On isogeny calculation by solving p-adic differential equations

Elie Eid

DOCTORAT BRETAGNE LOIRE / MATHSTIC

UNIVERSITÉ DE RENNES 1

THÈSE DE DOCTORAT DE

L'UNIVERSITÉ DE RENNES 1

ÉCOLE DOCTORALE N° 601
Mathématiques et Sciences et Technologies de l'Information et de la Communication
Spécialité : *Mathématiques et leurs Interactions*

Par
Elie EID

Sur le calcul d'isogénies par résolution d'équations différentielles p-adiques

Thèse présentée et soutenue à Rennes, le 22 Juin 2021
Unité de recherche : IRMAR, UMR CNRS 6625 Institut de Recherche Mathématique de Rennes

Rapporteurs avant soutenance :

Jennifer BALAKRISHNAN	Assistant Professor, Boston University
David KOHEL	Professeur des Universités, Université d'Aix-Marseille

Composition du Jury :

Président :	Ariane MEZARD	Professeure des Universités, Université de Paris
Examinateurs :	Cécile ARMANA	Maîtresse de conférences, Université de Franche-Comté
	Jennifer BALAKRISHNAN	Assistant Professor, Boston University
	Jean-Marc COUVEIGNES	Professeur des Universités, Université de Bordeaux
	David KOHEL	Professeur des Universités, Université d'Aix-Marseille
	Bernard LE STUM	Maître de conférences, Université de Rennes 1
Dir. de thèse :	Reynald LERCIER	Chercheur DGA, Université de Rennes 1
Co-dir. de thèse :	Xavier CARUSO	Directeur de Recherche CNRS, Université de Bordeaux

Résumé

Les premiers travaux sur le calcul d'isogénies ont été utilisés d'une manière cruciale dans l'algorithme SEA pour le comptage de points sur les courbes elliptiques définies sur des corps finis. D'autres applications en théorie des nombres ont suivies : construction de bases normales d'extensions de corps, de polynômes irréductibles, d'isomorphismes de corps finis, etc. Récemment, les isogénies ont été utilisés en cryptologie.
Pour avoir des algorithmes efficaces de calcul d'isogénies, en particulier celles qui sont définies sur des corps finis, plusieurs approches ont été proposées parmi lesquelles une méthode qui consiste à ramener ce problème à celui de la détermination d'une solution d'une équation différentielle. Dans certaines situations, il nous sera nécessaire de relever le problème dans les p-adiques. Cependant, le calcul numérique dans le corps des nombres p-adiques n'est en général pas possible sauf si on travaille à précision finie. Ceci nous oblige donc à manipuler des approximations au lieu de travailler avec des valeurs exactes. Nous proposons dans cette thèse des algorithmes effectifs de calcul d'isogénies entre courbes elliptiques et Jacobiennes de courbes hyperelliptiques via l'approche des équation différentielles p-adiques avec un bon contrôle de précision.
Plus précisément, nous nous intéressons dans un premier temps au calcul d'isogénies entre courbes elliptiques définies sur une extension de $\mathbb{Q}_2$. Ce travail vient ainsi compléter ceux réalisés pour le cas impair. Nous donnons quelques applications, en particulier le calcul d'isogénies entre courbes elliptiques sur des corps finis de caractéristique 2 et de polynômes irréductibles, tous deux en temps quasi-linéaire en le degré.
Dans un second temps, nous présentons un algorithme de calcul explicite de représentations rationnelles d'isogénies entre Jacobiennes de courbes hyperelliptiques sur une extension du corps des nombres p-adiques $\mathbb{Q}_p$. Par conséquent, après avoir éventuellement relevé le problème dans les p-adiques, nous obtenons des algorithmes efficaces pour le calcul d'isogénies entre Jacobiennes de courbes hyperelliptiques définies sur des corps finis de caractéristique impaire. Une autre application importante que nous en déduisons est le calcul des polynômes de Cantor de ℓ-divisions.
L'efficacité de ces algorithmes repose sur une analyse fine des solutions d'équations différentielles p-adiques.

Abstract

Interest in computing isogenies efficiently was first motivated by the Schoof-Elkies-Atkin (SEA) algorithm for counting points of elliptic curves defined over finite fields. Other applications in number theory have followed : normal basis of field extensions, computation of irreducible polynomials, finite field isomorphisms, etc. Recently, isogenies have been used in cryptology.

In order to have efficient algorithms for computing isogenies, in particular those which are defined over finite fields, several approaches have been suggested, including a method which consists of reducing the problem to the computation of a solution of a differential equation. In some cases, it will be necessary to lift the problem in the p-adics. However, calculations in the field of p-adic numbers is generally not possible unless working with finite precision. For this reason, we need to deal with approximations instead of working with exact values.

In this thesis, we propose efficient algorithms for computing isogenies between elliptic curves and Jacobians of hyperelliptic curves via p-adic differential equations with a sharp analysis of the loss of precision.

More precisely, on the one hand, we are interested in computing elliptic curve isogenies defined over an extension of $\mathbb{Q}_2$. This work complements the work carried out over extensions of $\mathbb{Q}_p$ for p odd. We give some applications, in particular computing over finite fields of characteristic 2 isogenies of elliptic curves and irreducible polynomials, both in quasi-linear time in the degree.

On the other hand, we present an algorithm for the explicit computation of rational representations between Jacobians of hyperelliptic curves defined over an extension of the field of p-adic numbers $\mathbb{Q}_p$. Consequently, after having possibly lifted the problem to the p-adics, we obtain efficient algorithms for computing isogenies between Jacobians of hyperelliptic curves defined over finite fields of odd characteristic. Another important application is the computation of Cantor ℓ-division polynomials.

The efficiency of these algorithms is based on an analysis of the solutions of p-adic differential equations.

Remerciements

Je n'aurais jamais pu réaliser ce travail doctoral sans le soutien d'un grand nombre de personnes dont la générosité et l'intérêt manifestés à l'égard de ma recherche m'ont permis de progresser dans cette phase délicate de mon parcours.

Je tiens tout d'abord à remercier mes deux directeurs de thèse, Reynald Lercier et Xavier Caruso, pour la confiance qu'ils m'ont accordée, pour leurs conseils qu'ils m'ont prodigués et pour toutes les heures qu'ils ont consacrées à diriger cette recherche. Je souhaiterai également les remercier pour leurs encouragements dans les moments difficiles et leur respect des délais serrés de relecture des documents que je leur ai adressés.

J'adresse de chaleureux remerciements à Christophe Ritzenthaler et Jean-Marc Couveignes pour avoir accepté de faire partie du comité de suivi de thèse. Je suis très reconnaissant pour leur suivi de mon cursus et leurs suggestions lors des réunions du comité.

Je souhaite également exprimer ma gratitude à David Kohel et Jennifer Balakrishnan d'avoir accepté d'être rapporteurs de ce travail. Merci pour leur relecture attentive et leurs commentaires.
Un grand merci à Ariane Mezard, Bernard Le Stum, Cécile Armana et Jean-Marc Couveignes pour être membre de mon jury.

Je suis très heureux d'avoir pu effectuer ma thèse à l'IRMAR et je tiens à remercier l'équipe de Géométrie et Algèbre Effectives de m'avoir accueilli chaleureusement depuis le début, et tout au long de ma thèse. Je remercie en particulier Delphine Boucher, Elisa Lorenzo García, Felix Ulmer et Sylvain Duquesne avec qui j'ai eu le plaisir d'enseigner, sans oublier aussi Stéphane Balac, Ludovic Marquis et Valérie Monbet.
Mes remerciements vont également à toute l'équipe administrative de l'IRMAR et au personnel, pour leur accueil, leur soutien et leur aide que ce soit dans les démarches administratives ou en informatique.
Merci à tous les doctorants de l'IRMAR et de l'extérieur avec qui j'ai passé de très bon

moments.

J'adresse mes vifs remerciements à mes enseignants du Lycée, de l'Université Libanaise et de l'Université de Rennes 1. Leurs soutiens et leurs encouragements m'ont été précieux et m'ont permis de progresser dans mon domaine. J'ai une pensée particulière à une personne qui m'est très chère, mais qui malheureusement nous a quitté, Latifé mon Prof. de maths, à qui je dédie cette thèse.
Un grand merci à tous mes amis en France et au Liban, d'être là, à mes côtés !

Pour terminer, je ne pourrais finir ces remerciements sans penser à ma famille. Mes mots ne seront jamais à la hauteur de l'amour et l'affection que vous m'avez témoignée tout au long de mes études. J'aimerais vous exprimer toute ma gratitude et ma reconnaissance. Cette dédicace serait pour moi, la meilleure façon de vous honorer et vous montrer à quel point vous avez été magnifique.

> The end of a melody is not its goal : but nonetheless, had the melody not reached its end it would not have reached its goal either. A parable.
>
> *Friedrich Nietzsche*

Table of Contents

Introduction (en français)

Depuis les travaux fondamenteurs de Diffie et Hellman [DH76] qui ont jeté les bases de la cryptographie asymétrique, cette dernière n'a pas cessé d'évoluer. Le premier cryptosystème à clé publique, qui est resté le plus célèbre, est le système RSA, conçu en 1977 par Rivest, Shamir et Adleman [RSA78]. Sa sécurité repose sur la difficulté du problème de factorisation d'un entier. En 1985, Miller [Mil86a] et Koblitz [Kob87] ont indépendamment suggéré d'utiliser le groupe des points d'une courbe elliptique définie sur un corps fini à la place du groupe multiplicatif d'un $\mathbb{Z}/n\mathbb{Z}$. Les schémas cryptographiques qui en résultent, appelés ECC pour *Elliptic Curve Cryptography*, sont des mécanismes à clé publique qui fournissent des fonctionnalités similaires à RSA. Cependant, leur sécurité repose sur la difficulté d'un nouveau problème : le logarithme discret. Actuellement, les meilleurs algorithmes connus pour résoudre le problème du logarithme discret sur une courbe elliptique ont une complexité exponentielle en temps, contrairement aux algorithmes sous-exponentiels connus pour le problème de la factorisation d'entiers. Cela signifie que nous pouvons atteindre un niveau de sécurité avec des clés nettement plus petites dans les systèmes à courbes elliptiques qu'avec le RSA.

En 1989, Koblitz [Kob89] a proposé de généraliser l'usage en cryptographie des courbes elliptiques au cas des courbes hyperelliptiques (généralement de genre 2), donnant ainsi naissance à la *cryptographie sur courbes hyperelliptiques* (HECC). Contrairement au cas elliptique, l'ensemble des points d'une courbe hyperelliptique ne forme pas un groupe. Cependant, on peut toujours associer à chacune de ces courbes un groupe abélien : leur Jacobienne. L'arithmétique sur la Jacobienne d'une courbe hyperelliptique est plus compliquée et moins efficace que sur une courbe elliptique. En contrepartie, elle permet d'assurer un même niveau de sécurité en manipulant des paramètres de courbes et des coordonnées de points plus petits.
La remise en question de la sécurité des cryptosystèmes actuels (notamment RSA, ECC, HECC, *etc.*) face à la puissance des ordinateurs quantiques a conduit la communauté scientifique à s'interroger sur des alternatives résistantes à cette future génération d'ordinateurs. Avec la cryptographie basée sur les réseaux et la cryptographie basée sur les codes, l'une des alternatives les plus prometteuses est la *cryptographie à base d'isogé-*

nies [DFJP14a] qui semble mieux résister à de tels ordinateurs. Les courbes elliptiques et hyperelliptiques reviennent ainsi sur le devant de la scène.

Cette thèse vise à la conception d'algorithmes efficaces de calcul d'isogénies entre courbes elliptiques et Jacobiennes de courbes hyperelliptiques et à explorer quelques applications. Cette introduction se poursuit par une présentation plus détaillée des objets mathématiques fondamentaux dont il est question dans cette thèse ; nous nous efforcerons en outre de les replacer dans leur contexte mathématique et historique de de donner à nos lectrices et nos lecteurs les clés pour mieux appréhender la portée de nos travaux. Dans un second temps, nous décrivons la problématique de la thèse et nous présentons nos contributions.

Contexte

Courbes elliptiques

Par une *courbe elliptique* sur un corps k nous entendons, une courbe lisse représentée dans le plan projectif $\mathbb{P}^2(\bar{k})$ par l'équation, dite de *Weierstrass* :

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

où a_1, a_2, a_3, a_4 et a_6 sont des éléments dans k.

La théorie des courbes elliptiques trouve son origine au 18-ième siècle dans le calcul des *intégrales elliptiques*, c'est-à-dire d'intégrales de la forme

$$\int_c^x R\Big(t, \sqrt{P(t)}\Big)\, dt$$

où R est une fonction rationnelle et P un polynôme de degré 3 ou 4 avec des racines simples. Ces intégrales sont intéressantes car elles sont directement reliées au problème de la rectification d'une ellipse, c'est-à-dire au calcul de la longueur d'arcs d'ellipse. Au 19-ième siècle, Abel porta son intérêt sur l'étude des *fonctions réciproques* de ces intégrales et définit alors une *fonction elliptique* comme étant la réciproque d'une intégrale elliptique. Un exemple fondamental de fonction elliptique est la fonction sinus qui est obtenue comme l'inverse de la fonction « circulaire »

$$x \mapsto \int_0^x \frac{1}{\sqrt{1-t^2}}\, dt.$$

De manière générale, les fonctions elliptiques peuvent ainsi être pensées comme un analogue des fonctions trigonométriques classiques lorsque l'on ne cherche plus à mesurer la longueur des cercles mais celle des ellipses. La notion de fonction elliptique fût reprise et développée dans plusieurs travaux. En particulier, Jacobi montra que toute fonction méromorphe sur $\mathbb{C}$ et doublement périodique est nécessairement une fonction elliptique. Les fonctions elliptiques apparaissent ainsi comme des fonction méromorphe sur un *tore complexe* de la forme $\mathbb{C}/\Lambda$ où Λ est le réseau engendré par deux nombres complexes linéairement indépendants ω_1 et ω_2.
En 1863, Weierstrass définit la fonction elliptique $\wp$:

$$\wp(z) = z^{-2} + \sum_{\lambda \in \Lambda \setminus \{0\}} \left((z+\lambda)^{-2} + \lambda^{-2} \right),$$

et montra que toute fonction elliptique de période $\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ est une fraction rationnelle de $\wp(z)$ et $\wp'(z)$. Il trouva la fameuse relation entre $\wp(z)$ et $\wp'(z)$:

$$(\wp(z)')^2 = 4\wp(z)^3 + g_2\wp(z) - g_3 \tag{1}$$

où g_2 et g_3 sont des nombres complexes (tels que $g_2^3 - 27g_3^2 \neq 0$) ne dépendant que de Λ. Il démontra de plus que les deux fonctions $\wp(z)$ et $\wp'(z)$ admettent des formules d'addition et de doublement, à savoir

$$\wp(z_1 + z_2) = -\wp(z_1) - \wp(z_2) + \frac{1}{4}\left(\frac{\wp'(z_1) - \wp'(z_2)}{\wp(z_1) - \wp(z_2)} \right)^2$$
$$\wp(2z_1) = -2\wp(z_1) + \left(\frac{12\wp(z_1) - g_2}{4\wp'(z_1)} \right)^2.$$

La théorie des courbes elliptiques était née. En effet, la relation (1) porte en germe la définition algébrique des courbes elliptiques tandis que la formule d'addition conduit naturellement à la loi de groupe. En langage moderne, la paramétrisation

$$z \mapsto \begin{cases} (\wp(z) : \wp'(z) : 1) & \text{si } z \neq 0 \\ (0:1:0) & \text{sinon} \end{cases}$$

induit une application de $\mathbb{C}/\Lambda$ dans la courbe elliptique E_Λ d'équation $Y^2Z = 4X^3 - g_2XZ^2 - g_3Z^3$. Un exercice permet de montrer que cette application est bijective. Sa

réciproque est donnée par l'intégrale elliptique

$$P \mapsto \int_{\gamma(P)} \frac{dx}{y} \mod \Lambda$$

(où $\gamma(P)$ est un chemin joignant le point $(0:1:0)$ à P), ce qui fait le lien avec le problème initial de la rectification des ellipses. Les formules d'addition et de doublement des deux fonctions $\wp(z)$ et $\wp'(z)$, qui généralisent les formules bien connues d'addition et de doublement pour les fonctions sinus et cosinus, conduisent à des relations remarquables entre les longueurs d'arcs d'ellipses séparant des points d'abscisses données.
Ne retenant que l'équation de Weierstrass et les formules d'addition et de doublement, la théorie des courbes elliptiques s'étend à un corps de base quelconque, ce qui fait d'elle un objet mathématique très puissant. D'un point de vue historique, il est important de souligner que l'existence d'une loi de groupe sur l'ensemble des solutions d'une équation cubique avait déjà été découverte de manière purement algébrique par Fermat et que l'interprétation géométrique « corde-et-tangente » que l'on présente classiquement apparaissait déjà dans les écrits de Newton. Toutefois ce n'est qu'au 19-ième siècle que le lien avec la théorie des fonctions doublement périodiques et le problème de la rectification des ellipses a été mis en lumière et ce n'est véritablement qu'à partir de ce moment que le développement de la théorie des courbes elliptiques a pris toute son ampleur.

L'étude des courbes elliptiques passe par l'étude des morphismes entre courbes elliptiques, c'est-à-dire des applications qui respectent à la fois la structure de variété algébrique (*i.e.* qui sont données par des fractions rationelles) et la structure de groupe. En réalité, préserver la structure de groupe est une condition très faible car elle est vérifiée dès lors que notre application envoie le neutre de la courbe de départ sur le neutre de la courbe d'arrivée. De tels morphismes, lorsqu'ils ne sont pas nuls, sont appelés *isogénies*. On dit que la courbe elliptique E est isogène à la courbe elliptique $\tilde{E}$ sur un corps k s'il existe une isogénie de E dans $\tilde{E}$ qui est définie sur k, *i.e.* peut être représentée par des fractions rationnelles à coefficients dans k.
L'exemple le plus simple d'isogénies est celui de l'application de la multiplication par un entier ℓ sur une courbe elliptique E. Cette application est un morphisme de courbes surjectif et son noyau est un groupe fini appelé le *sous-groupe de ℓ-torsion* de E. Plus généralement, nous pouvons montrer que toute isogénie entre courbes elliptiques est un morphisme de courbes surjectif et de noyau fini.
Nous clôturons le paragraphe par un résultat fondamental sur les isogénies : le théorème

de l'isogénie duale. Ce théorème dit qu'une isogénie est « presque » un isomorphisme, dans le sens où toute isogénie $f : E \to \tilde{E}$ admet une isogénie duale $g : \tilde{E} \to E$ telle que la composée $f \circ g$ (resp. $g \circ f$) soit la multiplication par un entier ℓ sur $\tilde{E}$ (resp. E). Ainsi l'existence d'une isogénie dans un sens implique l'existence d'une isogénie dans le sens opposé. Nous pouvons donc définir une relation d'équivalence sur l'ensemble des courbes elliptiques définies sur un corps k et obtenir des *classes d'isogénies* de courbes elliptiques. Cette notion est plus faible que celle d'isomorphisme, mais capture néanmoins une grande partie des propriétés arithmétiques des courbes elliptiques. Par exemple, sur les corps finis, deux courbes elliptiques sont isogènes si et seulement si elles ont le même nombre de points sur toute extension finie du corps de définition.

Variétés abéliennes et Jacobiennes de courbes algébriques

Les travaux d'Abel et de Jacobi ne se sont pas arrêtés aux intégrales elliptiques. Ils ont étendu la définition d'intégrales elliptiques à des intégrales de fractions de degré quelconque, développant ainsi la notion d'*intégrales abéliennes*. Plus précisément, une intégrale abélienne est une intégrale de la forme

$$\int R(x, y)\, dx$$

où R est une fraction rationnelle de x et de y à coefficients dans $\mathbb{C}$, reliées par une relation algébrique $f(x, y) = 0$ avec f un polynôme à coefficients dans $\mathbb{C}$. Pour faire simple, nous ne considérons que le cas des *intégrales hyperelliptiques*, *i.e.* de la forme

$$\int \frac{dx}{\sqrt{P(x)}}$$

où P est un polynôme de degré $d > 4$. Comme dans le cas elliptique, l'étude de ces intégrales est étroitement liée à celle de la *courbe hyperelliptique* C d'équation $Y^2 = P(X)$. Posons $g = \lfloor (d+1)/2 \rfloor - 1$, on dit que g est le *genre* de la courbe C. Les travaux de Jacobi montrèrent l'existence d'un réseau $\Lambda \subset \mathbb{C}^g$ (*i.e* un sous groupe abélien libre de $\mathbb{C}^g$ de rang $2g$) et d'une application

$$j : C \to \mathbb{C}^g/\Lambda.$$

Dans le language moderne, on dit que le groupe de Lie $J(C) = \mathbb{C}^g/\Lambda$ est la *Jacobienne* de la courbe C et que l'application j est *l'application d'Abel-Jacobi*.
Comme dans le cas des intégrales elliptiques, la compréhension de la structure (de groupes)

de cette Jacobienne vient de la résolution du problème de l'inversion des intégrales. Considérons alors l'application surjective

$$\begin{array}{rcl} j^{(g)} : C^g & \longrightarrow & J(C) \\ (P_1, \ldots, P_g) & \mapsto & j(P_1) + \cdots + j(P_g). \end{array} \tag{2}$$

Il est évident que $j^{(g)}$ n'est pas injective car $J(C)$ est un groupe abélien. Soit $C^{(g)}$ la variété complexe obtenue en identifiant deux éléments de C^g dont les coordonnées sont égales après permutation. L'application $j^{(g)}$ induit un morphisme $C^{(g)} \longrightarrow J(C)$ qui est bijectif sur un ouvert dense de $C^{(g)}$. On dit alors que $J(C)$ et $C^{(g)}$ sont *birationnellement équivalentes*. Il s'avère que la notion de Jacobienne peut être généralisée pour n'importe quelle courbe algébrique projective lisse définie sur $\mathbb{C}$, en particulier le morphisme donné dans l'équation (2) qui montre qu'un élément de la Jacobienne d'une courbe de genre g peut être représenté par un ensemble de g points sur C. Nous nous référons au livre de Birkenhake et Lange [LB04] pour une construction plus complète de la Jacobienne d'une courbe définie sur $\mathbb{C}$.

En 1948, Weil donna une construction de la Jacobienne sur un corps quelconque algébriquement clos dans le but de démontrer l'hypothèse de Riemann pour les courbes définies sur un corps fini. Pour ce faire, il voulut donner un sens algébrique à la Jacobienne d'une courbe, c'est-à-dire l'écrire en terme de sous-ensembles algébriques d'un espace projectif. Toutefois, à cette époque, les outils pour y parvenir n'étaient pas encore disponibles. Weil fût donc contraint de définir la Jacobienne comme étant une variété abstraite et introduit donc, à cette occasion, la notion de *variétés abéliennes*, inaugurant ainsi la géométrie algébrique moderne. D'une manière formelle, une variété abélienne est une variété algébrique propre qui admet une structure de groupe algébrique (nécessairement commutative dans ce cadre). En particulier, la Jacobienne d'une courbe de genre g est une variété abélienne de dimension g, mais la réciproque est fausse en général sauf si $g = 1$ (on est alors dans le cadre des courbes elliptiques) ou bien $g = 2$ avec quelques conditions supplémentaires.

Définissons maintenant la notion d'isogénies entre variétés abéliennes. Comme pour le cas des courbes elliptiques, on définit un *morphisme de variétés abéliennes* comme une application qui doit respecter les structures algébriques et géométriques des variétés. Une *isogénie* entre deux variétés abéliennes (de même dimension) est un morphisme de variétés abéliennes de noyau fini. À nouveau, un exemple typique d'isogénies est celui de la multiplication par ℓ

$$[\ell]_A : A \to A,\ x \mapsto \ell x$$

dont le noyau est formé des points de ℓ-torsion.
Les propriétés que nous avons données dans le paragraphe précédent sur les isogénies entre courbes elliptiques, se généralisent en dimension supérieure :

— Une isogénie entre variétés abéliennes est un morphisme surjectif.
— (Le théorème de l'isogénie duale.) Si $f : A \to B$ est une isogénie, alors il existe une isogénie $g : B \to A$ et un entier n telle que $g \circ f = [n]_A$ et $f \circ g = [n]_B$.
— (La conservation des propriétés arithmétiques sur un corps fini.) Deux variétés abéliennes sont isogènes sur un corps fini si et seulement si elles ont le même nombre de points sur toute extension finie de ce corps.

Calcul d'isogénies entre courbes elliptiques

Les premiers travaux explicites sur le calcul d'isogénies sont apparus dans les années 70 avec les formules de Vélu [Vél71] pour les courbes elliptiques. Étant donnés une courbe elliptique E et un sous-groupe fini G, celles-ci visent à calculer l'équation de la courbe quotient $\widetilde{E} = E/G$ et les fractions rationnelles qui définissent l'isogénie :

$$\begin{array}{rccl} I : & E & \longrightarrow & \widetilde{E} \\ & P & \mapsto & \left(x_P + \displaystyle\sum_{Q \in G \setminus \{\infty\}} (x_{P+Q} - x_Q),\ y_P + \sum_{Q \in G \setminus \{\infty\}} (y_{P+Q} - y_Q) \right), \end{array}$$

c'est-à-dire le morphisme de passage au quotient. Il est à noter que le problème du calcul de G, *i.e.* du calcul des sous-groupes de points de torsion, est indépendant et a été résolu de manière optimale par Elkies dans le cas des courbes elliptiques [Elk98], en utilisant des équations modulaires. L'utilisation des équations modulaires en genre supérieur est malaisée, puisqu'elles ont des coefficients entiers beaucoup trop gros. Dans la suite de cette thèse, nous ne considérerons pas ce problème et nous nous concentrerons sur le calcul de l'isogénie, une fois son noyau donné.

Le travail de Vélu a été amélioré dans plusieurs publications. Les premiers algorithmes de calcul d'isogénies ont été développés par Atkin et Elkies [Atk88] et utilisés pour accélérer l'algorithme de Schoof [Sch85], le premier algorithme de complexité polynomiale pour le comptage de points sur les courbes elliptiques définies sur des corps finis. D'autres articles ont suivis, notamment ceux de [Mor95] et [Sch95].
Lorsque la caractéristique du corps de base est petite (mais non nulle), des algorithmes de calcul d'isogénies sont présentés dans les travaux de Couveignes [Cou96] et Lercier [Ler96], publiés dans les années 90. Dans le cas de la grande caractéristique, suivant une approche

initiée par Elkies [Elk98], qui ramène le problème de calcul d'isogénies entre courbes elliptiques à celui de la détermination d'une solution d'une équation différentielle, Bostan *et al.* [Bos+08] obtiennent un algorithme de calcul d'isogénies de complexité quasi-linéaire en le degré. Cette approche a été par la suite étendue par Lercier et Sirvent [LS08] au cas de la petite caractéristique *impaire*. Leur méthode consiste à relever les courbes sur le corps des nombres p-adiques, afin de se ramener en caractérisque nulle. Plus tard, la complexité de l'algorithme de Lercier et Sirvent a été améliorée par Lairez et Vaccon [LV16] en utilisant des techniques p-adiques développées dans [CRV14].

Calcul d'isogénies entre Jacobiennes de courbes hyperelliptiques

Une extension naturelle du calcul d'isogénies entre courbes elliptiques est le cas des Jacobiennes de courbes hyperelliptiques (en particulier les courbes hyperelliptiques de genre 2 et 3). Le problème de calcul effectif d'isogénies entre des Jacobiennes a été initialement abordé en toute généralité dans les travaux de Cosset, Lubicz et Robert [CR15 ; LR12]. Ils ont proposé dans leurs articles des algorithmes qui calculent des $(\ell, \dots, \ell)$-isogénies séparables entre deux variétés abéliennes principalement polarisées de dimension g avec une complexité $\tilde{O}(\ell^g)$ si ℓ est un nombre premier, somme de deux carrés et différent de la caractéristique du corps de base et $\tilde{O}(\ell^{2g})$ dans le cas contraire. Une implémentation de ces algorithmes dans le logiciel MAGMA [BCP97] est disponible dans la bibliothèque AVIsogenies [BCR10] lorsque $g = 2$. Cependant l'entrée, et surtout la sortie, de ces algorithmes sont assez différentes des nôtres. D'autres algorithmes sont présents dans la littérature, parmi lesquels on peut citer ceux basés sur la construction de Richelot [CF96, Chapter 9] dans le cas $g = 2$ et $\ell = 2$, ceux basés sur une méthode algebro-géométrique introduite par Dolgachev et Lehavi [DL08] pour $g = 2$ et $\ell = 3$ et d'autres utilisant la construction trigonale de Recillas [Rec74] pour $g = 3$ et $\ell = 2$.
En caractéristique impaire ou nulle, des algorithmes quasi-linéaires en ℓ^g de calcul d'isogénies entre Jacobiennes de courbes de genre 2 et 3 ont été proposés par Couveignes, Ezome, Milio et Tian [CE15 ; Mil19 ; Tia20]. Ils reposent essentiellement sur le calcul de fonctions thêta algébriques sur les Jacobiennes et leurs quotients (par des sous-groupes isotropes maximaux) et la résolution de systèmes différentiels.

Applications du calcul d'isogénies

Avec l'arrivée de la cryptographie basée sur les courbes elliptiques et hyperelliptiques, les isogénies ont trouvé de nouvelles applications. Une des premières était l'algorithme

polynomial de Schoof-Elkies-Atkin (SEA) pour le comptage de points sur les courbes elliptiques [Sch95] qui améliore l'algorithme originel de Schoof. L'idée de l'algorithme de Schoof est de calculer la trace de l'action de l'endomorphisme du Frobenius sur les groupes de ℓ-torsion de la courbe, ℓ étant un nombre premier, ce qui permet de trouver la cardinalité de la courbe modulo ℓ. Il suffit donc de calculer cette trace modulo un nombre suffisamment grand de nombres premiers pour retrouver la cardinalité. Malgré la complexité polynomiale de cet algorithme, ce dernier est limité par la croissance quadratique du degré des polynômes de ℓ-division [1]. Les améliorations de Atkin et Elkies ont permis de calculer un petit facteur de ces polynômes en calculant des isogénies, ce qui a réduit la complexité de l'algorithme de Schoof.

Une seconde application qui a été abordée par Jao, Miller et Venkatesan [JMV05] est l'analyse de la difficulté du problème du logarithme discret sur les courbes elliptiques. Plus précisément, l'article montre que les isogénies peuvent être utilisées pour créer un algorithme randomisé qui réduit en temps polynomial le problème du logarithme discret sur un ensemble de courbes au même problème sur un nouvel ensemble de courbes significativement plus grand. La conclusion est que la difficulté de la résolution du problème du logarithme discret sur toutes les courbes de même ordre est la même.

Plus récemment, le calcul d'isogénies a servi à la construction de schémas cryptographiques résistant aux ordinateurs quantiques [DFJP14a]. Cette construction repose essentiellement sur la structure du graphe d'isogénies : les volcans d'isogénies [FM02]. Dans le cas des courbes supersingulières, cette structure est un graphe de Ramanujan dont les propriétés permettent la mise en place des protocoles cryptographiques post-quantiques. La cryptographie à base d'isogénies a de nombreux avantages, parmi lesquels un consensus plutôt large quant à sa sécurité vis-à-vis des attaques quantiques, des tailles de données (clefs, signatures, chiffrement, etc) très raisonnables, similaires à celles des cryptosystèmes actuels, et aussi une mise en œuvre quasi « plug and play » dans de nombreux protocoles de plus haut niveau déployés aujourd'hui.

En dimension supérieure, les isogénies peuvent être utilisées également dans le calcul du nombre de points sur les variétés abéliennes, en particulier les Jacobiennes des courbes de genre 2 [KPR20], et aussi au transfert du problème du logarithme discret d'une Jacobienne d'une courbe hyperelliptique de genre 3 à une autre où le logarithme discret est facile à résoudre [Smi09 ; Tia20]. Les graphes d'isogénies en dimension supérieure ont

1. Le polynôme de ℓ-division d'une courbe elliptique est un polynôme dont ses racines sont les abscisses des points de ℓ-torsion.

été récemment étudiés et utilisés pour introduire de nouveaux schémas cryptographiques post-quantiques [FT19 ; CS20]. En les comparant aux graphes d'isogénies de courbes elliptiques supersingulières, les graphes de dimension supérieure ont plus de sommets et leurs degrés sont plus élevés.
En plus des applications précédentes, nous pouvons citer également la construction de bases normales d'extensions de corps, de polynômes irréductibles, d'isomorphismes de corps finis, d'anneaux d'endomorphismes de variétés abéliennes, etc [CL09 ; CEL12 ; EL13 ; Nar18 ; Bri+19] .

Passage par les p-adiques

Précédemment, nous avons mentionné la méthode d'Elkies pour le calcul explicite d'isogénies entre courbes elliptiques qui ramène le problème à la résolution d'une équation différentielle. Lorsque la caractéristique du corps de base est grande ou nulle, cette équation différentielle peut être résolue directement par une méthode itérative de type Newton mais cela ne fonctionne malheureusement pas en petite caractéristique, auquel cas, il est nécessaire de passer par les p-adiques.
Cette stratégie est celle que nous allons suivre tout au long de cette thèse, aussi bien dans le cas des courbes elliptiques que dans celui des Jacobiennes de courbes hyperelliptiques. *In fine*, la stabilité numérique et l'efficacité de nos algorithmes reposeront sur une étude fine des équations différentielles p-adiques que nous serons amenés à manipuler. Les nombres p-adiques et les équations différentielles p-adiques joueront ainsi un rôle central tout au long de ce manuscrit.

Une première construction algébrique des nombres p-adiques a été découverte par Kurt Hensel vers la fin du 19-ième siècle [Hen97]. Depuis, leur étude s'est développée dans plusieurs directions. Les premiers travaux entrepris contenaient des résultats sur le principe local-global permettant l'étude des équations diophantiennes, allant jusqu'à leur résolution complètes dans certains cas favorables. Comme les nombres réels, les nombres p-adiques ont été étudiés d'une manière analytique dans les travaux de Robba et Christol dans lesquels sont abordés plusieurs thématiques : fonctions L p-adiques, équations différentielles p-adiques, *etc.* La théorie des nombres p-adiques a été utilisée dans plusieurs domaines mathématiques, notamment en géométrie arithmétique [Del74 ; Del80] (représentations galoisiennes p-adiques, relèvements canoniques, *etc*) et en cryptographie [Sat02] (comptage de points sur les variétés).

Au cours des dernières décennies, les méthodes p-adiques ont également pris une certaine importance dans le calcul symbolique. Depuis longtemps, les méthodes p-adiques ont été utilisés pour factoriser des polynômes à coefficients dans $\mathbb{Q}$ [LLL82] et résoudre des systèmes linéaires à coefficients entiers [Dix82]. Récemment, ils ont trouvé naturellement une place dans l'algorithmique et les calculs efficaces sur les corps finis, notamment dans les travaux de Bostan *et al.* [Bos+05] qui ont utilisé les sommes de Newton de polynômes sur $\mathbb{Z}_p$ pour calculer les produits composés pour des polynômes sur $\mathbb{F}_p$, Kedlaya [Ked01] et Lauder [Lau04] qui se sont servi de la cohomologie p-adique pour le comptage de points sur des courbes hyperelliptiques définies sur des corps finis, ainsi que les applications au calcul d'isogénies que nous avons déjà mentionnées.
La théorie des équations différentielles p-adiques, quant à elle, est un sujet relativement récent datant des années 60 avec les travaux de Dwork [Dwo60] sur la rationalité de la fonction Zeta d'une variété algébrique définie sur un corps de caractéristique positive et de Robba [Rob75 ; Rob76 ; Rob84] sur les opérateurs différentiels p-adiques. Depuis sa naissance, cette théorie n'a pas cessé d'évoluer grâce à son utilité dans différentes thématiques de recherche tels que la théorie de Hodge p-adique, le calcul numérique des fonctions zêtas, les cohomologies p-adiques, *etc.*
Au fil des décennies, elle est passée à travers plusieurs languages, le plus approprié étant celui de Berkovich [Ber88 ; Ber93]. L'usage de ce language a permis de contrôler le rayon de convergence, au sens de Berkovich, de ces équations et les travaux de Baldassarri [Bal10] ont aboutit à un résultat de continuité de ce rayon.
Hormis leur importance en théorie, les équations différentielles p-adiques interviennent également dans plusieurs applications, en particulier dans les travaux de Dwork pour étudier la variation de la fonction zeta d'une variété algébrique sur un corps fini (en se servant des équations différentielles hypergéométriques), de Bostan *et al.* pour calculer les sommes et produits composés pour des polynômes définis sur un corps fini et dans les algorithmes de calculs d'isogénies entre courbes elliptiques et Jacobiennes de courbes hyprelliptiques.
Soulignons pour conclure que, si la théorie des équations différentielles p-adiques *linéaires* a suscité beaucoup de travaux depuis son apparition, les équations différentielles p-adiques *non linéaires* n'ont été que peu étudiées et leur théorie en reste encore à ses balbutiements.

Résumé de la thèse

Cette thèse a pour objectif la conception d'algorithmes efficaces de calcul d'isogénies entre courbes elliptiques et Jacobiennes de courbes hyperelliptiques définies sur des corps finis basés sur la résolution effective d'équations différentielles, en particulier celles qui sont définies sur le corps des nombres p-adiques.

Problématique de la thèse

Grâce aux travaux d'Elkies publiés dans [Elk98], le problème de calcul d'isogénies entre courbes elliptiques peut être ramené à la résolution d'une équation différentielle ordinaire non linéaire. Cette approche fonctionne bien lorsque la caractéristique du corps de définition des courbes est égale à 0 ou est positive mais grande par rapport au degré de l'isogénie. Sous ces hypothèses, le calcul de la solution de l'équation différentielle se fait en calculant son développement en séries au voisinage d'un point par un schéma de Newton. Malheureusement, dans le cas des corps de petite caractéristique, des divisions par p peuvent apparaître et empêchent le calcul d'être mené à son terme. Ce problème a été contourné dans un article de Lercier et Sirvent [LS08] en relevant les deux courbes sur une extension K du corps des nombres p-adiques. Dans ce cas, les divisions par p peuvent être effectuées mais conduisent à des instabilités numériques si elles ne sont pas bien contrôlées. Il faut alors faire une analyse de précision très avancée afin d'obtenir des algorithmes à la fois efficaces et stables numériquement pour résoudre ces équations.
Typiquement, dans le cas de la caractéristique impaire, la première étude de précision menée par Lercier et Sirvent dans leur article conduisait à des pertes d'environ $O(\log^2 \ell)$ chiffres p-adiques (où ℓ désigne le degré de l'isogénie). Quelques années plus tard, en se basant sur les techniques p-adiques développées dans [CRV14], Lairez et Vaccon [LV16] ont proposé une version plus stable de l'algorithme de Lercier et Sirvent pour lequel les pertes de précisions sont limités à $\log \ell + O(1)$ chiffres significatifs, diminuant par là-même la complexité globale du calcul d'isogénies. On dispose donc dans le cas de la caractéristique impaire d'algorithmes de calcul d'isogénies trés efficaces, à la fois en théorie et en pratique.
Dans le cas précédent, les équations différentielles à résoudre sont des équations à variables séparées de la forme

$$y'(t) = g(t)h(y(t)) \tag{3}$$

où g et h sont deux séries entières à coefficients dans $\mathcal{O}_K$, l'anneau des entiers de K. En caractéristique paire, la résolution du problème de calcul d'isogénies est plus com-

pliquée. L'équation différentielle 2-adique que l'on obtient n'a pas la même forme que l'équation (3). Elle s'écrit

$$t(t-4a)u(t)^2y'(t)^2 = h(y(t)) \tag{4}$$

où $u, h \in \mathcal{O}_K[\![t]\!]$ et $a \in \mathcal{O}_K^*$. Ceci est dû au fait que l'équation d'une courbe elliptique en caractéristique 2 provient d'une extension d'Artin-Schreier : elle s'écrit sous la forme $y^2 + xy = x^3 + a_2x^2 + a_6$. En particulier, on observe que le polynôme en facteur de $y'(t)^2$ admet une racine de norme p-adique égale à $1/4$; l'équation (4) présente ainsi des singularités dans le domaine de convergence de son unique solution. Une autre complication, est dûe à la présence d'un carré sur $y'(t)$ dans l'équation, qui indique que la résolution va devoir passer à un moment par l'extraction de racines carrées qui est une opération instable dans les 2-adiques.

Comme dans le cas des courbes elliptiques, le calcul d'isogénies entre Jacobiennes de courbes hyperelliptiques peut être ramené à un problème de résolution d'équations différentielles, p-adiques lorsque la caractéristique du corps de base est petite par rapport au degré de l'isogénie. Cependant, dans cette nouvelle situation, on est confronté à un *système* d'équations différentielles p-adiques couplées de la forme

$$H\left(Y(t)\right) \cdot Y'(t) = G(t) \tag{5}$$

où H est une application analytique $H\colon \mathcal{O}_K[\![t]\!]^g \to M_g(\mathcal{O}_K[\![t]\!])$ de la forme

$$H(x_1(t), \ldots, x_g(t)) = (f_{ij}(x(t)))_{ij}$$

avec $f_{ij} \in \mathcal{O}_K[\![t]\!]$, $G(t) \in \mathcal{O}_K[\![t]\!]^g$ et $Y(t) \in \mathcal{O}_K[\![t]\!]^g$ est l'inconnue [CE15]. La question qui se pose est alors la même que dans le cas de la dimension 1 : obtenir des algorithmes à la fois efficaces et stables numériquement pour résoudre de telles équations.

Contributions

Nos contributions concernent essentiellement la résolution des équations (4) et (5). Nos méthodes reposent sur le théorème suivant de Caruso, Vaccon et Roe (appelé lemme de précision).

Théorème 1 ([CRV14])**.** *Soient $m, n \in \mathbb{N}^*$ et $f : U \to \mathbb{Q}_p^m$ une application définie sur un ouvert U de $\mathbb{Q}_p^n$. On suppose que f est strictement différentiable en un point $x_0 \in U$ et que $df(x_0)$ est surjective. Alors, pour tout $\rho \in]0,1]$, il existe $\delta > 0$ tel que, pour tout $r \in]0,\delta[$, pour tout réseau H compris entre les boules $B(0,\rho r)$ et $B(0,r)$ de $\mathbb{Q}_p^n$, nous avons la relation suivante*

$$f(x_0 + H) = f(x_0) + df(x_0) \cdot H.$$

Ce résultat nous permet d'évaluer la perte de précision optimale de nos problèmes par un simple calcul différentiel.

Étude de l'équation (4)**.** Dans un premier temps, en collaboration avec mes deux directeurs de thèse Xavier Caruso et Reynald Lercier, nous abordons l'étude théorique des propriétés de l'équation (4) et sa résolution. Après avoir montré que l'équation (4) admet une unique solution, nous concevons un algorithme basé sur une itération de Newton pour calculer une approximation de cette solution.
Pour estimer la perte de précision (optimale) de l'algorithme, nous construisons une fonction localement analytique f à laquelle nous appliquons le lemme de précision. Malheureusement, le Théorème 1 ne donne pas une condition explicite sur le réseau H pour que la conclusion $f(x_0 + H) = f(x_0) + df(x_0) \cdot H$ ait lieu. Lorsque la fonction f est localement analytique, il s'avère qu'une telle condition peut être explicitée (au prix d'un certain effort) en bornant les normes des différentielles d'ordre supérieur de f ; c'est l'approche qui a été utilisée dans [LV16] pour faire l'analyse de précision. Dans notre cas, il est plus difficile de majorer les normes des différentielles d'ordre supérieur à cause de la forme complexe que prend l'équation (4). Nous contournons ce problème en observant que la fonction f vérifie elle-même une équation différentielle dans un espace fonctionnel, qui prend la forme générale :

$$df = g \circ (f, h)$$

(où g et h sont des fonctions explicites), puis en utilisant cette équation pour majorer la taille les dérivées successives de f. Précisément, si $\Lambda(f)$ désigne la transformation de Legendre de la fonction convexe associée au polygone de Newton de f, nous obtenons une borne sur la fonction :

$$\Lambda(f)_{\geq 2} : x \mapsto \inf_{y \geq 0} \Big(\Lambda(f)(x+y) - 2y \Big).$$

qui nous permet finalement de conclure grâce à la proposition suivante.

Proposition 1 ([CRV14, Proposition 3.12])**.** *Soient E et F deux espaces vectoriels de dimension finie. Soit $f : E \to F$ une fonction localement analytique. Soit $C \in \mathbb{R}_+^*$ tel que $B_F(1) \subset df(B_E(C))$. Soit $\rho \in]0, 1]$ et $\upsilon \in \mathbb{R}$ tel que*

$$\Lambda(f)_{\geq 2}(\upsilon) < \upsilon + \log\left(\frac{\rho}{C}\right).$$

Alors la conclusion du Théorème 1 est satisfaite pour $\delta = e^{\upsilon}$.

L'algorithme que nous construisons, ainsi que son analyse de précision, nous donne *in fine* le théorème suivant.

Théorème 2. *Soit K une extension finie de $\mathbb{Q}_2$. Soit $\mathcal{O}_K$ son anneau d'entiers et $\mathcal{O}_K^\times$ l'ensemble des éléments inversibles de $\mathcal{O}_K$. Il existe un algorithme qui prend en entrée*

- *deux entiers positifs n and N,*
- *deux éléments $a, b \in \mathcal{O}_K^\times$,*
- *deux séries $u, v \in \mathcal{O}_K[\![t]\!]$ avec $u(0) \in \mathcal{O}_K^\times$*

et, qui lorsque l'équation différentielle en z

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

admet une unique solution dans $t\cdot\mathcal{O}_K[\![t]\!]$, retourne la solution modulo $(2^N, t^n)$ avec une complexité en temps égale à $O(\mathrm{M}(n) + \mathrm{C}_h(n))$ opérations dans $\mathcal{O}_K$ à une précision $O(2^M)$ avec $M = \max(N, 3) + \lfloor \log_2(n) \rfloor + 2$.

Application au calcul d'isogénies en caractéristique 2. Par la méthode d'Elkies, le Théorème 2 nous fournit directement un algorithme de calcul d'isogénies de complexité quasi-optimale en caractéristique 2, à condition de connaître des modèles de Weierstrass des courbes isogènes et la constante de normalisation.
Supposons toutefois à présent qu'on connaisse uniquement une courbe elliptique E définie sur un corps de caractéristique 2 et ℓ un nombre premier d'Elkies[2]. On suppose que $\mathrm{End}(E)$ est un ordre maximal d'un corps quadratique imaginaire. Si la taille du corps de définition de E est très petite par rapport à ℓ, à un endomorphisme prés, une ℓ-isogénie I s'écrit comme composée d'isogénies de petits degrés. Nous obtenons ainsi une chaine de

2. La condition d'être Elkies implique qu'il existe une ℓ-isogénie partant de E

la forme

$$E \xrightarrow{\alpha} E \overbrace{\xrightarrow{I_1} E_1 \xrightarrow{I_2} E_2 \longrightarrow \cdots \xrightarrow{I_{n-1}}}^{I} \widetilde{E} \xrightarrow{\beta} \widetilde{E}\,. \tag{7}$$

En remplaçant E dans la Chaine (7) par son relevé canonique, nous sommes en position d'utiliser le théorème 2 car une équation de $\widetilde{E}$ ainsi que la constante de normalisation de I peuvent à présent être calculées à l'aide des formules de Vélu et des images de α et β dans la structure abstraite de l'anneau d'endomorphisme de E (qui nous permettent de trouver les constantes de normalisations associées aux endomorphismes α et β). Nous obtenons ainsi le théorème suivant

Théorème 3. *Étant donnés une courbe elliptique ordinaire E définie sur un corps fini k de caractéristique p et cardinalité $q = p^n$ tel que l'anneau d'endomorphisme de E est un ordre maximal d'un corps quadratique imaginaire et ℓ un nombre d'Elkies pour E, il existe un algorithme qui calcule une équation d'une courbe elliptique ℓ-isogène à la courbe E et une représentation rationnelle de l'isogénie avec une complexité en temps égal à $\tilde{O}(n\,\ell + p^2 + q^{3/2})$.*

Construction de polynômes irréductibles. L'algorithme évoqué dans le paragraphe précédent permet la construction de polynômes irréductibles de grands degrés sur des petits corps en partant d'une idée de Couveignes et Lercier [CL13]. Même si leur algorithme a une complexité théorique quasi-linéaire en le degré, il est difficile d'atteindre cette complexité en pratique, surtout en caractéristique 2, à cause de l'utilisation de l'algorithme de Kedlaya-Umans [KU11] pour calculer la composée d'isogénies. Nous adaptons l'algorithme de Couveignes et Lercier pour la construction de polynômes irréductibles en caractéristique 2. Une implémentation en MAGMA de notre variante de l'algorithme nous a permis de trouver des polynômes irréductibles de degrés de l'ordre du million en moins d'une minute sur un ordinateur portable.

Étude de l'équation (5). Dans un second temps, nous abordons l'étude du système différentiel (5) pour le calcul d'isogénies entre Jacobiennes de courbes hyperelliptiques en caractéristique impaire. La situation est similaire à celle de l'équation (3) sauf que son étude est plus technique du fait qu'on est confronté à un système à plusieurs équations, et non plus à une seule. En se servant toujours du lemme de précision, nous obtenons le théorème suivant.

Théorème 4. *Soit p un nombre premier. Soit K une extension finie de $\mathbb{Q}_p$ et $\mathcal{O}_K$ son anneau d'entiers. Il existe un algorithme qui prend en entrée*

- *trois entiers positifs n,g et N,*
- *une fonction analytique $H : \mathcal{O}_K[\![t]\!]^g \to M_g(\mathcal{O}_K[\![t]\!])$ de la forme $H(y_1(t), \cdots, y_g(t)) = (f_{ij}(y(t)))_{ij}$ avec $f_{ij} \in \mathcal{O}_K[\![t]\!]$,*
- *un vecteur $G(t) \in \mathcal{O}_K[\![t]\!]^g$,*

et, qui lorsque l'équation différentielle en X

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

admet une unique solution dans $(t\mathcal{O}_K[\![t]\!])^g$, retourne une approximation de sa solution modulo (p^N, t^{n+1}) avec une complexité en temps égale à $O\left(\mathrm{MM}(g,n) + \mathrm{C}_H(n)\right)$ opérations dans K, où $\mathrm{MM}(g,n)$ est le nombre d'opérations arithmétiques pour calculer le produit de deux matrices de taille $g \times g$ contenant des polynômes de degrés inférieur à n, $\mathrm{C}_H(n)$ est le nombre d'opérations arithmétiques nécessaire pour calculer $H(X(t)) \mod t^n$, à une précision égale à $O(p^M)$ avec $M = \max(N,3) + \lfloor \log_p(n) \rfloor$ si $p = 2$, $M = \max(N,2) + \lfloor \log_p(n) \rfloor$ si $p = 3$ et $M = N + \lfloor \log_p(n) \rfloor$ sinon.

Application au calcul d'isogénies. Dans le cas d'un calcul d'isogénies en genre g, la complexité évoquée dans le Théorème 4 peut être réduite à $\tilde{O}(gn)$ opérations dans une extension du corps de base de l'isogénie. Malheureusement, le degré de cette extension peut être très grand par rapport à g, pouvant théoriquement aller jusqu'à atteindre $g!$. La complexité de l'algorithme du Théorème 4, bien que restant quasi-linéaire en n semble donc pouvoir exploser vis-à-vis du paramètre g. Par conséquent, ce théorème ne fournit *a priori* un algorithme efficace pour le calcul explicite d'une représentation rationnelle d'une $(\ell, \ldots, \ell)$-isogénie que pour les Jacobiennes de courbes hyperelliptiques de petit genre g. Ces propos doivent être néanmoins nuancés car il se trouve qu'en pratique, on n'atteint jamais la borne théorique $g!$ pour le degré de l'extension et que l'algorithme résultant reste compétitif, même en genre grand.

Malgré tout, il ne fait aucun doute que la complexité de l'algorithme du Théorème 4 vis-à-vis du genre g n'est pas optimale. Comme nous l'avons dit, ceci est dû au fait que les composantes de la solution $X(t) = (x_1(t), \ldots, x_g(t))$ de l'équation (5) ne sont pas définis sur le corps de base mais sur une extension de degré possiblement grand. Cependant, les fractions rationnelles de l'isogénie sont calculées à partir des coefficients du polynôme en

z, $U(t,z) = \prod_{i=1}^{g}(z - x_i(t))$, qui eux, sont définis sur le corps de base. Pour cette raison, nous revisitons l'algorithme du Théorème 4 en travaillant directement sur le polynôme U pour le rendre également quasi-linéaire en g.

Calcul des polynômes de Cantor de ℓ-division. Les polynômes de Cantor de ℓ-division sont, par définition, les numérateurs et les dénominateurs des composantes d'une représentation rationnelle de l'endomorphisme de la multiplication par ℓ. Comme dans le cas elliptique, ils jouent un rôle primordial dans les algorithmes de comptage de points sur les courbes hyperelliptiques. Les algorithmes classiques pour calculer la multiplication par ℓ sont généralement basés sur les formules récursives de Cantor [Can94] ou un algorithme plus direct qui applique les opérations d'additions de la Jacobienne sur un point générique [Abe18]. Cependant, leur complexité théorique n'a pas été bien étudiée.
L'algorithme du Théorème 4 donne une nouvelle approche à la fois simple et efficace pour calculer une représentation rationnelle de la multiplication par ℓ, mais nécessite de connaître par avance des majorations sur les degrés de ses composantes. Jusqu'à présent, la meilleure borne connue sur ces degrés était en $O_g(\ell^3)$ (où la notation O_g signifie que la constante cachée dans le O dépend de g) [Abe18, Section 4.2]. Nous améliorons ce résultat en démontrant le théorème suivant.

Théorème 5. *Étant donnés deux entiers g et ℓ, les polynômes de Cantor de ℓ-division sur une courbe hyperelliptique de genre g sont de degré au plus $4g\ell^2 + g + 1$.*

À partir de ce résultat, nous déduisons un algorithme de *complexité quasi-optimale* en g et en ℓ pour calculer une représentation rationnelle de la multiplication par ℓ sur une courbe hyperelliptique de genre g.

Organisation du manuscrit

Chapitre 1 Dans ce chapitre, nous proposons un algorithme de calcul d'isogénies entre courbes elliptiques définies sur une extension de $\mathbb{Q}_2$. Il repose essentiellement sur la résolution effective d'une équation différentielle 2-adique avec une perte de précision logarithmique en le degré de l'isogénie. Nous donnons quelques applications, notamment au calcul en temps quasi-linéaire des isogénies entre courbes elliptiques et de polynômes irréductibles de degrés grands sur des corps finis de petite caractéristique.

Chapitre 2 Nous étudions dans ce chapitre le calcul d'un vecteur de séries entières $X(t)$, solution d'un système d'équations différentielles p-adiques couplées. Nous proposons un algorithme numériquement stable qui détermine une approximation de cette solution avec une perte de précision logarithmique en le nombre des coefficients $X(t)$.

Chapitre 3 Dans ce chapitre, nous nous intéressons au calcul explicite d'une représentation rationnelle d'une isogénie entre Jacobiennes de courbes hyperelliptiques définies sur des corps finis de caractéristique impaire. Pour cela, nous proposons un algorithme quasi-optimal qui calcule une représentation rationnelle par un simple calcul d'une approximation de la solution d'un système d'équations différentielles p-adiques. Nous déduisons une méthode efficace pour calculer des polynômes de Cantor de ℓ-division sur une courbe hyperelliptique.

Chapitre 4 Ce chapitre est un premier pas vers les équations différentielles p-adiques non linéaires. Nous prouvons un résultat de semi-continuité du rayon de convergence des équations différentielles étudiées au Chapitre 1.

Publications

Chapter 1

Fast computation of elliptic curve isogenies in characteristic two

---

In this chapter, we propose an algorithm that calculates isogenies between elliptic curves defined over a finite extension K of $\mathbb{Q}_2$. It consists of 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 small characteristic isogenies of elliptic curves and irreducible polynomials, both in quasi-linear time in the degree.

1.1 Overview

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 $I : E \to \tilde{E}$ of degree ℓ 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 [Bos+08; 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:

$$E : y^2 = x^3 + a_2\,x^2 + a_4\,x + a_6 \quad \text{and} \quad \tilde{E} : y^2 = x^3 + \tilde{a}_2\,x^2 + \tilde{a}_4\,x + \tilde{a}_6. \tag{8}$$

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

$$I(x, y) = (\eta(x),\, c\,y\,\eta'(x)) \tag{9}$$

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 (one-dimensional) 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 Equations (8) and (9), we realize that the computation of I reduces to solving the following nonlinear differential equation:

$$c^2 \cdot (x^3 + a_2\, x^2 + a_4\, x + a_6) \cdot \eta'^2 = \eta^3 + \tilde{a}_2\, \eta^2 + \tilde{a}_4\, \eta + \tilde{a}_6. \tag{10}$$

For several reasons, it is convenient to perform the change of variables $t = 1/x$ and the change of functions $z(t) = 1/\eta(x)$. Equation (10) then becomes

$$c^2 \cdot (t + a_2 t^2 + a_4 t^3 + a_6 t^4) \cdot z'^2 = z + \tilde{a}_2 z^2 + \tilde{a}_4 z^3 + \tilde{a}_6 z^4\,. \tag{11}$$

When k has characteristic 0, Bostan *et al.* [Bos+08] proposed to solve Equation (11) using a well-designed Newton iteration. This strategy allows them to compute $z(t)$ mod $t^{2\ell+1}$ 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 sharp analysis of the loss 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 $y^2 = x^3 + a_2x^2 + a_4x + a_6$ but $y^2 + xy = x^3 + a_2x^2 + a_6$. As a consequence, the differential equation we need to study, which is defined over the 2-adics, now takes the form

$$c^2 \cdot \Big(4t + (4a_2{+}1)t^2 + 4a_6t^4\Big) \cdot z'^2 = 4z + (4\tilde{a}_2{+}1)z^2 + 4\tilde{a}_6z^4 \tag{12}$$

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, Equation (12) is much more difficult to handle than Equation (11). One reason is structural: the polynomial in front of z'^2, namely $4t + (4a_2+1)t^2 + 4a_6t^4$, 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 Equation (12) will require extracting 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 chapter, we reconsider the 2-adic case and propose a new algorithm to solve Equation (12). 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 1.2.

Theorem (See Theorem 1.2.10 and Proposition 1.2.11)**.** *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

$$t(t-4a)\,u(t)^2\,z'^2 = z\,(z-4b)\,v(z)^2 \tag{13}$$

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] (see Section 1.4.3).

1.2 Fast resolution of a 2-adic differential equation

This section is devoted to the effective resolution of the nonlinear differential equation (13), leading eventually to the proof of our main theorem. In more details, the computation model we will use throughout this paper is introduced in Section 1.2.1. The two next subsections are concerned with preliminary material: we show that Equation (13) has a unique solution in certain cases and study a pair of linear differential equations that will eventually play quite an important role. Our algorithm is presented in Section 1.2.4 and the proof of its correctness is explained in Section 1.2.5.

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 υ_2 and will always assume that it is normalized by $\upsilon_2(2) = 1$. 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 $\upsilon_2(\pi) = 1/e$. 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 $\upsilon_2(x) = M$ when $x = 0$ and $\upsilon_2(x) = \upsilon_2(\hat{x})$ where $\hat{x} \in \mathcal{O}_K$ is any lifting of x otherwise.

1.2.1 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 chapter, 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:

$$\begin{aligned}\big(x+O(2^M)\big)+\big(y+O(2^M)\big)&=(x+y)+O(2^M)\,,\\ \big(x+O(2^M)\big)-\big(y+O(2^M)\big)&=(x-y)+O(2^M)\,,\\ \big(x+O(2^M)\big)\times\big(y+O(2^M)\big)&=xy+O(2^M)\,.\end{aligned}$$

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 if $v_2(y) > v_2(x)$,
— returns $0 + O(2^M)$ if $x = 0$ in $\mathcal{O}_K/\pi^{eM}\mathcal{O}_K$,
— returns any representative $z + O(2^M)$ 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 can perform 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 algorithms that carry out these arithmetic operations. 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 $\mathrm{A}(K; M) \in \tilde{O}(dM)$ (reducing polynomial multiplications to integer ones with Kronecker substitution method [Kro82; Sch82]). 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 arithmetic operations in the base ring it performs). For convenience, we will also suppose that the function M satisfies the superadditivity assumption, that is: for all $n, n' \in \mathbb{N}$,

$$\mathrm{M}(n + n') \geq \mathrm{M}(n) + \mathrm{M}(n').$$

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.

1.2.2 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:

$$U \cdot z'^2 = V \circ z\,. \tag{14}$$

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 (14) 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 Equation (14).

Proposition 1.2.1. *Assuming that U and V have t-adic valuation* 1*, the differential equation* (14) *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 Equation (14) of the form $z = \sum_{n=1}^{\infty} z_n\, t^n$. Taking the n-th derivative of Equation (14) (and using Faà di Bruno's formula to evaluate the successive derivatives of $V \circ z$), we end up with the relations

$$\sum_{i=0}^{n-1} \sum_{j=0}^{i} (j+1)(i-j+1) z_{j+1} z_{i-j+1} u_{n-i} = \sum_{k_1+2k_2+\cdots+nk_n=n} \frac{(k_1+k_2+\cdots+k_n)!}{k_1!\,k_2!\,\cdots\,k_n!}\, v_{k_1+k_2+\ldots+k_n}\, z_1^{k_1} z_2^{k_2} \cdots z_n^{k_n}\,. \tag{15}$$

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 v_1/u_1 since u_1 and v_1 are nonzero scalars. 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 Equation (15) and the summand indexed by $(k_1, \ldots, k_n) = (0, \ldots, 0, 1)$ in the right hand side. Isolating them since $v_1 \neq 0$ by hypothesis, 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 Equation (14). □

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 1.2.2. Both Assumptions (H_U) and (H_V) are fulfilled for the differential equation (12) (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 explicitly given by

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

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. Finally, letting $u = c\sqrt{U_0}$, 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 1.2.3. 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 $E'/\mathbb{F}_{2^d} : y^2 + xy = x^3 + a_6$ by 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 Equation (12) 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 Equation (14) under Assumptions (H_U) and (H_V).

1.2.3 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 (14). Precisely, given $a \in \mathcal{O}_K^\times$, we consider

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

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 1.2.4. *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 for all $i \geq 0$,*

$$v_2(y_i) \geq \min_{0 \leq k \leq i} v_2(f_k) - \lfloor \log_2(i+1) \rfloor - 1\,;$$

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

$$\begin{aligned} & v_2(y_0) = v_2(f_0) - 1\,, \\ & v_2(y_1) \geq \min\Big(v_2(f_0) - 2,\, v_2(f_1) - 1\Big)\,, \\ \forall i \geq 2, \quad & v_2(y_i) \geq \min_{2\leq k\leq i} v_2(f_k) - \lfloor \log_2(i-1) \rfloor - 1\,. \end{aligned}$$

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

$$y_0 = -\frac{f_0}{2a}, \quad y_i = \frac{i\, y_{i-1} - f_i}{2a \cdot (2i+1)} \quad \text{for } i > 0. \tag{16}$$

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

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

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

$$v_2\left(\frac{2^{k-i-1} i!}{k!}\right) = (k - i - 1) + (i - S_2(i)) - (k - S_2(k)) = -S_2(i) + S_2(k) - 1\,. \qquad \square$$

The first part of Proposition 1.2.4 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 1.2.4 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 1.2.5. *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. $\square$

Algorithm 1: Linearized equation solver

`LinDiffSolve` (a, f, n)

Input : $a \in \mathcal{O}_K^\times$, $n \in \mathbb{N}$ and $f = \sum_{i=0}^{n-1} f_i t^i \in K[\![t]\!]/(t^n)$

Output: $\psi_{+,n}(f)$

$y_0 := \frac{-f_0}{2a}$

for $i := 1$ **to** $n-1$ **do**

$\quad y_i := \dfrac{iy_{i-1} - f_i}{2a \cdot (2i+1)}$;

return $\sum_{i=0}^{n-1} y_i t^i$;

We now move to the effective computation of ψ_+. Following the proof of Proposition 1.2.4, we directly get Algorithm 1, whose numerical stability is studied in Proposition 1.2.6 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 1.2.6. *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 in $\mathcal{O}_K$ 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 1.2.4 (applied with h) shows that $\psi_{+,n}(h) \in \pi^{eN}\mathcal{O}_K[\![t]\!]/(t^n)$. Hence $y \equiv \psi_{+,n}(f) \pmod{(\pi^{eN}, t^n)}$, which exactly means that y is correct at precision $O(2^N)$. □

Remark 1.2.7. It follows from the specifications on our computation model that, when the first m coefficients of f vanish, the m first coefficients of the output of `LinDiffSolve`(a, f, n) vanish as well.

1.2.4 The algorithm

We go back to the nonlinear differential equation (14) 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 Equation (14) 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

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

Identifying both terms, we obtain the relation

$$2\, U(t)\, z'_m \cdot h' - V'(z_m) \cdot h \;\equiv\; V(z_m) - U(t) \cdot {z'_m}^2 \pmod{t^{2m-1}}. \tag{17}$$

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 Equation (17), 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 1.2.3, 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 1.2.8. *We assume* (H_U). *Let $m > 1$ be an integer and let $z_m \in K[\![t]\!]$ be a solution of Equation* (14) *modulo t^m. Then*

$$z_m + z'_m u \cdot \psi_- \left(\frac{1}{2u(t)^3}\left(\frac{V(z_m)}{{z'_m}^2} - U(t)\right)\right) \tag{18}$$

is a solution of Equation (14) *modulo t^{2m-1}.*

It would be reasonable to expect that Proposition 1.2.8 could be easily turned into an

algorithm that solves the nonlinear differential equation (14). However, for several reasons (related to the precision analysis), we shall modify a bit our Newton iteration. From 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

$$z_m = \lambda t + t(t-4a)\, q_m \tag{19}$$

with $q_m \in K[\![t]\!]/(t^{m-1})$. So, z_m is a solution of Equation (14) modulo t^m if and only if q_m satisfies

$$W(t, q_m) \equiv u(t)^2 {z'_m}^2 \pmod{t^{m-1}}. \tag{20}$$

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 1.2.8, we obtain the following corollary.

Corollary 1.2.9. *We assume* (H_U) *and* (H_V). *Let $m > 1$ be an integer and let q_m be a solution of Equation* (20) *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 Equation (20) *modulo t^{2m-1}.*

Proof. The formula is easily obtained by plugging Equation (19) in Equation (18), and using Lemma 1.2.5. □

With Corollary 1.2.9 and a small optimization consisting of integrating the computation of $(z'_m)^{-2}$ in our Newton scheme, we get Algorithm 4 (`DiffSolve`) and Algorithm 3 (`IsoSolve`).

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 1.2.10. *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 Equation* (14) *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 $O(2^N)$.*

Algorithm 2: Non linear differential equation solver

`DiffSolve` $(a,\ u,\ u^2,\ u^{-3},\ b,\ v^2,\ n)$

Input : $u, u^2, v^2 \bmod t^n,\ u, u^{-3} \bmod t^{\lceil n/2 \rceil},\ a$ and b satisfying (H_U) and (H_V)

Output: $q_n \mod t^n,\ (z_n')^{-2} \bmod t^{\lceil n/2 \rceil}$

if $n \leq 1$ **then**
  return $v_1 u_1^{-1}(ba^{-1} - 4a)^{-1} \bmod t^n,\ 0 \bmod t^{n-1}$;
$m := \lceil \frac{n-1}{2} \rceil$;
$q_m, r_m :=$ `DiffSolve`$(a,\ u,\ u^2,\ u^{-3},\ b,\ v^2,\ m)$; `// recursive call`
$z_m := ba^{-1}t + t(t-4a)q_m \bmod t^{n+1}$;
$w_n := {z_m'}^2 \bmod t^n$; `// 1 coeff. lost`
$s_n := u^2 \cdot w_n - W \circ q_m \mod t^n$; `//` $s_n \bmod t^m = 0$
$r_n := r_m \cdot (2 - r_m \cdot w_n) \bmod t^{n-m}$; `//` $(z_n')^{-2}$ `(Newton iter.)`
$f_n := 2^{-1}\, s_n \cdot r_n \cdot u^{-3} \bmod t^n$; `// The argument of` ψ_+
$y_n :=$ `LinDiffSolve`$(a,\ f_n,\ n)$; `//` $y_n \bmod t^m = 0$
return $q_m + z_m' \cdot u \cdot y_n \bmod t^n,\ r_n$

Algorithm 3: Isogeny differential equation solver

`IsoSolve` $(U,\ V,\ n)$

Input : $U, V \bmod t^n$ satisfying Assumptions (H_U) and (H_V)

Output: the solution $z_n \mod t^n$ of Equation (14)

Compute a, b, $U_0 \bmod t^{n-1}$ and $V_0 \bmod t^{n-1}$; `//` $U_0 = u^2$ `and` $V_0 = v^2$
Compute $u \bmod t^{\lceil (n-1)/2 \rceil}$ and $u^{-3} \bmod t^{\lceil (n-1)/2 \rceil}$;
$z :=$ `DiffSolve`$(a,\ u,\ u^2,\ u^{-3},\ b,\ v^2,\ n-1)$;
return $ba^{-1}t + t(t-4a)\, z \bmod t^n$

We delay the proof of Theorem 1.2.10 to Section 1.2.5. 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 1.2.11. *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 1.2.12. *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 1.2.11 (combined with the fact that the three algorithms only performs operations in $\mathcal{O}_K$ as promised by Theorem 1.2.10). □

Remark 1.2.13. It is faster to compute the composition of two isogenies with Algorithm 3 than to compute each isogeny independently and then perform their compositions.

1.2.5 Precision analysis

The aim of this section is to prove Theorem 1.2.10. 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:

$$t(t-4a)\cdot z'^2 = g(t)^2\cdot V(z). \tag{21}$$

We are going to study how the solution z of the latter differential equation behaves when g varies. By Proposition 1.2.1, we know that Equation (21) has a unique nonzero solution $z_g \in tK[\![t]\!]$ as soon as $g(0) \neq 0$. Besides, the proof of Proposition 1.2.1 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

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

(we note that $t-4a$ is invertible in $K[\![t]\!]/(t^n)$). It follows from the proof of Proposition 1.2.1 that φ_n is a polynomial function in $g(0)^{-1}$ and the coefficients of g; in particular, it is locally analytic.

Proposition 1.2.14. *For $g \in \Omega_n$, the differential of φ_n at g is the function*

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

where $\psi_{+,n}$ is the function defined in Section 1.2.3.

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:

$$2t(t-4a)\; z'_g\cdot\delta z' = 2g(t)\;\delta g(t)\;V(z_g) + g(t)^2\;V'(z_g)\cdot\delta z. \tag{22}$$

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

$$\begin{aligned} t(t-4a)(z'_g)^2 &= g^2\,V(z_g)\\ 2t(t-4a)z'_g z''_g + 2(t-2a)(z'_g)^2 &= g^2 z'_g\,V'(z_g) + 2gg'\,V(z_g)\end{aligned}$$

(the second one being obtained from the first one by derivation), Equation (22) 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 1.2.5. 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 confusion, 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

$$\Big\|a_0+a_1x+\cdots+a_{n-1}x^{n-1}\Big\|_{F_n} = \max\Big(|a_0|,|a_1|,\ldots,|a_{n-1}|\Big).$$

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 1.2.15. *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 1.2.14. □

We now fix a series $g \in \mathcal{O}_K[\![t]\!]/(t^n)$ satisfying the assumptions of Lemma 1.2.15. 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 1.2.14 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

$$\Lambda(f)(x) = \begin{cases} \log\left(\sup\limits_{\gamma \in B_{E_n}(e^x)} \|f(\gamma)\|\right) & \text{if } f \text{ is defined over } B_{E_n}(e^x)\,, \\ \infty & \text{else}\,. \end{cases} \tag{23}$$

The notation "log" refers to the logarithm with base e.
We define $\Lambda(f)_{\geq 2}(x) = \inf\limits_{y \geq 0}(\Lambda(f)(x+y) - 2\,y)$ too.

Lemma 1.2.16. *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 1.2.17. *Under the assumption of Lemma 1.2.15, 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 1.2.16, 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 1.2.15. □

Remark 1.2.18. Using that φ_n is injective, we see that Proposition 1.2.17 implies that

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

as soon as g satisfies the assumption of Lemma 1.2.15 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 when restricted to the ball of centre g and radius $1/4$.

Correctness proof of Theorem 1.2.10. Let U, V and n be the input of Algorithm 3. We first claim that the output of Algorithm 2 satisfies

$$W(t, q_n) \equiv u^2 \cdot {z'_n}^2 \pmod{t^{n-1}, 2^M} \tag{24}$$

for all n. We shall prove it by induction on n. The case $n = 1$ is easy. Let $m \geq 1$ be a positive integer and $n = 2m - 1$. We suppose that Equation (24) 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

$$V(z_m) \equiv t(t{-}4a) \cdot W(t, q_m) \pmod{t^n}. \tag{25}$$

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 Equation (25), 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 1.2.7 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

$$\begin{aligned} W(t,q_n) &\equiv W(t,q_m) + z'_m u\, y_n \cdot \frac{\partial W}{\partial x}(t,q_m) \pmod{t^{n-1}, 2^M} \\ &\equiv W(t,q_m) + z'_m u\, y_n \cdot V'(z_m) \pmod{t^{n-1}, 2^M}. \end{aligned} \tag{26}$$

Besides, by definition of y_n, we have the relation

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

from which we derive

$$W(t,q_m) - u^2 {z'_m}^2 \equiv 2u^3 {z'_m}^2 \cdot \Big(t(t-4a)y'_n + (t-2a)y_n\Big) \pmod{t^{n-1}, 2^M}. \tag{27}$$

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

$$u^2\, {z'_n}^2 \equiv u^2\, {z'_m}^2 + 2u^2\, z'_m \Big(t(t-4a)z'_m u\, y_n\Big)' \pmod{t^{n-1}, 2^M}. \tag{28}$$

Combining Equations (26), (27) and (28), 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 Equation (25), we finally conclude that Equation (24) holds true for n; our claim is proved.

Multiplying Equation (24) 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 Re-

marks 1.2.2 and 1.2.3). 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 1.2.18, 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 1.2.6, 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 $\mathcal{O}_K[\![t]\!]$. □

1.3 Experiments

We made an implementation of both Algorithm 3 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 1.1, page 53). The degree 11 toy example presented below was computed with this software as well.

1.3.1 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 integers of $\mathbb{Q}_2(\sqrt{-7})$, the class group of which is trivial. In particular, 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 1.4.2), 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

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

from which it is easy to compute u and u^{-3}. All precomputations of Algorithm 3 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

$$\begin{aligned}
&z_0 = 41\,t + 10\,t^2 + O(2^9,t^3)\,, \quad && s_0 = 164\,t + O(2^9,t^2)\,, && r_0 = 113 + 152\,t + O(2^9,t^2)\,,\\
&f_0 = 228\,t + O(2^9,t^2)\,, && y_0 = -211\,t + O(2^9,t^2)\,, && q_1 = 10 - 43\,t + O(2^9,t^2)\,.
\end{aligned}$$

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

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

and a last iteration finally yields

$$\begin{aligned}
z_{11} &= 41\,t + 94\,t^2 + 5\,t^3 + 116\,t^4 + 210\,t^5 + 82\,t^6 - 201\,t^7 + 188\,t^8 + \\
&\qquad 214\,t^9 + 40\,t^{10} + 156\,t^{11} - 180\,t^{12} + O(2^9,t^{13})\,,\\
s_{11} &= 200\,t + 48\,t^2 - 4\,t^3 - 32\,t^4 + 224\,t^5 - 128\,t^6 + 32\,t^7 + 160\,t^8 + \\
&\qquad 96\,t^9 - 192\,t^{10} + 96\,t^{11} - 128\,t^{12} + O(2^9,t^{13})\,,\\
r_{11} &= 113 + 200\,t - 222\,t^2 - 136\,t^3 + 175\,t^4 - 56\,t^5 - 10\,t^6 + 48\,t^7 - 137\,t^8 + \\
&\qquad 168\,t^9 + 226\,t^{10} - 240\,t^{11} + 238\,t^{12} + O(2^9,t^{13})\,,\\
f_{11} &= -184\,t + 48\,t^2 - 100\,t^3 - 32\,t^4 + 184\,t^5 + 16\,t^6 - 4\,t^7 - 192\,t^8 - \\
&\qquad 24\,t^9 + 16\,t^{10} + 180\,t^{11} + 256\,t^{12} + O(2^9,t^{13})\,,
\end{aligned}$$

$$y_{11} = 94\,t^{12} + 131\,t^{13} - 172\,t^{14} - 82\,t^{15} + 34\,t^{16} - 215\,t^{17} + 80\,t^{18} - 120\,t^{19} + 70\,t^{20} - 233\,t^{21} + 110\,t^{22} + 161\,t^{23} + O(2^9, t^{24})\,,$$

then

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

and

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

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

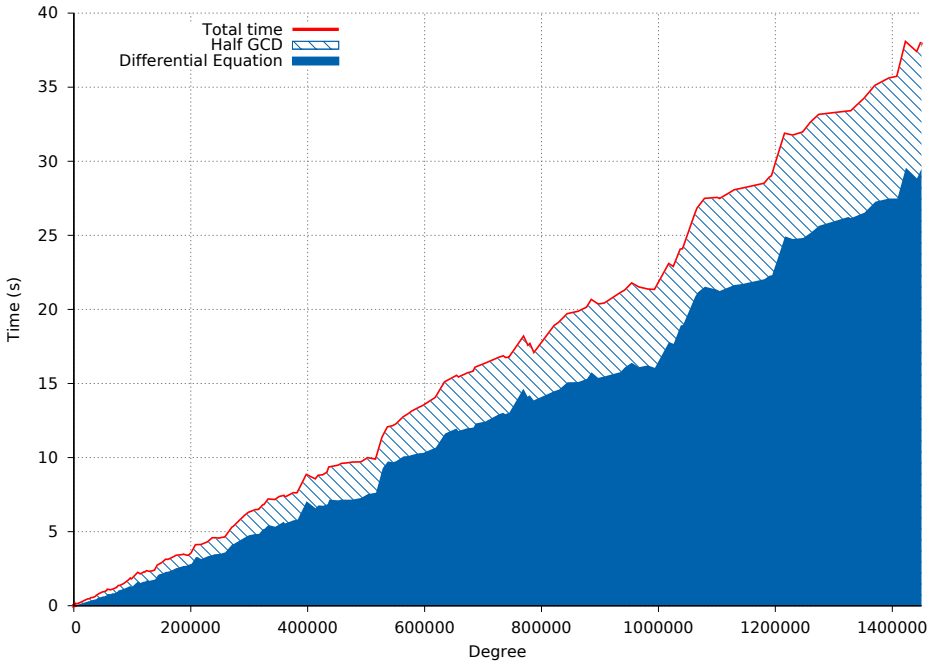
$$\frac{t^5 + t^3 + t^2 + t + 1}{t^5 + t^4 + t^3 + t^2 + 1} + O(t^{12})\,,$$

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

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

1.3.2 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 in Figure 1.1. Since multiplying 2-adic series can be done in almost linear time 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 3 and, second, the underlying polynomial arithmetic over $\mathbb{F}_2$ is slightly more efficient than the arithmetic with 2-adic series in MAGMA.



Timings obtained with MAGMA V2.24-10 on a laptop with an INTEL processor I7-8850H@2.60GHZ

Figure 1.1 – Isogeny computations in $\mathbb{F}_2$.

1.4 Applications

Thanks to the results of [Bos+08; LS08; LV16] in odd characteristic and the case of characteristic 2 being solved in Section 1.2, 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 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 start with a brief presentation on endomorphism rings and isogenies in Section 1.4.1, and show in Section 1.4.2 how to calculate the isogenous curves and the isogeny differentials over finite fields of small characteristic. Then, in Section 1.4.3, we apply this construction to build irreducible polynomials and we end with an example in Section 1.4.4.

1.4.1 Endomorphism ring and isogenies

We briefly introduce some facts about the theory of complex multiplication. Good references are [Lan73; Sil94; Cox13].

An isogeny $E_1 \to E_2$ of elliptic curves defined over a field k is a surjective morphism of curves that induces a group homomorphism $E_1(\bar{k}) \to E_2(\bar{k})$. We denote by $\mathrm{Hom}_k(E_1, E_2)$ the set of homomorphisms from E_1 to E_2 over k and let $\mathrm{End}_k(E) = \mathrm{Hom}_k(E, E)$. We write $\mathrm{End}(E) = \mathrm{End}_{\bar{k}}(E)$. Composition of endomorphisms gives a ring structure on $\mathcal{O} = \mathrm{End}(E)$, and we refer to $\mathcal{O}$ as the ring of endomorphisms of E.

As a $\mathbb{Z}$-module, $\mathrm{End}_k(E)$ is free of rank at most four. More precisely, $\mathrm{End}_k(E)$ is either $\mathbb{Z}$, an order in an imaginary quadratic field (ordinary case) or an order in a definite quaternion algebra (supersingular case). By definition, ordinary or supersingular elliptic curves have complex multiplication. Moreover, every endomorphism φ satisfies in $\mathrm{End}_k(E)$ a quadratic characteristic polynomial with integer coefficients, $\varphi^2 - t\,\varphi + d = 0$. The integer t, denoted $\mathrm{Tr}(\varphi)$, is called the trace of φ. Over $k = \mathbb{F}_q$, the Frobenius endomorphism ϕ_q takes a leading role, since it determines the group and $\mathrm{End}_k(E)$-structure of the rational points of E [Len96]. In particular, it satisfies the Weil polynomial

$$\phi_q^2 - t\,\phi_q + q = 0 \tag{29}$$

where $t = \mathrm{Tr}\,\phi_q := \mathrm{Tr}\,E$ is such that $q + 1 - t$ is the number of rational points of E over k.

What follows is for elliptic curves over $\mathbb{C}$, but these results reduce well to ordinary elliptic curves over finite fields. In the ordinary case, let $\mathcal{O}$ be an order in an imaginary quadratic field κ. Then the theory of complex multiplication states that there is a number field L containing κ and an elliptic curve E over L with $\mathrm{End}_{\bar{L}}(E) = \mathcal{O}$. Let p be a prime that splits completely in $\mathcal{O}_L$ and $\mathfrak{p}$ be a prime of $\mathcal{O}_L$ above p, so that $\mathcal{O}_L/\mathfrak{p} \simeq \mathbb{F}_p$. If $\mathfrak{p}$ does not divide the discriminant of E, then E has good reduction modulo $\mathfrak{p}$. Let $\bar{E}$ denote this reduction, then $\mathrm{End}_{\bar{\mathbb{F}}_p}(\bar{E}) \simeq \mathcal{O}$. Conversely, every elliptic curve $\bar{E}$ arises as the reduction of an elliptic curve E over some L with the same ring of endomorphisms $\mathcal{O}$, called the canonical lift of $\bar{E}$.

There is a one-to-one correspondence between the isomorphism classes of elliptic curves $E/\mathbb{F}_q$ with $\mathrm{End}(E) = \mathcal{O}$ and the ideal class group $\mathrm{Cl}(\mathcal{O})$ (*i.e.* the quotient group of the fractional $\mathcal{O}$-ideals that are prime to the conductor $\mathcal{O}$ by its subgroup of principal ideals). To an invertible $\mathcal{O}$-ideal $\mathfrak{a}$, one associates the elliptic curve $E_\mathfrak{a} \simeq \mathbb{C}/\mathfrak{a}$. An ideal $\mathfrak{a}'$ is equivalent to $\mathfrak{a}$ in $\mathrm{Cl}(\mathcal{O})$ if and only if $\mathbb{C}/\mathfrak{a}'$ is isomorphic to $E_\mathfrak{a}$.

Let now $\mathfrak{l}$ be an invertible $\mathcal{O}$-ideal, and define the the kernel of $\mathfrak{l}$ in $E_\mathfrak{a}$ to be the

intersection of the kernels of all +endomorphisms in $\mathfrak{l}$. We denote it $E_{\mathfrak{a}}[\mathfrak{l}]$,

$$\begin{aligned} E_{\mathfrak{a}}[\mathfrak{l}] &\simeq \{z \in \mathbb{C} : \alpha z \in \mathfrak{a}, \text{ for all } \alpha \in \mathfrak{l} \subset \mathrm{End}(E_{\mathfrak{a}})\}, \\ &\simeq \mathfrak{l}^{-1}\mathfrak{a}/\mathfrak{a}. \end{aligned}$$

The identity map on $\mathbb{C}$ induces the isogeny $I : \mathbb{C}/\mathfrak{a} \to \mathbb{C}/\mathfrak{l}^{-1}\mathfrak{a}$ with kernel $E_{\mathfrak{a}}[\mathfrak{l}]$. The norm of $\mathfrak{l}$ is equal to the degree of the isogeny. The terminology "quotient isogeny" is sometimes used, together with the notation $I : E_{\mathfrak{a}} \to E_{\mathfrak{a}}/E_{\mathfrak{a}}[\mathfrak{l}]$.

Every isogeny between elliptic curves with isomorphic ring of endomorphisms arises in this way. In particular, let $I_1 : E_1 \to E_2$ be a first isogeny defined by $\mathfrak{l}_1$, and $I_2 : E_2 \to E_3$ be a second isogeny defined by $\mathfrak{l}_2$, then the kernel of $I_2 \circ I_1 : E_1 \xrightarrow{I_1} E_2 \xrightarrow{I_2} E_3$ is $E_1[\mathfrak{l}_1\mathfrak{l}_2]$.

These facts are well summarized in the following proposition.

Proposition 1.4.1 ([Sil94, Prop. 1.2, Chap. II])**.**

(a) Let $E_{\mathfrak{a}}$ be an elliptic curve with endomorphism ring $\mathcal{O}_\kappa$ and let $\mathfrak{l}$ and $\mathfrak{l}'$ be non-zero fractional ideals of $\mathcal{O}_\kappa$.

(i) $\mathfrak{l}\,\mathfrak{a}$ is a lattice in $\mathbb{C}$.

(ii) The elliptic curve $E_{\mathfrak{l}\,\mathfrak{a}}$ satisfies $\mathrm{End}(E_{\mathfrak{l}\,\mathfrak{a}}) \simeq \mathcal{O}_\kappa$.

(iii) $E_{\mathfrak{l}\,\mathfrak{a}} \simeq E_{\mathfrak{l}'\,\mathfrak{a}}$ if and only if $\mathfrak{l} \simeq \mathfrak{l}'$ in $\mathrm{Cl}(\mathcal{O}_\kappa)$.

Hence there is a well-defined action of $\mathrm{Cl}(\mathcal{O}_\kappa)$ on the set of elliptic curves with endomorphism ring $\mathcal{O}_\kappa$ determined by $\mathfrak{l} * E_{\mathfrak{a}} = E_{\mathfrak{l}^{-1}\,\mathfrak{a}}$.

(b) The action of $\mathrm{Cl}(\mathcal{O}_\kappa)$ described in (a) is simply transitive. In particular $\#\,\mathrm{Cl}(\mathcal{O}_\kappa)$ is equal to the number of elliptic curves with endomorphism ring $\mathcal{O}_\kappa$.

1.4.2 Isogenies of large degree

Let E be an elliptic curve with complex multiplication defined over a finite field k and $\ell > 2$ a prime integer. Here, the cardinality of the field of definition of E is supposed to be very small compared to ℓ 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 1.4.2 ([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 $O(q^{1/3+\varepsilon})$.*

Since in our case of interest, the field of definition of the curves is rather small while the degrees of the isogenies are rather large, we can suppose that we are given the endomorphism ring $\mathrm{End}(E)$ of E as an order $\mathcal{O}_\kappa$ in an imaginary quadratic field $\kappa = \mathbb{Q}(\sqrt{-\Delta})$, for 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 the elliptic curve E. We more generally define *Elkies degrees* for E as integers whose prime divisors are all Elkies primes for E. Incidentally, there exist a k-rational ℓ-isogeny from E/k to another curve $\tilde{E}/k$. This said, the computation of the isogenous curve $\tilde{E}$ reduces to calculations in the ideal class group of $\mathcal{O}_\kappa$.

More precisely, let m be one of the Elkies prime divisor of ℓ. Let $\mathrm{Cl}(\mathcal{O}_\kappa)$ 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 $\sqrt{|\Delta|}$. Let $\mathfrak{m}$ be an ideal $(m, a_\mathfrak{m} + b_\mathfrak{m}\,\omega)$ 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, and $\mathfrak{e}_1$, $\mathfrak{e}_2$ correspond to endomorphisms. Their product yields an isogeny of degree m defined by the following chain of small degree isogenies,

$$\begin{aligned} E \longrightarrow E\,\big/\,E[\mathfrak{p}_1] \longrightarrow E\,\big/\,E[\mathfrak{p}_1^2] \longrightarrow \ldots \longrightarrow E\,\big/\,E[\mathfrak{p}_1^{e_1}] \longrightarrow \\ E\,\big/\,E[\mathfrak{p}_1^{e_1}\mathfrak{p}_2] \longrightarrow E\,\big/\,E[\mathfrak{p}_1^{e_1}\mathfrak{p}_2^2] \longrightarrow \ldots \longrightarrow E\,\big/\,E[\mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}] \longrightarrow \\ \ldots \\ E\,\big/\,E[\mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_{h-1}^{e_{h-1}}\mathfrak{p}_h] \longrightarrow \cdots \longrightarrow E\,\big/\,E[\mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_h^{e_h}]\,. \end{aligned} \quad (30)$$

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

Example 1.4.3. *Let $\ell = 10^{54} + 1551$ and $p = 5$. Consider the finite field $\mathbb{F}_{5^5} = \mathbb{F}_5(v)$ such that $v^5 + 4v + 3 = 0$. Let E be the elliptic curve defined by*

$$E/\mathbb{F}_{5^5} \ : y^2 = x^3 + (v^4 + 4v^3 + 4v)x + 3v^4 + 2v^3 + 2v.$$

The abstract structure of its endomorphism ring is the maximal order $\mathcal{O}_\kappa = \mathbb{Z}[\omega]$ *of* $\kappa = \mathbb{Q}(\omega)$*, where* $\omega = \sqrt{-2549}$ *and the class group* $\mathrm{Cl}(\mathcal{O}_\kappa)$ *is a cyclic group of order* 70*. Let* I *be the isogeny of degree* ℓ *defined by the ideal*

$$\mathfrak{l} = (\ell, -\omega - 325412660398298471698617723546304913438363897751401493).$$

We compute the image $\bar{\mathfrak{l}}$ *of* $\mathfrak{l}$ *in* $\mathrm{Cl}(\mathcal{O}_\kappa)$ *to obtain*

$$\bar{\mathfrak{l}} = 3\,\mathrm{Cl}(\mathcal{O}_\kappa) = \bar{\mathfrak{p}}^3$$

where $\mathfrak{p} = (3, -\omega + 1)$*. So there exists two principal ideals of* $\mathcal{O}$*,* $\mathfrak{e}_1$ *and* $\mathfrak{e}_2$ *such that*

$$\mathfrak{e}_1\mathfrak{l} = \mathfrak{p}^3\mathfrak{e}_2.$$

One can chose $\mathfrak{e}_1 = (27)$ *and*

$$\mathfrak{e}_2 = (-9811843057247097070526776 7\omega + 156850242604394761352522359 6).$$

Then to find an ℓ*-isogenous curve* $\tilde{E}$ *to* E*, it suffices to compute the following chain*

$$E \longrightarrow E\,\big/\,E[\mathfrak{p}] \longrightarrow E\,\big/\,E[\mathfrak{p}^2] \longrightarrow E\,\big/\,E[\mathfrak{p}^3] = \tilde{E}$$

of isogenies of degree 3*. We finally obtain an equation of* $\tilde{E}$

$$\tilde{E}\ : y^2 = x^3 + (v^4 + 4v^3 + 4v)x + 3v^4 + 4v^3 + v^2 + 3v + 1.$$

To avoid the divisions by p that do appear in calculations for computing explicitly all these isogenies, we reconsider Chain (30) from the standpoint of the canonical lifts of these curves. Results by Serre and Tate [LJPT64] enable to lift canonically E as $\mathcal{E}/K$ where K is an unramified extension of $\mathbb{Q}_p$ of degree n such that k is its residue field.

An algorithm for computing canonical lifts at p-adic precision N in time complexity $O(p^2\,N^2)$ up to some polylogarithmic factors can be for instance found in [Sat00; SST03]. According to Theorem 1.2.10 and [LV16, Theorem 2], the lifting process has to be done with p-adic precision equal to $O(\lceil \log_p(\ell) \rceil)$ in order to be able to reduce the results modulo p. Since in this situation the principal ideal (q) splits in $\mathcal{O}_\kappa$ into two prime ideals, one chooses arbitrarily the residue 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 (30), we use Vélu's formulas to compute for each $\mathfrak{p}_i$ a normalized isogenous curve [Vél71]. These formulas require that one knows the kernels $\mathcal{E}[\mathfrak{p}_i]$. This can be easily done for small degrees, *e.g.* degree 2, by factoring division polynomials. When this approach (of cubic complexity in the degree) is too expensive, an alternative approach is to use modular polynomials. It enables to find the j-invariant of the isogenous curve. Motivated by point counting on elliptic curves, Elkies gave an elegant method to derive from it an explicit normalized equation for this isogenous curve. This algorithm, of quadratic complexity in the degree, is far beyond the scope of this paper and we refer to [Sch95] for details. This process 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 at a ℓ-isogenous curve and its differential. We call Algorithm 4 to find the solution $z(t)$ of Eq. (14) modulo $t^{2\ell+2}$. It remains to reduce $z(t)$ modulo p and compute its Padé approximant to recover the rational function that gives the isogeny.

The conclusion of this section is that we can compute an ℓ-isogenous curve and a rational representation of the isogeny in quasi-linear time in ℓ when $\ell \gg q$.

Theorem 1.4.4. *Given an ordinary elliptic curve E defined over a finite field k with characteristic p and cardinality $q = p^n$ such that its endomorphism ring $\mathcal{O}_\kappa$ is maximal and ℓ is 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 $O(n\,\ell + p^2 + q^{3/2})$ up to some polylogarithmic factors.*

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

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

Remark 1.4.5. 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 $\mathbb{Q}_q$.

1.4.3 Irreducible polynomials over finite fields

Given a finite field k, with characteristic p and cardinality $q = p^n$, and a degree d, the Couveignes-Lercier Las Vegas algorithm achieves a notable quasi-linear asymptotic complexity in d for computing an irreducible polynomial of degree d over k [CL13]. It is based on elliptic curves with a number of points which is divisible by prime divisors of d. So, these curves define separable isogenies whose kernels have only rational points. In its primary form (see Lemma 1.4.6), this algorithm yields a highly efficient method to calculate an irreducible polynomial when d is a prime not dividing $p\,(q-1)$ such that $4d \leqslant q^{\frac{1}{4}}$. For the sake of completeness, we briefly present this construction in Section 1.4.3.1.

However, we note that when d is not a prime or when d is larger than $q+1+2\sqrt{q}$, [CL13] necessarily involves the use of the Kedlaya-Umans algorithm [KU11]. Unfortunately, this algorithm is widely considered impractical, and in our case of interest where q is negligible compared to d, especially the important case $k = \mathbb{F}_2$, we can no more rely on this method.

We show in this section that we can adapt the construction to elliptic curves that do not necessarily have a cardinality divisible by the prime divisors of d. They simply have to admit rational isogenies of degree ℓ where ℓ is of the form $p_1^{e_1}$ or of the form $p_1^{e_1}\,p_2^{e_2}$ with p_1 and p_2 odd prime integers. Given an elliptic curve, it yields a infinite dense list of reachable degree d. Except for the few degrees d that can not be written as $d = \phi(\ell)$ or $d = \phi(\ell)/2$, we more generally have a reasonable expectation to find an elliptic curve that may work for a degree d fixed in advance. We develop this aspect in Section 1.4.3.2.

1.4.3.1 Overview of [CL13]

Let $I/k : E/k \to \tilde{E}/k$ be a degree ℓ separable isogeny where E/k and $\tilde{E}/k$ is given by an affine Weierstrass equation in x, y. We denote by O_E and $O_{\tilde{E}}$ the points at infinity of E and $\tilde{E}$.

We assume that ℓ is a positive odd number and the kernel $\operatorname{Ker} I$ is cyclic. Let $T \in E(\bar{k})$ be a generator of $\operatorname{Ker} I$. Let $\psi_I(x) \in k[x]$ be the degree $(\ell-1)/2$ polynomial

$$\psi_I(x) = \prod_{1 \leqslant k \leqslant (\ell-1)/2} (x - x(kT))\,. \tag{31}$$

There exists a degree ℓ polynomial $\phi_I(x) \in k[x]$ such that the image of the abscissa of the point (x, y) by I is $\eta(x) = \phi_I(x)/\psi_I^2(x)$.

Now, let A be a k-rational point on $\tilde{E}$ such that $2A \neq O_{\tilde{E}}$ and let $B \in E(\bar{k})$ be a

point on E such that $I(B) = A$. We can define the degree ℓ polynomial

$$f_{I,A}(x) = \phi_I(x) - x(A)\psi_I^2(x) \in k[x].$$

Its roots are the $x(B+kT)$ for $0 \leqslant k < d$, and they are pairwise distinct because $2A \neq O_{\tilde{E}}$. So $f_{I,A}(x)$ is a degree ℓ separable polynomial. Furthermore, it is reducible if and only if the fiber $I^{-1}(A)$ is.

This happens to be true when ℓ is a prime not dividing $p\,(q-1)$ such that it divides exactly the number $q+1-\operatorname{Tr} E$ of rational points of E. In this case, Weil polynomial (29) splits as $(X-r)\,(X-s) \bmod \ell$ such that $r = 1 \bmod \ell$ and $s = q \bmod \ell$. Especially the Galois orbit of B has cardinality ℓ since $\phi_q(B) = r\,B$ and the order of r is ℓ in $(\mathbb{Z}/\ell^2\mathbb{Z})^\times$ [CL13, Section 4.2].

When ℓ is small enough, we can find with high confidence such an elliptic curve E. All in all, it yields a quite efficient method to compute an irreducible polynomial.

Lemma 1.4.6 ([CL13, Lemma 6 ($\delta = 1$)])**.** *There exists a probabilistic (Las Vegas) algorithm that on input a finite field k with characteristic p and cardinality $q = p^n$, a prime integer ℓ not dividing $p\,(q-1)$ such that $4\ell \leqslant q^{\frac{1}{4}}$, computes an irreducible polynomial in $k[x]$ of degree ℓ, at the expense of $\ell \times (\log q)^{5+o(q)} + \ell^{1+o(\ell)} \times (\log q)^{1+o(q)}$ elementary operations.*

1.4.3.2 An extended algorithm

Let now ℓ be an odd Elkies degree, prime to $p\,(q-1)$. The integer ℓ is thus odd. With the notation of Section 1.4.2, 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 $\sigma_q - r$ where $r \in \mathbb{Z}/\ell\mathbb{Z}$ is a root of $X^2 - \operatorname{Tr}(E)\,X + q \bmod \ell$.

Take for A the point at infinity $O_{\tilde{E}}$ in the construction of Section 1.4.3.1. We thus consider the polynomial $f_{I,O_{\tilde{E}}}(x) = \psi(x)$, whose roots are the abscissas of points in $\ker I$. Now, the factorizations $I = I_{\ell/m} \circ I_m$, 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 examine the polynomial $\Psi_\ell(x)$, of degree $\varphi(\ell)/2$. Here too, its irreducibility depends on the order of r in the multiplicative group $(\mathbb{Z}/\ell\mathbb{Z})^\times$ because the length of the Galois orbit of B is determined by the relation $\phi_q(B) = r\,B$. The polynomial $\Psi_\ell(x)$ splits thus in factors of degree $d = \mathrm{ord}_{\mathbb{Z}/\ell\mathbb{Z}}(r)/2$ or $d = \mathrm{ord}_{\mathbb{Z}/\ell\mathbb{Z}}(r)$ according to whether a power of r is equal to -1 or not. When $d = \varphi(\ell)/2$, the polynomial $\Psi_\ell(x)$ is therefore irreducible. Since ℓ is odd and $\mathrm{ord}_{\mathbb{Z}/\ell\mathbb{Z}}(r)$ can not be larger than the Carmichael function $\lambda(\ell)$, we may remark that it necessarily 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. The former corresponds to the only possibility for $(\mathbb{Z}/\ell\mathbb{Z})^\times$ to be cyclic (*e.g.* $\lambda(\ell) = \varphi(\ell)$ and $\mathrm{ord}_{\mathbb{Z}/\ell\mathbb{Z}}(r) = \lambda(\ell)/2$), the latter (*e.g.* $\mathrm{ord}_{\mathbb{Z}/\ell\mathbb{Z}}(r) = \lambda(\ell) = \varphi(\ell)/2$) follows from the recursive definition of λ,

$$\lambda(p_1^{e_1}\cdot p_2^{e_2}\cdots p_k^{e_k}) = \mathrm{lcm}\,(\lambda(p_1^{e_1}),\lambda(p_2^{e_2}),\ldots,\lambda(p_k^{e_k}))\ .$$

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

$$\nu_{I,A}(x) = f_{I,A}(x)\,/\,(\,x - x(B)\,)\,,$$

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 $\mathrm{ord}_{\mathbb{Z}/\ell\mathbb{Z}}(r)$. The polynomial $\Phi_\ell(x)$ is thus irreducible when $\mathrm{ord}_{\mathbb{Z}/\ell\mathbb{Z}}(r) = \varphi(\ell)$. We may also remark that in this case ℓ is necessarily a prime power (since ℓ is odd).

The main part of this construction is thus to determine the isogenous curve $\tilde{E}$ and the equations of the isogeny I following Theorem 1.4.4. Therefore, we can state this theorem.

Theorem 1.4.7. *Given an ordinary elliptic curve E defined over a finite field k with characteristic p and cardinality $q = p^n$, and ℓ an odd Elkies degree prime to $p\,(q-1)$ such that one of the roots r modulo ℓ of the Weil polynomial $X^2 - (\mathrm{Tr}\,E)\,X + q$ has order $\varphi(\ell)$ in $(\mathbb{Z}/\ell\mathbb{Z})^\times$, there exists an algorithm that computes two irreducible polynomials in k of degree $\varphi(\ell)$ and $\varphi(\ell)/2$ with time complexity $O(n\,\ell + p^2 + q^{3/2})$ up to some polylogarithmic factors.*

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

Note that $\varphi(\ell)$ is nearly ℓ in Theorem 1.4.7, since the necessary conditions on ℓ yields $\varphi(\ell) = p_1^{e_1-1}(p_1-1)$ or $\varphi(\ell) = p_1^{e_1-1}(p_1-1)\,p_2^{e_2-1}(p_2-1)$.

Remark 1.4.8. Applied to the elliptic curve $E/\mathbb{F}_2 : y^2 + xy = x^3 + 1$, whose Weil polynomial is $X^2 + X + 2$, this method gives an infinite list of irreducible polynomials over $\mathbb{F}_2$, of degree

$$3,\ 5,\ 6,\ 10,\ 11,\ 14,\ 21,\ 26,\ 28,\ 30,\ 33,\ 35,\ 39,\ 42,\ 52,\ 53,\ 54,\ 55,\ 56,\ 63,\ 66,$$
$$70,\ 74,\ 75,\ 78,\ 81,\ 84,\ 89,\ 95,\ 96,\ 98, 105, 106, 108, 110, 112, 119, 131, 138 \ldots$$

We give for the first ones the degree ℓ of the isogeny, the root r of $X^2 + X + 2$ and its order modulo ℓ in the following table.

d	3	5	5	6	10	11	14	21	21	26	28	30	33	33	35	39	42	52
ℓ	7	11	11	7	11	23	29	43	43	53	29	77	67	67	71	79	43	53
r	3	6	4	3	6	13	21	24	18	14	21	59	55	11	31	66	18	14
$\mathrm{ord}_\ell(r)$	6	10	5	6	10	11	28	21	42	52	28	30	33	66	70	78	42	52

Remark 1.4.9. Similarly to Remark 1.4.8, we can easily do an exhaustive search on degrees that are not reachable with this method, whatever the field or the curve are. The first ones are

$$7,\ 13,\ 17,\ 19,\ 24,\ 25,\ 31,\ 32,\ 34,\ 37,\ 38,\ 43,\ 45,\ 47,\ 49,\ 57,\ 59,\ 61,\ 62,\ 64,$$
$$67,\ 71,\ 73,\ 76,\ 77,\ 79,\ 85,\ 87,\ 91,\ 93,\ 94,\ 97,\ 101,\ 103,\ 104,\ 107,\ 109 \ldots$$

For instance, degree 7 is not possible because there is no integer ℓ such that $\varphi(\ell)$ equals 7 or 14.

Remark 1.4.10. Theorem 1.4.4 and Theorem 1.4.7 can be extended to supersingular elliptic curves if we lift them together with a quadratic order (see for instance [CH02]).

1.4.4 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 $\mathfrak{p}\,\mathfrak{l} = \mathfrak{e}_2$, where $\mathfrak{p} = (2, (\sqrt{-55}+1)/2)$ and $\mathfrak{e}_2 = (-\sqrt{-55}+23)/2$. 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 4 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

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

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 $\overline{\mathtt{C}} = v^3 + v^2$.

Chapter 2

Fast resolution of systems of p-adic differential equations

Throughout this chapter the letter p refers to a fixed prime number and K corresponds to a fixed finite extension of $\mathbb{Q}_p$. Let $g \geq 1$ be an integer. We study the computation of a vector of p-adic power series which is the solution of a system of ordinary differential equations in g variables. In Section 2.1 , we introduce our problem and present the main theorem. In Section 2.2.1, we explain the computational model that we use in our algorithm exposed in Section 2.2.2 and the proof of its correctness is presented in Section 2.2.3.

2.1 A general outlook

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 $\mathrm{f} = (f_{ij})_{i,j} \in M_g(K[\![t]\!])$ and H_f be the map defined by

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

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

$$\left\{ \begin{array}{rcl} H_\mathrm{f} \circ X \cdot X' & = & G \\ X(0) & = & 0. \end{array} \right. \tag{32}$$

Equation (32) is inspired from algorithms designed in Chapter 3, for computing isogenies between Jacobians of hyperelliptic curves.
We will always look for solutions of (32) in $(tK[\![t]\!])^g$ in order to ensure that $H_\mathrm{f} \circ X$ is well

defined. We further assume that $H_{\mathrm{f}}(0)$ is invertible in $M_g(K)$.

Given an approximation of f and $G(t)$, the goal of this chapter is to look for an approximation of $X(t)$. In Section 2.2.2, we prove that Equation (32) has a unique solution in $(tK[\![t]\!])^g$, but in this study, we will be interested in the particular case where $G \in \mathcal{O}_K[\![t]\!]^g$, $\mathrm{f} \in M_g(\mathcal{O}_K[\![t]\!])$ and the solution $X(t)$ is in $(t\mathcal{O}_K[\![t]\!])^g$.

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 bounded by n. Our main theorem is the following.

Theorem 2.1.1. *Let p be a prime number and $g \geq 1$ be an integer. 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:*

- *two positive integers n and N,*
- *an analytic map of the form H_{f} where $\mathrm{f} \in M_g(\mathcal{O}_K[\![t]\!])$,*
- *a vector $G(t) \in \mathcal{O}_K[\![t]\!]^g$,*

and, assuming that the differential equation

$$H_{\mathrm{f}}\left(X(t)\right) \cdot X'(t) = G(t)$$

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 $O\left(\mathrm{MM}(g,n) + \mathrm{C}_{H_{\mathrm{f}}}(n)\right)$ operations in $\mathcal{O}_K$, where $\mathrm{C}_{H_{\mathrm{f}}}(n)$ denotes the algebraic complexity of an algorithm computing the composition $H_{\mathrm{f}}(X(t)) \mod t^n$, 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.

2.2 Main result

In this section, we give a proof of the main theorem 2.1.1 by solving efficiently the nonlinear system of differential equations (32) in K. We denote by v_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 v_p to quotients of $\mathcal{O}_K$, the resultant valuation is also denoted by v_p.

2.2.1 Computational model

As in Section 1.2.1, we use the fixed point arithmetic model at precision $O(p^M)$, where $M \in \frac{1}{e}\mathbb{N}^*$, 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:

$$\left(A + O(p^M)\right) \pm \left(B + O(p^M)\right) = (A \pm B) + O(p^M),$$

$$\left(A + O(p^M)\right) \cdot \left(B + O(p^M)\right) = (A \cdot B) + O(p^M).$$

For inversions, we use standard Gaussian elimination.

Lemma 2.2.1 ([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.*

2.2.2 The algorithm

We now move to the effective resolution of Equation (32) assuming that $H_{\mathrm{f}}(0)$ is invertible in $M_g(K)$.
The next proposition guarantees the existence and the uniqueness of a solution of the differential equation (32).

Proposition 2.2.2. *Assuming that $H_{\mathrm{f}}(0)$ is invertible in $M_g(K)$, the system of differential equations (32) 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 (32). 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 (32) can be written as

$$X'(t) = \Big(H_{\mathrm{f}}(X(t))\Big)^{-1} \cdot G(t). \tag{33}$$

Equation (33) applied to 0, gives the non-zero vector X_1. Taking the n-derivative of Equation (33) 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 (32) 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

$$\begin{array}{rccl} dH_{\mathrm{f}}(Y) \ : & K[\![t]\!]^g & \longrightarrow & M_g(K[\![t]\!]) \\ & h & \longmapsto & dH_{\mathrm{f}}(Y)(h) = \Big(f'_{ij}\left(y_i\right) \cdot h_i\Big)_{1 \leq i,j \leq g} . \end{array} \tag{34}$$

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

$$H_{\mathrm{f}}\left(X_m\right) \cdot h' + dH_{\mathrm{f}}(X_m)(h) \cdot X'_m = -H_{\mathrm{f}}\left(X_m\right) \cdot X'_m + G \pmod{t^{2m-1}}. \tag{35}$$

It is easy to see that the left hand side of Equation (35) is equal to $\left(H_{\mathrm{f}}\left(X_m\right) \cdot h\right)'$, therefore integrating each component of Equation (35) and multiplying the result by $\left(H_{\mathrm{f}}\left(X_m\right)\right)^{-1}$

gives the following expression for h

$$h = \left(H_{\mathrm{f}}\left(X_m\right)\right)^{-1} \int \left(G - H_{\mathrm{f}}\left(X_m\right) \cdot X_m'\right)\, dt \pmod{t^{2m}}, \tag{36}$$

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 (32). Reversing the above calculations leads to the following proposition.

Proposition 2.2.3. *We assume that $H_{\mathrm{f}}(0)$ is invertible in $M_g(K)$. Let $m \geq 0$ be an integer, $n = 2m + 1$ and $X_m \in K[\![t]\!]^g$ a solution of Equation (32) mod t^{m+1}. 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 (32) mod t^{n+1}.

It is straightforward to turn Proposition 2.2.3 into an algorithm that solves the non-linear system (32). We make a small optimization by integrating the computation of $H_{\mathrm{f}}(X)^{-1}$ in the Newton scheme.

Algorithm 4: Differential Equation Solver

`DiffSolve` (G, f, n)

Input : $G, \mathrm{f} \pmod{t^n}$ such that $H_{\mathrm{f}}(0)$ is invertible in $M_g(K)$.

Output: The solution X of Equation (32) $\pmod{t^{n+1}}$, $H_{\mathrm{f}}\left(X\right) \pmod{t^{\lceil n/2 \rceil}}$

if $n = 0$ **then**
  return $0 \pmod{t}$, $H_{\mathrm{f}}(0)^{-1} \pmod{t}$

$m := \lceil \frac{n-1}{2} \rceil$;

$X_m, H_m := \texttt{DiffSolve}(G, \mathrm{f}, m)$;

$H_n := 2H_m - H_m \cdot H_{\mathrm{f}}(X) \cdot H_m \pmod{t^{m+1}}$

return $X_m + H_n \int \left(G - H_{\mathrm{f}}\left(X_m\right) \cdot X_m'\right)\, dt \pmod{t^{n+1}}$

According to Proposition 2.2.3, Algorithm 4 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 model.

Theorem 2.2.4. *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 (32) have coefficients in $\mathcal{O}_K$. Then, 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 2.2.4 at the end of Section 2.2.3. Right now, we concentrate on the complexity of Algorithm 4. Recall that $\mathrm{MM}(g, n)$ is the number of arithmetical operations required to compute the product of two $g \times g$ matrices containing polynomials of degree n 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 [Bos+17, Chapter 8], the two functions $\mathrm{M}(.)$ and $\mathrm{MM}(g, .)$ (in the worst case) are related by the following formula

$$\mathrm{MM}(g, n) = O\left(g^\omega \mathrm{M}(n)\right) \tag{37}$$

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

$$\begin{aligned} \mathrm{M}(n_1 + n_2) &\geq \mathrm{M}(n_1) + \mathrm{M}(n_2), \\ \mathrm{C}_H(n_1 + n_2) &\geq \mathrm{C}_H(n_1) + \mathrm{C}_H(n_2), \end{aligned} \tag{38}$$

for all $n_1, n_2 \in \mathbb{N}$.
Using Equation (37) we deduce the following relation

$$O(\mathrm{MM}(g, n_1 + n_2)) \geq \mathrm{MM}(g, n_1) + \mathrm{MM}(g, n_2). \tag{39}$$

Proposition 2.2.5. *Algorithm 4 performs $O\left(\mathrm{MM}(g, n) + \mathrm{C}_{H_{\mathrm{f}}}(n)\right)$ operations in K.*

Proof. Let D denote the algebraic complexity of Algorithm 4, 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 does not change at each iteration and using Equations (38) and (39), we find $\mathrm{D}(n) = O\left(\mathrm{MM}(g, n) + \mathrm{C}_{H_{\mathrm{f}}}(n)\right)$ and the result is proved. □

Remark 2.2.6. If the map H_{f} includes random univariate rational fractions of radicals of constant degrees, the algebraic complexity $\mathrm{C}_{H_{\mathrm{f}}}(n)$ is equal to $O\left(g^2\mathrm{M}(n)\right)$. Standard algorithms allow us to take $\mathrm{M}(n) \in \tilde{O}(n)$. Therefore, Algorithm 4 outputs the solution of Equation (32) mod t^{n+1} for a cost of $\tilde{O}(g^{\omega}n)$ operations in $\mathcal{O}_K$.

Corollary 2.2.7. *When performed with fixed point arithmetic at precision $O(p^M)$, the bit complexity of Algorithm 4 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 $\mathcal{O}_K/\pi^{eM}\mathcal{O}_K$.*

2.2.3 Precision analysis

The goal of this subsection is to prove Theorem 2.2.4. The proof relies on the the theory of "differential precision" developed in [CRV14; CRV15]. We follow the same strategy as in Section 1.2.5.

We study the solution $X(t)$ of Equation (32) when $G(t)$ varies, with the assumption $H_{\mathrm{f}}(0)$ is invertible in $M_g(\mathcal{O}_K)$. Proposition 2.2.2 showed that Equation (32) has a unique solution $X(G) \in K[\![t]\!]^g$. Moreover, if we examine the proof of Proposition 2.2.2, 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 2.2.2 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 2.2.8. *For $G \in \left(K[\![t]\!]/\left(t^n\right)\right)^g$, the differential of X_n with respect to G is the following function*

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

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

$$H_{\mathrm{f}}(X_n(G)) \cdot \Big(dX_n(G)(\delta G)\Big)' + dH_{\mathrm{f}}(X_n(G))(dX_n(G)(\delta G)) \cdot X_n(G)' = \delta G \qquad (40)$$

where $dH_{\mathrm{f}}(X_n(G))$ is the differential of H_{f} at $X_n(G)$ defined in (34). Making use of the relation

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

Equation (40) becomes

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

Integrating the above relation and multiplying by $(H_{\mathrm{f}}(X_n(G)))^{-1}$ 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 $F_n = (tK[\![t]\!]/(t^{n+1}))^g$; 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

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

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

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

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

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

Lemma 2.2.9. *Let $A \in M_g(\mathcal{O}_K[\![t]\!]/(t^n))$. If there exists a vector $x(t) \in (\mathcal{O}_K[\![t]\!]/(t^n))^g$ such that $\|A\,x\|_{F_n} < 1$ then A is not invertible in $M_g(\mathcal{O}_K[\![t]\!]/(t^n))$.*

Proof. Write $A = (a_{ij}(t))_{i,j}$ and $x(t) = (x_1(t), \ldots, x_g(t))$. By definition, the norm $\|A\,x\|_{F_n}$ is equal to

$$\|A\,x\|_{F_n} = \max_i \left\|\sum_j a_{ij}x_j\right\|_{K_n}.$$

Therefore, the condition $\|A\,x\|_{F_n} < 1$ is equivalent to the following inequality

$$\left\|\sum_j a_{ij}x_j\right\|_{K_n} < 1 \tag{41}$$

for all $i = 1, \dots, g$. Let k be the residue field of K. Equation (41) implies that $\sum_j a_{ij} x_j = 0$ in k. Hence, the reduction of A in $M_g(k[\![t]\!]/(t^n))$ is not invertible and A is not invertible in $M_g(\mathcal{O}_K[\![t]\!]/(t^n))$. □

Lemma 2.2.10. *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 $H_{\mathrm{f}}(0) \in \mathrm{GL}_g(\mathcal{O}_K)$ guarantee the invertibility of $H_{\mathrm{f}}(X_n(G))$ in $M_g(\mathcal{O}_K[\![t]\!])$. Let $\delta G \in E_n$ such that $\|\delta G\|_{E_n} = 1$. Using the fact that $H(X(G))^{-1} \int \delta G \in (t\mathcal{O}_K[\![t]\!]/(t^n))^g$ and applying Lemma 2.2.9, we get

$$\|dX_n(G)(\delta G)\| = \|H(X(G))^{-1} \int \delta G\|_{F_n} = 1.$$

□

We define the following function:

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

By Proposition 2.2.8, the map dX_n is equal to $\tau_n \circ (X_n, \mathrm{id})$, where id denotes the identity map on E_n.

Lemma 2.2.11. *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, by Lemma 2.2.11, $\Lambda(\tau_n)(x) \geq 0$ for all $x \in \mathbb{R}_+^*$. Applying [CRV15, Proposition 2.5], we get

$$\Lambda(X_n)_{\geq 2}(x) \leq 2\left(x + \frac{\log p}{p-1}\right)$$

for all $x \leq -\dfrac{\log p}{p-1}$. Therefore, $\Lambda(X_n)_{\geq 2}(x) < x$ if $x < -2\dfrac{\log p}{p-1}$. □

Proposition 2.2.12. *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 2.2.10, 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 2.2.11, 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 2.2.10. □

We end this section by giving a proof of Theorem 2.2.4.

Correctness proof of Theorem 2.2.4. Let G, f and n be the input of Algorithm 4. 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

$$H_{\mathrm{f}}(X_m) \cdot X_n = H_{\mathrm{f}}(X_m) \cdot X_m + \int e_m \, dt \mod (t^{n+1}, p^M) \tag{42}$$

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

$$H_{\mathrm{f}}(X_n) \cdot X_n' = H_{\mathrm{f}}(X_m) \cdot X_n' + dH_{\mathrm{f}}(X_m)\Big((H_{\mathrm{f}}(X_m))^{-1} \int e_m \, dt\Big) \cdot X_m' \mod (t^n, p^M). \tag{43}$$

In addition, one can easily verifies

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

Hence, Equation (43) 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 $\|G - G_n\|_{F_n} \leq p^{-M}$. Therefore, $\|G - G_n\|_{E_n} \leq p^{-M+\lfloor \log_p(n) \rfloor}$. By Proposition 2.2.12, we have that

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

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

2.3 Experiments

Using an implementation of Algorithm 4 in the MAGMA computer algebra system [BCP97], we compute an approximation modulo $(7, t^{4n^2+1})$ of the solution of the following differential system

$$H_{\mathrm{f}} \circ X \cdot X' = G, \quad X(0) = X_0, \tag{44}$$

where

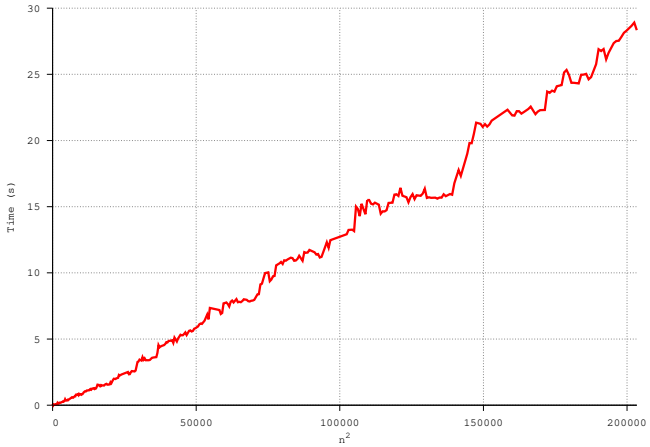
$$\mathrm{f} = \frac{1}{\sqrt{t^5 + t^4 + t^2 + 1}} \begin{pmatrix} 1 & 1 \\ t & t \end{pmatrix}$$

and

$$G(t) = \frac{1}{\sqrt{(t+a_n)^5 + (t+a_n)^4 + (t+a_n)^2 + 1}} \begin{pmatrix} \ell \\ \ell(t+a_n) \end{pmatrix}, \quad a_n \in \mathbb{Z}_7.$$

for several $n \in \mathbb{Z}$ coprime to 7. Equation (44) is inspired from algorithms for computing isogenies between Jacobian of genus two curves (see Chapter 3 for more details). The initial condition X_0 and the constant a_n depend on the choice of the curve and the integer n.

The calculations are done in $\mathbb{Z}_7$ at 7-adic precision $O(7^M)$ with $M = 1 + \lfloor \log_7(4n^2) \rfloor$. Results are reported in Figure 2.1. We observe that the complexity of our implementation is quasi-linear in n^2; this is due to two facts. First, according to Remark 2.2.6, the composition $H_{\mathrm{f}}(X)$ can be carried out with quasi-linear time complexity, and second, the multiplication of 7-adic series with a fixed precision can be done in almost linear time as well.



Timings obtained with MAGMA V2.25-7 on a laptop with an INTEL processor E5-2687WV4@3.00GHZ

Figure 2.1 – Computing an approximation modulo $(7, t^{4n^2+1})$ of the solution of Equation (44)

Chapter 3

Fast computation of hyperelliptic curve isogenies in odd characteristic

Let p be an odd prime number. In this chapter, we focus on p-adic algorithms that compute the explicit form of a rational representation of an isogeny between Jacobians of hyperelliptic curves for fields of odd characteristic. We divide the chapter into four main sections.
In Section 3.1 we provide a brief introduction by giving a general idea of the algorithms that we want to construct. Section 3.2 is devoted to some basic results about abelian varieties and isogenies: in Section 3.2.1, we briefly recall some elements about principally polarized abelian varieties and $(\ell, \dots, \ell)$-isogenies between them, the notion of rational representation is discussed in Section 3.2.2 and in Section 3.2.3, we construct, for a given rational representation, a system of differential equations that we associate with it.
In Section 3.3, we give a first algorithm for the computation of isogenies between Jacobians of hyperelliptic curves. It is based on Algorithm 4 of Chapter 2 and can be used efficiently only for small genus curves. In Section 3.4 we treat the case of Jacobians of hyperelliptic curves of arbitrary genus. We finally discuss an application of these results to the calculation of the multiplication-by-ℓ maps over finite fields of odd characteristic (see Section 3.5).

3.1 Introduction

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 3.2.2 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 $X(t) \in L[\![t]\!]^g$, where L is a finite extension of k of degree at most $O(g!)$, of a first order non-linear system of differential equations having the same form as Equation (32) (see Section 3.2.3):

$$H\left(X(t)\right) \cdot X'(t) = G(t). \tag{45}$$

This approach is a generalization of the elliptic curves case [LV16] for which Equation (45) is solved in dimension one.

Equation (45) 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 L then recover the rational fractions that defines the rational representation of the isogeny. Unfortunately, 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] 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.

We assume that k is a finite field of characteristic p. Let ℓ be an integer coprime to p and $g \geq 2$ an integer. After possibly lifting Equation (45) to the p-adics, it is straightforward to make use of Algorithm 4 to solve it. This gives rise to an algorithm that computes a rational representation of a given $(\ell, \ldots, \ell)$-isogeny between Jacobians of hyprelliptic curves of genus g. The complexity of this algorithm is quasi-linear with respect to ℓ but, unfortunately, it is at least quadratic in g. The main reason for this lack of efficiency is due to the fact that the components of the solution $X(t)$ of Equation (45) are power series over an unramified extension of degree bounded by $O(g!)$ of the base field. Another reason comes from the exponent g^ω in the complexity of Algorithm 4 which corresponds to the time needed to compute the product matrix-vector in dimension g. Thus, Algorithm 4 can only be used efficiently to compute isogenies of Jacobians of hyperelliptic curves of small genus. In Section 3.4, we revisit Algorithm 4 and manage to lower the complexity in g and make it quasi-linear as well but, unfortunately, it is difficult to implement the

new algorithm in an optimized way since it uses the Kedlaya-Umans [KU11] algorithm as a subroutine which has not yet given rise to fast practical implementations.

Note that these techniques do not allow us 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 (45) will require extracting 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.

3.2 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.

3.2.1 $(\ell, \ldots, \ell)$-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 [Mil86b] 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

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

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 3.2.1 ([Mil86b, 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 3.2.1, we give the definition of an $(\ell, \dots, \ell)$-isogeny.

Definition 3.2.2. *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 $j^{(g-1)}$; 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 3.2.3. 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 3.2.3, Definition 3.2.2 for Jacobian varieties gives the following

Proposition 3.2.4. *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 the square [Mil86b, Theorem 5.5] gives the following relation

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

Meaning that,

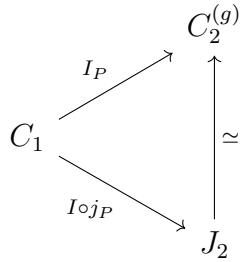
$$\lambda_{(\mathcal{L}_{A_1}^1)^{\otimes \ell}} = \lambda_{\mathcal{L}_{A_1}^{\ell}}.$$

From Proposition 3.2.1, we deduce that 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 3.2.3, $I^*\mathcal{L}_{A_2}^1$ corresponds to $I^*\Theta_2$ and $\left(\mathcal{L}_{A_1}^1\right)^{\otimes \ell}$ corresponds to $\ell\Theta_1$. □

3.2.2 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 $I : J_1 \longrightarrow J_2$. Let $P \in C_1$ be a Weierstrass point, 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 3.2.5. *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 Mumford 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

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

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 functions on C_1 in u and v and it is called a *rational representation* of I.
To avoid confusion, we reserve *rational fraction* to refer to a rational function on $\mathbb{P}^1$.

Lemma 3.2.6. *Let $\pi : C_1 \to \mathbb{P}^1$ be a rational function on C_1.*

1. *If $\pi(u, v)$ is invariant under the hyperelliptic involution of C_1 then there exists a rational fraction A in u, such that*

   $$\pi(u, v) = A(u)$$

   and $\deg(A) \le \deg(\pi)/2$.

2. *Otherwise, we can always find two rational fractions B and D in u such that*

   $$\pi(u, v) = B(u) + vD(u)$$

   and the degrees of B and D are bounded by $\deg(\pi)$ *and* $\deg(\pi) + g + 1$ *respectively. Moreover, if $B(u) = 0$ then* $\deg(D) \le \deg(\pi)/2 + g + 1$.

Proof. 1. The inequality $\deg(A) \le \deg(\pi)/2$ comes from the fact that the function u has degree 2.

2. The rational fractions $B(u)$ and $D(u)$ satisfy the following relations

   $$B(u) = \frac{\pi(u, v) + \pi(u, -v)}{2}, \quad D(u) = \frac{\pi(u, v) - \pi(u, -v)}{2v}.$$

   Since, $\pi(u, v) + \pi(u, -v)$ and $\pi(u, v) - \pi(u, -v)$ are invariant under the hyperelliptic involution and have degrees bounded by $2\deg(\pi)$, then $B(u)$ is a rational fraction

of degree bounded by $\deg(\pi)$ and $D(u)$ is a rational fraction of degree bounded by $\deg(\pi)+g+1$ (Note that v is a rational fraction of degree bounded by $2g+2$).

□

Proposition 3.2.7. *The functions $\sigma_1,\dots,\sigma_g$ can be seen as rational fractions in u. These rational fractions have the same degree bounded by $\deg(\sigma_1)/2$. Moreover, the rational functions $\rho_1/v,\dots,\rho_g/v$ can also be expressed as rational fractions in u of degrees bounded by $\deg(\rho_1)/2+g+1,\dots,\deg(\rho_g)/2+g+1$ respectively.*

Proof. It is a direct consequence of Lemma 3.2.6 and using the fact that $I_P(u,-v) = -I_P(u,v)$. □

Remark 3.2.8. If P is not a Weierstrass point, there exists rational fractions A_i,B_i,D_i and E_i in u such that $\sigma_i(u,v) = A_i(u) + vB_i(u)$ and $\rho_i(u,v) = D_i(u) + vE_i(u)$ for all $i \in \{1,\cdots,g\}$. Let $\bar{P}$ the image of P by the hyperelliptic involution. The morphism $I_{\bar{P}}$ gives a rational representation $(\overline{\sigma_1},\cdots,\overline{\sigma_g},\overline{\rho_1},\cdots,\overline{\rho_g})$ of I. From the relation $I_P(u,-v) = -I_{\bar{P}}(u,v)$, we deduce $\overline{\sigma_i}(u,v) = A_i(u) - vB_i(u)$ and $\overline{\rho_i}(u,v) = -D_i(u) + vE_i(u)$ for all $i \in \{1,\cdots,g\}$. This gives the following formulas

$$A_i(u) = (\sigma_i(u,v) + \overline{\sigma_i}(u,v))/2, \quad B_i(u) = (\sigma_i(u,v) - \overline{\sigma_i}(u,v))/2v,$$

$$D_i(u) = (\rho_i(u,v) - \overline{\rho_i}(u,v))/2, \quad E_i(u) = (\rho_i(u,v) + \overline{\rho_i}(u,v))/2v.$$

The degrees of A_i and D_i (resp. B_i and E_i) are bounded by $\deg(\sigma_i)$ (resp. $\deg(\rho_i)+g+1$).

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 $\sigma_1,\dots,\sigma_g,\rho_1,\dots,\rho_g$. In the case of an $(\ell,\dots,\ell)$-isogeny, we adapt the proof of [CE15, § 6.1] in order to obtain bounds in terms of ℓ and g.

Lemma 3.2.9. *Let $i \in \{1,\dots,g\}$. 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 $3\Theta_2$ if $\deg(f_2) = 2g+1$, and $4\Theta_2$ 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 two along the divisor $\{(R_1,\dots,R_{g-1},\infty)\,;R_i \in C_2\}$ which is algebraically equivalent to Θ_2. □

Lemma 3.2.10 ([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 3.2.11. *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 $3g\ell$ if $\deg(f_2) = 2g + 1$, and $4g\ell$ otherwise.*

Proof. The degrees of $\sigma_1, \dots, \sigma_g, \rho_1, \dots, \rho_g$ are obtained by computing the intersection of $I_P(C)$ with their pole divisors. By Lemma 3.2.9, it suffices to show that

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

Since I is an $(\ell, \dots, \ell)$-isogeny, Proposition 3.2.4 gives that $I^*\Theta_2$ is algebraically equivalent to $\ell\Theta_1$. Moreover, up to algebraic equivalence,

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

Using Lemma 3.2.10, we obtain

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

As

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

the result follows. □

3.2.3 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 3.2.5. 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 with 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

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

Let $(m_{ij})_{1 \leq i,j \leq g} \in \mathrm{GL}_g(\bar{k})$ be the matrix of F_P^* with respect to these two bases. We call it the *normalization matrix* of the isogeny I.

Remark 3.2.12. Let P_1 and P_2 be two points on C_1. The two morphisms I_{P_1} and I_{P_2} satisfy the following relation

$$I_{P_1} = I_{P_2} + I([P_2 - P_1]).$$

Therefore, the linear maps $I^*_{P_1}$ and $I^*_{P_2}$ are equal.

Let $Q = (u_Q, v_Q) \in C_1$ be a non-Weierstrass point different from P and $I_P(Q) = \{R_1, \ldots, R_g\}$ such that $I_P(Q)$ contains g distinct points and does not contain a point at infinity or a Weierstrass point. The points R_i may be defined over an extension k' of k of degree at most $O(g!)$.

Let t be a formal parameter of C_1 at Q; then we have the following commutative diagram

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

For all $i = 1, \ldots, g$, the pull back of $\sum_{j=1}^{i-1} x^{i-1} dx_j/y_j$ along the bottom horizontal arrow, then along the left vertical arrow, gives

$$\frac{du}{v} \sum_{j=1}^{g} m_{ij} u^{j-1}.$$

And the pull back of $\sum_{j=1}^{i-1} x^{i-1} dx_j/y_j$ along the right vertical arrow, then along the top

horizontal arrow gives

$$\sum_{j=1}^{g} x_j^{i-1} dx_j.$$

This gives the differential system

$$\begin{cases} \dfrac{dx_1}{y_1} + \cdots + \dfrac{dx_g}{y_g} = \left(m_{11} + m_{12}\cdot u + \ldots + m_{1g}\cdot u^{g-1}\right)\dfrac{du}{v}, \\ \dfrac{x_1\cdot dx_1}{y_1} + \cdots + \dfrac{x_g\cdot dx_g}{y_g} = \left(m_{21} + m_{22}\cdot u + \ldots + m_{2g}\cdot u^{g-1}\right)\dfrac{du}{v}, \\ \qquad\vdots \qquad\qquad\qquad\qquad\qquad\qquad \vdots \\ \dfrac{x_1^{g-1}\cdot dx_1}{y_1} + \cdots + \dfrac{x_g^{g-1}\cdot dx_g}{y_g} = \left(m_{g1} + m_{g2}\cdot u + \ldots + m_{gg}\cdot u^{g-1}\right)\dfrac{du}{v}, \\ y_1^2 = f_2(x_1), \quad \cdots \quad , y_g^2 = f_2(x_g)\,. \end{cases} \tag{46}$$

Equation (46) 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 (46) 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 (46) 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 (46) 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 (46) becomes

$$H(X(t))\cdot X'(t) = G(t) \tag{47}$$

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

Proposition 3.2.13. *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

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

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 $i \neq j$. □

3.3 The case of curves of small genus

We start by fixing some notation. Let k be a finite field of characteristic p and $\ell > 1$ be an integer coprime to p. Let C_1 (resp. C_2) be a hyperelliptic curve over k of small genus g given by the affine model $v^2 = f_1(u)$ (resp. $y^2 = f_2(x)$) and let J_1 (resp. J_2) be its Jacobian. We assume that there exists a separable $(\ell, \ldots, \ell)$-isogeny $I : J_1 \to J_2$ defined over k and let m be its normalization matrix. Fix a Weierstrass point $P \in C_1$ (we assume without loss of generality that P is a k-rational point). Let $Q = (u^{(0)}, v^{(0)})$ be a non-Weierstrass point on C_1 such that $I_P(Q) = \{(x_1^{(0)}, y_1^{(0)}), \ldots, (x_g^{(0)}, y_g^{(0)})\}$ contains g distinct points and does not contain a point at infinity or a Weierstrass point. Let t be a formal parameter of C_1 at Q and let $\{(x_1(t), y_1(t)), \ldots, (x_g(t), y_g(t))\}$ be the image of $Q(t) = (u(t), v(t))$ by I_P.

3.3.1 A first algorithm

As explained in Section 3.2.3 , the computation of the rational representation associated with I_P reduces to the problem of computing an approximation of the following differential system whose unknown is $X(t) = (x_1(t), \ldots, x_g(t)) \in L[\![t]\!]$, where L is a finite

extension of degree at most $O(g!)$.

$$\begin{cases} H(X(t)) \cdot X'(t) = G(t) \\ y_i(t)^2 = f_2(x_i(t)),\ i = 1, \dots, g \\ X(0) = (x_1^{(0)}, \cdots, x_g^{(0)}) \\ Y(0) = (y_1^{(0)}, \cdots, y_g^{(0)}) \end{cases} \tag{48}$$

where $G(t) \in k[\![t]\!]^g$ and $H(X(t))$ are the matrices defined by

$$G(t) = \frac{1}{v(t)} \cdot \mathrm{m} \cdot \begin{pmatrix} 1 \\ u(t) \\ u(t)^2 \\ \vdots \\ u(t)^{g-1} \end{pmatrix} \tag{49}$$

and

$$H(x_1(t), \dots, x_g(t)) = \begin{pmatrix} x_1(t)/y_1(t) & x_2(t)/y_2(t) & \cdots & x_g(t)/y_g(t) \\ x_1(t)^2/y_1(t) & x_2(t)^2/y_2(t) & & x_g(t)^2/y_g(t) \\ \vdots & & & \vdots \\ x_1^{g-1}(t)/y_1(t) & x_2(t)^{g-1}/y_1(t) & \cdots & x_g(t)^{g-1}/y_g(t) \end{pmatrix}. \tag{50}$$

Based on the discussion in Section 3.1, we are sometimes obliged to lift Equation (48) to the p-adics. Therefore, we can replace k by an extension K of $\mathbb{Q}_p$ and L by an unramified extension of K of degree at most $O(g!)$.
Since we are assuming that g is small, the next theorem shows that we can solve Equation (48) with quasi-linear complexity

Theorem 3.3.1. *Let K be an unramified extension of $\mathbb{Q}_p$ and k its residue field. Let $g \geq 2$ be a "small" positive integer. There exists an algorithm that takes as input:*

- *a positive integer n,*
- *a polynomial $f_2 \in \mathcal{O}_K[z]$ of degree bounded by $O(g)$,*
- *a vector $X_0 = (x_1^{(0)}, \dots, x_g^{(0)})$ such that $\prod_{i=1}^{g} (z - x_i^{(0)}) \in \mathcal{O}_K[z]$ is separable over k,*
- *a vector $Y_0 = (y_1^{(0)}, \dots, y_g^{(0)})$ such that $(y_i^{(0)})^2 = f_2(x_i^{(0)})$ for all $i = 1, \dots, g$,*
- *a vector $G(t) \in \mathcal{O}_K[\![t]\!]^g$ having the same form as in Equation (49),*

and, assuming that the solution of Equation (48) has coefficients in $\mathcal{O}_L$ with L an unramified extension of K, outputs an approximation of this solution modulo (p, t^{n+1}) for a cost of $\tilde{O}(n)$ operations in $\mathcal{O}_K$ at precision $O(p^M)$ with $M = 1 + \lfloor \log_p(n) \rfloor$.

Proof. This is a direct consequence of Theorem 2.1.1 and Remark 2.2.6. □

Let $(U(z), V(z))$ be the Mumford representation of I_P. Since the coefficients of $U(z)$ are rational fractions of degree at most $\mathrm{O}(g\ell)$, solving Equation (48) modulo $t^{O(g\ell)}$ allows to reconstruct all the components of the rational representation (note that the polynomial $V(z)$ can be recovered using the polynomial $U(z)$ and the equation of C_2). By Theorem 3.3.1 and due to the fact that the rational reconstruction can be done in quasi-linear time complexity (using Padé approximant) we obtain, possibly after having lifted the problem to the p-adics, an efficient algorithm that computes a rational representation of an isogeny between Jacobians of hyperelliptic curves of small genus over finite fields of odd characteristic.

3.3.2 Experiments

Using an implementation of both Algorithm 4 and the HALF-GCD variant given in [Tho03] with the MAGMA computer algebra system [BCP97], we compute the first g components $\sigma_1, \ldots, \sigma_g$ of the associated rational representation for the multiplication by an integer ℓ for Jacobians of genus 2 and 3. Timings are detailed in Section 3.3.3. 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.

3.3.2.1 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 an odd prime number different from 19. We look for a maximal isotropic subgroup V of the ℓ-torsion subgroup $J(C_1)[\ell]$ of $J(C_1)$ 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 4 to Equation (46).
The p-adic precision needed to do the calculations is therefore equal to $1 + \lfloor \log_{19}(66) \rfloor = 2$.

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

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

to

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

in $\mathcal{C}_2\left(\mathbb{Q}_{19}[\![t]\!]\right)^{(2)}$. We can therefore choose $X_0 = (-36 + O(19^2), -129 + O(19^2))$ as an initial condition for the differential equation, then send it to the point $(O(19^2), O(19^2))$ 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 $G(t)$ mod $(19^2, t^{111})$.
A call from Algorithm 4, 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

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

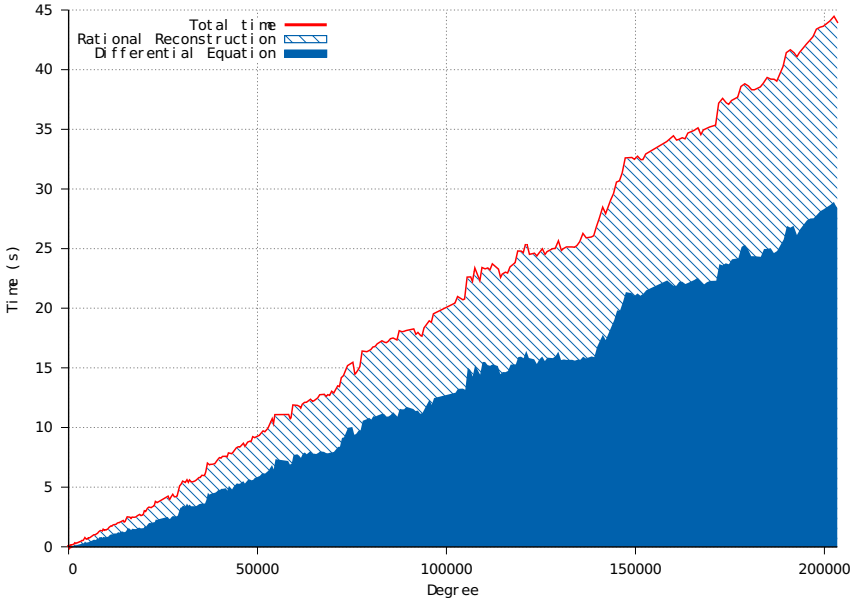
and its denominator D is equal to

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

3.3.3 Timings

We use an implementation in MAGMA of Algortihm 4 and the HALF-GCD 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 3.1 for $g = 2$ and Figure 3.2 for $g = 3$. We observe that the time complexity of our implementation is almost linear in ℓ^2 (note that the multiplication by ℓ is an $(\ell^2, \cdots, \ell^2)$-isogeny), this is due to the fact that the multiplication of p-adic series and the rational reconstruction can be done in almost linear time.
Since the rational fractions $\sigma_1, \cdots, \sigma_g$ have the same denominator, the rational reconstruction over $\mathbb{F}_p$ is done by applying the HALF-GCD variant only on σ_1. The other rational fractions are obtained by multiplying their associated power series by the denominator of

σ_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.



Timings obtained with MAGMA V2.25-7 on a laptop with an INTEL processor E5-2687WV4@3.00GHZ

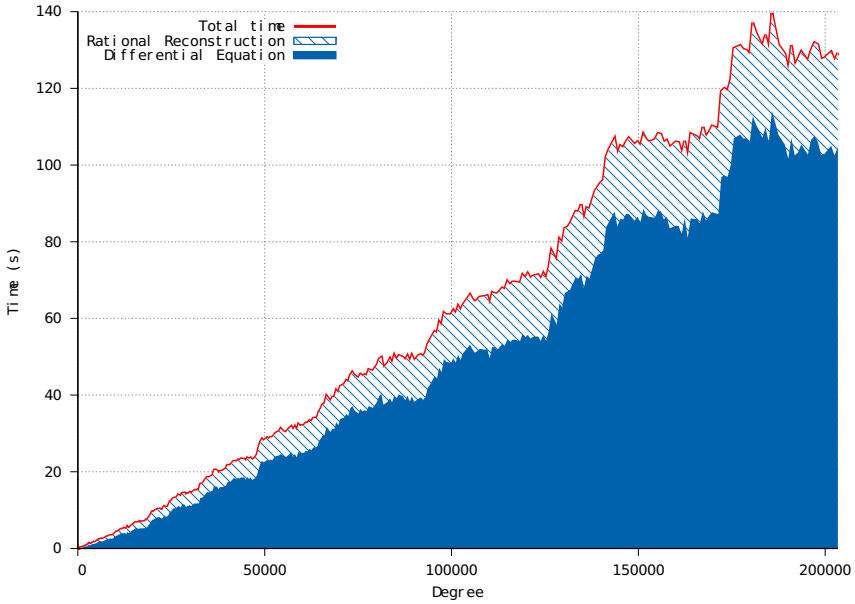
Figure 3.1 – Isogeny computations for the Jacobian of a genus 2 curve in $\mathbb{F}_7$.

3.4 The case of curves of arbitrary genus

In this section, we re-examine the Newton scheme of Algorithm 4 to make it quasi-linear in the genus of the curves. We keep the same notation as Section 3.3 and we recall the Newton iteration that we used to solve Equation (48)

$$X_{2m+1}(t) = X_m(t) + H(X_m(t))^{-1} \int (G - H(X_m(t)) \cdot X'_m(t))\, dt. \tag{51}$$

As explained in Section 3.1, the lack of efficiency of Algorithm 4 with respect to g is due to the fact that the components of the solution $X(t)$ of Equation (48) have coefficients defined over an unramified extension of degree at most $g!$ of the base field k. However, the rational fractions of the rational representation are defined over k (and more precisely over the ring of integers of k if k is an extension of $\mathbb{Q}_p$). For this reason, we work directly



Timings obtained with MAGMA V2.25-7 on a laptop with an INTEL processor E5-2687WV4@3.00GHZ

Figure 3.2 – Isogeny computations for the Jacobian of a genus 3 curve in $\mathbb{F}_7$.

on the first Mumford coordinate $U(z) = \prod_{i=1}^{g}(z - x_i(t))$ which has the decisive advantage to be defined over the base field: we rewrite the Newton scheme (51) accordingly and design fast algorithms for iterating it in quasi-linear time.

Our main theorem is the following

Theorem 3.4.1. *Let K be an unramified extension of $\mathbb{Q}_p$ and k its residue field. There exists an algorithm that takes as input:*

- *two positive integers g and n,*
- *A polynomial $f_2 \in \mathcal{O}_K[z]$ of degree bounded by $O(g)$,*
- *a vector $X_0 = (x_1^{(0)}, \dots, x_g^{(0)})$ represented by the polynomial $U_0(z) = \prod_{i=1}^{g}(z - x_i^{(0)}) \in \mathcal{O}_K[z]$ such that, over k, $U_0(z)$ is separable,*
- *a vector $Y_0 = (y_1^{(0)}, \dots, y_g^{(0)})$ represented by the interpolating polynomial $V_0(z) \in \mathcal{O}_K[z]$ of the data $\{(x_1^{(0)}, y_1^{(0)}), \dots, (x_g^{(0)}, y_g^{(0)})\}$ and such that U_0 divides $f_2^2 - V_0$,*
- *a vector $G(t) \in \mathcal{O}_K[\![t]\!]^g$,*

and, assuming that the solution of Equation (48) has coefficients in $\mathcal{O}_L$ with L an unramified extension of K, outputs a polynomial $U(t, z) = \prod_{i=1}^{g}(z - x_i(t)) \in \mathcal{O}_K[\![t]\!][z]$ such that $X(t) = (x_1(t), \dots, x_g(t))$ is an approximation of this solution modulo (p, t^{n+1}) for a cost $\tilde{O}(ng)$ operations in $\mathcal{O}_K$ at precision $O(p^M)$ with $M = 1 + \lfloor \log_p(n) \rfloor$.

3.4.1 Some useful results

Before we give a proof for Theorem 3.4.1, we recall some computational results for Newton sums, structured matrices and power projections. In this subsection, the lettrer K refers to a fixed field.

3.4.1.1 Computing Newton sums

Let $P(t,z)$ be a monic polynomial of degree d with coefficients in $K[\![t]\!]$ such that $P(0,z)$ is separable over K and $x_1(t), x_2(t), \cdots, x_d(t)$ its roots in $\overline{K}[\![t]\!]$, where $\overline{K}$ denotes the algebraic closure of K. We define the i-th Newton sum $s_i(t)$ of P by

$$s_i(t) = \sum_{j=1}^{d} x_j(t)^i \in K[\![t]\!],$$

and we are interested in designing an efficient algorithm to compute it, only from the coefficients of P.
Let P^* be the reciprocal polynomial of P, *i.e.* $P^*(t,z) = \prod_{i=1}^{d} (1 - x_i(t)z)$. It is well known that the i-th coefficient of the power series expansion of $(P^*)'/P^*$ in $K[\![t,z]\!]$ is equal to $-s_{i+1}(t)$ (see for instance [Bos+05, Lemma 2]). This gives Algorithm 5 to compute the first g Newton sums of the polynomial $P(t,z)$ modulo t^{n+1}.

Algorithm 5: Newton Sums

`NewtonSums` (P, g, n)

Input : $P \in K[\![t]\!][z]$, $g \in \mathbb{N}^*$, $n \in \mathbb{N}^*$.

Output: The sequence $s_1(t) \mod t^{n+1}, \cdots, s_g(t) \mod t^{n+1}$.

$f := -(P^*)'/P^* \mod (t^{n+1}, z^g)$; // $f = \sum_{i=0}^{g-1} f_i(t) z^i$

return $f_0(t), \cdots, f_{g-1}(t)$

Proposition 3.4.2. *Let $P \in K[\![t]\!][z]$ be a monic polynomial and $g, n \in \mathbb{N}^*$. When it is called on the input (P, g, n), the algorithm* `NewtonSums` *performs at most $\tilde{O}(ng)$ operations in K.*

Proof. The inverse power series of P^* modulo (t^{n+1}, z^g) in $K[\![t,z]\!]$ is computed by the Newton iteration $Q \mapsto Q(2 - QP^*)$. Therefore, the complexity of the computation of f

only depends on the complexity of multiplying two bivariate polynomials of total degree $n+g$. This can be done using at most $\tilde{O}(gn)$ operations in K. □

3.4.1.2 Hankel matrix-vector product

Let $g \in \mathbb{N}^*$. We recall that a $g \times g$ Hankel matrix A is a $g \times g$ matrix of the form

$$A = \begin{pmatrix} a_0 & a_1 & a_2 & \cdots & \cdots & a_{g-1} \\ a_1 & a_2 & & \cdots & \cdots & a_g \\ a_2 & & & & & \vdots \\ \vdots & & & & & \vdots \\ a_{g-1} & \cdots & \cdots & a_{2g-4} & a_{2g-3} & a_{2g-2} \end{pmatrix}.$$

Matrix-vector multiplication for this type of matrix can be computed in $O(M(g))$ arithmetic operations instead of $O(g^\omega)$, where $\omega \in [2,3[$ is the exponent of matrix multiplication. For $n \in \mathbb{N}$, let E_n be the K-vector space $K[\![t]\!]/(t^{n+1})$.

Proposition 3.4.3. *Let $n \in \mathbb{N}$. Let $A = (a_{i+j-2}(t))_{i,j} \in M_g(E_n)$ be a Hankel matrix and $v = (v_1(t), \cdots, v_g(t)) \in (E_n)^g$. Let f and h be the two polynomials*

$$f(t,z) = a_0(t) + a_1(t)z + a_2(t)z^2 + \cdots + a_{2g-3}(t)z^{2g-3} + a_{2g-2}(t)z^{2g-2}$$

and

$$h(t,z) = v_1(t)z^{g-1} + v_2(t)z^{g-2} + \cdots + v_g(t).$$

Write $f(t,z) \cdot h(t,z) \mod (t^{n+1}, z^{2g-1}) = \sum_{i=0}^{2g-2} w_i(t)z^i$ *then*

$$Av \mod t^{n+1} = (w_{g-1}, \cdots, w_{2g-2}).$$

Proof. Let $i \in \{1, \ldots, g\}$. The $(g-2+i)$-th coefficient of the product $R = f(t,z) \cdot h(t,z)$ is equal to

$$R_{g-2+i}(t) = \sum_{j=i-1}^{g-2+i} a_j(t)v_{j+2-i}(t) = \sum_{j=1}^{g} a_{i+j-2}(t)v_j(t).$$

Therefore, $R_{g-2+i}(t)$ is the i-th component of the product Av. □

This gives a quasi-linear algorithm to compute the matrix-vector product for Hankel matrices.

Algorithm 6: Hankel matrix-vector product

`HankelProd` (A, v, n)

Input : $A = (a_{i+j-2}(t))_{i,j} \in M_g(E_n)$,
$v = (v_1(t), \cdots, v_g(t)) \in (E_n)^g$, $n \in \mathbb{N}$.

Output: The product $Av \mod t^{n+1}$.

$f := a_0 + a_1 z + a_2 z^2 + \cdots + a_{2g-3} z^{2g-3} + a_{2g-2} z^{2g-2}$;

$h := v_1 z^{g-1} + v_2 z^{g-2} + \cdots + v_g$;

$w := fh \mod (t^{n+1}, z^{2g-1})$; // $w = \sum_{i=0}^{2g-2} w_i z^i$

return $w_{g-1}, \cdots, w_{2g-2}$

Proposition 3.4.4. *Let $n \in \mathbb{N}$. Let $A = (a_{i+j-2}(t))_{i,j} \in M_g(E_n)$ be a Hankel matrix and $v = (v_1(t), \cdots, v_g(t)) \in (E_n)^g$. When it is called on the input (A, v, n), the algorithm* `HankelProd` *performs at most $\tilde{O}(ng)$ operations in K.*

Proof. This is a direct consequence of Proposition 3.4.3. □

3.4.1.3 Transposed Vandermonde systems

We assume that K is an unramified extension of $\mathbb{Q}_p$. Let $g \in \mathbb{N}^*$. Let $U(t, z)$ be a degree g monic polynomial with coefficients in $\mathcal{O}_K[\![t]\!]$ such that $U(0, z)$ is separable over the residue field of K. Let L be the unramified extension $L = K[z]/U(0, z)$. Let $x_1(t), \cdots, x_g(t)$ be the roots of U in $L[\![t]\!]$ and A the matrix

$$A = \begin{pmatrix} f(t, x_1(t)) & f(t, x_2(t)) & \cdots & \cdots & f(t, x_g(t)) \\ x_1(t) f(t, x_1(t)) & x_2(t) f(t, x_2(t)) & & & x_n(t) f(x_g(t)) \\ \vdots & & & & \vdots \\ x_1(t)^{g-1} f(t, x_g(t)) & \cdots & & \cdots & x_g(t)^{g-1} f(t, x_g(t)) \end{pmatrix},$$

where $f \in \mathcal{O}_K[\![t]\!][z]$ is a polynomial of degree $g-1$ such that $f(t, x_i(t)) \mod (p, t) \neq 0$ for all $i = 1, \ldots, g$. Note that if $f = 1$ then A is a $g \times g$ Vandermonde matrix.
Let $v = (v_1(t), \cdots, v_g(t)) \in \mathcal{O}_K[\![t]\!]^g$ and consider the algebraic system

$$Aw = v \tag{52}$$

whose unknown is $w = (w_1(t), \cdots, w_g(t)) \in \overline{K}[\![t]\!]^g$.
Since A is an invertible matrix in $M_g(\mathcal{O}_L[\![t]\!])$, Equation (52) has a unique solution $w = A^{-1}v \in \mathcal{O}_L[\![t]\!]^g$.
Let $n \in \mathbb{N}$. Our goal is to find an approximation of the solution of Equation (52) modulo t^{n+1} by computing the polynomial $W(t,z) = \prod_{i=1}^{g}(z - w_i(t)) \mod t^{n+1}$.
The next proposition and its proof give a construction over $\mathcal{O}_K[\![t]\!]$ of an approximation of the interpolating polynomial of the data $\{(x_1, w_1), \cdots, (x_g, w_g)\}$ modulo t^{n+1}.

Proposition 3.4.5. *Let $n \in \mathbb{N}$. There exists a polynomial $h \in \mathcal{O}_K[\![t]\!][z]$ of degree $g-1$ such that $w_i = h(x_i) \mod t^{n+1}$ for all $i = 1, \cdots, g$.*

Proof. We give a construction of h using the approach in [KY89, Section 5]. Let $D(t,z)$ be the polynomial defined by

$$D(t,z) = v_1(t)z^g + v_2(t)z^{g-1} + \cdots + v_{n-1}(t)z^2 + v_g(t)z \mod t^{n+1}.$$

Write

$$U(t,z) \cdot D(t,z) = q_{2g}(t)z^{2g} + q_{2g-1}(t)z^{2g-1} + \cdots + q_1(t)z + q_0(t) \mod t^{n+1}$$

and

$$Q(t,z) = q_{2g}(t)z^{g-1} + q_{2g-1}(t)z^{g-2} + \cdots + q_{g+2}(t)z + q_{g+1}(t) \mod t^{n+1}.$$

For all $i = 1, \cdots, g$ we have the following relation

$$w_i(t) = \frac{Q(t, x_i(t))}{\partial_z U(t, x_i(t)) \cdot f(t, x_i(t))} \mod t^{n+1}.$$

Hence, we take h to be equal to

$$h(t,z) = \frac{Q(t,z)}{\partial_z U(t,z) \cdot f(t,z)} \mod U(t,z).$$

□

Corollary 3.4.6. *For all $i = 1, \ldots, g$, we have $w_i(t) \in L[\![t]\!]$. Moreover, the polynomial $W(t,z)$ has coefficients in $\mathcal{O}_K[\![t]\!]$.*

Proof. This is a direct consequence of Proposition 3.4.5 and the fact that $U(t,z) \in \mathcal{O}_K[\![t]\!][z]$. □

Until now, we have constructed an approximation $h(t,z)$ of the interpolating polynomial of the data $\{(x_1,w_1),\dots,(x_n,w_n)\}$ modulo t^{n+1}. The polynomial $W(t,z)$ is computed using the following relation:

$$W(t,h(t,z)) \equiv 0 \mod U(t,z).$$

Assuming that $W(0,z)$ is separable over K, we make use of a variant of the Kedlaya-Umans algorithm to find the polynomial $W(t,z)$ (see [KU11, Section 8.4]).

We summarize all the steps that we performed to solve Equation (52) in the following algorithm

Algorithm 7: Transposed Vandermonde system

`VandermondeSystem` (U,f,v,n)

Input : $U \in \mathcal{O}_K[\![t]\!][z]$, $f \in \mathcal{O}_K[\![t]\!][z]$, $v=(v_1,\cdots,v_g) \in \mathcal{O}_K[\![t]\!]^g$, $n \in \mathbb{N}$.

Output: $W(t,z)$ with the assumption: $W(0,z)$ is separable over K.

$D(t,z) := v_1(t)z^g + v_2(t)z^{g-1} + \cdots + v_{g-1}(t)z^2 + v_g(t)z \mod t^{n+1}$;

Write $U(t,z)\cdot D(t,z) = q_{2g}(t)z^{2g} + q_{2g-1}(t)z^{2g-1} + \cdots + q_1(t)z + q_0(t) \mod t^{n+1}$;

$Q(t,z) := q_{2g}(t)z^{g-1} + q_{2g-1}(t)z^{g-2} + \cdots + q_{g+2}(t)z + q_{g+1}(t) \mod t^{n+1}$;

$h(t,z) := Q(t,z)/(\partial_z U(t,z)\cdot f(t,z)) \mod U(t,z)$;

Compute $W(t,z)$ such that $W(t,h(t,z)) \equiv 0 \mod U(t,z)$

return $W(t,z)$

Proposition 3.4.7. *Let K be an unramified extension of $\mathbb{Q}_p$ and $g>0$ and $n \geq 0$ two integers. Let $U(t,z) = \prod_{i=1}^{g}(z-x_i(t))$ be a polynomial with coefficients in $\mathcal{O}_K[\![t]\!]$ such that $U(0,z)$ is separable over the residue field of K. Let $f \in \mathcal{O}_K[\![t]\!][z]$ be of degree $g-1$ such that $f(t,x_i(t)) \mod (p,t) \neq 0$ for all $i=1,\dots,g$ and $v=(v_1(t),\cdots,v_g(t)) \in \mathcal{O}_K[\![t]\!]^g$. When it is called on the input (U,f,v,n), the algorithm* `VandermondeSystem` *performs at most $\tilde{O}(ng)$ operations in $\mathcal{O}_K$.*

Proof. The final step of Algorithm 7 uses the Kedlaya-Umans algorithm, therefore it can be executed with time complexity $\tilde{O}(gn)$. It is easy to see that all the other steps can be executed with time complexity $\tilde{O}(gn)$ as well. □

3.4.2 Achieving quasi-optimality

In this subsection, we give a proof of Theorem 3.4.1 by showing that the Newton iteration given in Equation (51) can be executed with quasi-linear time complexity to give the desired polynomial in the theorem. The precision analysis has been already studied in Chapter 3.

Let K be a fixed unramified extension of $\mathbb{Q}_p$ of degree d and k its residue field. Let $g > 1$ be an integer and let $G(t) \in \mathcal{O}_K[\![t]\!]$. Let also f_2 be a polynomial of degree at most $O(g)$ and let $U_0(z) \in \mathcal{O}_K[z]$ be a polynomial of degree g which is separable over k. For the sake of simplicity, we assume that U_0 is irreducible, therefore its splitting field L is an unramified extension of degree g of K. Let $x_1^{(0)}, \ldots, x_g^{(0)}$ be the roots of $U_0(z)$ in L and $X_0 = (x_1^{(0)}, \ldots, x_g^{(0)})$. For $i = 1, \ldots, g$, we assume that $f_2(x_i^{(0)})$ has a square root $y_i^{(0)}$ in $\mathcal{O}_L$. Take $Y_0 = (y_1^{(0)}, \ldots, y_g^{(0)})$ and let $V_0(z) \in \mathcal{O}_K[z]$ be the interpolating polynomial of the data $\{(x_1^{(0)}, y_1^{(0)}), \ldots, (x_g^{(0)}, y_g^{(0)})\}$. We assume that the unique solution $X(t) = (x_1(t), \ldots, x_n(t))$ of Equation (48) has coefficients in $\mathcal{O}_L$ when X_0 and Y_0 are the initial conditions.

Let $m \in \mathbb{N}$ and $n = 2m+1$. Let $X_m(t) = (x_1^{(m)}(t), \ldots, x_g^{(m)}(t))$ be an approximation of $X(t)$ modulo t^{m+1} represented by the minimal polynomial of $x_1^{(m)}$, $U_m(t, z) = \prod(z - x_i^{(m)}(t))$. We show in the next proposition that we can compute efficiently an approximation $X_n(t) = (x_1^{(n)}(t), \ldots, x_g^{(n)}(t))$ of $X(t)$ modulo t^{n+1} represented by the minimal polynomial $U_n(t, z)$ of $x_1^{(n)}(t)$ using Equation (51).

Proposition 3.4.8. *Using the same notations as above, there exists an algorithm that computes $U_n(t, z)$ from $U_m(t, z)$ with time complexity $\tilde{O}(mg)$.*

Proof. Let $Y_m(t) = (y_1^{(m)}(t), \ldots, y_g^{(m)}(t))$ be the vector in $\mathcal{O}_L[\![t]\!]^g$ defined as follows

$$y_i^{(m)}(t)^2 = f_2(x_i^{(m)}(t)) \mod t^{m+1}, \qquad y_i^{(m)}(0) = y_i^{(0)}$$

for all $i = 1, \ldots, g$.

The algorithm performs the following steps.

1. Compute the degree $g-1$ polynomial $W_m(t, z) = \sum_{i=0}^{g-1} w_i^{(m)}(t)\, z^i$ such that

$$W_m(t, z)^2 \equiv 1/f(z) \mod (t^{m+1}, U_m(t, z))$$

and $W_m(0, z) = 1/V_0(z) \mod U_0(z)$. Observe that it is the interpolating polynomial

of the points:

$$\{(x_1^{(m)}, 1/y_1^{(m)}), \cdots, (x_g^{(m)}, 1/y_g^{(m)})\}.$$

2. Compute the Newton sums $s_i^{(m)}(t) = \sum_{j=1}^{g} (x_j^{(m)}(t))^i \mod t^{m+1}$ for $i = 1, \ldots, 2g-1$ using Algorithm 5. Deduce $r_i^{(m)}(t) = \sum_{j=1}^{g} (x_j^{(m)}(t))^{i-1} (x_j^{(m)}(t))' \mod t^m$.

3. Using Algorithm 6, compute the two products $H(X_m(t))X'_m(t)$ and $H(X_m(t))X_m(t)$ as follows:

$$H(X_m(t))X'_m(t) = \begin{pmatrix} r_1^{(m)} & r_2^{(m)} & \cdots & r_g^{(m)} \\ r_2^{(m)} & r_3^{(m)} & & r_{g+1}^{(m)} \\ \vdots & & & \\ r_g^{(m)} & r_{g+1}^{(m)} & \cdots & r_{2g-1}^{(m)} \end{pmatrix} \begin{pmatrix} w_0^{(m)} \\ w_1^{(m)} \\ \vdots \\ w_{g-1}^{(m)} \end{pmatrix} \mod t^m$$

and

$$H(X_m(t))X_m(t) = \begin{pmatrix} s_1^{(m)} & s_2^{(m)} & \cdots & s_g^{(m)} \\ s_2^{(m)} & s_3^{(m)} & & s_{g+1}^{(m)} \\ \vdots & & & \\ s_g^{(m)} & s_{g+1}^{(m)} & \cdots & s_{2g-1}^{(m)} \end{pmatrix} \begin{pmatrix} w_0^{(m)} \\ w_1^{(m)} \\ \vdots \\ w_{g-1}^{(m)} \end{pmatrix} \mod t^{m+1}$$

4. Compute $F_m(t) = H(X_m(t))X_m(t) - \int (G(t) - H(X_m(t))X'_m(t))\, dt$.

5. Compute $U_n(t, z) =$`VandermondeSystem` (U_m, W_m, F_m, n).

We now discuss the complexity analysis. The polynomial W_m in step 1 can be efficiently computed by the classical Newton scheme for extracting square roots. Since its coefficients are polynomials of degrees at most m defined over $\mathcal{O}_K$, the complexity of this step is $O(\mathrm{M}(m)\mathrm{M}(g))$. By Proposition 3.4.2, the computation of the Newton sums $s_i^{(m)}$ of U_m in step 2 can be carried out for a cost of $\tilde{O}(mg)$ operations. In step 3, we are dealing with two Hankel matrix-vector products. This can be done in $O(\mathrm{M}(m)\mathrm{M}(g))$ operations in $\mathcal{O}_K$ (see Proposition 3.4.4). Step 5 computes U_n, the minimal polynomial of $x_1^{(n)}$. We make use of Algorithm 7 to execute step 5; by Proposition 3.4.7 the resulting bit complexity is $\tilde{O}(mg)$. □

Remark 3.4.9. We gave in the proof of Proposition 3.4.8 a quasi-optimal algorithm that

solves Equation (51). Unfortunately, it cannot be implemented yet in an optimized way, since it uses the Kedlaya-Umans algorithm as a subroutine (step 5).

In conclusion, Theorem 3.4.1 is proved by executing the Newton iteration in Algorithm 4 using the algorithm constructed in the proof of Proposition 3.4.8.

3.5 Fast computation of the multiplication-by-ℓ maps

We discuss in this section important examples of isogenies: the multiplication-by-ℓ maps. It has been proved that the degrees of the components of a rational representation of the multiplication-by ℓ are bounded by $O(\ell^2)$, only for curves of genus 2 and 3 [Abe18, Chapter 4]. In the general case, it has been shown that these degrees are bounded by $O_g(\ell^3)$ [1] [Abe18, Theorem 4.13], although experiments show that they are only quadratic in ℓ.
In Section 3.5.1, we use the results of Section 3.2.2 to reduce the bound to $O(g\ell^2)$. Consequently, we obtain (using Theorem 3.4.1) a quasi-optimal algorithm to compute a rational representation of the multiplication by an integer.

Classical algorithms for computing a rational representation of the multiplication endomorphism are usually based on Cantor's paper [Can94] and Cantor's algorithm for adding points on Jacobians (see for example [Abe18]). Although, they exhibit acceptable running time in practice, their theoretical complexity has not been well studied yet and experiments show that they become much slower when the degree or the genus get higher. Actually, in many cases, we have observed that an optimized version [2] of Algorithm 4 performs better in practice even if its theoretical complexity in g is not optimal (see Section 3.5.2).

3.5.1 Cantor ℓ-division polynomials

Let $C : y^2 = f(x)$ be a hyperelliptic curve of genus g over a finite field k and $\ell > g$ an integer coprime to the characteristic of k.
Let $P \in C(k)$. For a generic point $Q = (x, y)$ on C, the Mumford representation of the

1. the notation O_g means that we are hiding the terms that depend on g
2. When computing rational representations, the matrix H in Algorithm 4 is a structured matrix. Therefore, the Newton iteration can be executed with complexity at most $\tilde{O}(g^2\ell)$ instead of $\tilde{O}(g^\omega\ell)$ operations in an unramified extension of the base field of degree at most $O(g!)$

element $\ell[Q-P]$ in the Jacobian of C can be written as follows

$$\ell[Q-P] = \left(X^g + \sum_{i=1}^{g-1} \frac{d_i(x)}{d_g(x)} X^i,\ y \sum_{i=1}^{g-1} \frac{e_i(x)}{e_g(x)} X^i \right).$$

where the numerators $d_0, \ldots, d_{g-1}, e_0, \ldots, e_{g-1}$ are polynomials in $k[x]$ and the denominators d_g and e_g are monic polynomials in $k[x]$. Therefore, $\left(\frac{d_0}{d_g}, \ldots, \frac{d_{g-1}}{d_g}, \frac{e_0}{e_g}, \ldots, \frac{e_{g-1}}{e_g}\right)$ is a rational representation of the multiplication-by-ℓ map.

Definition 3.5.1. *The $2g+2$ polynomials $d_0, \ldots, d_g, e_0, \ldots e_g$ are called Cantor's ℓ-division polynomials.*

Since the multiplication-by-ℓ endomorphism is a separable $(\ell^2, \ldots, \ell^2)$-isogeny, we can then apply Propositions 3.2.7 and 3.2.11 and Remark 3.2.8 in order to obtain bounds on the degrees of the Cantor's ℓ-division polynomials. This gives the following result

Proposition 3.5.2. *The degrees of the polynomials $d_0, \ldots, d_g$ are bounded by $g\ell^2$. Moreover,*

— *if P is a Weierstrass point, then the degrees of $e_0, \ldots, e_g$ are bounded by*

$$\begin{cases} \frac{3}{2}g\ell^2 + g + 1 & \text{if } \deg(f) = 2g+1 \\ 2g\ell^2 + g + 1 & \text{otherwise} \end{cases}$$

— *if P is not a Weierstrass point, then the degrees of $e_0, \ldots, e_g$ are bounded by*

$$\begin{cases} 3g\ell^2 + g + 1 & \text{if } \deg(f) = 2g+1 \\ 4g\ell^2 + g + 1 & \text{otherwise} \end{cases}$$

Remark 3.5.3. The bounds obtained in Propostion 3.5.2 are not optimal. In fact, the experiments carried out by Abelard in his thesis [Abe18, Section 4.2] show that Cantor ℓ-division polynomials have degrees smaller than the bounds that we have obtained in Propostion 3.5.2.

To conclude, we state the following theorem

Theorem 3.5.4. *Let p an odd prime number and $g > 1$ an integer. Let ℓ be an integer greater than g and coprime to p. Let $C : y^2 = f(x)$ be a hyperelliptic curve of genus g defined over a finite field k of odd characteristic p. There exists an algorithm that computes Cantor ℓ-division polynomials of C, performing at most $\tilde{O}(\ell^2 g^2)$ operations in k.*

Proof. Let p be the characteristic of k and $d = [k : \mathbb{F}_p]$. The algorithm performs the following steps:

1. Lift C arbitrarily as $\widetilde{C} : y^2 = \tilde{f}(x)$ over an unramified extension of $\mathbb{Q}_p$ of degree d with a p-adic precision equal to $1 + \lfloor \log_p(2g\ell^2) \rfloor$.
2. Pick a Weierstrass point $P \in C(k)$. If such a point doesn't exist, chose $P \in C(k)$ randomly.
3. Chose a point $Q \in C(k)$ different from P such that $\ell[Q - P]$ is generic.
4. Solve the differential equation (48) by applying the algorithm of Theorem 3.4.1 to the following input.
   — g and $n = 2g\ell^2$,
   — $f_2 = \tilde{f}$,
   — $U_0(z)$: the first Mumford coordinate of $\ell[Q - P]$,
   — $V_0(z)$: the second Mumford coordinate of $\ell[Q - P]$,
   — The matrix $G(t)$ given by the following relation

$$G = \frac{\ell}{v(t)} \begin{pmatrix} 1 \\ u(t) \\ u(t)^2 \\ \vdots \\ u(t)^{g-1} \end{pmatrix}$$

   where $u(t) = t + x_Q$ and $v(t) = \sqrt{f(u(t))}$ such that $v(0) = y_Q$.
   Let $U(t, z)$ be the reduction of the output of the algorithm in k.
5. Reconstruct from $U(t, z)$ the $g + 1$ polynomials $d_0, \ldots, d_g$.
6. Recover the polynomials $e_0, \ldots, e_g$ from $d_0, \ldots, d_g$ and the equation of C.

The time complexity of the algorithm depends mainly on the complexity of steps 4,5 and 6. According to Theorem 3.4.1, step 4 can be carried out for a cost of $\tilde{O}(g\ell^2)$ operations in k. The $g+1$ polynomials $d_0, \ldots, d_g$ are obtained by reconstructing (for example) d_0/d_g from the constant coefficient of U then multiplying the other coefficients of U by d_g to recover $d_1, \ldots, d_{g-1}$. Therefore, step 5 requires $\tilde{O}(g^2\ell^2)$ operations in k as well. Step 6 is executed as follows: we make use of the polynomials $d_0, \ldots, d_g$ to increase the t-adic approximation of the polynomial $U(t, z)$ to $2\deg(e_0)$. We compute, using a Newton iteration, the degree

g polynomial $V(t,z)$ such that $V(0,z) = V_0(z)$ and

$$V(z,t)^2 \equiv f(z) \mod (t^{2\deg(e_0)}, U(t,z)).$$

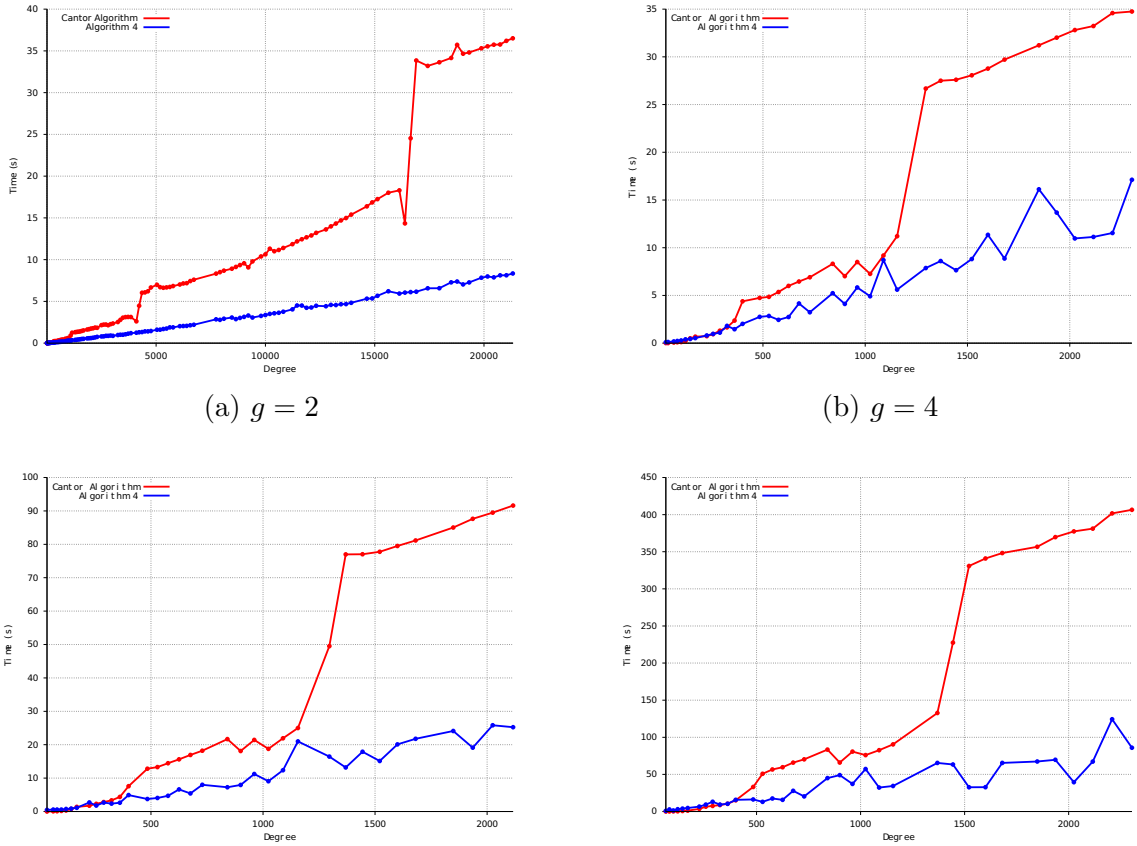
We reconstruct (for example) the rational fraction e_0/e_g from the constant coefficient of V. The polynomials $e_1, \ldots, e_{g-1}$ are obtained by multiplying e_g with the non-constant coefficients of V. This can be carried out using $\tilde{O}(g^2\ell^2)$ operations in k. □

3.5.2 Experiments

Since step 4 of the algorithm of Theorem 3.5.4 cannot yet be used in practice, we made an implementation in MAGMA of an optimized version of Algorithm 4 to compute Cantor ℓ-division polynomials in $\mathbb{F}_7$ for hyperelliptic curves of genus 2, 4, 5 and 7. We compare our implementation to an already existing one which uses Cantor's algorithm implemented in MAGMA and which formally calculates the Mumford representation of $\ell[Q-P]$. Timings are detailed in Figure 3.3. In most cases, the initial condition is chosen so that the degree of the extensions of $\mathbb{Q}_7$ on which we run our algorithm, is at most equal to g.

For $g = 2$, all the calculations were done in the ring $\mathbb{Z}_7$ with a fixed precision (this is why our algorithm is quasi-linear for $g = 2$). The sawtooth patterns on the blue curves of Figures (b), (c) and (d) appear because the degrees of the extensions that we work on varies depending on the initial condition we take to solve the differential system.

The different levels observed on the red curves in Figure 3.3 can be explained by the number of operations (additions and doublings) performed by Cantor's algorithm on the Jacobian of the curve, in order to compute the scalar multiplication $\ell[Q-P]$. For example, for $\ell = 2^6$, the computation of $\ell[Q-P]$ requires 6 operations. But for $\ell = 2^6+1$, we need 7 operations to compute $\ell[Q-P]$. We give an illustration of this phenomenon for $g = 2$ in Figure 3.4.



(a) $g = 2$ (b) $g = 4$

(c) $g = 5$ (d) $g = 7$

Timings obtained with MAGMA V2.25-7 on a laptop with an INTEL processor E5-2687WV4@3.00GHZ

Figure 3.3 – Computation of the multiplication-by-ℓ map for the hyperelliptic curve $y^2 = x^{2g+1} + 3x^2 + 4x + 1$ over $\mathbb{F}_7$

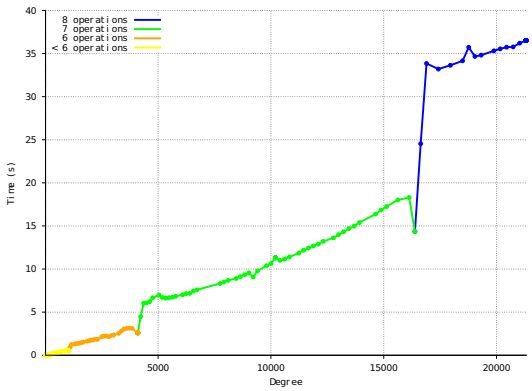


Figure 3.4 – The different levels observed when using Cantor's algorithm to compute $\ell[Q - P]$ for $g = 2$

Chapter 4

A SEMI-CONTINUITY RESULT

In Chapter 1, motivated by the explicit computation of isogenies in characteristic 2, we introduced and studied the following nonlinear 2-adic differential equation:

$$U \cdot z'^2 = V(z) \tag{53}$$

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 Equation (53) can be rewritten as follows:

$$t(t-4a) \cdot z'^2 = g^2 \cdot h(z). \tag{54}$$

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 chapter, we aim at revisiting our results and extracting from them theoretical information about the structure of the solutions of Equations (53) and (54).

4.1 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

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

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 1.2.3, 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 numbers 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 1.2.4 allow us to derive inequalities in the other direction.

Proposition 4.1.1. *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 estimate*

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

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 1.2.4, 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. □

4.2 Generic radius of convergence

We now come back to the nonlinear differential equations (53) and (54); 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 nonnegative 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 Equation (53) 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 4.2.1. *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 Equation (53) in $tK[\![t]\!]$ (*cf *Proposition 1.2.1). 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 to 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 Equation (15) (obtained in the proof of Proposition 1.2.1), 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

$$\|U\|_r \cdot |z_{j+1}| \cdot |z_{i-j+1}| \cdot r^{i-n} \leq C \cdot |v_1| \cdot \rho^{-n} \tag{55}$$

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 (55) 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. □

4.3 Overconvergence phenomena

Under Assumptions (H_U) and (H_V), Proposition 4.2.1 shows that the radius of convergence of the solution of Equation (53) 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 Equation (12) (*cf* page 32), 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 phenomenon we observed persists when the differential equation is slightly perturbed.

From now on, we work with the differential equation (54) (which is a particular case of Equation (53)). 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 1.2.4, we know that Equation (54) admits a unique solution $z_g \in tK[\![t]\!]$

for all $g \in \Omega$.

Lemma 4.3.1. *Let $r \in]0,1[$ and $g \in \mathcal{V}_r$. The following are equivalent:*

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

(b) $\|g\|_r = |g(0)|$, i.e. *the maximum of g is reached at the origin.*

Besides, if these conditions are satisfied then g is invertible in $\mathcal{V}_r$ and $\|g^{-1}\|_r = \|g\|_r^{-1}$.

Proof. It is a direct consequence of the Weierstrass Preparation Theorem. □

Proposition 4.3.2. *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 Equation (54) is in $\mathcal{V}_r$.

Then, for all $\gamma_1, \gamma_2 \in \mathcal{V}_{r,+}$ such that

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

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

Proof. Without loss of generality, we can assume that $\gamma_1 = 0$. For a general γ_1, we apply the same argument after having replaced g by $g + \gamma_1$ and γ_2 by $\gamma_2 - \gamma_1$.
We follow the proof of Proposition 1.2.17. 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 1.2.5, 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 1.2.14 shows that the differential of θ_n at a point $\gamma \in W_n$ is given by

$$d\theta_n(\gamma) : \delta g \mapsto z'_{g+\gamma} \cdot (g+\gamma)^{-1} \cdot \psi_{+,n}(\delta g). \tag{56}$$

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 confusion 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 Equation (56) 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 Equation (23), 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

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

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

$$\theta_n\Big(B_{E_n}(\delta)\Big) = d\theta_n(0)\Big(B_{E_n}(\delta)\Big) \subset B_{F_n}(\delta) \tag{57}$$
$$\text{when} \quad \delta < \min\left(\|z'_g\|_{F_n},\ \frac{\|g\|_{F_n}}{2},\ \frac{\|g\|^2_{F_n}}{4{\cdot}\|z'_g\|_{F_n}}\right) = \min\left(\|z'_g\|_{F_n},\ \frac{\|g\|^2_{F_n}}{4{\cdot}\|z'_g\|_{F_n}}\right).$$

The last equality comes from the observation that $\frac{1}{2}{\cdot}\|g\|_{F_n}$ is the geometric mean between the two other arguments in the minimum. Passing to the limit on n in Equation (57), we get the proposition when $\gamma_1 = 0$. □

Corollary 4.3.3. *Let $r \in]0,1[$. We consider $g_0 \in \mathcal{V}_r$ satisfying the two following assumptions:*

(a) g_0 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 Equation (54) is in $\mathcal{V}_r$.

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

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

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

Proof. We apply Proposition 4.3.2 with $r = \rho$, $g = g_0$, $\gamma_1 = g - g_0$ and $\gamma_2 = 0$ and then conclude by using Proposition 4.1.1 combined with the fact that $\|t(t-4a)\|_\rho \leq 1$. □

Corollary 4.3.3 implies in particular that, for any real number $r \in]0,1[$, the function $\mathcal{V}_r \to \mathbb{R}$ 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 4.3.2, it is even locally constant around each point g such that $\mathrm{RoC}(z_g) < r$.

Conclusion and perspectives

We end this thesis by summarizing the main contributions and some perspectives related to them.

Chapter 1

In Chapter 1, we filled a gap in the algorithmic toolbox for computing isogenies of elliptic curves defined over finite fields by designing fast algorithms that compute isogenies between elliptic curves over fields of characteristic two. Our algorithms are based on the computation of an approximation of Elkies' 2-adic differential equation:

$$c^2 \cdot \left(4t + (4a_2+1)t^2 + 4a_6t^4\right) \cdot z'^2 = 4z + (4\tilde{a}_2+1)z^2 + 4\tilde{a}_6z^4. \tag{58}$$

Since Equation (58) does not have the same form as the differential equations constructed for computing isogenies in odd characteristic, it will be necessary to study this case separately, which turns out to be much more complicated.
In Section 1.2.5, we showed that a small modification of the parameters of the differential equation modifies its solution z by some increment dz which is, itself, a solution of a linear differential equation. By analysing the analytical behaviour of this perturbation, we deduced some excellent properties behind the numerical stability of the algorithm.
As a consequence, we deduced a quasi-optimal algorithm that computes isogenies and irreducible polynomials of large degrees over finite fields of characteristic two [1]. An implementation with the Magma computer algebra is available in [CEL19]; it is fairly optimized as we saw in the Figure 1.1 of Section 1.3.2.

We saw that the solution of the 2-adic differential equation (58) obtained from the computation of isogenies has coefficients in the ring of integers of it base field. One can ask if this particular property only arises when computing isogenies of elliptic curves. In other words, if we are given two elliptic curves E and $\widetilde{E}$ over an extension K of $\mathbb{Q}_2$ with coefficients in $\mathcal{O}_K$ and $c \in \mathcal{O}_K^*$, is it true that E and $\widetilde{E}$ are isogenous over K if and only

1. it can be used also to compute isogenies and irreducible polynomials of large degrees over finite fields of small characteristic

if the solution of Equation (58) has coefficients in $\mathcal{O}_K$?

Chapter 2 and 3

In Chapter 2, we studied the solution of a system of p-adic differential equations of the form

$$H(X(t)) \cdot X'(t) = G(t) \tag{59}$$

that we used in Chapter 3 to compute a rational representation of an isogeny between hyperelliptic curves over fields of odd characteristic. The algorithms that we have designed are based on a Newton scheme, which gives more and more accurate (for the t-adic distance) solution of Equation (59). The good numerical behaviour of these algorithms that we constructed in the two chapters comes from a fine precision analysis as we did in Chapter 1.

The complexity of the first algorithm (Algorithm 4) given in Section 2.2.2 is quasi-linear with respect to the degree ℓ but, unfortunately, it is not optimal with respect to the genus g of the curves. Thus, it can only be used efficiently to compute isogenies of Jacobians of hyperlliptic curves of small genus (Section 3.3). In Section 3.4 we revisited the Newton iteration of the main algorithm and make it quasi-linear in g as well but, in the contrary of the small genus case, it is difficult to implement it in an optimized way since it uses the Kedlaya-Umans [KU11] algorithm as a subroutine. Therefore, it will be interesting to find another way to optimize Algorithm 4 in order to have an efficient implementation in the arbitrary genus case.

We made use of our algorithms to compute the rational representation of the multiplication-by-ℓ map. We observed that they perform better in practice than Cantor's (see Section 3.5).

Chapter 4

In Chapter 4, we reused the techniques of p-adic precision introduced in the core of Chapter 1 to prove that the radius of convergence of the solution of the 2-adic differential equation (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 the main algorithm of Chapter 1. Indeed, the assumption on z made in the main theorem of Chapter 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.

So far, all the p-adic differential equations that we deal with come from a geometric construction. Incidentally, our analysis highlights some remarkable properties of these non-linear equations (overconvergence, semi-continuity of the radius of convergence, *etc*). Therefore, it would be interesting to know if we can expect such behaviour for a wider class of p-adic non-linear differential equations and obtain general results for those equations.

BIBLIOGRAPHY

[Abe18] Simon Abelard, « Comptage de points de courbes hyperelliptiques en grande caractéristique : algorithmes et complexité », Thèse de doctorat dirigée par Gaudry, Pierrick et Spaenlehauer, Pierre-Jean Informatique Université de Lorraine 2018, PhD thesis, 2018, URL: http://www.theses.fr/2018LORR0104.

[Atk88] A. O. L. Atkin, *The number of points on an elliptic curve modulo a prime*, manuscript, Chicago IL, 1988.

[Bal10] Francesco Baldassarri, « Continuity of the radius of convergence of differential equations on p-adic analytic curves », *in*: *Inventiones mathematicae* 182.*3* (2010), pp. 513–584, DOI: 10.1007/s00222-010-0266-7, URL: https://doi.org/10.1007/s00222-010-0266-7.

[Bal+17] Sean Ballentine, Aurore Guillevic, Elisa Lorenzo García, Chloe Martindale, Maike Massierer, Benjamin Smith, and Jaap Top, « Isogenies for point counting on genus two hyperelliptic curves with maximal real multiplication », *in*: *Algebraic geometry for coding theory and cryptography*, Springer, 2017, pp. 63–94.

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust, « The Magma algebra system. I. The user language », *in*: *J. Symbolic Comput.* 24.*3-4* (1997), Computational algebra and number theory (London, 1993), pp. 235–265, ISSN: 0747-7171, DOI: 10.1006/jsco.1996.0125, URL: http://dx.doi.org/10.1006/jsco.1996.0125.

[BCR10] Gaetan Bisson, Robert Cosset, and Damien Robert, « AVIsogenies (abelian varieties and isogenies) », *in*: *Magma package for explicit isogenies between abelian varieties, http://avisogenies. gforge. inria. fr* (2010).

[Ber88] V G Berkovich, *Spectral theory and analytic geometry over non-Archimedean fields, 2*, tech. rep. IHES-M-88-43, Bures-sur-Yvette: Inst. Hautes Etud. Sci., 1988, URL: http://cds.cern.ch/record/191097.

[Ber93] Vladimir G. Berkovich, « Étale cohomology for non-Archimedean analytic spaces », en, *in*: *Publications Mathématiques de l'IHÉS* 78 (1993), pp. 5–161, URL: www.numdam.org/item/PMIHES_1993__78__5_0/.

[Bos+05] A. Bostan, L. González-Vega, H. Perdry, and É. Schost, « From Newton sums to coefficients: complexity issues in characteristic p », *in*: *MEGA'05*, Eighth International Symposium on Effective Methods in Algebraic Geometry, Porto Conte, Alghero, Sardinia (Italy), May 27th – June 1st, 2005.

[Bos+06] Alin Bostan, Bruno Salvy, Francois Morain, and Eric Schost, *Fast algorithms for computing isogenies between elliptic curves*, Research Report, 2006, p. 28, URL: https://hal.inria.fr/inria-00091441.

[Bos+08] A. Bostan, F. Morain, B. Salvy, and É. Schost, « Fast algorithms for computing isogenies between elliptic curves », *in*: *Math. Comp.* 77.*263* (2008), pp. 1755–1778, ISSN: 0025-5718, DOI: 10.1090/S0025-5718-08-02066-8, URL: https://doi.org/10.1090/S0025-5718-08-02066-8.

[Bos+17] Alin Bostan, Frédéric Chyzak, Marc Giusti, Romain Lebreton, Grégoire Lecerf, Bruno Salvy, and Éric Schost, « Algorithmes Efficaces en Calcul Formel », *in*: 2017.

[Bri+19] Ludovic Brieulle, Luca De Feo, Javad Doliskani, Jean-Pierre Flori, and Éric Schost, « Computing isomorphisms and embeddings of finite fields », *in*: *Math. Comp.* 88.*317* (2019), pp. 1391–1426, ISSN: 0025-5718, DOI: 10.1090/mcom/3363, URL: https://doi.org/10.1090/mcom/3363.

[BS11] Gaetan Bisson and Andrew V. Sutherland, « Computing the endomorphism ring of an ordinary elliptic curve over a finite field », *in*: *J. Number Theory* 131.*5* (2011), pp. 815–831, ISSN: 0022-314X, DOI: 10.1016/j.jnt.2009.11.003, URL: https://doi.org/10.1016/j.jnt.2009.11.003.

[BSS99] I. Blake, G. Seroussi, and N. Smart, *Elliptic Curves in Cryptography*, London Mathematical Society Lecture Note Series, Cambridge University Press, 1999, DOI: 10.1017/CBO9781107360211.

[Can94] David G. Cantor, « On the analogue of the division polynomials for hyperelliptic curves. », *in*: 1994.*447* (1994), pp. 91–146, DOI: doi:10.1515/crll.1994.447.91, URL: https://doi.org/10.1515/crll.1994.447.91.

[Car17] Xavier Caruso, « Computations with p-adic numbers », en, *in*: *Les cours du CIRM* 5.*1* (2017), DOI: 10.5802/ccirm.25, URL: https://ccirm.centre-mersenne.org/item/CCIRM_2017__5_1_A2_0.

[CE15] Jean-Marc Couveignes and Tony Ezome, « Computing functions on Jacobians and their quotients », *in*: *LMS Journal of Computation and Mathematics* 18.*1* (2015), 555–577, DOI: 10.1112/S1461157015000169.

[CEL12] Jean-Marc Couveignes, Tony Ezome, and Reynald Lercier, « A faster pseudo-primality test », *in*: *Rend. Circ. Mat. Palermo (2)* 61.*2* (2012), pp. 261–278, ISSN: 0009-725X, DOI: 10.1007/s12215-012-0088-0, URL: https://doi.org/10.1007/s12215-012-0088-0.

[CEL19] Xavier Caruso, Èlie Eid, and Reynald Lercier, *Package IsoCar2G1*, https://github.com/rlercier/isocar2g1, 2019.

[CEL20] Xavier Caruso, Elie Eid, and Reynald Lercier, « Fast computation of elliptic curve isogenies in characteristic two », working paper or preprint, Mar. 2020, URL: https://hal.archives-ouvertes.fr/hal-02508825.

[CF96] J. W. S. Cassels and E. V. Flynn, *Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2*, London Mathematical Society Lecture Note Series, Cambridge University Press, 1996, DOI: 10.1017/CBO9780511526084.

[CH02] Jean-Marc Couveignes and Thierry Henocq, « Action of Modular Correspondences around CM Points », *in*: *Algorithmic Number Theory*, ed. by Claus Fieker and David R. Kohel, Berlin, Heidelberg: Springer Berlin Heidelberg, 2002, pp. 234–243.

[CL09] Jean-Marc Couveignes and Reynald Lercier, « Elliptic periods for finite fields », *in*: *Finite Fields Appl.* 15.*1* (2009), pp. 1–22, ISSN: 1071-5797, DOI: 10.1016/j.ffa.2008.07.004, URL: https://doi.org/10.1016/j.ffa.2008.07.004.

[CL13] Jean-Marc Couveignes and Reynald Lercier, « Fast construction of irreducible polynomials over finite fields », *in*: *Israel J. Math.* 194.*1* (2013), pp. 77–105, ISSN: 0021-2172, DOI: 10.1007/s11856-012-0070-8, URL: https://doi.org/10.1007/s11856-012-0070-8.

[Cou06] Jean-Marc Couveignes, « Hard homogeneous spaces », http://eprint.iacr.org/2006/291/, 2006.

[Cou96] J.-M. Couveignes, « Computing l-isogenies using the p-torsion », *in*: *Algorithmic Number Theory*, ed. by H. Cohen, vol. 1122, Lecture Notes in Computer Science, Proceedings of the Second International Symposium, ANTS-II, Talence, France, May 1996, Springer-Verlag, 1996, pp. 59–65.

[Cox13] David A. Cox, *Primes of the form x^2+ny^2*, Second, Pure and Applied Mathematics (Hoboken), Fermat, class field theory, and complex multiplication, John Wiley & Sons, 2013, pp. xviii+356, ISBN: 978-1-118-39018-4, DOI: 10.1002/9781118400722, URL: https://doi.org/10.1002/9781118400722.

[CR15] Romain Cosset and Damien Robert, « Computing (ℓ, ℓ)-isogenies in polynomial time on Jacobians of genus 2 curves », *in*: *Mathematics of Computation* 84.*294* (2015), pp. 1953–1975.

[CRV14] Xavier Caruso, David Roe, and Tristan Vaccon, « Tracking p-adic precision », *in*: *LMS J. Comput. Math.* 17.*suppl. A* (2014), pp. 274–294, DOI: 10.1112/S1461157014000357, URL: https://doi.org/10.1112/S1461157014000357.

[CRV15] Xavier Caruso, David Roe, and Tristan Vaccon, « p-adic stability in linear algebra », *in*: *ISSAC'15—Proceedings of the 2015 ACM International Symposium on Symbolic and Algebraic Computation*, ACM, New York, 2015, pp. 101–108.

[CS20] Craig Costello and Benjamin Smith, « The supersingular isogeny problem in genus 2 and beyond », *in*: *International Conference on Post-Quantum Cryptography*, Springer, 2020, pp. 151–168.

[Del74] Pierre Deligne, « La conjecture de Weil : I », fr, *in*: *Publications Mathématiques de l'IHÉS* 43 (1974), pp. 273–307, URL: www.numdam.org/item/PMIHES_1974__43__273_0/.

[Del80] Pierre Deligne, « La conjecture de Weil : II », fr, *in*: *Publications Mathématiques de l'IHÉS* 52 (1980), pp. 137–252, URL: www.numdam.org/item/PMIHES_1980__52__137_0/.

[Deu41] Max Deuring, « Die Typen der Multiplikatorenringe elliptischer Funktionenkörper », *in*: *Abh. Math. Sem. Hansischen Univ.* 14 (1941), pp. 197–272, ISSN: 0025-5858, DOI: 10.1007/BF02940746, URL: https://doi.org/10.1007/BF02940746.

[DF11] Luca De Feo, « Fast algorithms for computing isogenies between ordinary elliptic curves in small characteristic », *in*: *J. Number Theory* 131.*5* (2011), pp. 873–893, ISSN: 0022-314X, DOI: 10.1016/j.jnt.2010.07.003, URL: https://doi.org/10.1016/j.jnt.2010.07.003.

[DFJP14a] Luca De Feo, David Jao, and Jérôme Plût, « Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies », *in*: *Journal of Mathematical Cryptology* 8.*3* (2014), pp. 209 –247, DOI: https://doi.org/10.1515/jmc-2012-0015, URL: https://www.degruyter.com/view/journals/jmc/8/3/article-p209.xml.

[DFJP14b] Luca De Feo, David Jao, and Jérôme Plût, « Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies », *in*: *J. Math. Cryptol.* 8.*3* (2014), pp. 209–247, ISSN: 1862-2976, DOI: 10.1515/jmc-2012-0015, URL: https://doi.org/10.1515/jmc-2012-0015.

[DH76] W. Diffie and M. Hellman, « New Directions in Cryptography », *in*: *IEEE Trans. Inf. Theor.* 22.*6* (Nov. 1976), 644–654, ISSN: 0018-9448, DOI: 10.1109/TIT.1976.1055638, URL: https://doi.org/10.1109/TIT.1976.1055638.

[Dix82] John D. Dixon, « Exact solution of linear equations using p-adic expansions », *in*: *Numerische Mathematik* 40.*1* (1982), pp. 137–141, DOI: 10.1007/BF01459082, URL: https://doi.org/10.1007/BF01459082.

[DL08] I. Dolgachev and D. Lehavi, *On isogenous principally polarized abelian surfaces*, 2008, arXiv: 0710.1298 [math.AG].

[Dwo60] Bernard Dwork, « On the Rationality of the Zeta Function of an Algebraic Variety », *in*: *American Journal of Mathematics* 82.*3* (1960), pp. 631–648, ISSN: 00029327, 10806377, URL: http://www.jstor.org/stable/2372974.

[Dwo69] B. Dwork, « p-adic cycles », *in*: *Publications Mathématiques de l'Institut des Hautes Études Scientifiques* 37.*1* (1969), pp. 27–115, DOI: 10.1007/BF02684886, URL: https://doi.org/10.1007/BF02684886.

[Eid20] Elie Eid, *Fast computation of hyperelliptic curve isogenies in odd characteristic*, 2020, arXiv: 2009.12180 [math.AG].

[EL13] Tony Ezome and Reynald Lercier, « Elliptic periods and primality proving », *in*: *J. Number Theory* 133.*1* (2013), pp. 343–368, ISSN: 0022-314X, DOI: 10.1016/j.jnt.2012.07.007, URL: https://doi.org/10.1016/j.jnt.2012.07.007.

[Elk98] N. Elkies, « Elliptic and modular curves over finite fields and related computational issues », *in*: Computational perspectives on number theory: Proceedings of a Conference in Honor of A.O.L. Atkin (D.A. Buell and J.T. Teitelbaum, eds.), AMS/International Press, 1998, pp. 21–76.

[FM02] Mireille Fouquet and François Morain, « Isogeny volcanoes and the SEA algorithm », *in*: *Algorithmic number theory (Sydney, 2002)*, vol. 2369, Lecture Notes in Comput. Sci. Springer, Berlin, 2002, pp. 276–291, DOI: 10.1007/3-540-45455-1_23, URL: https://doi.org/10.1007/3-540-45455-1_23.

[FT19] E. V. Flynn and Yan Bo Ti, « Genus Two Isogeny Cryptography », *in*: *Post-Quantum Cryptography*, ed. by Jintai Ding and Rainer Steinwandt, Cham: Springer International Publishing, 2019, pp. 286–306, ISBN: 978-3-030-25510-7.

[Gal12] Steven D. Galbraith, *Mathematics of public key cryptography*, Cambridge University Press, Cambridge, 2012, pp. xiv+615, ISBN: 978-1-107-01392-6, DOI: 10.1017/CBO9781139012843, URL: https://doi.org/10.1017/CBO9781139012843.

[GS12] Pierrick Gaudry and Éric Schost, « Genus 2 point counting over prime fields », *in*: *Journal of Symbolic Computation* 47.*4* (2012), pp. 368–400.

[Hen97] K.. Hensel, « Über eine neue Begründung der Theorie der algebraischen Zahlen. », *in*: *Jahresbericht der Deutschen Mathematiker-Vereinigung* 6 (1897), pp. 83–88, URL: http://eudml.org/doc/144593.

[JMV05] David Jao, Stephen D. Miller, and Ramarathnam Venkatesan, « Do All Elliptic Curves of the Same Order Have the Same Difficulty of Discrete Log? », *in*: *Proceedings of the 11th International Conference on Theory and Application of Cryptology and Information Security*, ASIACRYPT'05, Chennai, India: Springer-Verlag, 2005, 21–40, ISBN: 3540306846, DOI: 10.1007/11593447_2, URL: https://doi.org/10.1007/11593447_2.

[Ked01] Kiran S. Kedlaya, « Counting Points on Hyperelliptic Curves using Monsky-Washnitzer Cohomology », *in*: *arXiv Mathematics e-prints*, math/0105031 (May 2001), math/0105031, arXiv: math/0105031 [math.AG].

[Kob87] N. Koblitz, « Elliptic curve cryptosystems », *in*: *Mathematics of Computation* 48 (1987), pp. 203–209.

[Kob89] Neal Koblitz, « Hyperelliptic cryptosystems », *in*: *Journal of Cryptology* 1.*3* (1989), pp. 139–150, DOI: 10.1007/BF02252872, URL: https://doi.org/10.1007/BF02252872.

[Koh96] David Kohel, « Endomorphism rings of elliptic curves over finite fields », PhD thesis, University of California, Berkeley, 1996.

[KPR20] Jean Kieffer, Aurel Page, and Damien Robert, « Computing isogenies from modular equations between Jacobians of genus 2 curves », working paper or preprint, Jan. 2020, URL: https://hal.archives-ouvertes.fr/hal-02436133.

[Kro82] L. Kronecker, « Grundzüge einer arithmetischen Theorie der algebraische Grössen », *in*: *J. Reine Angew. Math.* 92 (1882), pp. 1–122, ISSN: 0075-4102, DOI: 10.1515/crll.1882.92.1, URL: https://doi.org/10.1515/crll.1882.92.1.

[KU11] Kiran S. Kedlaya and Christopher Umans, « Fast polynomial factorization and modular composition », *in*: *SIAM J. Comput.* 40.*6* (2011), pp. 1767–1802, ISSN: 0097-5397, DOI: 10.1137/08073408X, URL: https://doi.org/10.1137/08073408X.

[KY89] Erich Kaltofen and Lakshman Yagati, « Improved sparse multivariate polynomial interpolation algorithms », *in*: *Symbolic and algebraic computation (Rome, 1988)*, vol. 358, Lecture Notes in Comput. Sci. Springer, Berlin, 1989, pp. 467–474, DOI: 10.1007/3-540-51084-2_44, URL: https://doi.org/10.1007/3-540-51084-2_44.

[Lan73] Serge Lang, *Elliptic functions*, With an appendix by J. Tate, Addison-Wesley Publishing Co., 1973, pp. xii+326.

[Lau04] Alan G. B. Lauder, « Deformation theory and the computation of zeta functions », *in*: *Proceedings of the London Mathematical Society* 88.*3* (2004), 565–602, DOI: 10.1112/S0024611503014461.

[LB04] Herbert Lange and Christina Birkenhake, eng, Grundlehren der mathematischen Wissenschaften, Springer-Verlag Berlin Heidelberg, 2004.

[Len96] H. W. Lenstra Jr., « Complex multiplication structure of elliptic curves », *in*: *J. Number Theory* 56.*2* (1996), pp. 227–241, ISSN: 0022-314X, DOI: 10.1006/jnth.1996.0015, URL: https://doi.org/10.1006/jnth.1996.0015.

[Ler96] R. Lercier, « Computing isogenies in GF(2^n) », *in*: *Algorithmic Number Theory: Second International Symposium, ANTS-II Talence, France, May 18–23, 1996 Proceedings*, ed. by H. Cohen, vol. 1122, Lecture Notes in Computer Science, Springer Berlin / Heidelberg, May 1996, pp. 197–212.

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

[LL06] Reynald Lercier and David Lubicz, « A quasi quadratic time algorithm for hyperelliptic curve point counting », *in*: *The Ramanujan Journal* 12.*3* (2006), pp. 399–423.

[LLL82] A. K. Lenstra, H. W. Lenstra, and L. Lovász, « Factoring polynomials with rational coefficients », *in*: *Mathematische Annalen* 261.*4* (1982), pp. 515–534, DOI: 10.1007/BF01457454, URL: https://doi.org/10.1007/BF01457454.

[LM00] R. Lercier and F. Morain, « Computing isogenies between elliptic curves over GF(p^n) using Couveignes's algorithm », *in*: *Mathematics of Computation* 69.*229* (Jan. 2000), pp. 351–370.

[LM98] R. Lercier and F. Morain, « Algorithms for computing isogenies between elliptic curves », *in*: *Computational Perspectives on Number Theory: Proceedings of a Conference in Honor of A. O. L. Atkin*, ed. by D.A. Buell and J.T. Teitelbaum, vol. 7, AMS/IP Studies in Advanced Mathematics, Held in 1995 at the University of Illinois at Chicago, Providence: American Mathematical Society & Internationnal Press, 1998, pp. 77–96.

[LR12] David Lubicz and Damien Robert, « Computing isogenies between abelian varieties », *in*: *Compositio Mathematica* 148.*5* (2012), pp. 1483–1515.

[LS08] Reynald Lercier and Thomas Sirvent, « On Elkies subgroups of l-torsion points in elliptic curves defined over a finite field », *in*: *J. Théor. Nombres Bordeaux* 20.*3* (2008), pp. 783–797, ISSN: 1246-7405, URL: http://jtnb.cedram.org/item?id=JTNB_2008__20_3_783_0.

[LV16] Pierre Lairez and Tristan Vaccon, « On p-adic differential equations with separation of variables », *in*: *Proceedings of the 2016 ACM International Symposium on Symbolic and Algebraic Computation*, ACM, New York, 2016, pp. 319–323.

[Mat59] Teruhisa Matsusaka, « On a characterization of a Jacobian variety », *in*: *Memoirs of the College of Science, University of Kyoto. Series A: Mathematics* 32.*1* (1959), pp. 1–19.

[Mil19] Enea Milio, « Computing isogenies between Jacobian of curves of genus 2 and 3 », working paper or preprint, Aug. 2019, URL: https://hal.archives-ouvertes.fr/hal-01589683.

[Mil86a] Victor S. Miller, « Use of Elliptic Curves in Cryptography », *in*: *Advances in Cryptology — CRYPTO '85 Proceedings*, ed. by Hugh C. Williams, Berlin, Heidelberg: Springer Berlin Heidelberg, 1986, pp. 417–426, ISBN: 978-3-540-39799-1.

[Mil86b] James S Milne, « Abelian varieties », *in*: *Arithmetic geometry*, Springer, 1986, pp. 103–150.

[Mor95] François Morain, « Calcul du nombre de points sur une courbe elliptique dans un corps fini: aspects algorithmiques », *in*: *Journal de Théorie des Nombres de Bordeaux* 7.*1* (1995), pp. 255–282, ISSN: 12467405, 21188572, URL: http://www.jstor.org/stable/43972443.

[Nar18] Anand Kumar Narayanan, « Fast Computation of Isomorphisms Between Finite Fields Using Elliptic Curves », *in*: *Arithmetic of Finite Fields. WAIFI 2018.* Ed. by L. Budaghyan and F. Rodríguez-Henríquez, vol. 11321, Lecture Notes in Computer Science, Springer, Cham, 2018.

[OS86] Frans OORT and Tsutomu SEKIGUCHI, « The canonical lifting of an ordinary Jacobian variety need not be a Jacobian variety », *in*: *J. Math. Soc. Japan* 38.*3* (July 1986), pp. 427–437, DOI: 10.2969/jmsj/03830427, URL: https://doi.org/10.2969/jmsj/03830427.

[Put86] Marius Van der Put, « The cohomology of Monsky and Washnitzer », mul, *in*: *Introductions aux cohomologies p-adiques*, ed. by Daniel Barsky and Philippe Robba, Mémoires de la Société Mathématique de France 23, So-

ciété mathématique de France, 1986, pp. 33–59, URL: http://www.numdam.org/item/MSMF_1986_2_23__33_0.

[Rec74] Sevin Recillas, « Jacobians of curves with g_4^1's are the Prym's of trigonal curves », English, *in*: *Bol. Soc. Mat. Mex., II. Ser.* 19 (1974), pp. 9–13, ISSN: 0037-8615.

[Rob75] P. Robba, « On the Index of p-adic Differential Operators I », *in*: *Annals of Mathematics* 101.*2* (1975), pp. 280–316, ISSN: 0003486X, URL: http://www.jstor.org/stable/1970992.

[Rob76] P. Robba, « On the index of p-adic differential operators. II », *in*: *Duke Mathematical Journal* 43.*1* (1976), pp. 19 –31, DOI: 10.1215/S0012-7094-76-04303-9, URL: https://doi.org/10.1215/S0012-7094-76-04303-9.

[Rob84] Philippe Robba, « Index of p-adic differential operators III. Application to twisted exponential sums », en, *in*: *Cohomologie p-adique*, Astérisque 119-120, Société mathématique de France, 1984, URL: www.numdam.org/item/AST_1984__119-120__191_0/.

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

[RSA78] R. L. Rivest, A. Shamir, and L. Adleman, « A Method for Obtaining Digital Signatures and Public-Key Cryptosystems », *in*: *Commun. ACM* 21.*2* (Feb. 1978), 120–126, ISSN: 0001-0782, DOI: 10.1145/359340.359342, URL: https://doi.org/10.1145/359340.359342.

[Sat00] Takakazu Satoh, « The canonical lift of an ordinary elliptic curve over a finite field and its point counting », *in*: *J. Ramanujan Math. Soc.* 15.*4* (2000), pp. 247–270, ISSN: 0970-1249.

[Sat02] Takakazu Satoh, « On p-adic Point Counting Algorithms for Elliptic Curves over Finite Fields », *in*: *Algorithmic Number Theory*, ed. by Claus Fieker and David R. Kohel, Berlin, Heidelberg: Springer Berlin Heidelberg, 2002, pp. 43–66, ISBN: 978-3-540-45455-7.

[Sch82] Arnold Schönhage, « Asymptotically fast algorithms for the numerical multiplication and division of polynomials with complex coefficients », *in*: *Computer algebra (Marseille, 1982)*, vol. 144, Lecture Notes in Comput. Sci. Springer, Berlin-New York, 1982, pp. 3–15.

[Sch85] René Schoof, « Elliptic curves over finite fields and the computation of square roots mod p », *in*: *Math. Comp.* 44.*170* (1985), pp. 483–494, ISSN: 0025-5718, DOI: 10.2307/2007968, URL: https://doi.org/10.2307/2007968.

[Sch95] René Schoof, « Counting points on elliptic curves over finite fields », en, *in*: *Journal de Théorie des Nombres de Bordeaux* 7.*1* (1995), pp. 219–254, URL: www.numdam.org/item/JTNB_1995__7_1_219_0/.

[Sil09] Joseph H. Silverman, *The arithmetic of elliptic curves*, Second, vol. 106, Graduate Texts in Mathematics, Springer, Dordrecht, 2009, pp. xx+513, ISBN: 978-0-387-09493-9, DOI: 10.1007/978-0-387-09494-6, URL: https://doi.org/10.1007/978-0-387-09494-6.

[Sil94] Joseph H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, vol. 151, Graduate Texts in Mathematics, Springer-Verlag, New York, 1994, pp. xiv+525, ISBN: 0-387-94328-5, DOI: 10.1007/978-1-4612-0851-8, URL: https://doi.org/10.1007/978-1-4612-0851-8.

[Smi09] Benjamin Smith, « Isogenies and the Discrete Logarithm Problem in Jacobians of Genus 3 Hyperelliptic Curves, » *in*: *Journal of Cryptology* 22.*4* (2009), pp. 505–529, DOI: 10.1007/s00145-009-9038-1, URL: https://doi.org/10.1007/s00145-009-9038-1.

[SST03] Takakazu Satoh, Berit Skjernaa, and Yuichiro Taguchi, « Fast computation of canonical lifts of elliptic curves and its application to point counting », *in*: *Finite Fields Appl.* 9.*1* (2003), pp. 89–101, ISSN: 1071-5797, DOI: 10.1016/S1071-5797(02)00013-8, URL: https://doi.org/10.1016/S1071-5797(02)00013-8.

[Tho03] Emmanuel Thomé, « Algorithmes de calcul de logarithmes discrets dans les corps finis », PhD thesis, École polytechnique, 2003.

[Tia20] Song Tian, *Translating the discrete logarithm problem on Jacobians of genus 3 hyperelliptic curves with* (ℓ, ℓ, ℓ)*-isogenies*, 2020, arXiv: 2007.03172 [math.AG].

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

[Vél71] Jacques Vélu, « Isogénies entre courbes elliptiques », *in*: *Comptes-Rendus de l'Académie des Sciences, Série I* 273 (1971), pp. 238–241.

DOCTORAT BRETAGNE LOIRE / MATHSTIC

UNIVERSITÉ DE RENNES 1

Titre : Sur le calcul d'isogénies par résolution d'équations différentielles p-adiques

Mot clés : Isogénies, variétés abéliennes, courbes elliptiques, courbes hyperelliptiques, équations differentielles p-Adiques, calcul formel.

Résumé : Nous proposons dans cette thèse des algorithmes effectifs de calcul d'isogénies entre courbes elliptiques et Jacobiennes de courbes hyperelliptiques via l'approche des équation différentielles p-adiques avec un bon contrôle de précision.
Plus précisément, nous nous intéressons dans un premier temps au calcul d'isogénies entre courbes elliptiques définies sur une extension de $\mathbb{Q}_2$. Ce travail vient ainsi compléter ceux réalisés pour le cas impair. Nous donnons quelques applications, en particulier le calcul d'isogénies entre courbes elliptiques sur des corps finis de caractéristique 2 et de polynômes irréductibles, tous deux en temps quasi-linéaire en le degré.
Dans un second temps, nous présentons un algorithme de calcul explicite de représentations rationnelles d'isogénies entre Jacobiennes de courbes hyperelliptiques sur une extension de $\mathbb{Q}_p$. Par conséquent, après avoir éventuellement relevé le problème dans les p-adiques, nous obtenons des algorithmes efficaces pour le calcul d'isogénies entre Jacobiennes de courbes hyperelliptiques définies sur des corps finis de caractéristique impaire. Une autre application importante que nous en déduisons est le calcul des polynômes de Cantor de ℓ-divisions.
L'efficacité de ces algorithmes repose sur une analyse fine des solutions d'équations différentielles p-adiques.

Title: On isogeny calculation by solving p-adic differential equations.

Keywords: Isogenies, abelian varieties, elliptic curves, hyperelliptic curves, p-Adic differential equations, symbolic computation.

Abstract: In this thesis, we propose efficient algorithms for computing isogenies between elliptic curves and Jacobians of hyperelliptic curves via p-adic differential equations with a sharp analysis of the loss of precision.
More precisely, on the one hand, we are interested in computing elliptic curve isogenies defined over an extension of $\mathbb{Q}_2$. This work complements the work carried out over extensions of $\mathbb{Q}_p$ for p odd. We give some applications, in particular computing over finite fields of characteristic 2 isogenies of elliptic curves and irreducible polynomials, both in quasi-linear time in the degree.
On the other hand, we present an algorithm for the explicit computation of rational representations between Jacobians of hyperelliptic curves defined over an extension of $\mathbb{Q}_p$. Consequently, after having possibly lifted the problem to the p-adics, we obtain efficient algorithms for computing isogenies between Jacobians of hyperelliptic curves defined over finite fields of odd characteristic. Another important application is the computation of Cantor's ℓ-division polynomials.
The efficiency of these algorithms is based on an analysis of the solutions of p-adic differential equations.