FAST COMPUTATION OF ELLIPTIC CURVE ISOGENIES IN CHARACTERISTIC TWO

XAVIER CARUSO, ÉLIE EID, AND REYNALD LERCIER

ABSTRACT. We propose an algorithm that calculates isogenies between elliptic curves defined over an extension K of $\mathbb{Q}_2$. It consists in efficiently solving with a logarithmic loss of 2-adic precision the first order differential equation satisfied by the isogeny.

We give some applications, especially computing over finite fields of characteristic 2 isogenies of elliptic curves and irreducible polynomials, both in quasi-linear time in the degree.

1. INTRODUCTION

With the advent of public key cryptography in the 1970s, a keen interest for elliptic curves emerged. Pretty soon, attention has been given to their isogenies, especially for calculating the number of points of curves defined over finite fields [Sch95] and more recently for isogeny-based cryptography [RS06, Cou06, DFJP14]. Other applications have followed: primality proving, normal basis of field extensions, computation of irreducible polynomials, finite field isomorphisms, *etc* [CL09, CEL12, EL13, Nar18, BDFD+19]. In this work, we concentrate mainly on algorithms for fields of characteristic two that proceed by lifting curves and isogenies to the 2-adics.

Let k be a field and $\ell > 1$ an odd integer. Let E and $\tilde{E}$ be two elliptic curves defined over k. We suppose that there exists a separable isogeny $I : E \to \tilde{E}$ defined over k as well and we are interested in designing a fast algorithm for computing it. When $\mathrm{char}(k) \neq 2$, this can be achieved by solving a certain nonlinear differential equation attached to the situation [BMSS08, LS08, LV16]. Let us recall briefly how it works. It is well known that E and $\tilde{E}$ can be realized by the following equations:

$$E : y^2 = x^3 + a_2\,x^2 + a_4\,x + a_6 \quad \text{and} \quad \tilde{E} : y^2 = x^3 + \tilde{a}_2\,x^2 + \tilde{a}_4\,x + \tilde{a}_6. \tag{1}$$

These are the so-called Weierstrass models. Moreover, by [Koh96, § 2.4], we know that the isogeny I has an expression of the form

$$I(x,y) = \big(\eta(x),\, c\,y\,\eta'(x)\big) \tag{2}$$

where $c \in k^\times$ and η is a rational function whose numerator and denominator have degree ℓ and $\ell-1$ respectively. The constant c is the so-called *isogeny differential* and can be characterized as follows: if $I^* : \Omega_{\tilde{E}/k} \longrightarrow \Omega_{E/k}$ is the map induced by I on the tangent spaces at 0, we have $\frac{dx}{y} = c \cdot \frac{d\tilde{x}}{\tilde{y}}$. (see [Sil09, Sil94]). The terminology "normalized isogenies" is sometimes used in the case $c = 1$. Combining Eqs. (1) and (2), we realize that the computation of I reduces to solving the following nonlinear differential equation:

$$c^2 \cdot (x^3 + a_2\,x^2 + a_4\,x + a_6) \cdot \eta'^2 = \eta^3 + \tilde{a}_2\,\eta^2 + \tilde{a}_4\,\eta + \tilde{a}_6. \tag{3}$$

Date: March 13, 2020.

For several reasons, it is convenient to perform the change of variables $t = 1/x$ and the change of functions $z(t) = 1/\eta(x)$. Eq. (3) then becomes

$$c^2 \cdot (t + a_2 t^2 + a_4 t^3 + a_6 t^4) \cdot z'^2 = z + \tilde{a}_2 z^2 + \tilde{a}_4 z^3 + \tilde{a}_6 z^4 \,. \tag{4}$$

When k has characteristic 0, Bostan and al. [BMSS08] proposed to solve Eq. (4) using a well-designed Newton iteration. This strategy allows them to compute $z(t) \bmod t^{2\ell+1}$ for a cost of $\tilde{O}(\ell)$ operations in the ground field and, in a second time, to recover η using Pade approximations for the same cost. This approach continues to work well when the characteristic of k is positive but large compared to ℓ. However, in the case of small characteristic p, divisions by p do appear and prevent the computation to be carried out to its end. Lercier and Sirvent [LS08] tackled this issue by lifting E, $\tilde{E}$ and I to the p-adics. In the lifted situation, divisions by p can be performed but leads to numerical instability. One then needs to do a neat analysis of the losses of precision. When p is odd, Lercier and Sirvent showed that the number of lost digits stays within $O(\log^2 \ell)$. Later on, still assuming that p is odd, Lairez and Vaccon [LV16] managed to improve on this result and came up with a loss of precision in $\log \ell + O(1)$.

It turns out that extending this approach to characteristic 2 is not an easy task for a couple of reasons. First of all, the general equation of an ordinary elliptic curve in characteristic 2 is no longer $y^2 = x^3 + a_2 x^2 + a_4 x + a_6$ but $y^2 + xy = x^3 + a_2 x^2 + a_6$. As a consequence, the differential equation we need to study, which is defined over the 2-adics, now takes the form

$$c^2 \cdot \Big(4t + (4a_2{+}1)t^2 + 4a_6 t^4\Big) \cdot z'^2 = 4z + (4\tilde{a}_2{+}1)z^2 + 4\tilde{a}_6 z^4 \tag{5}$$

for some constants $c, a_2, a_6, \tilde{a}_2, \tilde{a}_6$ in the ring of Witt vectors of k (if k is the finite field $\mathbb{F}_{2^d}$, it is simply $\mathbb{Z}_{2^d}$, the ring of integers of the unique unramified extension of $\mathbb{Q}_2$ of degree d). Although they look similar, Eq. (5) is much more difficult to handle than Eq. (4). One reason is structural: the polynomial in front of z'^2, namely $4t + (4a_2{+}1)t^2 + 4a_6 t^4$, has a root of norm $1/4$, meaning that the differential equation we are interested in exhibits a singularity in the domain of convergence of the solution we look for. Another reason comes from the exponent 2 on z', which suggests that solving Eq. (5) will require to extract square roots at some point; however, extracting square roots in residual characteristic 2 is known to be a highly unstable operation. Actually a straightforward extension of Lercier and Sirvent's algorithm to characteristic 2 leads to dramatic losses of 2-adic precision of order of magnitude ℓ (instead of $\log \ell$ or $\log^2 \ell$). The conclusion is that this approach is suboptimal and, until now, we were merely reduced to rely on an old algorithm by Lercier [Ler96] whose theoretical efficiency is mitigated, although it behaves surprisingly well in practice (see [DF11] for a discussion on this).

In this paper, we reconsider the 2-adic case and propose a new algorithm to solve Eq. (5). Our algorithm is highly stable and reaches a logarithmic loss of 2-adic precision as Lairez and Vaccon's algorithm does. Moreover, it performs very well in practice, allowing for the computation of isogenies over $\mathbb{F}_2$ of degree up to one million in less than one minute. This is the main result of Section 2.

Theorem (See Theorem 10 and Proposition 11)**.** *Let K be a finite extension of $\mathbb{Q}_2$. Let $\mathcal{O}_K$ be its ring of integers and $\mathcal{O}_K^\times$ the set of invertible elements in $\mathcal{O}_K$. There exists an algorithm that takes as input*

- *two positive integers n and N,*
- *two elements $a, b \in \mathcal{O}_K^\times$,*

- *two series $u, v \in \mathcal{O}_K[\![t]\!]$ with $u(0) \in \mathcal{O}_K^\times$*

and, assuming that the differential equation in z

$$t(t-4a)\, u(t)^2\, z'^2 = z\,(z-4b)\, v(z)^2 \tag{6}$$

has a unique solution in $t\cdot\mathcal{O}_K[\![t]\!]$, outputs this solution modulo $(2^N, t^n)$ for a cost of $\tilde{O}(n)$ operations in $\mathcal{O}_K$ at precision $O(2^M)$ with $M = \max(N, 3) + \lfloor \log_2(n) \rfloor + 2$.

As a consequence, we obtain efficient algorithms to compute isogenies between elliptic curves defined over finite fields of characteristic 2. We finally discuss an application of these results to the calculation of irreducible polynomials defined over such fields in the spirit of the construction of Couveignes and Lercier [CL13].

This article is supplemented by an appendix of theoretical flavor, in which we reuse the techniques of p-adic precision introduced in the core of the paper to prove that the radius of convergence of the solution of Eq. (6) varies continuously with u. To some extent, this result can be understood as the theoretical essence at the origin of the excellent behaviour of our main algorithm. Indeed, the assumption on z made in Theorem 1 roughly means that z has a radius of convergence much larger than expected; the fact that this radius of convergence remains large when the input is perturbed is the key property behind the numerical stability of the algorithm.

2. Fast resolution of a 2-adic differential equation

This section is devoted to the effective resolution of the nonlinear differential equation (6), leading eventually to the proof of Theorem 1. In more details, the computation model we will use throughout this paper is introduced in Section 2.1. The two next subsections are concerned with preliminary material: we show that Eq. (6) has a unique solution in certain cases and study a couple of linear differential equations that will eventually play a quite important role. Our algorithm is presented in Section 2.4 and the proof of its correctness is exposed in Section 2.5. Finally the implementation and corresponding timings are discussed in Section 2.6.

Throughout this section, the letter K refers to a fixed algebraic extension of $\mathbb{Q}_2$. We recall that the 2-adic valuation extends uniquely to K; we will denote it by v_2 and will always assume that it is normalized by $v_2(2) = 1$. We let $\mathcal{O}_K$ denote the ring of integers of K and $\pi \in \mathcal{O}_K$ be a fixed uniformizer of K. We reserve the letter e for the ramification index of the extension $K/\mathbb{Q}_2$, so that we have $v_2(\pi) = 1/e$. It will be convenient to extend the valuation to quotients of $\mathcal{O}_K$: if $x \in \mathcal{O}_K/\pi^{eM}\mathcal{O}_K$, we define $v_2(x) = M$ when $x = 0$ and $v_2(x) = v_2(\hat{x})$ where $\hat{x} \in \mathcal{O}_K$ is any lifting of x otherwise.

2.1. **Computation model.**

Carrying explicit computations in K is not straightforward because elements of K carry an infinite amount of information and need to be truncated to fit in the memory of a computer: we sometimes say that K is an *inexact* field. Over the years, several computation models have been proposed to handle these difficulties: interval arithmetic, floating point arithmetic, lazy arithmetic, *etc.* We refer to [Car17] for a detailed discussion about this, including many examples illustrating the advantages and the disadvantages of each possible model.

Throughout this article, we will use the *fixed point arithmetic* model at precision $O(2^M)$, where M is a fixed positive number in $\frac{1}{e}\mathbb{Z}$. Concretely, this means that we shall represent elements of

K by expressions of the form $x + O(2^M)$ with $x \in \mathcal{O}_K/\pi^{eM}\mathcal{O}_K$. Additions, subtractions and multiplications are defined straightforwardly:

$$\big(x + O(2^M)\big) + \big(y + O(2^M)\big) = (x+y) + O(2^M)\,,$$
$$\big(x + O(2^M)\big) - \big(y + O(2^M)\big) = (x-y) + O(2^M)\,,$$
$$\big(x + O(2^M)\big) \times \big(y + O(2^M)\big) = xy + O(2^M)\,.$$

The specifications of division go as follows: for $x, y \in \mathcal{O}_K/\pi^{eM}\mathcal{O}_K$, the division of $x + O(2^M)$ by $y + O(2^M)$

- raises an error is $v_2(y) > v_2(x)$,
- returns $0 + O(2^M)$ if $x = 0$ in $\mathcal{O}_K/\pi^{eM}\mathcal{O}_K$,
- returns any representant $z + O(2^M)$ with the property $x = yz$ in $\mathcal{O}_K/\pi^{eM}\mathcal{O}_K$ otherwise.

Complexity notations and assumptions. In what follows, we shall always assume that we are given algorithms performing additions, subtractions, multiplications and divisions in the computation model described above. Let $\mathrm{A}(K; M)$ be an upper bound on the bit complexity of these algorithms. When $K = \mathbb{Q}_2$, the quotients $\mathcal{O}_K/\pi^{eM}\mathcal{O}_K$ are just $\mathbb{Z}/2^M\mathbb{Z}$ and, relying on fast Fourier transform, we can take $\mathrm{A}(\mathbb{Q}_2; M) \in \tilde{O}(M)$ (where the $\tilde{O}$-notation means that we are hiding logarithmic factors). More generally, if K is an extension of $\mathbb{Q}_2$ of degree d which is presented either by a polynomial which remains irreducible modulo 2 (unramified case) or by an Eisenstein polynomial (totally ramified case), elements of $\mathcal{O}_K/2^{eM}\mathcal{O}_K$ can be represented safely as polynomials over $\mathbb{Z}/2^M\mathbb{Z}$ of degree at most d and we can take $\mathrm{A}(K; M) \in \tilde{O}(dM)$. Finally, the same estimates remain valid when K is presented as a two-step extension, the first one being given by an "unramified" polynomial and the second one being given by an Eisenstein polynomial. We note that this covers all extensions of $\mathbb{Q}_2$.

We further assume that we are given a division-free algorithm for multiplying polynomials over any exact base ring and we let $\mathrm{M}(n)$ be a bound on its algebraic complexity (*i.e.* the number of arithmetical operations in the base ring it performs). For convenience, we will also suppose that the function M satisfies the superadditivity assumption, that is:

$$\forall n, n' \in \mathbb{N}, \quad \mathrm{M}(n + n') \geq \mathrm{M}(n) + \mathrm{M}(n').$$

Standard algorithms allow us to take $\mathrm{M}(n) \in \tilde{O}(n)$. Besides, we observe that an algorithm as above can be used to multiply polynomials over K in the fixed point arithmetic model since additions, multiplications and divisions in this model all reduce to the similar operations in the *exact* quotient ring $\mathcal{O}_K/\pi^{eM}\mathcal{O}_K$. As a consequence, when working in the fixed point arithmetic model at precision $O(2^M)$, the bit complexity of the multiplication of two polynomials of degree n over K is bounded by above by $\mathrm{M}(n) \cdot \mathrm{A}(K; M)$, which itself stays within $\tilde{O}\big(nM \cdot [K : \mathbb{Q}_2]\big)$ under standard assumptions.

2.2. **The setup.** Let $K[\![t]\!]$ be the ring of formal series over K (in the variable t). Given two series $U, V \in K[\![t]\!]$, we consider the following nonlinear differential equation whose unknown is z:

$$U \cdot z'^2 = V \circ z\,. \tag{7}$$

When V is an actual series, the composite $V \circ z$ is not always well defined; however, it is as soon as z vanishes at 0, *i.e.* $z \in tK[\![t]\!]$. For this reason, in what follows, we will always look for solutions of (7) in $tK[\![t]\!]$. We will also always assume that *both U and V have t-adic valuation* 1;

in other words, we suppose that there exist *nonzero* scalars $u_1, v_1 \in K$ such that $U = u_1 t + O(t^2)$ and $V = v_1 t + O(t^2)$.

The following proposition shows that these assumptions are enough to guarantee the existence and the uniqueness of a solution to Eq. (7).

Proposition 1. *Assuming that U and V have t-adic valuation 1, the differential equation (7) admits a unique nonzero solution in $tK[\![t]\!]$.*

Proof. Write $U = \sum_{n=1}^{\infty} u_n t^n$ and $V = \sum_{n=1}^{\infty} v_n t^n$. We are looking for a solution of Eq. (7) of the form $z = \sum_{n=1}^{\infty} z_n t^n$. Taking the n-th derivative of Eq. (7) (and using Faà di Bruno's formula to evaluate the successive derivatives of $V \circ z$), we end up with the relations

$$\sum_{i=0}^{n-1} \sum_{j=0}^{i} (j+1)(i-j+1) z_{j+1} z_{i-j+1} u_{n-i} = \sum_{k_1+2k_2+\cdots+nk_n=n} \frac{(k_1+k_2+\cdots+k_n)!}{k_1!\,k_2!\,\cdots\,k_n!}\, v_{k_1+k_2+\ldots+k_n}\, z_1^{k_1} z_2^{k_2} \cdots z_n^{k_n}\,. \quad (8)$$

When $n = 1$, this formula reduces to $u_1 z_1^2 = v_1 z_1$, showing that z_1 must be equal to 0 or $\frac{v_1}{u_1}$. For bigger n, we observe that the coefficient z_n only appears in the summands indexed by $(i,j) = (n{-}1, 0)$ and $(i,j) = (n{-}1, n{-}1)$ in the left hand side of Eq. (8) and the summand indexed by $(k_1, \ldots, k_n) = (0, \ldots, 0, 1)$ in the right hand side. Isolating them, one obtains

$$z_n = \frac{P_n(z_1, \ldots, z_{n-1})}{(2n{-}1)\, v_1}$$

for some polynomial $P_n \in K[X_1, \ldots, X_{n-1}]$ vanishing at $(0, \ldots, 0)$. It follows for this observation that z must vanish if z_1 vanishes. Otherwise, the coefficients z_n are all uniquely determined, then showing the existence and the unicity of a nonzero solution to Eq. (7). □

We now introduce the two following additional assumptions:

(H_U): there exists $a \in \mathcal{O}_K^\times$ and $u \in \mathcal{O}_K[\![t]\!]$ with $u(0) \in \mathcal{O}_K^\times$ s.t. $U(t) = t(t{-}4a) \cdot u(t)^2$;
(H_V): there exists $b \in \mathcal{O}_K^\times$ and $v \in \mathcal{O}_K[\![t]\!]$ with $v(0) \in \mathcal{O}_K^\times$ s.t. $V(t) = t(t{-}4b) \cdot v(t)^2$.

Remark 2. Both Assumptions (H_U) and (H_V) are fulfiled for the differential equation (5) (which is the one that we need to solve in order to compute isogenies between elliptic curves) after possibly replacing K by its unramified extension of degree 2. Indeed U is then the polynomial $c^2\big(4t + (4a_2+1)t^2 + 4a_6 t^4\big)$ for some $c \in \mathcal{O}_K^\times$ and some $a_2, a_6 \in \mathcal{O}_K$. Looking at valuations, we find that its Newton polygon has a segment of slope -2. Consequently U has a root of valuation 2, *i.e.* U is divisible by $(t{-}4a)$ for some $a \in \mathcal{O}_K^\times$. Since U is also obviously divisible by t, we find that $U(t) = c^2 \cdot t(t{-}4a) \cdot U_0(t)$ where U_0 is the polynomial of degree 2 explicitely given by

$$U_0(t) = 4a_6\, t^2 + 16aa_6\, t + (64a^2 a_6 + 4a_2 + 1).$$

In particular, we observe that $U_0(t) \equiv 1 \pmod 4$ and $U_0(0) \equiv 1{+}4a_2 \pmod 8$. This ensures that U_0 admits a square root in $\mathcal{O}_L[\![t]\!]$ with $L = K[\sqrt{1{+}4a_2}]$. It is easy to check that $L = K[\mu]$ where μ is a root of the polynomial $P(X) = X^2{-}X{-}a_2$. Since P is separable modulo 2, we deduce that L is unramified over K. More precisely, if $\mathrm{Tr}_{K/\mathbb{Q}_2}(a_2)$ is odd, L is the unique unramified extension of K of degree 2 and $L = K$ otherwise. Letting finally $u = c\sqrt{U_0}$, we find that (H_U) is satisfied over $\mathcal{O}_L[\![t]\!]$. The fact that (H_V) is satisfied as well is proved similarly.

Remark 3. We may further remark that an ordinary elliptic curve $E/\mathbb{F}_{2^d} : y^2+xy = x^3+a_2x^2+a_6$ is the twist of the elliptic curve $E'/\mathbb{F}_{2^d} : y^2 + xy = x^3 + a_6$ up to the twisting isomorphism $(x, y) \mapsto (x, y+sx)$ where s is a solution of the equation $s^2 + s + a_2 = 0$ (possibly defined over a quadratic extension of $\mathbb{F}_{2^d}$). Since (H_U) and (H_V) are fulfilled over K for the 2-adic differential equation obtained from E' and the twist $\tilde{E}'$ of the isogenous curve $\tilde{E}$, we can avoid the transition by the quadratic extension L for solving Eq. (5) between E' and $\tilde{E}'$, even if a quadratic extension may be finally needed to obtain the isogeny between E and $\tilde{E}$ by applying the twisting isomorphisms.

In the next subsections, we are going to design an efficient algorithm to compute the unique solution of Eq. (7) under Assumptions (H_U) and (H_V).

2.3. **Two linear differential equations.** We introduce two auxiliary linear differential equations that will appear later on as important ingredients in the resolution of the nonlinear differential equation (7). Precisely, given $a \in \mathcal{O}_K^\times$, we consider

$$(\mathrm{E}_+): \qquad t(t-4a)\, y' + (t-2a)\, y = f\,,$$
$$(\mathrm{E}_-): \qquad t(t-4a)\, y' - (t-2a)\, y = f\,,$$

where y is the unknown and the right hand side f lies in $K[\![t]\!]$.

In the following, if n is a nonnegative integer, we denote by $S_2(n)$ the sum of its digits in base 2. For example $S_2(3) = 2$. One easily checks that the inequality $S_2(n) \leq \lfloor \log_2(n+1) \rfloor$ is valid for all $n \geq 0$ (here $\lfloor x \rfloor$ denotes the integer part of x) and that the equality holds if and only if $n = 2^m - 1$ for some m.

Proposition 4. *For any* $f = \sum_{i=0}^{\infty} f_i t^i \in K[\![t]\!]$*, the differential equation* (E_+) *(resp.* (E_-)*) admits a unique solution in* $K[\![t]\!]$*. Moreover*

- *if* $y = \sum_{i=0}^{\infty} y_i t^i$ *is the solution of* (E_+)*, we have*

$$\forall i \geq 0, \quad \upsilon_2(y_i) \geq \min_{0 \leq k \leq i} \upsilon_2(f_k) - \lfloor \log_2(i+1) \rfloor - 1\,;$$

- *if* $y = \sum_{i=0}^{\infty} y_i t^i$ *is the solution of* (E_-)*, we have*

$$\begin{aligned} \upsilon_2(y_0) &= \upsilon_2(f_0) - 1\,, \\ \upsilon_2(y_1) &\geq \min\big(\upsilon_2(f_0) - 2,\, \upsilon_2(f_1) - 1\big)\,, \\ \forall i \geq 2, \quad \upsilon_2(y_i) &\geq \min_{2 \leq k \leq i} \upsilon_2(f_k) - \lfloor \log_2(i-1) \rfloor - 1\,. \end{aligned}$$

Proof. We only treat the equation (E_+), the case of (E_-) being totally similar. Plugging $f = \sum_{i=0}^{\infty} f_i t^i$ and $y = \sum_{i=0}^{\infty} y_i t^i$ in (E_+), we obtain

$$y_0 = -\frac{f_0}{2a}, \quad y_i = \frac{i\, y_{i-1} - f_i}{2a \cdot (2i+1)} \quad \text{for } i > 0. \tag{9}$$

The existence and the unicity of the solution of (E_+) follows. Regarding the growth of the coefficients, an easy induction on i shows that y_i can be written in the form

$$y_i = \sum_{k=0}^{i} \frac{2^{k-i-1} \cdot i!}{k!}\, e_{i,k}\, f_k$$

Algorithm 1: Linearized equation solver

```
LinDiffSolve (a, f, n)
    Input  : a ∈ O_K^×, n ∈ ℕ and f = Σ_{i=0}^{n−1} f_i t^i ∈ K⟦t⟧/(t^n)
    Output: ψ_{+,n}(f)
    y_0 := −f_0 / 2a
    for i := 1 to n − 1 do
        y_i := (i y_{i−1} − f_i) / (2a · (2i+1)) ;
    return Σ_{i=0}^{n−1} y_i t^i;
```

with $e_{i,k} \in \mathcal{O}_K$ for all i and k. We conclude by applying Euler's formula,

$$\upsilon_2\left(\frac{2^{k-i-1}i!}{k!}\right) = (k-i-1) + (i - S_2(i)) - (k - S_2(k)) = -S_2(i) + S_2(k) - 1\,. \qquad \square$$

The first part of Proposition 4 allows us to define the function $\psi_+ : K[\![t]\!] \to K[\![t]\!]$ (resp. $\psi_- : K[\![t]\!] \to K[\![t]\!]$) taking f to the unique solution of the differential equation (E_+) (resp. (E_-)). Clearly ψ_+ and ψ_- are K-linear mappings. Moreover, given a positive integer n, Proposition 4 again shows that ψ_+ and ψ_- map $t^n K[\![t]\!]$ to itself and then induce K-linear endomorphisms $\psi_{+,n}$ and $\psi_{-,n}$ of $K[\![t]\!]/(t^n)$.

Lemma 5. *For all $f \in K[\![t]\!]$, we have the relation*

$$t(t-4a)\cdot\psi_+(f) = \psi_-\big(t(t-4a)\cdot f\big).$$

Proof. It is enough to check that $t(t-4a)\,\psi_+(f)$ is a solution of

$$t(t-4a)\,y' - (t-2a)\,y = t(t-4a)\,f$$

which is a direct computation. $\square$

We now move to the effective computation of ψ_+. Following the proof of Proposition 4, we directly get Algorithm 1, whose numerical stability is studied in Proposition 6 hereafter. Before stating it, let us recall that e denotes the ramification index of K over $\mathbb{Q}_2$ and that, given $N \in \frac{1}{e}\mathbb{N}$, we use the notation $O(2^N)$ to refer to a quantity which is divisible by π^{eN}.

Proposition 6. *Let $n \in \mathbb{N}$, $N \in \frac{1}{e}\mathbb{N}$ and $f \in \mathcal{O}_K[\![t]\!]/(t^n)$. We assume that $\psi_{+,n}(f) \in \mathcal{O}_K[\![t]\!]/(t^n)$. Then, when* `LinDiffSolve`$(a, f, n)$ *is run with fixed point arithmetic at precision $O(2^M)$ with $M = N + \lfloor \log_2(n+1) \rfloor + 1$, all the performed computations are done in $\mathcal{O}_K$ and the result is correct at precision $O(2^N)$.*

Proof. The fact that all the computations stay within $\mathcal{O}_K$ is a direct consequence of the assumption that $\psi_{+,n}(f)$ has coefficients in $\mathcal{O}_K$. Let y be the output of `LinDiffSolve`(a, f, n). It follows from the definition of fixed point arithmetic that y is solution of

$$t(t-4a)y' + (t-2a)y = f + h$$

for some $h \in \pi^{eM}\mathcal{O}_K[\![t]\!]/(t^n)$. Consequently $y = \psi_{+,n}(f+h) = \psi_{+,n}(f) + \psi_{+,n}(h)$. On the other hand, Proposition 4 (applied with h) shows that $\psi_{+,n}(h) \in \pi^{eN}\mathcal{O}_K[\![t]\!]/(t^n)$. Hence $y \equiv \psi_{+,n}(f)$ (mod (π^{eN}, t^n)), which exactly means that y is correct at precision $O(2^N)$. $\square$

Remark 7. It follows from the specifications on our computation model that, when the m first coefficients of f vanish, the m first coefficients of the output of $\texttt{LinDiffSolve}(a, f, n)$ vanish as well.

2.4. **The algorithm.** We go back to the nonlinear differential equation (7) and assume the hypothesis (H_U). In this setting, we will construct the solution by successive approximations using a Newton scheme. In order to proceed, we suppose that we are given $z_m \in K[\![t]\!]$ for which Eq. (7) is satisfied modulo t^m. We look for a more accurate solution z_n of the form $z_n = z_m + h$ with $h \in t^m K[\![t]\!]$. We compute

$$U(t) \cdot {z'_n}^2 = U(t) \cdot (z'_m + h')^2 \equiv U(t) \cdot ({z'_m}^2 + 2\, z'_m h') \pmod{t^{2m-1}},$$
$$V(z_n) = V(z_m + h) \equiv V(z_m) + V'(z_m) \cdot h \pmod{t^{2m-1}}.$$

Identifying both terms, we obtain the relation

$$2\, U(t)\, z'_m \cdot h' - V'(z_m) \cdot h \;\equiv\; V(z_m) - U(t) \cdot {z'_m}^2 \pmod{t^{2m-1}}. \tag{10}$$

By assumption, we know that $U(t) \cdot {z'_m}^2 \equiv V(z_m) \pmod{t^m}$. Differentiating this equation and dividing by z'_m, we obtain $V'(z_m) \equiv U'(t)\, z'_m + 2\, U(t)\, z''_m \pmod{t^{m-1}}$. Plugging this congruence in Eq. (10), we find

$$2\, U(t)\, z'_m \cdot h' - \Big(U'(t)\, z'_m + 2\, U(t)\, z''_m\Big) \cdot h \;\equiv\; V(z_m) - U(t) \cdot {z'_m}^2 \pmod{t^{2m-1}}.$$

Replacing $U(t)$ by $t(t-4a)\, u(t)^2$ thanks to Hypothesis (H_U), and setting $h = z'_m u \cdot y$, we end up with the differential equation in y

$$t(t-4a)\, y' - (t-2a)\, y \;\equiv\; f_n \pmod{t^{2m-1}} \quad \text{with} \quad f_n = \frac{1}{2u(t)^3} \left(\frac{V(z_m)}{{z'_m}^2} - U(t) \right).$$

By the results of Section 2.3, we derive $h \equiv z'_m u \cdot \psi_-(f_n) \pmod{t^{2m-1}}$. Repeating the above calculations in the reverse direction, we obtain the next proposition.

Proposition 8. *We assume* (H_U)*. Let $m > 1$ be an integer and let $z_m \in K[\![t]\!]$ be a solution of Eq.* (7) *modulo t^m. Then*

$$z_m + z'_m u \cdot \psi_- \left(\frac{1}{2u(t)^3} \left(\frac{V(z_m)}{{z'_m}^2} - U(t) \right) \right) \tag{11}$$

is a solution of Eq. (7) *modulo t^{2m-1}.*

It would be reasonable to expect that Proposition 8 could be easily turned into an algorithm that solves the nonlinear differential equation (7). However, for several reasons (related to the precision analysis), we shall modify a bit our Newton iteration. For now on, we assume (H_V), set $\lambda = ba^{-1} \in \mathcal{O}_K^\times$. For $z_m \in tK[\![t]\!]/(t^m)$, we write

$$z_m = \lambda t + t(t-4a)\, q_m \tag{12}$$

with $q_m \in K[\![t]\!]/(t^{m-1})$. So, z_m is a solution of Eq. (7) modulo t^m if and only if q_m satisfies

$$W(t, q_m) \equiv u(t)^2 {z'_m}^2 \pmod{t^{m-1}}. \tag{13}$$

where W is defined by

$$W(t,x) = \big(\lambda + (t-4a)x\big) \cdot \big(\lambda + tx\big) \cdot v^2\big(\lambda t + t(t-4a)x\big) \in \mathcal{O}_K[\![t, x]\!].$$

Rewriting Proposition 8, we obtain the following corollary.

Algorithm 2: Non linear differential equation solver

```
DiffSolve (a, u, u^2, u^-3, b, v^2, n)
    Input  : u, u^2, v^2 mod t^n,  u, u^-3 mod t^⌈n/2⌉,  a and b satisfying (H_U) and (H_V)
    Output: q_n  mod t^n, (z'_n)^-2 mod t^⌈n/2⌉

    if  n ≤ 1 then
        return v_1 u_1^-1 (ba^-1 − 4a)^-1 mod t^n, 0 mod t^(n−1);
    m := ⌈(n−1)/2⌉;
    q_m, r_m := DiffSolve(a, u, u^2, u^-3, b, v^2, m);          // recursive call
    z_m := ba^-1 t + t(t − 4a) q_m mod t^(n+1);
    w_n := z'_m^2 mod t^n ;                                        // 1 coeff. lost
    s_n := u^2 · w_n − W ∘ q_m  mod t^n;                           // s_n mod t^m = 0
    r_n := r_m · (2 − r_m · w_n) mod t^(n−m);                      // (z'_n)^-2 (Newton iter.)
    f_n := 2^-1 s_n · r_n · u^-3 mod t^n;                          // The argument of ψ_+
    y_n := LinDiffSolve(a, f_n, n);                                // y_n mod t^m = 0
    return q_m + z'_m · u · y_n mod t^n, r_n
```

Algorithm 3: Isogeny differential equation solver

```
IsoSolve (U, V, n)
    Input  : U, V mod t^n satisfying Assumptions (H_U) and (H_V)
    Output: the solution z_n  mod t^n of Eq. (7)

    Compute a, b, U_0 mod t^(n−1) and V_0 mod t^(n−1) ;          // U_0 = u^2 and V_0 = v^2
    Compute u mod t^⌈(n−1)/2⌉ and u^-3 mod t^⌈(n−1)/2⌉;
    z := DiffSolve(a, u, u^2, u^-3, b, v^2, n − 1);
    return  ba^-1 t + t(t − 4a) z mod t^n
```

Corollary 9. *We assume* (H_U) *and* (H_V). *Let* $m > 1$ *be an integer and let* q_m *be a solution of Eq.* (13) *modulo* t^m. *Then*

$$q_m + z'_m u \cdot \psi_+ \left(\frac{1}{2u(t)^3} \left(\frac{W(q_m)}{{z'_m}^2} - u(t)^2 \right) \right)$$

is a solution of Eq. (13) *modulo* t^{2m-1}.

Proof. The formula is easily obtained by plugging Eq. (12) in Eq. (11), and using Lemma 5. ☐

With Corollary 9 and a small optimization consisting in integrating the computation of $(z'_m)^{-2}$ in our Newton scheme, we get Algorithm 2 and Algorithm 3.

If we could work at infinite p-adic precision, it would be clear that Algorithm 3 is correct. The next theorem shows that its correction still holds in the fixed point arithmetic model.

Theorem 10. *Let* $n \in \mathbb{N}$, $N \in \frac{1}{e}\mathbb{N}$ *and* $U, V \in K[\![t]\!]$. *We assume* (H_U) *and* (H_V) *and that the unique nonzero solution of Eq.* (7) *has coefficients in* $\mathcal{O}_K$. *Then, when* `IsoSolve`(U, V, n) *runs with fixed point arithmetic at precision* $O(2^M)$ *with* $M = \max(N, 3) + \lfloor \log_2(n) \rfloor + 2$, *all the performed computations are done in* $\mathcal{O}_K$ *and the result is correct at precision* $O(2^N)$.

We delay the proof of Theorem 10 to Section 2.5. Let us first study the complexity of the Algorithms 2 and 3. We recall that $\mathrm{M}(n)$ denotes the algebraic complexity of a feasible algorithm that computes the product of two polynomials on degree n. Similarly, given a fixed series $W \in K[\![t]\!]$, we define $\mathrm{C}_W(n)$ as the algebraic complexity of an algorithm computing the composite $W \circ z$ modulo t^n. In our case of interest, W turns out to be a polynomial of degree 4 and $\mathrm{C}_W(n) = O(\mathrm{M}(n))$. More generally, we observe that, when W is a polynomial of degree d, we have $\mathrm{C}_W(n) = O(d\mathrm{M}(n))$. In what follows, we assume that C_W satisfies the superadditivity hypothesis, *i.e.* that $\mathrm{C}_W(n+n') \geq \mathrm{C}_W(n) + \mathrm{C}_W(n')$ for all integers n and n'.

Proposition 11. *When it is called on the input (U, V, n), the algorithm* `IsoSolve` *performs at most $O\big(\mathrm{M}(n) + \mathrm{C}_W(n)\big)$ operations in K.*

Proof. The calculation of a and b is done with the Hensel lifting algorithm applied to $U(t)$. The series $u(t)^2$ and $v(t)^2$ are then obtained by Euclidean division by $t(t-4a)$. Then, the series $u(t)^{-1}$ can be computed by the Newton iteration $r \mapsto r \cdot (3 - u^2 r^2)/2$. Finally $u(t)$ is obtained by multiplying $u(t)^{-1}$ by $u(t)^2$ and $u(t)^{-3}$ is obtained by cubing $u(t)^{-1}$. The total complexity of the precomputation steps is then at most $O(\mathrm{M}(n))$ operations in K.

Examining the core of Algorithm 2, we find that its algebraic complexity $\mathrm{T}(n)$ satisfies the relation

$$\mathrm{T}(n) \leq \mathrm{T}\left(\left\lceil \frac{n+1}{2} \right\rceil\right) + O\big(\mathrm{M}(n) + \mathrm{C}_W(n)\big),$$

the complexity of `LinDiffSolve` being linear in n and hence dominated by $\mathrm{M}(n)$. Solving the recurrence and using the superadditivity of M and C_W, we find $\mathrm{T}(n) = O\big(\mathrm{M}(n) + \mathrm{C}_W(n)\big)$ which is also the complexity of Algorithm 3. ☐

Corollary 12. *When executed with fixed point arithmetic at precision $O(2^M)$, the bit complexity of the algorithm* `IsoSolve` *is $O\big((\mathrm{M}(n) + \mathrm{C}_W(n)) \cdot \mathrm{A}(K; M)\big)$.*

Proof. It is a direct consequence of Proposition 11 (combined with the fact that the three algorithms only performs operations in $\mathcal{O}_K$ as promised by Theorem 10). ☐

2.5. **Precision analysis.** The aim of this subsection is to prove Theorem 10. The general scheme of our proof follows that of Lairez and Vaccon [LV16] and relies mostly on the theory of "differential precision" developped by Caruso, Roe and Vaccon in [CRV14, CRV15]. Recall that the differential equation we have to solve reads

$$t(t-4a) \cdot u(t)^2 \cdot z'^2 = V(z)$$

where $a \in \mathcal{O}_K^\times$, $u \in \mathcal{O}_K[\![t]\!]$ with $u(0) \in \mathcal{O}_K^\times$ and $V \in \mathcal{O}_K[\![t]\!]$ with t-adic valuation 1. Letting $g(t) = u(t)^{-1}$, the above equation can be rewritten as follows:

$$t(t-4a) \cdot z'^2 = g(t)^2 \cdot V(z). \tag{14}$$

We are going to study how the solution z of the latter differential equation behaves when g varies. By Proposition 1, we know that Eq. (14) has a unique nonzero solution $z_g \in tK[\![t]\!]$ as soon as $g(0) \neq 0$. Besides, the proof of Proposition 1 shows that the $n+1$ first coefficients of z_g depend only on the n first coefficients of g. In other words, the association $g \mapsto z_g$ defines a function $\Omega_n \to tK[\![t]\!]/(t^{n+1})$ where Ω_n is the open subset of $K[\![t]\!]/(t^n)$ consisting of series with nonzero constant term. In a similar fashion, we notice that z'_g is a well-defined series in $K[\![t]\!]/(t^n)$, when g belongs to Ω_n.

For a given positive integer n, we define

$$\begin{array}{cccc} \varphi_n : & \Omega_n & \longrightarrow & K[\![t]\!]/(t^n) \\ & g & \mapsto & \dfrac{z_g}{t(t-4a)} \end{array}$$

(we note that $t-4a$ is invertible in $K[\![t]\!]/(t^n)$). It follows from the proof of Proposition 1 that φ_n is a polynomial function in $g(0)^{-1}$ and the coefficients of g; in particular, it is locally analytic.

Proposition 13. *For $g \in \Omega_n$, the differential of φ_n at g is the function*

$$\begin{array}{cccc} d\varphi_n(g) : & K[\![t]\!]/(t^n) & \longrightarrow & K[\![t]\!]/(t^n) \\ & \delta g & \mapsto & z'_g \cdot g^{-1} \cdot \psi_{+,n}(\delta g) \end{array}$$

where $\psi_{+,n}$ is the function defined in Section 2.3.

Proof. We first differentiate the function $g \mapsto z_g$. This amounts to find a quantity δz varying linearly with respect to δg for which the relation $z_{g+\delta g} = z_g + \delta z$ holds at order 1. Coming back to the definitions, we are led to the identity

$$t(t-4a) \cdot (z'_g + \delta z')^2 = (g(t) + \delta g(t))^2 \cdot V(z_g + \delta z) \ + \text{ higher order terms}.$$

Expanding this relation, we obtain the following linear differential equation in δz:

$$2t(t-4a)\, z'_g \cdot \delta z' = 2g(t)\, \delta g(t)\, V(z_g) + g(t)^2\, V'(z_g) \cdot \delta z. \qquad (15)$$

Observe that z_g and g are both invertible in $K[\![t]\!]/(t^n)$. We can then write $\delta z = z'_g\, g^{-1} \cdot y$ for some $y \in K[\![t]\!]/(t^n)$. Performing this change of functions and making use of the relations

$$t(t-4a)(z'_g)^2 = g^2\, V(z_g)$$
$$2t(t-4a)z'_g z''_g + 2(t-2a)(z'_g)^2 = g^2 z'_g\, V'(z_g) + 2gg'\, V(z_g)$$

(the second one being obtained from the first one by derivation), Eq. (15) becomes

$$t(t-4a)y' - (t-2a)y = t(t-4a) \cdot \delta g.$$

Therefore $y = \psi_{-,n+1}\big(t(t-4a) \cdot \delta g\big) = t(t-4a) \cdot \psi_{+,n}(\delta g)$ thanks to Lemma 5. We finally derive that $\delta z = t(t-4a) \cdot z'_g g^{-1} \cdot \psi_{+,n}(\delta g)$ and, simplifying by $t(t-4a)$, the proposition follows. □

We now need to introduce norms on $K[\![t]\!]/(t^n)$. In order to avoid confusions, we set $E_n = F_n = K[\![t]\!]/(t^n)$ and use E_n (resp. F_n) for the domain (resp. the codomain) of our functions. Then, for example, Ω_n will be considered as a subset of E_n and φ_n as a function from Ω_n to F_n. Similarly $d\varphi_n(g)$ will be viewed as an element of $\mathrm{Hom}(E_n, F_n)$.

We endow F_n with the usual Gauss norm

$$\big\| a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} \big\|_{F_n} = \max\big(|a_0|, |a_1|, \ldots, |a_{n-1}|\big).$$

On the contrary, we endow E_n with the norm $\|f\|_{E_n} = \|\psi_{+,n}(f)\|_{F_n}$. It is then clear that $\psi_{+,n} : E_n \to F_n$ is an isometry.

Lemma 14. *Let $g \in \mathcal{O}_K[\![t]\!]/(t^n)$. We assume $z_g \in \mathcal{O}_K[\![t]\!]/(t^n)$ and that both $g(0)$ and $z'_g(0)$ are invertible in $\mathcal{O}_K$. Then $d\varphi_n(g) : E_n \to F_n$ is an isometry.*

Proof. The assumptions ensure that g and z'_g are invertible in $\mathcal{O}_K[\![t]\!]/(t^n)$. Therefore the multiplication by $z'_g\, g^{-1}$ is an isometry of F_n. The lemma then follows from the explicit formula of $d\varphi_n(g)$ given by Proposition 13. □

We now fix a series $g \in \mathcal{O}_K[\![t]\!]/(t^n)$ satisfying the assumptions of Lemma 14. We define W_n as the open subset of E_n consisting of series γ for which $g + \gamma \in \Omega_n$. We introduce the two following functions:

$$\begin{array}{rccl} \theta_n : & W_n & \longrightarrow & F_n \\ & \gamma & \mapsto & \varphi_n(g+\gamma) - \varphi_n(g), \end{array}$$

$$\begin{array}{rccl} \tau_n : & F_n \times W_n & \longrightarrow & \mathrm{Hom}(E_n, F_n) \\ & (\zeta\ ,\ \gamma) & \mapsto & \left(\delta g \mapsto \dfrac{z_g' + t(t-4a)\zeta' + 2(t-2a)\zeta}{g+\gamma} \cdot \psi_{+,n}(\delta g)\right) \end{array}$$

It follows from Proposition 13 that $d\theta_n = \tau_n \circ (\theta_n, \mathrm{Id})$, where Id is the identity map on W_n. We can associate to any (locally) analytic function f, the Legendre transform of the convex function associated to the epigraph of f, *i.e.* $\Lambda(f) : \mathbb{R} \cup \{\infty\} \longrightarrow \mathbb{R} \cup \{\infty\}$ defined by

$$\Lambda(f)(x) = \begin{cases} \log\left(\sup\limits_{\gamma \in B_{E_n}(e^x)} \|f(\gamma)\|\right) & \text{if } f \text{ is defined over } B_{E_n}(e^x)\,, \\ \infty & \text{elsewise}\,. \end{cases} \tag{16}$$

We define $\Lambda(f)_{\geq 2}(x) = \inf\limits_{y \geq 0} (\Lambda(f)(x+y) - 2\,y)$ too.

Lemma 15. *Suppose $x < -\log 4$, then $\Lambda(\theta_n)_{\geq 2}(x) < x$.*

Proof. For all $x > 0$, one easily checks that $\Lambda(\mathrm{Id})(x) = x$ and $\Lambda(\tau_n)(x) \geq 0$. Applying [CRV15, Proposition 2.5], we obtain $\Lambda(\theta)_{\geq 2}(x) \leq 2\,(x + \log 2)$ for $x \leq -\log 2$. Especially, $\Lambda(\theta_n)_{\geq 2}(x) < x$ for $x < -\log 4$. □

We can now state the following important result, that gives the best possible precision that one can expect for $\varphi_n(g)$ when g is itself only known up to some finite precision. In the next proposition, $B_{E_n}(\delta)$ (resp. $B_{F_n}(\delta)$) stands for the closed ball in E_n (resp. in F_n) of centre 0 and radius δ.

Proposition 16. *Under the assumption of Lemma 14, we have*

$$\varphi_n\big(g + B_{E_n}(\delta)\big) = \varphi_n(g) + B_{F_n}(\delta) \quad \textit{for all} \quad \delta < 1/4.$$

Proof. Applying [CRV14, Proposition 3.12] with the bound of Lemma 15, we obtain for $\delta < 1/4$

$$\varphi_n\big(g + B_{E_n}(\delta)\big) = \varphi_n(g) + d\varphi_n(g)\big(B_{E_n}(\delta)\big).$$

We conclude by applying Lemma 14. □

Remark 17. Using that φ_n is injective, we see that Proposition 16 implies that

$$\|\varphi_n(g+\gamma) - \varphi_n(g)\|_{F_n} = \|\gamma\|_{E_n}$$

as soon as g satisfies the assumption of Lemma 14 and $\|\gamma\|_{E_n} \leq 1/4$. More generally, applying this result with g replaced with $g + \delta$ with $\|\delta\|_{E_n} \leq 1/4$, we find that φ_n is an isometry in restriction to the ball of centre g and radius $1/4$.

Correctness proof of Theorem 10. Let U, V and n be the input of Algorithm 3. We first claim that the output of Algorithm 2 satisfies

$$W(t, q_n) \equiv u^2 \cdot z_n'^2 \pmod{t^{n-1}, 2^M}. \tag{17}$$

for all n. We shall prove it by induction on n. The case $n = 1$ is easy. Let $m \geq 1$ be a positif integer and $n = 2m - 1$. We suppose that Eq. (17) is true for m. We set $\lambda = ba^{-1}$. Since $z_m \equiv \lambda t + t(t-4a)q_m \pmod{t^n}$, we derive the following relation

$$V(z_m) \equiv t(t-4a) \cdot W(t, q_m) \pmod{t^n}. \tag{18}$$

Taking the logarithmic derivative of W with respect to x, we get

$$\begin{aligned}
\frac{\partial W}{\partial x}(t, q_m) &= W(t, q_m) \cdot \left(\frac{t-4a}{\lambda + (t-4a)q_m} + \frac{t}{\lambda + tq_m} + \frac{2t(t-4a)\, v'\big(\lambda t + t(t-4a)q_m\big)}{v\big(\lambda t + t(t-4a)q_m\big)} \right) \\
&= W(t, q_m) \cdot \left(\frac{t(t-4a)}{z_m} + \frac{t(t-4a)}{z_m - 4b} + \frac{2t(t-4a)\, v'(z_m)}{v(z_m)} \right).
\end{aligned}$$

Using now Eq. (18), we get

$$\frac{\partial W}{\partial x}(t, q_m) \equiv (z_m - 4b)\, v(z_m)^2 + z_m\, v(z_m)^2 + 2\, v(z_m)\, v'(z_m) \equiv V'(z_m) \pmod{t^{n-1}}.$$

In addition, we have $q_n \equiv q_m + z_m' u \cdot y_n \pmod{t^n, 2^M}$ by construction. By Remark 7 combined with the induction hypothesis, we know moreover the m first coefficients of y_n vanish, *i.e.* $y_n \equiv 0 \pmod{t^m, 2^M}$. We then deduce

$$\begin{aligned}
W(t, q_n) &\equiv W(t, q_m) + z_m' u\, y_n \cdot \frac{\partial W}{\partial x}(t, q_m) \pmod{t^{n-1}, 2^M} \\
&\equiv W(t, q_m) + z_m' u\, y_n \cdot V'(z_m) \pmod{t^{n-1}, 2^M}.
\end{aligned} \tag{19}$$

Besides, by definition of y_n, we have the relation

$$t(t-4a)y_n' + (t-2a)y_n \equiv \frac{1}{2u^3} \left(\frac{W(t, q_m)}{z_m'^{\,2}} - u^2 \right) \pmod{t^{n-1}, 2^M},$$

for what we derive

$$W(t, q_m) - u^2 z_m'^{\,2} \equiv 2u^3 z_m'^{\,2} \cdot \big(t(t-4a)y_n' + (t-2a)y_n\big) \pmod{t^{n-1}, 2^M}. \tag{20}$$

Similarly, using the congruence $z_n \equiv z_m + t(t-4a)z_m' u\, y_n \pmod{t^n, 2^M}$, we obtain

$$u^2\, z_n'^2 \equiv u^2\, z_m'^{\,2} + 2u^2\, z_m' \left(t(t-4a)z_m' u\, y_n\right)' \pmod{t^{n-1}, 2^M}. \tag{21}$$

Combining Eqs. (19), (20) and (21), we end up with

$$\begin{aligned}
&W(t, q_n) - u^2\, z_n'^2 \\
&\quad \equiv u\, y_n \cdot \big(V(z_m)\big)' + 2u^3\, z_m'^{\,2}\big(t(t-4a)\, y_n' + (t-2a)\, y_n\big) - 2u^2\, z_m' \cdot \big(t(t-4a)z_m' u\, y_n\big)', \\
&\quad \equiv u\, y_n \cdot \big(V(z_m) - t(t-4a)u^2\, z_m'^{\,2}\big)' \pmod{t^n, 2^M}.
\end{aligned}$$

Using Eq. (18), we finally conclude that Eq. (17) holds true for n; our claim in proved.

Multiplying Eq. (17) by g^2 on both sides, we get

$$g^2 \cdot W(t, q_n) \equiv z_n'^2 \pmod{t^{n-1}, 2^M}.$$

We now observe that

$$W(t, q_n) \equiv (\lambda + tq_n)^2 \cdot v(\lambda t + t^2 q_n)^2 \pmod{4}$$

showing that $W(t, q_n)$ is a square modulo 4. It thus admits a square root $w \in \mathcal{O}_K[\![t]\!]$, up to possibly replacing K by its unique unramified extension of degree 2 (see also Remarks 2 and 3). We define $g_n = z_n'/w$, so that we have $z_n = t(t-4a)\,\varphi_n(g_n)$ and $\|g^2 - g_n^2\|_{F_{n-1}} \leq 2^{-M}$. The last inequality indicates in particular that $g(0)^2 \equiv g_n(0)^2 \pmod{\pi^{eM}}$. We normalize g_n in such a way that $g(0) \equiv g_n(0) \pmod 4$ (this is always possible because $M \geq 3$). Then the series $g + g_n$ is divisible by 2 and its constant term has valuation 1. As a consequence, $g + g_n$ is invertible in $K[\![t]\!]$ and its Gauss norm is $1/2$. We deduce that

$$\|g - g_n\|_{F_{n-1}} = \|g^2 - g_n^2\|_{F_{n-1}} \cdot \|g + g_n\|_{F_{n-1}}^{-1} = 2 \cdot \|g^2 - g_n^2\|_{F_{n-1}} \leq 2^{-M+1}.$$

So $\|g - g_n\|_{E_{n-1}} \leq 2^{-N}$. Using Remark 17, we conclude that

$$\|z_g - z_n\|_{F_n} \leq \|\varphi_n(g) - \varphi_n(g_n)\|_{F_{n-1}} = \|g - g_n\|_{E_{n-1}} \leq 2^{-N}.$$

We finally justify that all computations stay within $\mathcal{O}_K$, so that no error is raised during the execution of `IsoSolve`. Examining the successive operations performed by the algorithm, we see that nonintegral coefficients may show up only during the computation of f_n (because of the division by 2) and that of y_n (because of the call to `LinDiffSolve`). After Proposition 6, we are reduced to check that f_n and y_n have integral coefficients modulo t^n. By construction, they are related by the relation

$$t(t-4a)y_n' + 2(t-2a)y_n \equiv f_n \pmod{t^n}$$

so the integrality of y_n will directly imply that of f_n. By construction, $z_n \equiv z_m + z_m' u y_n \pmod{t^n}$. Besides, we know that z_m and z_n have integral coefficients. We deduce that y_n has integral coefficients as well, given that z_n' and u are invertible in $\mathcal{O}_K[\![t]\!]$. □

2.6. **Experiments.** We made an implementation of both Algorithm 1 and the HALF-GCD variant given in [Tho03] with the MAGMA computer algebra system [BCP97]. Our implementation is available at [CEL19]; it is fairly optimized and can compute isogenies up to degree 10^6 in less than one minute (see precise timings on Figure 1, page 16). The degree 11 toy example presented below was computed with this software as well.

2.6.1. *A toy example.* We consider the elliptic curve given by $E/\mathbb{F}_2 : y^2 + x\,y = x^3 + 1$. The abstract structure of its ring of endomorphism is the ring of integer of $\mathbb{Q}_2(\sqrt{-7})$, the class group of which is trivial. Especially, there exists an isogeny of degree 11, which turns out to be an endomorphism of E. Let us compute it.

We first lift E over $\mathbb{Q}_2$ as $\mathcal{E}/\mathbb{Q}_2 : y^2 = x^3 + 2^{-2}\,x^2 + 1 + O(2^9)$. Using computations in $\mathbb{Q}(\sqrt{-7})$ (as detailed in Section 3.1), we find that $\mathcal{E}/\mathbb{Q}_2$ is 11-isogenous to the curve $\mathcal{E}'/\mathbb{Q}_2 : y^2 = x^3 + 2^{-2}\,x^2 + 225 + O(2^9)$, the "differential constant" of the isogeny being equal to $41 + O(2^9)$. A simple Newton iteration leads to $4a = -16 + O(2^9)$ and $u^2 = 65 - 16t + 4t^2 + O(2^9)$. Extracting the inverse square root, we obtain

$$\frac{1}{u} = 225 - 248\,t - 226\,t^2 + 208\,t^3 - 122\,t^4 + 240\,t^5 + 172\,t^6 + 160\,t^7 - 250\,t^8 - 80\,t^9 - 60\,t^{10} + 96\,t^{11} + O\big(2^9, t^{12}\big),$$

from which it is easy to compute u and u^{-3}. All precomputations of Algorithm 2 are now finished and we can start the first step of the main Newton iteration. We begin with $q_0 = 10 + O\big(2^9, t\big)$ and find

$$z_0 = 41\,t + 10\,t^2 + O(2^9, t^3)\,, \qquad s_0 = 164\,t + O(2^9, t^2)\,, \qquad r_0 = 113 + 152\,t + O(2^9, t^2)\,,$$
$$f_0 = 228\,t + O(2^9, t^2)\,, \qquad y_0 = -211\,t + O(2^9, t^2)\,, \qquad q_1 = 10 - 43\,t + O(2^9, t^2)\,.$$

Three intermediary steps follow similarly, allowing to increase t-adic precision from $O(t^2)$ to $O(t^3)$, to $O(t^6)$ and then to $O(t^{12})$. After these computations, we are left with

$$q_{11} = 10-43\,t+140\,t^2-6\,t^3+182\,t^4-89\,t^5+228\,t^6+246\,t^7+248\,t^8+76\,t^9+20\,t^{10}+206\,t^{11}+O\big(2^9,t^{12}\big)$$

and a last iteration finally yields

$$\begin{aligned}
z_{11} &= 41\,t + 94\,t^2 + 5\,t^3 + 116\,t^4 + 210\,t^5 + 82\,t^6 - 201\,t^7 + 188\,t^8 + \\
&\qquad 214\,t^9 + 40\,t^{10} + 156\,t^{11} - 180\,t^{12} + O(2^9, t^{13})\,, \\
s_{11} &= 200\,t + 48\,t^2 - 4\,t^3 - 32\,t^4 + 224\,t^5 - 128\,t^6 + 32\,t^7 + 160\,t^8 + \\
&\qquad 96\,t^9 - 192\,t^{10} + 96\,t^{11} - 128\,t^{12} + O(2^9, t^{13})\,, \\
r_{11} &= 113 + 200\,t - 222\,t^2 - 136\,t^3 + 175\,t^4 - 56\,t^5 - 10\,t^6 + 48\,t^7 - 137\,t^8 + \\
&\qquad 168\,t^9 + 226\,t^{10} - 240\,t^{11} + 238\,t^{12} + O(2^9, t^{13})\,, \\
f_{11} &= -184\,t + 48\,t^2 - 100\,t^3 - 32\,t^4 + 184\,t^5 + 16\,t^6 - 4\,t^7 - 192\,t^8 - \\
&\qquad 24\,t^9 + 16\,t^{10} + 180\,t^{11} + 256\,t^{12} + O(2^9, t^{13})\,, \\
y_{11} &= 94\,t^{12} + 131\,t^{13} - 172\,t^{14} - 82\,t^{15} + 34\,t^{16} - 215\,t^{17} + 80\,t^{18} - 120\,t^{19} + \\
&\qquad 70\,t^{20} - 233\,t^{21} + 110\,t^{22} + 161\,t^{23} + O(2^9, t^{24})\,,
\end{aligned}$$

then

$$\begin{aligned}
q_{23} = {} & 10-43\,t+140\,t^2-6\,t^3+182\,t^4-89\,t^5+228\,t^6+246\,t^7+248\,t^8+76\,t^9+20\,t^{10}+206\,t^{11}+206\,t^{12}+243\,t^{13} \\
& -210\,t^{14}-143\,t^{15}-206\,t^{16}+145\,t^{17}+244\,t^{18}-218\,t^{19}+10\,t^{20}+137\,t^{21}-166\,t^{22}+147\,t^{23}+O(2^9,t^{24})\,,
\end{aligned}$$

and

$$\begin{aligned}
z_{24} = {} & 41\,t+94\,t^2+5\,t^3+116\,t^4+210\,t^5+82\,t^6-201\,t^7+188\,t^8+214\,t^9+40\,t^{10}+156\,t^{11}-180\,t^{12}+6\,t^{13} \\
& -102\,t^{14}-85\,t^{15}-14\,t^{16}+57\,t^{17}+118\,t^{18}+97\,t^{19}-116\,t^{20}-178\,t^{21}-210\,t^{22}-15\,t^{23}+166\,t^{24}+O(2^9,t^{25})\,.
\end{aligned}$$

A call to the HALF-GCD algorithm with input $\sqrt{z_{24}\,/\,t} \mod 2$, which is $1 + t + t^3 + t^7 + t^8 + t^9 + t^{11} + O(t^{12})$, allows us to recover the rational function

$$\frac{t^5 + t^3 + t^2 + t + 1}{t^5 + t^4 + t^3 + t^2 + 1} + O(t^{12})\,,$$

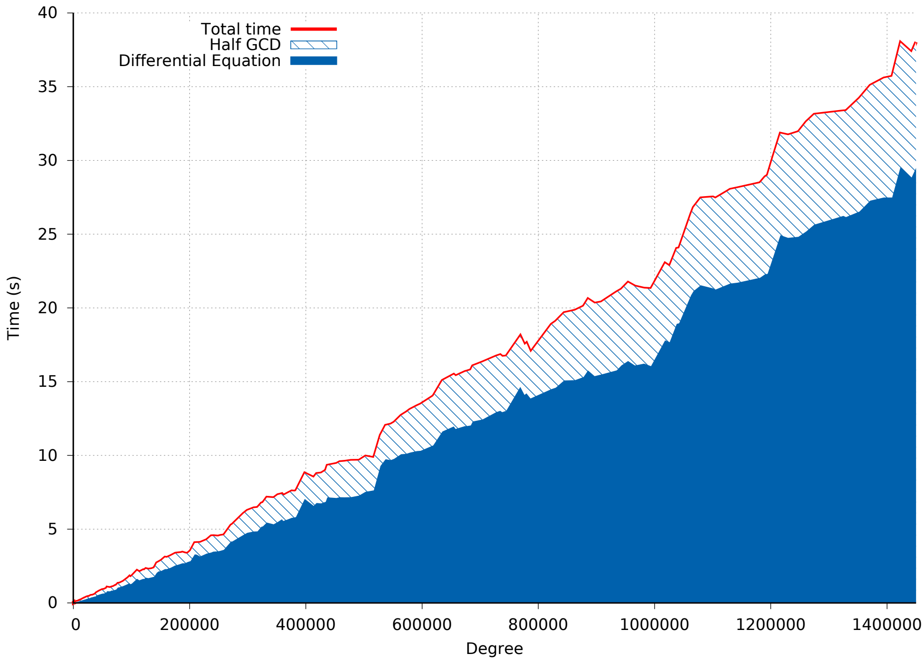
from which one deduces that the curve $E/\mathbb{F}_2$ is self 11-isogenous under the mapping

$$x \mapsto \frac{x\,(x^5 + x^3 + x^2 + x + 1)^2}{(x^5 + x^4 + x^3 + x^2 + 1)^2}\,.$$

2.6.2. *Some timings.* We made use of our MAGMA software to measure the time needed to compute isogenies up to degree 1 500 000 for an elliptic curve defined over $\mathbb{F}_2$. Results are reported on Figure 1. Since multiplying 2-adic series can be done in almost linear times with MAGMA, the time complexity of our implementation is almost linear as well: the observed timings fit rather well with the awaited time complexity, which is $O(\ell \log^2 \ell)$. The timings for HALF-GCD are significantly smaller (by a factor close to 3) because of two facts: first, the degree of the inputs is 2 times smaller than in Algorithm 1 and, second, the underlying polynomial arithmetic over $\mathbb{F}_2$ is slightly more efficient than the arithmetic with 2-adic series in MAGMA.

3. Applications

Thanks to the results of [BMSS08, LS08, LV16] in odd characteristic and the case of characteristic 2 being solved in Section 2, we now have in all characteristic fast algorithms for computing isogenies, at least if we have a Weierstrass model of the isogenous curve and the isogeny differential. In this section, we are interested in the calculation of irreducible polynomials. We



Timings obtained with MAGMA v2.24-10 on a laptop with an INTEL processor I7-8850H@2.60GHZ

FIGURE 1. Isogeny computations in $\mathbb{F}_2$.

show how we can extend to the case of very small finite fields, especially $\mathbb{F}_2$, the construction of [CL13]. With this aim, we show in Section 3.1 how to calculate the isogenous curves and the isogeny differentials over finite fields of small characteristic. Then, in Section 3.2, we apply this construction to build irreducible polynomial and we end with an example in Section 3.3.

Let $q = p^n$ be a power of a prime number p. From now, we fix from an unramified extension K of $\mathbb{Q}_p$ of degree n, and let $k = \mathbb{F}_q$ be its residual field (even if we heavily have in mind the case $p = 2$).

3.1. **Isogenies of large degree.** Let E be an elliptic curve with complex multiplication defined in full generality over a field and $\ell > 2$ a large prime integer. Note that in practice, the field of definition of E is very small so that in this case, up to an endomorphism, an ℓ-isogeny can be written as a composition of small isogenies. This can be done by working in the ideal class group of the endomorphism ring of E. In fact, the situation is very similar to that behind the algorithm given by Kohel in his thesis for computing the endomorphism ring of an elliptic curve.

Theorem 18 ([Koh96, Th. 1])**.** *There exists a deterministic algorithm that, given an elliptic curve E over a finite field k of q elements, computes the isomorphism type of the endomorphism ring of E and if a certain generalization of the Riemann hypothesis holds true, for any $\varepsilon > 0$ runs in time $O(q^{1/3+\varepsilon})$.*

In our case of interest, the field of definition of the curves is rather small while the degrees of the isogenies are rather large. So, we can suppose that we are given the abstract structure $\mathcal{O}_\kappa$ of the endomorphism ring $\mathrm{End}(E)$ of E as an order in an imaginary quadratic field $\kappa = \mathbb{Q}(\sqrt{-\Delta})$, Δ a primitive discriminant. For the sake of simplicity, we assume that this order is maximal, *i.e.* equal to the ring of integers $\mathbb{Z}[\omega]$ of κ.

In this context, a prime integer $\ell \neq p$ that splits in κ is usually called an Elkies prime for E. We more generally define *Elkies degrees* for E as integers whose prime divisors are all Elkies primes for E. This said, the computation of the isogenous curve $\tilde{E}$ reduces to calculations in the ideal class group of $\mathcal{O}_\kappa$.

Theorem 19. *Giving an ordinary elliptic curve E defined over $\mathbb{F}_q$ such that $\mathcal{O}_\kappa$ is maximal and ℓ an Elkies degree for E, there exists an algorithm that computes an equation of an ℓ-isogenous curve $\tilde{E}$ of E and the isogeny with time complexity* $O(M_{\mathcal{O}_K}(p^{\lceil \log_p(\ell) \rceil}, \ell) \log_p(\ell) + p^2 \log_p^2(\ell) + q^{3/2})$ *.*

Under reasonable heuristic assumptions detailed in [BS11], the $q^{3/2}$ term can be replaced by $L\left[1/2, \sqrt{3}/2\right](q)$ where L denotes the usual subexponential functions

$$L\left[\alpha, c\right](x) = \exp(\,(c + o(1))\;(\log x)^{\alpha}\;(\log\log x)^{1-\alpha}\,)\,.$$

Proof. Let m be a prime divisor of ℓ. Let $\mathcal{I}(\mathcal{O}_\kappa)$ be the group of fractional ideals of $\mathcal{O}_\kappa$ and $\mathcal{P}(\mathcal{O}_\kappa)$ its subgroup of principal ideals. Let $\mathrm{Cl}(\mathcal{O}_\kappa) = \mathcal{I}(\mathcal{O}_\kappa)/\mathcal{P}(\mathcal{O}_\kappa)$ be the ideal class group associated to $\mathcal{O}_\kappa$. We have $|\mathrm{Cl}(\mathcal{O}_\kappa)| = O(\sqrt{|\Delta|})$. In addition, every ideal class in $\mathrm{Cl}(\mathcal{O}_\kappa)$ contains an ideal of norm less than $\sqrt{|\Delta|}$. So, $\mathrm{Cl}(\mathcal{O}_\kappa)$ is generated by classes of ideals of norm less than $\sqrt{|\Delta|}$. We can associate an ideal $\mathfrak{m} = (m, a_{\mathfrak{m}} + b_{\mathfrak{m}}\,\omega)$ in $\mathcal{O}_\kappa$ that divides (m), and write $\mathfrak{e}_1\,\mathfrak{m} = \mathfrak{e}_2\,\prod_{i=1}^{h}\mathfrak{p}_i^{e_i}$, where $\mathrm{Norm}(\mathfrak{p}_i) \leq \sqrt{\Delta}$ and $\mathfrak{e}_1$ and $\mathfrak{e}_2$ are two principal ideals. Each prime ideal $\mathfrak{p}_i$ determines an isogeny, which in turn yields the following chain of small degree isogenies,

$$\begin{aligned} E \longrightarrow E \Big/ E[\mathfrak{p}_1] \longrightarrow E \Big/ E[\mathfrak{p}_1^2] \longrightarrow \ldots \longrightarrow E \Big/ E[\mathfrak{p}_1^{e_1}] \longrightarrow \\ E \Big/ E[\mathfrak{p}_1^{e_1}\mathfrak{p}_2] \longrightarrow E \Big/ E[\mathfrak{p}_1^{e_1}\mathfrak{p}_2^2] \longrightarrow \ldots \longrightarrow E \Big/ E[\mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}] \longrightarrow \\ \ldots \\ E \Big/ E[\mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_{h-1}^{e_{h-1}}\mathfrak{p}_h] \longrightarrow \cdots \longrightarrow E \Big/ E[\mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_h^{e_h}]\,. \end{aligned} \tag{22}$$

We arrive in this way at $\tilde{E} = E\,/\,E[\mathfrak{p}_1^{e_1}\,\mathfrak{p}_2^{e_2}\,\cdots\,\mathfrak{p}_h^{e_h}]$.

Results by Serre and Tate [LJPT64] enable to lift canonically E as $\mathcal{E}/\mathbb{Q}_q$. An algorithm for computing canonical lifts at p-adic precision λ in time complexity $O(p^2\,\lambda^2)$ up to some polylogarithmic factors can be for instance found in [Sat00, SST03]. According to Theorem 1 and [LV16, Theorem 2], the lifting process has to be done with p-adic precision equal to $O(\lceil \log_p(\ell) \rceil)$. Since in this situation the principal ideal (q) splits in $\mathcal{O}_\kappa$ into two prime ideals, one chooses arbitrarily the residual field given by one of the two, which allows us to embed integers from O_κ into K, $\omega \mapsto \sqrt{-\Delta}$.

Now, starting from $\mathcal{E}$ in Chain (22), the SEA machinery (or Vélu's formulas if m is very small, *e.g.* 2) enables to associate to each $\mathfrak{p}_i$ a normalized isogenous curve. This yields a $\prod_{i=1}^{h}\mathfrak{p}_i^{e_i}$-isogenous curve $\tilde{\mathcal{E}}$. Furthermore, the curve $\tilde{\mathcal{E}}$ is also m-isogenous to $\mathcal{E}$ up to the endomorphism $\mathfrak{e}_2\mathfrak{e}_1^{-1}$. The differential of this m-isogeny is thus equal to the embedding of $\mathfrak{e}_2\,\mathfrak{e}_1^{-1}$ in K.

We now iterate this construction for every remaining prime divisor m of ℓ, counting multiplicity, and go from one isogenous curve to the next. We arrive in this way to a ℓ-isogenous curve, and its differential. It remains to call Algorithm 2 to find the solution $z(t)$ of Eq. (7) modulo $t^{2\ell+2}$. Reducing $z(t)$ modulo p and calling the HALF-GCD algorithm, we can recover the isogeny. ∎

Remark 20. It is faster to compute the composition of two isogenies with Algorithm 2 than to compute each isogeny independently and then perform their compositions.

Remark 21. In some cases, the isogeny differential c is rational and the lifting does not need to be canonical. For example if ℓ is an integer coprime to p, then the multiplication map $[\ell] : E \longrightarrow E$ is a separable isogeny that can be computed by lifting arbitrarily the equation of the curve E and taking $c = 1/\ell$ in $\mathbb{Q}_q$.

3.2. **Irreducible polynomials over finite fields.** While the algorithm of [CL13] achieves a notable quasi-linear complexity in the degree for computing irreducible polynomials over a finite field, it is difficult to reach this complexity in practice for degrees d that require the use of Kedlaya-Umans algorithm [KU11], typically when d is not a prime or when d is larger than $q+1-2\sqrt{q}$. Under some weak conditions that we make precise in this section, we show that we can avoid this downside for much more degrees, at least when q is small. Especially, it includes the important case $k = \mathbb{F}_2$.

Let ℓ be an odd Elkies degree for an elliptic curve E/k. With the notations of Section 3.1, we denote by σ_q the image of the Frobenius endomorphism ϕ_q in $\mathcal{O}_\kappa$. In this setting, let $\mathfrak{l}$ be an ideal in $\mathcal{O}_\kappa$ above ℓ and containing $\sigma_q - \lambda$ where $\lambda \in \mathbb{Z}/\ell\mathbb{Z}$ is a root of $X^2 - \mathrm{Tr}(E)\,X + q \bmod \ell$.

The first coordinate of the image of a point (x, y) by the isogeny I returned by the algorithm of Theorem 19 is given by $\varphi(x)/\psi^2(x)$. The polynomial $\psi(x)$ is of degree $(\ell-1)/2$.

Take for B the point at infinity of the isogenous curves in the construction of [CL13], we are led to consider the polynomial $\nu_O(x) = \psi(x)$, whose roots are the abcissas of points in $\ker(I)$. Now, the factorizations $I = I_m \circ I_{\ell/m}$, where I_m are isogenies of degree m with m any divisor of ℓ, yield $\ker(I_m) \subset \ker(I)$. Consequently, the polynomial $\psi(x)$ splits as

$$\psi(x) = \prod_{m\,|\,\ell} \Psi_m(x)\,,$$

with $\deg \Psi_m(x) = \varphi(m)/2$, the Euler's totient function of m. Computing I_m for $m \neq \ell$ by the same procedure as I, we can obtain $\Psi_m(x)$. Dividing $\psi(x)$ by all of them, we are led to consider the polynomial $\Psi_\ell(x)$, of degree $\varphi(\ell)/2$. Its irreducibility depends on the order of λ in the multiplicative group $(\mathbb{Z}/\ell\mathbb{Z})^\times$ (see [CL13, Section 4.2]). In general, $\Psi_m(x)$ splits in factors of degree $d = \mathrm{ord}_{\mathbb{Z}/\ell\mathbb{Z}}(\lambda)/2$ or $d = \mathrm{ord}_{\mathbb{Z}/\ell\mathbb{Z}}(\lambda)$ following that a power of λ is equal to -1 or not. The polynomial $\Psi_m(x)$ is thus irreducible when $d = \varphi(\ell)/2$. Since ℓ is odd, it implies that ℓ is either of the form $p_1^{e_1}$ or of the form $p_1^{e_1}\,p_2^{e_2}$, where p_1 and p_2 are odd prime integers.

For the same reasons, take for A any non-zero point of $E(k)$ and let $B = I(A)$, then the polynomial

$$\nu_A(x) = (\,\phi(x) - x(B)\,\psi^2(x)\,)\,/\,(\,x - x(A)\,)\,,$$

of degree $\ell - 1$, splits in factors $\Phi_m(x)$ of degree $\varphi(m)$ where $m \neq 1$ divides ℓ. In turn, $\Phi_\ell(x)$ splits in factors of degree $\mathrm{ord}_{\mathbb{Z}/\ell\mathbb{Z}}(\lambda)$. When $\mathrm{ord}_{\mathbb{Z}/\ell\mathbb{Z}}(\lambda) = \varphi(\ell)$, which implies that ℓ is a prime since ℓ is odd, $\Phi_\ell(x)$ is thus an irreducible polynomial of degree $\varphi(\ell)$.

The main part of this construction is thus to determine the isogenous curve $\tilde{E}$ and the equations of the isogeny I following Theorem 19. Therefore, we can state this theorem.

Theorem 22. *Giving an ordinary elliptic curve E defined over $\mathbb{F}_q$ and ℓ an odd Elkies degree for E such that one of the root λ of the Weil polynomial modulo ℓ has order $\varphi(\ell)$ in $(\mathbb{Z}/\ell\mathbb{Z})^\times$, there* *exists an algorithm that computes two irreducible polynomials in* $\mathbb{F}_q$ *of degree* $\varphi(\ell)$ *and* $\varphi(\ell)/2$ *with time complexity* $O(M_{\mathcal{O}_K}(p^{\lceil \log_p(\ell) \rceil}, \ell) \log_p(\ell) + p^2 \log_p^2(\ell) + q^{3/2})$.

With same complexity, this algorithm computes an irreducible polynomial of degree $\varphi(\ell)/2$ *when* $\mathrm{ord}_{\mathbb{Z}/\ell\mathbb{Z}}(\lambda) = \varphi(\ell)/2$ *and* $-1 \notin \langle \lambda \rangle$ *.*

Remark 23. Applied to the elliptic curve $E\,/\,\mathbb{F}_2 : y^2 + x\,y = x^3 + 1$, whose Weil polynomial is $X^2 + X + 2$, this method gives an infinite list of irreducible polynomials, of degrees,

$$2,\ 4,\ 5,\ 6,\ 10,\ 11,\ 12,\ 14,\ 16,\ 18,\ 20,\ 22,\ 28,\ 30,\ 33,\ 35,\ 36,\ 39,\ 40,\ 42,\ 46,\\ 52,\ 53,\ 54,\ 55,\ 58,\ 60,\ 63,\ 66,\ 68,\ 70,\ 72,\ 75,\ 78,\ 81,\ 82,\ 88,\ 89,\ 96,\ 100,\ \ldots$$

Remark 24. Theorem 19 and Theorem 22 can be extented to supersingular elliptic curves (note that canonical lifts can also be computed for supersingular elliptic curves, see for instance [CH02]).

3.3. **An example.** We consider the finite field $\mathbb{F}_{16} = \mathbb{F}_2(v)$ such that $v^4 + v + 1 = 0$. Let E be the elliptic curve defined by $E/\mathbb{F}_{16}\ : y^2 + xy = x^3 + v^6$. Choose $\ell = 73$, the Weil polynomial of E satisfies

$$X^2 + 3X + 16 \equiv (X - 10)\,(X - 60) \mod \ell\,.$$

The endomorphism ring of E is isomorphic to the ring of integers $\mathcal{O}$ of the quadratic field $\mathbb{Q}(\sqrt{-55})$. The class group $\mathrm{Cl}(\mathcal{O})$ is cyclic of order 4. Let $\mathfrak{l}$ be the ideal of $\mathcal{O}$ generated by 73 and $\phi_{16} - 60$. The set $E[\mathfrak{l}]$ is a cyclic subgroup of E of order 73, closed under the action of the Frobenius endomorphism. Let $I\ : E \longrightarrow E/E[\mathfrak{l}]$ be the degree 73 isogeny with kernel $E[\mathfrak{l}]$. We give the first coordinate of I as the rational fraction $\phi(x)/\psi(x)^2$. Note that ψ is a degree 36 irreducible polynomial since 60 is a generator of the multiplicative group $\mathbb{F}_{73}^{\times}$.

Let us compute $\psi(x)$. The ideal $\mathfrak{l}$ can be decomposed as $\mathfrak{p}\,\mathfrak{l} = \mathfrak{c}_2$, where $\mathfrak{p} = (2, (\sqrt{-55}+1)/2)$ and $\mathfrak{c}_2 = (-\sqrt{-55} + 23)/2$. We begin by lifting E in the 2-adics such that $\mathrm{End}(E) = \mathrm{End}(\mathcal{E})$ as

$$\mathcal{E} : y^2 + xy = x^3 + 21\,v^3 + 261\,v^2 + 316\,v + 256 + O(2^{10})\,.$$

In order to compute an equation of $\tilde{\mathcal{E}}$ and the differential isogeny, we first construct the degree 2 isogeny $\mathcal{E}\,/\,\mathcal{E}[\mathfrak{p}] \cong \tilde{\mathcal{E}} \longrightarrow \mathcal{E}$, we deduce

$$\mathcal{E}\,/\,\mathcal{E}[\mathfrak{p}] : y^2 = x^3 - (27 + O(2^{10}))x + 2(-224\,v^3 + 96\,v^2 - 160, v + 315) + O(2^{11}).$$

In return, a 73-isogenous curve $\tilde{E}$ to E is given by

$$\tilde{E}\ : y^2 + xy = x^3 + v^{12}$$

and the isogeny differential is

$$c = 244v^3 + 164v^2 - 424v - 299 + O(2^{10})\,.$$

Applying Algorithm 2 with $U(t) = 4(21v^3 + 261v^2 + 316v + 256 + O(2^{10}))\,t^4 + t + 4$ and $V(t) = 4(v^3 + 123v^2 + 243v + 369 + O(2^{10})))\,t^4 + t + 4$ and c, and reducing modulo 2 we get the series $z(t)$. A final call to the HALF-GCD algorithm yields the irreducible polynomial

$$\psi(x) = \overline{\mathtt{F}} + \overline{\mathtt{E}}\,x + \overline{\mathtt{7}}\,x^2 + \overline{\mathtt{B}}\,x^3 + \overline{\mathtt{7}}\,x^4 + \overline{\mathtt{B}}\,x^5 + \overline{\mathtt{E}}\,x^6 + \overline{\mathtt{7}}\,x^7 + \overline{\mathtt{2}}\,x^9 + \overline{\mathtt{B}}\,x^{10} + \overline{\mathtt{7}}\,x^{13}\\ + \overline{\mathtt{9}}\,x^{14} + \overline{\mathtt{E}}\,x^{15} + \overline{\mathtt{7}}\,x^{16} + \overline{\mathtt{F}}\,x^{17} + \overline{\mathtt{6}}\,x^{18} + \overline{\mathtt{5}}\,x^{19} + \overline{\mathtt{D}}\,x^{20} + \overline{\mathtt{6}}\,x^{21} + \overline{\mathtt{1}}\,x^{22} + \overline{\mathtt{C}}\,x^{23} + \overline{\mathtt{7}}\,x^{24}\\ + \overline{\mathtt{B}}\,x^{26} + \overline{\mathtt{2}}\,x^{27} + \overline{\mathtt{3}}\,x^{28} + \overline{\mathtt{2}}\,x^{29} + \overline{\mathtt{5}}\,x^{30} + \overline{\mathtt{A}}\,x^{31} + \overline{\mathtt{C}}\,x^{32} + \overline{\mathtt{7}}\,x^{33} + \overline{\mathtt{9}}\,x^{34} + \overline{\mathtt{D}}\,x^{35} + \ x^{36},$$

where for brevity's sake, we represent elements of $\mathbb{F}_{16}$ by integers written in hexadecimal. In other words, we replace the element v by the integer 2, for instance $\overline{\mathtt{5}} = v^2 + 1$ and $\overline{\mathtt{C}} = v^3 + v^2$.

Appendix A. More on our differential equations

In the previous sections, motivated by the explicit computation of isogenies in characteristic 2, we introduced and studied the following nonlinear 2-adic differential equation:

$$U \cdot z'^2 = V(z) \tag{23}$$

where U and V are two series in $K[\![t]\!]$ with t-adic valuation 1. Most of our attention was actually focused on the particular case where the hypothesis (H_U) is satisfied, in which case Eq. (23) can be rewritten as follows:

$$t(t-4a) \cdot z'^2 = g^2 \cdot h(z). \tag{24}$$

Here a is a given element in $\mathbb{Z}_2^\times$ (or more generally $\mathcal{O}_K^\times$ where K is a finite extension of $\mathbb{Q}_2$), g and h are given analytic functions and the unknown is z. In this appendix, we aim at revisiting our results and extracting from them theoretical informations about the structure of the solutions of Eqs. (23) and (24).

A.1. **Some spaces of analytic functions.** As before, we fix a finite extension K of $\mathbb{Q}_2$ and denote by $|\cdot|$ the norm on it, normalized by $|2| = 1/2$. We set $\mathcal{V} = K[\![t]\!]$; it is the space of germs of analytic functions around 0. Given a positive real number r, we let $\mathcal{V}_r$ be the subset of $\mathcal{V}$ defined by

$$\mathcal{V}_r = \Big\{ \sum_{n=0}^{\infty} a_n t^n \quad \text{such that } |a_n|\, r^n \text{ is bounded} \Big\}.$$

Series in $\mathcal{V}_r$ converge when $|t| < r$ and thus define analytic functions in the open disc of centre 0 and radius r, denoted by $B(r)$ in what follows. Thanks to ultrametricity, these functions are moreover all bounded on $B(r)$. We equip $\mathcal{V}_r$ with the Gauss norm $\|\cdot\|_r$ defined by

$$\|f\|_r = \sup_{n\geq 0} |a_n|\, r^n \quad \text{where } f = \sum_{n=0}^{\infty} a_n t^n.$$

One can check that $\mathcal{V}_r$ is complete with respect to $\|\cdot\|_r$. Besides, it is obvious that, when $r \leq s$, we have $\mathcal{V}_s \subset \mathcal{V}_r$ and $\|f\|_r \leq \|f\|_s$ for all $f \in \mathcal{V}_s$. It is finally easy to check that the Gauss norm is compatible with multiplication in the following sense: for all positive real number r and all functions $f, g \in \mathcal{V}_r$, we have $\|fg\|_r \leq \|f\|_r \cdot \|g\|_r$.

The operator ψ_+. In Section 2.3, we have introduced a linear automorphism ψ_+ of $K[\![t]\!]$ which takes a function $f \in K[\![t]\!]$ to the unique solution of the following linear differential equation:

$$t(t-4a)y' + (t-2a)y = f.$$

For all positive real number r, we set $\mathcal{V}_{r,+} = \psi_+^{-1}(\mathcal{V}_r)$ and equip this space with the norm $\|\cdot\|_{r,+}$ defined by $\|f\|_{r,+} = \|\psi_+(f)\|_r$. Clearly ψ_+ induces a bijective isometry $\psi_+ : \mathcal{V}_{r,+} \to \mathcal{V}_r$. Besides, the equality $t(t-4a)\, \psi_+(f)' + (t-2a)\, \psi_+(f) = f$ ensures that $\mathcal{V}_{r,+} \subset \mathcal{V}_r$ and

$$\|f\|_r \leq \max\left(\tfrac{1}{2}, r\right) \cdot \|\psi_+(f)\|_r = \max\left(\tfrac{1}{2}, r\right) \cdot \|f\|_{r,+}$$

for all $r > 0$ and all $f \in \mathcal{V}_{r,+}$. The estimates of Proposition 4 allow us to derive inequalities in the other direction.

Proposition 25. *Let r and s be two real numbers such that $0 < r < s \leq 1$. Then $\mathcal{V}_s \subset \mathcal{V}_{r,+}$ and, for all $f \in \mathcal{V}_s$, we have the estimation*

$$\|f\|_{r,+} \leq \max\left(2,\ \frac{2}{\log(s/r)}\right) \cdot \|f\|_s.$$

Proof. We write $f = \sum_{i=0}^{\infty} f_i t^i$ and $\psi_+(f) = \sum_{i=0}^{\infty} y_i t^i$. From Proposition 4, we deduce that

$$|y_i| \leq 2 \cdot (i+1) \cdot \sup_{0 \leq k \leq i} |f_k|.$$

Multiplying by r^i on each side and noticing that $|f_k|\, r^i \leq \left(\frac{r}{s}\right)^i \|f\|_s$ for all $k \leq i$, we derive $|y_i|\, r^i \leq 2{\cdot}(i+1){\cdot}\left(\frac{r}{s}\right)^i \|f\|_s$. By calculus, we prove that, for any $a \in]0,1[$, the maximum of the function $x \mapsto (x{+}1)\, a^x$ is reached for $x_0 = \max(0, -1 - 1/\log a)$ and is equal to 1 if $a \leq e^{-1}$ and to $-1/(ea \log a)$ otherwise. (Here $e \approx 2.718...$ denotes the natural base of logarithms.) We deduce from this that the function $x \mapsto (x{+}1)\, a^x$ is bounded from above by $\max(1, -1/\log a)$ on the interval $]0, +\infty[$. The proposition follows, noticing that $\|f\|_{r,+} = \|\psi_+(f)\|_r = \sup_{i \geq 0} |y_i| r^i$ by definition. □

A.2. **Generic radius of convergence.** We now come back to the nonlinear differential equations (23) and (24); we are interested in the radius of convergence of their solutions. We recall that the radius of convergence of a function $f \in K[\![t]\!]$ is defined as the supremum of the non-negative real numbers r for which $f \in \mathcal{V}_r$. In the sequel, we will denote it by $\mathrm{RoC}(f)$ for short. If $f = \sum_{n=0}^{\infty} a_n t^n$, we have the classical explicit formula

$$\mathrm{RoC}(f) = \liminf_{n \to \infty}\ |a_n|^{-1/n}.$$

A general theorem indicates that the radii of convergence of the solutions of Eq. (23) are strictly positive as soon as U and V have positive radii of convergence as well. The next proposition makes this result effective in our setting.

Proposition 26. *Let $U, V \in K[\![t]\!]$ with t-adic valuation 1. We assume that $U \in \mathcal{V}_r$ and $V \in \mathcal{V}_s$ for some positive real numbers r and s. Let z be the unique solution of Eq. (23) in $tK[\![t]\!]$ (*cf *Proposition 1). Then,*

$$\mathrm{RoC}(z) \geq \min\left(\frac{rs^2 \cdot |U'(0)|^2}{\|U\|_r {\cdot} \|V\|_s},\ \frac{r^2 \cdot |U'(0)|}{\|U\|_r}\right).$$

Proof. Performing the change of function $z(t) = y(\lambda t)$ for a well chosen λ in a suitable extension of K, we may assume without loss of generality that $s = 1$. Up the rescaling U and V by the same constant, we may further suppose that $\|V\|_1 = 1$. We write

$$U = \sum_{i=1}^{\infty} u_i t^i, \quad V = \sum_{i=1}^{\infty} v_i t^i, \quad z = \sum_{i=1}^{\infty} z_i t^i$$

with $u_i, v_i, z_i \in K$. Observe that $U'(0) = u_1$. Moreover, by definition of the Gauss norm, we know that $|u_i| \leq \|U\|_r\, r^{-i}$ and $|v_i| \leq 1$ for all i. We set

$$\rho = \min\left(\frac{r {\cdot} |u_1|^2}{\|U\|_r},\ \frac{r^2 {\cdot} |u_1|}{\|U\|_r}\right) \quad \text{and} \quad C = \frac{\rho^2 {\cdot} |v_1|}{|u_1|^2}.$$

We are going to prove by induction that $|z_n| \leq C \cdot \rho^{-n}$ for all $n \geq 2$. This will directly imply the proposition.

We consider an integer $n \geq 2$. From Eq. (8) (obtained in the proof of Proposition 1), we derive $|z_n| \leq |v_1|^{-1} \cdot \max(A, B)$ with

$$A = \max_I \left(|z_1|^{k_1} \cdots |z_{n-1}|^{k_{n-1}}\right)$$
$$B = \|u\|_r \cdot \max_J \left(|z_{j+1}| \cdot |z_{i-j+1}| \cdot r^{i-n}\right)$$

where I is the set of all tuples of nonnegative integers $(k_1, \ldots, k_{n-1})$ such that $k_1 + 2k_2 + \cdots + (n-1)k_{n-1} = n$ and J is the set of pairs $(i, j) \in \mathbb{Z}^2$ with $0 \leq j \leq i < n$ and $0 < j < n-1$ if $i = n-1$. Let $(k_1, \ldots, k_{n-1}) \in I$. From the induction hypothesis, we deduce

$$|z_1|^{k_1} \cdots |z_{n-1}|^{k_{n-1}} \leq C_1^{k_1} \cdot C^{k_2+\cdots+k_{n-1}} \cdot \rho^{-n}$$

where C_1 is defined by $C_1 = \rho \cdot |z_1| = \rho \cdot \frac{|v_1|}{|u_1|} = \sqrt{|v_1| \cdot C}$. Our estimation then becomes

$$|z_1|^{k_1} \cdots |z_{n-1}|^{k_{n-1}} \leq \left(\frac{C}{|v_1|}\right)^{\frac{k}{2}+k'} \cdot |v_1|^{k+k'} \cdot \rho^{-n}$$

where, for simplicity, we have set $k = k_1$ and $k' = k_2 + \cdots + k_{n-1}$. On the other hand, from the definition of ρ, we deduce that $\rho \leq \frac{r \cdot |u_1|^2}{\|U\|_r} \leq |u_1|$; using then the definition of C, we find $C \leq |v_1|$. Noticing further that $|v_1| \leq 1$ and that, necessarily, $\frac{k}{2} + k' \geq 1$ and $k + k' \geq 2$, we end up with

$$|z_1|^{k_1} \cdots |z_{n-1}|^{k_{n-1}} \leq \frac{C}{|v_1|} \cdot |v_1|^2 \cdot \rho^{-n} = C \cdot |v_1| \cdot \rho^{-n}.$$

Taking the supremum over all $(k_1, \ldots, k_{n-1}) \in I$, we are finally left with $A \leq C \cdot |v_1| \cdot \rho^{-n}$.

Let us now focus on B. We consider a pair $(i, j) \in J$. We first assume that $i < n-1$. Clearly one of the indices $j+1$ or $i-j+1$ must be strictly greater than 1. We then deduce from the induction hypothesis that $|z_{j+1}| \cdot |z_{i-j+1}| \cdot r^{i-n} \leq C_1 \cdot C \cdot \rho^{-i-2} \cdot r^{i-n}$ where $C_1 = \rho \cdot \frac{|v_1|}{|u_1|}$ is the constant we have introduced in the first part of the proof. We rewrite the above inequality as follows

$$\|U\|_r \cdot |z_{j+1}| \cdot |z_{i-j+1}| \cdot r^{i-n} \leq \frac{\rho \cdot \|U\|_r}{r^2 \cdot u_1} \cdot \left(\frac{\rho}{r}\right)^{n-i-2} \cdot C \cdot |v_1| \cdot \rho^{-n}.$$

From the definition of ρ, it is clear that $\rho \leq \frac{r^2 \cdot |u_1|}{\|U\|_r}$, implying that the first factor $\frac{\rho \cdot \|U\|_r}{r^2 \cdot u_1}$ is at most 1. Similarly, using $r \cdot |u_1| \leq \|U\|_r$, we deduce that the quotient $\frac{\rho}{r}$ is at most 1 as well. Since the exponent $n-i-2$ is nonnegative by assumption, we find

$$\|U\|_r \cdot |z_{j+1}| \cdot |z_{i-j+1}| \cdot r^{i-n} \leq C \cdot |v_1| \cdot \rho^{-n} \tag{25}$$

in this case. We now consider the case where $i = n-1$. By definition of J, we cannot have $j = 0$ or $j = n-1$. Thus both indices $j+1$ and $i-j+1 = n-j$ are strictly greater than 1 and the induction hypothesis yields

$$\begin{aligned}\|U\|_r \cdot |z_{j+1}| \cdot |z_{n-j}| \cdot r^{-1} &\leq \|U\|_r \cdot C^2 \cdot \rho^{-n-1} \cdot r^{-1} \\ &= \frac{C \cdot \|U\|_r}{\rho r \cdot |v_1|} \cdot C \cdot |v_1| \cdot \rho^{-n} = \frac{\rho \cdot \|U\|_r}{r \cdot |u_1|^2} \cdot C \cdot |v_1| \cdot \rho^{-n}\end{aligned}$$

the last equality coming from the very first definition of C. It now follows from the definition of ρ that the factor $\frac{\rho \cdot \|U\|_r}{r \cdot |u_1|^2}$ is at most 1, implying that the inequality (25) is also valid when $i = n-1$. Taking the supremum over all $(i, j) \in J$, we obtain $B \leq C \cdot |v_1| \cdot \rho^{-n}$.

Coming back to the estimation $|z_n| \leq |v_1|^{-1} \cdot \max(A, B)$, we finally obtain $|z_n| \leq C \cdot \rho^{-n}$ and the induction goes. □

A.3. **Overconvergence phenomena.** Under Assumptions (H_U) and (H_V), Proposition 26 shows that the radius of convergence of the solution of Eq. (23) is at least 1/4 (by taking $r = 1/4$ and $s = 1$). Nonetheless, there do exist particular choices of U and V for which the solution z overconverges beyond this radius. For example, when U and V are built from the equations of two isogenous elliptic curves as in Eq. (5) (*cf* page 2), we know that z has integral coefficients; hence, its radius of convergence is at least 1. One may wonder if such examples are isolated or not; in what follows, we will prove a first result in this direction showing that the overconvergence phenomenom we observed persists when the differential equation is slightly perturbed.

From now on, we work with the differentiel equation (24) (which is a particular case of Eq. (23)). We fix $h \in \mathcal{V}_1$ with t-adic valuation 1, *i.e.* $h(0) = 0$ and $h'(0) \neq 0$. Let Ω denote the subset of $K[\![t]\!]$ consisting of series with non-vanishing constant coefficient. By Proposition 4, we know that Eq. (24) admits a unique solution $z_g \in tK[\![t]\!]$ for all $g \in \Omega$.

Proposition 27. *Let $r \in]0, 1[$. We consider $g \in \mathcal{V}_r$ satisfying the two following assumptions:*
(a) g does not vanish on the open ball of centre 0 and radius r in an algebraic closure of K,
(b) the solution z_g of Eq. (24) is in $\mathcal{V}_r$.
Then, for all $\gamma_1, \gamma_2 \in \mathcal{V}_{r,+}$ such that

$$\|\gamma_i\|_{r,+} < \min\left(\|z'_g\|_r, \frac{\|g\|_r^2}{4\cdot\|z'_g\|_r}\right) \quad \textit{for } i \in \{1, 2\}$$

we have $\dfrac{z_{g+\gamma_1} - z_{g+\gamma_2}}{t(t-4a)} \in \mathcal{V}_r$ *and* $\left\|\dfrac{z_{g+\gamma_1} - z_{g+\gamma_2}}{t(t-4a)}\right\|_r \leq \|\gamma_1 - \gamma_2\|_{r,+}$.

Remark 28. By Weierstrass Preparation Theorem, Assumption (a) is equivalent to the fact that $\|g\|_r = |g(0)|$, *i.e.* the maximum of g is reached at the origin. Besides, it implies that $g^{-1} \in \mathcal{V}_r$ as well and $\|g^{-1}\|_r = \|g\|_r^{-1}$.

Proof of Proposition 27. We follow the proof of Proposition 16. We fix a positive integer n. We set $E_n = \mathcal{V}_{r,+}/t^n\mathcal{V}_{r,+}$ and $F_n = \mathcal{V}_r/t^n\mathcal{V}_r$ and equip them with the induced norms. As K-vector spaces, both E_n and F_n are canonically isomorphic to $K[\![t]\!]/(t^n)$. However, the norms on them differ; we have

$$\|a_0 + a_1 t + \cdots + a_{n-1}t^{n-1}\|_{F_n} = \sup_{0\leq i<n} |a_i|\, r^i$$
$$\|f\|_{E_n} = \|\psi_{+,n}(f)\|_{F_n}$$

for $a_0, \ldots, a_{n-1} \in K$ and $f \in E_n$. As in Section 2.5, we consider the analytic function

$$\begin{array}{rccc} \theta_n : & W_n & \longrightarrow & F_n \\ & \gamma & \mapsto & \dfrac{z_{g+\gamma} - z_g}{t(t-4a)} \end{array}$$

where the domain W_n is the open subset of E_n consisting of series γ for which $g+\gamma$ does not vanish at 0. Proposition 13 shows that the differential of θ_n at a point $\gamma \in W_n$ is given by

$$d\theta_n(\gamma) : \delta g \mapsto z'_{g+\gamma} \cdot (g+\gamma)^{-1} \cdot \psi_{+,n}(\delta g). \tag{26}$$

Following [CRV15, Remark 2.6], we introduce a copy $\tilde{E}_n$ of E_n equipped with the modified norm defined as follows:

$$\|f\|_{\tilde{E}_n} = \frac{\|z'_g\|_{F_n}}{\|g\|_{F_n}} \cdot \|f\|_{E_n}.$$

Here f denotes at the same time a series in E_n and its copy in $\tilde{E}_n$. In order to avoid similar confusions in the future, we introduce the mapping $\mathrm{Id} : E_n \to \tilde{E}_n$ taking a series in E_n to its counterpart in $\tilde{E}_n$. We set $\tilde{W}_n = \mathrm{Id}(W_n)$. We deduce from Eq. (26) that θ_n is solution of the differential equation $d\theta_n = \tau_n \circ (\theta_n, \mathrm{Id})$ where τ_n is defined by

$$\begin{array}{rccl} \tau_n : & F_n \times \tilde{W}_n & \longrightarrow & \mathrm{Hom}(E_n, F_n) \\ & (\zeta \ , \ \tilde{\gamma}) & \mapsto & \left(\delta g \ \mapsto \ \dfrac{z'_g + t(t-4a)\zeta' + 2(t-2a)\zeta}{g + \mathrm{Id}^{-1}(\tilde{\gamma})} \cdot \psi_{+,n}(\delta g)\right). \end{array}$$

We consider a pair $(\zeta, \tilde{\gamma}) \in F_n \times \tilde{E}_n$ such that $\|\zeta\|_{F_n} < \|z'_g\|_{F_n}$ and $\|\tilde{\gamma}\|_{\tilde{E}_n} < \|z'_g\|_{F_n}$. Then,

$$\|z'_g + t(t-4a)\zeta' + 2(t-2a)\zeta\|_{F_n} = \|z'_g\|_{F_n}.$$

Write $\gamma = \mathrm{Id}^{-1}(\tilde{\gamma})$. From the definition of the norm on $\tilde{E}_n$, we derive $\|\gamma\|_{E_n} < \|g\|_{F_n}$, which further implies that $\|\gamma\|_{F_n} < \|g\|_{F_n}$. We deduce that $\|g{+}\gamma\|_{F_n} = |(g{+}\gamma)(0)| = \|g\|_{F_n}$, showing then that $\|(g{+}\gamma)^{-1}\|_{F_n} = \|g{+}\gamma\|_{F_n}^{-1} = \|g\|_{F_n}^{-1}$. As a consequence, we conclude that

$$\left\| \frac{z'_g + t(t-4a)\zeta' + 2(t-2a)\zeta}{g + \mathrm{Id}^{-1}(\tilde{\gamma})} \right\|_{F_n} \leq \frac{\|z'_g\|_{F_n}}{\|g\|_{F_n}}$$

whenever $\|\zeta\|_{F_n} < \|z'_g\|_{F_n}$ and $\|\tilde{\gamma}\|_{\tilde{E}_n} < \|z'_g\|_{F_n}$. With the Λ-notation introduced in Eq. (16), we have proved that $\Lambda(\tau_n)(x) \leq \log \|z'_g\|_{F_n} - \log \|g\|_{F_n}$ for all $x < \log \|z'_g\|_{F_n}$. Applying [CRV15, Proposition 2.5], we deduce that

$$\forall x < \min\left(\log \|z'_g\|_{F_n}, \log \frac{\|g\|_{F_n}}{2}\right), \quad \Lambda(\theta_n)(x) \ \leq \ 2x + \log\left(\frac{\|g\|_{F_n}^2}{4{\cdot}\|z'_g\|_{F_n}}\right).$$

Applying now [CRV14, Proposition 3.12], we find that

$$\theta_n\big(B_{E_n}(\delta)\big) = d\theta_n(0)\big(B_{E_n}(\delta)\big) \subset B_{F_n}(\delta) \tag{27}$$
$$\text{when} \quad \delta < \min\left(\|z'_g\|_{F_n}, \frac{\|g\|_{F_n}}{2}, \frac{\|g\|_{F_n}^2}{4{\cdot}\|z'_g\|_{F_n}}\right) = \min\left(\|z'_g\|_{F_n}, \frac{\|g\|_{F_n}^2}{4{\cdot}\|z'_g\|_{F_n}}\right).$$

The last equality comes from the observation that $\frac{1}{2}{\cdot}\|g\|_{F_n}$ is the geometrical mean between the two others arguments in the minimum. Passing to the limit on n in Eq. (27), we get the proposition when $\gamma_1 = 0$. Finally, for a general γ_1, we apply the same argument after having replaced g by $g + \gamma_1$ and γ_2 by $\gamma_2 - \gamma_1$. ☐

Corollary 29. *Let $r \in]0, 1[$. We consider $g_0 \in \mathcal{V}_r$ satisfying the two following assumptions:*

(a) g does not vanish on the open ball of centre 0 and radius r in an algebraic closure of K,

(b) the solution z_{g_0} of Eq. (24) is in $\mathcal{V}_r$.

Then, for all $\rho \in]0, r[$ and all $g \in \mathcal{V}_r$ such that

$$\|g - g_0\|_r < \tfrac{1}{2} \cdot \min\big(1, \log\big(\tfrac{r}{\rho}\big)\big) \cdot \min\left(\|z'_{g_0}\|_\rho, \frac{\|g_0\|_\rho^2}{4{\cdot}\|z'_{g_0}\|_\rho}\right)$$

we have $z_g \in \mathcal{V}_\rho$ and $\|z_g - z_{g_0}\|_\rho \leq \max\big(2, \frac{2}{\log(r/\rho)}\big) \cdot \|g - g_0\|_r$.

Proof. We apply Proposition 27 with $r = \rho$, $g = g_0$, $\gamma_1 = g - g_0$ and $\gamma_2 = 0$ and then conclude by using Proposition 25 combined with the fact that $\|t(t-4a)\|_\rho \leq 1$. ☐

Corollary 29 implies in particular that, for any real number $r \in]0, 1[$, the fonction $\mathcal{V}_r \to \mathbb{R}$ taking g to $\min(r, \mathrm{RoC}(z_g))$ is continuous (where the domain $\mathcal{V}_r$ is equipped with the topology of the norm $\|\cdot\|_r$). By Proposition 27, it is even locally constant around each point g such that $\mathrm{RoC}(z_g) < r$. This theoretical result looks quite interesting to us and raises a new range of questions. In particular, can we expect similar results for a wider class of nonlinear p-adic differential equations?

References

[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). 14

[BDFD+19] L. Brieulle, L. De Feo, J. Doliskani, J.-P. Flori, and E. Schost. Computing isomorphisms and embeddings of finite fields. *Math. Comp.*, 88(317):1391–1426, 2019. 1

[BMSS08] A. Bostan, F. Morain, B. Salvy, and E. Schost. Fast algorithms for computing isogenies between elliptic curves. *Math. Comp.*, 77(263):1755–1778, 2008. 1, 2, 15

[BS11] G. Bisson and A. V. Sutherland. Computing the endomorphism ring of an ordinary elliptic curve over a finite field. *J. Number Theory*, 131(5):815–831, 2011. 17

[Car17] X. Caruso. Computations with p-adic numbers. *Les cours du CIRM*, 5(1), 2017. 3

[CEL12] J.-M. Couveignes, T. Ezome, and R. Lercier. A faster pseudo-primality test. *Rend. Circ. Mat. Palermo (2)*, 61(2):261–278, 2012. 1

[CEL19] X. Caruso, E. Eid, and R. Lercier. Package isocar2g1. https://github.com/rlercier/isocar2g1, 2019. 14

[CH02] J.-M. Couveignes and T. Henocq. Action of Modular Correspondences around CM Points. In C. Fieker and D. R. Kohel, editors, *Algorithmic Number Theory*, pages 234–243, Berlin, Heidelberg, 2002. Springer Berlin Heidelberg. 19

[CL09] J.-M. Couveignes and R. Lercier. Elliptic periods for finite fields. *Finite Fields Appl.*, 15(1):1–22, 2009. 1

[CL13] J.-M. Couveignes and R. Lercier. Fast construction of irreducible polynomials over finite fields. *Israel J. Math.*, 194(1):77–105, 2013. 3, 16, 18

[Cou06] J.-M. Couveignes. Hard homogeneous spaces. http://eprint.iacr.org/2006/291/, 2006. 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, 24

[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, 23, 24

[DF11] L. De Feo. Fast algorithms for computing isogenies between ordinary elliptic curves in small characteristic. *J. Number Theory*, 131(5):873–893, 2011. 2

[DFJP14] L. De Feo, D. Jao, and J. Plût. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. *J. Math. Cryptol.*, 8(3):209–247, 2014. 1

[EL13] T. Ezome and R. Lercier. Elliptic periods and primality proving. *J. Number Theory*, 133(1):343–368, 2013. 1

[Koh96] D. Kohel. *Endomorphism rings of elliptic curves over finite fields.* PhD thesis, University of California, Berkeley, 1996. 1, 16

[KU11] K. S. Kedlaya and C. Umans. Fast polynomial factorization and modular composition. *SIAM J. Comput.*, 40(6):1767–1802, 2011. 18

[Ler96] R. Lercier. Computing isogenies in $\mathbf{F}_{2^n}$. In *Algorithmic number theory (Talence, 1996)*, volume 1122 of *Lecture Notes in Comput. Sci.*, pages 197–212. Springer, Berlin, 1996. 2

[LJPT64] J. Lubin, S. J.-P., and J. Tate. Elliptic curves and formal groups. Notes available at http://ma.utexas.edu/users/voloch/lst.html, 1964. 17

[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, 2, 15

[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, 15, 17

[Nar18] A. K. Narayanan. Fast computation of isomorphisms between finite fields using elliptic curves. In L. Budaghyan and F. Rodríguez-Henríquez, editors, *Arithmetic of Finite Fields. WAIFI 2018.*, volume 11321 of *Lecture Notes in Computer Science*. Springer, Cham, 2018. 1

[RS06] A. Rostovtsev and A. Stolbunov. Public-key cryptosystem based on isogenies. http://eprint.iacr.org/2006/145/, 2006. 1

[Sat00] T. Satoh. The canonical lift of an ordinary elliptic curve over a finite field and its point counting. *J. Ramanujan Math. Soc.*, 15(4):247–270, 2000. 17

[Sch95] R. Schoof. Counting points on elliptic curves over finite fields. *J. Théor. Nombres Bordeaux*, 7(1):219–254, 1995. 1

[Sil94] J. H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994. 1

[Sil09] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009. 1

[SST03] T. Satoh, B. Skjernaa, and Y. Taguchi. Fast computation of canonical lifts of elliptic curves and its application to point counting. *Finite Fields Appl.*, 9(1):89–101, 2003. 17

[Tho03] E. Thomé. *Algorithmes de calcul de logarithmes discrets dans les corps finis*. PhD thesis, École polytechnique, 2003. 14

Xavier Caruso, Univ. Bordeaux, CNRS - IMB - UMR 5251, F-33405 Talence, France.
Email address: xavier.caruso@normalesup.org

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

Reynald Lercier, DGA & Univ Rennes, CNRS, IRMAR - UMR 6625, F-35000 Rennes, France.
Email address: reynald.lercier@m4x.org