefficients of the vector $X(G)$ depends only on the first n coefficients of G. This gives a well-defined function

$$\begin{array}{rccc} X_n \ : & \left(K[\![t]\!]/\left(t^n\right)\right)^g & \longrightarrow & \left(tK[\![t]\!]/\left(t^{n+1}\right)\right)^g \\ & G & \longmapsto & X(G) \end{array}$$

for a given positive integer n. In addition, the proof of Proposition 13 states that for $G \in \left(K[\![t]\!]/\left(t^n\right)\right)^g$, $X_n(G)$ can be expressed as a polynomial in $G(0), G'(0), \ldots, G^{(n-1)}(0)$ with coefficients in K, therefore X_n is locally analytic.

Proposition 19. *For $G \in (K[\![t]\!]/(t^n))^g$, the differential of X_n with respect to G is the following function*

$$\begin{aligned} dX_n(G) \,:\, (K[\![t]\!]/(t^n))^g &\longrightarrow \left(tK[\![t]\!]/\left(t^{n+1}\right)\right)^g \\ \delta G &\longmapsto \left(H_{\mathrm{f}}\left(X_n(G)\right)\right)^{-1} \cdot \int \delta G. \end{aligned}$$

Proof. We differentiate the equation $H_{\mathrm{f}}(X_n(G)) \cdot X_n(G)' = G$ with respect to G, we obtain the following relation

$$H_{\mathrm{f}}(X_n(G)) \cdot \left(dX_n(G)(\delta G)\right)' + dH_{\mathrm{f}}(X_n(G))(dX_n(G)(\delta G)) \cdot X_n(G)' = \delta G \tag{11}$$

where $dH_{\mathrm{f}}(X_n(G))$ is the differential of H_{f} at $X_n(G)$ defined in (6). Making use of the relation

$$\left(\left(H_{\mathrm{f}}(X_n(G))\right) \cdot dX_n(G)(\delta G)\right)' = H_{\mathrm{f}}(X_n(G)) \cdot \left(dX_n(G)(\delta G)\right)' + dH_{\mathrm{f}}(X_n(G))(dX_n(G)(\delta G)) \cdot X_n(G)',$$

Equation (11) becomes

$$\left(H_{\mathrm{f}}(X_n(G)) \cdot dX_n(G)(\delta G)\right)' = \delta G.$$

Integrating the above relation and multiplying by $\left(H_{\mathrm{f}}(X_n(G))\right)^{-1}$ we get the result. □

We now introduce some norms on $(K[\![t]\!]/(t^n))^g$ and $(tK[\![t]\!]/(t^n))^g$. We set $E_n = (K[\![t]\!]/(t^n))^g$ and $F_n = \left(tK[\![t]\!]/\left(t^{n+1}\right)\right)^g$; for instance, X_n is a function from E_n to F_n.
First, we equip the vector space $K_n := K[\![t]\!]/(t^n)$ with the usual Gauss norm

$$\|a_0 + a_1 t + \cdots + a_{n-1}\|_{K_n} = \max\left(|a_0|, |a_1|, \ldots, |a_{n-1}|\right).$$

We equip $M_g(K[\![t]\!]/(t^n))$ with the induced norm: for every $A = (a_{ij}(t))_{ij} \in M_g(K[\![t]\!]/(t^n))$,

$$\|A\| = \max_i \sum_{j=1}^{g} \|a_{ij}(t)\|_{K_n}.$$

We endow F_n with the norm obtained by the restriction of the induced norm $\|.\|$ on F_n: for every $X = (x_i(t))_i \in F_n$,

$$\|x\|_{F_n} = \max_i \|x_i(t)\|_{K_n}.$$

In the other hand, we endow E_n with the following norm: for every $X = (x_i(t))_i \in E_n$,

$$\|x\|_{E_n} = \| \int x \|_{F_n} = \max_i \| \int x_i(t) \|_{K_n}.$$

Lemma 20. *The induced norm on $M_g(K[\![t]\!]/(t^n))$ is compatible with the norm on F_n, in other words we have*

$$\|A\, x\|_{F_n} \leq \|A\| \, \|x\|_{F_n}$$

for all $A \in M_g(K[\![t]\!]/(t^n))$ and $x \in F_n$.

Proof. The result follows immediately from the sub-multiplicativity of the norm $\|.\|_{K_n}$. □

Lemma 21. *Let $G \in (\mathcal{O}_K[\![t]\!]/(t^n))^g$. We assume that $X_n(G) \in (t\mathcal{O}_K[\![t]\!]/(t^n))^g$, then $dX_n(G) : E_n \longrightarrow F_n$ is an isometry.*

Proof. The assumptions $X_n(G) \in (t\mathcal{O}_K[\![t]\!]/(t^n))^g$ and $H_{\mathrm{f}}(0) \in \mathrm{GL}_g\left(\mathcal{O}_K\right)$ guarantee the invertibility of $H_{\mathrm{f}}(X_n(G))$ in $M_g(\mathcal{O}_K[\![t]\!])$. Therefore, the norm $\|H_{\mathrm{f}}(X_n(G))\|$ is equal to one. It follows from Lemma 20 that the product $\left(H_{\mathrm{f}}(X_n(G))\right) \cdot \int \delta G$ and $\int \delta G$ have the same norm on F_n, which is equal to $\|\delta G\|_{E_n}$. □

We define the following function:

$$\begin{array}{rccl} \tau_n : & F_n \times E_n & \longrightarrow & \mathrm{Hom}(E_n, F_n) \\ & (X\,,\,G) & \longmapsto & \left(\delta G \mapsto (H_{\mathrm{f}}(X))^{-1} \cdot \displaystyle\int \delta G\right). \end{array}$$

By Proposition 19, the map dX_n is equal to $\tau_n \circ (X_n, \mathrm{id})$, where id denotes the identity map on E_n. We associate to a locally analytic function f the Legendre function associated to the epigraph of f, $\Lambda(f) : \mathbb{R}\cup\{\infty\} \longrightarrow \mathbb{R}\cup\{\infty\}$ (see [CRV14, Section 3.2] for an explicit definition). Also, we define

$$\Lambda(f)_{\geq 2}(x) = \inf_{y\geq 0} \left(\Lambda(f)(x+y) - 2y\right).$$

Lemma 22. *Let $x \in \mathbb{R}$ such that $x < -2\dfrac{\log p}{p-1}$, then $\Lambda(X_n)_{\geq 2}(x) < x$.*

Proof. One checks easily that $\Lambda(\mathrm{id})(x) = x$ and $\Lambda(\tau_n)(x) \geq 0$ for all $x \in \mathbb{R}_+^*$. Applying [CRV15, Proposition 2.5], we get $\Lambda(X_n)_{\geq 2}(x) \leq 2\left(x + \dfrac{\log p}{p-1}\right)$ if $x \leq -\dfrac{\log p}{p-1}$. Therefore, $\Lambda(X_n)_{\geq 2}(x) < x$ if $x < -2\dfrac{\log p}{p-1}$. □

Proposition 23. *Let $B_{E_n}(\delta)$ (resp. $B_{F_n}(\delta)$) be the closed ball in E_n (resp. in F_n) of center 0 and radius δ. Under the assumption of Lemma 21, we have for all $\delta < p^{\frac{-2}{p-1}}$,*

$$X_n(G + B_{E_n}(\delta)) = X_n(G) + B_{F_n}(\delta).$$

Proof. As a direct consequence of [CRV14, Proposition 3.12] and Lemma 22, we have the following formula

$$X_n(G + B_{E_n}(\delta)) = X_n(G) + dX_n(G)(B_{E_n}(\delta)),$$

for all $\delta < p^{\frac{-2}{p-1}}$. The result follows from Lemma 21. □

We end this section by giving a proof of Theorem 15.

Correctness proof of Theorem 15. Let G, f, n and g be the output of Algorithm 1. We first prove by induction on $n \geq 1$ the following equation

$$H_{\mathrm{f}}(X_n) \cdot X_n' = G \mod (t^n, p^M).$$

Let m be a positive integer and $n = 2m+1$. Let $e_m = G - H_{\mathrm{f}}(X_m) \cdot X_m'$. From the relation

$$X_n = X_m + (H_{\mathrm{f}}(X_m))^{-1} \int e_m\, dt \mod (t^{n+1}, p^M),$$

we derive the two formulas

$$H_{\mathrm{f}}(X_m) \cdot X_n = H_{\mathrm{f}}(X_m) \cdot X_m + \int e_m\, dt \mod (t^{n+1}, p^M) \tag{12}$$

and

$$\begin{aligned} H_{\mathrm{f}}(X_m) \cdot X_n' &= H_{\mathrm{f}}(X_m) \cdot X_m' + (H_{\mathrm{f}}(X_m))' \cdot (X_m - X_n) + e_m \mod (t^n, p^M) \\ &= G + (H_{\mathrm{f}}(X_m))' \cdot (X_m - X_n) \mod (t^n, p^M) \\ &= G - (H_{\mathrm{f}}(X_m))' \cdot (H_{\mathrm{f}}(X_m))^{-1} \int e_m\, dt \mod (t^n, p^M). \end{aligned}$$

Using the fact that the first m coefficients of e_m vanish, we get

$$H_{\mathrm{f}}(X_n)\cdot X_n' = H_{\mathrm{f}}(X_m)\cdot X_n' + dH_{\mathrm{f}}(X_m)\left((H_{\mathrm{f}}(X_m))^{-1}\int e_m\,dt\right)\cdot X_m' \mod (t^n, p^M)\,. \quad (13)$$

In addition, one can easily verifies

$$dH_{\mathrm{f}}(X_m)\left((H_{\mathrm{f}}(X_m))^{-1}\int e_m\,dt\right)\cdot X_m' = (H_{\mathrm{f}}(X_m))'\cdot(H_{\mathrm{f}}(X_m))^{-1}\int e_m\,dt$$

Hence, Equation (13) becomes

$$H_{\mathrm{f}}(X_n)\cdot X_n' = G \mod (t^n, p^M).$$

Now, we define $G_n = H_{\mathrm{f}}(X_n)\cdot X_n'$ so that we have $X_n = X_n(G_n)$ and $\|G - G_n\|_{F_n} \le p^{-M}$. Therefore, $\|G - G_n\|_{E_n} \le p^{-M+\lfloor \log_p(n)\rfloor}$. By Proposition 23, we have that

$$X_n(G_n) = X_n(G) \mod (t^{n+1}, p^N).$$

Thus $X_n = X_n(G) \mod (t^{n+1}, p^N)$. □

4. Experiments

Using an implementation of both Algorithm 1 and the HALF-GCD variant given in [Tho03] with the MAGMA computer algebra system [BCP97], we compute the first g components $\sigma_1, \dots \sigma_g$ of the associated rational representation for the multiplication by an integer ℓ for Jacobians of genus 2 and 3, timings are detailed in Section 4.2. The calculations are done at p-adic precision $O(p^M)$ with $M = 1+\lfloor \log_p(2g\ell)\rfloor$. In addition to our implementation, we make use of Couveignes and Ezome's Algortihm [CE15] to compute explicit isogenies between Jacobians of genus two curves over a finite extension of $\mathbb{F}_p$ by passing through a finite extension of $\mathbb{Q}_p$. A complete example is given below.

4.1. **An example.** We consider the genus two curve given by $C_1/\mathbb{F}_{19}: y^2 = x^5+16\,x^4+11\,x^3+3\,x^2+5\,x+17$. Let $J(C_1)$ its Jacobian and ℓ be a prime number different from 19. We look for a maximal isotropic subgroup V of $J(C_1)[\ell]$ which is invariant by the Frobenius endomorphism. Such a group is found for $\ell = 11$, therefore an $(11,11)$-isogeny over $\mathbb{F}_{19}$ exists. Let us compute its rational representation by applying Algorithm 1 to Equation (2).
The p-adic precision needed to do the calculations is therefore equal to $1 + \lfloor \log_{19}(110)\rfloor = 2$. We first lift C_1 over $\mathbb{Q}_{19}$ as

$$\mathcal{C}_1/\mathbb{Q}_{19}: y^2 = x^5 + (16+O(19^2))\,x^4 + (11+O(19^2))\,x^3 + (3+O(19^2))\,x^2 + (5+O(19^2))\,x + 17 + O(19^2)\,.$$

We lift the subgroup V as $\mathcal{V}$ in a finite extension of $\mathbb{Q}_{19}$ by lifting its two generators. Let C_2 (resp $\mathcal{C}_2$) be the curve such that $J(C_2) = J(C_1)/V$ (resp $J(\mathcal{C}_1)/\mathcal{V}$). Using the main algorithm of [CE15], we find an equation of $\mathcal{C}_2$,

$$\mathcal{C}_2/\mathbb{Q}_{19}: y^2 = (2+O(19^2))\,x^5 - (176+O(19^2))\,x^4 - (100+O(19^2))\,x^3 + (2546+O(19^2))\,x^2 - (68+O(19^3))\,x\,,$$

and the normalization matrix being equal to

$$\begin{pmatrix} 95+O(19^2) & 233+O(19^2) \\ 155+O(19^2) & 228+O(19^2)\end{pmatrix}.$$

The computation of the normalization matrix is done by sending the formal point

$$P_1(t) = \big(t + O(19^2), 146 - 21\,t + 179\,t^2 + O\big(19^2, t^3\big)\big) \in \mathcal{C}_1\left(\mathbb{Q}_{19}[\![t]\!]\right)$$

to

$$\Big\{R_1 = \big(-36 + 353\,t + O\big(19^2, t^2\big), -13 + 326\,t + O\big(19^2, t^2\big)\big)\,,$$
$$R_2 = \big(-129 + 102\,t + O\big(19^2, t^2\big), -47 + 2\,t + O\big(19^2, t^2\big)\big)\Big\}$$

in $\mathcal{C}_2\left(\mathbb{Q}_{19}[\![t]\!]\right)^{(2)}$. We can therefore choose $X_0 = \big(O(19^2), 146 + O(19^2)\big)$ as an initial condition for the differential equation, then send it to the point $\big(O(19^2), O(19^2)\big)$ by making the change of variables $X(t) \leftarrow X(t) - X_0$. Using the equation of the curve $\mathcal{C}_1$, we compute the y-coordinate of $P_1(t)$ modulo $(19^2, t^{111})$, then we compute $G \mod (19^2, t^{111})$.
A call from Algorithm 1, gives the series $x_1(t), x_2(t), y_1(t)$ and $y_2(t)$ modulo $(19^2, t^{111})$. For instance, the first 21 terms of $x_1(t)$ and $x_2(t)$ are given by

$$x_1(t) = -36-8t-58t^2-90t^3-90t^4-145t^5-124t^6-107t^7-13t^8-114t^9+154t^{10}+129t^{11}+88t^{12}$$
$$+ 103t^{13} - 22t^{14} - 147t^{15} - 178t^{16} + 168t^{17} + 144t^{18} - 166t^{19} - 77t^{20} + O(19^2, t^{21})$$

and

$$x_2(t) = -129+102t+100t^2+94t^3+45t^4+91t^5+29t^6+137t^7-132t^8-52t^9+51t^{10}+150t^{11}+80t^{12}$$
$$+ 90t^{13} - 124t^{14} - 163t^{15} + 90t^{16} + 102t^{17} + 55t^{18} + 44t^{19} + 23t^{20} + O(19^2, t^{21}).$$

Applying the HALF-GCD algorithm to the series $x_1(t)+x_2(t), x_1(t)\cdot x_2(t), (y_2(t)-y_1(t))/(x_2(t)-x_1(t))$ and $(y_1(t)\cdot x_2(t)-y_2(t)\cdot x_1(t))/(x_2(t)-x_1(t))$ modulo 19, we recover the rational functions $\sigma_1, \sigma_2, \alpha_1$ and α_2. For instance, the numerator N of $-\sigma_1$ is given by

$$N = x^{20} + 8x^{19} + 12x^{18} + 4x^{17} + 16x^{16} + 2x^{15} + 18x^{14} + 2x^{13} + 18x^{12} + 16x^{11} + 13x^{10}$$
$$+ 6x^9 + 5x^8 + 10x^7 + 5x^6 + 10x^5 + 9x^4 + 17x^3 + 18x^2 + 1$$

and its denominator D is equal to

$$D = 12x^{21} + 11x^{20} + 18x^{19} + 14x^{18} + 13x^{16} + 18x^{15} + 8x^{14} + 5x^{13} + 13x^{12} + 16x^{11} + 2x^{10}$$
$$+ 5x^9 + 3x^8 + 4x^7 + 6x^6 + 5x^5 + 18x^4 + 11x^3 + 16x^2 + 9x + 16.$$

4.2. **Timings.** We use an implementation in MAGMA of Algortihm 1 to compute the components $\sigma_1, \ldots, \sigma_g$ of the rational representation of the multiplication by ℓ map in $\mathbb{F}_7$ for Jacobians of hyperelliptic curves of genus 2 and 3 for some $\ell \in \{0, \ldots, 461\}$. Results are detailed on Figure 1. The base ring of all our computations does not change, it is always $\mathbb{Z}/7^\lambda\mathbb{Z}$ for $\lambda = 1+\lfloor \log_7(2g\ell^2) \rfloor$, so the timings for $g = 3$ are significantly larger than those of $g = 2$ by a small constant factor.

References

[BCG+17] A. Bostan, F. Chyzak, M. Giusti, R. Lebreton, G. Lecerf, B. Salvy, and É. Schost. Algorithmes efficaces en calcul formel. 2017. 10

[BCP97] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993). 13

[BGG+17] S. Ballentine, A. Guillevic, E. L. García, C. Martindale, M. Massierer, B. Smith, and J. Top. Isogenies for point counting on genus two hyperelliptic curves with maximal real multiplication. In *Algebraic geometry for coding theory and cryptography*, pages 63–94. Springer, 2017. 1

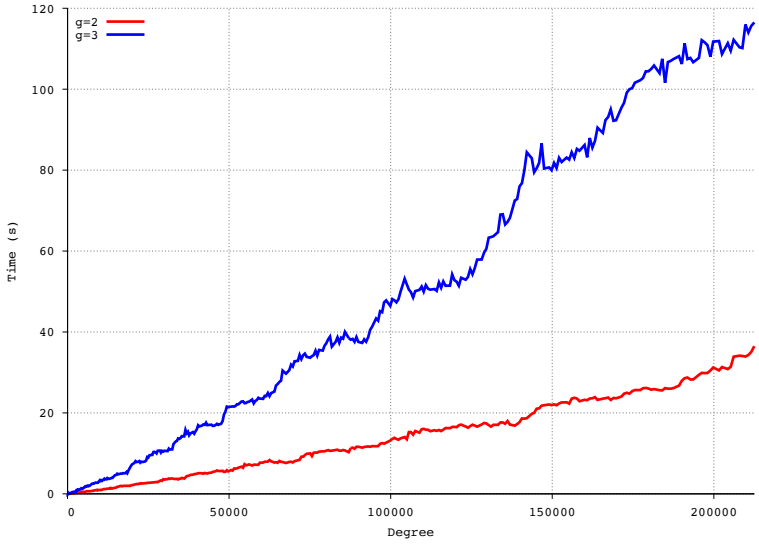


FIGURE 1. Isogeny computations for Jacobians of genus 2 and 3 curves in $\mathbb{F}_7$.

[Car17] X. Caruso. Computations with p-adic numbers. *Les cours du CIRM*, 5(1), 2017. 7

[CE15] J.-M. Couveignes and T. Ezome. Computing functions on jacobians and their quotients. *LMS Journal of Computation and Mathematics*, 18(1):555–577, 2015. 1, 4, 5, 6, 13

[CEL20] X. Caruso, E. Eid, and R. Lercier. Fast computation of elliptic curve isogenies in characteristic two. working paper or preprint, March 2020. 1, 10

[CR15] R. Cosset and D. Robert. Computing (ℓ, ℓ)-isogenies in polynomial time on jacobians of genus 2 curves. *Mathematics of Computation*, 84(294):1953–1975, 2015. 1

[CRV14] X. Caruso, D. Roe, and T. Vaccon. Tracking p-adic precision. *LMS J. Comput. Math.*, 17(suppl. A):274–294, 2014. 10, 12

[CRV15] X. Caruso, D. Roe, and T. Vaccon. p-adic stability in linear algebra. In *ISSAC'15—Proceedings of the 2015 ACM International Symposium on Symbolic and Algebraic Computation*, pages 101–108. ACM, New York, 2015. 10, 12

[CS20] C. Costello and B. Smith. The supersingular isogeny problem in genus 2 and beyond. In *International Conference on Post-Quantum Cryptography*, pages 151–168. Springer, 2020. 1

[FT19] E. V. Flynn and Y. B. Ti. Genus two isogeny cryptography. In J. Ding and R. Steinwandt, editors, *Post-Quantum Cryptography*, pages 286–306, Cham, 2019. Springer International Publishing. 1

[GS12] P. Gaudry and É. Schost. Genus 2 point counting over prime fields. *Journal of Symbolic Computation*, 47(4):368–400, 2012. 1

[KPR20] J. Kieffer, A. Page, and D. Robert. Computing isogenies from modular equations between Jacobians of genus 2 curves. working paper or preprint, January 2020. 1, 4, 5, 6

[LL06] R. Lercier and D. Lubicz. A quasi quadratic time algorithm for hyperelliptic curve point counting. *The Ramanujan Journal*, 12(3):399–423, 2006. 1

[LS08] R. Lercier and T. Sirvent. On Elkies subgroups of l-torsion points in elliptic curves defined over a finite field. *J. Théor. Nombres Bordeaux*, 20(3):783–797, 2008. 1

[LV16] P. Lairez and T. Vaccon. On p-adic differential equations with separation of variables. In *Proceedings of the 2016 ACM International Symposium on Symbolic and Algebraic Computation*, pages 319–323. ACM, New York, 2016. 1, 2, 10

[Mat59] T. Matsusaka. On a characterization of a Jacobian variety. 1959. 5

[Mil86] J. S. Milne. Abelian varieties. In *Arithmetic geometry*, pages 103–150. Springer, 1986. 2, 3

[Mil19] E. Milio. Computing isogenies between Jacobian of curves of genus 2 and 3. working paper or preprint, August 2019. 1

[OS86] F. OORT and T. SEKIGUCHI. The canonical lifting of an ordinary jacobian variety need not be a jacobian variety. *J. Math. Soc. Japan*, 38(3):427–437, 07 1986. 1

[Tho03] E. Thomé. *Algorithmes de calcul de logarithmes discrets dans les corps finis*. PhD thesis, École polytechnique, 2003. 13

[Tia20] S. Tian. Translating the discrete logarithm problem on jacobians of genus 3 hyperelliptic curves with (ℓ, ℓ, ℓ)-isogenies, 2020. 1

[Vac15] T. Vaccon. *Précision p-adique: applications en calcul formel, théorie des nombres et cryptographie*. PhD thesis, University of Rennes 1, 2015. 7

Élie Eid, Univ. Rennes, CNRS, IRMAR - UMR 6625, F-35000 Rennes, France.
Email address: elie.eid@univ-rennes1.fr