Volcans et calcul d'isogénies

Cyril Hugounenq

université PARIS-SACLAY

UNIVERSITÉ DE VERSAILLES ST-QUENTIN-EN-YVELINES
université PARIS-SACLAY

NNT : 2017SACLV050

Volcans et calcul d'isogénies

Thèse de doctorat de l'Université Paris-Saclay
préparée à l'Université de Versailles-Saint-Quentin-en-Yvelines

École doctorale n°580 Sciences et Technologies de l'Information et de la communication (STIC)
Spécialité de doctorat: Informatique

Thèse présentée et soutenue à Versailles, le 25 septembre 2017, par

Cyril Hugounenq

Composition du Jury :

Frédéric Chyzak Chargé de recherches, Inria-Saclay	Examinateur
Luca De Feo Maître de conférences, Université de Versailles	Co-encadrant
Mireille Fouquet Maître de conférences, Université Paris VII	Examinatrice
Louis Goubin Professeur, Université de Versailles	Directeur de thèse
David Kohel Professeur, Université Aix-Marseille	Rapporteur
Ariane Mézard Professeur, Université Paris VI	Présidente du jury
Josep M. Miret Professeur associé, Université de Lleida	Rapporteur
François Morain Professeur, École Polytechnique	Co-Directeur de thèse

Thèse de doctorat

Remerciements

Après tout ce temps il me faut écrire ces quelques pages pour conclure la rédaction de cette thèse. Certains pourraient penser que c'est la partie la plus évidente mais celle-ci étant la plus scrutée, elle n'en sera que plus critiquée ou adorée...

Je voudrais tout d'abord remercier Luca (je m'excuse de n'avoir jamais fait l'effort de prononcer son prénom avec l'accent italien) pour m'avoir proposé ce projet. Je remercie également François Morain et Louis Goubin pour avoir accepté de faire également partie de ce projet Digiteo qui a financé mes 3 premières années de thèse, je tiens également à remercier les (anonymes) décisionnaires de cette bourse. Ensuite il y a eu une quatrième année qui a été financée par le département d'informatiques de Versailles que je remercie vivement pour le choix de me financer au détriment d'autres (bonnes) candidatures. J'espère sincèrement avoir fourni un travail à la hauteur des investissements faits dans ce projet.

Avant de parler du déroulement de cette thèse permettez-moi de faire un retour dans le passé et de parler de ceux qui sont aussi à l'origine de celle-ci.

De mon passage au Lycée Joffre je garderai surtout cette maxime, que je n'ai cessé d'essayer de suivre, formulée par M. Bondil :«On regarde sous le capot et on comprend comment cela fonctionne», sans oublier cette volonté de M. Carré du meilleur pour moi.

De mon passage à l'ENSMM à Besançon, je ne retiendrai que des bon moments accompagné d'excellents camarades Florent M. (dont je m'excuse de ne pas avoir tenu ma promesse), Émile, Benjamin, les deux Guillaume, Vincent ; ceux-ci rendirent difficile cette ré-orientation nécessaire car les mathématiques me manquaient trop. Je remercie d'ailleurs mes parents pour avoir compris ce choix et m'avoir soutenu (y compris financièrement) dans mes études.

Mon choix de reprendre les études en mathématiques à Grenoble fût conforté par l'excellent cours de M. Berhuy (dont je continue encore le grand combat aujourd'hui). L'un des autres apports de Grenoble fût ce magistère qui peut signifier insignifiant pour certains et coûteux mais celui-ci a permis de me plonger dans une excellente ambiance de travail et convivialité grâce à son responsable Greg McShane et Loïc Gaillard. Ainsi j'ai eu d'excellents camarades au cours de mes études je pense tout particulièrement à (l'autre) Loïc, Clément, Moran, Laure, Frédérique, Vincent, Valentin, Kamil. Sans oublier le pire des joueurs de StarCraft II que je connaisse (;-) Jean-Charles.

Enfin nous arrivons à la thèse. D'un point de vue plus personnel, je tiens encore une fois à remercier Luca, il était plus que prêt pour encadrer un tel projet. Je le remercie pour la liberté qu'il m'a offerte tout au long de ma thèse, pour l'extrême gentillesse et bienveillance dont je le soupçonne à mon égard.

Si je n'étais pas épuisé par cette thèse je recommencerai sans hésiter une autre thèse avec lui. Je tiens à remercier également François Morain pour son franc parler, ses remarques (notamment le 7.1 c'est grâce à lui) et sa gentillesse. Je remercie également Louis Goubin avec qui j'aurai pris plaisir à travailler au cours de notre collaboration qui n'a pas encore mûri, «last but not least» Louis m'aura aidé au cours de nos (trop) nombreux problèmes administratifs (j'en tremble encore...).

Grâce à ma bourse Digiteo (et aux encouragements de Luca) j'ai pu voyager et rencontrer de nombreuses personnes. Il y a tout d'abord Éric Schost que je remercie pour son accueil au cours des 2 mois que j'ai passés à l'université de Waterloo (Ontario), sans oublier toute l'équipe de Symbolic Computation qui a été chaleureuse avec moi, plus particulièrement George Labahn qui s'est assuré que mon arrivée se passe bien. Je tiens également à remercier le FIELDS d'avoir financé une partie de mon séjour à Toronto, j'aurai aimé pouvoir les remercier dans un article mais aucune collaboration n'est née de ma présence au FIELDS institute. Je tiens également à remercier Jérôme Plût, son apport dans cette thèse est essentiel, cela m'aura toujours fasciné sa capacité d'abstraction mathématique. Puis il y a de nombreux (ex-)doctorants que j'ai rencontrés, je pense en particulier à Vincent Neiger (son aide inestimable à Waterloo et ses honnêtes mots), Simon Abelard, Laurent Grémy, Vlad Dragoi, Enea Milio, Marie Paindavoine, Jean-Marc Robert, Alexandre Gélin.

Il y a bien évidemment les 2 équipes que j'ai côtoyées au cours de cette thèse. Tout d'abord l'équipe GRACE au LiX dont la gentillesse et la sympathie sont à la hauteur de leurs talents scientifiques. Ensuite l'équipe Crypto de Versailles, je pense tout d'abord à Michaël qui m'aura toujours traité comme son égal avec toutes ses questions, Jacques Patarin pour ses anecdotes (historiques), Christina (tout particulièrement pour ne pas m'avoir donné de copies à corriger durant ma quatrième année) ainsi que Nicolas, Johan et Valentin. Il ne faut pas oublier les doctorants de l'équipe pour qui j'ai une pensée amicale et qui en ont eu à mon égard : Antoine, Bastien, Rodolphe, Benoît, Ilaria (ma fausse Sicilienne Sarde préférée), Cécile (qui n'est pas restée), Ninon (qui heureusement pour ma thèse n'est pas trop venue au bureau parler de BD), mon ami (tête en l'air) Francisco, enfin Axel qui m'aura supporté durant cette quatrième année, j'espère y avoir autant apporté que lui il a fait pour moi. Je tiens également à remercier mes amis de l'(ex-)association ADUVSQ : Bastien, Yoann, Jean-Pierre et William pour s'être engagé dans cette aventure. Il ne faut pas oublier Khaled qui est un très grand ami pour moi malgré son amour pour le F.C. Metz, j'espère que l'on aura été héroïques dans le bon sens du terme (selon Cartier).

De manière plus générale je tiens à remercier l'ensemble du département d'informatiques pour leur gentillesse à mon égard et la bonne ambiance de travail qu'ils perpétuent. Je n'aurai jamais compris cette séparation du laboratoire... Je tiens à remercier tout particulièrement Sandrine Vial, Franck Quessette, Didier Riou, Stéphane Lopez, Michaël Quisquater, Louis Goubin et Christina Boura pour m'avoir fait confiance pour donner des TD/TP.

Enfin il me faut remercier mes amis et ma famille. Tout d'abord toute la famille Henry pour m'avoir accueilli lorsque je suis arrivé en région parisienne, ensuite toute ma famille qui je l'espère aura compris certaines de mes absences. Sans oublier mes amis : Arthur(toujours partant), Anthony(l'éternel), Vincent(toujours là), Quentin (le raisonnable fou), Florent(le seul et unique dieu de la spé), Florian(le collectionneur) qui auront répondu présent les rares

fois où j'étais là et qui ont eux aussi fait preuve d'une grande compréhension pour mes absences. Je tiens également à remercier Cristian, Aura et N'Dugu qui m'ont accueilli dans leur maison à Waterloo et qui m'ont offert bien plus qu'un toit.

Je vais donc paraphraser H. H. que j'ai eu le plaisir de rencontrer à Paris pour la (presque) fin de ces remerciements :«Parents proches et amis remerciés... qui reste-t-il ? Les absents sans doute. Vous avez toujours tort, vous ne rendez pas beaucoup service... Mais vous me manquez. Des fois...»

Enfin il y a Jennifer pour qui cette thèse n'a peut être pas beaucoup de sens mais sans elle pour moi cette thèse n'en aurait pas.

Table des matières

Nomenclature **13**

Introduction **15**

1 Rappels théoriques **19**
1.1 Complexité 19
1.2 Théorie de Galois 20
1.3 Courbes Elliptiques 20
1.3.1 Équations de Weierstrass 21
1.3.2 Loi de groupe 22
1.3.3 Isogénies 23
1.3.4 Endomorphismes 27
1.4 Courbes elliptiques définies sur un corps fini 27
1.4.1 L'endomorphisme de Frobenius 28
1.4.2 Algorithme de Schoof et ses améliorations 29

2 Calcul d'isogénies sur les corps finis **33**
2.1 Rappel et applications des formules de Vélu 33
2.2 L'algorithme de Elkies 1998 34
2.3 L'algorithme de Bostan-Morain-Salvy-Schost 36
2.4 L'algorithme de Lercier Sirvent 39
2.5 L'algorithme de Couveignes 1996 et ses améliorations 40
2.5.1 Algorithme original de Couveignes 41
2.5.2 Apports de l'utilisation de l'action du Frobenius sur des tours p-adiques à l'algorithme de Couveignes 46

3 Construction efficaces de tours ℓ-adiques **51**
3.1 Construction d'une tour d'extensions ℓ-adiques 52
3.2 Représentation des éléments de la tour d'extensions ℓ-adiques . . 53
3.3 Opérations dans la tour d'extension ℓ-adique 54
3.4 Calcul de polynômes d'interpolations 58

4 Volcans d'isogénies **63**
4.1 Anneau des endomorphismes 63
4.1.1 Rappel sur les ordres d'un corps de nombres quadratique 63
4.1.2 Anneau des endomorphismes de courbes elliptiques ordinaires 65
4.2 Lien entre les niveaux d'une courbe dans le volcan et la structure de la ℓ^∞ torsion rationnelle 70

5 Détermination de directions dans le volcan des ℓ-isogénies à l'aide de l'action du Frobenius **73**
5.1 Cas Elkies . . . 73
5.1.1 Étude de l'action du Frobenius sur le module de Tate . . 74
5.1.2 Calcul des directions dans le volcan de ℓ-isogénies 81
5.2 Cas Atkin . . . 89
5.2.1 Étude de l'action du Frobenius sur le module de Tate . . 90
5.2.2 Calculs de directions dans le volcan de ℓ-isogénies. 94

6 Algorithme de Couveignes ℓ-adique **97**
6.1 Cas Elkies . . . 98
6.1.1 Présentation du cas spécifique où l'on connaît un premier ℓ de Elkies . . . 99
6.1.2 Analyse générale . . . 102
6.1.3 Partie expérimentale . . . 105
6.2 Cas Atkin . . . 106
6.3 Conclusion . . . 111

7 Variantes de l'algorithme de Couveignes ℓ-adique dans le cas Elkies **113**
7.1 Algorithme de Couveignes ℓ-adique dans le cas Elkies avec un point horizontal . . . 113
7.2 Algorithme de Couveignes ℓ-adique avec différents nombres de Elkies . . . 115
7.3 Algorithme de Couveignes ℓ-adique généralisé avec un nombre composé de Elkies . . . 117
7.3.1 Théorème des Restes Chinois et son application à l'algorithme de Couveignes ℓ-adique . . . 118
7.3.2 Construction de composita d'extensions ℓ_i-adiques 119
7.3.3 Estimation du coût de l'algorithme de Couveignes ℓ_i-adique avec un nombre composé de Elkies . . . 121

Conclusion **125**

A Algorithmes **133**
*

Liste des algorithmes

1 Résolution d'équation différentielle 38
2 BMSS 38
3 Algorithme de Lercier-Sirvent 39
4 Algorithme original de Couveignes 42
5 Calcul d'une base diagonale de $E_s[\ell^{h+1}]$ à partir d'une base triangulaire de $E[\ell^{h-e+1}]$ pour E au niveau $h-e$ 85
6 Calcul d'une base diagonale de $E_s[\ell^k]$ 86
7 Calcul d'une base diagonale de $E_s[\ell^k]$ à partir de E au niveau $h-e$ 87
8 Calcul d'un point horizontal d'ordre ℓ^k 89
9 Calcul d'un point R d'ordre ℓ^{h-e+i} tel que $\pi(P,R)=M$ 95
10 Algorithme de Couveignes ℓ-adique dans le cas Elkies. 101
11 Algorithme de Couveignes ℓ-adique dans le cas Atkin. 109
12 Algorithme de Couveignes ℓ-adique avec différents nombres de Elkies 116
13 Algorithme de Couveignes avec nombre composé de Elkies. . . . 122
14 Couveignes ℓ-adique dans le cas Elkies avec un seul sous-groupe cyclique. 133
15 Calcul de $P \in E[\upsilon_n]$ tel que $[\upsilon_{i_0}]P = P_{i_0}$ et $[\ell_{i_0}^{k_{i_0}}]P = 0_E$ 134
16 Théorème des restes chinois sur une courbe elliptique 134

Table des figures

1 Exemple de graphe (*volcan*) d'isogénies 16

2.1 Classification des points de p^k-torsion selon l'action du Frobenius. 45
2.2 Arbre de sous produits pour le calcul de $T_0^{(0)}$ dans le cas d'une tour d'extension quadratique. 48

3.1 Coûts des opérations dans F_k exprimées en nombre d'opérations sur $\mathbb{F}_q$ 58

4.1 Représentation d'un volcan de 2-isogénies avec les différents ordres. 66
4.2 Différents types de volcans des 2-isogénies. 68
4.3 Exemples de structures de la 2^∞-torsion rationnelle par rapport au niveau des courbes dans le volcan. 71

5.1 Différentes formes de matrices du Frobenius à conjugaison près selon le niveau dans le volcan des isogénies. 75
5.2 Exemples de différents points diagonaux $P \in E_s$ d'ordre 2^3 tels que $\pi(P) = [\mu]P$. 77
5.3 Exemple de construction de point horizontal d'ordre 2^2. 78
5.4 Construction d'un point ascendant horizontal. 79
5.5 Exemples de matrices du Frobenius obtenues sur les différents niveaux d'un volcan de ℓ-isogénies 91
5.6 Exemples des isogénies correspondant aux différentes matrices du Frobenius, calculées sur la courbe E au sommet du volcan des ℓ-isogénies. 93

6.1 Exemple de candidats pour la mise en correspondances de points diagonaux par la r-isogénie ϕ 99
6.2 Comparaison entre la phase d'initialisation et la phase d'interpolation pour une courbe définie sur $\mathbb{F}_{101}$ pour r croissant. La courbe est en échelle logarithmique. 106
6.3 Comparaison d'une phase d'interpolation pour r croissant pour différentes courbes définies sur les corps finis $\mathbb{F}_{101}$, $\mathbb{F}_{2^{18}+93}$, $\mathbb{F}_{2^{30}+669}$, $\mathbb{F}_{2^{62}+189}$ et $\mathbb{F}_{2^{252}+421}$. La courbe est en échelle logarithmique. . . 107
6.4 Phase d'interpolation pour r croissant pour différentes courbes définies sur les corps finis $\mathbb{F}_{521}$ et $\mathbb{F}_{1033}$. La courbe est en échelle logarithmique. 107

Nomenclature

La liste suivante décrit certains symboles qui seront utilisés tout au long de ce document.

$[n]P$ Multiplication scalaire par n d'un point P d'une courbe elliptique

$\left(\frac{\ell}{d_K}\right)$ Symbole de Kronecker

$\mathbb{F}_q$ Corps fini à q éléments

$\mathbb{K}_j$ Le compositum isomorphe à $\otimes_{i=1}^{j} \mathsf{F}_{(i,k_i)}$

$\mathbb{Z}_\ell$ L'ensemble des entiers ℓ-adiques

$\mathcal{O}$ L'ordre associé à isomorphisme près à l'anneau des endomorphisme de la courbe elliptique E

$\mathsf{End}(E)$ L'anneau des endomorphismes de la courbe elliptique E

F_j j-ième corps de la tour d'extensions ℓ-adiques

$\mathsf{F}_{(i,j)}$ j-ième corps de la tour d'extensions ℓ_i-adiques

$\mathsf{Gal}(\mathbb{L} : \mathbb{K})$ Le groupe d'automorphismes de $\mathbb{L}$ qui laisse fixe $\mathbb{K}$ avec $\mathbb{L}/\mathbb{K}$ une extension Galoisienne.

$\mathsf{T}_\ell(E)$ Le module de Tate ℓ-adique de la courbe elliptique E

$\phi^{-1}(S)$ Ensemble des pré-images de S par l'application ϕ

Φ_ℓ ℓ-ième polynôme modulaire

π L'endomorphisme de Frobenius

$\pi(P, Q)$ Représente l'action du Frobenius π dans une base P, Q sous forme matricielle.

υ_n L'entier $\prod_{i=1}^{n} \ell_i^{k_i}$

ϑ_{i_0} L'entier $\frac{\upsilon_n}{\ell_{i_0}^{k_{i_0}}}$

$\widehat{\psi}$ Isogénie duale de ψ

d_1 Le degré de l'extension F_1 par rapport à $\mathbb{F}_q$

$d_{(i,1)}$ Le degré de l'extension $F_{(i,1)}$ par rapport à $\mathbb{F}_q$

d_π Discriminant du Frobenius

$E[n]$ Ensemble des points de n-torsion d'une courbe elliptique

f_{E_1}	Application f de E_1 dans E_1
$j(E)$	j-invariant de la courbe elliptique E
$P \odot Q$	Le produit composé de P et Q
p_j	Le degré de l'extension $\mathbb{K}_j$ par rapport à $\mathbb{F}_q$
t_π	Trace du Frobenius
$v_\ell(n)$	La valuation ℓ-adique de n

Introduction

Les courbes (hyper)elliptiques sont beaucoup étudiées et utilisées, notamment en cryptographie [Mil85, Kob87, Kob89]. Dans les domaines applicatifs, on s'intéresse tout particulièrement aux courbes elliptiques sur les corps finis. Les algorithmes de calculs de cardinalité de courbes elliptiques sont donc fondamentaux, afin par exemple de définir les paramètres des cryptosystèmes. L'algorithme de Schoof [Sch85] est le premier algorithme de complexité polynomiale à calculer la cardinalité de courbes elliptiques sur les corps finis. Il a été amélioré par la suite par les travaux de Atkin [Atk88] et Elkies [Elk91] aboutissant à l'algorithme SEA [Sch95].

Les isogénies sont des morphismes de groupes de noyau fini entre deux courbes elliptiques. Le calcul d'isogénies apparaît dans SEA et a donc un intérêt central. Les courbes elliptiques sont représentées, entre autres, à l'aide de leur j-invariant qui les définit à isomorphisme près. Nous formulons donc le problème suivant de calcul d'isogénies :

Problème du calcul explicite d'isogénie Etant donnés deux courbes elliptiques E_0 et E_1, un entier r tel que E_0 et E_1 soient r-isogènes, c'est à dire qu'il existe une isogénie de degré r qui relie ces deux courbes, calculer l'isogénie $\phi : E_0 \to E_1$.

Les premiers algorithmes de calcul d'isogénies sont dus à Atkin [Atk91] et Charlap, Coley et Robbins [CCR91]. Ensuite des algorithmes utilisables sur les corps finis ont été développés [Elk98], [Cou94], [Cou96], [Ler96]. Les trois algorithmes sus-cités de Couveignes [Cou94], [Cou96] et Lercier [Ler96] ne sont pratiques que dans le cas de petite caractéristique. L'algorithme de Elkies [Elk98], au contraire, est mieux adapté à la caractéristique grande ou zéro, et ne peut pas être utilisé en petite caractéristique. Ce dernier a été ensuite amélioré par le travail de Bostan, Morain, Salvy et Schost [BMSS08], puis par celui de Lercier et Sirvent [LS08] qui a permis d'utiliser cette méthode sans contrainte de caractéristique ; ce dernier algorithme a été récemment amélioré par un résultat de Lairez et Vaccon [LV16] sur la précision p-adique.

Bien que l'algorithme de Couveignes [Cou96] ait une meilleure complexité en le degré de l'isogénie que l'algorithme de Lercier et Sirvent, il n'est pas utilisé en pratique à cause d'une dépendance polynomiale en la caractéristique p qui le rend trop coûteux dès que p augmente. Ainsi, l'algorithme de Lercier et Sirvent, avec une dépendance logarithmique en p, est préféré pour les plus grandes caractéristiques.

Soulignons que le calcul d'isogénies n'est pas une étape dominante du point de vue de la complexité dans l'algorithme SEA.

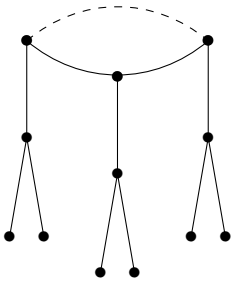


FIGURE 1 – Exemple de graphe (*volcan*) d'isogénies

Le problème du calcul de l'isogénie explicite a trouvé récemment de nouvelles applications, par exemple pour les crypto-systèmes à trappe de Teske [Tes06], les travaux de cryptanalyse de [MMT01], la construction de fonctions de hachage [CGL09], l'accélération de la multiplication scalaire [GLV01, LS14], ou les crypto-systèmes post-quantiques à base de graphes d'isogénies [Cou06] [RS06] [DFJP14].

Dans ces récentes applications le calcul d'isogénies peut être dominant. Ainsi, il est pertinent d'approfondir le travail de Couveignes [Cou96] sur le calcul d'isogénies à cause de sa bonne complexité en le degré de l'isogénie. L'algorithme de Couveignes interpole l'évaluation de l'isogénie sur les points d'ordre p^k, pour k assez grand, où p est la caractéristique du corps de base. Ce travail a été amélioré par la suite par De Feo [DF11], qui se sert notamment d'une construction efficace de tours d'extensions de degré p de corps finis [Cou00, DFS12].

Cette thèse s'inscrit dans la continuité des travaux de Couveignes [Cou96] et De Feo [DF11], et cherche notamment à les généraliser à l'étude des points d'ordre ℓ^k, avec ℓ premier quelconque, afin de s'affranchir de la dépendance polynomiale en p. Pour cela, nous devons en particulier déterminer des ensembles de points préservés par l'évaluation de l'isogénie que nous voulons calculer, tout en nous servant d'une construction efficace de tours d'extensions de degré ℓ de corps finis.

Pour une étude fine de l'évaluation de l'isogénie sur les points d'ordre ℓ^k, nous nous servons de *graphes d'isogénies*. Sur la Figure 1 nous pouvons en voir un exemple. Les sommets de ce graphe sont des courbes elliptiques définies à isomorphisme près ; elles sont reliées par des arêtes symbolisant les isogénies d'un degré fixé. Il est à noter que toutes les courbes d'un même graphe d'isogénies ont la même cardinalité.

Les graphes d'isogénies ont été étudiés pour la première fois par Kohel [Koh96] ; ses travaux ont été inspirés par ceux de [Mes86, Piz90, Piz95] dans le contexte particulier des courbes elliptiques supersingulières que Kohel a adapté et développé dans ce contexte ; Kohel a aussi étudié le cas des courbes elliptiques ordinaires. Cela afin de calculer l'anneau des endomorphismes d'une courbe elliptique. Kohel a défini une nomenclature sur les niveaux dans le graphe d'isogénies. Ainsi le graphe de la Figure 1 a été représenté selon cette convention ; les isogénies allant entre deux courbes situées au même niveau sont appelées horizontales ; celles allant vers une courbe située plus bas (haut) sont appelées descendantes (ascendantes). Kohel détermine le niveau d'une courbe dans le

graphe tout en connaissant la cardinalité de celle-ci afin de calculer son anneau des endomorphismes. Fouquet et Morain [FM02] ont par la suite résolu le même problème, en adaptant les méthodes de Kohel sans la connaissance préalable de la cardinalité de la courbe, afin d'améliorer SEA, et ont nommé les graphes d'isogénies *volcans d'isogénies*.

Ensuite les travaux de Miret *et al.* [MMRV05] [MMS$^+$06] [MMS$^+$08] ont permis d'expliciter un lien entre le niveau d'une courbe dans le volcan de ℓ-isogénies et la structure des ℓ-sous-groupes de Sylow ; cette relation peut être aussi vue comme une conséquence des travaux de Kohel [Koh96] et Lenstra [Len96]. Le travail de Ionica et Joux [IJ10] a permis, à l'aide de couplages, de déterminer un changement de niveau dans le volcan d'isogénies sous certaines conditions.

Ces travaux ont donc été faits dans le but de déterminer la direction d'une isogénie : montante, descendante ou horizontale pour améliorer celui de Fouquet et Morain, et donc SEA.

Concernant la construction de tours d'extensions, nos travaux se placent dans la suite de ceux de Doliskani et Schost [DS15], De Feo, Doliskani et Schost [DFDS13], et en donnent quelques généralisations utiles.

Ainsi, l'un des résultats principaux de cette thèse est le théorème suivant :

Théorème. Pour presque tous les nombres premiers q et presque toutes les courbes elliptiques ordinaires E, E' définies sur $\mathbb{F}_q$, il est possible de résoudre le problème du «Calcul explicite de l'isogénie» en un temps quasi-quadratique en le degré de l'isogénie, avec une dépendance logarithmique en la caractéristique de $\mathbb{F}_q$.

L'énoncé détaillé est le théorème 6.9 démontré dans la sous-section 6.1.2.

Pour arriver à ce résultat nous avons développé de nouvelles méthodes pour définir et déterminer des directions dans les volcans de ℓ-isogénies.

Organisation de la thèse

Nous présentons dans le premier chapitre des notions de bases, notamment sur les courbes elliptiques et leurs endomorphismes, et tout particulièrement l'endomorphisme de Frobenius.

Dans le deuxième chapitre nous abordons les différents algorithmes de calcul d'isogénies sur des corps finis, dont ceux de Elkies [Elk98], Bostan *et al.* [BMSS08], Lercier et Sirvent [LS08], avant de présenter l'algorithme de Couveignes [Cou96] et ses améliorations par De Feo [DF11].

Dans le chapitre 3, nous nous plaçons dans la continuité des travaux de Doliskani et Schost [DS15], De Feo, Doliskani et Schost [DFDS13], et nous présentons les tours d'extensions ℓ-adiques. Nous généralisons notamment un résultat de De Feo [DF11] pour le calcul de polynômes d'interpolation.

Dans le chapitre 4 nous rappelons les résultats principaux sur les volcans d'isogénies, dont notamment le lien entre les niveaux dans le volcan et la structure des ℓ-sous-groupes de Sylow ; pour cela nous utilisons des résultats de Kohel [Koh96], Fouquet et Morain [FM02], Miret *et al.* [MMRV05] [MMS$^+$06] [MMS$^+$08], et Ionica et Joux [IJ10].

Nous abordons dans les deux chapitres suivants les principaux apports de la thèse.

Tout d'abord nous étudions dans le chapitre 5 l'action de l'endomorphisme de Frobenius sur la ℓ^k-torsion d'une courbe elliptique. Nous développons de nouvelles méthodes pour déterminer des directions dans le volcan de ℓ-isogénies, y compris pour les directions descendantes dans le cas Atkin. Nous présentons aussi dans ce chapitre des algorithmes permettant de calculer certaines isogénies, spécifiées par leurs directions, dans le volcan.

Ensuite, nous présentons dans le chapitre 6 comment ces isogénies peuvent être utilisées dans un algorithme de Couveignes où l'isogénie est interpolée sur les points d'ordre ℓ^k. Nous appellerons «*ℓ-adiques*» ces variantes de l'algorithme de Couveignes. Nous présentons et analysons deux algorithmes ℓ-adiques qui ensemble permettent de proposer une solution au problème de l'isogénie explicite pour presque tout ℓ premier différent de p. Après une étude de l'application du premier algorithme présenté à l'aide d'un résultat de Shparlinski et Sutherland [SS14], nous pouvons à l'aide du second algorithme donner directement une borne sur le paramètre ℓ pour résoudre le problème étudié.

Enfin nous présentons dans le chapitre 7 trois variantes de notre premier algorithme du chapitre 6 avec une variante qui utilise un seul sous-groupe cyclique des points d'ordre ℓ^k, une variante qui utilise différents nombres premiers favorables, une variante qui travaille avec un nombre composé favorable, et nous étudions leur intérêt.

Chapitre 1

Rappels théoriques

1.1 Complexité

Dans ce document, nous utilisons la notation classique de Landau O pour mesurer la complexité des algorithmes présentés. Étant données deux fonctions $f, g : \mathbb{N} \to \mathbb{N}$, on dit que $f \in O(g)$ lorsqu'il existe deux constantes x_0 et M telles que :

$$f(x) < Mg(x) \quad \text{pour} \quad x > x_0.$$

Nous définissons également la notation $f \in \Omega(g)$ de la façon suivante à l'aide de deux constantes x_0 et M telles que :

$$f(x) > Mg(x) \quad \text{pour} \quad x > x_0.$$

Nous définissons la notation Θ pour laquelle que $f \in \Theta(g)$ si et seulement si $f \in O(g)$ et $f \in \Omega(g)$.

Dans ce document, de nombreux algorithmes vont utiliser la multiplication rapide, nous notons alors $\mathsf{M} : \mathbb{N} \to \mathbb{N}$ la *fonction de multiplication* telle que le coût de la multiplication de deux polynômes de de degré n définis dans $\mathbb{F}_q[x]$ coûte $M(n)$ opérations arithmétiques dans $\mathbb{F}_q$. En utilisant les résultats de [vzGG03, §8.3] nous pouvons supposer que :

— $\mathsf{M}(n)$ est superlinéaire, c'est à dire $\frac{\mathsf{M}(n)}{n} \geqslant \frac{\mathsf{M}(m)}{m}$ si $n \geqslant m$,

— $\mathsf{M}(n)$ est au plus quadratique : $\mathsf{M}(mn) \leqslant m^2\mathsf{M}(n)$.

À l'aide des méthodes de [SS71] et de leurs généralisations [Sch77] [CK91] utilisant des transformées de Fourier rapides, la multiplication de polynômes de degré n appartenant à $R[x]$ pour un anneau R quelconque est de $O(n\log(n)\log\log(n))$ opérations arithmétiques dans R.

Dans ce document nous notons par ω un constante telle que l'on peut multiplier des matrices de taille m définies sur un anneau A quelconque en utilisant $O(m^\omega)$ opérations $(+, \times)$ dans A. À l'aide des algorithmes de [CW90] et [Wil12] nous avons $\omega \leqslant 2,38$.

Nous notons par $\tilde{O}_r$ le coût de la complexité en omettant les facteurs logarithmiques en la variable r. Ainsi nous avons $O(r\ell\log(r)\log(\ell)) \subset \tilde{O}_r(r\ell\log(\ell)) \subset \tilde{O}_{r,\ell}(r\ell)$. Nous omettrons de préciser la variable quand il n'y a pas d'ambiguïtés possibles.

Enfin des algorithmes de type Las Vegas vont être utilisés dans ce travail ; ces algorithmes sont des algorithmes probabilistes qui produisent un résultat

toujours correct mais dont la complexité dépend de l'aléa fourni. Dès que nous utilisons un algorithme de type Las Vegas, nous analysons sa complexité dans le cas moyen, et nous ignorons le pire cas. Nous indiquons donc l'utilisation d'algorithme de type Las Vegas dès que nous parlons de complexité moyenne.

1.2 Théorie de Galois

On définit tout d'abord un *corps de décomposition*.

Définition 1.1. Soit $\mathbb{K}$ un corps, soit un ensemble fini de polynômes $(P_i)_{i\in I}$. On dit alors que $\mathbb{L}$ est le *corps de décomposition* de cet ensemble de polynômes si chaque polynôme P_i se factorise en un produit de facteurs linéaires et si $\mathbb{L}$ est généré sur $\mathbb{K}$ par les racines des polynômes P_i. Le *corps de décomposition* est unique à isomorphisme près.

Définition 1.2. Une extension de corps $\mathbb{L}/\mathbb{K}$ est dite *normale* ou quasi-galoisienne lorsque tout polynôme défini sur celle-ci se scinde ou n'admet aucune racine.

Définition 1.3. Soit une extension de corps $\mathbb{L}/\mathbb{K}$, un élément x de $\mathbb{L}$ est dit séparable sur $\mathbb{K}$ si son polynôme minimal défini sur $\mathbb{K}$ n'admet aucune racine multiple. Une extension de corps $\mathbb{L}/\mathbb{K}$ est dite *séparable* si tout élément $x \in \mathbb{L}$ est séparable.

Définition 1.4. Une extension de corps $\mathbb{L}/\mathbb{K}$ est dite une *extension Galoisienne* si elle est à la fois séparable et normale.

Théorème 1.5. *Soit* $\mathbb{L}/\mathbb{K}$ *une extension Galoisienne. Alors il existe un élément* $x \in \mathbb{L}$ *appelé* élément primitif *tel que* $\mathbb{L} = \mathbb{K}[x]$.

Soit $\mathbb{L}/\mathbb{K}$ une extension Galoisienne alors on appelle *groupe de Galois* de $\mathbb{L}/\mathbb{K}$ le groupe d'automorphismes de $\mathbb{L}$ qui laisse fixe $\mathbb{K}$, on le note $\mathsf{Gal}(\mathbb{L} : \mathbb{K})$.

Soit $x \in L$, soit $\sigma \in \mathsf{Gal}(\mathbb{L} : \mathbb{K})$ alors on appelle $\sigma(x)$ les conjugués de x et ils constituent les racines du polynôme minimal de x défini sur $\mathbb{K}$. On appelle représentant de l'orbite de x sous l'action d'un élément de $\mathsf{Gal}(\mathbb{L} : \mathbb{K})$ n'importe quel élément de l'orbite.

Définition 1.6. Pour une extension de corps $\mathbb{L}/\mathbb{K}$, avec $\mathbb{K}$ de caractéristique positive, un élément de $\mathbb{L}$ est dit *purement inséparable* ou radiciel si il est stable sous l'action d'un élément de $\mathsf{Gal}(\mathbb{L} : \mathbb{K})$. Une extension de corps $\mathbb{L}/\mathbb{K}$ est alors dite purement inséparable (ou radicielle) si tout élément de $\mathbb{L}$ l'est.

Définition 1.7.

- Le degré de séparabilité d'une extension $\mathbb{L}/\mathbb{K}$ est le degré de l'extension $\mathbb{L}$ par rapport à $\mathbb{K}$ lorsque celle-ci est séparable.
- Le degré d'inséparabilité d'une extension $\mathbb{L}/\mathbb{K}$ est le degré de l'extension $\mathbb{L}$ par rapport à $\mathbb{K}$ lorsque celle-ci est purement inséparable.

1.3 Courbes Elliptiques

Dans cette section nous allons faire quelques rappels sur les courbes elliptiques. Pour approfondir le sujet le lecteur pourra consulter [Sil86] ou encore [Was08].

1.3.1 Équations de Weierstrass

Soit $\mathbb{K}$ un corps de clôture algébrique $\overline{\mathbb{K}}$. Sauf mention explicite du contraire, par convention on notera p la caractéristique du corps $\mathbb{K}$. On rappelle tout d'abord la définition d'un espace projectif sur $\mathbb{K}$.

Définition 1.8. On appelle espace projectif de dimension 2 sur un corps $\mathbb{K}$ et on note $\mathbb{P}^2(\mathbb{K})$, l'ensemble des classes $(X : Y : Z)$ de la relation d'équivalence définie comme suit :

$$\forall (X,Y,Z) \in \mathbb{K}^3 \setminus (0,0,0), (X,Y,Z) \equiv (X',Y',Z') \Leftrightarrow \exists c \in \mathbb{K}^*, X' = cX, Y' = cY, Z' = cZ.$$

Définition 1.9. Une courbe elliptique E est définie comme la variété projective lisse associée à l'équation

$$E : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \tag{1.1}$$

avec a_1, a_2, a_3, a_4, a_6 des éléments de $\overline{\mathbb{K}}$. Dès lors que a_1, a_2, a_3, a_4, a_6 appartiennent à $\mathbb{K}$ alors la courbe est dite définie sur $\mathbb{K}$.

Définition 1.10. Soit une courbe E définie sur $\mathbb{K}$ on note $E(\mathbb{K})$, l'ensemble des points d'une courbe elliptique E définie sur $\mathbb{K}$, c'est l'ensemble :

$$E(\mathbb{K}) = \{(X : Y : Z) \in \mathbb{P}^2(\mathbb{K}) : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3.\}$$

Le seul point correspondant à $Z = 0$ est le *point à l'infini* $0_E = (0 : 1 : 0)$, chaque classe différente de 0_E a un unique représentant de la forme $(X, Y, 1)$.

Ainsi cette dernière remarque nous amène à considérer le changement de variables $x = \frac{X}{Z}$, $y = \frac{Y}{Z}$ (pour $Z \neq 0$), on passe alors en coordonnées affines et on obtient l'équation affine de Weierstrass :

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{1.2}$$

On peut alors définir l'ensemble des points de la courbe définis sur $\mathbb{K}$ dans ce système de coordonnées affines comme :

$$E(\mathbb{K}) = \{(x,y) \in \mathbb{K}^2 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{0_E\}$$

Nous travaillerons désormais dans la suite de ce document avec ce système de coordonnées affines des points d'une courbe elliptique.

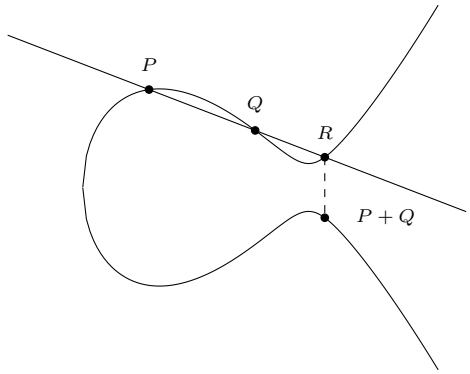
On définit aussi :

$$b_2 = a_1^2 + 4a_2, b_4 = a_1a_3 + 2a_4, b_6 = a_3^2 + 4a_6, b_8 = a_1^2a_6 - a_1a_3a_4 + 4a_2a_6 + a_2a_3^2 - a_2^4.$$

À l'aide de ceux-ci on définit le discriminant Δ de l'équation de Weierstrass (1.2) :

$$\Delta = -b_2^2b_8 - 8b_4 - 27b_6^2 + 9b_2b_4b_6.$$

La courbe E admet un unique point singulier si et seulement si Δ est nul, la courbe est non singulière si et seulement si Δ est non nul ([Sil86, Prop. III.1.4]).



On définit :

$$j = \frac{(b_2^2 - 24b_4)^3}{\Delta}.$$

La constante j est appelée *j-invariant* de la courbe.

Une question naturelle est de se demander à quel point l'équation de Weierstrass définit de façon unique une courbe elliptique. En considérant les changements de variables qui préservent le point à l'infini 0_E, il est montré [Sil86, III.3.1b] que le seul changement de variables préservant la forme de l'équation de Weierstrass et 0_E est :

$$x = u^2x' + r \quad y = u^3y' + u^2sx' + t$$

avec u, r, s, t des éléments de $\overline{\mathbb{K}}$ et u différent de 0. En calculant alors les coefficients a_i' de la nouvelle équation de Weierstrass obtenue par le changement de variables, on obtient un j-invariant identique, ce qui justifie alors la dénomination de celui-ci.

On rappelle que si l'on note $f(x, y) = 0$ l'équation affine de Weierstrass d'une courbe elliptique E définie sur $\mathbb{K}$, alors son corps des fonctions $\mathbb{K}(E)$ est le corps des fractions de l'anneau des coordonnées

$$\mathbb{K}(E) := \mathbb{K}[x, y]/(f(x, y)).$$

1.3.2 Loi de groupe

On peut définir sur $E(\mathbb{K})$ une loi de groupe abélienne à l'aide de la méthode dite de la *corde et de la tangente*.

Définition 1.11 (Loi d'addition)**.** Soient $P, Q \in E(\mathbb{K})$, L la droite reliant P à Q (ou tangente à la courbe en P si $P = Q$) et R le troisième point d'intersection de L avec E. Soit L' la droite reliant R à 0_E cette droite intersecte alors la courbe en un troisième point $P + Q$.

En utilisant la notation (x_P, y_P) pour les coordonnées affines d'un point P de la courbe, on obtient alors pour des points P, Q de $E(\mathbb{K})$ les formules suivantes :

— $P + 0_E = 0_E + P = (x_P, y_P)$;

— $-P = (x_P, -y_P - a_1x_P - a_3)$;

— En posant $\lambda = \begin{cases} \frac{y_Q - y_P}{x_Q - x_P} & \text{si } P \neq Q \\ \frac{3x_P^2 + 2a_2 x_P + a_4 - a_1 y_P}{2y_P + a_1 x_P + a_3} & \text{si } P = Q \end{cases}$,
on peut alors exprimer les coordonnées de $P + Q$ par

$$x_{P+Q} = \lambda^2 + a_1\lambda - a_2 - x_P - x_Q,$$
$$y_{P+Q} = -(\lambda + a_1)x_{P+Q} - y_P - \lambda x_P - a_3.$$

Une preuve que cette loi définit bien une loi de groupe abélienne est montrée dans [Sil86, III.2.2] ainsi qu'une démonstration des formules énoncées.

Multiplication scalaire

À l'aide de la loi additive on peut définir la multiplication scalaire par l'entier naturel m comme suit :

$$\begin{aligned} [m] : E(\mathbb{K}) &\to E(\mathbb{K}) \\ P &\mapsto \underbrace{P + \cdots + P}_{m\text{fois}}. \end{aligned} \tag{1.3}$$

Définition 1.12. On appelle points de *m-torsion* l'ensemble des points de E qui sont envoyés sur l'élément neutre 0_E par $[m]$. Cet ensemble est noté $E[m]$.

1.3.3 Isogénies

Définition 1.13. Soient E_1 et E_2 deux courbes elliptiques, une isogénie φ de E_1 dans E_2 est un morphisme de variétés algébriques surjectif :

$$\varphi : E_1 \to E_2$$

avec $\varphi(0_{E_1}) = 0_{E_2}$.

En particulier, on a le résultat suivant qui nous permet de spécifier le lien entre les isogénies et les homomorphismes de groupe :

Théorème 1.14. *Soit $\varphi : E_1 \to E_2$ une isogénie alors pour tous points P, Q de E_1 on a :*

$$\varphi(P + Q) = \varphi(P) + \varphi(Q)$$

Démonstration. Voir [Sil86, Theoreme III.4.8] □

Exemple 1.15. La multiplication par m est une isogénie :

$$[m](P + Q) = [m]P + [m]Q.$$

On dira que E_1 et E_2 sont isogènes lorsqu'il existe une isogénie φ de E_1 dans E_2.

L'ensemble des isogénies de E_1 vers E_2 adjoint à l'application nulle est appelé groupe des homomorphismes et est noté $\mathrm{Hom}(E_1, E_2)$.

Lorsque $E_1 = E_2$ l'ensemble $\mathrm{Hom}(E_1, E_1)$ est appelé anneau des endomorphismes et est noté $\mathrm{End}(E_1) = \mathrm{Hom}(E_1, E_1)$. Les éléments de $\mathrm{End}(E_1)$ inversibles sont appelés automorphismes et sont notés $\mathrm{Aut}(E_1)$.

Définition 1.16. Soient E_1, E_2 deux courbes définies sur $\mathbb{K}$, alors l'isogénie qui relie E_1 et E_2 est définie sur $\mathbb{K}$ si elle commute avec tout élément de $\mathsf{Gal}(\overline{\mathbb{K}} : \mathbb{K})$

Notation 1.17. Soient E_1, E_2 deux courbes elliptiques définies sur $\mathbb{K}$, alors on note $\mathrm{Hom}_{\mathbb{K}}(E_1, E_2)$, l'ensemble des isogénies de E_1 vers E_2 définies sur $\mathbb{K}$.

Une isogénie définie sur $\mathbb{K}$ sera dite $\mathbb{K}$-*rationnelle* ou simplement *rationnelle* quand il n'y a pas d'ambiguïté.

En particulier par la suite on étudiera comment calculer un élément de cet ensemble. Le résultat suivant permet de donner une autre représentation des isogénies.

Proposition 1.18. Soit E une courbe elliptique, alors il y a une correspondance bijective entre les isogénies séparables qui ont pour domaine de définition E et les sous-groupes finis de E :

$$(\varphi : E \to \varphi(E)) \iff \ker(\varphi)$$

Démonstration. Voir [Sil86, Proposition 4.12]. □

En utilisant le résultat de la proposition précédente nous introduisons la notation suivante :

Notation 1.19. Pour E une courbe elliptique et C un sous-groupe fini des points de E la notation ${}^{E}\!/_{C}$ désigne la courbe obtenue par l'isogénie séparable de noyau C.

Nous pouvons alors illustrer l'énoncé de la proposition 1.18 par les correspondances bijectives suivantes entre les isogénies séparables qui ont pour domaine de définition E et les sous-groupes finis C de E :

$$\begin{aligned}(\varphi : E \to \varphi(E)) &\mapsto \ker(\varphi)\\ (E \to {}^{E}\!/_{C}) &\leftarrow\!\shortmid C.\end{aligned}$$

Pour une isogénie φ on peut définir sur les corps de fonctions associés à E_1 et E_2 l'injection suivante :

$$\begin{aligned}\varphi^* : \mathbb{K}(E_2) &\to \mathbb{K}(E_1)\\ f &\mapsto f \circ \varphi.\end{aligned}$$

Définition 1.20. Soit $\mathbb{K}$ un corps algébriquement clos, φ une isogénie définie sur $\mathbb{K}$ de E_1 dans E_2, alors φ est dite *séparable* ou *inséparable* selon que l'extension $\mathbb{K}(E_1)/\varphi^*(\mathbb{K}(E_2))$ l'est ou pas. On note alors $\deg_s \varphi$, $\deg_i \varphi$ les degrés de séparabilité et d'inséparabilité de l'extension de corps $\mathbb{K}(E_1)/\varphi^*(\mathbb{K}(E_2))$ (voir définition 1.7). Nous avons donc $\deg \varphi = \deg_s \varphi \deg_i \varphi$ qui est égal aussi au degré de l'extension de corps $\mathbb{K}(E_1)/\varphi^*(\mathbb{K}(E_2))$.

Une isogénie de degré ℓ sera alors appelée une ℓ-isogénie.

Théorème 1.21. *Soit φ une isogénie de E_1 dans E_2, alors :*
- *pour tout point Q de E_2 on a $|\varphi^{-1}(Q)| = \deg_s(\varphi)$,*
- *si φ est séparable alors $\deg_s(\varphi) = \deg(\varphi) = |\ker(\varphi)|$.*

Démonstration. Voir [Sil86, III.4.10] □

Comme les isogénies peuvent être décomposées de façon unique en une composition d'isogénies inséparables et séparables, alors on se concentre dans la suite sur la détermination d'isogénies séparables.

Voyons maintenant plus en détails le lien entre une isogénie séparable et son noyau. Pour cela on va d'abord rappeler les formules de Vélu et une application de celles-ci.

Formules de Vélu

Pour un sous-groupe C de $E(\mathbb{K})$ les formules de Vélu [Vél71] permettent d'exprimer de façon canonique une isogénie séparable $E \to E'$ de noyau C et de codomaine E'. L'isogénie est définie sur $\mathbb{K}$ si et seulement si le polynôme qui s'annule sur les abscisses des points du noyau C est défini dans $\mathbb{K}[X]$.

Soit P un point de E alors les formules de Vélu nous donnent l'isogénie I de noyau C par :

$$I(P) = \Big(x(P) + \sum_{Q \in C \setminus \{0_E\}} x(P+Q) - x(Q), \\ y(P) + \sum_{Q \in C \setminus \{0_E\}} y(P+Q) - y(Q)\Big). \tag{1.4}$$

On peut alors exprimer l'équation de la courbe image de l'isogénie à l'aide des formules d'addition. Par un souci de simplicité on se restreint au cas où l'on a $p \neq 2$, dans ce cas on peut exprimer l'équation de E par :

$$y^2 = x^3 + a_2 x^2 + a_4 x + a_6.$$

On note alors par f et f' les deux fonctions suivantes dans $\mathbb{K}(E)$:

$$\begin{aligned} f(P) &= x(P)^3 + a_2 x(P)^2 + a_4 x(P) + a_6 \\ f'(P) &= 3x(P)^2 + 2a_2 x(P) + a_4 \end{aligned}$$

Avec les formules d'addition on peut réécrire la formule de Vélu (1.4) de la façon suivante en explicitant l'isogénie sur les coordonnées affines x, y de chaque point de la courbe :

$$I(x,y) = \Big(x + \sum_{Q \in G \setminus \{0_E\}} \frac{f'(Q)}{x - x(Q)} + \frac{2f(Q)}{(x-x(Q))^2}, \\ y + \sum_{Q \in G \setminus \{0_E\}} -\frac{yf'(Q)}{(x-x(Q))^2} - \frac{4yf(Q)}{(x-x(Q))^3}\Big). \tag{1.5}$$

Alors si on note :

$$h(x) = \prod_{Q \in G \setminus \{0_E\}} (x - x(Q)),$$

on obtient :

$$I(x,y) = \left(\frac{g(x)}{h(x)}, y\left(\frac{g(x)}{h(x)}\right)'\right) \tag{1.6}$$

avec g un polynôme. On pose ensuite :

$$t = \sum_{Q \in G \setminus \{0_E\}} f'(Q), \quad u = \sum_{Q \in G \setminus \{0_E\}} 2f(Q), \quad w = u + \sum_{Q \in G \setminus \{0_E\}} x(Q) f'(Q).$$

Remarque 1.22. On peut calculer l'isogénie à l'aide de la connaissance de son noyau. Une méthode pratique reste celle préconisée par Elkies [Elk98] qui utilise les équations (1.6) et (1.5) :

$$\frac{g(x)}{h(x)} = x + \sum_{Q \in G \setminus \{0_E\}} \frac{f'(Q)}{x - x(Q)} + \frac{2f(Q)}{(x-x(Q))^2}$$

ce qui a été reformulé ([BMSS08, Proposition 4.1]) par :

$$\frac{g(x)}{h(x)} = \deg(I)x - p_1 - f'(x)\frac{h'(x)}{h(x)} - 2f(x)\left(\frac{h'(x)}{h(x)}\right)' \tag{1.7}$$

avec p_1 la somme des abscisses des points du noyau. Ainsi à partir de $h(x)$ et p_1 on est capable de calculer l'isogénie en $O(\mathsf{M}(\deg(I)))$ opérations sur $\mathbb{K}$ en développant les fractions puis en simplifiant.

Il est à noter qu'il existe une autre méthode énoncée dans [Koh96, Section 2.4] qui diffère de celle de Elkies car elle utilise le polynôme qui s'annule sur les points du groupe et exprime l'isogénie en fonction de ce polynôme.

Ainsi on explicite le lien entre le noyau de l'isogénie et sa représentation à l'aide des formules de Vélu.

Théorème 1.23 (Isogénie duale)**.** *Soit φ une isogénie définie sur $\mathbb{K}$ d'une courbe elliptique E_1 vers une courbe elliptique E_2, alors il existe une unique isogénie $\widehat{\varphi}$ de E_2 vers E_1 telle que $\widehat{\varphi}\circ\varphi = [\deg(\varphi)]_{E_1}$ est appelée* isogénie duale.

Démonstration. Voir [Sil86, III.6.1] □

Théorème 1.24. *Soit $\varphi : E_1 \to E_2$ une isogénie.*

1. *Soit $\lambda : E_2 \to E_3$ une autre isogénie, alors*
$$\widehat{\lambda\circ\varphi} = \widehat{\varphi}\circ\widehat{\lambda}.$$
2. *Soit $\phi : E_1 \to E_2$ une autre isogénie, alors*
$$\widehat{\varphi+\phi} = \widehat{\varphi} + \widehat{\phi}.$$
3. *Pour tout m entier relatif,*
$$\widehat{[m]} = [m] \text{ et } \deg[m] = m^2.$$
4. $\widehat{\widehat{\varphi}} = \varphi$,
5. $\deg(\varphi) = \deg(\widehat{\varphi})$.

Démonstration. Voir [Sil86, Theorem III.6.2]. □

Corollaire 1.25. Soit E une courbe elliptique définie sur $\mathbb{K}$ et $m \in \mathbb{Z}^*$,

1. Si $m \neq \mathrm{car}(\mathbb{K})$ alors
$$E[m] = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$
2. Si $\mathrm{car}(\mathbb{K}) = p > 0$ alors :
   (a) Soit $E[p^e] = \{0_E\}$ pour tout $e \geqslant 1$ et alors E est dite *supersingulière*,
   (b) Soit $E[p^e] = \mathbb{Z}/p^e\mathbb{Z}$ pour tout $e \geqslant 1$ et alors E est dite *ordinaire*.

Démonstration. Voir [Sil86, Corrolary III.6.4]. □

Définition 1.26 (Module de Tate)**.** Soit E une courbe elliptique et ℓ un nombre premier. Le *module de Tate ℓ-adique* de E est le groupe :

$$\mathsf{T}_\ell(E) = \varprojlim_n E[\ell^n],$$

la limite projective étant définie par rapport à l'application naturelle

$$E[\ell^{n+1}] \xrightarrow{[\ell]} E[\ell^n].$$

Comme chacun des $E[\ell^n]$ est un $\mathbb{Z}/\ell^n\mathbb{Z}$-module, on observe alors que le module de Tate a une structure naturelle de $\mathbb{Z}_\ell$-module.

Proposition 1.27. En tant que $\mathbb{Z}_\ell$ module, le module de Tate a la structure suivante :

$$\mathsf{T}_\ell \cong \begin{cases} \mathbb{Z}_\ell \times \mathbb{Z}_\ell & \text{si } \ell \neq \text{car}(\mathbb{K}), \\ \mathbb{Z}_\ell & \text{si } \ell = \text{car}(\mathbb{K}) \text{ et E est } \textit{ordinaire}, \\ \{0_E\} & \text{si } \ell = \text{car}(\mathbb{K}) \text{ et E est } \textit{supersingulière}. \end{cases}$$

1.3.4 Endomorphismes

Soit E une courbe elliptique, alors si l'on munit $\text{End}(E)$ de la composition et l'addition d'endomorphismes cela forme un anneau. De plus la multiplication scalaire fournit une injection de $\mathbb{Z}$ dans $\text{End}(E)$. Cependant $\text{End}(E)$ n'est pas nécessairement réduit à $\mathbb{Z}$. Avant de parler de cela nous avons besoin d'introduire des notions.

Définition 1.28. Un ordre $\mathcal{O}$ dans un corps de nombres quadratique K est un sous-ensemble de K tel que :

1. $\mathcal{O}$ est un sous-anneau de K,
2. $\mathcal{O}$ est un $\mathbb{Z}$-module libre de rang 2.

On a le résultat suivant sur la structure de $\text{End}(E)$.

Théorème 1.29. $\text{End}(E)$ *est*
- *soit isomorphe à* $\mathbb{Z}$ *dans ce cas la courbe est* ordinaire,
- *soit isomorphe à un ordre dans un corps de nombres quadratique imaginaire dans ce cas la courbe est* ordinaire,
- *soit isomorphe à un ordre dans une algèbre de quaternions, la courbe est* supersingulière.

Démonstration. Voir [Sil86, Corollary III.9.4], et [Sil86, Theorem V.3.1] □

Définition 1.30. Une courbe elliptique E est dite à multiplication complexe si $\text{End}(E)$ n'est pas réduit à $\mathbb{Z}$ mais isomorphe à ordre dans un corps de nombre quadratique imaginaire.

1.4 Courbes elliptiques définies sur un corps fini

Soit p un nombre premier, on notera $\mathbb{F}_q = \mathbb{F}_{p^e}$ le corps fini à q éléments. Travailler sur un corps fini entraîne le fait que le nombre de points d'une courbe elliptique est fini, ainsi nous travaillons avec un groupe abélien fini. Afin d'étudier ce groupe, et en particulier d'établir sa cardinalité, nous allons introduire l'endomorphisme de Frobenius. Dans la suite de ce document nous considérerons que les courbes elliptiques mentionnées sont définies sur un corps fini.

On a tout d'abord le résultat suivant sur la structure des points d'une courbe elliptique :

Proposition 1.31. Le groupe abélien $E(\mathbb{F}_q)$ est isomorphe à $\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$ avec $n_2 \mid n_1$ et $n_2 \mid q-1$

Démonstration. Voir [Was08, Theorem 4.1] □

Notation 1.32. On notera par $E(\mathbb{F}_q)[\ell^\infty]$ le plus grand groupe de points de la courbe E, au sens de l'inclusion, qui contient les points de ℓ-torsion définis sur $\mathbb{F}_q$.

On a le résultat suivant qui donne l'égalité entre la cardinalité de deux courbes elliptiques isogènes.

Proposition 1.33. Soient E, E' deux courbes elliptiques définies sur un corps fini avec E et E' reliées par une isogénie alors E et E' ont la même cardinalité sur $\mathbb{F}_q$.

Démonstration. Voir [Sil86, Exercise V.5.4.a] □

1.4.1 L'endomorphisme de Frobenius

Définition 1.34. Soit E une courbe définie sur $\mathbb{F}_q$, l'application :

$$\begin{aligned} \pi : E &\mapsto E \\ (X : Y : Z) &\mapsto (X^q : Y^q : Z^q) \end{aligned}$$

est un homomorphisme de la courbe et est appelée *endomorphisme de Frobenius*.

Maintenant que nous avons défini l'endomorphisme de Frobenius, voyons les différentes propriétés qu'il a selon que la courbe sur laquelle il est défini soit ordinaire ou supersingulière.

Proposition 1.35. Soit E une courbe elliptique définie sur $\mathbb{F}_q$, soit π l'endomorphisme de Frobenius. Les conditions suivantes sont équivalentes :

1. E est supersingulière,
2. $E[p^e] = \{0_E\}$ pour tout $e > 0$,
3. la duale $\widehat{\pi}$ de l'endomorphisme de Frobenius est purement inséparable,
4. la trace t_π de l'endomorphisme de Frobenius est divisible par p,
5. l'anneau des endomorphismes $\mathrm{End}(E)$ est isomorphe à un ordre dans une algèbre de quaternions.

Si ces conditions ne sont pas vérifiées alors on a les conditions équivalentes suivantes :

1. E est ordinaire,
2. $E[p^e] = \mathbb{Z}/p^e\mathbb{Z}$ pour tout $e > 0$,
3. la duale $\widehat{\pi}$ de l'endomorphisme de Frobenius est séparable,
4. la trace t_π de l'endomorphisme de Frobenius est première avec p,
5. l'anneau des endomorphismes $\mathrm{End}(E)$ est isomorphe à un ordre dans un corps de nombres quadratique imaginaire.

Démonstration. Voir [Sil86, Theorem V.3.1] □

Dorénavant on ne va travailler qu'avec des courbes elliptiques ordinaires dans tout le reste du document.

L'endomorphisme de Frobenius π relatif à $\mathbb{F}_q$ admet pour équation :

$$\pi^2 - t_\pi \pi + q = 0$$

avec t_π la trace de l'endomorphisme de Frobenius. Cette équation a un rôle important dans le calcul de cardinalité de courbes elliptiques [Sch85].

Proposition 1.36. Soit E une courbe elliptique définie sur $\mathbb{F}_q$, soit t_π la trace de l'endomorphisme de Frobenius relatif à $\mathbb{F}_q$ alors :

$$|E(\mathbb{F}_q)| = q + 1 - t_\pi.$$

Démonstration. Voir [Sil86, Theorem V.1.1] □

Théorème 1.37 (Hasse)**.** *Soit E une courbe définie sur $\mathbb{F}_q$, alors*

$$|t_\pi| \leqslant 2\sqrt{q} \tag{1.8}$$

Démonstration. Voir [Sil86, Theorem V.1.1] □

Nous rappelons qu'une courbe elliptique est dite à multiplication complexe si son anneau des endomorphismes est isomorphe à un ordre dans un corps quadratique imaginaire. Ainsi toute courbe elliptique ordinaire définie sur un corps fini est à multiplication complexe.

1.4.2 Algorithme de Schoof et ses améliorations

Dans cette sous-section une partie plus technique va être abordée. Celle-ci permettra au lecteur non initié de se familiariser avec des méthodes déterminant des sous ensembles de la ℓ-torsion à l'aide du Frobenius. Cette partie présente aussi l'avantage de montrer le contexte d'algorithmes (Elkies 1998 et BMSS 2008 présentés dans le chapitre 2) de calculs d'isogénies auxquels il est pertinent de se comparer.

L'algorithme de Schoof [Sch85] consiste à calculer le cardinal d'une courbe elliptique E définie sur $\mathbb{F}_q$ à l'aide de l'équation caractéristique du Frobenius π :

$$X^2 - t_\pi X + q = 0.$$

Une fois la valeur de la trace du Frobenius t_π déterminée, on a alors $|E(\mathbb{F}_q)| = q + 1 - t_\pi$. En pratique cette équation est résolue modulo ℓ_i, avec ℓ_i un nombre premier. Cette résolution est répétée pour un ensemble L de nombres premiers tel que : $\prod_{\ell_i \in L} \ell_i > 4\sqrt{q}$. Le théorème des restes chinois est alors utilisé pour déterminer t_π modulo $\prod_{\ell_i \in L} \ell_i$. On utilise ensuite le théorème de Hasse pour déterminer la cardinalité de la courbe.

Le principal problème avec cette approche est que l'on travaille avec la ℓ-torsion qui lorsque l'on a $\ell \neq p$ est de la forme $E[\ell] \simeq \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$. On doit alors travailler modulo le polynôme de ℓ-division (le polynôme unitaire qui s'annule sur les abscisses des points de ℓ-torsion) qui est de degré $(\ell^2 - 1)/2$. L'objectif de l'amélioration d'Elkies [Elk91] est alors de considérer des sous-groupes de la ℓ-torsion afin de diminuer le coût de l'algorithme.

Des améliorations ont donc été apportées à l'algorithme de Schoof par Atkin et Elkies en analysant plus précisément l'action du Frobenius sur la ℓ-torsion afin d'exhiber des sous-groupes de la ℓ-torsion. En particulier comme l'objectif de l'algorithme de Schoof est de calculer la trace du Frobenius, il est naturel d'étudier la détermination de ses valeurs propres. Ainsi en analysant l'équation de caractéristique de π sur la ℓ-torsion :

$$X^2 - t_\pi X + q = 0 \bmod \ell,$$

on peut voir quand il est possible de déterminer des sous-groupes de la ℓ-torsion stables par π, c'est à dire des espaces propres pour l'action du Frobenius. On a

plusieurs cas possibles selon les propriétés du discriminant du Frobenius $d_\pi = t_\pi^2 - 4q$.

Définition 1.38. Soient E une courbe elliptique ordinaire définie sur $\mathbb{F}_q$ de j-invariant $j(E) \neq 0, 1728$, d_π le discriminant du polynôme caractéristique du Frobenius π associé à E. Soit ℓ un nombre premier différent de p la caractéristique de $\mathbb{F}_q$. Alors :

pour $\ell \neq 2$, on a la distinction suivante :
- si d_π est un résidu quadratique dans $\mathbb{Z}/\ell\mathbb{Z}$ alors ℓ est dit nombre premier de Elkies,
- si d_π est un non-résidu quadratique dans $\mathbb{Z}/\ell\mathbb{Z}$ alors ℓ est dit nombre premier de Atkin,

pour $\ell = 2$, on a la distinction suivante :
- si $d_\pi = 0 \bmod 4$ ou si $d_\pi = 1 \bmod 8$, alors ℓ est dit nombre premier de Elkies,
- si $d_\pi = 5 \bmod 8$, alors ℓ est dit nombre premier de Atkin.

Avec cette distinction il va être possible selon les cas de déterminer des espaces propres pour le Frobenius appliqué à la ℓ-torsion.

Notation 1.39. Soit E une courbe elliptique ordinaire définie sur $\mathbb{F}_q$. Soit C un sous-groupe de $E[\ell]$ d'ordre ℓ. On note s le plus petit entier ρ tel que $\pi^\rho(C) = C$.

Dans le cas Elkies, on doit faire une distinction selon la nullité du discriminant d_π modulo ℓ.
- Si $d_\pi = 0 \bmod \ell$ lorsque $\ell \neq 2$ et $d_\pi = 0 \bmod 4$ lorsque $\ell = 2$ alors il n'y a qu'une seule valeur propre λ pour le Frobenius restreint à la ℓ-torsion et l'espace propre est défini sur $\mathbb{F}_{q^s}$ avec $s = 1$ si l'espace propre est de dimension 2 sur $\mathbb{F}_q$ et $s = \ell$ si seulement un espace propre de dimension 1 est défini sur $\mathbb{F}_q$.
- Si $d_\pi \neq 0 \bmod \ell$ lorsque $\ell \neq 2$ et $d_\pi = 1 \bmod 8$ alors il y a deux valeurs propres λ, μ pour le Frobenius restreint à la ℓ-torsion et les espaces propres sont définis sur $\mathbb{F}_q$.

Dans le cas Atkin les valeurs propres ne sont pas définies sur $\mathbb{F}_\ell$ mais sur $\mathbb{F}_{\ell^2}$, les espaces propres sont alors définis sur $\mathbb{F}_{q^s}$ avec $s \mid \ell + 1$.

On ne peut appliquer a priori ce résultat, car il suppose la connaissance de t_π et donc la cardinalité de la courbe. On doit donc travailler avec un autre objet : le ℓ-ième polynôme modulaire $\Phi_\ell(X, Y) \in \mathbb{Z}[X, Y]$, qui est de degré $\ell + 1$ et symétrique.

Proposition 1.40. Soient $j_0 \in \mathbb{F}_q$ le j-invariant d'une courbe elliptique E_0 définie sur $\mathbb{F}_q$ de j-invariant $j(E) \neq 0, 1728$ et $\Phi_\ell(X, Y) \in \mathbb{Z}[X, Y]$ le ℓ-ième polynôme modulaire. Les $\ell + 1$ racines du polynôme $\Phi_\ell(X, j_0)$ sont les j-invariants de courbes ℓ-isogènes à E_0.

Démonstration. Voir [Fou01, Théorème 4.1.1] qui utilise notamment le résultat de [Cox89, Theorem 11.23]. □

Les j invariants des courbes ℓ-isogènes à E_0, racines du polynôme modulaire évalué en j_0, correspondent exactement aux j-invariants des courbes générées par les ℓ isogénies $E \to E/C$ avec C(noyau de l'isogénie) un des $\ell + 1$ sous-groupes cycliques de la ℓ-torsion.

On montre alors le lien entre l'existence des espaces propres et les racines du ℓ-ième polynôme modulaire Φ_ℓ par la proposition suivante.

Proposition 1.41. Soit E une courbe ordinaire définie sur $\mathbb{F}_q$ de j-invariant $j(E) \neq 0, 1728$. Alors :

1. le polynôme $\Phi_\ell(X, j)$ a une racine $j_0 \in \mathbb{F}_q^r$ si et seulement si le noyau C de l'isogénie $E \to E/C$ avec $j(E/C) = j_0$ est un espace propre de dimension 1 pour π^r restreint à $E[\ell]$;
2. le polynôme $\Phi_\ell(X, j)$ se scinde complètement sur $\mathbb{F}_q^r[X]$ si et seulement si π^r agit comme une matrice scalaire sur $E[\ell]$.

Le théorème suivant de Atkin permet de déterminer plus spécifiquement les cas possibles de factorisation de $\Phi(X, j)$ et aussi d'énoncer si le nombre est de Elkies ou de Atkin selon les cas :

Théorème 1.42 (Atkin)**.** *Soit E une courbe ordinaire définie sur $\mathbb{F}_q$ de j-invariant $j(E) \neq 0, 1728$. Soit $\Phi_\ell(X, j(E)) = f_1 f_2 \cdots f_s$ la factorisation de $\Phi_\ell(X, j(E))$ dans $\mathbb{F}_q[X]$ en éléments irréductibles, alors les degrés possibles de $f_1, f_2, \cdots, f_s$ sont :*

1. *$(1, \ell)$ ou $(1, 1, \cdots, 1)$. Dans les deux cas $t_\pi^2 - 4q = 0 \bmod \ell$, dans le premier cas on pose $r = \ell$ et dans le second $r = 1$;*
2. *$(1, 1, r, r, \cdots, r)$. Dans ce cas $t_\pi^2 - 4q$ est un résidu quadratique modulo ℓ. On a alors r qui divise $\ell - 1$ et π agit comme une matrice scalaire sur $E[\ell]$;*
3. *$(r, r, \cdots, r)$ avec $r > 1$. Dans ce cas $t_\pi^2 - 4q$ n'est pas un résidu quadratique, r divise $\ell + 1$ et la restriction de π à $E[\ell]$ admet un polynôme caractéristique irréductible sur $\mathbb{F}_q$.*

Dans tous les cas on a r qui correspond à l'ordre de la matrice π dans $\mathrm{PGL}_2(\mathbb{Z}/\ell\mathbb{Z})$ et la trace du Frobenius t_π vérifie :

$$t_\pi^2 = q(\zeta + \zeta^{-1})^2 \bmod \ell \tag{1.9}$$

avec $\zeta \in \overline{\mathbb{F}_q}$ une racine r-ième primitive de l'unité. Ainsi dans le cas Atkin pour déterminer t_π on est amené à tester $\varphi(r)/2$ racines primitives r-ième de l'unité.

En pratique pour déterminer la nature d'un nombre premier ℓ on calcule $g(X) = \mathrm{pgcd}(\Phi(X, \ell), X^q - X)$. Lorsque l'on a $g(X) = 1$ alors ℓ est un nombre de Atkin, sinon ℓ est un nombre de Elkies.

Les nombres premiers de Elkies sont les plus favorables au calcul de t_π car une fois que l'on a un nombre premier de Elkies alors par la proposition 1.41 il existe un sous groupe cyclique C de la ℓ torsion qui est un espace propre de dimension 1 pour le Frobenius π. On résout alors

$$X^2 - t_\pi X + q = 0 \bmod g_\ell$$

avec g_ℓ le polynôme qui s'annule sur les abscisses des points de C. Ce groupe C étant plus petit que celui de la ℓ-torsion, on va diminuer la complexité du calcul à effectuer pour trouver la trace modulo ℓ. En effet la ℓ-torsion étant isomorphe à un produit de deux groupes cycliques, une fois une valeur propre trouvée λ, alors l'autre valeur propre est $\mu = q/\lambda \bmod \ell$ et l'on obtient alors la trace $t_\pi = \lambda + \mu \bmod \ell$.

Par contre pour les nombres premiers ℓ de Atkin, comme un sous groupe cyclique de la ℓ-torsion ne peut être déterminé dans $\mathbb{F}_q$ alors on ne peut déterminer les valeurs exactes de t_π modulo ℓ. On doit donc considérer toutes les

valeurs possibles données par (1.9). On répète alors cette opération pour différents nombres premiers de Atkin, puis on utilise un algorithme pas de bébé pas de géant pour déterminer la trace du Frobenius. Il existe des améliorations sur l'algorithme pas de bébé pas de géant proposées par [Ler97], ces améliorations utilisent notamment un tri sur les nombres premiers de Atkin en fonction de leur coût. Ce coût est dû au nombre de racines primitives r-ième de l'unité, qui donnent le nombre de solutions possibles de (1.9).

On va donc dans la suite de ce document se concentrer sur le cas où ℓ est un nombre de Elkies car cela nous permettra de déterminer un sous-espace particulier de la ℓ-torsion et de la ℓ^k torsion en général avec k un entier.

Voyons le cas Elkies plus précisément car l'algorithme proposé dans ce document se compare à de la littérature qui se place dans ce contexte particulier.

Cas Elkies

Lorsque l'on est dans le cas Elkies, on cherche à déterminer un sous-groupe de la ℓ-torsion qui est aussi espace propre pour le Frobenius, le but étant de déterminer la trace du Frobenius à travers son action sur cet espace propre.

Ce sous-groupe C est calculé comme étant le noyau de l'isogénie qui relie la courbe E_0 (dont on cherche le cardinal) et une des courbes ℓ-isogènes à E_0. Pour trouver l'une des courbes ℓ-isogènes à E_0 il faut calculer les racines du ℓ-ième polynôme modulaire $\Phi_\ell(X, Y)$ évalué en j_0 (j-invariant de E_0), on obtient alors le j-invariant des courbes ℓ-isogènes définies sur $\mathbb{F}_q$. Ces courbes sont définies sur $\mathbb{F}_q$ par leur j-invariant à tordue près. Il faut donc se servir du résultat suivant prouvé par Elkies afin de déterminer exactement la courbe isogène à l'aide des formes de Weierstrass.

Proposition 1.43. Soit E_0 une courbe elliptique définie sur $\mathbb{F}_q$, un corps de caractéristique différente de 2 et de 3, de j-invariant différent de 0 et 1728, on suppose de plus que E_0 admet une courbe ℓ-isogène $\tilde{E}$. On note l'équation de Weierstrass de E_0 : $y^2 = x^3 + a_4x + a_6$. On a alors $\tilde{j}$ le j-invariant de $\tilde{E}$ et son équation de Weierstrass

$$\tilde{E} : y^2 = x^3 + \tilde{a_4}x + \tilde{a_6}$$

qui nous est donnée par les équations :

$$\tilde{a_4} = -\frac{1}{48}\frac{\tilde{j'}^2}{\tilde{j}(\tilde{j} - 1728)} \quad \tilde{a_6} = -\frac{1}{864}\frac{\tilde{j'}^3}{\tilde{j}^2(\tilde{j} - 1728)}$$

avec $\tilde{j'} \in \mathbb{F}_q$ donné par :

$$\tilde{j'} = -\frac{18}{\ell}\frac{a_6}{a_4}\frac{\Phi_{\ell,X}(j, \tilde{j})}{\Phi_{\ell,Y}(j, \tilde{j})}j$$

avec $\Phi_{\ell,X}$(resp. $\Phi_{\ell,Y}$) la dérivée partielle de Φ_ℓ en X (resp. Y) : $\frac{\partial \Phi_\ell}{\partial X}$.

Démonstration. Voir [Sch95][§7] □

Maintenant que la courbe isogène est entièrement déterminée, il reste à déterminer le noyau de l'isogénie de celle-ci à l'aide d'algorithmes tels que [Elk98], [BMSS08] puis [LS08] qui cherchent à résoudre ce problème dans un tel contexte. Une présentation de ces algorithmes est faite dans le chapitre 2.

Chapitre 2

Calcul d'isogénies sur les corps finis

Dans ce chapitre vont être présentés différents algorithmes pour résoudre le problème suivant : soient E, E' deux courbes elliptiques définies sur $\mathbb{K}$, on cherche alors à calculer la fraction $\mathbb{K}$-rationnelle qui définit une isogénie séparable qui a pour domaine $E(\mathbb{K})$ et pour codomaine $E'(\mathbb{K})$. On va s'intéresser tout particulièrement au cas des corps finis $\mathbb{F}_q$, bien que certains algorithmes (Elkies et BMSS) présentés peuvent aussi s'utiliser sur des corps de caractéristique nulle.

2.1 Rappel et applications des formules de Vélu

Comme vu dans la sous-section 1.3.3, à l'aide des formules de Vélu on peut expliciter une isogénie séparable I de degré r sous la forme :

$$I(x,y) = \left(\frac{g(x)}{h(x)}, y\left(\frac{g(x)}{h(x)}\right)'\right) \tag{2.1}$$

avec

$$h(x) = \prod_{Q \in G \setminus \{0_E\}} (x - x(Q)),$$

où $G = \ker(I)$, g un polynôme de degré r. De plus à l'aide de la reformulation d'Elkies on a :

$$\frac{g(x)}{h(x)} = \deg(I)x - p_1 - f'(x)\frac{h'(x)}{h(x)} - 2f(x)\left(\frac{h'(x)}{h(x)}\right)' \tag{2.2}$$

avec f donné par l'équation de Weierstrass de $E : y^2 = f(x)$, p_1 la somme des abscisses des points du noyau que l'on peut lire sur le coefficient de x^{r-2} dans h. Ainsi à partir de $h(x)$ on est capable de calculer l'isogénie en $\mathsf{M}(\deg(I))$ opérations sur $\mathbb{F}_q$. On va donc expliciter dans le reste de ce document des algorithmes qui calculent h.

Il est important de noter qu'il existe des isogénies de la forme :

$$I(x,y) = \left(\frac{g(x)}{h(x)}, cy\left(\frac{g(x)}{h(x)}\right)'\right) \tag{2.3}$$

avec $c \in \overline{\mathbb{F}_q}$. Ainsi on énonce les définitions suivantes :

Définition 2.1. Une isogénie I de la forme (2.3) avec $c = 1$ est dite *normalisée*. L'isogénie est alors séparable.

Soit I une isogénie qui relie deux courbes E_1, E_2 définies sur $\mathbb{K}$. Les représentations de Weierstrass des courbes sont dites *normalisées* si l'isogénie I associée à ces représentations est normalisée.

2.2 L'algorithme de Elkies 1998

Dans cette sous-section on se restreint au cas où la caractéristique p de $\mathbb{F}_q$ est supérieure ou égale à 5. En pratique on souhaite $p \gg r$. Dans le modèle de Elkies on travaille avec des courbes à équations de Weierstrass normalisées. Celles-ci sont calculées à l'aide du r-ième polynôme modulaire (voir proposition 1.43 pour la construction et [Sch95] pour plus de détails). Le r-ième polynôme modulaire est calculé en $\tilde{O}(r^3)$ opérations sur $\mathbb{F}_q$ d'après [Eng09] [BLS12, Algorithm 6.1, Theorem 1]. Les idées présentées ici sont issues du travail de Elkies [Elk98, The kernel of the isogeny]. Celui-ci commence à partir des équations de Weierstrass normalisées de E

$$y^2 = x^3 + Ax + B \tag{2.4}$$

et $\tilde{E}$

$$y^2 = x^3 + \tilde{A}x + \tilde{B} \tag{2.5}$$

et de l'équation de l'isogénie **normalisée** :

$$I(x, y) = \left(\frac{g(x)}{h(x)}, y \left(\frac{g(x)}{h(x)} \right)' \right) \tag{2.6}$$

on injecte l'équation de E et I dans l'équation de $\tilde{E}$:

$$(x^3 + Ax + B) \left(\frac{g(x)}{h(x)} \right)'^2 = \left(\frac{g(x)}{h(x)} \right)^3 + \tilde{A} \left(\frac{g(x)}{h(x)} \right) + \tilde{B}. \tag{2.7}$$

Cette équation est alors dérivée pour obtenir une équation différentielle du second ordre :

$$(3x^2 + A) \left(\frac{g(x)}{h(x)} \right)' + 2(x^3 + Ax + B) \left(\frac{g(x)}{h(x)} \right)'' = 3 \left(\frac{g(x)}{h(x)} \right)^2 + \tilde{A}. \tag{2.8}$$

On écrit alors le développement en série de la fraction rationnelle $\frac{g(x)}{h(x)}$ à l'infini :

$$\frac{g(x)}{h(x)} = x + \sum_{i \geqslant 1} \frac{d_i}{x^i} \tag{2.9}$$

que l'on injecte dans (2.8) pour trouver des relations de récurrence entre les d_i en identifiant les coefficients des x^{-i} :

$$\forall k \geqslant 3, d_k = \frac{3}{(k-2)(2k+3)} \sum_{i=1}^{k-2} d_i d_{k-1-i} - \frac{2k-3}{2k+3} A d_{k-2} - \frac{2(k-3)}{2k+3} B d_{k-3} \tag{2.10}$$

les termes d_1, d_2 étant déterminés par :

$$d_1 = \frac{A - \tilde{A}}{5}, \quad d_2 = \frac{B - \tilde{B}}{7}. \tag{2.11}$$

Ainsi, à l'aide de cette récurrence, le coût de calcul de $d_3, \cdots, d_{r-2}$ est de $O(r^2)$ opérations sur $\mathbb{F}_q$.

Il est à noter que la condition $p \gg r$ est là pour nous assurer que $2, \cdots, 2r-1$ sont inversibles dans $\mathbb{F}_q$ ce qui permet de pouvoir appliquer l'équation (2.10).

On peut alors énoncer le théorème suivant.

Théorème 2.2. *Soient E et $\tilde{E}$ deux courbes elliptiques r-isogènes définies sur $\mathbb{F}_q$ de caractéristique p avec des équations de Weierstrass normalisées pour $p > 2r-1$. Alors l'algorithme de Elkies calcule la r-isogénie en $O(r^2)$ opérations sur $\mathbb{F}_q$.*

Pour $p \gg r$ on applique la remarque suivante.

Remarque 2.3. Soit P un polynôme de degré $r - 1 > 0$ défini sur $\mathbb{F}_q[X]$ de caractéristique $p > r - 1$ ou $p = 0$. Alors P peut être déterminé à l'aide de la formule :

$$P = \exp\left(\int \frac{P'}{P}\right). \tag{2.12}$$

Ainsi à l'aide des sommes de Newton (somme des puissances successives des racines de P) $p_0 = r - 1, p_1, \cdots, p_{r-1}$ nous avons l'équation suivante :

$$\frac{P'}{P} = \frac{r-1}{X} + \sum_{i=1}^{r-1} \frac{p_i}{X^{i+1}}, \tag{2.13}$$

ce qui nous donne :

$$P = \exp\left(r - 1\log(X) - \sum_{i=1}^{r-1} \frac{p_i}{i!X^i}\right). \tag{2.14}$$

Ainsi à l'aide de l'exponentiation et de la connaissance des sommes de Newton on est capable d'exprimer P. On peut donc calculer $h(x)$ sans faire une reconstruction rationnelle (i.e. déterminer la fraction $\frac{g(x)}{h(x)}$ à partir de son développement en série $x + \sum_{i \geqslant 1} \frac{d_i}{x^i}$). Ceci nous permet donc à cette étape d'éviter un facteur $\log(r)$ (r le degré de l'isogénie) pour le calcul de h. En effet on peut déterminer les sommes de Newton : $p_0, p_1, \cdots, p_n$ de h à l'aide de la connaissance de $p_0 = r - 1, p_1$ et du développement en série de $\frac{g(x)}{h(x)}$: $x + \sum_{i \geqslant 1} \frac{d_i}{x^i}$. Dans le cas considéré par Elkies il est tout à fait vraisemblable de supposer la connaissance de p_1. En effet comme le calcul du r-ième polynôme modulaire Φ_r a été effectué (voir 1.4.2 pour plus de contexte), alors à l'aide des dérivées partielles de Φ_r on peut calculer celui-ci. Une formule explicite de ce calcul est donnée dans [CFA+05, Theorem 17.22] et sa preuve est dans [Sch95, §7]. En utilisant (2.9) et (2.13) dans (2.2) on établit la récurrence :

$$d_i = (2i+1)p_{i+1} + (2i-1)Ap_{i-1} + (2i-2)Bp_{i-2} \tag{2.15}$$

à l'aide de laquelle on calcule tous les p_i en $O(r)$ opérations sur $\mathbb{F}_q$. Ensuite à l'aide de la remarque 2.3 et des sommes de Newton de h on calcule h en $O(\mathsf{M}(r))$ opérations sur $\mathbb{F}_q$ par [BMSS08, §2.2]. Enfin à l'aide de h on peut calculer g en $O(\mathsf{M}(r))$ opérations sur $\mathbb{F}_q$.

2.3 L'algorithme de Bostan-Morain-Salvy-Schost

L'algorithme BMSS [BMSS08] propose de résoudre le même problème que l'algorithme de Elkies [Elk98] et a une meilleure complexité car il change notamment de méthode pour le calcul des h_i :

Théorème 2.4. *Soient $E, \tilde{E}$ deux courbes elliptiques r-isogènes définies sur $\mathbb{F}_q$ sous forme de Weierstrass normalisée, avec r différent de p, la caractéristique de $\mathbb{F}_q$, qui doit vérifier $p \gg r$, alors :*

- *si la somme des abscisses des points du noyau de l'isogénie est connue l'algorithme BMSS calcule l'isogénie qui relie les deux courbes en $O(\mathsf{M}(r))$ opérations sur $\mathbb{F}_q$,*
- *si la somme des abscisses des points du noyau de l'isogénie n'est pas connue l'algorithme BMSS calcule l'isogénie qui relie les deux courbes en $O(\mathsf{M}(r)\log(r))$ opérations sur $\mathbb{F}_q$.*

L'algorithme BMSS part du même principe que Elkies1998, à savoir, en reprenant les notations de la section précédente, trouver le développement en série de la solution de l'équation différentielle suivante :

$$(x^3 + Ax + B)\left(\frac{g(x)}{h(x)}\right)'^2 = \left(\frac{g(x)}{h(x)}\right)^3 + \tilde{A}\left(\frac{g(x)}{h(x)}\right) + \tilde{B}. \tag{2.16}$$

Cependant on ne connaît pas des conditions initiales en 0 pour cette équation différentielle vérifiée par $\frac{g(x)}{h(x)}$ et comme $\deg(g) = r > \deg(h) = r-1$ alors on ne peut travailler avec des conditions à l'infini. On pose donc :

$$S(x) = \sqrt{\frac{h(1/x^2)}{g(1/x^2)}} \quad \text{équivalent à} \quad \frac{g(x)}{h(x)} = \frac{1}{S(1/\sqrt{x})} \tag{2.17}$$

avec

$$S(x) = x + \frac{\tilde{A} - A}{10}x^5 + \frac{\tilde{B} - B}{14}x^7 + O(x^9). \tag{2.18}$$

L'équation (2.16) devient alors :

$$(1 + Ax^4 + Bx^6)(S'(x))^2 = 1 + \tilde{A}(S(x))^4 + \tilde{B}(S(x))^6 \tag{2.19}$$

que l'on reformule à l'aide des fonctions $G(x) = 1/(Bx^6 + Ax^4 + 1)$ et $H(t) = \tilde{B}t^6 + \tilde{A}t^4 + 1$. Ainsi (2.19) est réécrite comme

$$(S')^2 = (H \circ S)G. \tag{2.20}$$

On va d'abord exposer une solution pour résoudre cette équation différentielle (2.20), puis on présentera la résolution complète du problème énoncé dans le théorème 2.4.

Lemme 2.5. Soient $H(t) = 1 + \tilde{A}t^4 + \tilde{B}t^6$, $G(x) = \frac{1}{1+Ax^4+Bx^6}$ telles que $G(0)H(\alpha) = \beta^2$ alors à partir de S une solution de l'équation différentielle $(S')^2 = (H \circ S)G$ définie modulo x^{k+1} avec $S(0) = \alpha$ et $S'(0) = \beta$, une solution de cette même équation définie modulo x^{2k} peut être calculée à l'aide de l'algorithme 1 en utilisant $O(\mathsf{M}(2^k))$ opérations sur $\mathbb{F}_q$ avec $p \gg r$.

Démonstration. La preuve complète est donnée dans [LS08] la principale différence par rapport à [BMSS08] est que la résolution de l'équation différentielle linéaire issue de (2.20) est faite à l'aide d'un calcul de racine carrée et non plus d'une exponentiation comme dans [BMSS08]. On va donc présenter l'idée pour accroître la précision d'une solution de (2.20) et partiellement démontrer le lemme 2.5.

Soit f_1 une solution de (2.20) modulo x^{k+1} et f_2 telle que :

$$S = f_1 + f_2 \bmod x^{2k+1} \tag{2.21}$$

avec x^{k+1} qui divise f_2. Comme x^{2k} divise $f_2'^2$ par (2.20) on obtient :

$$2f_1'f_2' + f_1'^2 = G(x)H(f_1 + f_2) \bmod x^{2k}. \tag{2.22}$$

Le développement en série de Taylor de H en f_1 nous donne l'équation différentielle linéaire :

$$2f_1'f_2' + f_1'^2 = G(x)H(f_1) + G(x)H'(f_1)f_2 \bmod x^{2k} \tag{2.23}$$

avec la condition initiale $f_2(0) = 0$. On reformule cette équation différentielle linéaire :

$$f_2' - \frac{G(x)H'(f_1)}{2f_1'}f_2 = \frac{G(x)H(f_1) - f_1'^2}{2f_1'}, \tag{2.24}$$

cette équation a alors pour solution :

$$f_2 = \frac{1}{J}\int \frac{(G(x)H(f_1) - f_1'^2)J}{2f_1'}dx, \tag{2.25}$$

avec

$$J = \exp\left(-\int \frac{G(x)H'(f_1)}{2f_1'}dx\right). \tag{2.26}$$

Il est à noter que, comme on souhaite uniquement calculer une solution à précision x^{2k+1}, on a besoin uniquement de calculer J et son inverse à précision x^k. f_1' étant une solution de (2.20) alors on peut réexprimer f_1' à l'aide de (2.20) dans (2.26) et obtenir :

$$\frac{G(x)H'(f_1)}{2f_1'} = \frac{H'(f_1)f_1'}{2H(f_1)} \bmod x^k, \tag{2.27}$$

ainsi

$$J = \exp\left(-\frac{1}{2}\log H(f_1)\right) = \frac{1}{\sqrt{H(f_1)}}. \tag{2.28}$$

À chaque nouvelle itération pour résoudre (2.20) on a uniquement besoin de calculer les quantités suivantes :

$$S, \quad U = 1/S', \quad V = \sqrt{H \circ S}, \quad J = 1/V. \tag{2.29}$$

La précision de ces quantités est doublée dès lors à chaque itération de Newton. Les uniques opérations effectuées étant des inversions et des multiplications de séries, alors la i-ième itération coûte $O(\mathsf{M}(2^i))$ opérations sur $\mathbb{F}_q$, et donc par la superlinéarité de M, l'algorithme a la même complexité que la dernière itération. □

Algorithme 1 Résolution d'équation différentielle

Entrée : $k > 1, \alpha \in \mathbb{F}_q, \beta \in \mathbb{F}_q^*, H \in \mathbb{F}_q[t], G \in \mathbb{F}_q[[x]]$,
Sortie : $S \in \mathbb{F}_q[x]$ solution de $S'^2 = (H \circ S)G \bmod x^{2k}$

1: Soient $U \leftarrow 1/\beta + O(x), J \leftarrow 1/\sqrt{H(\alpha)} + O(x), V \leftarrow \sqrt{H(\alpha)} + O(x)$
2: Soit $S \leftarrow \alpha + \beta x + \frac{G'(0)H(\alpha)+G(0)H'(\alpha)\beta}{4\beta}x^2 + O(x^3)$;
3: **pour** $i \in 2, \cdots, 2^{k-1}$ **faire**
4: $\quad U \leftarrow U(2 - S'U) \bmod x^{2i}$
5: $\quad V \leftarrow (V + (H \circ S)J(2 - VJ))/2 \bmod x^i$
6: $\quad J \leftarrow J(2 - VJ) \bmod x^i$
7: $\quad S \leftarrow S + V \int ((H \circ S)G - S'^2)UJ/2 \bmod x^{2i+1}$
8: **fin pour**
9: **retourner** S.

Une solution S de l'équation différentielle (2.20) est calculée à précision x^{4r} à l'aide de l'algorithme 1. On définit les valeurs suivantes :

$$S(x) = xT(x^2), \quad R(x) = \frac{1}{T(x)^2} \quad \text{tel que } \frac{g(x)}{h(x)} = xR(1/x) \tag{2.30}$$

que l'on détermine successivement dans l'algorithme 2. La dernière étape de 2 est une reconstruction rationnelle qui a un coût de $O(\mathsf{M}(r)\log(r))$ [BCG+17, Théorème 7.5] et domine toutes les autres.

Algorithme 2 BMSS

Entrée : $r > 1$, deux courbes $E, \tilde{E}$ r-normalisées ,
Sortie : La fraction rationnelle $\frac{g(x)}{h(x)}$ qui représente la r-isogénie

1: Calculer $G(x) = 1/(1 + Ax^4 + Bx^6) \bmod x^{4r-1}$.
2: Calculer $S(x) \bmod x^{4r-1}$ à l'aide de l'algorithme 1.
3: Soit $T(x) = \sum_{i=0}^{2r-1} s_{2i+1}x^i$.
4: Calculer $R(x) = 1/T(x)^2 \bmod (x^{2r-1})$.
5: Calculer $\frac{g(x)}{h(x)}$ à l'aide de reconstruction rationnelle.

Remarque 2.6. Il est à noter que si p_1 est connu alors on peut effectuer la reconstruction rationnelle avec la méthode énoncée pour l'algorithme de Elkies et précisée dans la remarque 2.3. Il est dés lors suffisant de calculer S à précision x^{2r} car la connaissance $\frac{g(x)}{h(x)}$ à précision $r-2$ est suffisante pour connaître $p_0, p_1, \cdots, p_{r-1}$. Ainsi avec la connaissance de p_1 la complexité de l'étape 5 de l'algorithme 2 est de $O(\mathsf{M}(r))$ opérations sur $\mathbb{F}_q$ et donne la complexité de celui-ci.

Remarque 2.7. L'algorithme BMSS impose le fait d'avoir $p \gg r$ car à l'étape 7 de l'algorithme 1 une intégration est nécessaire, ce qui entraîne des divisions par les entiers compris entre 1 et $2r$ lorsque p_1 est connu, entre 1 et $4r-1$ sinon. Cela pose donc des limites aux applications de BMSS.

2.4 L'algorithme de Lercier Sirvent

L'algorithme de Lercier Sirvent répond à la problématique posée par le fait que BMSS ne peut pas s'utiliser sur des corps de petite caractéristique à cause de possibles division par 0, une solution naturelle envisagée est donc de résoudre ce problème en travaillant dans les entiers p-adiques.

Ainsi l'algorithme de Lercier Sirvent transpose l'algorithme BMSS dans les nombres p-adiques et spécifie la précision dont on a besoin sur les entrées de l'algorithme. De plus comme l'algorithme BMSS travaille avec des courbes elliptiques sous forme de Weierstrass normalisée, il est nécessaire de calculer des équations normalisées des relevés des courbes dans les p-adiques. L'algorithme est énoncé dans le cas où l'on a $p \geqslant 5$, les calculs ont lieu dans $\mathbb{Q}_q$ une extension non ramifiée de degré d de $\mathbb{Q}_p$.

L'algorithme de Lercier Sirvent calcule un relevé $\overline{E}$ de E dans $\mathbb{Q}_p$ et un relèvement $\overline{j_{E'}}$ du j-invariant j' de la courbe ℓ-isogène E'. Ensuite les formules de Elkies [Elk98] sont utilisées afin de calculer une équation de Weierstrass normalisée de $\overline{E''}$, codomaine de $\overline{I}$. L'algorithme BMSS [BMSS08] est utilisé pour calculer l'isogénie $\overline{I} : \overline{E} \to \overline{E''}$ on réduit alors $\overline{I}$ et $\overline{E''}$, enfin on calcule $I : E \to E'$ à l'aide de l'isomorphisme $E' \cong E''$.

Algorithme 3 Algorithme de Lercier-Sirvent

Entrée : E, E' deux courbes elliptiques ordinaires r-isogènes définies sur $\mathbb{F}_q$,
Sortie : I une r-isogénie telle que $I : E \to E'$

1: Calculer un relèvement de l'équation de Weierstrass de E dans $\mathbb{Q}_p$
2: Calculer un relevé $\overline{j_{E'}}$ de la solution de $\Phi_r(X, j_E)$ dans $\mathbb{Q}_p$ à partir de $j_{E'}$
3: Calculer une equation de Weierstrass normalisée de $\overline{E''}$ de j-invariant $\overline{j_{E'}}$ à l'aide des formules de Elkies (voir proposition 1.43)
4: Utiliser l'algorithme BMSS pour calculer l'isogénie $\overline{I}$
5: Réduire modulo p $\overline{E''}$ et $\overline{I}$ vers E'' et I
6: Utiliser l'isomorphisme $:E' \to E''$ pour calculer l'isogénie $I : E \to E'$.
7: **retourner** S.

Proposition 2.8 (Lairez-Vaccon)**.** Soient deux courbes r-isogènes E, E' définies sur $\mathbb{F}_q$ de caractéristique p avec $p \geqslant 5$, l'algorithme 3 calcule l'isogénie normalisée que relie E à E' à l'aide d'une précision d'au plus :

- $1+\lfloor \log_p(4r-1) \rfloor$ coefficients p-adiques si l'on ne connaît pas p_1, la somme des abscisses du noyau,
- $1 + \lfloor \log_p(2r-1) \rfloor$ coefficients p-adiques si l'on connaît p_1, la somme des abscisses du noyau.

Ce résultat issu de [LV16, Theorem 2] est une amélioration du résultat original de Lercier et Sirvent [LS08]. Cette amélioration porte notamment sur la précision de la solution de l'équation différentielle que l'on doit résoudre à l'étape 2 de l'algorithme BMSS qui est décrite dans l'algorithme 1.

Une preuve détaillée pour calculer une solution de l'équation différentielle à précision donnée est dans [LV16], cette méthode repose notamment sur la différenciation précisionnelle qui repose sur une analyse du premier ordre de la propagation des erreurs.

Détaillons un peu ce résultat : on a vu précédemment que l'on avait besoin de calculer une solution de l'équation différentielle linéaire (2.24) de précision $4r-1$

si l'on ne connaît pas p_1, la somme des abscisses des points du noyau de la r-isogénie. Dans ce cas on applique le résultat de Lairez-Vaccon : pour obtenir une solution p-adique de précision $4r-1$ on a besoin d'avoir en entrée des éléments de précision $1+\lfloor \log_p(4r-1)\rfloor$. Tandis que dans le cas où l'on connaît p_1 on a besoin de calculer une solution de (2.24) de précision $2r-1$ et avec [LV16, Theorem 2] on a besoin d'avoir une précision en entrée de $1+\lfloor \log_p(2r-1)\rfloor$ nombres p-adiques.

Remarque 2.9. Lors de l'étape 2 de l'algorithme de Lercier Sirvent (décrit dans l'algorithme 3) on a besoin de connaître l'évaluation du r-ième polynôme modulaire en j_E : $\Phi_r(X, j_E)$ et on a aussi besoin de connaître des dérivées partielles de Φ_ℓ lors de l'étape 3 (voir 1.4.2), ceci suppose donc la connaissance de Φ_r qui à l'aide de formules (voir [CFA+05, Theorem 17.22]) peut nous permettre de connaître p_1. Ainsi il est très raisonnable de penser que l'algorithme de Lercier Sirvent peut être utilisé dans certains cas avec une précision d'au plus $1+\lfloor \log_p(2r-1)\rfloor$.

Proposition 2.10. L'algorithme 3 calcule une r-isogénie à l'aide de $O(r^2)$ opérations sur $\mathbb{Q}_q$.

Démonstration. On ne considère pas dans cette analyse le coût de la construction de $\mathbb{Q}_q$. L'étape 1 de relèvement de la courbe E dans $\mathbb{Q}_q$ est considéré comme nul car on prend un relevé trivial de E. L'étape 2 peut être faite en $\tilde{O}(r)$ opérations sur $\mathbb{F}_q$ à l'aide d'un relèvement de Hensel. L'étape 3 du calcul d'une équation de Weierstrass normalisée a une complexité de $O(\ell^2)$ opérations sur $\mathbb{Q}_q$ à l'aide des formules de Elkies [Elk98] (voir 1.4.2). L'étape 4 est l'algorithme BMSS et a une complexité de $O(\mathsf{M}(r)\log(r))$ opérations sur $\mathbb{Q}_q$ si on ne connaît pas la valeur de p_1 (somme des abscisses des points du noyau de l'isogénie). L'étape 4 a un coût de $O(\mathsf{M}(r))$ opérations sur $\mathbb{Q}_q$ si on connaît la valeur de p_1 ce qui est envisageable dès lors que l'on se sert des dérivées du polynôme modulaire à l'étape 3 et d'une évaluation du polynôme modulaire à l'étape 2. Les deux dernières étapes ont, elles, un coup négligeable par rapport au reste des opérations, d'où le coût total de $O(r^2)$ opérations sur $\mathbb{Q}_q$. □

Remarque 2.11. Le coût de calcul des coefficients de ϕ_r à précision $p^{1+\log(4r-1)}$ est de $O(r^3\log^3 r\log\log r)$ opérations binaires et $O(r^2\log r)$ d'espace binaire pour stocker les $O(r^2)$ coefficients de $\phi_r \in \mathbb{Z}_p[X,Y]$ d'après [BLS12, Algorithm 6.1, Theorem 1] en utilisant la précision $1+\lfloor \log_p(4r-1)\rfloor$ préconisée par [LV16, Theorem 2].

2.5 L'algorithme de Couveignes 1996 et ses améliorations

Dans cette section nous présentons tout d'abord l'algorithme de Couveignes [Cou96], puis ensuite les différentes améliorations apportées par De Feo dans [DF11].

L'algorithme de Couveignes prend en entrée deux courbes elliptiques ordinaires r-isogènes définies sur un corps fini $\mathbb{F}_q$ avec r premier avec p et calcule la r-isogénie $\mathbb{F}_q$-rationnelle qui les relie. L'algorithme est présenté ici uniquement en caractéristique p impaire, par simplification.

2.5.1 Algorithme original de Couveignes

Soit I la r-isogénie qui relie deux courbes elliptiques ordinaires E, E' en entrée de l'algorithme de Couveignes, alors pour tout $k \geqslant 0$ on a : $I(E[p^k]) = E'[p^k]$. C'est cette correspondance qui, lorsque k est assez grand, donne une information suffisante pour interpoler la r-isogénie I. Comme la p^k-torsion est cyclique, alors cette correspondance est une correspondance entre deux groupes cycliques. Soient P un générateur de $E[p^k]$ et P' un générateur de $E'[p^k]$ tous deux calculés itérativement, l'algorithme fait alors l'hypothèse que le point P a pour image le point $[a]P'$ par la r-isogénie I avec $a \in (\mathbb{Z}/p^k\mathbb{Z})^\times$. Ainsi si l'on représente I à l'aide d'une fraction rationnelle on a :

$$\frac{g(x([j]P))}{h(x([j]P))} = x([ja]P') \quad \forall j \in \mathbb{Z}/p^k\mathbb{Z}. \tag{2.31}$$

avec $\deg g = r$ et $\deg h = r - 1$. Pour calculer la r-isogénie, l'algorithme de Couveignes calcule un polynôme $A_a \in \mathbb{F}_q[X]$ tel que l'on ait

$$A_a(x([k]P)) = x([ka]P') \bmod T \quad \forall k \in \mathbb{Z}/p^k\mathbb{Z} \tag{2.32}$$

avec $T \in \mathbb{F}_q[x]$ qui s'annule sur les abscisses des points de $E[p^k]$.

On définit alors l'interpolation de Cauchy qui nous permet de faire un lien entre ces deux représentations :

Définition 2.12. Soit $T \in \mathbb{F}_q[x]$ un polynôme de degré $n > 0$ avec $T = \prod_{i=1}^{n}(x - u_i)$ et les u_i distincts deux à deux, $A \in \mathbb{F}_q[x]$ un polynôme de degré $< n$. Pour $j \in [1, n]$ une *interpolation de Cauchy* est la recherche de polynômes $R, V \in \mathbb{F}_q[x]$ tels que :

$$\mathsf{pgcd(V, T) = 1} \quad \mathsf{deg(R) < j} \quad \mathsf{deg(V) < n - j} \quad \frac{\mathsf{R}}{\mathsf{V}} = \mathsf{A} \bmod \mathsf{T}.$$

On veut donc faire une interpolation de Cauchy appliquée à A_a et T pour calculer la forme explicite de l'isogénie de degré r. La valeur de k devrait donc être choisie telle que $p^k \geqslant 2r + 1$ mais comme tout point a son opposé de même abscisse on doit doubler le nombre de points à considérer et donc choisir k tel que $p^k \geqslant 4r + 1$. Une fois appliqué à A_a et T un algorithme de reconstruction rationnelle on vérifie si la fraction rationnelle obtenue est bien la restriction d'une isogénie sur les abscisses. Si ce n'est pas le cas on choisit alors un autre coefficient $b \neq a \in \left(\mathbb{Z}/p^k\mathbb{Z}\right)^\times$ et l'on recommence l'algorithme en supposant que $I(P) = [b]P'$.

Description détaillée de l'algorithme de Couveignes

Nous donnons ici la démarche à utiliser pour effectuer une utilisation pratique de l'algorithme de Couveignes afin de permettre de voir les différences avec notre approche ℓ-adique de l'algorithme de Couveignes faite dans le chapitre 6. Pour les détails non abordés le lecteur intéressé peut se reporter à [Cou96] et [DF11].

Calcul de la p-torsion La première étape de l'algorithme est le calcul de générateurs de la p^k torsion. On a tout d'abord besoin de définir les points de p-torsion pour cela on se sert du travail de Gunji [Gun76] et on se place dans

Algorithme 4 Algorithme original de Couveignes

Entrée : E, E' deux courbes elliptiques ordinaires r-isogènes définies sur $\mathbb{F}_q$,
Sortie : I une r-isogénie telle que $I : E \to E'$

1: Calculer du plus petit k tel que $p^k \geqslant 4r + 1$;
2: Calcul de P, P' générateurs de $E[p^k], E'[p^k]$;
3: **pour** $a \in (\mathbb{Z}/p^k\mathbb{Z})^*$ **faire**
4: Calcul de A_a et T tels que $A_a(x([k]P)) = x([ka]P) \bmod T$
5: Calcul de la fraction rationnelle $F = A_a \bmod T$ à l'aide d'une interpolation de Cauchy
6: **si** $\mathsf{Test}(F)$ **alors**
7: **retourner** F
8: **fin si**
9: **fin pour**

le cas où $p \neq 2$. Le lecteur intéressé par le cas $p = 2$ pourra se référer à [DF11, §3.2].

Le travail de Gunji [Gun76, Theorem 4] permet donc de déterminer les abscisses de points d'ordre p à l'aide d'éléments définis dans une extension de $\mathbb{F}_q$ de degré au plus $p - 1$.

Le calcul de la p^k-torsion est alors effectué itérativement à l'aide d'une p-descente, pour celle-ci on se sert de la décomposition de la multiplication par p :

$$[p] = \pi \circ V \tag{2.33}$$

avec π le Frobenius défini sur $\mathbb{F}_q$ et V le Verschiebung. L'idée originale est donc d'inverser chacune de ces isogénies pour calculer itérativement des antécédents de points d'ordre p^i par $[p]$. Inverser l'isogénie séparable V revient notamment à factoriser un polynôme de degré p dans une extension de $\mathbb{F}_q$, V pouvant être explicité à l'aide de la p-torsion de E.

Une autre approche a été proposé par De Feo pour prendre avantage notamment des constructions de tour d'Artin Schreier en s'appuyant sur les travaux de p-descente de Voloch dont notamment [Vol90, Lemma 1.1], cette approche a été suggéré dans l'article original [Cou96].

Cette méthode est plus efficace que la méthode standard car à l'aide des constructions de Tour d'Artin-Schreier on peut effectuer plus rapidement cette p-descente qui nécessite en particulier de résoudre une équation d'Artin-Schreier (équation de la forme $x^p - x = \alpha$ avec $\alpha \in \mathbb{F}_q$ de caractéristique p) qui peut être résolue à l'aide de méthodes de [DFS12, §6.1] ou par algèbre linéaire comme dans [Cou96].

Définition 2.13. Soit $\mathbb{F}_q$ un corps fini sur lequel on définit la tour de corps finis $\mathbb{L}_0 \subset \mathbb{L}_1 \subset \mathbb{L}_2 \subset \cdots \subset \mathbb{L}_i$ telle que $\mathbb{L}_i$ soit la plus petite extension de corps de $\mathbb{F}_q$ dans laquelle on a $E[p^i] \subset E(\mathbb{L}_i)$. On pose $\mathbb{L}_0 = \mathbb{F}_q$.

Pour le calcul de la p^k-torsion on a tout d'abord besoin de savoir la taille du corps dans lequel on est amené à effectuer les calculs. Le résultat suivant issu de [DF10] est une généralisation de [Ler97, Proposition 26] il montre en particulier que prendre une extension de degré p dans une telle tour augmente exactement de 1 la valuation p-adique de la torsion rationnelle de la courbe.

Proposition 2.14. Pour une tour de corps finis de $\mathbb{F}_q$ définie comme dans 2.13 on a :
— $[\mathbb{L}_1 : \mathbb{F}_q] \mid p-1$
— Pour tout $i \geqslant 1$ on a soit $[\mathbb{L}_{i+1} : \mathbb{L}_i] = p$ soit $\mathbb{L}_{i+1} = \mathbb{L}_i = \cdots = \mathbb{L}_1$.

Avant de prouver cela on a besoin du lemme suivant :

Lemme 2.15. Soit p un nombre premier, soit c un nombre premier avec p. Pour tout $k \geqslant 1$ on note $\mathrm{ord}_k(c)$ l'ordre de c dans $\mathbb{Z}/p^k\mathbb{Z}$. Alors $\mathrm{ord}_{k+1}(c) = \mathrm{ord}_k(c)$ implique que $\mathrm{ord}_k(c) = \mathrm{ord}_{k-1}(c)$.

La preuve suivante de la proposition 2.14 n'est pas différente de celle dans [DF11, Proposition 5] mais celle-ci est tout de même intéressante par son approche dont notamment l'étude de l'action du Frobenius sur le p-module de Tate d'où sa retranscription ici.

Démonstration de la proposition 2.14. On a $[\mathbb{L}_1 : \mathbb{F}_q] \mid p-1$ par [Gun76, Theorem 4]. Prouvons maintenant le second point, on rappelle tout d'abord l'équation caractéristique du Frobenius :

$$X^2 - t_\pi X + q = 0.$$

Maintenant si l'on regarde cette équation restreinte à la p-torsion, on voit que l'équation a deux solutions : 0 mod p et t_π mod p. La solution 0 mod p est écartée car le Frobenius ne peut avoir de noyau non trivial. Ainsi l'action du Frobenius sur la p-torsion revient à une multiplication par t_π mod p. Dés lors si l'on regarde cette équation sur $T_p(E)$ on voit que l'action du Frobenius peut être représentée par une multiplication par $\mathfrak{t}_\pi \in \mathbb{Z}_p$. Regardons alors l'action du groupe de Galois $\mathsf{Gal}(\mathbb{L}_k : \mathbb{F}_q)$ sur $T_p(E)$. Comme $\mathsf{Gal}(\mathbb{L}_k : \mathbb{F}_q)$ est engendré par l'automorphisme de $\mathbb{F}_q$, la restriction de son action à $E[p^k]$ peut être représentée par la multiplication de $t_k = \mathfrak{t}_\pi \bmod p^k$. Ainsi on a $[\mathbb{L}_k : \mathbb{F}_q] = \mathrm{ord}(t_k)$.

Dés lors pour tout $k \geqslant 1$ en appliquant le résultat du lemme 2.15 à $t_{k+1} = \mathfrak{t}_\pi \bmod p^{k+1}$ on obtient que $\mathrm{ord}(t_{k+1}) = \mathrm{ord}(t_k)$ implique que $\mathrm{ord}(t_k) = \mathrm{ord}(t_{k-1})$ ce qui termine la preuve. □

On voit donc à travers la preuve de la proposition 2.14 que si $E[p] \subset E(\mathbb{F}_q)$ alors il est possible que $\mathbb{L}_0 = \mathbb{L}_1 = \mathbb{L}_2$, de même lorsque l'on a $E[p] \not\subset E(\mathbb{F}_q)$ il est possible que $\mathbb{L}_1 = \mathbb{L}_2$, dés lors la distinction suivante est nécessaire.

Définition 2.16. Soit $\mathbb{L}_0, \mathbb{L}_1, \mathbb{L}_2, \cdots$, une tour de corps finis de $\mathbb{F}_q$ définie comme dans 2.13 alors on définit
— $v_p(E(\mathbb{F}_q)) = \max_i (\mathbb{L}_i \subset \mathbb{F}_q)$,
— $v_p(E(\mathbb{L}_1)) = \max_i (\mathbb{L}_i \subset \mathbb{L}_1)$.

Remarque 2.17. Il est à noter que si $v_p(E(\mathbb{F}_q)) \neq 0$ alors $v_p(E(\mathbb{F}_q)) = v_p(E(\mathbb{L}_1))$.

Ainsi on a $[\mathbb{L}_i : \mathbb{L}_1] = p^{i - v_p(E(\mathbb{L}_1))}$ pour tout $i \geqslant v_p(E(\mathbb{L}_1))$. Asymptotiquement on a donc $[\mathbb{L}_k : \mathbb{L}_1] \in O(p^k)$.

Interpolation de Cauchy L'interpolation de Cauchy se fait en deux étapes : tout d'abord il faut calculer un polynôme d'interpolation A d'après la donnée de valeurs prises en les points primitifs de p^k-torsion. Ensuite on doit reconstruire à l'aide d'une interpolation de Cauchy la fraction rationnelle $\frac{R}{V}$ égale à A modulo le polynôme unitaire T qui s'annule sur les abscisses des points d'ordre p^k.

Dans l'algorithme de Couveignes [Cou96] l'interpolation est effectuée distinctement sur les différentes orbites sous l'action du Frobenius puis en utilisant le théorème des restes chinois on obtient alors un polynôme d'interpolation modulo la p^k-torsion. Cette idée de travailler selon les différentes orbites sous l'action du Frobenius est importante et sera donc développée ici, elle a été reprise et améliorée par [DF11] ainsi que dans l'algorithme ℓ-adique de Couveignes présenté dans le chapitre 6.

Remarque 2.18. On étudie seulement les points d'ordre p^k et non de p^k-torsion car une généralisation de cette étude peut être faite pour avoir un résultat sur les points de p^k-torsion. D'un point de vue pratique prendre k tel que $p^{k-1}(p-1) \geqslant 4\ell+1$ est suffisant, asymptotiquement le résultat reste le même.

L'ensemble des abscisses des points primitifs de p^k-torsion est de taille $p^{k-1}\frac{p-1}{2}$. La taille d'une orbite sous l'action du Frobenius est quant à elle égale à $[\mathbb{L}_k : \mathbb{F}_q]$ (ou $\frac{[\mathbb{L}_k:\mathbb{F}_q]}{2}$ voir corollaire 2.19). Ainsi si l'on note e la taille de ces orbites et f le nombre de représentants on a $e \times f = p^{k-1}(p-1)/2$.

Étudions maintenant plus en détail les orbites des abscisses de points d'ordre p^k sous les actions d'éléments de groupes de Galois.

Corollaire 2.19. Soit k tel que que $\mathbb{L}_k \neq \mathbb{F}_q$ avec $\mathbb{L}_k$ défini comme dans 2.13. La taille des orbites des abscisses des points d'ordre p^k selon l'action du groupe de Galois $\mathsf{Gal}(\mathbb{L}_k : \mathbb{F}_q)$ est égale à :

1. $[\mathbb{L}_k : \mathbb{F}_q]$ si $2 \nmid [\mathbb{L}_k : \mathbb{F}_q]$,
2. $[\mathbb{L}_k : \mathbb{F}_q]/2$ si $2 \mid [\mathbb{L}_k : \mathbb{F}_q]$.

Démonstration. Comme vu dans la preuve de la proposition 2.14 on peut considérer les points d'ordre p^k comme des vecteurs propres pour le Frobenius associés à t_π. Ainsi avoir e la taille de l'orbite des abscisses plus petite que $[\mathbb{L}_k : \mathbb{F}_q]$ veut dire que $t_\pi^e = 1 \bmod p^k$ ou $t_\pi^e = -1 \bmod p^k$; par définition de $[\mathbb{L}_k : \mathbb{F}_q]$ seul le second cas est envisageable. Dés lors pour un tel $e \neq [\mathbb{L}_k : \mathbb{F}_q]$, $(t_\pi^e)^2 = 1 \bmod p^k$, ainsi $2e \mid [\mathbb{L}_k : \mathbb{F}_q]$. Ce cas n'est donc possible que si $2 \mid [\mathbb{L}_k : \mathbb{F}_q]$ et l'on aura $e = \frac{[\mathbb{L}_k:\mathbb{F}_q]}{2}$. □

Remarque 2.20. Ce résultat peut aussi être démontré à l'aide de [Gun76, Theorem 4].

On va se placer dans la suite de cette section dans le cas où l'on a $2 \nmid [\mathbb{L}_k : \mathbb{F}_q]$ afin de ne pas complexifier l'étude.

Lemme 2.21. Soit E une courbe elliptique ordinaire définie sur une tour de corps finis de la définition 2.13 telle que $\mathbb{L}_k \ncong \mathbb{L}_{k-1}$. Soient P_{k-1}, P_k deux points de E d'ordres $p^{k-1} \neq 1$ et p^k tels que $[p]P_k = P_{k-1}$. Alors il y a une bijection entre les points de p-division de $P_{k-1} \in \mathbb{L}_{k-1}$ et les points de l'orbite générée par l'action de σ un générateur de $\mathsf{Gal}(\mathbb{L}_k : \mathbb{L}_{k-1})$ appliqué à P_k.

Démonstration. L'ensemble des points de p-division de P_{k-1} est de cardinalité p car P appartient à E une courbe elliptique ordinaire. La taille de l'orbite de σ est quant à elle égale $[\mathbb{L}_k : \mathbb{L}_{k-1}]$ égale à p car $\mathbb{L}_k \ncong \mathbb{L}_{k-1}$. Il ne reste donc qu'à montrer une inclusion pour montrer l'égalité. On a vu dans la preuve de la proposition 2.14 que l'on pouvait déterminer les points de p^k torsion comme des vecteurs propres pour le Frobenius. Ainsi les points conjugués à P_k correspondent à $\sigma^i(P_k)$ avec $i \in \{0, \cdots, p-1\}$ et l'on a $[p](\sigma^i(P_k)) = \sigma^i([p]P_k) = [1]P_{k-1}$ car $P_{k-1} \in \mathbb{L}_{k-1}$. □

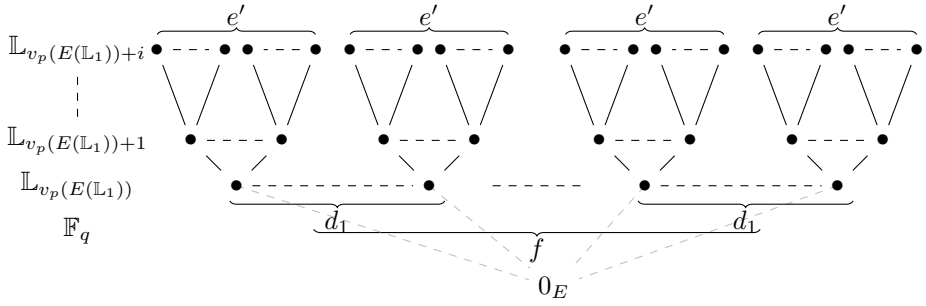


FIGURE 2.1 – Classification des points de p^k-torsion selon l'action du Frobenius.

Théorème 2.22. *Soit $k \geqslant v_p(E(\mathbb{L}_1)) \geqslant 1$, $P \in E(\mathbb{L}_k)$ tel que $\langle P \rangle = E[p^k]$ alors l'orbite de P sous l'action d'un élément générateur de $\mathsf{Gal}(\mathbb{L}_k : \mathbb{L}_{v_p(E(\mathbb{L}_1))})$ est $\mathsf{orb}(x(P)) = \{x([n]P), n = \pm 1 \bmod p^{v_p(E(\mathbb{L}_1))}\}$.*

Démonstration. Soit n tel que $n = \pm 1 \bmod p^{v_p(E(\mathbb{L}_1))}$, alors $[n]P$ est d'ordre p^k et il appartient à l'orbite de P. En effet P et $[n]P$ étant tous les deux des points de p-division d'un même point d'ordre p^{k-1} on conclue par le lemme 2.21. On montre par récurrence que P et $[n]P$ sont des points de $p^{k-v_p(E(\mathbb{L}_1))}$-division de $[p^{k-v_p(E(\mathbb{L}_1))}]P \in \mathbb{L}_{v_p(E(\mathbb{L}_1))}$ d'ordre $p^{v_p(E(\mathbb{L}_1))}$. Ainsi on a $[np^{k-v_p(E(\mathbb{L}_1))}]P = [p^{k-v_p(E(\mathbb{L}_1))}]P$; comme P est un point d'ordre p^k, on a $np^{k-v_p(E(\mathbb{L}_1))} = p^{k-v_p(E(\mathbb{L}_1))} \bmod p^k$, ce qui nous permet de déduire que l'on a $n = 1 \bmod p^{v_p(E(\mathbb{L}_1))}$. Par un argument de cardinalité on montre que l'on a déterminé tous les points de l'orbite. Les opposés des points ayant la même abscisse, alors les abscisses des points $[n]P$ avec $n = -1 \bmod p^{v_p(E(\mathbb{L}_1))}$ appartiennent aussi à l'orbite de $x(P)$ sous l'action d'un élément générateur de $\mathsf{Gal}(\mathbb{L}_{k-v_p(E(\mathbb{L}_1))} : \mathbb{L}_{v_p(E(\mathbb{L}_1))})$, mais on préférera éviter dans les calculs ces doublons inutiles. □

Corollaire 2.23. Soient E une courbe elliptique définie sur $\mathbb{F}_q$ telle que $E(\mathbb{F}_q)[p] = \{0_E\}$, $\mathbb{L}_1$ tel que $[\mathbb{L}_1 : \mathbb{F}_q] = d_1$ avec $d_1 \mid p-1$, $k \geqslant 1$, alors les orbites des abscisses de points d'ordre p^k sous l'action de $\mathsf{Gal}(\mathbb{L}_k : \mathbb{F}_q)$ sont de taille $d_1 p^{k-v_p(E(\mathbb{L}_1))}$ et il y a f orbites telles que $f \times d_1 p^{k-v_p(E(\mathbb{L}_1))} = p^{k-1}(p-1)/2$.

Sur la figure 2.1 on peut voir une répartition des abscisses des points d'ordre $p^{i+v_p(E(\mathbb{L}_1))}$ selon l'action du Frobenius et les différentes orbites. f le nombre d'abscisses des représentants des points d'ordre $p^{v_p(E(\mathbb{L}_1))}$ sous l'action de $\mathsf{Gal}(\mathbb{L}_1 : \mathbb{F}_q)$ est égal aux nombres d'abscisses de points d'ordre $p^{v_p(E(\mathbb{L}_1))}$. f est égal à $\frac{p^{v_p(E(\mathbb{L}_1))-1}(p-1)}{2d_1}$ sauf dans le cas où $2|[\mathbb{L}_1 : \mathbb{F}_q]$ où l'on a $\frac{p^{v_p(E(\mathbb{L}_1))-1}(p-1)}{d_1}$ par le corollaire 2.19.

Ainsi asymptotiquement la taille des orbites e est dans $O(p^k)$, dés lors ne serait-ce que pour représenter un polynôme d'interpolation défini sur une orbite on a besoin de $O(p^{2k})$ éléments de $\mathbb{F}_q$, et donc à minima un nombre de $O(p^{2k}) = O(r^2)$ opérations à effectuer sur $\mathbb{F}_q$. De plus il faut calculer tous les points d'ordre p^k afin de calculer le polynôme T et donc effectuer p^k additions de points de courbes elliptiques définis sur une extension de taille $[\mathbb{L}_k : \mathbb{F}_q] \in O(p^k)$, ce précalcul a un coût de $O(p^k \mathsf{M}(p^k) \log(p^k)) = O(r\mathsf{M}(r)\log(r))$. Il faut donc utiliser des techniques supplémentaires pour optimiser ce temps de calcul trop élevé. Les

améliorations de De Feo [DF11] ont donc résolu cette question et sont présentées dans la sous section 2.5.2.

L'interpolation de Cauchy réalisée à partir du polynôme A et du polynôme T qui s'annule sur les abscisses des points d'ordre p^k est faite à l'aide de $O(\mathsf{M}(p^k)\log(p^k)) = O(\mathsf{M}(r)\log(r))$ opérations sur $\mathbb{F}_q$ d'après [vzGG03, § 11.1] (voir [BCG+17, Théorème 7.5] pour plus de détails).

Validation de l'isogénie On doit ensuite tester si la fraction rationnelle $\frac{R}{V}$ calculée définit bien une isogénie, si l'un des tests échoue alors ce n'est pas l'isogénie que l'on cherche à calculer et on peut passer à un nouvel essai. Le tout premier test consiste à regarder si $\deg(R) = r$ et $\deg(V) = r-1$. Ensuite on vérifie que V est bien un carré (ou, si r est pair, que c'est le produit d'un facteur du polynôme de 2-division et d'un carré). Ces deux tests suffisent généralement à conclure et ils ont un coût de $O(\mathsf{M}(r)\log(r))$ opérations sur $\mathbb{F}_q$. Pour plus de sûreté on peut évaluer la fonction sur différents points et vérifier que c'est bien un morphisme de groupes. Enfin si une preuve déterministe est souhaitée on vérifie que V est bien un diviseur du polynôme de r-division, pour cela on calcule le polynôme de r division en $O(\mathsf{M}(r)\log(r))$ opérations sur $\mathbb{F}_q$ (pour une formule explicite voire [CFA+05, §4.4.5.a]).

2.5.2 Apports de l'utilisation de l'action du Frobenius sur des tours p-adiques à l'algorithme de Couveignes

On va se placer dans toute cette section dans le cas où la tour de corps finis définie à la définition 2.13 correspond au pire des cas où $\mathbb{F}_q \not\simeq \mathbb{L}_1$et $\mathbb{L}_1 \not\simeq \mathbb{L}_2$. En pratique une telle tour est implémentée à l'aide d'une tour d'Artin-Schreier (voir [DF11] et [DFS12] pour plus de détails).

Cette partie sur le calcul du polynôme d'interpolation est cruciale car, comme vu précédemment, c'est la partie la plus coûteuse de l'algorithme de Couveignes. On peut déjà noter qu'interpoler $p^{k-1}(p-1)$ paires de points $(P, I(P))$ avec P et $I(P)$ à coordonnées dans $\mathbb{L}_k$ entraîne un coût minimal de $O(p^{2k}) = O(r^2)$ opérations sur $\mathbb{F}_q$ à l'aide de la méthode précédemment présentée.

Bien que le polynôme A que l'on souhaite calculer soit de degré $p^{k-1}(p-1)-1$, il est possible avec moins d'informations de le calculer. En effet le polynôme A étant à coefficients dans $\mathbb{F}_q$ alors A, comme l'isogénie qu'il est censé représenter, doit commuter avec le Frobenius sur les points d'ordre p^k. Ainsi connaître l'image d'un générateur d'une orbite selon l'action du Frobenius fixe la valeur des autres points de l'orbite. Couveignes [Cou96] ne tirait pas pleinement de cette information. Il manquait pour l'algorithme original des techniques efficaces pour faire agir le Frobenius ce que les constructions de tours d'Artin Schreier de De Feo et Schost [DFS12] permettent désormais.

On va montrer dans cette sous-sous-section les idées directrices pour calculer le polynôme d'interpolation défini sur toute une orbite avec des coefficients dans $\mathbb{F}_q$. Pour faire cela on va se servir de la seule connaissance de l'image d'un représentant de l'orbite défini dans $\mathbb{L}_k \setminus \mathbb{L}_{k-1}$. Nous travaillons donc avec les points d'ordre p^k puisque que parmi les points de ℓ^k-torsion eux seuls sont définis dans $\mathbb{L}_k \setminus \mathbb{L}_{k-1}$, ils sont de plus tous dans des orbites de tailles identiques. La méthode peut alors se généraliser aux points de p^k-torsion en travaillant avec des orbites de tailles différentes.

Soient P et P' deux d'ordre p^k de E et E'. On veut calculer le polynôme d'interpolation de degré minimal $A \in \mathbb{F}_q[X]$ tel que :

$$A(x([n]P)) = x([n]P') \bmod T(x) \quad \text{pour } n \in \left(\mathbb{Z}/p^k\mathbb{Z}\right)^\times \tag{2.34}$$

avec $T(X) = \prod_{n<\frac{p^{k-1}(p-1)}{2}, n\wedge p=1}(X - x([n]P))$.

Comme on souhaite travailler distinctement sur les différentes orbites du Frobenius, on regarde la factorisation de $T(X)$ sur $\mathbb{F}_q$ comme préconisé dans [Cou96] :

$$T(X) = \prod_{i=1}^{f} T_i(X)$$

avec $\deg(T_i) = e = [\mathbb{L}_k : \mathbb{F}_q]$ (ou $e = [\mathbb{L}_k : \mathbb{F}_q]/2$ voir corollaire 2.23) et $ef = p^{k-1}(p-1)/2$.

À l'aide du théorème des restes chinois on réduit le problème au calcul de chacun des T_i et l'on définit :

$$A_i = A \bmod T_i. \tag{2.35}$$

Dés lors on va se concentrer sur le calcul de A_0.

Soit $x(P) \in \mathbb{L}_k \setminus \mathbb{L}_{k-1}$ on veut calculer :

1. le polynôme minimal T_0 de $x(P)$ défini sur $\mathbb{F}_q$ de degré égal à e,
2. le polynôme d'interpolation A_0 défini sur $\mathbb{F}_q$ de degré strictement inférieur à e tel que $A_0(x(P)) = x(P')$.

Définition 2.24. Soient $j > i \geqslant 0$, $\sigma \in \mathsf{Gal}(\mathbb{L}_j : \mathbb{L}_i)$, $T = \sum_{s=0}^{d} t_s X^s \in \mathbb{L}_k[X]$ alors :

$$\sigma(T) = \sum_{s=0}^{d} \sigma(t_s) X^s.$$

Soit A_0 un polynôme d'interpolation défini sur $\mathbb{F}_q$, alors on a pour tout $\sigma \in \mathsf{Gal}(\mathbb{L}_k : \mathbb{F}_q)$:

$$A_0(\sigma(x(P)) = \sigma(A_0(x(P))) = \sigma(x(P')).$$

L'information de l'image de $x(P) \in \mathbb{L}_k$ entraîne bien la connaissance des images des éléments de l'orbite de $x(P)$ sous l'action de n'importe quel élément de $\mathsf{Gal}(\mathbb{L}_k : \mathbb{F}_q)$, ainsi dans [DF11] l'auteur prend avantage du faible coût du Frobenius dans une tour d'Artin-Schreier à l'aide de l'algorithme [DFS12, Iter Frobenius,Theorem 17 et 18].

On présente uniquement les idées directrices pour calculer T, le calcul de A_0 et les idées développées par [DF11] et auparavant par [EM03] étant repris très largement dans la section 3.4 ils seront plus détaillés à cette occasion.

Pour plus de détails sur la description des orbites selon les cas possibles le lecteur peut regarder le lemme 2.21, le théorème 2.22 ainsi que le corollaire 2.23.

Soient $k \geqslant 1$, P un point d'ordre p^k alors $x(P) \in \mathbb{L}_k \setminus \mathbb{L}_{k-1}$. On note $\mathsf{orb}(x(P))$ l'ensemble des abscisses des points de l'orbite créée par l'action d'un élément générateur π de $\mathsf{Gal}(\mathbb{L}_k : \mathbb{F}_q)$ sur l'élément $x(P) \in \mathbb{L}_k$. On a donc :

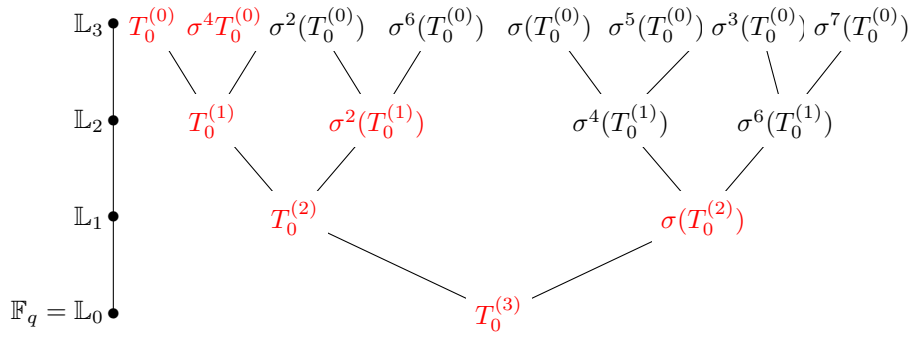


FIGURE 2.2 – Arbre de sous produits pour le calcul de $T_0^{(0)}$ dans le cas d'une tour d'extension quadratique.

$$T_0(x) = \prod_{\substack{x([n]P)\in \mathsf{orb}(x(P)) \\ n\leqslant (p^k-1)/2}} (x - x([n]P)) = \prod_{i=0}^{p^{k-1}d_1-1} (x - \pi^i(x(P)))$$

$$= \prod_{i=0}^{p^{k-1}d_1-1} \pi^i(x - x(P))$$

On note $T_0^{(0)} = x - x(P)$, soit $k \geqslant i \geqslant 0$ σ_i un élément générateur de $\mathsf{Gal}(\mathbb{L}_{k-i+1} : \mathbb{L}_{k-i})$ pour $i \geqslant 1$, supposons que l'on connaisse $T_0^{(i)}$ dés lors on définit $T_0^{(i,j)} = \sigma_i^j(T_0^{(i)})$ et l'on a

$$T_0^{(i+1)} = \prod_{j=0}^{b} \sigma_i^j(T_0^{(i)}) \quad b = \begin{cases} p-1 & \text{si } i < k-1, \\ d_1 - 1 & \text{si } (\ i = k-1 \text{ et } 2 \nmid d_1), \\ d_1/2 - 1 & \text{si } (\ i = k-1 \text{ et } 2 \mid d_1). \end{cases}$$

$T_0^{(k)}$ est égal à T_0 le polynôme minimal de $x(P)$ sur $\mathbb{F}_q$.

Une représentation de ce calcul sur un arbre de produit binaire permet de voir sur la figure 2.2 que le calcul de T_0 n'est effectué qu'en travaillant avec une branche de celui-ci à l'aide de la méthode décrite ci-dessus. En effet seul les éléments en rouge de l'arbre sont pris en compte pour le calcul de T_0. σ peut être n'importe quel élément générateur de $\mathsf{Gal}(\mathbb{L}_3 : \mathbb{L}_0)$.

Remarque 2.25. La figure 2.2 est à mettre en parallèle avec la figure 2.1 puisque l'arbre 2.2 représente un seul des fd_1 arbres de 2.1 et que les extrémités de l'arbre 2.2 représentent les polynômes qui s'annulent en les abscisses de points des extrémités d'un des arbres de 2.1.

L'algorithme de Couveignes avec les modifications apportées par l'utilisation de tours d'Artin-Schreier et du Frobenius pour le calcul du polynôme d'interpolation, dénommé «C2-AS-FI» par [DF11], a alors la complexité suivante :

Théorème 2.26. *Soient E et E' deux courbes r-isogènes, l'algorithme de Couveignes «C2-AS-FI» a, en supposant que $M(n) = O(n\log(n)\log\log(n))$, une complexité de :*

$$\tilde{O}_{p,d,\log r}(p^2d^3 + \mathsf{C}(p)pd + (pd)^\omega \log^2 r + p^3r^2d\log^3 r + p^2r^2d^2 + (\frac{r^2}{p} + p)\mathsf{C}(pd))$$

opérations sur $\mathbb{F}_p$ avec $\mathsf{C}(n)$ le nombres d'opérations à effectuer dans $\mathbb{F}_p$ pour effectuer la composition de deux polynômes de degré au plus n, par [BK78] on a $\mathsf{C}(n) \in O(n^{(\omega+1)/2})$.

Démonstration. Voir section 5.2 de [DF11]. □

Remarque 2.27. La complexité ici est donnée en termes d'opérations sur $\mathbb{F}_p$ car les tours d'Artin-Schreier sur lesquelles sont utilisées les améliorations apportées à l'algorithme de Couveignes sont construites comme des extensions de corps sur $\mathbb{F}_p$ et ainsi tout élément d'une tour d'Artin-Schreier est exprimé à l'aide d'un polynôme à coefficients dans $\mathbb{F}_p$.

On peut généraliser les travaux de DeFeo et Schost [DFS12] et De Feo [DF11] avec une tour d'Artin-Schreier construite sur une extension de $\mathbb{F}_q$ (ainsi tout élément d'une tour d'Artin-Schreier est exprimé à l'aide d'un polynôme à coefficients dans $\mathbb{F}_q$). Il faut en particulier que $\mathrm{Tr}_{\mathbb{L}_1/\mathbb{F}_q}(x_0) \neq 0$ avec Tr qui représente la Trace, $\mathbb{L}_1 = \mathbb{F}_q[X_0]/Q_0$ avec Q_0 un polynôme de degré divisant $p-1$ (par [Gun76]) et $x_0 = X_0 \bmod Q_0$. Ici $\mathbb{L}_1$ représente le premier élément de la tour, les suivant étant construits comme des extensions de degré p du précédent à l'aide d'une équation d'Artin Schreier (comme dans [DFS12]). Dans ces conditions on donne une estimation du coût de «C2-AS-FI» en termes d'opérations sur $\mathbb{F}_q$.

Théorème 2.28. *La complexité totale de l'algorithme «C2-AS-FI» à l'aide de constructions de tour d'Artin-Schreier construite sur $\mathbb{F}_q$ est dominée par le terme*

$$O(p^3r^2\log_p(p^3r)^2)$$

opérations sur $\mathbb{F}_q$.

Nous ne donnons pas une preuve de cette estimation juste quelques pistes. Le pré-calcul des points de p-torsion et de l'extension $\mathbb{L}_1$ est majoré grossièrement par $\tilde{O}_{p,\log(r)}(M(rp^2)\log_p(r)^4)$ opérations sur $\mathbb{F}_q$. Le coût dominant de l'étape d'interpolation est de $O(p^3r\log_p(p^3r)^2)$ opérations sur $\mathbb{F}_q$, nous devons répéter celle-ci $p^{k-1} \in O(r)$ fois ainsi nous obtenons ce terme dominant.

Chapitre 3

Construction efficaces de tours ℓ-adiques

La construction d'extension de corps finis est un problème naturel dès lors que l'on travaille sur des corps finis. On peut être amené à construire des extensions de corps de taille arbitraire pour lesquelles on voudra une construction dite *compatible* de telle sorte que l'on puisse projeter, lorsque cela est possible, des éléments du corps dans les constructions pré-existantes efficacement.

Définition 3.1 (Tour ℓ-adique)**.** Soit $\mathbb{F}_q$ un corps fini à q éléments de caractéristique p, soit ℓ un nombre premier différent de p, on appelle tour d'extensions ℓ-adiques du corps fini $\mathbb{F}_q$ la suite d'extensions : $\mathbb{F}_q, \mathsf{F}_1, \mathsf{F}_2, \mathsf{F}_3, \cdots$ telles que :

- F_1 est une extension de $\mathbb{F}_q$ de degré $d_1 \mid \ell - 1$. De plus $r \mid d_1$ avec r qui représente l'ordre multiplicatif de q dans $\mathbb{Z}/\ell\mathbb{Z}$,
- F_i pour $i \geqslant 2$ est une extension de F_{i-1} de degré ℓ.

Une façon naturelle de construire une extension d'un corps fini $\mathbb{F}_q$ est de trouver un polynôme P irréductible défini sur $\mathbb{F}_q$ et de degré égal à celui de l'extension désirée et de quotienter ensuite $\mathbb{F}_q[X]$ par celui-ci. Ainsi les éléments des tours d'extensions seront toujours représentés comme des polynômes à coefficients dans $\mathbb{F}_q$, la taille des éléments de F_k sera donc $O(d_1\ell^{k-1})$ éléments de $\mathbb{F}_q$.

Les travaux de [DFS12] sur les tours p-adiques ont ouvert la voie à d'autres travaux sur les tours 2-adiques [DS15] et les tours ℓ-adiques [DFDS13]. Dans ces travaux l'idée pour obtenir des constructions de tours de corps finis compatibles est le passage de représentation *univariée* à *bivariée*. Ici représentation univariée signifie que l'on peut représenter tout élément de F_i comme un polynôme de $\mathbb{F}_q[x_i]$ avec x_i un élément générateur de F_i sur $\mathbb{F}_q$, de même une représentation bivariée signifie que l'on peut représenter tout élément de F_i comme un polynôme de $\mathbb{F}_q[x_i, x_{i-1}]$ avec x_i(resp. x_{i-1}) élément générateur de F_i (resp. F_{i-1}) sur $\mathbb{F}_q$. Ces idées ont permis d'obtenir des résultats satisfaisants en terme de complexité, comparés aux résultats obtenus en utilisant de l'algèbre linéaire dans les constructions préconisées par [BCS97] et implantées dans le système de calcul formel Magma [BCP97]. Ainsi certains algorithmes tels que le *relèvement* ou la *descente* d'éléments dans les corps de la tour ℓ-adique ont des complexités optimales et correspondent seulement à une réécriture des éléments. Le relèvement correspond au fait de prendre un élément de F_{i-1} et de l'écrire comme un

élément de F_i, la descente correspond à l'opération inverse. Il y a aussi des opérations comme le Frobenius, crucial pour l'algorithme de Couveignes ℓ-adique présenté dans le chapitre 6, ou le calcul de racine carrée qui ont des coûts satisfaisants. Tout cela va être détaillé dans ce qui suit. Les travaux de [DFS12] sur les tours p-adiques ne seront pas étudiés ici, ces travaux sont en effet complémentaires de ceux étudiés et utilisés ici [DS15], [DFDS13].

Les complexités sont calculées en nombre d'opérations $(+, \times, \div)$ dans $\mathbb{F}_q$, indépendamment de la construction de $\mathbb{F}_q$.

On notera par $\mathsf{M} : \mathbb{N} \to \mathbb{N}$ l'application telle que la multiplication d'un polynôme de degré n à coefficients dans $\mathbb{F}_q$ coûte $\mathsf{M}(n)$ opérations dans $\mathbb{F}_q$ et telle que M est super-linéaire, en utilisant les résultats de [CK91] on a $\mathsf{M}(n) = O(n\log(n)\log\log(n))$.

L'idée de base de [DS15] est de permettre un passage efficace d'une représentation bivariée à une représentation univariée afin de rajouter à la volée des extensions de la tour compatibles avec ce qui a été fait auparavant.

3.1 Construction d'une tour d'extensions ℓ-adiques

L'objectif est de calculer une tour d'extensions ℓ-adiques du corps fini $\mathbb{F}_q$, avec $q \wedge \ell = 1$.

Théorème 3.2. *Soit $\mathbb{F}_q$ un corps fini de caractéristique p, soit ℓ un nombre premier différent de p, alors une tour d'extensions ℓ-adiques du corps $\mathbb{F}_q$: $\mathbb{F}_q, \mathsf{F}_1, \mathsf{F}_2, \mathsf{F}_3, \cdots$ est initialisée en $O(d_1\mathsf{M}(d_1)\log(d_1)\log(d_1 q) + \mathsf{M}(\ell)\log(\ell) + d_1^2)$ opérations en moyenne sur $\mathbb{F}_q$.*

Démonstration. On construit tout d'abord F_1 l'extension de $\mathbb{F}_q$ de degré d_1 qui divise $\ell - 1$ et est donc premier avec ℓ. Cette construction de F_1 est faite en même temps que la détermination d'un non-résidu ℓ-adique.

Pour construire F_1 on calcule tout d'abord un polynôme irréductible de degré d_1 défini sur $\mathbb{F}_q$, pour cela on utilise par exemple l'algorithme probabiliste de Ben-Or qui calcule un tel polynôme avec une complexité moyenne de $O(d_1\mathsf{M}(d_1)\log(d_1)\log(d_1 q))$ opérations sur $\mathbb{F}_q$ d'après [vzGG03, Theorem 14.42]. Soit R_1 un tel polynôme, alors par construction il existe un non-résidu ℓ-adique dans $\mathbb{F}_q[X_1]/\langle R_1\rangle$. On trouve après avoir testé $O(1)$ éléments tirés au hasard un tel non-résidu ℓ-adique, chaque essai a un coût moyen de $O(\mathsf{M}(\ell)\log(\ell))$ opérations sur $\mathbb{F}_q$ d'après [vzGG03, 11.1]. Une fois un tel non-résidu ℓ-adique y_1 trouvé on calcule son polynôme minimal P_1, ce calcul coûte $O(d_1^2) = O(\ell^2)$ opérations sur $\mathbb{F}_q$ d'après [Sho93, Th. 3.4]. On construit donc $\mathsf{F}_1 = \mathbb{F}_q[X_1]/\langle P_1(X_1)\rangle$ et le non-résidu ℓ-adique sera alors l'image de X_1 dans F_1. On définit le polynôme irréductible $P_i = P_1(X^{\ell^{i-1}})$ dans $\mathbb{F}_q[X]$ et on construit toute extension F_i de $\mathbb{F}_q$ comme étant $\mathsf{F}_i = \mathbb{F}_q[X]/P_i(X)$.

□

Remarque 3.3. Sachant que $d_1 \mid \ell - 1$ ce coût peut être borné à l'aide de ℓ par $O(\ell\mathsf{M}(\ell)\log(\ell)\log(\ell q))$ opérations en moyenne sur $\mathbb{F}_q$.

3.2 Représentation des éléments de la tour d'extensions ℓ-adiques

Les éléments de F_k peuvent être représentés de deux manières différentes : *univariée* et *bivariée*, de la même manière que dans [DFS12].

Soit P_1 le polynôme minimal défini sur $\mathbb{F}_q$ d'un résidu non ℓ adique défini sur une extension de degré d_1, à l'aide de celui-ci sont définies les suites de polynômes $T_1, T_2, T_3, \cdots, T_k$ en les indéterminées $X_1, X_2, X_3, \cdots X_k$ de la façon suivante :

$$T_1 = P_1(X_1) \quad \text{et} \quad T_k = X_k^{\ell} - X_{k-1} \quad \text{avec } k \geqslant 1 \text{ entier naturel.}$$

De la même manière la suite de polynômes $P_1, P_2, \cdots P_k$ est définie à l'aide de P_0 de la façon suivante :

$$P_k = P_1(X_k^{\ell^{k-1}}) \quad \text{avec } k \geqslant 1 \text{ entier naturel.}$$

Il y a égalité entre les idéaux suivants :

$$\langle T_1, T_2, T_3, \cdots, T_k \rangle = \langle P_k, X_{k-1} - X_k^{\ell}, ..., X_2 - X_k^{\ell^{k-2}}, X_1 - X_k^{\ell^{k-1}} \rangle. \quad (3.1)$$

Cet idéal premier sera appelé A_k et l'on a :

$$\mathsf{F}_k \cong \mathsf{F}_q[X_1, X_2, X_3, \cdots, X_k]/A_k$$

Soit $k \geqslant 1$ on note x_k l'image de l'indéterminée X_k dans l'anneau résiduel $\mathbb{F}_q[X_1, X_2, X_3, ..., X_k]/A_k$, alors par inclusion naturelle de $\mathbb{F}_q[X_1, X_2, X_3, ..., X_k]/A_k$ dans $\mathbb{F}_q[X_1, X_2, X_3, ..., X_{k+1}]/A_{k+1}$, x_k peut aussi être vu comme un élément de F_j pour $j \geqslant k$.

De plus grâce à l'équation (3.1), représenter un élément de F_k peut être fait soit comme un polynôme en $x_1, x_2, ..., x_k$ de degré au plus $\ell - 1$ en chaque variable grâce au côté gauche de l'équation (3.1), soit comme un polynôme en x_k de degré au plus $d_1\ell^{k-1} - 1$ grâce au côté droit de l'équation.

L'écriture par défaut des éléments de F_k sera donc la représentation univariée c'est à dire un élément de F_k sera représenté sous la forme $g(x_k)$ avec g un polynôme de $\mathbb{F}_q[X_k]$ de degré strictement inférieur à $d_1\ell^{k-1}$.

Cependant lors des représentations d'éléments de F_k il ne va pas être fait des changements de représentation d'un élément sous la forme $g(x_k)$ avec g un polynôme de $\mathbb{F}_q[X_k]$ à un élément sous la forme $h(x_1, x_2, \cdots, x_k)$ avec h un polynôme de $\mathbb{F}_q[X_1, X_1, X_2, \cdots, X_k]$ mais seulement à un élément de la forme $i(x_k, x_{k-1})$ avec i un polynôme de $\mathbb{F}_q[X_k, X_{k-1}]$. Cette dernière représentation est suffisante pour permettre d'effectuer la descente d'un élément dans la tour d'extensions ℓ-adiques.

On représentera alors F_k pour $k \geqslant 1$ des deux façons suivantes :

$$\mathsf{F}_k \cong \mathbb{F}_q[X_k]/\langle P_k(X_k) \rangle \cong \mathbb{F}_q[X_k, X_{k-1}]/\langle P_{k-1}(X_{k_1}), X_k^{\ell} - X_{k-1} \rangle$$

Définition 3.4. Soit F_k un élément de la tour d'extensions ℓ-adiques de $\mathbb{F}_q$. La $\mathbb{F}_q$ base univariée de F_k est :

$$1, x_k, x_k^{\ell}, ..., x_k^{d_1\ell^{k-1}-1}$$

la $\mathbb{F}_q$ base bivariée de F_k est :

$$1, x_{k-1}, x_{k-1}^{\ell}, ..., x_{k-1}^{d_1\ell^{k-2}-1}, x_k, x_k x_{k-1}, x_k x_{k-1}^2, ..., x_k x_{k-1}^{d_1\ell^{k-1}-1}, \cdots, x_k^{\ell-1} x_{k-1}^{d_1\ell^{k-2}-1}$$

En pratique le changement de base monovariée à bivariée se fait de la façon suivante à partir d'une expression $G(x_k)$ d'un élément de F_k avec G un polynôme de degré inférieur à $d_1\ell^{k-1}-1$:

$$\begin{aligned} G(x_k) &= G_0(x_k) + G_1(x_k^\ell) + x_k G_2(x_k^\ell) + \cdots + x_k^{\ell-1} G_\ell(x_k^\ell) \\ &= G_0(x_k) + G_1(x_{k-1}) + x_k G_2(x_{k-1}) + \cdots x_k^{\ell-1} G_\ell(x_{k-1}) \end{aligned}$$

avec $G_1, \cdots G_\ell$ des polynômes de degré inférieur à $d_1\ell^{k-2}-1$ et G_0 de degré strictement inférieur à ℓ. Ce changement de base ne requiert aucun calcul arithmétique, ainsi celui-ci pourra être utilisé sans coût supplémentaire et en particulier un élément pourra être considéré indifféremment dans une base bivariée ou univariée.

La descente correspond donc au passage d'un élément de F_k écrit sous la forme $G(x_k)$ en un élément de la forme $G_1(x_{k-1})$ appartenant à F_{k-1}. Le relèvement est l'opération inverse.

Exemple 3.5. Soit $\mathbb{F}_q, \mathsf{F}_1, \mathsf{F}_2, \cdots, \mathsf{F}_k$ une tour d'extensions 5-adiques telle que $\mathbb{F}_q \cong \mathsf{F}_1$, soit $\alpha \in \mathsf{F}_4$ qui s'écrit dans la $\mathbb{F}_q$ base monomiale de F_4 :

$$\alpha_0 + \alpha_5 x_4^5 + \alpha_{10} x_4^{10} + \alpha_{15} x_4^{15} + \cdots + \alpha_{5k} x_4^{5k} + \cdots + \alpha_{120} x_4^{120} \tag{3.2}$$

alors α s'écrit de la façon suivante dans la base bivariée de F_4 :

$$\alpha_0 + \alpha_5 x_3^1 + \alpha_{10} x_3^2 + \alpha_{15} x_3^3 + \cdots + \alpha_{5k} x_3^k + \cdots + \alpha_{120} x_3^{24}. \tag{3.3}$$

Ainsi on voit que α est aussi un élément de F_3. Le passage de la représentation de α de (3.2) à (3.3) correspond à une *descente*, l'opération inverse est elle un *relèvement*.

Par contre pour β un élément de F_4 écrit de la façon suivante dans la base monovariée :

$$\beta_0 + \beta_1 x_4 + \cdots + \beta_{5k} x_4^{5k} + \beta_{5k+1} x_4^{5k+1} + \beta_{5k+2} x_4^{5k+2} + \beta_{5k+3} x_4^{5k+3} + \beta_{5k+4} x_4^{5k+4} + \cdots + \beta_{124} x_4^{124}$$

l'écriture de β dans la base bivariée est :

$$\beta_0 + \beta_1 x_4 + \cdots + x_3^k(\beta_{5k} + \beta_{5k+1} x_4 + \beta_{5k+2} x_4^2 + \beta_{5k+3} x_4^3 + \beta_{5k+4} x_4^4) + \cdots + \beta_{124} x_3^{24} x_4^4.$$

On voit ici que $\beta \notin \mathsf{F}_3$ et donc on ne peut le faire descendre dans la tour d'extension mais seulement s'arrêter à cette écriture dans la base bivariée.

3.3 Opérations dans la tour d'extension ℓ-adique

Inversion d'un élément dans le cas $\ell = 2$

L'inversion d'un élément peut être effectuée dans une base univariée en utilisant l'algorithme d'Euclide étendu. Le coût d'inversion d'un élément de F_k serait de $O(\mathsf{M}(\ell^{k-1}d_1)\log(\ell^{k-1}d_1))$ opérations sur $\mathbb{F}_q$ en utilisant les résultats de [vzGG03, ch.11]. Une autre technique plus avantageuse est préférée uniquement pour le cas $\ell = 2$ dans [DS15], soit $G(x_k)$ un élément inversible de F_k alors en écrivant $G(x_k) = G_0(x_{k-1}) + x_k G_1(x_{k-1})$ on obtient :

$$\begin{aligned} \frac{1}{G(x_k)} &= \frac{1}{G_0(x_{k-1}) + x_k G_1(x_{k-1})} \\ &= \frac{G_0(x_{k-1}) - x_k G_1(x_{k-1})}{G_0(x_{k-1})^2 - x_{k-1} G_1(x_{k-1})^2} \end{aligned}$$

Le coût d'une inversion d'un élément de F_k est le coût d'une addition, de la multiplication d'éléments de F_k ainsi que le coût d'une inversion d'éléments dans F_{k-1}, on a donc affaire à un algorithme récursif de coût $T(k) = T(k-1) + O(\mathsf{M}(\ell^{k-1}d_1))$; avec la super linéarité de M on obtient un coût de calcul de $O(\mathsf{M}(\ell^{k-1})d_1)$ opérations sur $\mathbb{F}_q$. Pour les tours dyadiques on a $d_1 \mid 2$ dés lors on peut exprimer le coût comme $O(\mathsf{M}(\ell^{k-1}))$. La complexité de l'inversion est donc de $O(\mathsf{M}(\ell^{k-1}))$ opérations sur $\mathbb{F}_q$ dans le cas où l'on considère une extension dyadique.

Calcul du Frobenius

Cette opération est très importante pour déterminer des ensembles spécifiques de points d'une courbe elliptique (voir chapitre 5), c'est pourquoi on s'attache ici à montrer que l'on peut effectuer cette opération à un coût raisonnable. Le résultat ici est une généralisation de [DS15].

Théorème 3.6. *Soit $\mathbb{F}_q, \mathsf{F}_1, \mathsf{F}_2, \cdots \mathsf{F}_n$ une tour d'extensions ℓ-adiques Soit a un élément de F_i pour tout entier j le calcul de la puissance $|\mathsf{F}_j|$ de a coûte $O(\ell^{i-1}M(d_1))$ opérations sur $\mathbb{F}_q$ après un pré-calcul de $O(M(d_1)\log(|\mathsf{F}_1|))$ opérations sur $\mathbb{F}_q$ auquel il faut ajouter un calcul booléen de $O(\log(\ell^j)\log(\ell^{i-1}|\mathsf{F}_1|))$.*

Démonstration. Sans perte de généralité on peut supposer que l'on a $j < i$, le résultat étant sinon a lui-même. Notons $s = |\mathsf{F}_j|$ et rappelons que $[\mathsf{F}_i : \mathsf{F}_1] = \ell^{i-1}$. Soit x_i l'image de x dans $\mathsf{F}_i = \mathsf{F}_1[x]/P_i(x)$, on a en particulier $x_i^{\ell^{i-1}} = x_1$.

La première étape est de calculer $y = x_i^s$. En écrivant $s = u\ell^{i-1} + v$ avec $0 \leqslant v < \ell^{i-1}$ on a alors $y = x_1^{u \bmod |\mathsf{F}_1|-1} x_i^v$. Une méthode rapide est préconisée pour le calcul de $u \bmod |\mathsf{F}_1|-1$ et v. Dans un premier temps il faut calculer $\rho = s \bmod \ell^{i-1}(|\mathsf{F}_1| - 1)$ à l'aide de l'exponentiation rapide puis $u \bmod |\mathsf{F}_1| - 1$ et v sont obtenus comme le quotient et le reste de la division euclidienne de ρ par ℓ^{i-1}. Le coût booléen d'une telle opération est de $O(\log(\ell^j)\log(\ell^{i-1}|\mathsf{F}_1|))$. L'opération majeure étant l'exponentiation avec un exposant de taille $O(\ell^j \log(|\mathsf{F}_1|))$ modulo un entier de taille $O(\log(\ell^{i-1}|\mathsf{F}_1|))$, le calcul de $x_1^{u \bmod |\mathsf{F}_1|-1}$ se fait en utilisant $O(M(d_1)d_1\log(q))$ opérations sur $\mathbb{F}_q$. On conserve ce résultat sous la forme d'un monôme dans $\mathsf{F}_1[x_i]$.

Dans la tour d'extensions ℓ-adiques les éléments de la tour peuvent être représentés sous forme $G(x_k)$ avec G un polynôme de degré d à coefficients dans F_1, or un élément $G(x_k)$ peut aussi être représenté sous forme $H(x_k)$ avec H un polynôme de degré $d_1\ell^{i-1}$ à coefficients dans $\mathbb{F}_q$. À travers le calcul du Frobenius on va expliciter ces changements de représentation. Soit a représenté sous la forme d'un polynôme en x_i de degré inférieur ou égal à $[\mathsf{F}_i : \mathbb{F}_q]$:

$$a_0^* + a_1^* x_i + \cdots + a_{d_1\ell^{i-1}-1}^* x_i^{d_1\ell^{i-1}-1}$$

avec les $a_i^* \in \mathbb{F}_q$. On réécrit a sous la forme :

$$a_0 + a_1 x_i + \cdots + a_{\ell^{i-1}-1} x_i^{\ell^{i-1}-1}$$

avec les $a_w = a_w^* + \sum_{k=1}^{\lfloor d_1\ell^{i-1}-1/d \rfloor} a_{w+dk}^* x_1^k \in \mathsf{F}_1$ pour w appartenant à $[0; \ell^{i-1} - 1]$. Pour obtenir cette réécriture on s'est servi du fait que pour t appartenant à $[1; d_1\ell^{i-1} - 1]$ tel que $t = \ell^{i-1}u_t + v_t$ avec $0 \leqslant v_t < \ell^{i-1}$ on a $x_w^t =$

$x_1^{u_t \bmod |\mathsf{F}_1|-1} x_w^{v_t}$. Ainsi cette opération est seulement un réarrangement des coefficients de a.

On écrit a^s sous la forme :

$$a_0 + a_1 y + a_2 y^2 + \cdots + a_{\ell^i-1} y^{\ell^{i-1}-1}$$

On calcule alors a^s par la méthode de Horner. Les puissances y^k étant des monômes dans $F_1[x_i]$, on calcule chacune des puissances successives à l'aide de la précédente en $O(M(d_1))$ opérations sur $\mathbb{F}_q$. On a alors un coût total de $O(\ell^{i-1}M(d_1)))$ opérations dans $\mathbb{F}_q$. En réarrangeant les monômes $a_k y^k$ on obtient un polynôme en (x_1, x_i) de degré $(d_1 - 1, \ell^{i-1} - 1)$, on réécrit alors a^s sous la forme $G(x_i)$ avec G un polynôme à coefficients dans $\mathbb{F}_q$ de degré $d_1\ell^{i-1}$ à l'aide du changement de représentation inverse de celui effectué précédemment. En effet a^s est représenté sous la forme :

$$b_0 + b_1 x_i + b_2 x_i^2 + \cdots + b_{\ell^{i-1}-1} x_i^{\ell^{i-1}-1}$$

avec b_k un élément de F_1 pour tout k. En remarquant que

$$\begin{aligned} b_k =& b_{k,0} + b_{k,1}x_1 + \cdots + b_{k,d_1-1}x_1^{d_1-1} \\ =& b_{k,0} + b_{k,1}x_i^{\ell^{i-1}} + b_{k,2}x_i^{2\times\ell^{i-1}} + \cdots + b_{k,d_1-1}x_i^{(d_1-1)\times\ell^{i-1}} \end{aligned}$$

avec $b_{k,i}$ un élément de $\mathbb{F}_q$ pour tous k, i, on représente a^s sous la forme :

$$b_0^* + b_1^* x_i + b_2^* x_i^2 + \cdots + b_{d_1\ell^{i-1}-1}^* x_i^{d_1\ell^{i-1}-1}$$

en utilisant la transformation $b_k^* = b_{u,v}$ pour tous k, u, v tels que $k = ud + v$ avec $0 \leqslant v < d$. □

Maintenant que le coût du Frobenius a été établi nous allons voir une autre opération nécessaire pour le calcul d'isogénies dans le cas de tours dyadiques, le calcul de racines carrées.

Calcul d'une racine carrée

Les résultats présentés sont issus d'idées développées dans [DS14] et sont adaptés à la construction de tour d'extensions ℓ-adiques présentée ici où le coût du Frobenius est très faible. Le résultat à retenir est celui pour les extensions dyadiques du fait de son usage pratique même si une généralisation est présentée.

Proposition 3.7. Soit $\mathbb{F}_q, \mathsf{F}_1, \cdots \mathsf{F}_k$ une tour d'extensions ℓ-adiques. Soit δ un carré non nul de F_k, alors une racine carrée γ de δ est calculée avec une complexité de $O(M(\ell^{k-1}d_1)\log(\ell^{k-1}q))$ opérations sur $\mathbb{F}_q$.

Démonstration. Soit δ un carré non nul de F_k ayant pour racine carrée γ. Soit β dans F_1 défini de la manière suivante :

$$\beta = T_{\mathsf{F}_k/\mathsf{F}_1}(\gamma) = \sum_{i=0}^{\ell^{k-1}-1} \gamma^{|\mathsf{F}_1|^i} = \gamma(1 + \gamma^{|\mathsf{F}_1|-1} + \cdots + \gamma^{|\mathsf{F}_1|^{\ell^{k-1}-1}-1}) \tag{3.4}$$

$$= \gamma(1 + \delta^{(|\mathsf{F}_1|-1)/2} + \cdots + \delta^{(|\mathsf{F}_0|^{\ell^{k-1}-1}-1)/2}) \tag{3.5}$$

$$= \gamma\eta \tag{3.6}$$

en posant

$$\eta = 1 + \delta^{(|\mathsf{F}_0|-1)/2} + \cdots + \delta^{(|\mathsf{F}_0|^{\ell^{k-1}-1}-1)/2}.$$

Maintenant si l'on met au carré l'équation (3.4) on obtient alors l'équation suivante dans F_1 :

$$\beta^2 = \delta\eta^2.$$

Dés lors si η est connu, β peut être déduit depuis cette équation et γ calculé car

$$\gamma = \beta\eta^{-1}.$$

Sans perte de généralité on peut supposer que l'on a $\eta \neq 0$, si ce n'est pas le cas alors on peut remplacer δ par δc^2 avec c choisi aléatoirement parmi les inversibles de F_k. $O(1)$ essais sont nécessaires en moyenne pour obtenir $T_{\mathsf{F}_k/\mathsf{F}_1}(\gamma c) \neq 0$. En effet il y a $|\mathsf{F}_1|^{\ell^{k-1}}/|\mathsf{F}_1|$ valeurs de c pour lesquelles on a $T_{\mathsf{F}_k/\mathsf{F}_1}(\gamma c) = 0$ ainsi la probabilité d'avoir $T_{\mathsf{F}_k/\mathsf{F}_1}(\gamma c) \neq 0$ est de $1 - (|\mathsf{F}_1|^{\ell^{k-1}}/|\mathsf{F}_1|)/(|\mathsf{F}_1|^{\ell^{k-1}}) = 1 - 1/|\mathsf{F}_1| > 1/2$.

Le coût de calcul de β est de $O(M(d_1)\log(q) + C(d_1)\log(d_1))$ opérations en moyenne sur $\mathbb{F}_q$ avec $C(n) = O(n^{1.67})$ d'après [DS14]. Ainsi seul le coût du calcul de η est crucial pour obtenir une complexité satisfaisante.

Soit λ un élément de F_k défini par $\lambda = \delta^{(|\mathsf{F}_1|-1)/2}$ on a alors la relation suivante :

$$\eta = 1 + \lambda + \lambda^{1+|\mathsf{F}_1|} + \lambda^{1+|\mathsf{F}_1|+|\mathsf{F}_1|^2} + \cdots + \lambda^{1+|\mathsf{F}_1|+|\mathsf{F}_1|^2+\cdots+|\mathsf{F}_1|^{\ell^{k-1}-2}}.$$

Pour $m \geqslant 0$ on définit :

$$\zeta_m = \lambda^{|\mathsf{F}_1|+|\mathsf{F}_1|^2+\cdots+|\mathsf{F}_1|^m} \tag{3.7}$$

que l'on peut construire par récurrence :

$$\zeta_1 = \gamma^{|\mathsf{F}_1|} \quad \text{et} \quad \zeta_m = \begin{cases} \zeta_{m/2}\zeta_{m/2}\zeta_{m/2}^{|\mathsf{F}_1|^{m/2}} & \text{si m est pair,} \\ \zeta_1\zeta_{m-1}^{|\mathsf{F}_1|} & \text{si m est impair.} \end{cases}$$

On définit aussi

$$\varepsilon_m = \lambda^{|\mathsf{F}_1|} + \lambda^{|\mathsf{F}_1|+|\mathsf{F}_1|^2} + \cdots + \lambda^{|\mathsf{F}_1|+|\mathsf{F}_1|^2+\cdots+|\mathsf{F}_1|^m}$$

on a alors une relation de récurrence pour le calcul de ε :

$$\varepsilon_1 = \lambda^{|\mathsf{F}_1|} \quad \text{et} \quad \varepsilon_m = \begin{cases} \varepsilon_{m/2} + \zeta_{m/2}\varepsilon_{m/2}^{|\mathsf{F}_1|^{m/2}} \text{si m est pair,} \\ \varepsilon_{m-1} + \zeta_m \text{si m est impair.} \end{cases} \tag{3.8}$$

Ainsi on obtient $\eta = 1 + \lambda + \lambda\varepsilon_{\ell^k-2}$.

Le calcul de λ a un coût de $O(M(\ell^{k-1}d_1)\log(q))$ opérations sur $\mathbb{F}_q$. Le calcul de ε_1 et ζ_1 se fait quant à lui à l'aide de $O(1)$ fois le Frobenius. Calculons alors par récurrence le coût total, en supposant que le calcul de ε_m et ζ_m ait déjà été effectué. En utilisant les équations (3.8) ε_{2m} et ζ_{2m} ou ε_{2m+1} et ζ_{2m+1} peuvent être calculés en utilisant $O(1)$ Frobenius et $O(1)$ multiplications sur F_k. Ainsi ε_n et $\eta = 1 + \lambda + \lambda\varepsilon_{n-2}$ sont calculés en $O(M(\ell^{k-1}d_1)\log(\ell^{k-1}) + M(\ell^{k-1}d_1)\log(q)) = O(M(\ell^{k-1}d_1)\log(\ell^{k-1}q))$ opérations sur $\mathbb{F}_q$. Le coût de calcul de γ et β étant négligeables par rapport à celui de η, on a alors un coût total de $O(M(\ell^{k-1}d_1)\log(\ell^{k-1}q))$ opérations sur $\mathbb{F}_q$.

□

Opérations	Coûts
addition/soustraction	$O(\ell^{k-1}d_1)$
multiplication	$\mathsf{M}(\ell^{k-1}d_1) + O(\ell^{k-1}d_1)$
division	$O(\mathsf{M}(\ell^{k-1}d_1)\log(\ell^{k-1})d_1)$
Frobenius	$O(\ell^{k-1}\mathsf{M}(d_1) + d_1\mathsf{M}(d_1)\log(q))$
racine carrée	$O(\mathsf{M}(\ell^{k-1}d_1)\log(\ell^{k-1}q))$(en moyenne)
racine ℓ-ième	$\mathsf{R}(i) = O(\ell^i\mathsf{M}(\ell^{i+1})\log(\ell)\log(\ell q))$

FIGURE 3.1 – Coûts des opérations dans F_k exprimées en nombre d'opérations sur $\mathbb{F}_q$

Il est à noter que en pratique pour le calcul de racine carrée de δ on peut parfois être amené à considérer un élément de F_k qui n'est pas un carré. Cela est testé en pratique sur β qui est un résidu quadratique si et seulement si δ l'est. Une astuce consiste alors à multiplier δ par l'élément générateur x_k du corps F_k afin de multiplier cet élément par un résidu non quadratique, on injecte alors δx_k dans F_{k+1}. On applique l'algorithme vu précédemment, le résultat obtenu est alors divisé par x_{k+1} pour obtenir la racine carrée de δ souhaitée.

On propose les résultats suivant concernant les opérations sur les polynômes à coefficients dans la tour d'extensions ℓ-adiques :

Proposition 3.8. La multiplication et la division euclidienne de polynômes de degré au plus d appartenant à $\mathsf{F}_i[x]$ coûte $O(\mathsf{M}(d\ell^{i+1}))$ opérations sur $\mathbb{F}_q$.

Démonstration. On utilise la substitution de Kronecker déjà apparue dans [vzGS92, Lemma 2.2], une description est tout de même faite dans cette preuve. Soit f un polynôme de $\mathsf{F}_i[x]$ de degré d alors on peut représenter f comme un polynôme de $\mathbb{F}_q[x, y]$, avec $\mathsf{F}_i = \mathbb{F}_q[y]$, en utilisant la substitution de Kronecker $x \to y^{2\ell^i d_0 - 1}$. f est alors représenté comme un polynôme univarié de degré au plus $2\ell^{i+1}d$, d'où le résultat. □

Notation 3.9. On note $\mathsf{R}(i)$ une borne sur le coût moyen du calcul de racine d'un polynôme de degré ℓ à coefficients dans F_i.

Les coûts des différentes opérations dans de telles tours d'extensions ℓ-adiques sont résumés dans le tableau 3.1. On a $\mathsf{R}(i) = O(\ell^i\mathsf{M}(\ell^{i+1})\log(\ell)\log(\ell q))$ en utilisant la variante de l'algorithme de Cantor-Zassenhaus décrite dans [vzGG03, Chapter 14.5]. Il est à noter que pour le calcul d'une racine le coût est un coût en moyenne, cela est dû à une partie de l'algorithme qui est de type non déterministe (Las Vegas).

Une implantation de construction de tours dyadiques et des opérations du Frobenius et du calcul de racine carrée ont été réalisé en SageMath le code est disponible à cette adresse : `https://github.com/Hugounenq-Cyril/Two_curves_on_a_volcano/blob/master/Code/extension_corps.sage`.

3.4 Calcul de polynômes d'interpolations

Cette section reprend les travaux effectués en collaboration avec Luca De Feo, Jérome Plut et Éric Schost qui ont fait l'objet d'une publication [DFHPS16], ces travaux s'inspirent notamment de ceux de [DF10, 8.7] qui utilise des idées

originales de [EM03] et qui ont fait l'objet d'une brève présentation dans la sous-section 2.5.2.

Dans cette section on s'intéresse au calcul d'un polynôme d'interpolation défini sur $\mathbb{F}_q$ entre deux éléments $u, v \in \mathsf{F}_i$ avec F_i un corps de la tour d'extensions ℓ-adiques définie dans la définition 3.1.

On va donc présenter ici l'algorithme utilisé dans [DF10, 8.7] et l'adapter à notre contexte pour l'analyse de complexité.

Le contexte de notre travail est le suivant, soit deux éléments $v, w \in F_n \setminus F_{n-1}$ on veut alors calculer le polynôme $A \in \mathbb{F}_q[x]$ tel que :

$$A(v) = w. \tag{3.9}$$

En particulier si l'on note T le polynôme minimal de v il est clair que $A(v) + T(v) = w$, on va donc chercher à calculer le représentant minimal de A dans la classe de polynômes $\mathbb{F}_q[x]/\langle T\rangle$. Pour un polynôme A solution de 3.9 pour tout $\pi \in \mathsf{Gal}(\mathsf{F}_n : \mathbb{F}_q) : A(\pi(v)) = \pi(w)$. De même tout polynôme interpolant $\pi(v)$ sur $\pi(w)$ pour tout $\pi \in \mathsf{Gal}(\mathsf{F}_n : \mathbb{F}_q)$ est invariant sous l'action de tout élément de de $\mathsf{Gal}(\mathsf{F}_n : \mathbb{F}_q)$ et est donc défini dans $\mathbb{F}_q$. On peut donc construire un tel polynôme A par interpolation.

La première étape est donc de calculer T, on pourrait faire cela simplement à l'aide d'un arbre de produit binaire mais comme abordé dans dans la sous section 2.5.2 qui fait référence au travail de [DF10, 8.7] on utilise un arbre de produit tronqué qui prend avantage du faible coût du Frobenius.

Ainsi on note $T^{(0)} = (x - v)$, σ_i l'application qui applique à tous les coefficients d'un polynôme à coefficients dans F_{n-i} l'action d'un élément générateur de $\mathsf{Gal}(\mathsf{F}_{n-i} : \mathsf{F}_{n-i-1})$. En supposant que l'on connaisse un $T^{(i)}$ pour $i < n$ de degré ℓ^i à coefficients dans F_{n-i} alors pour $j \in [0; \ell-1]$ on définit $T^{(i,j)} = \sigma_i^j(T^{(i)})$, et l'on pose :

$$T^{(i+1)} = \prod_{j=0}^{b} T^{(i,j)} \qquad \text{avec} \qquad b = \begin{cases} \ell - 1 & \text{si } i < n-1, \\ d_1 - 1 & \text{sinon.} \end{cases}$$

Il est alors évident que $T^{(i+1)}$ est le polynôme minimal de v sur F_{n-i-1}.

Lemme 3.10. Le coût de calcul de $T = T^{(n)}$ est de $O(n\mathsf{M}(\ell^{n+1})\log(\ell))$ opérations dans $\mathbb{F}_q$.

Démonstration. À l'étape i, à partir de la connaissance de $T^{(i)}$ on calcule tous les $T^{(i,j)}$ en utilisant le théorème 3.6. Le coût du Frobenius pour un polynôme $T^{(i,j)}$ est de $O(\ell^i \ell^{n-i-1}\mathsf{M}(\ell))$ opérations, *i.e.* $O(\ell^n \mathsf{M}(\ell))$ pour chacun des $O(\ell)$ calculs. À partir des $T^{(i,j)}$ on calcule $T^{(i+1)}$ en utilisant un arbre de sous-produits comme décrit dans [vzGG03, Lemma 10.4]. Le polynôme résultant de cette opération est de degré $O(\ell^{i+1})$ et a ses coefficients définis dans F_{n-i}, le coût total est donc $O(\mathsf{M}(\ell^{n+1})\log(\ell))$ opérations sur $\mathbb{F}_q$. Une fois que $T^{(i+1)}$ a été calculé de cette manière, on opère une *descente* sur ses coefficients dans F_{n-i-1} à l'aide d'une réécriture qui n'a aucun coût algébrique. On additionne ces coûts pour tous les i pour obtenir le résultat énoncé. □

Il reste maintenant à calculer le polynôme d'interpolation. Supposons que l'on ait calculé un tel polynôme d'interpolation $A^{(i)}$ défini sur F_{n-i}. On calcule alors le polynôme $L \in \mathsf{F}_{n-i}[x]/\langle T^{(i)}\rangle$ tel que

$$L = \sigma(A^{(i)}) \bmod \sigma(T^{(i)}) \quad \text{pour tout} \quad \sigma \in \mathsf{Gal}(\mathsf{F}_{n-i} : \mathsf{F}_{n-i-1}). \tag{3.10}$$

Ce polynôme L étant invariant sous l'action du groupe de Galois : $\mathsf{Gal}(\mathsf{F}_{n-i} : \mathsf{F}_{n-i-1})$, il est alors défini dans F_{n-i-1}. Par 3.10 on a bien $L(v) = A^{(i)}(v) = w$, ainsi on a $L = A^{(i+1)}$.

Cette discussion nous permet donc de définir la suite de polynômes $A^{(i)}$ définie pour $i \in [0, n]$, $A^{(0)} = w/T'(v)$. En supposant que l'on connaisse un $A^{(i)}$ pour $i < n$ de degré inférieur à ℓ^i à coefficients dans F_{n-i} alors pour $j \in [0; \ell-1]$ on définit $A^{(i,j)} = \sigma_i^j(A^{(i)})$, et l'on pose :

$$A^{(i+1)} = \sum_{j=0}^{b} A^{(i,j)} \frac{T^{(i+1)}}{T^{(i,j)}} \qquad \text{avec} \qquad b = \begin{cases} \ell - 1 & \text{si } i < n-1, \\ d_1 - 1 & \text{sinon.} \end{cases}$$

$A^{(i)}$ est alors le polynôme d'interpolation défini par 3.9 à coefficients dans F_{n-i}.

Proposition 3.11. Soient $v, w \in F_n \setminus F_{n-1}$, le coût de calcul du polynôme minimal $T \in \mathbb{F}_q[x]$ de v et le polynôme d'interpolation $A \in \mathbb{F}_q[x]$ tel que $A(v) = w$ est $O(n\mathsf{M}(\ell^{n+1})\log(\ell))$ opérations dans $\mathbb{F}_q$.

Démonstration. Une fois que les polynômes $T^{(i)}$ ont été calculé, on doit tout d'abord calculer $T'(v)$. Cette opération est faite à l'aide de calculs de restes de division Euclidiennes, en effet $T'(v) = (((T' \bmod T^{(n)}) \bmod T^{(n-1)}) \cdots \bmod T^{(0)})$. À l'étape $n - i$, on calcule la division Euclidienne d'un polynôme de degré $O(\ell^{n-i+1})$ par un polynôme de degré $O(\ell^{n-i})$ dans $F_i[x]$. Le coût de chaque division est alors de $O(\mathsf{M}(\ell^{n+1}))$ par la proposition 3.8 ce qui donne un coût total de $O(n\mathsf{M}(\ell^{n+1}))$ opérations. Le calcul de $w' = w/T'(v)$ est de $O(\mathsf{M}(\ell^n)\log(\ell^n))$ opérations.

À chaque étape i, les polynômes $A^{(i,j)}$ sont calculés à un coût de $O(\ell^n\mathsf{M}(\ell))$ opérations, comme dans la preuve du lemme 3.10. Le calcul de $L^{(i+1)}$ utilise le même arbre de produit que celui utilisé pour $T^{(i)}$, utilisant $O(\log \ell)$ additions, multiplications et divisions de polynômes de degré $O(\ell^{i+1})$ à coefficients dans F_{n-i}, pour un coût total de $O(\mathsf{M}(\ell^{n+1})\log(\ell))$. En additionnant pour tous les i on obtient la complexité annoncée. □

Ce résultat est à comparer aux algorithmes d'interpolations rapides tel que celui présenté dans [vzGG03, Chapter 10.2] il donnerait un temps de calcul de $O\big(n\mathsf{M}(\ell^{2n})\log(\ell)\big)$ opérations sur $\mathbb{F}_q$.

On énonce un problème plus général de calcul de polynôme d'interpolation à l'aide de plusieurs couples de points de F_n.

Proposition 3.12. Soit $(v_1, w_1), \ldots, (v_s, w_s)$ des paires d'éléments de F_n, t_i le degré des polynômes minimaux de v_i, et l'on note $t = \sum t_i$. Les polynômes

— $T \in \mathbb{F}_q[x]$ de degré t tel que $T(v_i) = 0$ pour tout i,

— $A \in \mathbb{F}_q[x]$ de degré inférieur à t tel que $A(v_i) = w_i$ pour tout i

sont calculés avec un coût de $O\big(\mathsf{M}(t)\log(s) + n\mathsf{M}(\ell^2 t)\log(\ell)\big)$ opérations dans $\mathbb{F}_q$.

Démonstration. Le polynôme T est le produit de tous les polynômes minimaux T_i. Soit $n_i = v_\ell(t_i)$, de telle sorte que $v_i, w_i \in F_{n_i+1} \setminus F_{n_i}$, et $\ell^{n_i} \leqslant t_i < \ell^{n_i+1}$, on effectue une *descente* sur (v_i, w_i) pour les écrire comme des éléments de F_{n_i+1}, cette opération étant juste une réécriture elle a un coût algébrique nul. On calcule les T_i à l'aide de $O(n\mathsf{M}(\ell^{n_i+2})\log(\ell))$ opérations par le lemme 3.10. En bornant ℓ^{n_i} par t_i, en additionnant cela pour tout i, et en utilisant la superlinéarité de M on obtient un coût total de $O(n\mathsf{M}(\ell^2 t)\log(\ell))$ opérations. De

la même manière on calcule les polynômes A_i tels que $A_i(v_i) = w_i$ au même coût. On ordonne ensuite les T_i dans une arbre de sous-produit binaire et on les multiplie entre eux. Un arbre équilibré, pas nécessairement optimal, a une profondeur de $O(\log(s))$ et nécessite $O(\mathsf{M}(t))$ opérations par niveau. Ainsi le coût de calcul de T est borné par $O(\mathsf{M}(t)\log(s))$ opérations sur $\mathbb{F}_q$.

Enfin, en utilisant la même structure d'arbre de sous-produit on applique le théorème des restes chinois proposé dans [vzGG03, Chapter 10] pour calculer A au coût de $O(\mathsf{M}(t)\log(s))$ opérations sur $\mathbb{F}_q$. □

Chapitre 4

Volcans d'isogénies

Les deux documents à citer pour cette section sont [Koh96] qui a introduit les graphes d'isogénie et [Fou01] qui a développé ces idées pour donner une structure à ces graphes.

4.1 Anneau des endomorphismes

Dans cette section on va aborder les anneaux des endomorphismes, car c'est cet objet qu'a étudié Kohel dans sa thèse [Koh96] qui a permis ensuite de définir les volcans des l-isogénies. Faisons tout d'abord quelques rappels sur les ordres d'un corps de nombres quadratique imaginaire car, comme vu précédemment (proposition 1.35), ceux-ci correspondent à isomorphisme près aux anneaux des endomorphismes de courbes elliptiques ordinaires définies sur un corps fini.

4.1.1 Rappel sur les ordres d'un corps de nombres quadratique

Soit K un corps de nombres quadratique, alors il existe un entier N sans facteur carré tel que l'on peut écrire $K = \mathbb{Q}[\sqrt{N}]$. On définit alors alors le discriminant de K :

Définition 4.1. Soit $K = \mathbb{Q}[\sqrt{N}]$, on définit le discriminant d_K de K de la façon suivante :

$$d_K = \begin{cases} N & \text{si } N \equiv 1 \bmod 4, \\ 4N & \text{sinon.} \end{cases}$$

Définition 4.2. Un corps de nombres quadratique $K = \mathbb{Q}[\sqrt{N}]$ est dit imaginaire si $N < 0$.

On va dés lors se restreindre à ce cas.

Définition 4.3. Soit K un corps de nombres quadratique imaginaire, on note $\mathcal{O}_K$ l'ensemble des entiers algébriques de K c'est à dire les $\alpha \in K$ qui sont solution de polynômes unitaires à coefficients dans les entiers relatifs. $\mathcal{O}_K$ est aussi appelé l'anneau des entiers de K.

Proposition 4.4. Soit K un corps de nombres quadratique imaginaire, d_K son discriminant alors :

$$\mathcal{O}_K = \mathbb{Z}\left[\frac{d_K + \sqrt{d_K}}{2}\right]$$

Démonstration. Voir [Cox89, exercise 5.7]. □

Nous définissons alors les ensembles sur K avec lesquels nous allons travailler :

Définition 4.5. Un ordre $\mathcal{O}$ d'un corps de nombres quadratique K est un sous-ensemble vérifiant les conditions suivantes :

1. $\mathcal{O}$ est un sous-anneau de K,
2. $\mathcal{O}$ est $\mathbb{Z}$-module libre de rang 2.

Le résultat suivant nous permet de définir le plus grand ordre au sens de l'inclusion.

Proposition 4.6. Soit K un corps de nombres quadratique imaginaire, $\mathcal{O}_K$ l'anneau des entiers de K alors $\mathcal{O}_K$ est l'ordre maximal de K.

Démonstration. Soit $\mathcal{O}$ un ordre de K et soit $\alpha \in \mathcal{O}$. Comme $\mathcal{O}$ est sous-anneau de K, on a $\alpha \in K$. $\mathcal{O}$ étant un $\mathbb{Z}$-module libre de rang 2 alors α est un entier algébrique et donc $\alpha \in \mathcal{O}_K$. □

Remarque 4.7. On pourra aussi noter $\mathcal{O}_K$ de la façon suivante

$$\mathcal{O}_K = [1, \omega_K]$$

avec $\omega_K = \frac{d_K + \sqrt{d_K}}{2}$, on met ainsi en avant la base de $\mathbb{Z}$-module : $1, \omega_K$ de $\mathcal{O}_K$.

Cette notation nous permet alors d'exprimer les indices des ordres $\mathcal{O}$ par rapport à $\mathcal{O}_K$ comme le spécifie le lemme suivant :

Lemme 4.8. Soit $\mathcal{O}$ un ordre dans un corps de nombres quadratique imaginaire K de discriminant d_K, alors $\mathcal{O}$ a un indice fini dans $\mathcal{O}_K$. De plus si l'on note : $f = [\mathcal{O}_K : \mathcal{O}]$, alors

$$\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K = [1, f\omega_K].$$

Démonstration. voir [Cox89, lemma 7.7.2]. □

La définition suivante nous permet de nommer les indices dans ce contexte :

Définition 4.9. Soit $\mathcal{O}$ un ordre du corps de nombres quadratique imaginaire K, l'indice $f = [\mathcal{O}_K : \mathcal{O}]$ est appelé le conducteur de $\mathcal{O}$.

Remarque 4.10. À l'aide des conducteurs on peut définir une relation d'ordre sur les ordres, en effet si on a $m \mid n$ alors on a l'ordre $n\mathcal{O}_K \subset m\mathcal{O}_K$.

C'est cette idée que l'on va retrouver dans les volcans des l-isogénies en essayant de donner une structure aux relations entre les différents ordres isomorphes aux anneaux des endomorphismes.

On définit un autre invariant pour un ordre, son discriminant.

Définition 4.11. Soit $\alpha \mapsto \overline{\alpha}$ l'automorphisme non-trivial d'un corps de nombres quadratique imaginaire K, soit $\mathcal{O}$ un ordre de K avec $\mathcal{O} = [\alpha, \beta]$, alors le discriminant de $\mathcal{O}$ est le nombre

$$D = \left(\det \begin{pmatrix} \alpha & \beta \\ \overline{\alpha} & \overline{\beta} \end{pmatrix}\right)^2.$$

On rappelle que le discriminant de $\mathcal{O}_K$ est noté d_K.

Le discriminant est un invariant de la base choisie, en prenant la base $[1, f\omega_K]$ de $\mathcal{O}$, on a :

$$D = f^2 d_K.$$

Remarque 4.12. Soit E une courbe elliptique dont l'ordre, associé à isomorphisme près à son anneau des endomorphismes, est $\mathbb{Z}[\pi]$. Alors de par l'isomorphisme de groupes entre le groupe de classes de formes (quadratiques) et le groupes de classes d'idéaux (voir [Cox89, Theorem 7.7] ou [Coh96, Theorem 5.2.8]) on peut définir le discriminant d_π de l'ordre $\mathbb{Z}[\pi]$ comme étant le discriminant du polynôme minimal du Frobenius : $x^2 - t_\pi + 4q$, ainsi $d_\pi = t_\pi^2 - 4q$.

De même pour $\mathcal{O} = [1, \omega_K f]$, le polynôme minimal de $f\omega_K$ est :

$$x^2 - f d_K x + f^2 \frac{d_K(d_K - 1)}{4} = 0.$$

On retrouve bien que le discriminant de $\mathcal{O}$ est $f^2 d_K$.

4.1.2 Anneau des endomorphismes de courbes elliptiques ordinaires

Dans cette sous-section on va se concentrer sur les anneaux des endomorphismes de courbes elliptiques ordinaires définies sur un corps fini qui sont, comme vu dans la proposition 1.35, isomorphes à des ordres dans un corps de nombres quadratique imaginaire. On va voir en détail les relations possibles et les structures qu'ont les anneaux des endomorphismes dans un tel contexte.

La première remarque à faire c'est que pour toute courbe elliptique ordinaire définie sur un corps fini pour $\mathcal{O}$ l'ordre associé à isomorphisme près à $\mathrm{End}(E)$ on a :

$$\mathbb{Z}[\pi] \subset \mathcal{O} \subset \mathcal{O}_K.$$

Ainsi pour tout ordre associé à un anneau d'endomorphisme on a un ordre minimal au sens de l'inclusion celui qui contient toutes les multiplications scalaires et l'endomorphisme de Frobenius.

Remarque 4.13. On va noter désormais $\mathcal{O}$(resp. $\mathcal{O}'$) pour l'ordre défini à isomorphisme près associé à $\mathrm{End}(E)$ (resp. $\mathrm{End}(E')$).

Lemme 4.14. Soient E, E' deux courbes elliptiques ordinaires, $\phi : E \mapsto E'$ une isogénie de degré ℓ alors :

1. soit $[\mathcal{O} : \mathcal{O}'] = \ell$,
2. soit $[\mathcal{O} : \mathcal{O}'] = 1$,
3. soit $[\mathcal{O}' : \mathcal{O}] = \ell$.

Démonstration. Voir [Koh96, Proposition 21]. □

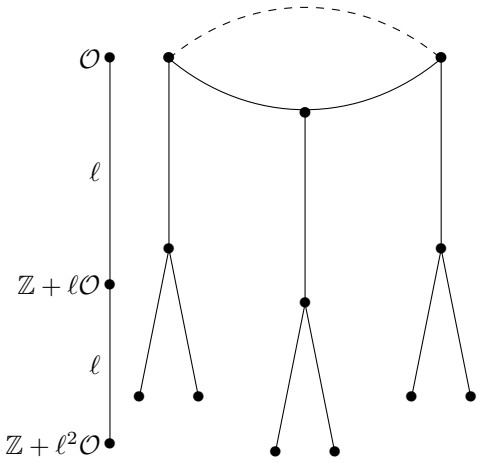


FIGURE 4.1 – Représentation d'un volcan de 2-isogénies avec les différents ordres.

Définition 4.15. Soient E, E' deux courbes elliptiques ordinaires, $\phi : E \mapsto E'$ une ℓ-isogénie alors $\phi : E \mapsto E'$ est dite :

1. montante si $[\mathcal{O}' : \mathcal{O}] = \ell$,
2. descendante si $[\mathcal{O} : \mathcal{O}'] = \ell$,
3. horizontale si $[\mathcal{O}' : \mathcal{O}] = 1$.

On fait alors la remarque suivante sur les duales des isogénies :

Remarque 4.16. Soit $\phi : E \mapsto E'$ une isogénie et sa duale $\widehat{\phi}$. Alors :

1. ϕ est une isogénie montante si et seulement si $\widehat{\phi}$ est une isogénie descendante,
2. ϕ est une isogénie horizontale si et seulement si $\widehat{\phi}$ est une isogénie horizontale.

Sur la figure 4.1 est représenté un volcan d'isogénies, les points représentent les courbes elliptiques définies à isomorphisme près, les traits reliant les points représentent les ℓ-isogénies qui lient les courbes elliptiques. On observe que le volcan représenté ici est un volcan de 2-isogénies car toutes les courbes ne se situant pas en bas du volcan sont reliées à 3 autres courbes. On a pris comme convention de représenter ici un graphe non orienté. En effet chaque arrête représente toutes les isogénies de noyaux identiques ainsi que leurs duales. On a aussi les différents ordres qui sont représentés, ils est à noter qu'avec la convention donnée par la définition 4.15 les ordres qui apparaissent dans un même niveau du graphe ont le même conducteur par rapport à l'ordre maximal, ainsi à l'aide du conducteur on peut établir des niveaux dans le volcan et donc illustrer les notions d'isogénies descendantes, montantes et horizontales.

Définition 4.17. Soit ℓ un nombre premier, soit D un discriminant associé à un ordre dans un corps de nombres quadratique imaginaire, on définit alors le

symbole de Kronecker en particulier pour le cas $\ell = 2$:

$$\left(\frac{D}{\ell}\right) = \begin{cases} \text{symbole de Kronecker} & \text{si } \ell \neq 2 \\ 0 & \text{si } \ell = 2 \text{ et } D = 0 \bmod 4 \\ 1 & \text{si } \ell = 2 \text{ et } D = 1 \bmod 8 \\ -1 & \text{si } \ell = 2 \text{ et } D = 5 \bmod 8 \end{cases}$$

On peut alors énoncer le théorème suivant qui donne la structure de tels graphes.

Théorème 4.18. *Soit E une courbe elliptique ordinaire définie sur un corps fini $\mathbb{F}_q$ avec $j(E) \neq 0, 1728$ et soit ℓ un nombre premier différent de la caractéristique de $\mathbb{F}_q$*

1. *Si $\ell \nmid [\mathcal{O}_K : \mathcal{O}]$ alors E admet $1 + \left(\frac{d_K}{\ell}\right)$ ℓ-isogénies horizontales*
2. *Si $\ell \mid [\mathcal{O}_K : \mathcal{O}]$ alors E admet une ℓ-isogénie montante*
3. *Si $\ell \nmid [\mathcal{O} : \mathbb{Z}[\pi]]$ alors E n'admet pas de ℓ-isogénie descendante*
4. *Si $\ell \mid [\mathcal{O} : \mathbb{Z}[\pi]]$ et $\ell \nmid [\mathcal{O}_K : \mathcal{O}]$ alors E admet $\ell - \left(\frac{d_K}{\ell}\right)$ ℓ-isogénies descendantes*
5. *Si $\ell \mid [\mathcal{O} : \mathbb{Z}[\pi]]$ et $\ell \mid [\mathcal{O}_K : \mathcal{O}]$ alors E admet ℓ isogénies de degré ℓ descendantes.*

Si $j(E) = 0$ ou $j(E) = 1728$ alors il faut prendre en compte l'action des automorphismes de E sur les sous-groupes cycliques de $E[\ell]$. Dans ce cas les valeurs énoncées ne donnent que le nombre de représentants sous l'action du groupe des automorphismes de E.

Démonstration. Voir [Koh96, Proposition 23]. □

On peut dés lors relier ce théorème avec les racines du ℓ-ième polynôme modulaire évalué en le j-invariant de la courbe que l'on étudie :

Corollaire 4.19. Dans le tableau suivant sont résumées les différentes possibilités de types d'isogénies selon la valeur de $\mathcal{N}_\ell(E)$ qui représente le nombre de solutions à l'équation : $\Phi_\ell(X, j(E)) = 0$ sur $\mathbb{F}_q$ pour $j \neq 0, 1728$.

$\mathcal{N}_\ell(E)$	Type des ℓ-isogénies		$\left(\frac{d_K}{\ell}\right)$	$\left(\frac{d_\pi}{\ell}\right)$
0	aucune	$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$ et $\ell \nmid [\mathcal{O} : \mathbb{Z}[\pi]]$	-1	-1
2	$\rightarrow$	$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$ et $\ell \nmid [\mathcal{O} : \mathbb{Z}[\pi]]$	$+1$	$+1$
1	cas 1 : $\rightarrow$	$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$ et $\ell \nmid [\mathcal{O} : \mathbb{Z}[\pi]]$	0	0
	cas 2 : $\uparrow$	$\ell \mid [\mathcal{O}_K : \mathcal{O}]$ et $\ell \nmid [\mathcal{O} : \mathbb{Z}[\pi]]$	0	0
$\ell + 1$	cas 1 : $\begin{cases} (1 + \left(\frac{d_K}{\ell}\right)) & \rightarrow \\ (\ell - \left(\frac{d_K}{\ell}\right)) & \downarrow \end{cases}$	$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$ et $\ell \mid [\mathcal{O} : \mathbb{Z}[\pi]]$	$0, 1$ ou -1	0
	cas 2 : $\begin{cases} 1 & \uparrow \\ \ell & \downarrow \end{cases}$	$\ell \mid [\mathcal{O}_K : \mathcal{O}]$ et $\ell \mid [\mathcal{O} : \mathbb{Z}[\pi]]$	0	0

Pour $j = 0$ ou $j = 1728$ il faut prendre en compte l'action des automorphismes de E sur les sous-groupes cycliques de $E[\ell]$. Dans ce cas les valeurs dans la seconde colonne ne donnent que le nombre de représentants sous l'action du groupe des automorphismes de E.

Démonstration. Voir [FM02, §4], [Koh96, Proposition 23]. □

Maintenant que l'on a introduit les relations possibles entre les ordres on définit certains termes de la littérature.

Définition 4.20. Soit ℓ un nombre premier, le terme *volcan* de ℓ-isogénies désigne le graphe composé de courbes ℓ-isogènes entre elles.

Le terme *cratère* du volcan des ℓ-isogénies désigne le sous-graphe composé uniquement de courbes dont la valuation ℓ-adique du conducteur est 0.

Définition 4.21. Soit ℓ un nombre premier, soit φ une ℓ^k-isogénie, alors φ est dite une ℓ^k-isogénie descendante s'il existe k isogénies de degré ℓ descendantes $\varphi_i, i \in [1,k]$ telles que $\varphi = \varphi_1 \circ \cdots \circ \varphi_k$. De même une ℓ^k-isogénie $\widehat{\varphi}$ est dite ascendante si il existe k isogénies de degré ℓ ascendantes $\widehat{\varphi}_i, i \in [1,k]$ telles que $\widehat{\varphi} = \widehat{\varphi_1} \circ \cdots \circ \widehat{\varphi_k}$. Enfin une ℓ^k-isogénie ψ est dite horizontale si il existe k ℓ-isogénies horizontales $\psi_i, i \in [1,k]$ telles que $\psi = \psi_1 \circ \cdots \circ \psi_k$.

Définition 4.22. Soit ℓ un nombre premier, un chemin descendant sur un volcan des ℓ-isogénies d'une courbe elliptique E est une suite de courbes elliptiques ℓ-isogènes $E = E_0 \to E_1 \to E_2 \to ... \to E_m$ telles que $E_i \mapsto E_{i+1}$ est une ℓ -isogénie descendante et que l'on ait $\ell \nmid [\mathcal{O}_m : \mathbb{Z}[\pi]]$.

Définition 4.23. Pour une courbe sur le volcan son niveau est la longueur d'un chemin descendant.
La hauteur h d'un volcan est le niveau maximal des courbes dans le volcan.

Remarque 4.24. Pour un volcan de ℓ-isogénies de hauteur h par les définitions 4.15 et 4.23 $\ell^{2h} | d_\pi$. En particulier pour $\ell \neq 2$ $\ell^{2h} || d_\pi$, ce résultat ne peut être énoncé pour $\ell = 2$ car il est possible que $4 \mid d_K$ par définition de d_K (définition 4.1).

Définition 4.25. Soit E une courbe elliptique située au niveau n du volcan des ℓ-isogénies, soit E_s la courbe codomaine de la ℓ^{h-n}-isogénie ascendante $\widehat{\varphi}$ de domaine E. Alors E_s est dite la *courbe sommet* de E.

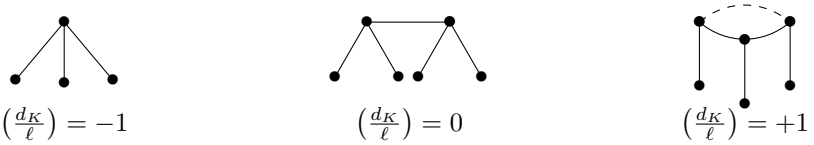


FIGURE 4.2 – Différents types de volcans des 2-isogénies.

On peut voir sur le dessin 4.2 les 3 différentes formes de volcans qui existent. Celles-ci sont distinguées par la forme de leur cratère qui est déterminée par la valeur de $\left(\frac{d_K}{\ell}\right)$.

On peut vouloir travailler avec des ℓ-isogénies qui ne sont pas définies dans $\mathbb{F}_q$ qui vont en dessous de la base du volcan, dés lors on doit travailler dans une extension de degré ℓ et la question du comportement du volcan se pose.

Lemme 4.26. Soit g le conducteur de $\mathbb{Z}[\pi]$, ℓ un nombre premier différent de p tel que $\ell \mid g$, n la valuation ℓ-adique de g, alors la valuation ℓ-adique de $\mathbb{Z}[\pi^\ell]$ est $n+1$.

Démonstration. Voir [MMS+08, Proposition 6]. □

Algorithme de Fouquet-Morain

L'algorithme de Fouquet-Morain [FM02] est un algorithme qui calcule un chemin descendant d'une courbe elliptique située sur le cratère afin de calculer la valuation ℓ-adique du conducteur de $\mathbb{Z}[\pi]$. Cet algorithme est une adaptation de l'algorithme «Probing the depths» de Kohel [Koh96, Section 4.2] au contexte SEA. Pour trouver une courbe sur le cratère la première chose à faire est de savoir déterminer un chemin descendant.

Chemin descendant En pratique une courbe admet au plus 2 isogénies horizontales et au moins une isogénie descendante (voir corollaire 4.19), ainsi à l'aide du calcul en parallèle de 3 isogénies on est sûr d'avoir une des 3 qui soit descendante. Il est aussi important de noter que toute courbe du volcan admet au plus une isogénie montante. Dés lors que l'on parcourt le volcan d'isogénies à partir d'une isogénie descendante et que l'on ne retourne pas sur une courbe déjà visitée alors la suite des isogénies parcourues seront descendantes jusqu'à ce que l'on se retrouve sur une courbe située en bas du volcan. On détecte qu'une courbe est en bas du volcan dés qu'il y a une seule courbe isogène à celle-ci.

Ainsi en pratique [FM02] calcule 3 chemins à partir de la courbe de départ et le(s) chemin(s) le(s) plus court(s) sera(ont) alors un(des) chemin(s) descendant(s).

Détection d'une courbe sur le cratère Pour détecter une courbe située sur le cratère on doit calculer les $\ell + 1$ chemins différents partants de la courbe E :

- si celle-ci admet deux chemins plus longs que les $\ell-1$ autres alors $\left(\frac{D}{\ell}\right) = 1$ le cratère est un cycle et la courbe est située sur le cratère,
- si celle-ci admet $\ell + 1$ chemins de longueurs identiques alors $\left(\frac{D}{\ell}\right) = -1$ le cratère est réduit à un point et la courbe est située sur le cratère,
- si celle-ci admet 1 chemin plus grand d'une isogénie que les ℓ autres et si elle est isogène à une courbe qui admet les mêmes longueurs de chemins alors $\left(\frac{D}{\ell}\right) = 0$ le cratère est réduit à deux points et la courbe est située sur le cratère,
- si celle-ci admet 1 chemin plus grand que les ℓ autres et si elle est isogène à une courbe E_h qui n'admet pas les mêmes longueurs de chemin alors E_h se situe au dessus de E dans le volcan et on recommence le test avec E_h.

Algorithme de Fouquet-Morain L'algorithme de Fouquet-Morain [FM02] calcule donc pour différents nombres premiers ℓ_i la valuation v_i ℓ_i-adique du conducteur de $\mathbb{Z}[\pi]$. À l'aide de cette valuation on obtient la valeur du carré de la trace modulo $\ell_i^{v_i}$, le signe est calculé à l'aide d'une détermination de valeurs propres pour le Frobenius en factorisant le polynôme de ℓ_i-division. Ainsi l'algorithme de Fouquet-Morain a une application dans l'algorithme de Schoof [Sch85] (voir sous-section 1.4.2) qui calcule la cardinalité d'une courbe elliptique à partir de la valeur de sa trace modulo différents nombres premiers et utilise ensuite le théorème des restes chinois pour trouver la cardinalité de la courbe elliptique.

4.2 Lien entre les niveaux d'une courbe dans le volcan et la structure de la ℓ^∞ torsion rationnelle

Dans cette section on met en avant les liens qui existent entre le niveau d'une courbe dans un volcan des ℓ-isogénies et la structure de sa ℓ-torsion rationnelle. Les résultats exposés ici sont tirés de [MMS+08] et [IJ10].

Proposition 4.27 (Lenstra)**.** Soit E une courbe elliptique ordinaire définie sur $\mathbb{F}_q$, π l'endomorphisme de Frobenius alors pour les extension de corps de la forme $\mathbb{F}_{q^r}$ $\mathrm{End}(E)$ est un $\mathbb{Z}$-module de rang 2 et on a l'isomorphisme de $\mathbb{Z}$-modules suivant :

$$E(\mathbb{F}_{q^r}) \cong \frac{\mathrm{End}(E)}{\pi^r - 1}$$

Démonstration. [Len96, Theorem 1] □

Corollaire 4.28. Sur un volcan des ℓ-isogénies, deux courbes elliptiques ordinaires E, E' situées au même niveau ont la même structure de ℓ-torsion rationnelle.

Démonstration. Comme E et E' sont situées au même niveau alors leurs anneaux des endomorphismes sont isomorphes, par la proposition 4.27 on obtient le résultat. □

Lemme 4.29. Soit E une courbe elliptique ordinaire définie sur $\mathbb{F}_q$ de conducteur f, $\pi = a + g\omega_K$ l'endomorphisme de Frobenius, alors le plus grand n_2 tel que $E[n_2] \subset E(\mathbb{F}_q)$ est $n_2 = \mathrm{pgcd}(a-1, g/f)$.

Démonstration. Voir [Rüc87, Lemma 1]. □

Avant d'énoncer le résultat principal sur la structure de la ℓ-torsion rationnelle on a besoin du résultat intermédiaire suivant :

Proposition 4.30. Soit E une courbe elliptique ordinaire définie sur $\mathbb{F}_q$, $\pi = a+g\omega_K$ l'endomorphisme de Frobenius alors : $v_\ell(a-1) \geqslant \min(v_\ell(g), v_\ell(|E(\mathbb{F}_q)|/2))$.

Démonstration. Voir [Ion10, Lemma 5.2] □

On peut maintenant relier la structure de la ℓ-torsion et le niveau de la courbe dans le volcan des ℓ-isogénies.

Proposition 4.31. Soit E une courbe elliptique ordinaire définie sur $\mathbb{F}_q$ telle que $E(\mathbb{F}_q)[\ell^\infty] = \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$ avec $n_2 \mid n_1$, $\pi = a + g\omega_K$ l'endomorphisme de Frobenius :

- si $v_\ell(n_1) > v_\ell(n_2)$ alors E se situe au niveau n_2,
- si $v_\ell(n_1) = v_\ell(n_2)$ alors E se situe à un niveau supérieur ou égal à $v_\ell(|E(\mathbb{F}_q)|)/2$.

Démonstration. La preuve est issue du travail de [MMS+08], [Ion10].

- On se place tout d'abord dans le premier cas où l'on a $v_\ell(n_1) > v_\ell(n_2)$, on a par conséquent $v_\ell(n_2) < v_\ell(|E(\mathbb{F}_q)|)/2$. On va d'abord prouver que la valuation ℓ-adique de n_2 diminue de 1 à chaque descente d'un niveau dans le volcan, puis déterminer la structure d'une courbe située en bas du

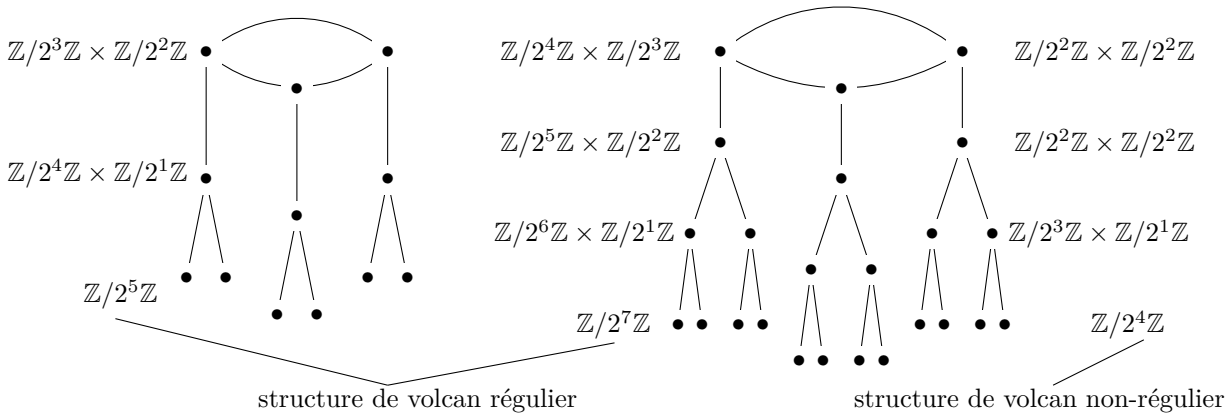


FIGURE 4.3 – Exemples de structures de la 2^∞-torsion rationnelle par rapport au niveau des courbes dans le volcan.

volcan pour ensuite obtenir le résultat. On a n_2 qui est égal à $\text{pgcd}(a-1, g/f)$ par le lemme 4.29.
Supposons que $\min(v_\ell(g), v_\ell(|E(\mathbb{F}_q)|)/2) = v_\ell(g)$, on a alors $v_\ell(a-1) \geqslant v_\ell(g)$ et comme $n_2 = \text{pgcd}(a-1, g/f)$ alors on a $v_\ell(n_2) = v_\ell(g/f)$. Supposons maintenant que $\min(v_\ell(g), v_\ell(|E(\mathbb{F}_q)|)/2) = v_\ell(|E(\mathbb{F}_q)|)/2)$ alors on obtient $v_\ell(a-1) \geqslant v_\ell(|E(\mathbb{F}_q)|)/2) > v_\ell(n_2)$ ce qui est absurde.
Dés lors quand on descend d'un niveau dans le volcan la valuation ℓ-adique de f augmente de 1 et par conséquent $v_\ell(n_2) = v_\ell(g/f)$ diminue de 1 aussi, en particulier cela implique que la valuation ℓ-adique de n_2 pour une courbe en bas du volcan est nulle. Ainsi on voit bien la bijection entre la valuation ℓ-adique de n_2 et le niveau de la courbe dans le volcan.

— On se place désormais dans le cas où l'on a $v_\ell(n_1) = v_\ell(n_2)$ (et par conséquent $2 \mid v_\ell(|E(\mathbb{F}_q)|)$). Dans ce cas la structure de la ℓ-torsion ne change pas du cratère jusqu'à un niveau appelé premier niveau de stabilité. Dés lors pour le niveau en dessous du premier niveau de stabilité on a $v_\ell(n_1) \neq v_\ell(n_2)$ en appliquant alors le résultat du premier point on a le premier niveau de stabilité qui se trouve au niveau $v_\ell(|E(\mathbb{F}_q)|)/2$, par conséquent E se trouve à un niveau supérieur à $v_\ell(|E(\mathbb{F}_q)|)/2$.

□

Définition 4.32. Sur un volcan des ℓ-isogénies on appelle le niveau à partir duquel la structure de la ℓ-torsion ne change pas en même temps que les niveaux du volcan le *premier niveau de stabilité*.

Un volcan dont tous les niveaux ont des structures de ℓ-torsion distinctes est dit un *volcan régulier*.

Corollaire 4.33. Soit E une courbe elliptique ordinaire définie sur $\mathbb{F}_q$ située en dessous du premier niveau de stabilité telle que $E[\ell^\infty] = \mathbb{Z}/\ell^r\mathbb{Z} \times \mathbb{Z}/\ell^s\mathbb{Z}$ alors pour E_b une des courbes situées un niveau en dessous de E dans le volcan des ℓ-isogénie on a $E_b[\ell^\infty] = \mathbb{Z}/\ell^{r+1}\mathbb{Z} \times \mathbb{Z}/\ell^{s-1}\mathbb{Z}$

Remarque 4.34. Il existe un second niveau de stabilité introduit et développé dans [IJ10] mais nous ne nous servirons pas de cette définition.

Proposition 4.35. Soit E une courbe elliptique ordinaire définie sur $\mathbb{F}_q$ avec : $E(\mathbb{F}_q)[\ell^\infty] = \mathbb{Z}/\ell^r\mathbb{Z} \times \mathbb{Z}/\ell^s\mathbb{Z} = \langle P, Q\rangle$, $r > s+1 \geqslant 1$ et P un point d'ordre ℓ^r, alors :

1. la ℓ-isogénie engendrée par $\ell^{r-1}P$ est une isogénie montante avec pour codomaine un courbe elliptique E' telle que :
$$E'(\mathbb{F}_q)[\ell^\infty] = \mathbb{Z}/\ell^{r-1}\mathbb{Z} \times \mathbb{Z}/\ell^{s+1}\mathbb{Z},$$
2. les autres ℓ-isogénies sont descendantes.

Démonstration. Une preuve est disponible dans [MMS+08, Proposition 4] pour le cas $\ell = 2$, mais on va proposer ici une preuve plus directe et générale. Par le corollaire 4.19 on a $\ell+1$ isogénies de degré ℓ et si l'on a une ℓ-isogénie montante alors les autres sont descendantes.
Considérons l'isogénie ϕ engendrée par $[\ell^{r-1}]P$. L'image $\widetilde{P}$ de P par l'isogénie ϕ est alors d'ordre ℓ^{r-1}.

Montrons par l'absurde que l'on n'a pas $\mathbb{Z}/\ell^r\mathbb{Z} \subset \phi(E)(\mathbb{F}_q)[\ell^\infty]$. Supposons qu'il existe un point $\widetilde{R}$ d'ordre ℓ^n avec $n \geqslant r$. Cela implique donc qu'il existe $R \in E(\mathbb{F}_q)$ tel que R soit d'ordre ℓ^n et $R \notin \langle P\rangle$ ou $[\ell^n]R = [\ell^{r-1}]P$. La deuxième hypothèse est impossible car cela implique qu'il existe $S \in E(\mathbb{F}_q)$ tel que $[\ell]S = P$ et contredit donc l'hypothèse sur la structure de $E(\mathbb{F}_q)[\ell^\infty]$. De même la première hypothèse : $[\ell^n]R = \mathcal{O}$ contredit elle aussi la structure de $E(\mathbb{F}_q)[\ell^\infty]$. On a donc :

$$\phi(E)(\mathbb{F}_q)[\ell^\infty] = \mathbb{Z}/\ell^{r-1}\mathbb{Z} \times \mathbb{Z}/\ell^{s+1}\mathbb{Z}.$$

On observe bien que c'est une isogénie montante par le corollaire 4.33. □

Corollaire 4.36. Soit E une courbe elliptique ordinaire définie sur $\mathbb{F}_q$ avec $E(\mathbb{F}_q)[\ell^\infty] = \mathbb{Z}/\ell^r\mathbb{Z} \times \mathbb{Z}/\ell^s\mathbb{Z}$, alors $E(\mathbb{F}_{q^\ell})[l^\infty] = \mathbb{Z}/\ell^{r+1}\mathbb{Z} \times \mathbb{Z}/\ell^{s+1}\mathbb{Z}$.

Démonstration. Le résultat est démontré dans [Ion10, §5.3.1]. □

On peut donc résumer les résultats de cette section sur le lien entre les volcans des ℓ-isogénies et la structure de la ℓ^∞ torsion rationnelle à l'aide de la figure 4.3. Le volcan des 2-isogénies *régulier* à gauche illustre l'évolution de la structure de la 2^∞-torsion rationnelle, on voit le lien direct entre la structure de la 2^∞-torsion rationnelle d'une courbe et son niveau dans le volcan comme énoncé dans la proposition 4.31.

Le volcan des 2-isogénies représenté à droite est présenté avec deux structures de la 2^∞-torsion rationnelle à gauche et à droite du volcan. Sur la droite du volcan est représenté un exemple de structure de la 2^∞-torsion rationnelle pour un volcan *non régulier*, on observe que dès que la 2^∞-torsion rationnelle est isomorphe à un produit de deux sous-groupes cycliques de tailles identiques, comme c'est le cas au deuxième niveau du volcan, alors la structure de la 2^∞-torsion rationnelle ne change pas pour les courbes situées au-dessus dans le volcan. Enfin le volcan de droite avec la structure montrée à sa gauche représente le volcan que l'on obtient en travaillant dans l'extension quadratique du corps sur lequel est défini le volcan des 2-isogénies de gauche, la structure de la 2^∞-torsion illustre le résultat du corollaire 4.36.

Chapitre 5

Détermination de directions dans le volcan des ℓ-isogénies à l'aide de l'action du Frobenius

Dans cette partie nous allons étudier l'action du Frobenius sur le module de Tate $\mathsf{T}_\ell(E)$ et voir comment cette action détermine des directions dans le volcan des ℓ-isogénies. On rappelle que l'on se place dans toute la suite de ce document dans le cas où la courbe elliptique est ordinaire. Ceci peut permettre par exemple dans le cas Elkies (défini plus bas) de savoir rester sur le cratère cyclique et, par exemple, de calculer l'équation de classe d'idéaux (voir [Fou01, Définition 2.3.1]), de calculer un diviseur du nombre de classe d'idéaux en parcourant le cratère d'un volcan des ℓ-isogénies(voir [Fou01, §6.4]). Cela peut permettre aussi d'atteindre et détecter le cratère du volcan directement y compris lorsque l'on est sur des volcans non-réguliers et par conséquent de déterminer la hauteur du volcan par des méthodes plus directes que celles de [FM02].

5.1 Cas Elkies

La majeure partie du travail présenté dans cette sous-section a été effectué en collaboration avec Luca De Feo, Jérôme Plût et Éric Schost. Il a fait l'objet d'une publication [DFHPS16].

On se place tout d'abord dans un cas particulier le cas Elkies que l'on définit de suite :

Définition 5.1. Soit E une courbe elliptique définie sur $\mathbb{F}_q$, ℓ est dit un nombre premier de Elkies si le polynôme caractéristique du Frobenius : $\pi^2 - t_\pi \pi + q$ se factorise dans $\mathbb{Z}_\ell$ à l'aide de deux valeurs propres distinctes notées dans le document λ et μ. On a donc dans ce cas

$$\pi^2 - t_\pi \pi + q = (\pi - \lambda)(\pi - \mu) \text{ dans } \mathbb{Z}_\ell[\pi], \text{ avec } \lambda \neq \mu.$$

Dès lors puisque $\ell^{2h} \mid d_\pi$ et pour $\ell \neq 2$ $\ell^{2h} || d_\pi$, pour $\ell = 2$ on peut avoir $2^{2h+1} \mid d_\pi$ lorsque $2 \mid d_K$ (voir remarques 4.12 et 4.24) avoir d_π un résidu

quadratique est équivalent à avoir $\left(\frac{d_K}{\ell}\right) = 1$. Ainsi dans le cas Elkies le cratère est cyclique par le corollaire 4.19.

On note $h = v_\ell(\lambda - \mu)$, ainsi le polynôme caractéristique de π admet deux valeurs propres distinctes modulo ℓ^k dès que $k > h$.

Proposition 5.2. Soit E une courbe elliptique ℓ un nombre premier de Elkies alors on a $h = v_\ell(\lambda - \mu)$ est la hauteur du volcan des ℓ-isogénies contenant E.

Démonstration. Dans la section 4.1 on a vu que l'on avait $d_\pi = \ell^{2h'} d_K$ avec $\ell^2 \nmid d_K$ pour un volcan des ℓ-isogénies de hauteur h' sur $\mathbb{F}_q$. Ainsi comme $\ell^2 \nmid \frac{d_\pi}{\ell^{2v_\ell(\lambda-\mu)}} = \frac{(\lambda-\mu)^2}{\ell^{2v_\ell(\lambda-\mu)}}$ alors on a bien $h = h'$ et h représente bien la hauteur du volcan. □

Désormais lorsque l'on parlera de hauteur h du volcan on fera référence à la hauteur du volcan des ℓ-isogénies définies sur $\mathbb{F}_q$, sauf mention explicite contraire.

5.1.1 Étude de l'action du Frobenius sur le module de Tate

On représente l'action du Frobenius sur $\mathsf{T}_\ell(E)$ à l'aide d'une matrice 2×2. On a le résultat suivant qui nous donne la forme de ces matrices à conjugaison près.

Proposition 5.3. Soit E une courbe elliptique ordinaire, telle que ℓ est un nombre Elkies à deux racines distinctes λ, μ appartenant à $\mathbb{Z}_\ell$. Il existe un unique $e \in [0, h]$ tel que l'action du Frobenius dans toute base de $\mathsf{T}_\ell(E)$ est conjuguée, sur $\mathbb{Z}_\ell$, à la matrice

$$\begin{pmatrix} \lambda & \ell^{h-e} \\ 0 & \mu \end{pmatrix}.$$

De plus $e = 0$ si E se situe sur le cratère, sinon $h - e$ est le niveau de E dans le volcan, e est appelé la *profondeur* de la courbe dans le volcan.

Remarque 5.4. $\left(\begin{smallmatrix} \lambda & \ell^h \\ 0 & \mu \end{smallmatrix}\right)$ est conjuguée à $\left(\begin{smallmatrix} \lambda & 0 \\ 0 & \mu \end{smallmatrix}\right)$ sur $\mathbb{Z}_\ell$.

Démonstration. Comme le polynôme caractéristique de π admet deux valeurs propres sur $\mathbb{Z}_\ell$ alors pour toute base de $\mathsf{T}_\ell(E)$ la matrice représentant l'action du Frobenius dans cette base est trigonalisable. La conjugaison de la matrice $\left(\begin{smallmatrix} \lambda & a \\ 0 & \mu \end{smallmatrix}\right)$ par $\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right)$ change le coefficient a en $a - b(\lambda - \mu)$, et la conjugaison par $\left(\begin{smallmatrix} c & 0 \\ 0 & 1 \end{smallmatrix}\right)$ change a en $c \cdot a$, ainsi la valuation ℓ-adique $h - e = v_\ell(a)$ est invariante sous la conjugaison matricielle. Cela prouve la première partie de la proposition.

Pour la seconde partie, par le théorème de Tate [Sil86, Isogeny theorem III.7.7 (a)], $\mathcal{O} \otimes \mathbb{Z}_\ell$ est isomorphe à l'ordre dans $\mathbb{Q}_\ell[\pi_\ell]$ des matrices avec coefficients entiers, cet ordre est engendré par la matrice identité et la matrice $\ell^{-\min(h, v_\ell(a))}(\pi_\ell - \lambda)$, dés lors l'indice de cet ordre par rapport à $\mathbb{Z}[\pi_\ell]$ est de $\ell^{\min(h, v_\ell(a))}$, lui donnant son niveau $\min(h, v_\ell(a))$ dans le volcan des ℓ-isogénies. □

Ainsi avec la proposition 5.3 on a un moyen de déterminer la hauteur d'une courbe dans un volcan des ℓ-isogénies à l'aide de l'étude de l'action du Frobenius sur $\mathsf{T}_\ell(E)$. Dans la figure 5.1 est représenté un volcan des 2-isogénies de hauteur 2, où l'on observe le lien entre le niveau de la courbe dans le volcan (de hauteur

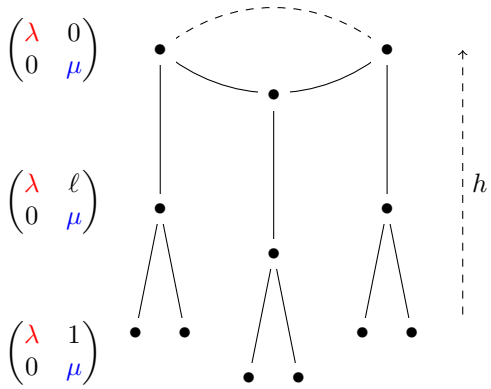


FIGURE 5.1 – Différentes formes de matrices du Frobenius à conjugaison près selon le niveau dans le volcan des isogénies.

2 ici) et la forme de la matrice du Frobenius à conjugaison près. Par conséquent, pour les courbes situées tout en bas du volcan, le coefficient triangulaire supérieur est de valuation ℓ-adique nulle, et augmente de 1 à chaque fois que l'on monte d'un niveau dans le volcan.

Le résultat suivant nous donne un moyen de savoir comment monter et descendre à l'intérieur d'un volcan des ℓ-isogénies en étudiant l'action du Frobenius sur leurs noyaux. C'est d'ailleurs l'approche que l'on aura tout au long de cette section : pour déterminer les directions des isogénies on étudiera l'action du Frobenius sur un générateur de leur noyau.

Proposition 5.5. Soient E une courbe elliptique située au niveau $h - e \neq h$ du volcan des ℓ-isogénies avec ℓ un nombre premier de Elkies, $P, Q \in E$ tels que $\langle P, Q\rangle = E[\ell^k]$ avec $k > h - e$, pour lesquels la matrice du Frobenius est de la forme $\left(\begin{smallmatrix}\lambda & \delta\ell^{h-e}\\ 0 & \mu\end{smallmatrix}\right)$ mod ℓ^k avec $\delta \wedge \ell = 1$. Alors la ℓ-isogénie montante de domaine E a pour noyau le groupe $\langle[\ell^{k-1}]P\rangle$, les isogénies descendantes ont pour noyau les groupes $\langle[\ell^{k-1}](Q + [a]P)\rangle$ avec $a \in \mathbb{Z}/\ell\mathbb{Z}$.

Démonstration. Soit $\widehat{\varphi} : E \to E'$ la ℓ-isogénie de noyau $\langle \ell^{k-1}P\rangle$. Soit $P' \in E'$ un point de ℓ-division de $\widehat{\varphi}(P)$, alors le Frobenius de E' agit sur la base $(P', \widehat{\varphi}(Q))$ comme la matrice $\left(\begin{smallmatrix}\lambda & \delta\ell^{h-e+1}\\ c\ell^{k-1} & \mu\end{smallmatrix}\right)$ mod ℓ^k, avec $c \in \mathbb{Z}/\ell\mathbb{Z}$. Par la proposition 5.3 E' se situe au niveau $h - e + 1$. En effet un changement de base de la forme $\left(\begin{smallmatrix}1 & 0\\ \gamma\ell^{k-1} & 1\end{smallmatrix}\right)$, avec $\gamma \in (\mathbb{Z}/\ell\mathbb{Z})^\times$ tel que $\ell^{k-1}(c + \gamma(\lambda - \mu)) = 0 \bmod \ell^k$, permet d'obtenir une matrice triangulaire supérieure comme dans la proposition 5.3.

De même on peut montrer que pour φ une ℓ-isogénie de noyau $\langle[\ell^{k-1}](Q + [a]P)\rangle$ avec $a \in \mathbb{Z}/\ell\mathbb{Z}$ on obtient, pour Q' un point de ℓ-division de $Q+[a]P$, dans la base $(\varphi(P), Q')$ une matrice du Frobenius de la forme $\left(\begin{smallmatrix}\lambda & \delta\ell^{h-e-1}+b\ell^{k-1}\\ 0 & \mu\end{smallmatrix}\right)$ mod ℓ^k avec $b \in \mathbb{Z}/\ell\mathbb{Z}$. Donc, par la proposition 5.3, le codomaine de φ se situe au niveau $h - e + 1$. □

On pourra noter qu'avec cette proposition on retrouve bien la proposi-

tion 4.35 qui énonçait que pour une courbe E non située sur le cratère, telle que $E(\mathbb{F}_q)[\ell^\infty] \simeq \mathbb{Z}/\ell^{n_1+i}\mathbb{Z} \times \mathbb{Z}/\ell^{n_1}\mathbb{Z}$ avec $i > 0$, la ℓ-isogénie engendrée par un point de $E(\mathbb{F}_q)$ d'ordre ℓ^{n_1+i} est montante.

On voit aussi que cette détermination n'est pas sujette à l'existence de niveau de stabilité vu que la preuve ne se fait pas à l'aide de la structure de la ℓ-torsion.

On va maintenant se focaliser sur la détermination d'autres directions à l'aide du Frobenius, on va tout naturellement commencer par le cratère car c'est l'endroit où le Frobenius se diagonalise et où l'on peut donc distinguer l'action du Frobenius sur deux espaces propres distincts. Introduisons tout d'abord quelques définitions nécessaires :

Définition 5.6 (Bases horizontales et diagonales)**.** Soit E une courbe se situant sur le cratère, on appelle un point de $E[\ell^k]$ *horizontal* si il génère le noyau d'une isogénie horizontale. On appelle une base de $E[\ell^k]$ *diagonale* si π est diagonal dans cette base, *horizontale* si les deux points de la base sont horizontaux.

Avant de montrer les liens entre bases horizontales et diagonales on a besoin du résultat intermédiaire suivant qui, pour $\phi : E \mapsto E'$, montre comment calculer l'image de la matrice du Frobenius $\pi|\mathsf{T}_\ell(E)$, notée Π, dans une base de $\mathsf{T}_\ell(E')$.

Lemme 5.7. Soit une base fixée de $\mathsf{T}_\ell(E)$ dont la projection sur $E[\ell^k]$ est $\langle P, Q\rangle$ avec $k > 0$, soit $\phi : E \to E'$ l'isogénie de noyau engendré par $R = [x]P + [y]Q$ avec $x \wedge \ell = 1$ et $y = \ell^m y'$ avec $y' \wedge \ell = 1$, $0 \leqslant m \leqslant k$. Soit M_R la matrice de forme normale réduite de Hermite qui correspond au réseau engendré par R, $\ell^k\mathsf{T}_\ell(E)$ alors la matrice du Frobenius sur $\mathsf{T}_\ell(E')$ est donnée par $M_R^{-1} \cdot \Pi \cdot M_R$ à conjugaison près, avec Π la matrice du Frobenius dans la base fixée de $\mathsf{T}_\ell(E)$.

Démonstration. Le sous-groupe $\langle R\rangle$ définit un point dans l'espace projectif de $E[\ell^k]$, celui-ci est une ligne projective sur $\mathbb{Z}/\ell^k\mathbb{Z}$. Il existe une bijection canonique [Ser77, II.1.1] entre cette ligne projective et l'ensemble des réseaux d'indice ℓ^k dans le $\mathbb{Z}_\ell$ module $\mathsf{T}_\ell(E)$: la ligne $\langle R\rangle$ est donc en bijection avec le réseau $\Lambda_R = \langle R\rangle + \ell^k\mathsf{T}_\ell(E)$. Ce réseau est aussi la pré-image du réseau $\ell^k\mathsf{T}_\ell(E')$ par ϕ.

Le réseau Λ_R est engendré par les colonnes de la matrice $L_R = \begin{pmatrix} \ell^k & 0 & x \\ 0 & \ell^k & y \end{pmatrix}$. La forme normale réduite de Hermite de L_R est $M_R = \begin{pmatrix} \ell^{k-m} & x/y' \\ 0 & \ell^m \end{pmatrix}$, et les colonnes de M_R génèrent le réseau Λ_R. On peut vérifier que M_R a pour déterminant ℓ^k. Comme $\Lambda_R = \phi^{-1}(\ell^k\mathsf{T}_\ell(E'))$, alors il existe une base de $\mathsf{T}_\ell(E')$ dans laquelle ϕ a pour matrice $\ell^k M_R^{-1}$. Ainsi, dans cette base de $\mathsf{T}_\ell(E')$ la matrice de $\pi|\mathsf{T}_\ell(E')$ est $M_R^{-1} \cdot \Pi \cdot M_R$. □

Proposition 5.8. Soit E une courbe se situant sur le cratère et P un point de $E[\ell^k]$ tel que $\ell^h P$ soit un vecteur propre de π, alors $\ell^h P$ est horizontal si et seulement si P est un vecteur propre pour π. Si $\pi(P) = \lambda P$ alors on dit que $\ell^h P$ a pour direction λ.

Démonstration. La proposition étant évidente pour $h \geqslant k$, on suppose que $k \geqslant h$.

Soit $\langle R, S\rangle = E[\ell^k]$ une base qui diagonalise π. On peut alors exprimer $P = [x]R + [y]S$, on suppose sans perte de généralité que $y = 1$.

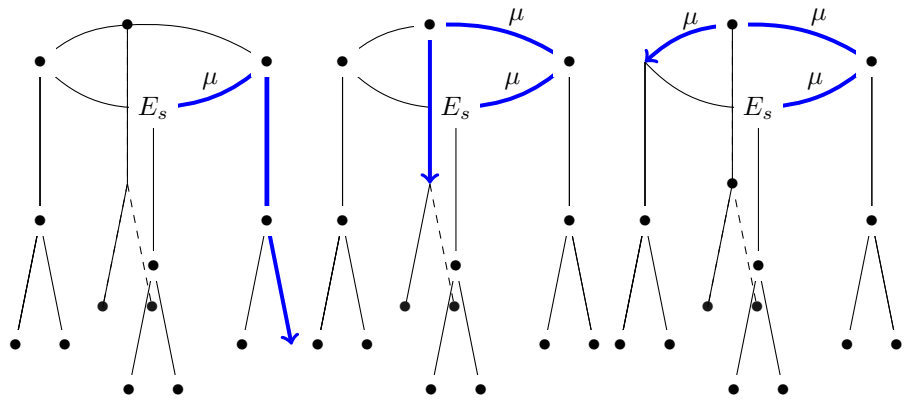


FIGURE 5.2 – Exemples de différents points diagonaux $P \in E_s$ d'ordre 2^3 tels que $\pi(P) = [\mu]P$.

Soit ϕ l'isogénie de noyau $\langle [\ell^h]P \rangle$ et E' son codomaine. Comme $[\ell^h]P$ est un vecteur propre de π, alors ϕ est une isogénie rationnelle. Par le lemme 5.7, pour toute base de $\mathsf{T}_\ell(E')$ la matrice $\pi|\mathsf{T}_\ell(E')$ est conjuguée à $\begin{pmatrix} \lambda & \ell^{h-k}x(\lambda-\mu) \\ 0 & \mu \end{pmatrix}$.

Cette matrice est diagonalisable seulement si $v_\ell(x) \geqslant k - h$.

Pour l'autre sens de la preuve supposons, sans perte de généralité, que P soit un vecteur propre de π pour la valeur propre μ, alors $(\pi - \mu)P = x(\lambda - \mu)R$ et l'on obtient le résultat. □

Sur la Figure 5.2 sont représentées les isogénies qui ont pour noyau différents points $P \in E_s$ diagonaux d'ordre 2^3, tels que $\pi(P) = [\mu]P$. On remarque tout d'abord que l'on peut avoir uniquement la ℓ-isogénie de noyau $\langle [2^2]P \rangle$ qui soit horizontale, comme représenté sur le volcan dessiné à gauche. Or on voudrait, comme sur le volcan dessiné à droite, déterminer un point P tel que la 2^3-isogénie de noyau $\langle P \rangle$ soit horizontale. On pourrait, par exemple, diagonaliser une base de la 2^{3+2} torsion et l'on aurait le résultat à l'aide de la proposition 5.8. Cependant pour faire cela on peut être amené à travailler dans des extensions de corps uniquement pour avoir un point horizontal défini dans un sous-corps. Le résultat suivant répond à ce problème et nous permet de construire des bases horizontales de taille aussi grande que la ℓ-torsion définie sur le corps sur lequel on travaille, sans que l'on ait à travailler dans des extensions de corps supplémentaires.

Proposition 5.9. Soit $\psi : E \to E'$ une ℓ-isogénie horizontale de direction λ, $Q \in E[\ell^\infty]$, si $[\ell]Q$ est horizontal de direction μ, alors $\psi(Q)$ est horizontal de direction μ.

Démonstration. Soit $Q' = \psi(Q)$ et $\widehat{\psi}$ l'isogénie duale de ψ, comme $\widehat{\psi}$ et $\widehat{\psi}(Q') = [\ell]Q$ sont horizontaux de direction μ, alors Q' est horizontal de direction μ. □

On présente donc sur la figure 5.3 un exemple de construction de point horizontal : on a repris le premier exemple de point diagonal de la figure 5.2, pour lequel on était certain par la proposition 5.8 que $[2^2]P$ était horizontal de direction λ. On utilise alors la proposition 5.8 pour déterminer l'isogénie ψ :

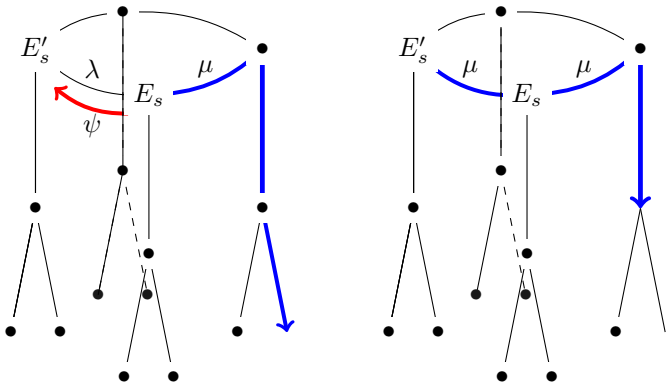


FIGURE 5.3 – Exemple de construction de point horizontal d'ordre 2^2.

$E_s \to E'_s$ de direction μ, $\psi(P)$ est alors un point d'ordre $[2^3]$ tel que $[2]\psi(P)$ est un point horizontal d'ordre 2^2 par la proposition 5.9. L'isogénie de noyau $\langle\psi(P)\rangle$ est donc représentée sur le volcan de droite. Pour obtenir un point horizontal d'ordre 2^3 on utilise à nouveau une 2-isogénie de direction μ et de domaine E'_s, que l'on applique à $\psi(P)$.

On va donc montrer comment transporter cette information pour des courbes situées en dessous du cratère. Avant cela voyons comment déterminer à l'aide d'une base horizontale les isogénies descendantes d'une courbe située sur le cratère.

Proposition 5.10. Soit E une courbe elliptique située sur le cratère cyclique d'un volcan des ℓ-isogénies, $\langle P, Q\rangle = E[\ell]$ une base horizontale. Alors les ℓ-isogénies descendantes sont générées par les sous-groupes $\langle P + [b]Q\rangle$ avec $b \wedge \ell = 1$.

Démonstration. Comme il y a en tout $\ell + 1$ sous groupes de $E[\ell]$, avec les sous-groupes $\langle P\rangle$, $\langle Q\rangle$ qui engendrent des ℓ-isogénies horizontales, alors les $\ell - 1$ sous groupes restants de la forme $\langle P + [b]Q\rangle$ avec $b \wedge \ell = 1$ engendrent des ℓ-isogénies descendantes par le théorème 4.18. □

Corollaire 5.11. Soit E une courbe située sur le cratère, $k \geqslant i \geqslant 1$, $\langle P, Q\rangle = E[\ell^k]$ une base horizontale. Alors les ℓ^i-isogénies descendantes sont générées par les sous-groupes $\langle [a\ell^{k-i}]P + [b\ell^{k-i}]Q\rangle$ avec $b \wedge \ell = 1$ et $a = 1 \bmod \ell$.

Il est important de noter que, comme dit dans la sous-sous-section 4.1.2 et dans [FM02], lorsque la décomposition de la ℓ^i-isogénie en i ℓ-isogénies ne comporte pas d'isogénie duale d'une autre isogénie alors le fait d'avoir la première ℓ-isogénie (celle de noyau $\langle [\ell^{k-1}]([a]P + [b]Q)\rangle$) descendante est suffisant pour avoir une ℓ^i-isogénie descendante de noyau $\langle \ell^{k-i}]([a]P + [b]Q)\rangle$. Enfin il n'y a pas de ℓ-isogénie duale d'une autre ℓ-isogénie dans la composition de la ℓ^i-isogénie car celle-ci est générée par un point et donc par un groupe cyclique.

Définition 5.12. Soient E une courbe qui se situe à une profondeur $e \geqslant 1$ du cratère (*id est* au niveau $h - e$), E_s la courbe sommet de E (voir définition 4.25), $P \in E_s$ un point d'ordre ℓ^k, avec $k > e$, tel que $[\ell^e]P$ soit horizontal de direction

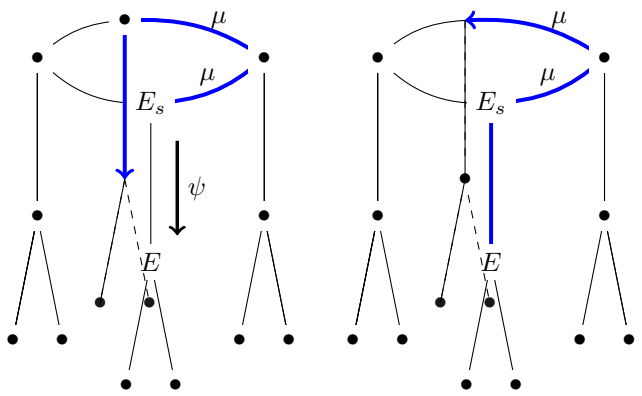


FIGURE 5.4 – Construction d'un point ascendant horizontal.

λ (resp. μ), φ la ℓ^e-isogénie $\varphi : E_s \to E$, alors $\varphi(P)$ est appelé point *ascendant horizontal* de direction λ (resp. μ) et de profondeur e.

Remarque 5.13. Il est porté à l'attention du lecteur qu'un point horizontal est aussi un point *ascendant horizontal* de profondeur 0.

On voit sur la figure 5.4 la construction d'un point ascendant horizontal sur un volcan de 2-isogénies. Sur le volcan de gauche est représentée l'isogénie de noyau $\langle P \rangle$ avec $P \in E_s$ tel que $[2]P$ est horizontal de direction μ. On calcule alors l'image de P par la 2-isogénie descendante $\psi : E_s \to E$ pour construire le point ascendant horizontal $R = \psi(P) \in E$. Sur le volcan de droite est représenté l'isogénie de noyau $\langle R \rangle$.

Proposition 5.14. Soit $P \in E[\ell^k]$ un vecteur propre de π, $i \leqslant k$ tel que $[\ell^i]P$ soit horizontal de direction λ, $\varphi : E \mapsto E_i$ une isogénie descendante de degré ℓ^i, on note $P' = \varphi(P)$, alors :

1. $\langle [\ell^{k-i}]P' \rangle$ est le noyau d'une isogénie montante de degré ℓ^i duale de φ notée $\widehat{\varphi}$,
2. $\langle \widehat{\varphi}(P') \rangle$ est le noyau d'une isogénie horizontale de direction λ de degré ℓ^{k-i}.

Démonstration. Pour le point (1) comme $[\ell^{k-1}]P$ n'est pas dans le noyau de φ, alors $\langle [\ell^{k-i}]\varphi(P) \rangle$ est le noyau de $\widehat{\varphi}$.

Pour le point (2) il suffit d'écrire que $\widehat{\varphi}(P') = [\ell^i]P$; on conclut alors à l'aide des hypothèses sur P. □

Maintenant nous allons voir si l'on peut distinguer les ℓ^i-isogénies descendantes dans le volcan à l'aide d'une étude de l'action du Frobenius. Pour cette étude on fixe un point d'ordre ℓ^k qui engendre la ℓ-isogénie montante (ou l'une des deux horizontales lorsque l'on est sur le cratère) et on regarde si la forme de la matrice du Frobenius est liée à la ℓ^i-isogénie descendante engendrée par le second point qui forme une base de $E[\ell^k]$. Ces travaux s'inspirent de ceux de [Hug13, Chapitre 6].

Notation 5.15. Soient E une courbe elliptique, P, Q deux points tels que $E[\ell^k] = \langle P, Q \rangle$ on note alors $\pi(P, Q)$ la représentation matricielle de l'action

du Frobenius dans la base (P, Q). Ainsi dans ce document nous avons pris la convention que :

$$\pi(P, Q) = \begin{pmatrix} \lambda & a \\ 0 & \mu \end{pmatrix}$$

signifie que l'on a $\pi(P) = [\lambda]P$ et $\pi(Q) = [a]P + [\mu]Q$.

Proposition 5.16. Soit E une courbe elliptique située au niveau $h - e$ d'un volcan des ℓ-isogénies pour lequel ℓ est un nombre de Elkies. Soient $P, R \in E$ tels que $\langle P, R\rangle = E[\ell^{h-e+i}]$ et $\pi(P, R) = \begin{pmatrix} \lambda & \beta\ell^{h-e} \\ 0 & \mu \end{pmatrix} \bmod \ell^{h-e+i}$ avec $\beta \wedge \ell = 1$, alors pour toute ℓ^i-isogénie descendante ϕ de domaine E il existe une base $\langle P, R'\rangle$ de $E[\ell^{h-e+i}]$ telle que $\ker(\phi) = \langle R'\rangle$ et $\pi(P, R) = \pi(P, R')$.

Démonstration. À l'aide du changement de base $(P, R) \to ([\beta^{-1}]P, R)$ nous supposons sans perte de généralités que $\beta = 1$. Soit $Q \in E$ tel que $\langle P, Q\rangle = E[\ell^{h-e+i}]$. Alors nous posons $R = [a]P + [b]Q$ et nous allons montrer qu'il existe une transformation

$$R = [a]P + [b]Q \mapsto R' = [c]P + [yb]Q$$

telle que $\pi(P, R) = \pi(P, R')$ et $\langle[\ell^{h-e}]R'\rangle = \ker(\phi)$.
Par la forme de la matrice $\pi(P, R)$ nous avons :

$$\pi([a]P + [b]Q) = [\ell^{h-e}]P + [\mu]([a]P + [b]Q).$$

De plus, comme π est un morphisme $\pi([a]P + [b]Q) = [a\lambda]P + [b]\pi(Q)$, nous déduisons l'expression suivante pour $[b]\pi(Q)$:

$$[b]\pi(Q) = [\ell^{h-e} + (\mu - \lambda)a]P + [\mu b]Q.$$

Nous avons alors $\pi([c]P+[by]Q) = [c\lambda]P+[y]([b]\pi(Q))$. La condition $\pi(P, R') = \pi(P, R)$ est vérifiée si et seulement si :

$$\begin{aligned} \pi([c]P + [by]Q) &= [\ell^{h-e}]P + [\mu]([c]P + [by]Q) \\ &= [\lambda c]P + [y]([\ell^{h-e} + (\mu - \lambda)a]P + [\mu b]Q). \end{aligned}$$

Cela se traduit donc par l'égalité suivante :

$$\ell^{h-e} + c(\mu - \lambda) = y(\ell^{h-e} + (\mu - \lambda)a) \bmod \ell^{h-e+i}.$$

Ainsi nous faisons une distinction selon que $h - e + i \leqslant h$ ou $h - e + i > h$, car $\ell^h || \lambda - \mu$.

$h - e + i \leqslant h$ Dans ce cas nous obtenons l'équation suivante :

$$\ell^{h-e} = y\ell^{h-e} \bmod \ell^{h-e+i},$$

et donc la valeur de la matrice ne dépend que de y. Or la ℓ^i-isogénie de noyau $\langle \ell^{h-e}R'\rangle = \langle[\ell^{h-e}]([c(by)^{-1}]P + Q)\rangle$ est déterminée par la valeur de $\ell^{h-e}b^{-1}y^{-1}c \bmod \ell^{h-e+i}$, ainsi en faisant varier la valeur de c nous pouvons faire en sorte que $[\ell^{h-e}]R'$ soit le générateur de n'importe quelle ℓ^i-isogénie descendante.

$h-e+i>h$ Montrons dans ce cas comment déterminer y et c tels que $\ell^{h-e}\gamma = \ell^{h-e}c(by)^{-1} \bmod \ell^{h-e+i}$, avec $\ell^{h-e}\gamma \bmod \ell^{h-e+i}$ qui détermine une ℓ^i-isogénie descendante spécifique (celle de noyau $\langle[\ell^{h-e}]([\gamma]P+Q)\rangle$). Nous posons $\ell^h\alpha = \lambda - \mu$ avec $\alpha \wedge \ell = 1$, l'égalité $\pi(P,R) = \pi(P,R')$ se traduit donc par :

$$\ell^{h-e} + \ell^h \alpha c = y(\ell^{h-e} + \ell^h(\alpha)a) \bmod \ell^{h-e+i},$$

nous multiplions alors cette équation par $(by)^{-1}$

$$\begin{aligned} \ell^{h-e}(by)^{-1} + \ell^e\alpha\ell^{h-e}\gamma &= b^{-1}(\ell^{h-e} + \ell^h(\alpha)a) \bmod \ell^{h-e+i} \\ \ell^{h-e}(by)^{-1} &= b^{-1}(\ell^{h-e} + \ell^h(\alpha)a) - \ell^e\alpha\ell^{h-e}\gamma \bmod \ell^{h-e+i} \end{aligned}$$

Nous pouvons alors déterminer y puis c afin d'avoir une transformation pour laquelle nous obtenons un point R' tel que $[\ell^{h-e}]R'$ soit un générateur de l'isogénie spécifiée par $\ell^{h-e}\gamma \bmod \ell^{h-e+i}$.

□

On voit donc que l'on n'est pas capable de distinguer les isogénies descendantes entre elles dans un volcan de ℓ-isogénies, quand ℓ est un nombre premier de Elkies. En effet pour toute forme de matrice du Frobenius triangulaire observée on est capable de trouver pour chacune des différentes ℓ-isogénies descendantes un second point de la base qui engendre cette isogénie et pour lequel l'action du Frobenius est identique dans cette base.

5.1.2 Calcul des directions dans le volcan de ℓ-isogénies

Dans cette sous-section on s'intéresse à la partie algorithmique du calcul des objets présentés dans la sous-section 5.1.1. Sont aussi utilisés les résultats et définitions du chapitre 3, dont notamment les extensions de corps de la définition 3.1.

Étude de la rationalité de la ℓ^k-torsion dans une tour d'extensions ℓ-adique

On va maintenant étudier la structure de la torsion rationnelle des courbes elliptiques ordinaires, et déterminer l'extension de corps nécessaire pour avoir une torsion ℓ-adique de valuation fixée. On va en particulier étudier cela pour une courbe située sur le cratère d'un volcan de ℓ-isogénies, car c'est à ce niveau du volcan que l'on peut calculer les points horizontaux. Pour les courbes inférieures dans le volcan, le corollaire 5.20 permet de conclure.

Définition 5.17. On introduit la notation suivante afin de spécifier la structure de la ℓ-torsion sur une extension de $\mathsf{F}_1/\mathbb{F}_q$ où l'on aurait $E[\ell] \subset E(\mathsf{F}_1)$.

— Pour ℓ premier impair, on note $\alpha = v_\ell(\lambda^{\ell-1} - 1)$ et $\beta = v_\ell(\mu^{\ell-1} - 1)$;

— pour $\ell = 2$, on note $\alpha = v_2(\lambda^2 - 1) - 1$ et $\beta = v_2(\mu^2 - 1) - 1$;

on suppose sans perte de généralité que $\alpha \geqslant \beta$. On s'intéresse à ces valeurs-là, car pour n'importe quel corps fini $\mathbb{F}_q$, on a $E[\ell] \subset E(\mathbb{F}_q^{\ell-1})$ pour $\ell \neq 2$ et $E[4] \subset E(\mathbb{F}_q^2)$ pour $\ell = 2$.

Remarque 5.18. Comme $\lambda \neq \mu \bmod \ell^{h+1}$ et que $\lambda = \mu \bmod \ell^h$, il est impossible que $\lambda^{\ell-1} \equiv \mu^{\ell-1} \equiv 1 \bmod \ell^{h+1}$, ainsi au moins une des deux valuations α, β est $\leqslant h$, par conséquent on va supposer sans perte de généralité que $\beta \leqslant h$.

Proposition 5.19. Soit E une courbe elliptique ordinaire telle que son anneau des endomorphismes soit maximal par rapport à ℓ. Pour tout k, on note d_k le degré de la plus petite extension de corps $F/\mathbb{F}_q$ telle que $E[\ell^k] \subset E(F)$. On a alors :

1. l'ordre de q dans $(\mathbb{Z}/\ell\mathbb{Z})^\times$ divise d_1, et d_1 divise $(\ell-1)$.
2. Si ℓ est impair alors pour tout $k > 1$, $d_k = \ell^{\max(v_\ell(d_1),k-\beta)} d_1$.
3. Si $\ell = 2$ alors $d_2 \in \{1, 2\}$ et pour tout $k > 2$, $d_k = \ell^{\max(0,k-\beta)} d_2$.
4. Soit $[F : \mathbb{F}_q] = d_1\ell^n$, le groupe $E[\ell^\infty](F)$ est isomorphe à $(\mathbb{Z}/\ell^{n+\alpha}\mathbb{Z}) \times (\mathbb{Z}/\ell^{n+\beta}\mathbb{Z})$.
5. Le groupe $E[\ell^k]$ contient au plus $k \cdot \ell^{k+\beta}$ classes de conjugaisons selon l'action de $\mathsf{Gal}(\mathsf{F}_{k-\beta} : \mathsf{F}_1)$ avec $\mathsf{F}_1 = \mathbb{F}_{q^{d_1}}$.

Démonstration. Le degré d_k correspond à l'ordre de la matrice $\pi|E[\ell^k]$. d_k est donc le plus petit multiple commun des ordres multiplicatifs de λ, μ modulo ℓ^k, on obtient donc (1) en utilisant le fait que $\lambda \cdot \mu = q$. Pour les points (2)–(5) on suppose sans perte de généralité que l'on a $d_1 = 1$, alors pour tout entier N, $v_\ell(\lambda^{2N} - 1) = \alpha + v_\ell(2N)$. Soit (P, Q) une base diagonale de $E[\ell^k]$, le point $(\pi^N - 1)([x]P + [y]Q) = [(\lambda^N - 1)x]P + [(\mu^N - 1)y]Q$ est nul si et seulement si $v_\ell(x) + \alpha + v_\ell(N) \geq k$ et $v_\ell(y) + \beta + v_\ell(N) \geq k$, cela montre (4). Les plus grandes classes de Galois sont celles pour lesquelles on a $v_\ell(y) = 0$ et leur taille est $\ell^{k-\beta}$, ce qui prouve (2) et (3). De plus, pour tout $i \leq k - \beta$ les points dans une orbite de taille $\leqslant \ell^i$ sont ceux pour lesquels $v_\ell(x) \geqslant k - \alpha - i$ et $v_\ell(y) \geqslant k - \beta - i$; il y a au plus $\ell^{\min(\alpha+i,k)+\min(\beta+i,k)}$ tels points, par conséquent il y a $\ell^{\min(\alpha+i,k)+\min(\beta,k-i)} \leqslant \ell^{k-i+\beta}$ classes correspondantes. En additionnant ce résultat pour tous les i on prouve (5). □

Maintenant voyons le lien entre β et h la hauteur du volcan selon que celui-ci soit régulier ou non.

Corollaire 5.20. Soit E une courbe elliptique, ℓ un nombre premier de Elkies, et supposons que l'anneau des endomorphismes de E est localement maximal par rapport à ℓ. Soit $\mathsf{F}_1/\mathbb{F}_q$ la plus petite extension de corps telle que $E[\ell] \subset E[\mathsf{F}_1]$. Le volcan des ℓ-isogénies définies sur F_1 contenant E est *régulier* si et seulement si $\beta = h$. Lorsque le volcan est *non-régulier*, β est égal au premier niveau de stabilité.

Démonstration. Lorsque le volcan est régulier, par la proposition 4.31, la valuation ℓ-adique du plus petit sous-groupe de Sylow de la ℓ-torsion augmente de 1 à chaque fois que l'on monte d'un niveau dans le volcan. Sachant que au niveau en bas du volcan $E(\mathsf{F}_1)[\ell^\infty]$ est cyclique, on déduit que $\beta = h$.

Le raisonnement est le même pour un volcan non-régulier car au-dessus du premier niveau de stabilité la structure de la ℓ-torsion ne change pas, et en dessous elle change comme décrit juste au-dessus. □

Algorithmes pour le calcul des directions dans le volcan de ℓ-isogénies

L'objectif de cette sous-section est de calculer, pour une courbe se trouvant sur un volcan de ℓ-isogénies une base horizontale (ou ascendante horizontale) de la ℓ^k-torsion. On a vu à la proposition 5.8 que l'on devait avoir $k \geqslant h+1$ avec h la hauteur du volcan afin de pouvoir déterminer une ℓ-isogénie horizontale car sinon on ne peut distinguer l'action du Frobenius sur les espaces propres. On

rappelle aussi que β représente la plus grande valuation ℓ-adique de la ℓ-torsion rationnelle pour une courbe située sur le cratère du volcan de ℓ-isogénies(voir définition 5.17).

On commence tout d'abord par énoncer un algorithme qui sera utilisé dans tous les autres par la suite c'est le calcul d'un antécédent à la multiplication par ℓ d'un point P, on note cette application $\mathsf{divise}(\ell, P)$. Ce résultat sera aussi utilisé dans le cas Atkin (voir sous-section 5.2.2).

Lemme 5.21. Soit P un point de E tel que $P \in E(\mathsf{F}_n)$, alors le coût moyen de calcul de $E(\mathsf{F}_1)[\ell]$ est de $O(\ell \mathsf{M}(\ell^2)\log(\ell)\log(\ell q))$. Le coût de calcul de $\mathsf{divise}(\ell, P)$ est de $O(\mathsf{R}(n+1))$ lorsque $E[\ell](\mathsf{F}_1)$ a déjà été calculé. Ces coûts sont des coûts moyens.

Démonstration. $E[\ell](\mathsf{F}_1)$ est calculé en factorisant le polynôme de ℓ-division avec un coût moyen de $O(\ell \mathsf{M}(\ell^2)\log(\ell)\log(\ell q))$ opérations, en utilisant la variante de l'algorithme de Cantor-Zassenhaus décrite dans [vzGG03, Chapter 14.5]. Une fois que $E[\ell](\mathsf{F}_1)$ a été calculé, on peut factoriser la multiplication par ℓ par un produit de deux ℓ-isogénies. Ainsi on calcule un antécédent d'un point par la multiplication par ℓ en calculant successivement des antécédents de ce point P par les ℓ-isogénies qui composent la multiplication par ℓ. Pour calculer ces antécédents on a donc besoin de calculer les racines d'un polynôme de degré ℓ, ainsi le coût de $\mathsf{divise}(\ell, P)$ est de $O(\mathsf{R}(n))$, d'après la définition de $R(i)$ (voir notation 3.9 dans chapitre 3). □

Avant de présenter l'algorithme 7 qui, pour une courbe E située au niveau $h-e$, calcule une base diagonale de la $E_s[\ell^k]$-torsion (avec E_s la courbe sommet de E voir définition 4.25) nous présentons tout d'abord des algorithmes qui composent celui-ci. Ainsi nous présentons tout d'abord l'algorithme 5 qui calcule une base diagonale de $E_s[\ell^{h+1}]$ à partir d'une base triangulaire de $E[\ell^{h-e+1}]$, pour $e > 0$ et E située au niveau $h - e$. Mais avant cela nous rappelons un résultat sur la rationalité des points et leur niveau dans le volcan de ℓ-isogénies.

Remarque 5.22. Dans le cas des volcans réguliers, la hauteur du volcan de ℓ-isogénies n'a pas d'influence sur le coût des algorithmes qui remontent dans le volcan (tels 5, 7). En effet par la proposition 4.31, lorsque l'on monte d'un niveau dans le volcan de ℓ-isogénies, la valuation ℓ-adique de la torsion rationnelle des points de la courbe augmente de 1. De plus comme on a uniquement besoin de travailler avec la ℓ^{h-e+1}-torsion, pour une courbe située au niveau $h - e$, pour déterminer la ℓ-isogénie montante (voir proposition 5.5) alors on travaille avec des points définis dans F_2. Par conséquent pour travailler avec une plus grande ℓ-torsion rationnelle, que $E[\ell^h]$, on privilégiera de monter de niveaux dans le volcan afin d'éviter de travailler avec des extensions de corps supplémentaires. Le lemme 5.24 en est une illustration.

On présente donc tout d'abord l'algorithme 5 qui, à partir d'une base de $E[\ell^{h-e+1}]$ située au niveau $h - e$ dans laquelle l'action du Frobenius est triangulaire, calcule une base diagonale de $E_s[\ell^{h+1}]$.

Afin de permettre au lecteur de se rendre compte du niveau dans le volcan auquel les points et les courbes sont définis on introduit la notation suivante :

Notation 5.23. Soit $P \in E$ avec E située au niveau $h - e + i$ d'un volcan des ℓ-isogénies, alors on notera $P^{(h-e+i)}$ et $E^{(h-e+i)}$ pour signifier que le point et la courbe sont définis au niveau $h - e + i$ du volcan des ℓ-isogénies.

Cette notation étant très lourde elle ne sera utilisée que lorsque le niveau auquel ces objets sont définis n'est pas évident.

Avant d'énoncer et démontrer la complexité de l'algorithme 5, il y a un résultat important et intéressant de l'algorithme qui sera énoncé ici afin d'éviter de surcharger la preuve.

Lemme 5.24. Dans l'algorithme 5, avec comme entrée une courbe située en dessous du cratère d'un volcan de ℓ-isogénies, les points utilisés et calculés entre les étapes 3 et 18 sont définis dans $\mathsf{F}_{h-(e-i)+1-\beta+\max(0,e-i-(h-\beta))}$.

Démonstration. Lors de la boucle $h-e+i$ qui commence à l'étape 3 et se termine à l'étape 18 les points $P_{h-e+i+1}^{(h-e+i)}$ et $Q_{h-e+i+1}^{(h-e+i)}$ situés sur une courbe au niveau $h-(e-i)$ sont d'ordre $\ell^{h-e+i+1}$ et définis dans $\mathsf{F}_{h-(e-i)+1-\beta+\max(0,e-i-(h-\beta))}$ par la proposition 4.31 (*i.e.* F_1 lorsque $h=\beta$ et $\mathsf{F}_{h-\beta-(e-i)+1}$ lorsque $h-\beta > e-i$). En particulier, les antécédents par $[\ell]$ de $P_{h-e+i+1}^{(h-e+i)}$ d'ordre ℓ^{h+1} sont définis dans $\mathsf{F}_{h-e+i+1-\beta+\max(0,e-i-(h-\beta))}$. Or cette boucle s'arrête lorsque l'on atteint la ℓ^{h+1} torsion pour la courbe au niveau h du cratère, les opérations $\mathsf{divise}(\ell, P')$ et $\pi(P') = [u]P' + [v]Q'$ sont donc toujours faites dans $\mathsf{F}_{h-e+i+1-\beta+\max(0,e-i-(h-\beta))}$. De même pour les points Q', car à l'étape 10 on transporte la base sur une courbe située un niveau au-dessus dans le volcan, et dès lors les points de ℓ-division de $\widehat{\varphi}(Q_{h-e+i+1}^{(h-e+i)})$ sont aussi définis dans $\mathsf{F}_{h-e+i+1-\beta+\max(0,e-i-(h-\beta))}$. Ainsi on vérifie bien qu'à la fin de la boucle on a des points d'ordre $\ell^{h-e+i+2}$ définis sur une courbe au niveau $h-(e-i)+1$ et donc encore définis dans $\mathsf{F}_{h-e+i+1-\beta+\max(0,e-i-(h-\beta))}$. □

Maintenant on présente l'algorithme 5 qui prend en entrée une courbe elliptique E située au niveau $h-e$ dans le volcan des ℓ-isogénies et qui retourne une base diagonale de $E_s[\ell^{h+1}]$ ainsi que la liste de ℓ-isogénies montantes qui permettent de relier E à sa courbe sommet E_s.

Proposition 5.25. L'algorithme 5 est correct et a une complexité moyenne de

$$O(\max(0,e-(h-\beta))(\mathsf{R}(1)+\ell^1\mathsf{M}(\ell)+\ell^2\mathsf{M}(\ell^1))+\mathsf{R}(h+1)+\ell^{h+1}\mathsf{M}(\ell)+\ell^2\mathsf{M}(\ell^{h+1}))$$

opérations sur $\mathbb{F}_q$.

Démonstration. Des calculs matriciels directs montrent que les changements de base aux étapes 14 7 permettent de trigonaliser la matrice. De même le changement de base à l'étape 20 permet de diagonaliser la matrice. À l'étape 9 la ℓ-isogénie construite est bien montante par la proposition 5.5. Enfin la matrice représentant l'action du Frobenius sur une base de $E[\ell^{h-e+1}]$ pour E au niveau $h-e+i$ est trigonalisable par la proposition 5.3. De même, au niveau h, l'action du Frobenius sur une base de $E_s[\ell^{h+1}]$ est diagonalisable par la proposition 5.3.

Analysons maintenant la complexité de l'algorithme. Entre les étapes 3 et 18 on calcule à chaque boucle une base de la ℓ^{h-e+i}-torsion dans laquelle l'action du Frobenius est triangulaire, et l'on remonte d'un niveau dans le volcan et l'on trigonalise la $\ell^{h-e+i+1}$ torsion. Cette étape est répétée du niveau $h-e$, où l'on exprime l'action du Frobenius dans une base de la ℓ^{h-e+1} torsion, au niveau h, où l'on exprime l'action du Frobenius dans une base de la ℓ^{h+1} torsion. Par le lemme 5.24 les points avec lesquels on travaille sont toujours définis dans le même corps $\mathsf{F}_{h-(e-i)+1-\beta+\max(0,e-i-(h-\beta))}$. Ainsi le coût des étapes 10 et 15 est de $\mathsf{R}(h-(e-i)+1-\beta+\max(0,e-i-(h-\beta)))$. Pour le calcul de

Algorithme 5 Calcul d'une base diagonale de $E_s[\ell^{h+1}]$ à partir d'une base triangulaire de $E[\ell^{h-e+1}]$ pour E au niveau $h-e$

Entrée : E : une courbe elliptique ordinaire située au niveau $h-e$ d'un volcan de ℓ-isogénies ; $P, Q \in E, \lambda, \mu, b \in \mathbb{Z}/\ell^{h-e+1}\mathbb{Z}$ tels que $E[\ell^{h-e+1}] = \langle P, Q\rangle$, $\pi(P,Q) = \begin{pmatrix} \lambda+a\ell^{h-e+1} & b\ell^{h-e+1} \\ c\ell^{h-e+i} & \mu+d\ell^{h-e+1}\end{pmatrix}$;

Sortie : (P_h, Q_h) : une base de $E_s[\ell^{h+1}]$; $\lambda, \mu \in \mathbb{Z}/\ell^{h+1}\mathbb{Z}$ tels que $\pi|(P_h,Q_h) = \left(\begin{smallmatrix}\lambda & 0\\ 0 & \mu\end{smallmatrix}\right) \bmod \ell^{h+1}$; L une liste de ℓ-isogénies montantes reliant E à E_s.

1: $(i, \delta) \leftarrow (0,0)$
2: **si** $b = 0$ **alors** $(P, Q, a, b, c, d) \leftarrow (Q, P, d, c, b, a)$; **fin si**.
3: **tant que** $v_\ell(\lambda - \mu) = v_\ell(\delta)$ **faire**
4: $\quad \delta \leftarrow \delta + b\ell^{h-e+i}$
5: $\quad$ **si** $c = 0$ **alors** $y \leftarrow 0$;
6: $\quad$ **sinon** résoudre equation $y^2\delta\ell + y(\ell^{h-e+i}(a-d) + \lambda - \mu) - c\ell^{h-e+i}$; **fin si**.
7: $\quad P^{(h-e+i)}_{h-e+i+1} \leftarrow P' + [y]Q'$; $Q^{(h-e+i)}_{h-e+i+1} \leftarrow Q'$.
8: $\quad \lambda \leftarrow \lambda + a\ell^{h-e+i} + \delta y$; $\mu \leftarrow \mu + d\ell^{h-e+i} - \delta y$;
9: $\quad \widehat{\varphi} \leftarrow$ isogénie montante de noyau $\langle [\ell^{h-e+i}] P^{(h-e+i)}_{h-e+i+1}\rangle$
10: $\quad P' \leftarrow \mathsf{divise}\left(\ell, \widehat{\varphi}\left(P^{(h-e+i)}_{h-e+i+1}\right)\right)$; $Q' \leftarrow \widehat{\varphi}\left(Q^{(h-e+i)}_{h-e+i+1}\right)$; $L \leftarrow L \bigcup \widehat{\varphi}$.
11: $\quad$ Calcul $\pi|(P', Q') = \begin{pmatrix} \lambda+a\ell^{h-e+i} & \ell\delta \\ c\ell^{h-e+i} & \mu+d\ell^{h-e+i}\end{pmatrix} \bmod \ell^{h-e+i+1}$.
12: $\quad$ **si** $c = 0$ **alors** $y \leftarrow 0$;
13: $\quad$ **sinon** résoudre équation $y^2\delta\ell + y(\ell^{h-e+i}(a-d) + \lambda - \mu) - c\ell^{h-e+i}$; **fin si**.
14: $\quad P' \leftarrow P' + [y]Q'$; $\lambda \leftarrow \lambda + a\ell^{h-e+i} + \delta y, \mu \leftarrow \mu + d\ell^{h-e+i} - \delta y$.
15: $\quad P' \leftarrow \mathsf{divise}(\ell, P')$; $Q' \leftarrow \mathsf{divise}(\ell, Q')$; $\delta \leftarrow \ell\delta$.
16: $\quad i \leftarrow i + 1$.
17: $\quad$ calcul $\pi|(P', Q') = \begin{pmatrix} \lambda+a\ell^{h-e+i} & b\ell^{h-e+i}+\delta \\ c\ell^{h-e+i} & \mu+d\ell^{h-e+i}\end{pmatrix} \bmod \ell^{h-e+i+1}$.
18: **fin tant que**
19: résoudre équation $\delta + x(\lambda - \mu) = 0$;
20: $Q^{(h)}_{h+1} \leftarrow Q^{(h)}_{h+1} + [x]P^{(h)}_{h+1}$
21: **retourner** $P^{(h)}_{h+1}, Q^{(h)}_{h+1}, \lambda \bmod \ell^{h+1}, \mu \bmod \ell^{h+1}, L$

$E^{(h-e+i)}[\ell]$ il est à noter qu'il est tout à fait vraisemblable de supposer que l'on connaît déjà une base de $E^{(h-e+i-1)}[\ell]$, car à chaque étape le coût de détermination d'une telle base peut se faire à l'aide d'une évaluation de la ℓ-isogénie montante sur un point d'ordre ℓ^2 et un point d'ordre ℓ définis sur $E^{(h-e+i-2)}$. Le coût de calcul de $\pi(P)$ est de $O(\ell^{h-(e-i)+1-\beta+\max(0,e-i-(h-\beta))}\mathsf{M}(\ell))$ par le théorème 3.6 . L'écriture de $\pi(P) = [u]P + [v]Q$ aux étapes 11 et 17 a un coût de $O(\ell^2\mathsf{M}(\ell^{h-(e-i)+1-\beta+\max(0,e-i-(h-\beta))}))$. Lors de la boucle $h-e+i$, les étapes 6 et 13 sont résolues à l'aide d'une recherche exhaustive et ont un coût négligeable par rapport aux autres opérations.

L'algorithme 5 a donc une complexité moyenne de $O(\sum_{i=0}^{e}(\mathsf{R}(\bigstar)+\ell^{\bigstar}\mathsf{M}(\ell)+\ell^2\mathsf{M}(\ell^{\bigstar})))$ opérations sur $\mathbb{F}_q$ avec $\bigstar = h-\beta-(e-i)+1+\max(0,e-i-(h-\beta))$. En particulier en décomposant la complexité selon le premier niveau de stabilité la complexité s'écrit : $O(\max(0,e-(h-\beta))(\mathsf{R}(1)+\ell^1\mathsf{M}(\ell)+\ell^2\mathsf{M}(\ell^1))+\sum_{i=e-\beta}^{e}(\mathsf{R}(\bigstar)+\ell^{\bigstar}\mathsf{M}(\ell)+\ell^2\mathsf{M}(\ell^{\bigstar}))$ or chacun des termes de $\sum_{i=e-\beta}^{e}(\mathsf{R}(\bigstar)+\ell^{\bigstar}\mathsf{M}(\ell)+\ell^2\mathsf{M}(\ell^{\bigstar}))$ a une complexité géométrique c'est donc la dernière itération qui domine la complexité et donne le résultat □

On énonce maintenant l'algorithme 6 qui fait partie de l'algorithme 7 et calcule une base diagonale de $E_s[\ell^k]$ à partir d'une base diagonale de $E_s[\ell^j]$ pour $j < k$.

Algorithme 6 Calcul d'une base diagonale de $E_s[\ell^k]$

Entrée : E_s : une courbe elliptique ordinaire située sur le cratère d'un volcan de ℓ-isogénies ; k : un entier positif ; $j < k$; $\lambda, \mu \in \mathbb{Z}/\ell^j\mathbb{Z}$; P_j, Q_j tels que $E_s[\ell^j] = \langle P_j, Q_j\rangle$ $\pi(P_j) = [\lambda]P_j, \pi(Q_j) = [\mu]Q_j$;

Sortie : (P_k, Q_k) : une base de $E_s[\ell^k]$; $\lambda, \mu \in \mathbb{Z}/\ell^k\mathbb{Z}$ tels que $\pi(P_k) = [\lambda]P_k$, $\pi(Q_k) = [\mu]Q_k$.

1: **pour** $i = j$ à $k-1$ **faire**
2: $P' \leftarrow \mathsf{divise}(\ell, P_i)$; $Q' \leftarrow \mathsf{divise}(\ell, Q_i)$.
3: Calcul $\pi|(P', Q') = \begin{pmatrix} \lambda+a\ell^i & b\ell^i \\ c\ell^i & \mu+d\ell^i \end{pmatrix} \bmod \ell^{i+1}$.
4: **si** $b = 0$ **alors** $x \leftarrow 0$; résoudre équation $c\ell^i + ((d-a)\ell^i + \mu - \lambda)y = 0$;
5: **sinon** résoudre équation $c\ell^i x^2 + ((d-a)\ell^i + \mu - \lambda)x - b\ell^i = 0$; $y \leftarrow -cx/b$; **fin si**.
6: $P_{i+1} \leftarrow P' + [y]Q'$; $Q_{i+1} \leftarrow [x]P' + Q'$.
7: $\lambda \leftarrow \lambda + \ell^i(a + bx)$; $\mu \leftarrow \mu + \ell^i(d + cy)$.
8: **fin pour**
9: **retourner** (P_k, Q_k, λ, μ).

Proposition 5.26. L'algorithme 6 est correct et calcule une base diagonale de $E_s[\ell^k]$ avec une complexité espérée de

$$O(\mathsf{R}(k-\beta) + \ell^2\mathsf{M}(\ell^{k-\beta}) + \ell\mathsf{M}(\ell^2)\log(\ell)\log(\ell q))$$

opérations dans $\mathbb{F}_q$.

Démonstration. Un simple calcul permet de vérifier qu'à la fin de chaque boucle (P_{i+1}, Q_{i+1}) est diagonal. Une base de la $E[\ell^{h+i}]$ est diagonalisable par la proposition 5.3.

Nous analysons maintenant la complexité de l'algorithme. Pour $i = 0$, une base de $E[\ell](\mathsf{F}_1)$ à l'étape 2 est calculée en factorisant le polynôme de ℓ-division

à un coût espéré de $O(\ell \mathsf{M}(\ell^2)\log(\ell)\log(\ell q))$ opérations en utilisant l'algorithme de Cantor-Zassenhaus [vzGG03, Chapter 14.5]. Pour tout point P d'ordre ℓ^{i-1} défini dans $E(\mathsf{F}_{i-\beta-1})$, le calcul de $\mathsf{divise}(\ell, P)$ à l'étape 2 coûte $O(\mathsf{R}(i-\beta))$ opérations par le lemme 5.21. L'évaluation de $\pi(P')$ à l'étape 3, pour P' défini dans $\mathsf{F}_{i-\beta}$, a un coût de $O(\ell^{i-\beta}\mathsf{M}(\ell))$ par le théorème 3.6. Écrire $\pi(P')$ comme une combinaison linéaire $[u]P' + [v]Q'$ avec P', Q' définis dans $\mathsf{F}_{i-\beta}$ nécessite au plus ℓ^2 additions de points, avec un coût de $\ell^2\mathsf{M}(\ell^{i-\beta})$. L'équation à la ligne 4 ou 5 est tout d'abord divisée par la plus grande puissance de ℓ possible : $\ell^{\min(h,i)}$, elle est ensuite résolue modulo ℓ. Pour $i \leqslant h-1$, comme $a = d$ et $b = c = 0$, les solutions sont $x = y = 0$, et les étapes 4 à 6 ne font rien. Le coût de résolution des équations aux étapes 4 et 5 par recherche exhaustive est négligeable, comme les autres opérations restantes. Comme le coût de chaque boucle augmente de façon géométrique, la dernière boucle domine les autres, et donne la complexité annoncée. □

On énonce maintenant l'algorithme 7 qui avec pour entrée une courbe E calcule une base diagonale de $E_s[\ell^k]$ et une liste de ℓ-isogénies montantes reliant E à E_s.

Algorithme 7 Calcul d'une base diagonale de $E_s[\ell^k]$ à partir de E au niveau $h-e$

Entrée : E : une courbe elliptique ordinaire située sur un volcan de ℓ-isogénies avec cratère cyclique ; k : une entier positif ;

Sortie : (P_k, Q_k) : une base de $E_s[\ell^k]$; $\lambda, \mu, b \in \mathbb{Z}/\ell^k\mathbb{Z}$ tels que $\pi(P_k) = [\lambda]P_k$, $\pi(Q_k) = [\mu]Q_k$.

1: $(\lambda, \mu, i) \leftarrow (0,0,0)$; $L \leftarrow \emptyset$; $P', Q' \leftarrow$ tels que $\langle P', Q'\rangle = E[\ell]$.
2: calcul $\pi|(P', Q') = \begin{pmatrix} \lambda + a\ell^i & b\ell^i \\ c\ell^i & \mu + d\ell^i \end{pmatrix} \bmod \ell^{i+1}$.
3: **tant que** scalaire **faire**
4: $\quad i \leftarrow i+1$.
5: $\quad P_i \leftarrow P'$; $Q_i \leftarrow Q'$; $\lambda \leftarrow \lambda + a\ell^i$; $\mu \leftarrow \mu + a\ell^i$.
6: $\quad P' \leftarrow \mathsf{divise}(\ell, P_i)$; $Q' \leftarrow \mathsf{divise}(\ell, Q_i)$.
7: $\quad$ calcul $\pi|(P', Q') = \begin{pmatrix} \lambda + a\ell^i & b\ell^i \\ c\ell^i & \mu + d\ell^i \end{pmatrix} \bmod \ell^{i+1}$;
8: **fin tant que**
9: Calcul d'une base diagonale (P_{h+1}, Q_{h+1}) de $E_s[\ell^{h+1}]$, $\lambda, \mu \in \mathbb{Z}/\ell^{h+1}\mathbb{Z}$ tels que $\pi(P_{h+1}, Q_{h+1}) = \left(\begin{smallmatrix} \lambda & 0 \\ 0 & \mu \end{smallmatrix}\right) \bmod \ell^{h+1}$ et L à l'aide de l'algorithme 5 avec entrées $P', Q', \lambda, \mu, a, b, c, d$
10: Calcul d'une base diagonale de $E_s[\ell^k]$ à l'aide de l'algorithme 6 avec entrées P_h, Q_h, λ, μ
11: **retourner** $(P_k, Q_k, \lambda, \mu, L)$.

Proposition 5.27. L'algorithme 7 a une complexité moyenne de

$$O(\ell \mathsf{M}(\ell^2)\log(\ell)\log(\ell q) + \mathsf{R}(k-\beta) + \ell^2\mathsf{M}(\ell^{k-\beta}) + \mathsf{R}(h+1) + \ell^2\mathsf{M}(\ell^{h+1}))$$

opérations sur $\mathbb{F}_q$.

Démonstration. On analyse l'algorithme selon les 3 parties qui le composent :

1. La première partie, de l'étape 3 à 8, détermine l'action du Frobenius sur la ℓ^i-torsion et augmente la valuation ℓ-adique de la torsion sur laquelle on

travaille tant que l'action du Frobenius est scalaire. L'action du Frobenius est scalaire pour une courbe située au niveau $h-e$, sans diagonalisation, tant que l'on travaille avec la ℓ^{h-e}-torsion par la proposition 5.3.

2. La seconde partie, correspondant à l'étape 9, est l'application de l'algorithme 5 qui, à partir d'une base triangulaire de la ℓ^{h-e+1} torsion d'une courbe située au niveau $h-e$, calcule une base diagonale de $E_s[\ell^{h+1}]$ ainsi que la liste de ℓ-isogénies montantes reliant E à E_s.
3. La troisième et dernière partie correspond à l'étape 10 qui, à partir d'une base diagonale de $E_s[\ell^{h+1}]$, calcule une base diagonale de $E_s[\ell^k]$.

Analysons maintenant les complexités de ces différentes parties de l'algorithme.

Étapes 3 à 8 Pour une courbe E qui se trouve au niveau $h-e$, la première boucle de l'algorithme entre les étapes 3 et 8, celle où l'action du Frobenius est représentable à l'aide d'une matrice scalaire, dure jusqu'à ce que l'on travaille avec des points d'ordre ℓ^{h-e+1}. Ainsi cette première boucle est répétée $h-e+1$ fois. Pour une boucle i qui calcule l'action du Frobenius sur la ℓ^{i+1} torsion, les points d'ordre ℓ^{i+1} sont définis dans $\mathsf{F}_{i+1-\beta+\max(0,e-(h-\beta))}$ par la proposition 4.31, ainsi le coût de calcul de $\mathsf{divise}(\ell, P)$ appliqué à un tel point P à l'étape 6 est de $\mathsf{R}(i+1-\beta+\max(0,e-(h-\beta)))$ par le lemme 5.21. Le coût de calcul de $\pi(P)$ pour P défini dans $\mathsf{F}_{i+1-\beta+\max(0,e-(h-\beta))}$ est de $O(\ell^{i+1-\beta+\max(0,e-(h-\beta))}\mathsf{M}(\ell))$ par le théorème 3.6. L'écriture de $\pi(P) = [u]P$ pour P défini dans $\mathsf{F}_{i+1-\beta+\max(0,e-(h-\beta))}$ a un coût de $O(\ell\mathsf{M}(\ell^{i+1-\beta+\max(0,e-(h-\beta))}))$ (on se limite à ce cas là car on est dans le cas où la matrice représentant l'action du Frobenius est scalaire). Comme le coût de chaque boucle grandit géométriquement, c'est la dernière qui domine et donne la complexité. Ainsi cette première partie de l'algorithme a un coût total de $O(\mathsf{R}(h-\beta-e+1+\max(0,e-(h-\beta))+\ell^{h-\beta-e+1+\max(0,e-(h-\beta)}M(\ell)+\ell\mathsf{M}(\ell^{h-\beta-e+1+\max(0,e-(h-\beta)}))$, auquel il faut ajouter le coût de calcul de la base de la ℓ-torsion : $O(\ell\mathsf{M}(\ell^2)\log(\ell)\log(\ell q))$.

Étape 9 Par la proposition 5.25 cette étape a une complexité de

$$O\Big(\max(0,e-(h-\beta))(\mathsf{R}(1)+\ell^1\mathsf{M}(\ell)+\ell^2\mathsf{M}(\ell^1))+ \mathsf{R}(h+1)+\ell^{h+1}\mathsf{M}(\ell)+\ell^2\mathsf{M}(\ell^{h+1})\Big).$$

Étape 10 Par la proposition 5.26, cette étape a un coût de $O(\mathsf{R}(k-\beta)+\ell^{k-\beta}\mathsf{M}(\ell)+\ell^2\mathsf{M}(\ell^{k-\beta}))$ opérations sur $\mathbb{F}_q$.

□

Une fois que l'on a calculé une base diagonale (P,Q) de la ℓ^k torsion pour $k>h$, on connaît (par la proposition 5.8) deux points horizontaux de directions opposées et d'ordre ℓ^{k-h}, à savoir $[\ell^h]P, [\ell^h]Q$. On va donc maintenant se servir de la proposition 5.9 pour concevoir un algorithme qui nous donne des points horizontaux sur le cratère.

Proposition 5.28. Soit E une courbe située sur le cratère d'un volcan de ℓ-isogénies dont on connaît une base diagonale de la ℓ^{h+1} torsion alors pour $k \geqslant h+1$ l'algorithme 8 est correct et calcule un point horizontal avec un coût moyen de $O(\mathsf{R}(k-\beta)+k\mathsf{R}(h-\beta+1)+k\ell^2\mathsf{M}(\ell^{h-\beta+1}))$ opérations dans $\mathbb{F}_q$.

Algorithme 8 Calcul d'un point horizontal d'ordre ℓ^k

Entrée : (P_0, Q_0) : une base diagonale de $E[\ell^{h+1}]$; k : un entier, $k \geqslant h+1$.
Sortie : R : un point horizontal de $E[\ell^k]$ avec direction λ.

1: **pour** $i = 1$ to $k-1$ **faire**
2: $\quad \psi_i \leftarrow$ isogénie de noyau $\langle [\ell^h] P_{i-1} \rangle$
3: $\quad Q_i \leftarrow \psi_i(Q_{i-1})$
4: $\quad P' \leftarrow \mathsf{divise}(\ell, \psi_i(P_{i-1}))$.
5: $\quad$ Écrire $\pi(P') = [\lambda]P' + [c\ell^h]Q_i$ pour $c \in \mathbb{Z}/\ell\mathbb{Z}$
6: $\quad y$ solution de $c + y(\lambda - \mu) = 0$
7: $\quad P_i \leftarrow P' + [y\ell^h]Q_i$.
8: **fin pour**
9: **retourner** $R = \widehat{\psi}_1 \circ \ldots \circ \widehat{\psi}_{k-1}(\mathsf{divise}(\ell^{k-(h+1)}, P_{k-1}))$.

Démonstration. Soit E_i le codomaine de ψ_i. Un simple calcul montre qu'à l'itération i de la boucle, les points (P_i, Q_i) forment un base diagonale de $E_i[\ell^{h+1}]$, et ψ_i a direction λ. Le fait que R est horizontal est une conséquence de la proposition 5.9. Les deux opérations les plus coûteuses des boucles sont les étapes 4 et 5, coûtant respectivement $O(\mathsf{R}(h - \beta + 1))$ et $O(\ell^2\mathsf{M}(\ell^{h-\beta+1}))$, comme dit dans la preuve de la Proposition 5.26. Elles sont répétées k fois. Enfin, l'étape 9 est dominée par la dernière opération divise qui coûte $O(\mathsf{R}(k-\beta))$. □

Remarque 5.29. Ce résultat est à comparer avec le calcul de point horizontal d'ordre ℓ^k à l'aide d'une base de la la ℓ^{k+h}-torsion (voir proposition 5.8). Par exemple, pour une courbe située sur le cratère, à l'aide de l'algorithme 6 on obtiendrait un point horizontal d'ordre ℓ^k avec une complexité moyenne de : $O(\mathsf{R}((k+h)-\beta) + \ell^2\mathsf{M}(\ell^{k+h-\beta}) + \ell\mathsf{M}(\ell^2)\log(\ell)\log(\ell q)$.

Proposition 5.30. Soit E une courbe située au niveau $h-e$ dans un volcan de ℓ-isogénies, soit E_s sa courbe sommet, dont on connaît un point horizontal P_h d'ordre ℓ^k. Soit $\varphi_s : Es \to E$ la ℓ^e isogénie descendante, dont on connaît une décomposition en e ℓ-isogénies descendantes : $\varphi = \varphi_1 \circ \cdots \circ \varphi_e$. Alors le coût de calculer $\varphi(P)$ est de $O(e\mathsf{M}(\ell^{k-\beta+1}))$ opérations sur $\mathbb{F}_q$.

Démonstration. On rappelle que si $P \in \mathsf{F}_{k-\beta}$ point horizontal, alors $\varphi(P) \in \mathsf{F}_{k-\beta}$. Le coût de l'évaluation d'une isogénie rationnelle de degré ℓ sur un point $P \in \mathsf{F}_{k-\beta}$ étant de $O(\mathsf{M}(\ell^{k-\beta+1}))$ opérations sur $\mathbb{F}_q$, on obtient le résultat. □

Remarque 5.31. Il est normal que dans le coût de la proposition 5.30 on ne prenne pas en compte le calcul des isogénies descendantes φ_i, car, si l'on veut calculer un point ascendant horizontal pour une courbe non située sur le cratère, alors il est raisonnable de penser que l'un des deux algorithmes 5 ou 7 a été utilisé pour obtenir une base diagonale pour la courbe située sur le cratère, ainsi on peut calculer les duales des isogénies φ_i dans l'algorithme 5 ou 7.

5.2 Cas Atkin

Dans cette section nous nous intéressons au cas particulier suivant :

Définition 5.32. Soit E une courbe elliptique définie sur $\mathbb{F}_q$, ℓ est dit un nombre premier de Atkin si le polynôme caractéristique du Frobenius : $\pi^2 - t_\pi \pi + q$ est

irréductible dans $\mathbb{Z}_\ell$. Dés lors, comme on a $d_\pi = \ell^{2h} d_K$ avec $\ell^2 \nmid d_K$, d_π est un non-résidu quadratique si et seulement si $\left(\frac{d_K}{\ell}\right) = -1$. Ainsi dans le cas Atkin le cratère est réduit à un point par le corollaire 4.19.

Nous allons nous placer dans tout ce document dans le cas où le volcan de ℓ-isogénies dans le cas Atkin est de hauteur $h > 0$. La remarque 5.39 donne un moyen pour se ramener à ce cas-là.

5.2.1 Étude de l'action du Frobenius sur le module de Tate

Nous allons donc étudier dans cette partie l'action du Frobenius sur $\mathsf{T}_\ell(E)$ et voir si nous pouvons déterminer des directions d'isogénies descendantes, c'est à dire les distinguer entre elles.

Proposition 5.33. Soit E une courbe elliptique définie sur un volcan de ℓ-isogénies de hauteur $h > 0$ tel que ℓ soit un nombre premier de Atkin. Il existe un unique $e \in [0, h]$ tel que $\pi|\mathsf{T}_\ell(E)$ est égale, sur $\mathbb{Z}_\ell$, à la matrice

$$\begin{pmatrix} a & b\ell^{h-e} \\ c\ell^{h-e} & d \end{pmatrix} \bmod \mathbb{Z}_\ell \quad \text{avec } a, d \text{ premiers avec } \ell, \ell^h | a - d.$$

Pour $e = 0$ E se situe sur le cratère, sinon e est la profondeur de E dans le volcan. De plus, soit b et c sont premiers avec ℓ, soit l'un des deux est premier avec ℓ et l'autre a sa valuation ℓ-adique qui appartient à l'intervalle $[2, 2e]$. Lorsque $\ell = 2$ et $e = 0$, on a $2^h || a - d$.

Démonstration. Soit E une courbe située au niveau $h - e$ du volcan de ℓ-isogénies, alors, comme les ℓ-isogénies sont rationnelles, les ℓ^{h-e}-isogénies sont rationnelles, ainsi l'action du Frobenius sur une base de la ℓ^{h-e}-torsion est diagonale. Mais, comme le polynôme caractéristique de π est irréductible sur $\mathbb{Z}_\ell$, alors l'action du Frobenius doit être scalaire, ainsi $a = d \bmod \ell^{h-e}$. La matrice du Frobenius sur $\mathbb{Z}_\ell$ est

- lorsque $e = 0$, de la forme $\left(\begin{smallmatrix} a & b\ell^h \\ c\ell^h & d \end{smallmatrix}\right)$ avec $b \wedge \ell = 1$ et $c \wedge \ell = 1$. En effet on a $\left(\frac{d_K}{\ell}\right) = \left(\frac{d_\pi/\ell^{2h}}{\ell}\right)$, or $\frac{d_\pi}{\ell^{2h}} = \frac{(a-d)^2}{\ell^{2h}} + 4bc$, ainsi on doit avoir $bc \wedge \ell = 1$. Comme dans le cas $\ell = 2$ on a $d_K = 5 \bmod 8$, alors $(\frac{a-d}{\ell^h})^2 \neq 0 \bmod 2$.
- lorsque $e > 0$, de la forme $\left(\begin{smallmatrix} a & b\ell^{h-e} \\ c\ell^{h-e} & d \end{smallmatrix}\right)$, avec soit b, c premiers avec ℓ, soit b ou c premier avec ℓ, l'autre ayant une valuation ℓ-adique comprise entre 2 et $2e$. Ce second cas correspond au cas où un point de la base dans laquelle est exprimée l'action du Frobenius est un générateur de l'unique ℓ-isogénie montante. Le plus grand degré d'isogénie définie sur $\mathbb{F}_q$ ayant pour domaine E étant égal à ℓ^{h+e}, on a alors le résultat. En effet une telle ℓ^{h+e}-isogénie est obtenue comme la composition des e ℓ-isogénies montantes qui permettent d'atteindre le cratère et de h ℓ-isogénies descendantes reliant le courbe sommet au bas du volcan, la borne minimale (2) est atteinte en ne montant que d'un niveau dans le volcan puis en descendant en bas de celui-ci. Comme vu précédemment on a $\ell^{2h} | d_\pi = (a-d)^2 + 4bc\ell^{2h-2e}$, en particulier $\ell^{2h-2e} | d_\pi$ et donc $\ell^{2h-2e} | (a-d)^2$.

Nous montrons alors, matriciellement, que tout changement de base préserve les propriétés énoncées. La conjugaison de la matrice $\left(\begin{smallmatrix} a & b\ell^{h-e} \\ c\ell^{h-e} & d \end{smallmatrix}\right)$ par $\left(\begin{smallmatrix} 1 & \beta \\ 0 & 1 \end{smallmatrix}\right)$ nous

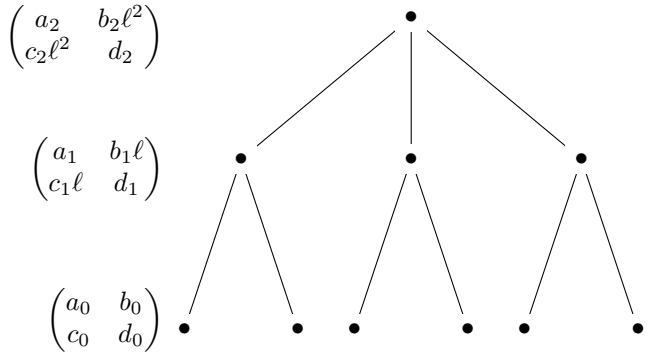


FIGURE 5.5 – Exemples de matrices du Frobenius obtenues sur les différents niveaux d'un volcan de ℓ-isogénies

donne la matrice $\begin{pmatrix} a+\beta(c\ell^{h-e}) & \ell^{h-e}(-\beta^2 c+\beta(d-a)/\ell^{h-e}+b) \\ c\ell^{h-e} & d-\beta c\ell^{h-e} \end{pmatrix}$, dont les coefficients diagonaux sont encore égaux modulo ℓ^{h-e}. Le coefficient $(-\beta^2 c+\beta(d-a)/\ell^{h-e}+b)$ peut être divisible par ℓ seulement si $\frac{d-a}{\ell^{h-e}} + 4bc = d_\pi/\ell^{2h-2e}$ est un résidu quadratique dans $\mathbb{Z}_\ell$. La conjugaison de la matrice $\begin{pmatrix} a & b\ell^{h-e} \\ c\ell^{h-e} & d \end{pmatrix}$ par $\left(\begin{smallmatrix} \gamma & 0 \\ 0 & 1 \end{smallmatrix}\right)$ avec $\gamma \wedge \ell = 1$ donne la matrice $\begin{pmatrix} a & b\gamma^{-1}\ell^{h-e} \\ c\gamma\ell^{h-e} & d \end{pmatrix}$. □

La figure 5.5 montre les différentes matrices représentant l'action du Frobenius que nous pouvons obtenir selon le niveau de la courbe. Pour une courbe située au niveau du cratère (ici le 2-ième niveau), les coefficients b_2 et c_2 sont premiers avec ℓ, et la valuation ℓ-adique des coefficients anti-diagonaux qui vaut h. Pour les niveaux en dessous du cratère, au moins un des deux coefficients anti-diagonaux (ici $(b_1\ell, c_1\ell)$ pour le niveau 1 et (b_0, c_0) pour le niveau 0) est de valuation ℓ-adique égal au niveau $h-e$ de la courbe, l'autre coefficient peut avoir une valuation ℓ-adique comprise entre $h-e+2$ et $h+e$.

Nous avons vu dans la preuve de la proposition 5.33 un moyen de trouver un point générateur d'une isogénie montante, nous énonçons donc le résultat suivant :

Corollaire 5.34. Soit E située au niveau $h-e < h$ d'un volcan de ℓ-isogénies avec ℓ un nombre premier de Atkin. Soit $\langle P, Q\rangle$ une base de $E[\ell^k]$, avec $k > h-e$, telle que :

$$\pi|(P,Q) = \begin{pmatrix} a & b\ell^{h-e} \\ c\ell^{h-e} & d \end{pmatrix} \bmod \ell^k,$$

avec $b \wedge \ell = 1$ et $\ell \mid c$. Alors la ℓ-isogénie montante de domaine E a pour noyau $\langle[\ell^{k-1}P]\rangle$.

Ce résultat peut aussi être prouvé avec la même méthode que celle employée dans la preuve de la proposition 5.5. Ce corollaire permet lui aussi de retrouver le résultat de la proposition 4.35.

Maintenant nous allons voir comment distinguer les ℓ^{i-e}-isogénies entre elles. Vu que nous ne pouvons, comme dans le cas Elkies, distinguer deux sous-groupes cycliques d'ordre ℓ^{h+i} de $E[\ell^{h+i}]$ pour $i \geqslant e$ des autres sous-groupes cycliques,

nous allons voir quelles informations nous obtenons lorsque un point de la base de $E[\ell^{h+i}]$ est fixé arbitrairement.

Proposition 5.35. Soient P, R, R' trois points d'une courbe E, située au niveau $h-e$ du volcan des ℓ-isogénies, tels que $\langle P, R\rangle = \langle P, R'\rangle = E[\ell^{h+i}]$ avec $i \geqslant e$ alors $\pi(P,R) = \pi(P,R')$ si et seulement si $[\ell^{h+e}]R = [\ell^{h+e}]R'$.

Démonstration. Montrons tout d'abord le sens direct. Soient R, R' deux points tels que $\pi(P,R) = \pi(P,R') = \left(\begin{smallmatrix} a & b\ell^{h-e} \\ c\ell^{h-e} & d \end{smallmatrix}\right)$ alors cette égalité nous donne : $\pi(P) = [a]P + [c\ell^{h-e}]R = [a]P + [c\ell^{h-e}]R'$, de cette égalité on déduit avec $v_\ell(c) \leqslant 2e$ que $[\ell^{h+e}]R = [\ell^{h+e}]R'$ ce qui permet de conclure pour ce sens de l'équivalence.

Pour prouver que $[\ell^{h-e}]R = [\ell^{h-e}]R' \Rightarrow \pi(P,R) = \pi(P,R')$, il suffit de remarquer que la conjugaison de la matrice $\left(\begin{smallmatrix} a & b\ell^{h-e} \\ c\ell^{h-e} & d \end{smallmatrix}\right)$ mod ℓ^{h+i} par $\left(\begin{smallmatrix} 1 & k'\ell^{i+e} \\ 0 & 1+k\ell^{i+e} \end{smallmatrix}\right)$ laisse la matrice invariante modulo ℓ^{h+i}. □

La proposition 5.35 nous dit en particulier que deux points R et R' tels que $\pi(P,R) = \pi(P,R')$ engendrent la même ℓ^{i-e}-isogénie de noyau $\langle[\ell^{h+e}]R'\rangle = \langle[\ell^{h+e}]R\rangle$.

Pour une courbe située au niveau $h-e$, si nous souhaitions étudier la direction des ℓ^i-isogénies, nous aurions à travailler avec une base de la ℓ^{h+i+e}-torsion. Comme, à l'aide du corollaire 5.34 nous savons monter dans le volcan des ℓ-isogénies, si nous voulions étudier le même problème (déterminer les ℓ^i-isogénies ayant pour domaine une courbe située au niveau $h-e$) à partir de la courbe sur le cratère, nous aurions alors à étudier la ℓ^{h+i+e}-torsion. Ainsi en pratique il sera intéressant d'étudier cette formulation du même problème, car nous pouvons être amené à travailler avec des extensions de corps plus petites pour le même résultat (voir proposition 5.40 pour plus de détails).

Le résultat suivant nous permet de distinguer les différents générateurs d'une même ℓ^{i-e}-isogénie dans notre contexte.

Proposition 5.36. Soient P, Q deux points définis sur une courbe elliptique E située au niveau $h-e$ du volcan des ℓ-isogénies, tels que $E[\ell^{h+i}] = \langle P, Q\rangle$ avec $i \geqslant e$. On pose $R = [x]P + [y]Q$ avec $y \wedge \ell = 1$, alors la matrice

$$\pi(P,R) = \begin{pmatrix} a & b\ell^{h-e} \\ c\ell^{h-e} & d \end{pmatrix} \bmod \ell^{h+i}$$

représentant l'action du Frobenius dans la base $\langle P, R\rangle$ est conjuguée aux matrices de la forme :

$$\pi(P,R') = \begin{pmatrix} a & b\ell^{h-e}\beta^{-1} \\ c\ell^{h-e}\beta & d \end{pmatrix} \bmod \ell^{h+i}$$

si et seulement si $\beta\ell^{h+e}R = \ell^{h+e}R'$ avec $\beta \in \left(\mathbb{Z}/\ell^{i-e}\mathbb{Z}\right)^\times$. De plus tous les points S tels que $\langle[\ell^{h+e}]R\rangle = \langle[\ell^{h+e}]S\rangle$ sont obtenus à partir de tous les changements de la forme $R \mapsto [\beta]R$ avec $\beta \in \left(\mathbb{Z}/\ell^{i-e}\mathbb{Z}\right)^\times$.

Démonstration. Par la proposition 5.35 $\pi(P,R') = \pi(P,\beta R)$ si et seulement si $[\ell^{h+e}]\beta R = [\ell^{h+e}]R'$. Or, en observant que la conjugaison de la matrice $\left(\begin{smallmatrix} a & b\ell^{h-e} \\ c\ell^{h-e} & d \end{smallmatrix}\right)$ par $\left(\begin{smallmatrix} 1 & 0 \\ 0 & \beta \end{smallmatrix}\right)$ avec $\beta \in \left(\mathbb{Z}/\ell^{i-e}\mathbb{Z}\right)^\times$ nous donne une matrice de la

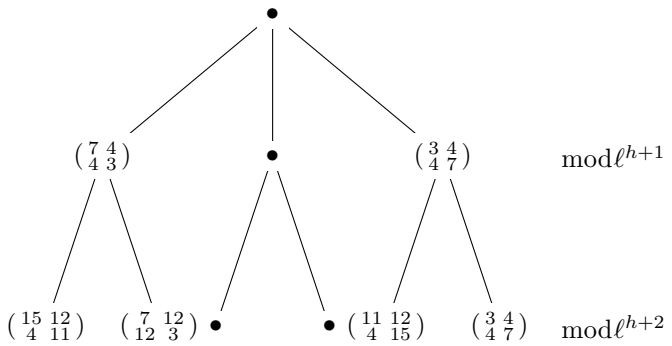


FIGURE 5.6 – Exemples des isogénies correspondant aux différentes matrices du Frobenius, calculées sur la courbe E au sommet du volcan des ℓ-isogénies.

forme $\left(\begin{smallmatrix} a & b\ell^{h-e}\beta \\ c\ell^{h-e}\beta^{-1} & d \end{smallmatrix}\right)$, nous avons bien $\pi(P, \beta R) = \left(\begin{smallmatrix} a & b\ell^{h-e}\beta \\ c\ell^{h-e}\beta^{-1} & d \end{smallmatrix}\right)$, ce qui nous donne le résultat.

Montrons maintenant le second point. Soit S tel que $\langle [\ell^{h+e}]R\rangle = \langle [\ell^{h+e}]S\rangle$ alors il existe $\beta \in \left(\mathbb{Z}/\ell^{i-e}\mathbb{Z}\right)^\times$ tel que $[\beta]R = S$, d'où le résultat. □

La figure 5.6 représente les isogénies que l'on obtient selon la forme des matrices du Frobenius de la courbe au sommet du volcan. Dans cet exemple, E est la courbe de j-invariant 56 définie sur $\mathbb{F}_{149}$, et $\ell = 2$. Nous avons donc représenté dans le volcan la matrice à l'endroit correspondant au codomaine de la ℓ^i-isogénie engendrée par le second vecteur de la base de $E[\ell^{h+i}]$ dans laquelle est calculée l'action du Frobenius. Le premier vecteur de la base a été choisi au hasard parmi les points d'ordre ℓ^{h+i}. Ainsi les courbes dans le volcan atteintes par les isogénies engendrées par le premier point de la base ne sont pas associées à des matrices du Frobenius, voilà pourquoi seulement 2 des 3 branches descendantes ont des matrices associées à chaque courbe. Les matrices sont représentées modulo ℓ^{h+1} pour le niveau $h-1$ car il est nécessaire de calculer une base de $E[\ell^{h+1}]$ pour distinguer les ℓ-isogénies, de même pour le niveau $h-2$ une base de $E[\ell^{h+2}]$ est nécessaire. Il est à noter que pour chaque branche on a $\left(\begin{smallmatrix}15 & 12\\ 4 & 11\end{smallmatrix}\right) = \left(\begin{smallmatrix}7 & 12\\ 12 & 3\end{smallmatrix}\right) = \left(\begin{smallmatrix}7 & 4\\ 4 & 3\end{smallmatrix}\right) \bmod \ell^{h+1}$ et $\left(\begin{smallmatrix}3 & 4\\ 4 & 7\end{smallmatrix}\right) = \left(\begin{smallmatrix}11 & 12\\ 4 & 15\end{smallmatrix}\right) \bmod \ell^{h+1}$, ce qui est normal car nous avons un seul générateur possible de la 2-isogénie, et donc une seule matrice par conjugaison possible (voir proposition 5.35). Pour la base du volcan il est à noter qu'une seule des matrices que l'on peut obtenir par conjugaison (voir proposition 5.35) a été représentée.

Ces résultats sur la détermination du second point ne nécessitent pas forcément la détermination complète du premier point de la base, comme le montre le résultat suivant.

Corollaire 5.37. Soient P, P' deux points d'ordre ℓ^{h+i}, avec $i \geqslant e$, d'une courbe elliptique E située au niveau $h-e$ du volcan des ℓ-isogénies, tels que $[\ell^{h+e}]P = [\ell^{h+e}]P'$. Soient R, R' deux points tels que $\langle P, R\rangle = \langle P', R'\rangle = E[\ell^{h+i}]$ et $\pi(P, R) = \pi(P', R')$, alors $[\ell^{h+e}]R = [\ell^{h+e}]R'$.

Démonstration. Par la proposition 5.35 $\pi(P', R') = \pi(P, R')$, l'égalité $\pi(P, R') = \pi(P, R)$ permet de conclure. □

5.2.2 Calculs de directions dans le volcan de ℓ-isogénies.

Nous allons maintenant étudier la structure de la torsion rationnelle des courbes elliptiques situées sur le cratère, et déterminer l'extension de corps nécessaire pour avoir une torsion ℓ-adique de valuation fixée. La proposition 5.40 permet d'étendre notre résultat aux courbes inférieures dans le volcan.

Proposition 5.38. Soit E une courbe elliptique ordinaire située sur le cratère d'un volcan de ℓ-isogénies de hauteur $h > 0$. On note d_1 le degré de la plus petite extension de corps $F/\mathbb{F}_q$ telle que $E[\ell] \subset E(F)$. Alors l'ordre de q dans $(\mathbb{Z}/\ell\mathbb{Z})^\times$ divise d_1, et d_1 qui divise $(\ell - 1)$.

Démonstration. Nous procédons de manière similaire à la preuve de la proposition 5.19. Le degré d_1 correspond à l'ordre de la matrice $\pi|E[\ell]$. Nous obtenons donc le résultat par la proposition 5.33 en utilisant le fait que $a \cdot d = q \bmod \ell$. □

Remarque 5.39. Lorsque le volcan est de hauteur 0, nous pouvons nous ramener au cas d'un volcan de hauteur $h > 0$ en travaillant dans une extension de degré divisant $\ell^2 - 1$ pour que le ℓ-ième polynôme de division possède des racines dans cette extension.

Nous mettons en avant un résultat qui est une conséquence du chapitre 4.

Proposition 5.40. Soit E une courbe elliptique ordinaire située sur le cratère d'un volcan de ℓ-isogénies de hauteur $h > 0$, avec ℓ un nombre premier de Atkin,

- si $\ell \neq 2$ on note $\mathsf{F}/\mathbb{F}_q$ la plus petite extension de corps de $\mathbb{F}_q$ de degré d_1 telle que $E[\ell] \subset E(\mathsf{F})$,
- si $\ell = 2$ on note $\mathsf{F}/\mathbb{F}_q$ la plus petite extension de corps de $\mathbb{F}_q$ de degré $d_2 \in 1, 2$ telle que $E[4] \subset E(\mathsf{F})$.

Nous avons alors :

$$E(\mathsf{F})[\ell^\infty] \simeq \mathbb{Z}/\ell^\beta\mathbb{Z} \times \mathbb{Z}/\ell^\beta\mathbb{Z},$$

avec $\beta \in [1, h]$ pour $\ell \neq 2$, et $\beta \in [2, h]$ pour $\ell = 2$. De plus $\beta = h$, la hauteur du volcan sur F, si et seulement si le volcan est *régulier*. Pour un volcan *non-régulier* β est égal au niveau du premier niveau de stabilité.

Démonstration. Notons $E(\mathsf{F})[\ell^\infty] \simeq \mathbb{Z}/\ell^\alpha\mathbb{Z} \times \mathbb{Z}/\ell^\beta\mathbb{Z}$.

Supposons par l'absurde que $\alpha > \beta$ dans le cas où le volcan serait *régulier*. Nous aurions alors $\beta = h$ et, comme $\alpha > \beta$, il existerait des isogénies ayant pour domaine E, située sur le cratère, de degré ℓ^α ce qui contredirait le fait que le volcan soit de hauteur $h = \beta$.

Dans le cas où le volcan serait *non-régulier* par la structure de volcans non-réguliers nous obtenons $\alpha = \beta$ voir [Ion10, §5.3.1]. Pour le lien entre h et β le lecteur peut voir [Ion10, §5.3.1]. □

Dorénavant nous allons garder cette notation de β que nous définissons comme suit.

Définition 5.41. La notation suivante permet de spécifier la structure de la ℓ-torsion sur une extension de $\mathsf{F}_1/\mathbb{F}_q$ où nous aurions $E[\ell] \subset E(\mathsf{F}_1)$.

- Pour ℓ premier impair, on note β la plus grande valuation ℓ-adique de la torsion rationnelle de la courbe sur le cratère du volcan des ℓ-isogénies défini sur F_1 ;
- pour $\ell = 2$, on note β la plus grande valuation 2-adique moins un de la torsion rationnelle de la courbe sur le cratère du volcan des 2-isogénies défini sur F_1.

Proposition 5.42. Soit E une courbe elliptique ordinaire située sur le cratère d'un volcan de ℓ-isogénies. En reprenant les notations de la proposition 5.40 pour tout k, on note d_k le degré de la plus petite extension de corps $\mathsf{F}/\mathbb{F}_q$ telle que $E[\ell^k] \subset E(\mathsf{F})$. Alors :

1. l'ordre de q dans $(\mathbb{Z}/\ell\mathbb{Z})^\times$ divise d_1, et d_1 divise $(\ell-1)$.
2. Si ℓ est impair alors pour tout $k > 1$, $d_k = \ell^{\max(0,k-\beta)} d_1$.
3. Si $\ell = 2$ alors $d_2 \in \{1, 2\}$ et pour tout $k > 2$, $d_k = \ell^{\max(0,k-\beta)} d_2$.
4. Si $\ell \neq 2$ pour $[\mathsf{F} : \mathbb{F}_q] = d_1\ell^n$, le groupe $E[\ell^\infty](\mathsf{F})$ est isomorphe à $(\mathbb{Z}/\ell^{n+\beta}\mathbb{Z}) \times (\mathbb{Z}/\ell^{n+\beta}\mathbb{Z})$.
5. Si $\ell = 2$ pour $[\mathsf{F} : \mathbb{F}_q] = d_2\ell^n$, le groupe $E[\ell^\infty](\mathsf{F})$ est isomorphe à $(\mathbb{Z}/\ell^{n+\beta}\mathbb{Z}) \times (\mathbb{Z}/\ell^{n+\beta}\mathbb{Z})$.

Démonstration. Le premier résultat a déjà été montré dans la proposition 5.40. Les résultats suivants viennent du fait que pour augmenter de 1 la hauteur du volcan de ℓ-isogénies nous devons travailler avec une extension de degré ℓ, par [Fou01, Lemme 6.5.2]. Dés que la hauteur du volcan est augmentée de 1 en travaillant sur F_ℓ, l'extension de degré ℓ de F, pour $E[\ell^\infty](\mathsf{F}) = \mathbb{Z}/\ell^{n_1}\mathbb{Z} \times \mathbb{Z}/\ell^{n_2}\mathbb{Z}$, nous avons $E[\ell^\infty](\mathsf{F}_\ell) = \mathbb{Z}/\ell^{n_1+1}\mathbb{Z} \times \mathbb{Z}/\ell^{n_2+1}\mathbb{Z}$ comme montré dans [Ion10, §5.3.1]. □

Notation 5.43. F_i représente la plus petite extension de corps de $\mathbb{F}_q$ de degré d_i, avec d_i défini comme dans la proposition 5.42 et similaire à la définition 3.1 des tours d'extensions ℓ-adiques

Maintenant que nous avons défini dans quels éléments de la tour d'extensions ℓ-adique sont définis les points, nous présentons et analysons l'algorithme 9. Cet algorithme calcule, à partir d'un point P fixé d'ordre ℓ^{h-e+i} et d'une matrice M à coefficients dans $\mathbb{Z}/\ell^{h-e+i}\mathbb{Z}$, un second point Q d'ordre ℓ^{h-e+i} tel que l'action du Frobenius exprimée dans la base $\langle P, Q\rangle$ soit de la même forme que M.

Algorithme 9 Calcul d'un point R d'ordre ℓ^{h-e+i} tel que $\pi(P, R) = M$

Entrée : E une courbe située au niveau $h-e$; (P, Q) une base de $E[\ell^{h-e+i}]$ avec P un point fixé de E, un entier $i > e$; M une matrice représentant l'action du Frobenius dans une base de la ℓ^{h-e+i}-torsion d'une courbe elliptique située au niveau $h - e$.
Sortie : $R = [\gamma]P + [\kappa]Q$: un point d'ordre ℓ^{h-e+i} de E tel que $\pi(P, R) = M$.

1: $(\gamma, \kappa) \leftarrow (0, 0)$
2: **pour** $j = 1$ to $h - e + i$ **faire**
3: Calcul de $P_j = [\ell^{h-e+i-j}]P, Q_j = [\ell^{h-e+i-j}]Q$;
4: Calcul de $R_j = [\gamma + x\ell^{j-1}]P_j + [\kappa + y\ell^{j-1}]Q_j$ avec $\pi(P_j, R_j) = M \bmod \ell^j$;
5: $(\gamma, \kappa) \leftarrow (\gamma + x\ell^{j-1}, \kappa + y\ell^{j-1})$;
6: **fin pour**
7: **retourner** $R = [\gamma]P + [\kappa]Q$.

Proposition 5.44. L'algorithme 9 a une complexité de

$$O(\ell^4(\mathsf{M}(\ell^{h-e+i-\beta+1+\max(0,e-(h-\beta))}) + (\beta - \max(0, e-(h-\beta)))\mathsf{M}(\ell)))$$

opérations sur $\mathbb{F}_q$.

Démonstration. Par la proposition 5.42 les points P_j, R_j sont définis dans $\mathsf{F}_{j-\beta+\max(0,e-(h-\beta))}$ lorsque $j-\beta+\max(0,e-(h-\beta))>1$ et définis dans F_1 sinon. L'étape 3 est faite en tant que pré-calcul, ainsi nous calculons successivement des multiplications par ℓ de points définis dans $\mathsf{F}_{j-\beta+\max(0,e-(h-\beta))}$ à F_1 en décomposant la multiplication par ℓ par deux isogénies de degré ℓ, qui coûtent chacune $O(\mathsf{M}(\ell^{j-\beta+\max(0,e-(h-\beta))}))$ opérations sur $\mathbb{F}_q$. Nous avons donc un coût total pour l'étape 3 de $O(\mathsf{M}(\ell^{h-e+i-\beta+1+\max(0,e-(h-\beta))})+(\beta-\max(0,e-(h-\beta))\mathsf{M}(\ell))$. À l'étape 4 le calcul de R_j peut être actualisé à chaque itération de la boucle à l'aide de ℓ^2 additions de points définis dans $\mathsf{F}_{j-\beta+\max(0,e-(h-\beta))}$, lorsque $j-\beta+\max(0,e-(h-\beta))>1$, ou F_1 sinon. Ainsi le calcul de R_j a un coût total de $O(\ell^2(\mathsf{M}(\ell^{h-e+i-\beta+1+\max(0,e-(h-\beta))})+(\beta-(\max(0,e-(h-\beta)))\mathsf{M}(\ell)))$. Le calcul du Frobenius sur un point R_j, fixé défini dans $\mathsf{F}_{j-\beta+\max(0,e-(h-\beta))}$ lorsque $j-\beta+\max(0,e-(h-\beta))>1$, dans F_1 sinon, a un coût total de $O(\ell^{\max(j-\beta+\max(0,e-(h-\beta)),1)}\mathsf{M}(\ell))$ par le théorème 3.6. Le coût total du calcul du Frobenius pour cet algorithme est donc de

$$O(\ell^2\mathsf{M}(\ell)(\ell^{h-e+i-\beta+1+\max(0,e-(h-\beta))}+(\beta-\max(0,e-(h-\beta)))\ell))$$

opérations sur $\mathbb{F}_q$.

À R_j fixé, pour le test d'égalité $\pi(P_j,R_j)=M \bmod \ell^j$, nous actualisons à chaque itération la valeur de MP_j et MR_j. Pour cela nous sommes amenés à effectuer jusqu'à ℓ^2 additions de points d'ordre ℓ^j définis dans $\mathsf{F}_{j-\beta+\max(0,e-(h-\beta))}$, lorsque $j-\beta+\max(0,e-(h-\beta))>1$, dans F_1 sinon. Ce test d'égalité a donc un coût total de $O(\ell^4(\mathsf{M}(\ell^{h-e+i-\beta+1\max(0,e-(h-\beta))})+(\beta-\max(0,e-(h-\beta)))\mathsf{M}(\ell)))$ opérations sur $\mathbb{F}_q$, c'est cette opération qui domine la complexité et donne le résultat annoncé. □

Chapitre 6

Algorithme de Couveignes ℓ-adique

On précise le contexte dans lequel on se place :

Problème du calcul explicite d'isogénie Le problème du *calcul explicite d'isogénie* est : étant donnés deux j-invariants j_0 et j_1, un entier r tel que les j-invariants soient r-isogènes, c'est à dire qu'il existe deux courbes elliptiques E_0 et E_1 reliées par une isogénie de degré r telles que $j(E_0) = j_0$ et $j(E_1) = j_1$, calculer les courbes E_0, E_1 et l'isogénie $\phi : E_0 \to E_1$.

Pour résoudre ce problème du calcul explicite d'isogénie on pourrait directement utiliser les même méthodes que celles développées dans [Cou96] et [DF11] (voir chapitre 2 pour plus de détails) en remplaçant les points de p-torsion par ceux de ℓ-torsion, ainsi on enlèverait la dépendance exponentielle en la taille du corps sur lequel on travaille. Avec une telle démarche on

— calcule une base de la ℓ^k-torsion telle que $\ell^{2k} \in \tilde{O}_{r,q}(r)$ sur chacune des 2 courbes ;
— teste toutes les matrices $M \in \mathbb{GL}_2(\mathbb{Z}/\ell^k\mathbb{Z})$ qui modélisent toutes les correspondances possibles entre les deux bases de la ℓ^k-torsion induites par la r-isogénie.

Le problème avec cette approche c'est que l'on a un nombre beaucoup trop grand $\tilde{O}(r^2)$ de matrices à tester. En effet dans l'algorithme original de [Cou96] amélioré ensuite par [DF11] on avait à tester toutes les correspondances entre les groupes cycliques de la p-torsion, or ici les groupes avec lesquels on travaille ne sont plus cycliques mais un produit de deux groupes cycliques, d'où la complexité plus élevée pour le nombre de tests à effectuer. On doit donc travailler avec un ensemble de points plus restrictifs, mais encore invariant sous l'évaluation de r-isogénies si l'on veut obtenir une complexité quadratique comme dans les algorithmes de [DF11]. On présente donc deux approches toutes les deux basées sur les directions dans le volcan de ℓ-isogénies une pour le cas Elkies et une pour le cas Atkin.

6.1 Cas Elkies

Cette section s'inspire de travaux effectués en collaboration avec Luca De Feo, Jérôme Plût et Éric Schost qui ont fait l'objet d'une publication [DFHPS16].

On justifie tout d'abord l'intérêt des bases horizontales par rapport à un algorithme de Couveignes [Cou96] modifié pour travailler avec la ℓ-torsion. Cette section utilise les résultats de la sous-section 5.1.1 sur les isogénies horizontales.

Proposition 6.1. Soit $\phi : E \to E'$ une isogénie de degré r, soit ℓ un entier premier avec r.

1. les courbes E, E' ont la même profondeur dans leur volcan des ℓ-isogénies ;
2. pour tout point $P \in E[\ell^k]$, les isogénies de noyau $\langle P\rangle$ et $\langle\phi(P)\rangle$ sont de même type (ascendantes, descendantes, ou horizontales de même direction) ;
3. si $P \in E[\ell]$ et $P' \in E'[\ell]$ sont tous les deux des points générateurs d'isogénies ascendantes, ou horizontales de même direction alors $E/\langle P\rangle$ et $E'/\langle P'\rangle$ sont encore r-isogènes.

Démonstration. Les points (1) et (2) découlent de la proposition 5.3 et du fait que pour ϕ isogénie rationnelle de degré r premier avec ℓ on a un isomorphisme de modules de Tate qui commute avec le Frobenius. Pour le point (3) il suffit de remarquer qu'il existe un unique sous-groupe d'ordre ℓ qui génère soit une isogénie ascendante soit une isogénie de direction fixée, ainsi on doit avoir $\langle P'\rangle = \langle\phi(P)\rangle$.

□

Le troisième point de cette proposition nous permet de réduire le problème du calcul de la r-isogénie entre deux courbes elliptiques au même problème pour deux courbes situées sur le cratère du volcan de ℓ-isogénies. Cependant la proposition suivante montre que cela n'est pas nécessaire on peut tout aussi bien, à l'aide de points ascendants horizontaux, travailler avec des sous-groupes cycliques invariants selon l'évaluation de r-isogénies.

Proposition 6.2. Soient $\phi : E \to E'$ une r-isogénie avec E et E' qui se situent à une profondeur e du cratère (donc au niveau $h-e$), $P \in E, P' \in E'$ des points ascendants horizontaux de même direction alors $\phi(P) \in \langle P'\rangle$.

Démonstration. Par définition(5.12) on peut trouver $R \in E_s$ et $R' \in E'_s$ tels que $[\ell^e]R$ et $[\ell^e]R'$ soient des points horizontaux de même direction avec deux ℓ^e-isogénies $\psi : E_s \to E$ et $\psi' : E'_s \to E'$ telles que $\psi(R) = P$ et $\psi'(R') = P'$. On a tout d'abord $\phi([\ell^{k-e}]P) \in \langle[\ell^{k-e}]P'\rangle$ par la proposition 6.1 (2) car par la proposition 5.14 (1) $\ker(\widehat{\psi}) = \langle[\ell^{k-e}]P\rangle$ et $\ker(\widehat{\psi'}) = \langle[\ell^{k-e}]P'\rangle$. Ensuite on a $\langle[\ell^e]R\rangle = \langle\widehat{\psi}(P)\rangle$ et $\langle[\ell^e]R'\rangle = \langle\widehat{\psi'}(P')\rangle$. Ainsi les ℓ^k-isogénies engendrées par P et P' sont du même type : une composition d'une ℓ^e isogénie montante et d'une ℓ^{k-e}-isogénie horizontale de direction identique, donc par la proposition 6.1 (2) $\phi(P) \in \langle P'\rangle$. □

La différence entre des points horizontaux $P_\lambda, Q_\mu \in E_s$ d'ordre ℓ^k et des points *ascendants* horizontaux $R_\lambda, R_\mu \in E$ d'ordre ℓ^k de profondeur $e > 0$ de directions opposées c'est que l'on a $\langle R_\lambda, R_\mu\rangle \neq E[\ell^k]$ (en particulier$\langle[\ell^{k-e}]R_\lambda\rangle = \langle[\ell^{k-e}]R_\mu\rangle$) alors que pour deux points horizontaux de directions opposées on avait $E_s[\ell^k] = \langle P_\lambda, Q_\mu\rangle$. Ainsi avec deux points ascendants horizontaux on ne

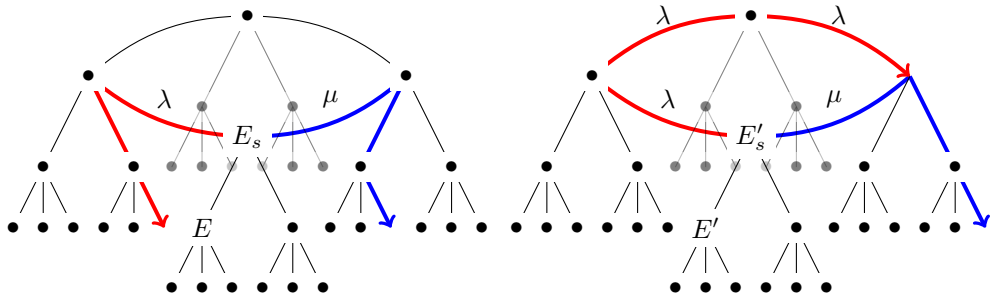


FIGURE 6.1 – Exemple de candidats pour la mise en correspondances de points diagonaux par la r-isogénie ϕ

peut travailler avec toute la ℓ^k-torsion. On va donc faire le choix par la suite, afin d'avoir une présentation uniforme,de travailler avec les points d'ordre ℓ^k(avec $k > h$). En effet on ne peut pas générer tous les point de ℓ^e-torsion et donc pour éviter toute redondance on ne travaille qu'avec les points d'ordre ℓ^k. Si l'on souhaitait travailler avec les points de la ℓ^e-torsion on utiliserait dans le cas de deux points ascendants horizontaux R_λ, R_μ (de profondeur $e > 0$) par exemple le groupe $\langle [\ell^{k-e}]R_\lambda \rangle$.

6.1.1 Présentation du cas spécifique où l'on connaît un premier ℓ de Elkies

On se place tout d'abord dans le cas particulier où l'on connaît un nombre premier ℓ de Elkies.

On montre tout d'abord en quoi ce n'est pas optimal de travailler avec une base diagonale de la ℓ^k-torsion et l'avantage que cela procure de travailler avec des bases horizontales.

Soient E, E' deux courbes elliptiques de j-invariants j et j' reliées par une r-isogénie ϕ, alors, par la proposition 5.3 pour k plus grand que h la hauteur du volcan des ℓ-isogénies, on peut calculer deux bases diagonales $(P, Q), (P', Q')$ de $E_s[\ell^k]$ et $E'_s[\ell^k]$ les courbes sommets respectives de E et E'. L'action du Frobenius peut être représentée matriciellement de la façon suivante dans ces bases :

$$\pi(P, Q) = \pi(P', Q') = \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}.$$

Comme la r-isogénie ϕ commute avec le Frobenius (et que E_s et E'_s sont encore r-isogènes par la proposition 6.1) on devrait avoir $\phi(P) \in \langle P' \rangle$ et $\phi(Q) \in \langle Q' \rangle$, or la matrice π est scalaire modulo la ℓ^h torsion ainsi la représentation de ϕ dans les bases (P, Q) et (P', Q') n'est pas diagonale :

$$\phi \begin{pmatrix} P \\ Q \end{pmatrix} = \begin{pmatrix} a & b\ell^h \\ c\ell^h & d \end{pmatrix} \begin{pmatrix} P' \\ Q' \end{pmatrix} \quad \text{avec} \quad a, d \in \left(\mathbb{Z}/\ell^k\mathbb{Z}\right)^\times ; b, c \in \mathbb{Z}/\ell^k\mathbb{Z}.$$

On illustre cela avec l'exemple de bases diagonales de la 3^3-torsion choisies sur la figure 6.1. On voit en particulier que ce choix ne permet une correspondance exacte que pour la 3-isogénie qui correspond à l'isogénie horizontale. En

effet comme on a vu plus tôt un point diagonal d'ordre ℓ^k ne donne une information que sur la ℓ^{k-h}-isogénie-horizontale (voir proposition 5.8). Dès lors on ne sait dire, à partir de cette information, si les isogénies de degré supérieur à 3 engendrées par le point diagonal sont du même type et respectent l'évaluation de la r-isogénie ϕ. En effet pour le choix d'un de ces points diagonaux on peut choisir comme sur l'exemple un point horizontal pour la direction λ pour la courbe E_s et un point non horizontal pour la direction λ sur la courbe E'_s. Dès lors on a pas une correspondance de sous-groupes cycliques et l'on doit considérer les combinaisons linéaire avec le second point de la base diagonale de direction μ pour les correspondances induites par la r-isogénie. Enfin on ne sait dire si la correspondance entre les ℓ-isogénies descendantes qui composent l'isogénie engendrée par les points de diagonaux de direction μ sont correctes. En effet nous avons vu à la proposition 5.16 qu'une étude à l'aide du Frobenius des ℓ-isogénies descendantes ne permet pas de distinguer les ℓ-isogénies entre elles.

On travaille donc avec deux bases $(P_\lambda, Q_\mu), (P'_\lambda, Q'_\mu)$ (ascendantes) horizontales de $E[\ell^k]$ et $E'[\ell^k]$. On doit à nouveau avoir $k \geqslant h+1$ pour pouvoir calculer ces bases (ascendantes) horizontales par la proposition 5.8. Dans ces bases ϕ peut être représentée comme une matrice diagonale car par la proposition 6.1 et la proposition 6.2 les groupes cycliques engendrés par des points (ascendants) horizontaux de même direction sont en bijection :

$$\phi \begin{pmatrix} P_\lambda \\ Q_\mu \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \begin{pmatrix} P'_\lambda \\ Q'_\mu \end{pmatrix} \quad \text{avec} \quad a, b \in \left(\mathbb{Z}/\ell^k\mathbb{Z}\right)^\times .$$

On énumère donc toutes les ℓ^{2k-2} matrices M possibles $\left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right)$. Pour chaque matrice M on interpole celle-ci sur les bases $(P_\lambda, Q_\mu), (P'_\lambda, Q'_\mu)$ en calculant le polynôme d'interpolation $A_{a,b}$ tel que

$$A_{a,b}(x([u]P_\lambda + [v]Q_\mu)) = x([au]P'_\lambda + [bv]Q'_\mu) \quad \text{pour tout } [u]P_\lambda + [v]Q_\mu \text{ d'ordre } \ell^k.$$

Ensuite à l'aide du polynôme $A_{a,b}$ on calcule la fraction rationnelle F telle que :

$$F = A_{a,b} \bmod T$$

avec T le polynôme minimal qui s'annule sur tout point $[u]P_\lambda + [v]Q_\mu$ d'ordre ℓ^k. C'est la fraction rationnelle F qui lorsque l'on a bien choisi M doit représenter la r-isogénie ϕ, on cherche donc à calculer F de degré $(r, r-1)$. Or une telle fraction rationnelle est déterminée par $2r$ coefficients on doit donc avoir le nombre d'abscisses de points d'ordre ℓ^k : $\frac{\ell^{2k-2}(\ell+1)}{2}$ strictement plus grand que $2r$ pour avoir suffisamment d'informations.

On peut donc maintenant énoncer dans l'algorithme 10 l'algorithme complet pour calculer une r-isogénie entre deux courbes elliptiques E, E' définies sur des volcans des ℓ-isogénies avec ℓ un nombre premier de Elkies.

Proposition 6.3. En supposant que l'on a $\ell^h < \sqrt{r}$, l'algorithme 10 calcule une r-isogénie $\phi : E \to E'$ en un temps espéré de

$$O\Big(\sqrt{r}\mathsf{M}(\sqrt{r}\ell^{1,5})\log(r)\log(\ell)\log(\ell q) + r\ell(\mathsf{M}(r\ell^4)\log(r)\log(\ell) + \mathsf{M}(r\ell^3)\log(r)^2\log(\ell))\Big)$$

Algorithme 10 Algorithme de Couveignes ℓ-adique dans le cas Elkies.

Entrée : E, E' : deux courbes elliptiques r-isogènes ordinaires situées au niveau $h - e$ d'un volcan de ℓ-isogénies avec cratère cyclique.

Sortie : ϕ la r-isogénie qui relie E à E'.

1: Calcul du plus petit k tel que $\ell^{2k-2}(\ell + 1) > 4r$;
2: Calcul de $(P, Q), (P', Q')$ bases diagonales de $E_s[\ell^k], E'_s[\ell^k]$ à l'aide de l'algorithme 7 ;
3: Calcul de $(P_\lambda, Q_\mu), (P'_\lambda, Q'_\mu)$ bases horizontales de $E_s[\ell^k], E'_s[\ell^k]$ à l'aide de l'algorithme 8 ;
4: **si** $(E_s, E'_s) \neq (E, E')$ **alors**
5: Calcul de $((P_\lambda, Q_\mu), (P'_\lambda, Q'_\mu)) = ((\varphi(P_\lambda), \varphi(Q_\mu)), (\varphi'(P'_\lambda), \varphi'(Q'_\mu)))$ bases ascendantes horizontales de $E[\ell^k], E'[\ell^k]$ avec les ℓ^e-isogénies descendantes $\varphi : E_s \to E$, $\varphi' : E_s \to E'$;
6: **fin si**
7: Calcul des liste de représentants L, L' des orbites de points d'ordre ℓ^k sous l'action de π ;
8: **pour** $M \in \mathsf{diag}(a, b)$ avec $a, b \in \left(\mathbb{Z}/\ell^k\mathbb{Z}\right)^*$ **faire**
9: Actualisation des représentants de la liste L' en $L'_{a,b}$ afin de respecter la correspondance induite par le choix de M ;
10: Calcul des des polynômes $A_{a,b}$ et T par les méthodes décrites dans la section 3.4 ;
11: Calcul de la fraction rationnelle $F = A_{a,b} \bmod T$ à l'aide d'une interpolation de Cauchy ;
12: **si** $\mathsf{Test}(F)$ **alors**
13: **retourner** F
14: **fin si**
15: **fin pour**

Démonstration. Par définition de k, on a $\ell^{2k-1} \in O(r\ell^2)$. Par la proposition 5.19, il existe $\beta \leqslant h$ tel que $E[\ell^k]$ est inclus dans $E(F_{k-\beta})$. On construit donc une tour d'extensions ℓ-adiques $\mathsf{F}_0 \subset \cdots \subset \mathsf{F}_{k-\beta}$, et l'on effectue les précalculs nécessaires au théorème 3.6 avec un coût de $O(\ell\mathsf{M}(\ell)\log(q))$. Ces étapes sont faites en pratique au cours de l'étape 2.

On attire l'attention sur le fait que la condition $\ell^h < \sqrt{r}$ se traduit par k strictement plus grand que h par définition de k. On va utiliser ce résultat tout au long de la preuve.

Le coût de calcul des bases diagonales de courbes sommets à l'étape 2 se fait à l'aide de l'algorithme 7 qui a une complexité dans le pire des cas de $O(\ell\mathsf{M}(\ell^2)\log(\ell)\log(\ell q) + \mathsf{R}(k) + \ell^2\mathsf{M}(\ell^k))$ par la proposition 5.27.

L'étape 3 qui utilise l'algorithme 8 coûte dans le pire des cas un coût moyen de $O(k\mathsf{R}(k-\beta)+k\ell^2\mathsf{M}(\ell^{k-\beta})+\ell\mathsf{M}(\ell^2)\log(\ell)\log(\ell q))$ d'après la proposition 5.28. En utilisant le résultat donné par [vzGG03, Chapter 14.5] pour le coût de R, on a alors un coût borné pour les étapes 3 et 2 par $O(\sqrt{r}\mathsf{M}(\sqrt{r}\ell^{1,5})\log(r)\log(\ell)\log(\ell q))$.

Il faut éventuellement rajouter le coût de calcul des points ascendants horizontaux si les courbes en entrée ne se situent pas sur le cratère. Celui-ci est dans le pire des cas de $O(k\mathsf{M}(\ell^{k-\beta+1})) = O(\log(r)\mathsf{M}(\sqrt{r}\ell^{1,5}))$ par la proposition 5.30, ce coût est donc majoré par le calcul de la base horizontale sur le cratère.

Par la proposition 5.19(5), il y a au plus $O(k \cdot \ell^{k+\beta})$ classes de Galois dans $E[\ell^k]$. Pour les polynômes d'interpolation on a besoin d'un représentant de chaque classe que l'on stocke dans les listes L et L'. Chaque représentant est calculé à partir de la base (P_λ, Q_μ) et (P'_λ, Q'_μ) en multipliant les deux points définis dans $\mathsf{F}_{k-\beta}$ par des entiers définis dans $\left(\mathbb{Z}/\ell^k\mathbb{Z}\right)^\times$ une telle multiplication coûte $O(\mathsf{M}(\ell^{k-\beta})\log(\ell^k))$ opérations. On a donc un coût total de $O(k\mathsf{M}(\ell^{2k})\log(\ell^k)) \subset O(\mathsf{M}(r\ell^3)\log(r)^2\log(\ell))$ pour calculer tous les représentants.

On utilise ensuite la proposition 3.12, avec un degré total $t = (\ell^{2k-2}(\ell+1))/2 \in O(r\ell^2)$, et le nombre de points d'interpolations est $s \in O(k \cdot \ell^{k+\beta})$, on calcule alors les polynômes T et $A_{a,b}$ avec un coût de $O(\mathsf{M}(r\ell^4)\log(r)\log(\ell))$. Le coût de calcul de $F_{a,b}$ est de $O(\mathsf{M}(r)\log(r))$ par [BCG+17, Théorème 7.5]. Le coût de calcul du test de l'isogénie (voir paragraphe dans la sous-section 2.5.1 pour une description détaillée des tests possibles) a pour opérations les plus coûteuses : regarder si le dénominateur de F est un carré (dans le cas où r est pair on regarde si c'est le produit d'un facteur du polynôme de 2-division et d'un carré) ou regarder si le dénominateur divise le polynôme de r-division. Cela coûte $O(\mathsf{M}(r)\log(r))$ opérations, on ne prend pas en compte toutefois le coût de calcul du polynôme de r-division de $O(r\mathsf{M}(r^2)\log(r)\log(rq))$ car les autres tests suffisent en général pour conclure. Tous ces coûts sont donc dominés par celui du calcul de $A_{a,b}$ et T. Enfin, en moyenne $\ell^{2k-2} = O(r\ell)$ matrices candidates doivent être testées avant de trouver l'isogénie. □

Il est à noter que la condition $\ell^h < \sqrt{r}$ est en fait une condition permettant d'avoir $k \geqslant h+1$.

6.1.2 Analyse générale

La complexité donnée pour résoudre le problème du calcul explicite de l'isogénie dans la proposition 6.3 a une dépendance polynomiale en ℓ, en pratique on souhaiterait avoir ℓ petit (voir sous-section 6.1.3) et donc on veut borner ℓ

à l'aide des paramètres d'entrée du problème : r, q afin de montrer que notre algorithme est utilisable en pratique.

Un résultat de Shparlinski et Sutherland [SS14, Theorem 1] nous permet de savoir dans quelle mesure on peut trouver des nombres premiers ℓ de Elkies pour une courbe quelconque et par conséquent donner une borne sur ℓ. Plus précisément pour presque tous les nombres premiers q et courbes $E/\mathbb{F}_q$, pour $L \geqslant \log(q)^{\varepsilon}$ pour n'importe quel $\varepsilon > 0$, on obtient asymptotiquement que la moitié des nombres premiers $\ell \leqslant L$ sont des nombres premiers de Elkies. On utilise donc ce résultat pour démontrer le théorème suivant, notamment en donnant une borne sur ℓ pour le pire des cas en fonction uniquement de r et q.

Proposition 6.4. Pour presque tous les nombres premiers q et presque toutes les courbes ordinaires E, E' définies sur $\mathbb{F}_q$, il existe un nombre premier ℓ de Elkies dans l'intervalle $[1, L]$ tel que $\ell^h < \sqrt{r}$ pour $L \in O(\log(q))$.

Démonstration. Soit une courbe E, on cherche le plus petit nombre premier de Elkies qui vérifie les conditions de la proposition 6.3. En appliquant le résultat de [SS14, Theorem 1], on fixe $L \in O(\log(q))$ tel que le produit de tous les nombres premiers de Elkies dépasse $\Omega(\sqrt{q})$. On enlève alors les nombres premiers de Elkies $\ell \leqslant L$ tels que $\ell^h > \sqrt{r}$, cette condition empêchant d'utiliser notre algorithme 10, pour de tels nombres premiers ceux-ci sont des diviseurs de d_π et leur produit est donc borné par $O(\sqrt{q})$. Ainsi il reste suffisamment de nombres premiers de Elkies satisfaisant $\ell^h < \sqrt{r}$ dans l'intervalle $[1, L]$, dans le pire des cas on a donc un nombre premier de Elkies $\ell \in O(\log(q))$ que l'on peut utiliser dans l'algorithme 10. □

Remarque 6.5. Ce résultat comme le [SS14, Theorem 1] s'applique aussi aux nombres premiers de Atkin.

On énonce donc un tout premier résultat qui nous permet par la suite de déterminer le coût pour une courbe choisie de trouver un nombre premier de Elkies dans l'intervalle $[1, L]$ pour $L \in O(\log(q))$.

Lemme 6.6. Le coût de trouver un courbe sur le cratère d'un volcan de ℓ-isogénies pour un nombre premier ℓ dans l'intervalle $[1, L]$ pour $L \in O(\log(q))$ est majoré par : $O(\log(q)^5)$.

Démonstration. En utilisant les algorithmes décrits dans [FM02] et abordés dans la sous-section 4.1.2 on peut déterminer une courbe sur le sommet du volcan de ℓ-isogénies à l'aide de $O(\ell h^2)$ factorisations du ℓ-ième polynôme modulaire. Or $h \in O(\log(q))$ et le coût de calcul du polynôme modulaire est de $O(\ell^3 \log(\ell))$ sa factorisation de $O(\mathsf{M}(\ell)\log(\ell)\log(\ell q))$ par l'algorithme de Cantor-Zassenhaus décrit dans [vzGG03, Chapter 14.5]. Ainsi le coût total pour trouver un nombre premier de ℓ de Elkies tel que $\ell^h < \sqrt{r}$ est de $O(\log(q)^5)$ en bornant ℓ par $\log(q)$. □

Remarque 6.7. Les algorithmes de [FM02] utilisés pour trouver une courbe sur le volcan de ℓ-isogénies dans la preuve du lemme 6.6 sont moins efficaces que ceux de [IJ10] et [MMRV05] mais ils ont l'avantage de fonctionner sur tous types de volcans, non-réguliers compris, d'où le fait que l'on ne considère que ceux-ci.

Corollaire 6.8. Le coût pour trouver un nombre de Elkies est de :

$$O(\sqrt{r}\mathsf{M}(\sqrt{r})\log(q)\log(\log(q)q) + \log(q)^6)$$

opérations sur $\mathbb{F}_q$, le coût pour trouver un nombre de Atkin est identique.

Démonstration. Par la proposition 6.4 on sait qu'il existe un nombre premier ℓ de Elkies (Atkin) appartenant à $[1; L]$ pour $L \in O(\log(q))$ et qui vérifie $\ell^h < \sqrt{r}$. Pour trouver un nombre premier de Elkies qui vérifie cette condition on doit tester tous les nombres premier de l'intervalle $[1; L]$ avec $L \in O(\log(q))$. On a vu dans le lemme 6.6 que pour chacun de ces nombres premiers de Elkies on trouvait une courbe sur le cratère en au plus $O(\log(q)^5)$ opérations, une fois qu'une telle courbe est trouvée sur le cratère alors on calcule une base diagonale de la ℓ^k torsion à l'aide des méthodes utilisées dans l'algorithme 6 si l'on arrive à diagonaliser la base c'est que le nombre premier testé est de Elkies et valide pour appliquer l'algorithme 10 sinon c'est un nombre premier de Atkin et l'algorithme 11 peut s'appliquer. L'algorithme 6 ayant une complexité de $O(\mathsf{R}(h+1-\beta) + \ell^2\mathsf{M}(\ell^{h+1-\beta}) + \ell\mathsf{M}(\ell^2)\log(\ell)\log(\ell q))$ (avec $h < k$ et $\ell^{2k-1} \in O(r\ell^2)$) par la proposition 5.26, en appliquant les résultats de [vzGG03, Chapter 14.5] on obtient le résultat. □

On peut dés lors énoncer le résultat suivant qui permet d'exprimer le coût de résolution du problème du «Calcul de l'isogénie explicite» en terme de r et q.

Théorème 6.9. *Pour presque tous les nombres premiers q et presque toutes les courbes ordinaires E, E' définies sur $\mathbb{F}_q$, il est possible de résoudre le problème du «Calcul explicite de l'isogénie» en un temps moyen de*

$$O\Big(\sqrt{r}\mathsf{M}(\sqrt{r}\log(q)^{1,5})\log(r)\log(\log(q))\log(\log(q)q) + r\log(q)^2\log(r)^2\mathsf{M}(r\log(q)^4)\Big)$$

Démonstration. Par le corollaire 6.8 on trouve un nombre premier de Elkies avec une complexité de $O(\sqrt{r}\mathsf{M}(\sqrt{r})\log(q)\log(\log(q)q) + \log(q)^6)$ opérations sur $\mathbb{F}_q$. Ainsi en bornant ℓ par $\log(q)$ dans la complexité obtenue à la proposition 6.3 on obtient un résultat auquel il faut rajouter le coût de la recherche de courbe sur le volcan : $O(\log(q)^6)$ par le lemme 6.6, le test pour savoir si le nombre est de Elkies est lui majoré par la complexité donnée dans la proposition 6.3. □

Ce résultat est donc à comparer avec le coût de calcul du r-ième polynôme modulaire Φ_r car les algorithmes de Elkies [Elk98], Bostan, Morain, Salvy et Schost [BMSS08] et Lercier et Sirvent [LS08] supposent que les courbes sont données sous forme d'équation de Weierstrass normalisée (ou dans le cas de Lercier et Sirvent prennent en compte ce coût) calculées à l'aide du r-ième polynôme modulaire (voir chapitres 2 et 1 pour plus de détails). Ainsi l'algorithme de Bröker, Lauter et Sutherland [BLS12], le plus rapide connu pour calculer le r-ième polynôme modulaire a une complexité de $O(r^3\log^3(r)\log\log(r))$ opérations sur $\mathbb{F}_p$ d'après [BLS12, Theorem 1], nous avons donc une complexité cubique en r supérieure à notre résultat. Nous comparons aussi la complexité énoncée dans le théorème 6.9 avec l'algorithme appelé «C2-AS-FI» de De Feo [DF11] car nous utilisons des méthodes similaires. Nous voyons donc que comparé aux résultats des théorèmes 2.26 et 2.28 nous obtenons une complexité qui est aussi quasi-quadratique en le degré de l'isogénie et pour laquelle nous nous sommes affranchis de toute dépendance polynomiale en la caractéristique.

6.1.3 Partie expérimentale

Les résultats expérimentaux ont été obtenu à partir de code implanté pour le logiciel SageMath v7.1 [The16], le code est disponible sur le projet github :`https://github.com/Hugounenq-Cyril/Two_curves_on_a_volcano`. Les calculs ont été effectué sur une machine Intel Xeon E5530 CPU avec l'horloge réglée à 2.4GHz. La partie expérimentale a été faite uniquement pour le cas $\ell = 2$ et des courbes en entrée se situant sur le cratère cyclique d'un volcan de 2-isogénies.

La construction des tours d'extensions 2-adiques, implantée elle aussi en SageMath, a été faite selon la méthode décrite dans l'article [DS15], l'étude s'est restreinte au cas favorable où $p = 1 \bmod 4$.

En pratique la recherche d'exemples s'est faite à l'aide des méthodes décrites dans les algorithmes de l'article [FM02] (voir sous-section 4.1.2) en résolvant donc les polynômes modulaires (ici Φ_2) utilisés d'après la base de données «database-kohel» implantée par David Kohel. La détermination de la forme du cratère se faisait elle à l'aide de la valeur du discriminant d_K. Un module a été fait par Sébastien Besnier [Bes14] sur Sagemath celui-ci permet d'afficher directement les volcans des ℓ-isogénies à partir d'une courbe et il est disponible à cette adresse `https://trac.sagemath.org/ticket/16942`.

Pour l'analyse des temps de calcul de notre algorithmes de Couveignes 2-adique, nous avons décomposé notre algorithme en 3 parties :

Tate Module est la première partie qui calcule une base horizontale de la ℓ^k torsion avec k le plus petit entier tel que $2^{2k-2}(2+1) > 4r$, cela représente donc les étapes 2 à 3 de l'algorithme 10 ;

Calcul Isogenie Init est la seconde partie qui calcule les listes de représentants L, L' ainsi que le polynôme T, mais aussi le polynôme $A_{1,1}$ et certains pré-calculs pour les Théorème des Restes Chinois dans l'algorithme sont aussi effectués, cela représente donc en partie les étapes 7 à 10 de l'algorithme 10 ;

Calcul Isogenie Step est la troisième partie qui calcule uniquement un polynôme d'interpolation $A_{i,j}$ puis l'interpolation de Cauchy, cela représente une itération des étapes 9 à 11 de l'algorithme 10.

Nous avons donc regroupé dans la figure 6.2 les deux premières parties qui sont en fait du pré-calcul avec notamment le calcul de bases horizontales et comparé cela avec la troisième partie qui représente l'interpolation. Nous voyons donc la linéarité en r des temps de calcul. Le comportement en escalier observé est tout à fait normal car pour toutes les isogénies de degré $\frac{\ell^{2k-2}(\ell+1)}{4} \leqslant r < \frac{\ell^{2k}(\ell+1)}{4}$ nous avons besoin de travailler avec la même taille de ℓ^k torsion. Ainsi pour différents r dans cet intervalle nous obtenons des polynômes $A_{a,b}$ et T de même degré ce qui fait que la complexité et le temps de calcul sont les mêmes. Ceci est une raison suffisante pour motiver la recherche du plus petit nombre ℓ de Elkies car alors nous aurions des paliers plus petits pour l'algorithme. Il pourrait toutefois s'avérer que pour un autre nombre de Elkies ℓ' plus grand que ℓ, r se trouve à la fin du palier $\frac{\ell'^{2k-2}(\ell+1)}{4} \leqslant r < \frac{\ell'^{2k}(\ell+1)}{4}$, il serait alors plus utile de travailler avec ℓ' plutôt que ℓ.

Comme l'étape d'interpolation va être répétée $O(r\ell)$ fois et domine la complexité de l'algorithme 10 nous comparons donc le temps de calcul obtenu pour une étape d'interpolation pour différentes tailles de corps fini. Nous présentons une première série de tests qui a été réalisé sur des courbes qui ont toutes leur $\beta = h = 2$, ainsi notre algorithme 10 a travaillé avec la 2^3 torsion jusqu'à la 2^8

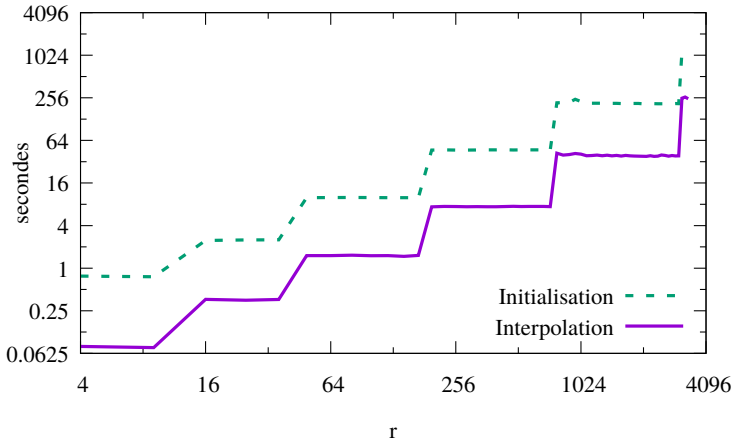


FIGURE 6.2 – Comparaison entre la phase d'initialisation et la phase d'interpolation pour une courbe définie sur $\mathbb{F}_{101}$ pour r croissant. La courbe est en échelle logarithmique.

torsion sur des courbes elliptiques définies sur corps finis premiers allant d'une taille de 7 bits à 252 bits. Le volcan de 2-isogénies de gauche de la figure 4.3 est celui sur lequel se trouve la courbe définie sur $\mathbb{F}_{101}$ ayant servi aux calculs montrés dans la figure 6.3.

Nous observons sur la figure 6.3 que la dépendance en q est plus grande que ce à quoi nous aurions pu nous attendre d'après la borne théorique, cela doit être dû à des détails d'implantation bas-niveau que SageMath ne nous permet pas de maîtriser.

La deuxième série de tests montrée sur la figure 6.4 a été réalisée sur des courbes qui ont toutes $\beta = h = 3$, définies sur des corps finis premiers de taille 9 bits. Notre algorithme 10 a donc travaillé avec la 2^4 torsion jusqu'à la 2^7 torsion des courbes elliptiques. Nous voyons ici que comme $\beta = h = 3$, alors contrairement aux précédents tests il n'y a pas de palier où nous travaillons avec la ℓ^3 torsion mais directement avec la ℓ^4 torsion. En effet il est nécessaire d'avoir k strictement supérieur à $h = 3$.

Le détail des timings pour les différentes parties est disponible sur le projet github : `https://github.com/Hugounenq-Cyril/Two_curves_on_a_volcano`.

6.2 Cas Atkin

Nous justifions tout d'abord l'intérêt de l'étude faite sur la forme de la matrice du Frobenius avec un vecteur de la base fixée par rapport à un algorithme de Couveignes [Cou96] modifié pour travailler avec la ℓ-torsion. Cette section utilise les résultats de la sous-section 5.2.

Nous énonçons donc un résultat qui est une transposition de la proposition 6.1 qui s'appliquait au cas Elkies.

Proposition 6.10. Soit $\phi : E \to E'$ une isogénie de degré r premier avec ℓ un nombre premier de Atkin.

1. les courbes E, E' ont la même profondeur dans leur volcan des ℓ-isogénies,

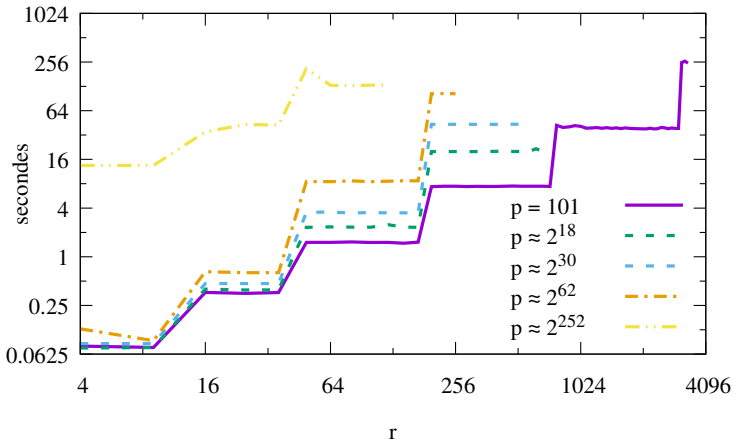


FIGURE 6.3 – Comparaison d'une phase d'interpolation pour r croissant pour différentes courbes définies sur les corps finis $\mathbb{F}_{101}$, $\mathbb{F}_{2^{18}+93}$, $\mathbb{F}_{2^{30}+669}$, $\mathbb{F}_{2^{62}+189}$ et $\mathbb{F}_{2^{252}+421}$. La courbe est en échelle logarithmique.

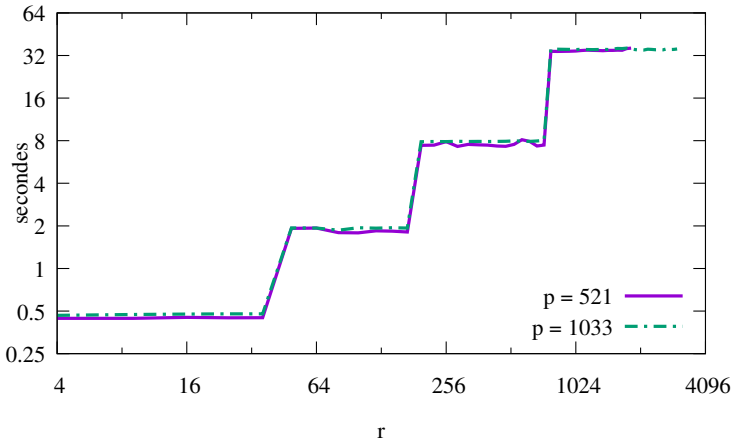


FIGURE 6.4 – Phase d'interpolation pour r croissant pour différentes courbes définies sur les corps finis $\mathbb{F}_{521}$ et $\mathbb{F}_{1033}$. La courbe est en échelle logarithmique.

2. pour tout point $P \in E[\ell^k]$, les isogénies de noyau $\langle P \rangle$ et $\langle \phi(P) \rangle$ sont de même type (ascendantes, descendantes, ou horizontales de même direction),
3. si $P \in E[\ell]$ et $P' \in E'[\ell]$ sont tous les deux des points générateurs d'isogénies ascendantes alors $E/\langle P \rangle$ et $E'/\langle P' \rangle$ sont encore r-isogènes.

Démonstration. La preuve est exactement la même que celle de la proposition 6.1, toutefois ici nous faisons référence à la proposition 5.33 pour la preuve. □

Voyons maintenant un résultat qui est une conséquence de la proposition 5.35 et qui étudie donc l'invariance des groupes de points de $E[\ell^\infty]$ déterminés par l'action du Frobenius par rapport aux actions de r-isogénies rationnelles, avec r premier avec ℓ.

Corollaire 6.11. Soit $\phi : E \to E'$ une r-isogénie avec $r \wedge \ell = 1$ et E et E' deux courbes elliptiques, soient $P \in E$ et $P' \in E'$ deux points d'ordre ℓ^k avec $k > h$ tels que $P' = \phi(P)$ alors pour deux base $(P, Q), (P', Q')$ de $E[\ell^k]$ et $E'[\ell^k]$ telles que $\pi(P, Q) = \pi(P', Q')$ on a $[\ell^h]Q' = [\ell^h]\phi(Q)$.

Démonstration. Comme le Frobenius commute avec l'isogénie ϕ alors $\pi(P, Q) = \pi(\phi(P), \phi(Q))$. De plus $P' = \phi(P)$ donc pour Q' tel que $\pi(P, Q) = \pi(P', Q')$ nous obtenons $\pi(P', Q') = \pi(\phi(P), \phi(Q))$, la proposition 5.35 nous permet alors de conclure. □

Nous rappelons que nous travaillons avec deux courbes r-isogènes, avec $r \wedge \ell = 1$, qui se situent sur un volcan de ℓ-isogénies de hauteur h, dont le cratère est réduit à une courbe (car nous nous plaçons dans le cas Atkin). Nous supposons de plus qu'un nombre ℓ de Atkin tel que $\ell^h < \sqrt{r}$ est déjà connu (pour plus de détails voir la proposition 6.4). De plus nous allons dans un premier temps nous restreindre au cas où les courbes avec lesquelles nous travaillons se situent sur le cratère d'un volcan de ℓ-isogénies, nous verrons par la suite comment généraliser notre problème à des courbes non situées sur le cratère.

Maintenant nous faisons une description de la méthode employée dans notre algorithme 11 pour résoudre le problème du calcul explicite d'isogénie. Soient E, E' deux courbes elliptiques de j-invariants j et j' reliées par une r-isogénie ϕ, $P \in E$ et $S' \in E'$ deux points d'ordre ℓ^k, avec k plus grand que h, tels que $\phi(P) = S'$. Pour deux bases $(P, Q), (S', Q')$ de $E[\ell^k]$ et $E'[\ell^k]$ nous déterminons $R' \in E'[\ell^k]$ tel que $\pi(P, Q) = \pi(S', R')$ et $\langle S', R' \rangle = E'[\ell^k]$. Par le corollaire 6.11 nous avons $\phi([\ell^h]Q) = [\ell^h]R'$. Nous déterminons ensuite le point $\phi(Q)$ en testant pour tout point U' antécédent par $[\ell^h]$ de $[\ell^h]R'$ si la correspondance $(P, Q) \to (S', U')$ permet de définir une r-isogénie. Ce test consiste, comme dans le cas Elkies (voir sous-section 6.1.1), à calculer le polynôme d'interpolation $A_{S',U'}$ tel que

$$A_{R'}(x([u]P + [v]Q)) = x([u]S' + [v]U') \quad \text{pour tout } [u]P + [v]Q \text{ d'ordre } \ell^k.$$

Ensuite à l'aide du polynôme $A_{S',U'}$ nous calculons la fraction rationnelle F telle que :

$$F = A_{S',U'} \bmod T$$

avec T le polynôme minimal qui s'annule sur tout point $[u]P + [v]Q$ d'ordre ℓ^k. C'est la fraction rationnelle F qui lorsque nous avons bien choisi U' doit

représenter la r-isogénie ϕ. Nous cherchons donc à calculer F de degré $(r, r-1)$. Or une telle fraction rationnelle est déterminée par $2r$ coefficients, nous devons donc avoir le nombre d'abscisses de points d'ordre ℓ^k : $\frac{\ell^{2k-2}(\ell+1)}{2}$ strictement plus grand que $2r$ pour avoir suffisamment d'informations.

Comme nous savons seulement que l'image de P par ϕ est un point d'ordre ℓ^k, nous proposons donc de faire la procédure décrite dans le paragraphe précédent en testant toutes les valeurs possibles pour l'image de P par ϕ, c'est à dire tous les points d'ordre ℓ^k de E'.

Nous énonçons des résultats qui sont des conséquences de la proposition 5.42 et qui nous seront utiles lors de l'étape du calcul de polynôme d'interpolation à l'aide des méthodes de la section 3.4.

Corollaire 6.12. Soit P un point d'ordre $\ell^{\beta+i}$ de la courbe elliptique E située au niveau du cratère du volcan de ℓ-isogénies telle que $E(\mathsf{F}_1)[\ell^\infty] \simeq \mathbb{Z}/\ell^\beta\mathbb{Z} \times \mathbb{Z}/\ell^\beta\mathbb{Z}$, alors la taille de l'orbite de P selon l'action de $\mathsf{Gal}(\mathsf{F}_{i+1} : \mathsf{F}_1)$ est ℓ^i.

Corollaire 6.13. Soit E une courbe elliptique située au niveau du cratère du volcan de ℓ-isogénies telle que $E(\mathsf{F}_1)[\ell^\infty] \simeq \mathbb{Z}/\ell^\beta\mathbb{Z} \times \mathbb{Z}/\ell^\beta\mathbb{Z}$, alors il y a $\ell^{2\beta+i-2}(\ell+1)$ classes de conjugaison de points d'ordre $\ell^{\beta+i}$ selon l'action de $\mathsf{Gal}(\mathsf{F}_{i+1} : \mathsf{F}_1)$.

Nous pouvons dès lors énoncer une version ℓ-adique de l'algorithme de Couveignes dans le cas Atkin dans l'algorithme 11.

Algorithme 11 Algorithme de Couveignes ℓ-adique dans le cas Atkin.

Entrée : E, E' : deux courbes elliptiques r-isogènes ordinaires situées au niveau du cratère d'un volcan de ℓ-isogénies avec cratère réduit à une courbe.
Sortie : ϕ la r-isogénie qui relie E à E'.

```
Calcul du plus petit k tel que ℓ^{2k-2}(ℓ+1) > 4r ;
Calcul de (P,Q),(P',Q') bases de E[ℓ^k], E'[ℓ^k] ;
Calcul de la matrice π(P,Q) ;
pour S' ∈ E' d'ordre ℓ^k faire
    Calcul de R' ∈ E' tel que π(S',R') = π(P,Q) à l'aide de l'algorithme 9
    pour U' ∈ E' tel que [ℓ^h]U' = [ℓ^h]R' faire
        Calcul des listes de représentants pour les orbites selon l'action du Frobenius L et L'_{U',R'} afin de respecter la correspondance induite par le choix de U' et R' ;
        Calcul des des polynômes A_{S',U'} et T par les méthodes décrites dans la section 3.4 ;
        Calcul de la fraction rationnelle F = A_{S',U'} mod T à l'aide d'une interpolation de Cauchy ;
        si Test(F) alors
            retourner F
        fin si
    fin pour
fin pour
```

Proposition 6.14. En supposant que $\ell^h < \sqrt{r}$, l'algorithme 11 calcule une r-isogénie $\phi : E \to E'$ avec un coût moyen de

$$O(r\ell^2\ell^{2h}(\mathsf{M}(r\ell^4)\log(r)\log(\ell) + \mathsf{M}(\sqrt{r}\ell^{1,5})\sqrt{r}\log(\ell)\log(\ell q))$$

auquel il faut ajouter un temps de pré-calcul de : $O(r\mathsf{M}(\sqrt{r})\log(r)\log(\ell) + \sqrt{r}\mathsf{M}(\sqrt{r})\log(\ell)\log(\ell q))$.

Démonstration. Nous faisons remarquer que la condition $\ell^h < \sqrt{r}$ signifie que $k > h$, nous allons utiliser cette condition tout au long de la preuve. Par définition de k nous avons $\ell^{2k-1} \in O(r\ell^2)$. Par la proposition 5.42, il existe $\beta \leqslant h$ tel que $E[\ell^k]$ est inclus dans $E(F_{k-\beta})$. Nous construisons donc une tour d'extensions ℓ-adiques $\mathsf{F}_0 \subset \cdots \subset \mathsf{F}_{k-\beta}$, et nous effectuons les pré-calculs nécessaires au théorème 3.6 avec un coût de $O(\ell\mathsf{M}(\ell)\log(q))$. À l'étape 2 le coût de calcul des bases de la ℓ^k-torsion se fait à partir d'une base de la ℓ-torsion puis nous inversons la multiplication par ℓ l'aide de deux ℓ-isogénies qui composent la multiplication par ℓ. Par le lemme 5.21 le coût de calcul de $E[\ell]$ est de $O(\ell\mathsf{M}(\ell^2)\log(\ell)\log(\ell q))$ opérations sur $\mathbb{F}_q$, ensuite le coût de calcul de divise(ℓ, P) pour $P \in E(F_n)$ est de $\mathsf{R}(n+1)$, ce coût est donc dominé par la dernière étape $O(\mathsf{R}(k-\beta+1) + \ell\mathsf{M}(\ell^2)\log(\ell)\log(\ell q))$. Par [vzGG03, Chapter 14.5] nous avons $\mathsf{R}(n) = O(\ell^n\mathsf{M}(\ell^{n+1})\log(\ell)\log(\ell q))$. L'étape 2 a donc un coût total de

$$O(\ell^k\mathsf{M}(\ell^{k+1})\log(\ell)\log(\ell q)) = O(\sqrt{r}\ell^{1,5}\mathsf{M}(\sqrt{r}\ell^{2,5})\log(\ell)\log(\ell q))$$

dans le pire des cas où $\beta = 1$.

De la même manière que l'algorithme 9 à l'étape 3 nous calculons itérativement l'action du Frobenius sur la ℓ^j-torsion pour j allant de 1 à k, ainsi à l'étape $i \in [1;k]$ le coût du Frobenius appliqué à un point de $\mathsf{F}_{i-\beta}$ lorsque $i > \beta$, F_1 sinon, est de $O(\ell^{\max(1,i-\beta)}\mathsf{M}(\ell))$ opérations sur $\mathbb{F}_q$ d'après le théorème 3.6. Nous effectuons ensuite jusqu'à $2\ell^2$ additions de points définis sur $\mathsf{F}_{i-\beta}$ afin d'identifier l'action du Frobenius. Chaque étape a donc un coût de $O(\ell^2\mathsf{M}(\ell^{\max(1,i-\beta)}))$, le coût total de l'étape 3 est donc de $O(\ell^2(\beta\mathsf{M}(\ell) + \mathsf{M}(\ell^{k-\beta+1}))) = O(\ell^2(\mathsf{M}(\ell) + \mathsf{M}(\sqrt{r}\ell^{1,5})))$ opérations sur $\mathbb{F}_q$ dans le pire des cas où $\beta = 1$.

Le calcul de tous les points d'ordre ℓ^k à l'étape 4 à partir d'une base de $E'[\ell^k]$ coûte $O(\mathsf{M}(\ell^k)\log(\ell^k)\ell^{2k}) = O(\mathsf{M}(\sqrt{r}\ell^{1,5})r\ell^3\log(r)\log(\ell))$ ce coût est considéré comme un pré-calcul.

L'étape 5 a un coût de $O(\ell^4(\mathsf{M}(\ell^{k-\beta+1}) + \beta\mathsf{M}(\ell)))$ opérations sur $\mathbb{F}_q$ d'après la proposition 5.44. Ce qui donne un coût de $O(\ell^4(\mathsf{M}(\sqrt{r}\ell^{1,5}) + \mathsf{M}(\ell)))$.

L'étape 6 calcule les antécédents d'un point d'ordre ℓ^{k-h} par $[\ell^h]$ ainsi nous utilisons successivement la fonction divise(ℓ, P) sur des points définis dans $\mathsf{F}_{k-h-\beta}$ à $\mathsf{F}_{k-\beta}$, chaque itération de divise(ℓ, P) a un coût de $R(n+1)$ pour $P \in \mathsf{F}_n$ par le lemme 5.21. Ainsi par [vzGG03, Chapter 14.5] cette étape a un coût total de : $O(\mathsf{M}(\ell^{k-\beta+1})\ell^{k-\beta}\log(\ell)\log(\ell q) + \beta(\mathsf{M}(\ell^2)\ell\log(\ell)\log(\ell q)))$ ce qui donne dans le pire des cas $O(\mathsf{M}(\sqrt{r}\ell^{1,5})\sqrt{r}\ell\log(\ell)\log(\ell q))$.

Par le corollaire 6.13 nous avons $\ell^{k+\beta-2}(\ell+1)/2$ représentants à calculer, chaque représentant étant calculé comme la multiplication scalaire d'un point d'ordre ℓ^k défini dans $\mathsf{F}_{k-\beta}$ par un coefficient dans $(\mathbb{Z}/\ell^k\mathbb{Z})^\times$ une telle multiplication a un coût de $O(\log(\ell^k)\mathsf{M}(\ell^{k-\beta}))$. Le coût total de total est donc $O(\mathsf{M}(\ell^{2k})\log(\ell^k)) = O(\mathsf{M}(r\ell^3)\log(r))$ opérations sur $\mathbb{F}_q$ pour l'étape 7.

Pour l'étape 8 à l'aide de la proposition 3.12 avec $t = \ell^{2k-2}(\ell+1)/2 \in O(r\ell^2)$ et le nombre de points d'interpolations $s = \ell^{k+\beta-2}(\ell+1)$, nous calculons les polynômes T et $A_{U',R'}$ avec un coût de $O(\mathsf{M}(r\ell^4)\log(r)\log(\ell))$.

L'étape 9 a une complexité de $O(r\log(r))$ d'après [BCG+17, Théorème 7.5]. Le coût du test de la fraction rationnelle est dominé par les autres opérations (pour plus de détails le lecteur peut voir la preuve de la proposition 6.3). Les

étapes 6 à 10 étant répétées ℓ^{2h} fois celles-ci ont une complexité de $O(\ell^{2h}(\mathsf{M}(r\ell^4)\log(r)\log(\ell)+\mathsf{M}(\sqrt{r}\ell^{1,5})\sqrt{r}\log(\ell)\log(\ell q)))$ à S' fixé.

Enfin l'étape 3 et la boucle commençant à l'étape 4 étant répétées $\ell^{2k-2}(\ell+1)/2 \in O(r\ell^2)$ fois cela donne une complexité de $O(r\ell^2\ell^{2h}(\mathsf{M}(r\ell^4)\log(r)\log(\ell)+\mathsf{M}(\sqrt{r}\ell^{1,5})\sqrt{r}\log(\ell)\log(\ell q))$ à laquelle il faut ajouter les pré-calculs pour obtenir le résultat. □

L'expression en ℓ^{2h} dans le calcul de complexité a été délibérément laissée dans la complexité énoncée afin de montrer l'influence de la boucle entre les étapes 6 à 10 et de pouvoir énoncer le résultat suivant intéressant pour les volcans de Atkin de hauteur 0.

Corollaire 6.15. En supposant que $h = 0$, l'algorithme 11 calcule une r-isogénie $\phi : E \to E'$ avec un coût moyen de

$$O(r\ell^2(\mathsf{M}(r\ell^5)\log(r)\log(\ell) + \mathsf{M}(\sqrt{r}\ell^{2,5})\sqrt{r}\log(\ell)\log(\ell q))$$

auquel il faut ajouter un temps de pré-calcul de : $O(r\mathsf{M}(\sqrt{r}\ell)\log(r)\log(\ell) + \sqrt{r}\mathsf{M}(\sqrt{r}\ell)\log(\ell)\log(\ell q))$.

Il faut tout de même préciser que dans ce cas-là le premier étage de la tour d'extensions sera de degré d_1 avec $d_1|\ell^2 - 1$ (voir remarque 5.39), ce qui asymptotiquement ne change pas grandement l'analyse mais qui a ajouté un facteur ℓ dans le calcul de la complexité.

Maintenant nous abordons le cas général où les courbes r-isogènes ne sont pas situées sur le cratère du volcan de ℓ-isogénies. Par la proposition 6.10(1), la profondeur de E et E' sous leur cratère respectif est la même, par 6.10 (3), les courbes sommets E_s et E'_s sont encore r-isogènes ; nous notons les isogénies $\alpha : E \to E_s$ et $\alpha' : E' \to E'_s$. Nous utilisons alors l'algorithme 11 pour calculer une r-isogénie ψ_s. Ensuite comme $\ell \wedge r = 1$ alors $\psi = (\alpha')^{-1} \circ \psi_s \circ \alpha$ est bien définie et est la r-isogénie cherchée. Le noyau de cette isogénie peut être calculé en $O(h\mathsf{M}(\ell r)\log(\ell r))$ opérations en évaluant l'isogénie duale $\widehat{\alpha}$ sur le noyau de ψ_s à l'aide d'une suite de résultants.

Comme dit précédemment les résultats du de la proposition 6.4, du lemme 6.6, et du corollaire 6.8 sont aussi valables dans le cas Atkin, nous pouvons donc trouver un $\ell \in O(\log(q))$ nombre premier de Atkin tel que $\ell^h < \sqrt{r}$ et énoncer un résultat similaire à celui du théorème 6.9. Vu le peu d'intérêt, par rapport au cas Elkies, d'un tel résultat nous ne l'énoncerons pas. Cependant il est à noter que la complexité obtenue à la proposition 6.14 est meilleure que Lercier et Sirvent [LS08].

6.3 Conclusion

Nous avons donc vu deux cas où l'on a un algorithme de Couveignes ℓ-adique quasi-quadratique : la proposition 6.3 et le corollaire 6.15. On peut alors énoncer la borne suivante pour trouver un premier ℓ qui permette de résoudre le problème du calcul explicite de l'isogénie en temps quasi-quadratique.

Théorème 6.16. *Soient q une puissance d'un nombre premier, deux courbes elliptiques ordinaires E, E' définies sur $\mathbb{F}_q$, un entier r tel que E et E' soient r-isogènes, alors la r-isogénie peut être calculée avec une complexité de*

$$\tilde{O}(r^2\log(q)^8) \text{ opérations sur } \mathbb{F}_q$$

en ayant borné le paramètre ℓ par $O(\log(q))$.

Démonstration. L'idée est de montrer que l'on peut trouver un premier ℓ de Elkies ou de Atkin pour un volcan de hauteur $h = 0$ borné par $O(\log(q))$, ainsi avec un tel premier on pourra conclure avec soit la proposition 6.3 soit le corollaire 6.15. d_π est borné par $O(q)$ par le théorème de Hasse. Les nombres de Elkies et d'Atkin pour des volcans de hauteur strictement positive sont des diviseurs de d_π, de tels nombres ainsi que les entiers qui divisent d_K sont bornés par $O(\log(q))$. On peut donc trouver un nombre de Elkies ou de Atkin pour un volcan de hauteur $h = 0$ borné par $O(\log(q))$. □

Chapitre 7

Variantes de l'algorithme de Couveignes ℓ-adique dans le cas Elkies

Dans les améliorations de l'algorithme de Couveignes que nous avons présentées celles concernant le cas Elkies ont un meilleur résultat en terme de complexité lorsque $h \neq 0$. Nous allons donc étudier des variantes à l'algorithme de Couveignes avec approche ℓ adique que dans le cas Elkies y compris lorsque celles-ci auraient pu être appliquées à notre approche proposée pour le cas Atkin.

7.1 Algorithme de Couveignes ℓ-adique dans le cas Elkies avec un point horizontal

Au lieu de travailler avec une base (ascendante) horizontale dans l'algorithme de Couveignes ℓ-adique nous pourrions tout aussi bien travailler avec un point (ascendant) horizontal. C'est l'approche que nous allons avoir dans cette sous-section. Dés lors nous devons déterminer le plus petit entier k tel que le nombre d'abscisses de points d'ordre ℓ^k engendrés par un point d'ordre ℓ^k : $\frac{\ell^{k-1}}{2}$ soit strictement plus grand que $2r$.

Pour le calcul du point horizontal d'ordre ℓ^k nous sommes tout de même obligés de calculer une base diagonale de la ℓ^{h+1}-torsion et donc de travailler dans l'élément $\mathsf{F}_{h+1-\beta}$ de la tour d'extensions ℓ-adiques.

Proposition 7.1. Soit k tel que $\ell^{k-1} \in O(r\ell)$, alors pour $h < k$ le coût de calcul d'une base diagonale de la ℓ^{h+1} torsion à l'aide de l'algorithme 7 est de :

$$O(r\ell^2\mathsf{M}(r\ell^3)\log(\ell)\log(\ell q))$$

Démonstration. Nous travaillons, toujours, avec la convention $\alpha \geqslant \beta$, avec α et β définis comme dans la définition 5.17. Le coût de calcul de la base horizontale est par la proposition 5.27 : $O(\mathsf{R}(h+1)+\mathsf{R}(k-\beta)+\ell^2\mathsf{M}(\ell^{h+1})+\ell\mathsf{M}(\ell^2)\log(\ell)\log(\ell q))$. En bornant h par k nous avons $\ell^h \in O(r\ell)$ ce qui en utilisant cette borne et le coût de $\mathsf{R}(i)$ donné par [vzGG03, chapter 14.5] nous donne une complexité de : $O(r\ell^2\mathsf{M}(r\ell^3)\log(\ell)\log(\ell q))$. □

Nous observons que dans ce cas-là on a un coût quadratique en r pour le calcul d'une base diagonale de la ℓ^{h+1} alors que dans le cas de la proposition 6.3 nous montrions dans la preuve que le coût d'une telle opération était quasi-linéaire.

Ensuite nous calculons un point horizontal d'ordre ℓ^k à l'aide de l'algorithme 8. Nous rappelons qu'ici comme on détermine un seul sous-groupe cyclique on choisit de travailler avec celui défini sur la plus petite extension ℓ-adique : $\mathsf{F}_{k-\alpha}$ d'où le fait que l'on ait α ici et non β (α et β ont été définis dans 5.17). Le calcul du point horizontal a un coût de $O(\mathsf{R}(k-\alpha)+k\mathsf{R}(h-\alpha+1)+k\ell^2\mathsf{M}(\ell^{h-\alpha+1}))$ d'après la proposition 5.28, ce qui appliqué à notre cas donne une complexité de : $O(r\ell\mathsf{M}(r\ell^2)\log(\ell)\log(\ell q)\log(r))$.

Pour le calcul du polynôme d'interpolation nous utilisons des méthodes similaires à celles de la section 3.4 mais plus proches de celles de [DF11, §5] car ici nous travaillons uniquement avec un sous-groupe cyclique défini dans $\mathsf{F}_{k-\alpha}$. Nous avons au plus $\frac{\ell^{k-1}}{\ell^{k-\alpha}} = \ell^{\alpha-1}$ représentants des orbites selon l'action du Frobenius à calculer dans $\mathsf{F}_{k-\alpha}$. Le calcul de ces représentants a un coût de $O(\ell^{\alpha-1}\mathsf{M}(\ell^{k-\alpha})\log(\ell^k)) \subset O(\mathsf{M}(r\ell)\log(r)\log(\ell))$ opérations.

Ensuite nous devons calculer le polynôme d'interpolation, en appliquant le résultat de la proposition 3.12 avec $t = \ell^{k-1} \in O(r\ell)$, $s = \ell^{\alpha-1}$, $n = k-\alpha$ nous obtenons une complexité de $O(\mathsf{M}(\ell^3 r)\log(\ell)\log(r))$ qui est l'étape dominante dans les étapes 9 à 11 de l'algorithme 10.

Ainsi pour le calcul de la r-isogénie nous devons répéter l'étape d'interpolation ℓ^{k-1} fois ce qui nous donne un coût total de : $O(r\ell\mathsf{M}(\ell^3 r)\log(\ell)\log(r))$ opérations sur $\mathbb{F}_q$.

L'algorithme décrit ici est retranscrit dans l'algorithme 14 en appendice A afin de ne pas surcharger ce document car comme vu juste au-dessus il est très similaire à l'algorithme 10.

Proposition 7.2. Soit ℓ un nombre de Elkies tel que $\ell^h < r$ alors le coût moyen de la variante de l'algorithme de Couveignes ℓ-adique avec détermination d'un seul point horizontal présenté dans l'algorithme 14 est de :

$$O(r\ell\log(\ell)(\mathsf{M}(r\ell^3)(\log(r)+\ell\log(q))+\mathsf{M}(r\ell^2)\log(\ell q)\log(r)))$$

opérations sur $\mathbb{F}_q$.

Le coût de cette variante de Couveignes ℓ-adique dans le cas Elkies a donc une complexité qui est un peu plus faible que le résultat obtenu à la proposition 6.3 avec un facteur ℓ en moins dans le calcul du polynôme d'interpolation. Ce facteur ℓ en moins vient du fait que nous travaillons avec le plus petit k tel que $\ell^{k-1} > 4r$ au lieu de $\ell^{2k-2}(\ell+1) > 4r$, dés lors nous obtenons une meilleure précision dans le cas de cette variante pour le choix de k, ceci explique que le coût du calcul du polynôme d'interpolation est moins élevé de ce facteur ℓ.

Nous pourrions alors penser que cette variante est meilleure que l'algorithme 10 cependant l'algorithme 10 travaille dans des extensions de corps plus petites. De plus notre estimation du nombre d'abscisses de points différentes utilisées lors de l'interpolation est toujours très pessimiste car nous pourrions nous contenter de prendre un nombre d'abscisses plus grand que $4r$, tout en ayant que des orbites complètes pour le Frobenius. Dès lors nous ne travaillerions pas avec $O(r\ell^2)$ abscisses lors de l'étape d'interpolation. Cependant la taille des orbites est comprise entre $\ell^{k-\beta}$ et $\ell^{k-\alpha}$ dans notre approche (voir chapitres 5 et 6). Nous aurions pu travailler avec des orbites de taille plus petites si nous avions

utilisé uniquement des courbes situées sur le cratère du volcan de ℓ-isogénies. En effet nous aurions pu utiliser des points d'ordre compris entre ℓ^k et ℓ^{k-h}. Ceci nous aurait permis de travailler avec des orbites plus petites et donc d'approcher $4r$ avec plus de précision.

Une différence notable est que dans cette variante la complexité pour le calcul d'une base diagonale de la ℓ^{h+1} torsion est quadratique alors que dans l'algorithme 10 cette partie est seulement quasi-linéaire en r. Ainsi l'algorithme 10 présente l'avantage d'avoir une partie quasi-linéaire fixe et une partie variable (pour le calcul de l'interpolation) quasi-quadratique en r avec un aléa qui varie dans $O(r\ell)$ d'où le fait que cette variante ne propose pas de grand avantage par rapport à l'algorithme 10.

Cette variante de l'algorithme 10 proposé dans le cas Elkies non transposable à l'algorithme 11 proposé dans le cas Atkin souligne le fait que l'étude de l'action du Frobenius dans le cas Elkies nous permet de spécifier des sous-groupe cycliques invariants sous l'évaluation de r-isogénies (avec $r \wedge \ell = 1$), alors que dans le cas Atkin nous ne pouvons que déterminer un sous-groupe cyclique à partir de la connaissance d'un autre sous-groupe cyclique.

Maintenant voyons d'autres pistes d'améliorations de l'algorithme de Couveignes ℓ-adique. Nous pourrions penser à utiliser l'algorithme de Couveignes ℓ-adique avec différents nombres de Elkies $\ell_1, \ell_2, \ell_3, \ldots, \ell_n$, pour une isogénie de degré r premier avec tous les ℓ_i. Nous calculons alors des bases (ascendantes) horizontales de la $\ell_i^{k_i}$ torsion, on peut travailler avec les deux ensembles de points :

— $\cup_{i=1}^{n} \mathbb{Z}/\ell_i^{k_i}\mathbb{Z} \times \mathbb{Z}/\ell_i^{k_i}\mathbb{Z}$,
— $\prod_{i=1}^{n} \mathbb{Z}/\ell_i^{k_i}\mathbb{Z} \times \mathbb{Z}/\ell_i^{k_i}\mathbb{Z}$.

Nous allons détailler chacune de ces approches dans les deux sous-sections qui suivent.

7.2 Algorithme de Couveignes ℓ-adique avec différents nombres de Elkies

La première approche est de considérer l'ensemble de points S isomorphe à : $\cup_{i=1}^{n} \mathbb{Z}/\ell_i^{k_i}\mathbb{Z} \times \mathbb{Z}/\ell_i^{k_i}\mathbb{Z}$, avec les ℓ_i tous des nombres premiers de Elkies. Dés lors il faut fixer comme condition $\sum_{i=1}^{n} \ell_i^{2k_i-2}(\ell_i + 1) > 4r$, afin que le polynôme d'interpolation que l'on cherche à construire puisse définir la fraction rationnelle F candidate pour représenter la r-isogénie ϕ que l'on veut calculer. L'avantage de cette approche est que bien que nous soyons obligés de travailler sur différentes tours d'extensions ℓ-adiques, il n'est pas nécessaire de travailler avec des composita de tours d'extensions ℓ-adiques.

Détaillons comment nous procédons, la méthode est retranscrite dans l'algorithme 12.

Les étapes 3 à 4 de l'algorithme 12 qui calculent une base (ascendante) horizontale et des représentants des orbites de points (ascendants) horizontaux d'ordre $\ell_i^{k_i}$ sous l'action du Frobenius sont faites en parallèle sur chacune des tours d'extension ℓ_i-adiques, les méthodes utilisées sont les mêmes que celles dans l'algorithme 10. Par les propositions 6.1 et 6.2 pour tout i ϕ peut être représentée sur une base $(P_{\lambda,i}, Q_{\mu,i})$ (ascendante) horizontale de $E[\ell_i^{k_i}]$ de la fa-

Algorithme 12 Algorithme de Couveignes ℓ-adique avec différents nombres de Elkies

Entrée : E, E' : deux courbes elliptiques r-isogènes ordinaires situées au niveau $h_i - e_i$ d'un volcan de ℓ_i-isogénies avec cratère cyclique.
Sortie : ϕ la r-isogénie qui relie E à E'.

1: Calcul des k_i tel que $\sum_{i=1}^{n} \ell_i^{2k_i-2}(\ell_i+1) > 4r$;
2: **pour** $i = 1$ à n **faire**
3: Calcul de $(P_{\lambda,i}, Q_{\mu,i}), (P'_{\lambda,i}, Q'_{\mu,i})$ bases (ascendantes) horizontales de $E[\ell_i^{k_i}], E'[\ell_i^{k_i}]$ à l'aide de l'algorithme 7 et de l'étape 3 de l'algorithme 10 ;
4: Calcul des liste de représentants L_i, L'_i des orbites de points d'ordre $\ell_i^{k_i}$ sous l'action de π ;
5: **fin pour**
6: **pour** $M \in \mathsf{diag}(a, b)$ avec $a, b \in \left(\mathbb{Z}/\prod_{i=1}^{n} \ell_i^{k_i}\mathbb{Z}\right)^{\times}$ **faire**
7: **pour** $M_i \in \mathsf{diag}(a_i, b_i)$ avec $a = a_i \bmod \ell_i^{k_i}, b = b_i \bmod \ell_i^{k_i}$ **faire**
8: Actualisation de la liste des représentants L'_i en $L'_{a,b,i}$ afin de respecter la correspondance induite par le choix de M_i ;
9: Calcul des des polynômes $A_{a,b,i}$ et T_i par les méthodes décrites dans la section 3.4 ;
10: **fin pour**
11: Calcul des polynômes $A_{a,b}$ et T à l'aide d'un théorème des restes chinois appliqué sur tous les $A_{a,b,i}$ et T_i ;
12: Calcul de la fraction rationnelle $F = A_{a,b} \bmod T$ à l'aide d'une interpolation de Cauchy ;
13: **si** $\mathsf{Test}(F)$ **alors**
14: **retourner** F
15: **fin si**
16: **fin pour**

çon suivante : $\phi\begin{pmatrix} P_{\lambda,i} \\ Q_{\mu,i} \end{pmatrix} = \begin{pmatrix} a_i & 0 \\ 0 & b_i \end{pmatrix}\begin{pmatrix} P'_{\lambda,i} \\ Q'_{\mu,i} \end{pmatrix}$ avec $a_i, b_i \in \left(\mathbb{Z}/\ell_i^{k_i}\mathbb{Z}\right)^\times$ et $(P'_{\lambda,i}, Q'_{\mu,i})$ base (ascendante) horizontale de $E'[\ell_i^{k_i}]$.

Nous définissons à l'aide du théorème des restes chinois deux coefficients $a, b \in \left(\mathbb{Z}/\prod_{i=1}^n \ell_i^{k_i}\mathbb{Z}\right)^\times$ tels que $a = a_i \bmod \ell_i^{k_i}$ et $b = b_i \bmod \ell_i^{k_i}$ pour $i \in [1, n]$. Nous calculons ensuite pour chaque couple de coefficients $(a, b) \in (\mathbb{Z}/\prod_{i=1}^n \ell_i^{k_i}\mathbb{Z})^\times$, à l'aide des méthodes de la section 3.4 appliquées à chacune des tours d'extensions ℓ_i-adiques, les polynômes d'interpolation $A_{a,b,i}$ et T_i définis dans $\mathbb{F}_q$. Alors par le théorème des restes chinois appliqué à ces polynômes nous obtenons les polynômes $A_{a,b}, T \in \mathbb{F}_q[x]$ tels que :

$$A_{a,b} = A_{a,b,i} \bmod T_i \text{ pour tout } i \in [1, n] \text{ et } \quad T = \prod_{i=1}^n T_i$$

Nous calculons ensuite la fraction rationnelle $F = A_{a,b} \bmod T$ à l'aide d'une interpolation de Cauchy. Nous testons si celle-ci est bien une r-isogénie, si cela n'est pas le cas alors nous recommençons avec d'autres coefficients $a, b \in (\mathbb{Z}/\prod_{i=1}^n \ell_i^{k_i}\mathbb{Z})^\times$.

Analyse du coût Une telle approche a forcément des coûts de pré-calcul (pour le calcul des bases (ascendantes) horizontales et des représentants) plus faibles que notre approche dans l'algorithme 10. De même dans la boucle que nous effectuons pour chaque choix de coefficients $a, b \in (\mathbb{Z}/\prod_{i=1}^n \ell_i^{k_i}\mathbb{Z})^\times$ le calcul des polynômes $A_{a,b,i}$ et T_i définis dans $\mathbb{F}_q$ est inférieur au calcul de $A_{a,b}$ et T à l'étape 10 de l'algorithme 10. Cependant le coût de calcul de l'interpolation de Cauchy est de $O(\mathsf{M}(r)\log(r))$ par [BCG+17, Théorème 7.5]. Sachant que nous devons répéter en moyenne cette boucle pour tous les a, b possibles appartenant à $(\mathbb{Z}/\prod_{i=1}^n \ell_i^{k_i}\mathbb{Z})^\times$ le coût d'un tel algorithme est minoré par $\Omega(\prod_{i=1}^n \ell_i^{2k_i-2}\mathsf{M}(r)\log(r))$ et donc en particulier par $\Omega(r\mathsf{M}(r)\log(r))$.

Une telle approche serait bien évidemment meilleure que l'algorithme 10 si nous avions un moyen de préciser si un polynôme A_{a,b,i_0} était correct sans connaître la valeur des autres $A_{a,b,i}$, dans un cas comme celui-ci nous aurions à tester $\sum_{i=1}^n \ell_i^{2k_i-2} \in \Theta(r)$ choix possibles pour le polynôme d'interpolation, comme dans l'algorithme 10.

Le principal inconvénient de cette approche c'est que nous fixons comme condition sur les k_i : $\sum_{i=1}^n \ell_i^{2k_i-2}(\ell_i + 1) > 4r$ à cause du théorème des restes chinois à appliquer sur tous les $A_{a,b,i}$. Nous voudrions dés lors travailler avec des k_i sur lesquels nous aurions comme condition nécessaire : $\prod_{i=1}^n \ell_i^{2k_i-2}(\ell_i + 1) > 4r$. C'est ce que nous allons aborder dans la seconde approche avec des points (ascendants) horizontaux d'ordre composé $\prod_{i=1}^n \ell_i^{k_i}$.

7.3 Algorithme de Couveignes ℓ-adique généralisé avec un nombre composé de Elkies

Dans cette approche nous voulons travailler avec des points d'ordre $\prod_{i=1}^n \ell_i^{k_i}$ qui arrivent à porter l'information donnée par les bases (ascendantes) horizontales $(P_{\lambda_i}, Q_{\mu_i})$ de $E[\ell_i^{k_i}]$ avec ℓ_i un nombre premier de Elkies. Pour cela nous

avons besoin de définir quelques notions, nous allons supposer sans perte de généralités que les k_i pour $i \in [1, n]$ sont fixés tels que l'on ait $\prod_{i=1}^{n} \ell_i^{2k_i-2}(\ell_i+1) > 4r$.

7.3.1 Théorème des Restes Chinois et son application à l'algorithme de Couveignes ℓ-adique

Notation 7.3. Introduisons la notation suivante afin d'alléger l'écriture par la suite : $\upsilon_n = \prod_{i=1}^{n} \ell_i^{k_i}$, $\vartheta_i = \frac{\upsilon_n}{\ell_i^{k_i}}$.

Nous énonçons une généralisation du théorème des restes chinois pour une courbe elliptique à n nombres premiers distincts.

Théorème des Restes Chinois sur une courbe Elliptique E Soient $\ell_1, \ldots, \ell_n$ n nombres premiers distincts, les points $P_1 \in E[\ell_1^{k_1}], \ldots, P_n \in E[\ell_n^{k_n}]$, alors par le Théorème des Restes Chinois il existe un point $P \in E[\upsilon_n]$ tel que $[\vartheta_{i_0}]P = P_{i_0}$ pour $i_0 \in [1, n]$.
Nous présentons tout d'abord en appendice A l'algorithme 15 qui prend en entrée un point P_i d'ordre $\ell_i^{k_i}$ et calcule alors un point P d'ordre υ_n tel que $[\vartheta_i]P = P_i$ et $[\ell_i^{k_i}]P$ pour $i \in [1, n]$. À l'aide de l'algorithme 15 nous résolvons le Théorème des Restes Chinois (TRC) comme montré dans l'algorithme 16 lui aussi en appendice A.

Cette approche du TRC a été motivée pour l'appliquer à des points (ascendants) horizontaux d'ordre $\ell_i^{k_i}$, la proposition suivante montre que cette utilisation du TRC fait sens dans le contexte de l'algorithme de Couveignes.

Proposition 7.4. Soient ℓ_1, ℓ_2 deux nombres premiers distincts de Elkies, $P_1 \in E[\ell_1^{k_1}]$ un point horizontal d'ordre $\ell_1^{k_1}$ et de direction λ_1, $P_2 \in E[\ell_2^{k_2}]$ un point horizontal d'ordre $\ell_2^{k_2}$ et de direction λ_2. Soit $P \in E[\mathbb{Z}/\ell_1^{k_1}\ell_2^{k_2}\mathbb{Z}]$ un point d'ordre $\ell_1^{k_1}\ell_2^{k_2}$ tel que $\ell_1^{k_1}P = P_2$ et $\ell_2^{k_2}P = P_1$. Soit ϕ une isogénie de degré r premier avec ℓ_1, ℓ_2 alors $\phi(P)$ est tel que

- $\ell_1^{k_1}\phi(P)$ est un point horizontal d'ordre $\ell_2^{k_2}$ et de direction λ_2,
- $\ell_2^{k_2}\phi(P)$ est un point horizontal d'ordre $\ell_1^{k_1}$ et de direction λ_1,

Démonstration. Par un raisonnement similaire à la preuve de la proposition 6.1, comme ϕ est de degré r premier avec ℓ_1 et ℓ_2 alors il y a un isomorphisme de modules de Tate qui commute avec le Frobenius. □

Corollaire 7.5. La proposition 7.4 se généralise à n nombre premiers de Elkies distincts premiers avec r.

Notation 7.6. Soient $\ell_1, \ldots, \ell_n$ n nombres premiers de Elkies distincts, P un point d'ordre υ_n de E construit à l'aide du Théorème des Restes Chinois (voir algorithme 16) tel que $[\vartheta_i]P = P_i$ avec P_i des points (ascendants) horizontaux de direction λ_i et profondeur e_i, alors on dit que P est de direction $(\lambda_1, \ldots, \lambda_n)$ et de profondeur $(e_1, \ldots, e_n)$.

Remarque 7.7. Soient E, E' deux courbes elliptiques r-isogènes avec r premier avec les nombres de Elkies $\ell_1, \ldots, \ell_n$ un point $P \in E$ d'ordre υ_n, de direction $(\lambda_1, \ldots, \lambda_n)$ et profondeur $(e_1, \ldots, e_n)$. Par le corollaire 7.5 P a pour image par ϕ un point $[a]P' \in E'$ avec $a \in (\mathbb{Z}/\upsilon_n\mathbb{Z})^\times$ et P' un point d'ordre υ_n, de direction $(\lambda_1, \ldots, \lambda_n)$ et profondeur $(e_1, \ldots, e_n)$.

7.3.2 Construction de composita d'extensions ℓ_i-adiques

Cette partie s'appuie sur la construction de compositum à partir d'une idée de [DFDS14], cet article donne aussi le moyen de calculer à un coût sous-quadratique le changement de représentation d'éléments du compositum. Nous voulons donc construire un corps dans lequel nous pourrions représenter des points d'ordre υ_n construits à l'aide de points d'ordre $\ell_i^{k_i}$ représentés dans des tours d'extensions ℓ_i-adiques comme celles décrites dans le chapitre 3. Afin de ne pas surcharger la lecture de ce document de nombreuses preuves étant l'adaptation de techniques présentées dans le chapitre 3 elles ne seront pas détaillées.

Soient $\ell_1, \ldots, \ell_n$ n nombres premiers distincts, nous allons supposer dans le reste de ce document que les différentes tours d'extensions ℓ_i-adiques sont définies comme dans le chapitre 3 dont nous notons les éléments $\mathbb{F}_q \subset \mathsf{F}_{(i,1)} \subset \cdots \subset \mathsf{F}_{(i,j)}$ et ont chacune des degrés $d_{(i,1)} = [\mathsf{F}_{(i,1)} : \mathbb{F}_q]$ qui lorsqu'ils ne sont pas égaux à 1 doivent être premiers entre eux (cette dernière restriction sera justifiée plus tard dans le document).

Nous voulons donc tout d'abord définir un compositum de tours d'extensions ℓ_i-adiques, en particulier nous voulons calculer un compositum qui contient tous les éléments des tours d'extensions ℓ_i-adiques suivant : $\mathsf{F}_{(1,k_1)}, \ldots \mathsf{F}_{(n,k_n)}$. Nous supposons de plus que les ℓ_i sont ordonnés de telle sorte que pour tout $i \in [2, n]$ $\prod_{j=1}^{i-1} d_{(j,1)}\ell_j^{k_j} \geqslant d_{(i,1)}\ell_i^{k_i}$, cette restriction sert juste à simplifier les calculs.

On introduit un objet nécessaire à la construction de compositum.

Définition 7.8. Soient P un polynôme unitaire de degré $\deg(P)$ de racines r_i pour $i \in [1, \deg(P)]$, Q un polynôme unitaire de degré $\deg(Q)$ de racines s_j, tels que P et Q aient des racines distinctes et des degrés $\deg(P), \deg(Q)$ premiers entre eux, alors on définit R le *produit composé* comme étant le polynôme de degré $\deg(P)\deg(Q)$ unitaire et de racines $r_i s_j$ avec $i \in [1, \deg(P)], j \in [1, \deg(Q)]$. On note $R = P \odot Q$.

Nous pouvons alors construire un compositum à l'aide de la proposition suivante :

Proposition 7.9. Soient ℓ_1 un nombre premier, P, Q deux polynômes unitaires irréductibles de degré $d_{(1,1)}\ell_1^{k_1}$ et $\deg(Q)$ premiers entre eux tels que $\mathbb{F}_q[x]/\langle P\rangle \cong \mathsf{F}_{(1,k_1)}$ (le k_1 ième élément de la tour d'extensions ℓ_1-adique vu dans le chapitre 3), $\mathbb{F}_q[y]/\langle Q\rangle$ une extension degré $\deg(Q)$ de $\mathbb{F}_q$. Soit $R = P \odot Q$ le produit composé de P et Q, alors $\mathbb{F}_q[z]/\langle R\rangle$ est un corps fini de taille $q^{d_{(1,1)}\ell_1^{k_1}\deg(Q)}$ et est isomorphe à $\mathbb{F}_q[x, y]/\langle P, Q\rangle$.

Démonstration. Voir [BC87, Theorem 2] □

Nous définissons alors les composita qui nous intéressent dans le cas présent.

Définition 7.10. $\mathbb{K}_1$ est le corps $\mathsf{F}_{(1,k_1)}$. Soit $i \in [1, n-1]$ supposons que $\mathbb{K}_i$ est défini, alors à l'aide de la proposition 7.9 $\mathbb{K}_{i+1}$ est défini comme le compositum de $\mathbb{K}_i$ et $\mathsf{F}_{(i+1,k_{i+1})}$.

Remarque 7.11. Dans la définition 7.10 le cas où $d_{(i,1)} = d_{(j,1)}$ avec $d_{(i,1)} \neq 1$ pour $i \neq j$ empêcherait d'avoir les conditions pour appliquer la proposition 7.9. Cette condition est assez restrictive car comme vu dans le chapitre 3 $d_{(i,1)} | \ell_i - 1$, ainsi il est possible que pour $d_{(i,1)}, d_{(j,1)}$ distincts $\mathrm{pgcd}(d_{(i,1)}, d_{(j,1)}) \neq 1$. Une solution pour contourner ce problème serait alors de construire le compositum à partir d'une extension de $\mathbb{F}_q$ pour laquelle $\mathrm{pgcd}(d_{(i,1)}, d_{(j,1)}) \neq 1$ pour tout (i, j).

Notation 7.12. Nous posons $p_i = \prod_{j=1}^{i} d_{(j,1)}\ell_j^{k_j}$, en particulier p_i est le degré du compositum $\mathbb{K}_i$ comme extension de $\mathbb{F}_q$, par ailleurs $p_0 = 1$.

Le coût de la construction d'un tel compositum n'est pas étudié en détails afin de ne pas surcharger le document car ce coût ne sera pas majeur pour une application dans l'algorithme de Couveignes. Le résultat à utiliser pour évaluer un tel coût est [BFSS06, Theorem 1] avec les coûts de construction de tours d'extension ℓ-adiques vus dans le chapitre 3.

Comme motivé dans la sous sous section précédente 7.3.1 nous calculons les points (ascendants) horizontaux sur les volcans des ℓ_i-isogénies à l'aide des méthodes vues dans la section 5.1.2 afin de les utiliser pour le Théorème des Restes Chinois dans l'algorithme 16. Pour faire cela nous devons exprimer les différents points dans un corps commun : le compositum.

Voyons à quel coût nous pouvons exprimer un élément de $\mathsf{F}_{(i,k_i)}$ dans $\mathbb{K}_n = \otimes_{i=1}^{n}\mathsf{F}_{(i,k_i)}$, pour cela nous avons besoin du résultat suivant issu de [DFDS14, Theorem 1]

Proposition 7.13 (De Feo, Doliskani, Schost)**.** Soient $i \in [2,n]$ P, Q deux polynômes irréductibles unitaires de degrés premiers entre eux $d_{(i,1)}\ell_i^{k_i}$ et p_{i-1} avec $\mathbb{F}_q[x]/\langle P\rangle \cong \mathsf{F}_{(i,k_i)}$ et $\mathbb{F}_q[y]/\langle Q\rangle \cong \mathbb{K}_{i-1}$. Alors le plongement d'un élément de $\mathsf{F}_{(i,k_i)}$ dans $\mathbb{K}_i$ a un coût de $O(d_{(i,1)}\ell_i^{k_i}\mathsf{M}(p_{i-1}) + p_{i-1}\mathsf{M}(d_{(i,1)}\ell_i^{k_i}))$ opérations sur $\mathbb{F}_q$. La descente d'un élément de $\mathbb{K}_i$ vers un élément de $\mathsf{F}_{(i,k_i)}$ a un coût identique. De même le plongement d'un élément de $\mathbb{K}_{i-1}$ dans $\mathbb{K}_i$ ainsi que la descente d'un élément de $\mathbb{K}_i$ dans $\mathbb{K}_{i-1}$ ont le même coût.

Démonstration. Voir [DFDS14]. □

Nous serons amenés à multiplier des polynômes à coefficients dans un compositum, ainsi nous énonçons le résultat suivant.

Proposition 7.14. La multiplication et la division euclidienne de polynômes de degré au plus d à coefficients dans $\mathbb{K}_n \cong \mathbb{F}_q[x]/\langle P\rangle$ avec P un polynôme irréductible de degré p_n est de $O(\mathsf{M}(p_n d))$ opérations sur $\mathbb{F}_q$.

Démonstration. La preuve est la même que celle de la proposition 3.8. □

Maintenant voyons un résultat qui nous permet de changer la représentation d'un élément de $\mathbb{K}_i$ afin de le représenter comme un élément de $\mathbb{K}_{i-1} \otimes \mathsf{F}_{(i,k_i)}$.

Proposition 7.15 (De Feo, Doliskani, Schost)**.** Soient $i \in [1,n]$, $P(x), Q(y)$ deux polynômes irréductibles unitaires de degrés $d_{(i,1)}\ell_i^k, p_{i-1}$ premiers entre eux à coefficients dans $\mathbb{F}_q$ qui définissent $\mathbb{F}_q[x]/\langle P\rangle \cong \mathsf{F}_{(i,k)}$, $\mathbb{F}_q[x]/\langle Q\rangle \cong \mathbb{K}_{i-1}$. Soit $R = P \odot Q$ le produit composé de P et Q alors l'application de l'isomorphisme :

$$\begin{aligned}\varrho : \mathbb{F}_q[x,y]/\langle P,Q\rangle &\to \mathbb{F}_q[z]/\langle R\rangle\\ xy &\mapsto z\end{aligned}$$

a un coût de :

1. $O((d_{(i,1)}\ell_i^k)^2\mathsf{M}(p_{i-1}))$ opérations sur $\mathbb{F}_q$ et l'application de l'inverse de ϱ a un coût de $O(\mathsf{M}(d_{(i,1)}\ell_i^k p_{i-1})p_{i-1}^{1/2} + \mathsf{M}(d_{(i,1)}\ell_i^k)p_{i-1}^{(\omega+1)/2})$ opérations sur $\mathbb{F}_q$ lorsque $d_{(i,1)}\ell_i^k \leqslant p_{i-1}$,
2. $O(p_{i-1}^2\mathsf{M}(d_{(i,1)}\ell_i^k))$ opérations sur $\mathbb{F}_q$ et l'application de l'inverse de ϱ a un coût de $O(\mathsf{M}(p_{i-1}d_{(i,1)}\ell_i^k)(d_{(i,1)}\ell_i^k)^{1/2} + \mathsf{M}(p_{i-1})(d_{(i,1)}\ell_i^k)^{(\omega+1)/2})$ opérations sur $\mathbb{F}_q$ lorsque $d_{(i,1)}\ell_i^k \geqslant p_{i-1}$.

Démonstration. Voir [DFDS14]. □

Ainsi, nous allons pouvoir appliquer ce résultat pour calculer le coût du Frobenius avec une méthode similaire à celle du théorème 3.6. Cela sera abordé dans la prochaine sous-section.

7.3.3 Estimation du coût de l'algorithme de Couveignes ℓ_i-adique avec un nombre composé de Elkies

Nous avons vu dans la sous-section 7.3.1 qu'un point construit à l'aide du Théorème des Restes Chinois appliqué à des points P_i, Q_i (ascendants) horizontaux de directions λ_i, μ_i d'ordre $\ell_i^{k_i}$, avec r, ℓ_i tous premiers entre eux, était mis en correspondance avec un autre point de même direction. Ainsi avec deux bases de points (ascendants) horizontaux $(P_{\lambda_1,\dots,\lambda_n}, Q_{\mu_1,\dots,\mu_n}), (P'_{\lambda_1,\dots,\lambda_n}, Q'_{\mu_1,\dots,\mu_n})$ de $E[\prod_{i=1}^n \ell_i^{k_i}]$ et $E'[\prod_{i=1}^n \ell_i^{k_i}]$ la r-isogénie ϕ peut être représentée de la façon suivante :

$$\phi\begin{pmatrix} P_{\lambda_1,\dots,\lambda_n} \\ Q_{\mu_1,\dots,\mu_n} \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \begin{pmatrix} P'_{\lambda_1,\dots,\lambda_n} \\ Q'_{\mu_1,\dots,\mu_n} \end{pmatrix} \quad \text{avec} \quad a, b \in \left(\mathbb{Z}/\prod_{i=i}^{n} \ell_i^{k_i}\mathbb{Z}\right)^{\times}.$$

Nous avons donc bien une correspondance entre les points définis à l'aide du TRC appliqué à des points (ascendants) horizontaux définis sur deux courbes elliptiques r-isogènes avec r premier avec $\ell_1, \dots, \ell_n$.

Dans le but d'appliquer les même méthodes que celles de la sous-section 6.1.1 nous devons déterminer des représentants d'orbites sous l'action de groupes de Galois sur des éléments de $\mathbb{K}_n = \otimes_{i=1}^n \mathsf{F}_{(i,k_i)}$ défini dans la sous-section 7.3.2.

Proposition 7.16. Soit P un point d'ordre υ_n de $E(\mathbb{K}_n)$ obtenu à l'aide du Théorème des Restes Chinois appliqué aux points P_i de E d'ordre $\ell_i^{k_i}$ tels que l'orbite générée par l'action de $\mathsf{Gal}(\mathsf{F}_{(i,k_i)} : \mathbb{F}_q)$ sur P_i soit de taille maximale : $d_{(i,1)}\ell_i^{k_i}$. Alors l'orbite de P selon l'action de $\mathsf{Gal}(\mathbb{K}_n : \mathbb{F}_q)$ est elle aussi de taille maximale : $p_n = \prod_{i=1}^n d_{(i,1)}\ell_i^{k_i}$.

La preuve n'est pas retranscrite pour ne pas surcharger le document.

Notation 7.17. Soient $\ell_1, \dots \ell_n$ n nombres premiers de Elkies, alors on note ϵ_i le nombre de représentants de points d'ordre $\ell_i^{k_i}$ sous l'action d'un générateur de $\mathsf{Gal}(\mathsf{F}_{(i,k_i)} : \mathbb{F}_q)$.

Ainsi, pour déterminer des représentants des différentes orbites selon l'action de $\mathsf{Gal}(\mathsf{K}_n : \mathbb{F}_q)$ pour des points d'ordre υ_n il suffit, par la proposition 7.16, de calculer à l'aide du TRC tous les points P d'ordre υ_n à partir de tous les choix possibles de représentants $P_i = [\vartheta_i]P$ par rapport à l'action de $\mathsf{Gal}(\mathsf{F}_{(i,k_i)} : \mathbb{F}_q)$. Le nombre de représentants est donc de $\prod_{i=1}^n \epsilon_i$. Ainsi, nous calculons tout d'abord les représentants d'ordre $\ell_i^{k_i}$ dans les tours d'extensions ℓ_i-adiques, puis nous les exprimons dans le compositum et enfin nous appliquons $\prod_{i=1}^n \epsilon_i$ fois le TRC.

Nous pouvons dès à présent modifier l'algorithme 10 pour prendre en entrée deux couples de points d'ordre $\prod_{i=1}^n \ell_i^{k_i}$ de même direction.

Nous présentons donc l'algorithme 13 qui résulte de cette approche ainsi qu'une estimation de son coût.

Algorithme 13 Algorithme de Couveignes avec nombre composé de Elkies.

Entrée : E, E' : deux courbes elliptiques r-isogènes ordinaires situées au niveau $h_i - e_i$ d'un volcan de ℓ_i-isogénies avec cratère cyclique pour i allant de 1 à n.

Sortie : ϕ la r-isogénie qui relie E à E'.

1: Calcul des k_i tels que $\prod_{i=1}^{n} \ell_i^{2k_i-2}(\ell_i+1) > 4r$;
2: **pour** $i = 1$ à n **faire**
3: Calcul de $(P_{\lambda,i}, Q_{\mu,i}), (P'_{\lambda,i}, Q'_{\mu,i})$ bases (ascendantes) horizontales de $E[\ell_i^{k_i}], E'[\ell_i^{k_i}]$ à l'aide de l'algorithme 7 et de l'étape 3 de l'algorithme 10 ;
4: Calcul des représentants des orbites de points d'ordre $\ell_i^{k_i}$ sous l'action de $\mathsf{Gal}(\mathsf{F}_{(i,k_i)} : \mathbb{F}_q)$;
5: **fin pour**
6: Calcul de $(P, Q), (P', Q') \in E^2 \times E'^2$ d'ordres $\mathbb{Z}/\prod_{i=1}^{n} \ell_i^{k_i}\mathbb{Z}$ tels que P et P' sont de direction $(\lambda_1, \ldots, \lambda_n)$ et Q et Q' de direction $(\mu_1, \ldots, \mu_n)$ à l'aide de l'algorithme 16 ;
7: Calcul des listes de représentants L_i, L'_i des orbites de points d'ordre $\prod_{i=1}^{n} \ell_i^{k_i}$ sous l'action de $\mathsf{Gal}(\mathbb{K}_n : \mathbb{F}_q)$;
8: **pour** $M \in \mathsf{diag}(a, b)$ avec $a, b \in \left(\mathbb{Z}/\prod_{i=1}^{n} \ell_i^{k_i}\mathbb{Z}\right)^{\times}$ **faire**
9: Actualisation de la liste L'_i en $L'_{a,b}$ afin de respecter la correspondance induite par le choix de M ;
10: Calcul des des polynômes $A_{a,b}$ et T par des méthodes similaires à celles décrites dans la section 3.4 ;
11: Calcul de la fraction rationnelle $F = A_{a,b} \bmod T$ à l'aide d'une interpolation de Cauchy ;
12: **si** $\mathsf{Test}(F)$ **alors**
13: **retourner** F
14: **fin si**
15: **fin pour**

Avant d'évaluer le coût de l'algorithme 13, qui, comme nous avons vu avec l'algorithme 10, est dominé par le coût de l'interpolation (étape 10) nous énonçons le coût du Frobenius (sans rentrer dans les détails) puis nous estimons le coût du calcul de polynômes d'interpolation.

Proposition 7.18. Soit $i \in [1,n]$, P un polynôme irréductible de degré $d_i\ell_i^m$ avec $m \in [1,k_i]$ tel que $\mathsf{F}_{(i,m)} = \mathbb{F}_q[x]/\langle P\rangle$, Q un polynôme irréductible de degré $p_{i-1} = \prod_{j=1}^{i-1} d_{(j,1)}\ell_j^{k_j}$ tel que $\mathbb{K}_{i-1} = \mathbb{F}_q[y]/\langle Q\rangle$, $R = P \odot Q$ tel que $\mathsf{K} = \mathbb{F}_q[z]/\langle R\rangle$, alors pour un élément a du corps K le coût de calcul de a à une puissance $q^{rp_{i-1}}$ est de $O(\mathsf{M}(d_{(i,1)}\ell_i^m p_{i-1})p_{i-1}^{1/2} + \mathsf{M}(d_{(i,1)}\ell_i^m)p_{i-1}^{(\omega+1)/2})$ opérations dans $\mathbb{F}_q$ avec un pré-calcul qui a un coût booléen de $O(\log(p_i)\log(\ell_i^{k_i} q d_{(i,1)}))$ et de $O(M(d_{(i,1)})d_{(i,1)}\log(q))$ opérations sur $\mathbb{F}_q$.

Nous obtenons un résultat moins bon que celui du théorème 3.6, or en adaptant les mêmes méthodes nous aurions du avoir le coût de cette opération dominé par $O(d_{(i,1)}\ell_i^{k_i})\mathsf{M}(p_{i-1})$. Cependant ici, contrairement au cas du théorème 3.6, nous devons prendre en compte le coût du changement de représentation qui domine la complexité. Ainsi il est crucial pour obtenir des résultats similaire à la section 3.4 d'avoir une construction de compositum permettant un changement de représentation à un coût quasi-linéaire.

Une adaptation des méthodes de calcul de polynôme d'interpolation décrites dans la section 3.4 à ce contexte est faite pour le calcul de polynôme minimal $T = T^{(n)}$(en reprenant une notation similaire) d'éléments de $\mathbb{K}_n \setminus \mathbb{K}_{n-1}$. Ainsi, comme dans la section 3.4, pour le calcul d'un tel polynôme d'interpolation nous devons multiplier des polynômes à coefficients dans $\mathbb{K}_{n-i-1} \otimes \mathsf{F}_{(n-i,k)}$ qui de par leur degré font que le coût d'une telle multiplication n'est que de $\tilde{O}_{p_n,q}(\mathsf{M}(p_n))$. Ce coût de $\tilde{O}_{p_n,q}(\mathsf{M}(p_n))$ en comparant avec les résultats du lemme 3.10 devrait être le coût dominant. Cependant par le coût de l'application du Frobenius aux polynômes $T_k^{(i)}$ de $O(\mathsf{M}(p_n)p_{n-i-1}^{(\omega-1)/2})$, nous majorons le coût total du Frobenius par $O(n\mathsf{M}(p_n)p_{n-1}^{(\omega-1)/2}\max_i(\ell_i(k_i+1)))$.

De la même manière pour le calcul des polynômes d'interpolation A tels $A(v) = w$ avec $v, w \in \mathbb{K}_n \setminus \mathbb{K}_{n-1}$, le coût est encore une fois dominé par l'application du Frobenius et nous majorons le coût d'un tel calcul par

$$O(n\mathsf{M}(p_n \max_i(d_{(i,1)}\ell_i^{k_i}))\max_i(\ell_i(k_i+1))p_{n-1}^{(\omega-1)/2}).$$

Ensuite pour $(v_1,w_1),\ldots,(v_s,w_s)$ des paires d'éléments de $\mathbb{K}_n \setminus \mathbb{K}_{n-1}$, t_j le degré des polynômes minimaux de v_j, nous posons $t = \sum t_j$. Nous cherchons alors à calculer les polynômes

— $T \in \mathbb{F}_q[x]$ de degré t tel que $T(v_j) = 0$ pour tout j, et
— $A \in \mathbb{F}_q[x]$ de degré inférieur à t tel que $A(v_j) = w_j$ pour tout j.

Nous utilisons à nouveau la méthode de la section 3.4, le calcul de T à partir des T_j a un même coût que dans la proposition 3.12 de $O(\mathsf{M}(t)\log(s))$. Cependant comme vu précédemment le coût de calcul des A_j est de

$$O(n\mathsf{M}(t_j \max_i(d_{(i,1)}\ell_i^{k_i}))(p_{n-1})^{(\omega-1)/2}\max_i(\ell_i(k_i+1)))$$

nous majorons donc le coût total par

$$O(n\mathsf{M}(t \max_i(d_{(i,1)}\ell_i^{k_i}))(p_{n-1})^{(\omega-1)/2}\max_i(\ell_i(k_i+1)))$$

par superlinéarité de M.

L'interpolation étant répétée $O(r\prod_{i=1}^{n}\ell_i)$ en moyenne, nous obtenons une estimation de cette version ℓ-adique de l'algorithme de Couveignes

$$O(r(\prod_{i=1}^{n}\ell_i)n\mathsf{M}(r(\prod_{i=1}^{n}\ell_i^2)\max_i(d_{(i,1)}\ell_i^{k_i}))(p_{n-1})^{(\omega-1)/2}\max_i(\ell_i(k_i+1))).$$

Avec $p_n \in O(r(\prod_{i=1}^{n}\ell_i)^{3,5})$ l'estimation est de

$$O(r(\prod_{i=1}^{n}\ell_i)n\mathsf{M}(r(\prod_{i=1}^{n}\ell_i^{3,5})\max_i(d_{(i,1)}\ell_i^{k_i}))(r(\prod_{i=1}^{n}\ell_i^{3,5}))^{(\omega-1)/4}\max_i(\ell_i(k_i+1)))$$

sachant que la borne du calcul des T_i et A_i est large car nous avons majoré $\sum_{i=1}^{n}p_{n-i}^{(\omega-1)/2}$ par $np_{n-1}^{(\omega-1)/2}$ d'où le n en facteur et que de plus nous avons $\max_i(d_{(i,1)}\ell_i^{k_i})p_{n-1} \in \Omega(p_n)$.

Ainsi nous voyons que par l'apport d'opérations de changement de représentations non-linéaires en la taille des composita nous ne pouvons avoir une complexité quadratique en r pour le calcul de l'isogénie montrant ainsi qu'une telle approche en l'état actuel n'est pas intéressante. Cependant cette approche avait l'avantage de proposer une meilleure estimation de r par $\prod_{i=1}^{n}\ell_i^{k_i}$ et donc de réduire les coûts apportés par l'étape d'interpolation dus au choix des nombres premiers de Elkies.

Conclusion

Nous avons donc vu dans ce manuscrit comment généraliser l'algorithme de Couveignes [Cou96] au cas ℓ-adique et s'affranchir de la dépendance polynomiale en la caractéristique. En particulier, nous avons présenté un algorithme qui résout le problème du calcul explicite d'isogénie avec une complexité quasi-quadratique en le degré de l'isogénie, et ce dans des cas particuliers de nombres de Elkies et d'Atkin qui sont fréquents. Nous avons aussi vu au travers de notre étude de nouveaux moyens pour déterminer des directions dans le volcan de ℓ-isogénies à l'aide de l'étude de l'action du Frobenius sur le module de Tate. En particulier pour le cas Atkin on a permis de spécifier, sous certaines conditions, les isogénies descendantes.

Voyons maintenant quelques améliorations possibles (ou à explorer) des résultats présentés dans cette thèse.

L'objectif d'une complexité quadratique pour notre amélioration de l'algorithme de Couveignes dans le cas Atkin avec la même méthode que [Cou96] nécessite de distinguer un sous-groupe cyclique de la ℓ^k-torsion. Ainsi, le couplage qui n'a pas été abordé dans ce document mais seulement mentionné, à travers les travaux de Ionica et Joux [IJ10], serait intéressant à étudier afin de voir aussi si il ne nous apporte pas un critère restrictif, pertinent du point de vue de la complexité, sur les images de points par la r-isogénie, et en particulier sur les points ascendants horizontaux.

Enfin, parmi les pistes proposées mais non satisfaisantes dans le chapitre 7, seule celle présentée dans la section 7.3 utilisant un nombre composé de Elkies pourrait aboutir, en supposant qu'on ait des meilleures représentations de composita permettant des changements de représentation de corps finis en un temps quasi-linéaire.

Nous donnons, pour conclure, quelques perspectives d'application des résultats de cette thèse.

Calcul d'anneau des endomorphismes Les propositions 5.3 et 5.33 nous permettent de savoir exactement à quel niveau se trouve une courbe dans un volcan de ℓ_i-isogénies. Ainsi, en se plaçant dans le même contexte que [Koh96, BS11], où l'on connaît déjà une factorisation de d_π, on peut déterminer la valuation ℓ_i-adique du conducteur de la courbe par rapport à $\mathbb{Z}[\pi]$ et donc on peut calculer l'anneau des endomorphismes de la courbe. Cette approche présente l'avantage par rapport à Kohel [Koh96] et Fouquet et Morain [FM02] d'être plus directe et de ne pas calculer le ℓ-ième polynôme modulaire Φ_ℓ. Par rapport à l'algorithme de Bisson et Sutherland [BS11] on évite de devoir calculer toutes les relations dues aux représentations polycycliques dans le groupe de classe des idéaux. Ainsi notre approche a l'air plus simple, mais il reste toutefois à évaluer

son coût dans un tel contexte. Cela pourrait avoir par exemple une application dans l'algorithme de Bröker [Brö08] utilisé pour calculer un polynôme de Hilbert. En effet dans l'algorithme de Bröker, il est nécessaire de calculer une courbe avec un anneau des endomorphismes spécifique à partir d'une courbe choisie au hasard dont $\mathbb{Z}[\pi]$ est fixé.

Déplacement sur le cratère de volcans de ℓ-isogénies et ses applications aux algorithmes de calcul de polynômes de Hilbert et modulaire Des articles tels que [CM96], [Brö08], [Sut11], [BLS12], utilisent des marches sur le cratère cyclique d'un volcan de ℓ-isogénies avec ℓ petit. Certains algorithmes ([CM96]) se limitent, à juste titre, au cas de volcans réduits à leur cratère, d'autres ne peuvent, et on va donc aborder l'éventuel impact de nos travaux sur ceux-ci. Dans l'algorithme de Sutherland [Sut11] pour le calcul de polynômes de Hilbert on est obligé, de par la taille du ℓ-ième polynôme modulaire, de traiter les cas où le volcan n'est pas réduit à un cratère cyclique. Dés lors il serait pertinent de voir l'apport de notre travail (proposition 5.8) dans ce contexte par rapport à l'algorithme utilisé par Sutherland, similaire aux travaux de [FM02] (voir sous-section 4.1.2) se servant du ℓ-ième polynôme modulaire, ainsi on pourrait rendre cet algorithme non dépendant du (pré)calcul des polynômes modulaires. Dans l'algorithme de Bröker, Lauter et Sutherland [BLS12], pour calculer le ℓ-ième polynôme modulaire les auteurs se placent dans le cas d'un volcan de ℓ_i-isogénies de hauteur 1 de Elkies et régulier. On pourrait à nouveau étudier, dans ce cas très spécifique, l'impact d'une méthode utilisant la proposition 5.8.

Multiplication scalaire et points ascendants horizontaux On a aussi vu dans le chapitre 3, en adaptant les méthodes de [DS15], un moyen de calcul rapide du Frobenius de la courbe. Il serait intéressant de voir si on ne peut pas se servir de cela pour obtenir des résultats intéressants sur la multiplication scalaire avec une approche similaire à [GLV01]. Pour le moment tout ce que l'on est capable de faire c'est, à partir d'une décomposition d'un point R d'ordre ℓ^k en deux points (ascendant) horizontaux P_λ, Q_μ décomposer la multiplication scalaire de $R = [a]P_\lambda + [b]Q_\mu$ par c en le calcul de $[c]R = [c_\lambda]\pi^{\lfloor c/\lambda \rfloor}([a]P) + [c_\mu]\pi^{\lfloor c/\mu \rfloor}([a]Q_\mu)$ avec $c_\lambda = c \bmod \lambda$ et $c_\mu = c \bmod \mu$. L'intérêt d'une telle approche reste à étudier.

Bibliographie

[Atk88] Arthur O. L. Atkin. The number of points on an elliptic curve modulo a prime. *Email on the Number Theory Mailing List*, 1988.

[Atk91] Arthur O. L. Atkin. The number of points on an elliptic curve modulo a prime. Mail to the number theory mailing list available at http ://www.lix.polytechnique.fr/Labo/Francois.Morain/AtkinEmails/19910614.txt, 1991.

[BC87] Joel V. Brawley and Leonard Carlitz. Irreducibles and the composed product for polynomials over a finite field. *Discrete Mathematics*, 65(2) :115–139, 1987.

[BCG+17] Alin Bostan, Frédéric Chyzak, Marc Giusti, Romain Lebreton, Grégoire Lecerf, Bruno Salvy, and Éric Schost. *Algorithmes Efficaces en Calcul Formel*. published by the Authors, January 2017. Cette version est la prépublication de l'ouvrage du même nom à paraître dans la collection https ://hal.archives-ouvertes.fr/AECF/.

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system I : The user language. *Journal of Symbolic Computation*, 24(3) :235–265, 1997.

[BCS97] Wieb Bosma, John J. Cannon, and Allan K. Steel. Lattices of Compatibly Embedded Finite Fields. *Journal of Symbolic Computation*, 24(3/4) :351–369, 1997.

[Bes14] Sébastien Besnier. Courbes elliptiques et isogénies : implantation dans Sage. Master's thesis, Université de Versailles Saint-Quentin en Yvelines, Versailles, 2014.

[BFSS06] Alin Bostan, Philippe Flajolet, Bruno Salvy, and Éric Schost. Fast computation of special resultants. *Journal of Symbolic Computation*, 41(1) :1–29, 2006.

[BK78] Richard P. Brent and Hsiang T. Kung. Fast algorithms for manipulating formal power series. *Journal of the ACM (JACM)*, 25(4) :581–595, 1978.

[BLS12] Reinier Bröker, Kristin Lauter, and Andrew V. Sutherland. Modular polynomials via isogeny volcanoes. *Mathematics of Computation*, 81(278) :1201–1231, 2012.

[BMSS08] Alin Bostan, François Morain, Bruno Salvy, and Éric Schost. Fast algorithms for computing isogenies between elliptic curves. *Mathematics of Computation*, 77(263) :1755–1778, 2008.

[Brö08] Reinier Bröker. A p-adic algorithm to compute the Hilbert class polynomial. *Mathematics of Computation*, 77(264) :2417–2435, 2008.

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

[CCR91] Leonard S. Charlap, Raymond Coley, and David P. Robbins. Enumeration of rational points on elliptic curves over finite fields, 1991.

[CFA+05] Henri Cohen, Gerhard Frey, Roberto Avanzi, Christophe Doche, Tanja Lange, Kim Nguyen, and Frederik Vercauteren, editors. *Handbook of Elliptic and Hyperelliptic Curve Cryptography*. Chapman and Hall/CRC, 2005.

[CGL09] Denis X. Charles, Eyal Z. Goren, and Kristin E. Lauter. Cryptographic Hash Functions from Expander Graphs. *Journal of Cryptology*, 22, 2009.

[CK91] David G. Cantor and Erich Kaltofen. On Fast Multiplication of Polynomials over Arbitrary Algebras. *Acta Informatica*, 28(7) :693–701, 1991.

[CM96] Jean-Marc Couveignes and François Morain. Isogeny cycles and the Schoof-Elkies-Atkin algorithm. In *Research Report LIX/RR/96/03, LIX*, page 96, 1996.

[Coh96] Henri Cohen. A Course in Computational Algebraic Number Theory.(3rd corrected printing), 1996.

[Cou94] Jean-Marc Couveignes. *Quelques calculs en théorie des nombres*. PhD thesis, Université de Bordeaux 1, November 1994.

[Cou96] Jean Marc Couveignes. Computing l-Isogenies Using the p-Torsion. In Henri Cohen, editor, *ANTS*, volume 1122 of *Lecture Notes in Computer Science*, pages 59–65. Springer, 1996.

[Cou00] Jean Marc Couveignes. Isomorphisms between Artin-Schreier towers. *Mathematics of Computation*, 69(232) :1625–1631, 2000.

[Cou06] Jean Marc Couveignes. Hard Homogeneous Spaces. *IACR Cryptology ePrint Archive*, 2006 :291, 2006.

[Cox89] David A. Cox. *Primes of the form $x^2 + ny^2$*. Wiley-Interscience, 1989.

[CW90] Don Coppersmith and Shmuel Winograd. Matrix Multiplication via Arithmetic Progressions. *Journal of Symbolic Computation*, 9(3) :251–280, 1990.

[DF10] Luca De Feo. *Fast Algorithms for Towers of Finite Fields and Isogenies. (Algorithmes Rapides pour les Tours de Corps Finis et les Isogénies)*. PhD thesis, École Polytechnique, Palaiseau, France, 2010.

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

[DFDS13] Luca De Feo, Javad Doliskani, and Éric Schost. Fast Algorithms for l-adic Towers over Finite Fields. In Manuel Kauers, editor, *International Symposium on Symbolic and Algebraic Computation, ISSAC'13, Boston, MA, USA, June 26-29, 2013*, pages 165–172. ACM, 2013.

[DFDS14] Luca De Feo, Javad Doliskani, and Éric Schost. Fast arithmetic for the algebraic closure of finite fields. In *International Symposium on Symbolic and Algebraic Computation, ISSAC'14, Kobe, Japan, July 23-25, 2014*, pages 122–129. ACM, 2014.

[DFHPS16] Luca De Feo, Cyril Hugounenq, Jérôme Plût, and Éric Schost. Explicit isogenies in quadratic time in any characteristic. *LMS Journal of Computation and Mathematics*, 19(A) :267–282, 2016.

[DFJP14] Luca De Feo, David Jao, and Jérôme Plût. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. *Journal of Mathematical Cryptology*, 8(3) :209–247, 2014.

[DFS12] Luca De Feo and Éric Schost. Fast Arithmetics in Artin-Schreier Towers over Finite Fields. *Journal of Symbolic Computation*, 47(7) :771–792, July 2012.

[DS14] Javad Doliskani and Éric Schost. Taking roots over high extensions of finite fields. *Mathematics of Computation*, 83(285), 2014.

[DS15] Javad Doliskani and Éric Schost. Computing in degree 2^k-extensions of finite fields of odd characteristic. *Designs, Codes and Cryptography*, 74(3) :559–569, 2015.

[Elk91] Noam D. Elkies. Explicit isogenies. *preprint*, 1991.

[Elk98] Noam D. Elkies. Elliptic and modular curves over finite fields and related computational issues. *AMS IP STUDIES IN ADVANCED MATHEMATICS*, 7 :21–76, 1998.

[EM03] Andreas Enge and François Morain. Fast Decomposition of Polynomials with Known Galois Group. In Marc P. C. Fossorier, Tom Høholdt, and Alain Poli, editors, *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, 15th International Symposium, AAECC-15, Toulouse, France, May 12-16, 2003, Proceedings*, volume 2643 of *Lecture Notes in Computer Science*, pages 254–264. Springer, 2003.

[Eng09] Andreas Enge. Computing modular polynomials in quasi-linear time. *Mathematics of Computation*, 78(267) :1809–1824, 2009.

[FM02] Mireille Fouquet and François Morain. Isogeny Volcanoes and the SEA Algorithm. In Claus Fieker and David R. Kohel, editors, *ANTS*, volume 2369 of *Lecture Notes in Computer Science*, pages 276–291. Springer, 2002.

[Fou01] Mireille Fouquet. *Anneau d'endomorphismes et cardinalité des courbes elliptiques*. PhD thesis, École Polytechnique, 2001.

[GLV01] Robert Gallant, Robert Lambert, and Scott Vanstone. Faster Point Multiplication on Elliptic Curves with Efficient Endomorphisms. In *Advances in Cryptology—CRYPTO 2001*, pages 190–200. Springer, 2001.

[Gun76] Hiroshi Gunji. The Hasse Invariant and p-division Points of an Elliptic Curve. *Archiv der Mathematik*, 27(1) :148–158, 1976.

[Hug13] Cyril Hugounenq. Amélioration de l'algorithme de Couveignes à l'aide de la structure de 2-Sylow. Master's thesis, Université Joseph Fourrier, Grenoble, 2013.

[IJ10] Sorina Ionica and Antoine Joux. Pairing the Volcano. In Guillaume Hanrot, François Morain, and Emmanuel Thomé, editors, *ANTS*, volume 6197 of *Lecture Notes in Computer Science*, pages 201–218. Springer, 2010.

[Ion10] Sorina Ionica. *Algorithmique des couplages et cryptographie*. PhD thesis, Université de Versailles-St Quentin en Yvelines, 2010.

[Kob87] Neal Koblitz. Elliptic Curve Cryptosystems. *Mathematics of Computation*, 48(177) :203–209, 1987.

[Kob89] Neal Koblitz. Hyperelliptic Cryptosystems. *Journal of Cryptology*, 1(3) :139–150, 1989.

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

[Len96] Hendrick W Lenstra, Jr. Complex Multiplication Structure of Elliptic Curves. *Journal of Number Theory*, 56(2) :227–241, 1996.

[Ler96] Reynald Lercier. Computing Isogenies in $\mathbb{F}_{2^n}$. In Henri Cohen, editor, *Algorithmic Number Theory, Second International Symposium, ANTS-II, Talence, France, May 18-23, 1996, Proceedings*, volume 1122 of *Lecture Notes in Computer Science*, pages 197–212. Springer, 1996.

[Ler97] Reynald Lercier. *Algorithmique des courbes elliptiques dans les corps finis*. PhD thesis, École polytechnique, Palaiseau, June 1997. In french.

[LS08] Reynald Lercier and Thomas Sirvent. On Elkies subgroups of ℓ-torsion points in elliptic curves defined over a finite field. *Journal de Théorie des Nombres de Bordeaux*, 20(3) :783–797, 2008.

[LS14] Patrick Longa and Francesco Sica. Four-Dimensional Gallant–Lambert–Vanstone Scalar Multiplication. *Journal of Cryptology*, 27(2) :248–283, 2014.

[LV16] Pierre Lairez and Tristan Vaccon. On p-Adic Differential Equations with Separation of Variables. In Sergei A. Abramov, Eugene V. Zima, and Xiao-Shan Gao, editors, *Proceedings of the ACM on International Symposium on Symbolic and Algebraic Computation, ISSAC 2016, Waterloo, ON, Canada, July 19-22, 2016*, pages 319–323. ACM, 2016.

[Mes86] Jean-Francois Mestre. La méthode des graphes. Exemples et applications. In *Proceedings of the international conference on class numbers and fundamental units of algebraic number fields (Katata)*, pages 217–242, 1986.

[Mil85] Victor S. Miller. Use of Elliptic Curves in Cryptography. In Hugh C. Williams, editor, *Advances in Cryptology - CRYPTO '85, Santa Barbara, California, USA, August 18-22, 1985, Proceedings*, volume 218 of *Lecture Notes in Computer Science*, pages 417–426. Springer, 1985.

[MMRV05] Josep M. Miret, Ramiro Moreno, Anna Rio, and Magda Valls. Determining the 2-Sylow subgroup of an elliptic curve over a finite field. *Mathematics of computation*, 74(249) :411–427, 2005.

[MMS+06] Josep M. Miret, Ramiro Moreno, Daniel Sadornil, Juan Tena, and Magda Valls. An algorithm to compute volcanoes of 2-isogenies of elliptic curves over finite fields. *Applied Mathematics and Computation*, 176(2) :739–750, 2006.

[MMS+08] Josep M. Miret, Ramiro Moreno, Daniel Sadornil, Juan Tena, and Magda Valls. Computing the height of volcanoes of l-isogenies of elliptic curves over finite fields. *Applied Mathematics and Computation*, 196(1) :67–76, 2008.

[MMT01] Markus Maurer, Alfred Menezes, and Edlyn Teske. Analysis of the GHS Weil descent attack on the ECDLP over characteristic two finite fields of composite degree. *Progress in Cryptology—INDOCRYPT 2001*, pages 195–213, 2001.

[Piz90] Arnold K. Pizer. Ramanujan graphs and Hecke operators. *Bulletin of the American Mathematical Society*, 23(1) :127–137, 1990.

[Piz95] Arnold K. Pizer. Ramanujan graphs. *AMS IP STUDIES IN ADVANCED MATHEMATICS*, 7 :159–178, 1995.

[RS06] Alexander Rostovtsev and Anton Stolbunov. Public-Key Cryptosystem Based on Isogenies. *IACR Cryptology ePrint Archive*, 2006 :145, 2006.

[Rüc87] Hans-Georg Rück. A Note on Elliptic Curves Over Finite Fields. *Mathematics of Computation*, 49(179) :301–304, 1987.

[Sch77] Arnold Schönhage. Schnelle Multiplikation von Polynomen über körpern der Charakteristik 2. *Acta Informatica*, 7(4) :395–398, 1977.

[Sch85] René Schoof. Elliptic curves over finite fields and the computation of square roots mod p. *Mathematics of computation*, 44(170) :483–494, 1985.

[Sch95] René Schoof. Counting points on elliptic curves over finite field. In *Journal de Théorie des Nombres de Bordeaux*, volume 7, pages 219–254, 1995.

[Ser77] Jean Pierre Serre. *Arbres, amalgames, SL2 : cours au Collège de France*. Société Mathématique de France, 1977.

[Sho93] Victor Shoup. Fast Construction of Irreducible Polynomials over Finite Fields. In Vijaya Ramachandran, editor, *Proceedings of the Fourth Annual ACM/SIGACT-SIAM Symposium on Discrete Algorithms, 25-27 January 1993, Austin, Texas.*, pages 484–492. ACM/SIAM, 1993.

[Sil86] Joseph H. Silverman. *The arithmetic of elliptic curves*. Springer-Verlag, 1986.

[SS71] Arnold Schönhage and Volker Strassen. Schnelle Multiplikation grosser Zahlen. *Computing*, 7(3-4) :281–292, 1971.

[SS14] Igor E. Shparlinski and Andrew V. Sutherland. On the Distribution of Atkin and Elkies Primes. *Foundations of Computational Mathematics*, 14(2) :285–297, 2014.

[Sut11] Andrew V. Sutherland. Computing Hilbert class polynomials with the Chinese remainder theorem. *Mathematics of Computation*, 80(273) :501–538, 2011.

[Tes06] Edlyn Teske. An Elliptic Curve Trapdoor System. *Journal of Cryptology*, 19(1) :115–133, 2006.

[The16] The Sage Developers. *Sage Mathematics Software (Version 7.1)*, 2016.

[Vél71] Jacques Vélu. Isogénies entre courbes elliptiques. *Comptes Rendus hebdomadaires de l'Académie des Sciences de Paris Série AB*, 273 :A238–A241, july 1971.

[Vol90] José F. Voloch. Explicit p-descent for elliptic curves in characteristic p. *Compositio Mathematica*, 74(3) :247–258, 1990.

[vzGG03] Joachim von zur Gathen and Jürgen Gerhard. *Modern computer algebra (2. ed.)*. Cambridge University Press, 2003.

[vzGS92] Joachim von zur Gathen and Victor Shoup. Computing frobenius maps and factoring polynomials. *Computational complexity*, 2(3) :187–224, 1992.

[Was08] Lawrence C. Washington. *Elliptic curves : number theory and cryptography*. CRC press, 2008.

[Wil12] Virginia Vassilevska Williams. Multiplying matrices faster than Coppersmith-Winograd. In *Proceedings of the forty-fourth annual ACM symposium on Theory of computing*, pages 887–898. ACM, 2012.

Annexe A

Algorithmes

Dans ce chapitre sont présentés des algorithmes qui n'ont pas été laissé dans le manuscrit pour ne pas surcharger celui-ci.

Algorithme 14 Couveignes ℓ-adique dans le cas Elkies avec un seul sous-groupe cyclique.

Entrée : E, E' : deux courbes elliptiques r-isogènes ordinaires situées au niveau $h - e$ d'un volcan de ℓ-isogénies avec cratère cyclique.
Sortie : ϕ la r-isogénie qui relie E à E'.

1: Calcul du plus petit k tel que $\ell^{k-1} > 4r$;
2: Calcul de $(P, Q), (P', Q')$ bases diagonales de $E_s[\ell^{h+1}], E'_s[\ell^{h+1}]$ à l'aide de l'algorithme 7 ;
3: Calcul de $P_\lambda \in E_s[\ell^k]$, $P'_\lambda \in E'_s[\ell^k]$ points horizontaux à l'aide de l'algorithme 8 ;
4: **si** $(E_s, E'_s) \neq (E, E')$ **alors**
5: Calcul de P_λ, P'_λ points ascendants horizontaux de $E_s[\ell^k], E'_s[\ell^k]$ avec les ℓ^e-isogénies descendantes $\varphi : E_s \to E$, $\varphi' : E_s \to E'$;
6: **fin si**
7: Calcul des liste de représentants L, L' des orbites de points d'ordre ℓ^k sous l'action de π ;
8: **pour** $a \in \left(\mathbb{Z}/\ell^k\mathbb{Z}\right)^*$ **faire**
9: Actualisation de la liste des représentants L' en L'_a afin de respecter la correspondance induite par le choix de a ;
10: Calcul des des polynômes A_a et T par les méthodes décrites dans la section 3.4 ;
11: Calcul de la fraction rationnelle $F = A_a \bmod T$ à l'aide d'une interpolation de Cauchy ;
12: **si** $\mathsf{Test}(F)$ **alors**
13: **retourner** F
14: **fin si**
15: **fin pour**

Algorithme 15 Calcul de $P \in E[\upsilon_n]$ tel que $[\upsilon_{i_0}]P = P_{i_0}$ et $[\ell_{i_0}^{k_{i_0}}]P = 0_E$

Entrée : E : une courbe elliptique, $\ell_1, \ldots, \ell_n$ n nombres premiers distincts, un point P_{i_0} d'ordre $\ell_i^{k_{i_0}}$ pour $i_0 \in [1, n]$.

Sortie : P un point de E d'ordre $\prod_{i=1}^{n} \ell_i^{k_i}$ tel que $[\prod_{\substack{i=0 \\ i \neq i_0}}^{n} \ell_i^{k_i}]P = P_{i_0}$ et $[\ell_{i_0}^{k_{i_0}}]P = 0_E$.

1: $P \leftarrow P_{i_0}$;
2: Calcul de $P' = \mathsf{divise}(P_{i_0}, \prod_{\substack{j=0 \\ j \neq i_0}}^{n} \ell_j^{k_j})$;
3: Calcul de $Q = [\ell_{i_0}^{k_{i_0}}]P'$ un point d'ordre $\prod_{\substack{j=0 \\ j \neq i_0}}^{n} \ell_j^{k_j}$;
4: Calcul de R la pré-image de Q d'ordre $\prod_{\substack{j=0 \\ j \neq i_0}}^{n} \ell_j^{k_j}$ par $[\ell_{i_0}^{k_{i_0}}]$;
5: $P \leftarrow P' - R$
6: **retourner** P

Algorithme 16 Théorème des restes chinois sur une courbe elliptique

Entrée : E : une courbe elliptique, $\ell_1, \ell_2, \ldots \ell_n$ n nombres premiers distincts, des points P_i d'ordre $\ell_i^{k_i}$ pour $i \in [1, n]$.

Sortie : P un point de E d'ordre υ_n tel que $[\vartheta_{i_0}]P = P_{i_0}$ pour $i_0 \in [1, n]$.

1: $P \leftarrow 0_E$;
2: **pour** $i = 1$ à n **faire**
3: Q sortie de l'algorithme 15 tel que $\ell_i^{k_i} Q = 0$ et $[\vartheta_i]Q = P_i$;
4: $P \leftarrow P + Q$;
5: **fin pour**
6: **retourner** P ;

université PARIS-SACLAY

ÉCOLE DOCTORALE
Sciences et technologies de l'information et de la communication (STIC)

Titre : Volcans et calcul d'isogénies

Mots clés : cryptographie , courbes elliptiques, isogénies, calcul formel

Résumé : Le problème du calcul d'isogénies est apparu dans l'algorithme SEA de comptage de points de courbes elliptiques définies sur des corps finis. L'apparition de nouvelles applications du calcul d'isogénies (cryptosystème à trappe, fonction de hachage, accélération de la multiplication scalaire, cryptosystème post quantique) ont motivé par ailleurs la recherche d'algorithmes plus rapides en dehors du contexte SEA. L'algorithme de Couveignes (1996), malgré ses améliorations par De Feo (2011), présente la meilleure complexité en le degré de l'isogénie mais ne peut s'appliquer dans le cas de grande caractéristique.

L'objectif de cette thèse est donc de présenter une modification de l'algorithme de Couveignes utilisable en toute caractéristique avec une complexité en le degré de l'isogénie similaire à celui de Couveignes.

L'amélioration de l'algorithme de Couveignes se fait en suivant deux axes : la construction de tours d'extensions de corps finis de degré ℓ efficaces pour rendre les opérations plus rapides, à l'image des travaux de De Feo (2011), De Feo Doliskani Schost (2013), Doliskani Schost (2015), et la détermination d'ensembles de points d'ordre ℓ^k stables sous l'évaluation d'isogénies.

L'apport majeur de cette thèse est fait sur le second axe pour lequel nous étudions les graphes d'isogénies. Nous utilisons pour notre travail les résultats précédents de Kohel (1996), Fouquet et Morain (2001), Miret *et al.* (2005,2006,2008), Ionica et Joux (2001). Nous présentons donc dans cette thèse, à l'aide d'une étude de l'action du Frobenius sur les points d'ordre ℓ^k, un nouveau moyen de déterminer les directions dans le graphe (volcan) d'isogénies.

Title : Volcanoes and isogeny computation

Keywords : cryptography , ellitpic curves, isogeny, symbolic computation

Abstract : The isogeny computation problem appeared in the SEA algorithm to count the number of points on an elliptic curve defined over a finite field. Algorithms using ideas of Elkies (1998) solved this problem with satisfying results in this context. The appearance of new applications of the isogeny computation problem (trapdoor cryptosystem, hash function, scalar multiplication acceleration, post quantic cryptosystem) motivated the search for a faster algorithm outside the SEA context. Couveignes's algorithm (1996) offers the best complexity in the degree of the isogeny but, despite improvements by DeFeo (2011), it proves itself unpractical with great characteristic.

The aim of this work is to present a modified version of Couveignes's algorithm (1996) that maintains the same complexity in the degree of the isogeny but is practical in any characteristic.

Two approaches contribute to the improvement of Couveignes's algorithm (1996) : firstly, the construction of towers of degree ℓ extensions of finite field which are efficient for faster arithmetic operations, as used in the work of De Feo (2011),De Feo Doliskani Schost (2013), Doliskani Schost (2015), and secondly, the specification of sets of points of order ℓ^k that are stable under the application of isogenies.

The main contribution of this document is done following the second approach. Our work uses the graph of isogenies . We based our work on the previous results of David Kohel (1996), Fouquet and Morain (2001), Miret *& al.* (2005,2006,2008), Ionica and Joux (2001). We therefore present in this document, through the study of the action of the Frobenius endomorphism on points of order ℓ^k, a new way to specify directions in the isogeny graph (volcano).

Université Paris-Saclay
Espace Technologique / Immeuble Discovery
Route de l'Orme aux Merisiers RD 128 / 91190 Saint-Aubin, France