Quelques aspects de l'arithmétique des courbes hyperelliptiques de genre 2

Oumar Diao

N° d'ordre : 4187 ANNÉE 2010

THÈSE / UNIVERSITÉ DE RENNES 1
sous le sceau de l'Université Européenne de Bretagne

pour le grade de

DOCTEUR DE L'UNIVERSITÉ DE RENNES 1

Mention : Mathématiques et Applications

Ecole doctorale MATISSE

présentée par

Oumar DIAO

préparée à l'unité de recherche 6625 CNRS - IRMAR
Instutit de Recherche de Mathématiques de Rennes
U.F.R. de Mathématiques

Quelques aspects de l'arithmétique des courbes hyperelliptiques de genre 2

Thèse soutenue à Rennes
le 23 juillet 2010

devant le jury composé de :

Maurice MIGNOTTE
Professeur, Université de Strasbourg / président

Jean-Marc COUVEIGNES
Professeur, Université de Toulouse II, Le Mirail (France) / rapporteur

Reynald LERCIER
Chercheur, Université de Rennes 1 (France) / examinateur

Djiby SOW
Enseignant Chercheur, Université C.A.D. de Dakar (Sénégal) / examinateur

David LUBICZ
Chercheur, Université de Rennes 1 (France) / directeur de thèse

Mamadou SANGHARÉ
Professeur, Université C.A.D. de Dakar (Sénégal) / co-directeur de thèse

Remerciements

Je rend grâce à DIEU, LE TOUT PUISSANT.

Si je devais écrire les noms de toutes les personnes qui me sont chères, alors cela prendrait plusieurs pages (plus d'une trentaine) et peu de gens le liront intégralement. C'est une tâche difficile que je ne peux me dérober et veuillez m'excuser si vous ne trouvez pas votre nom dans ces quelques lignes qui suivront.

Je tiens à exprimer toute ma reconnaissance aux Professeurs David LUBICZ et Mamadou SANGHARÉ qui ont accepté, avec beaucoup de disponibilité, d'écoute et de conseil de co-diriger mes premiers pas dans le monde de la recherche.

Je suis profondemment touché de l'honneur que me fait le Professeur Maurice MIGNOTTE de présider le jury de ma thèse. Et je suis très touché de l'honneur que me font les Professeurs Jean-Marc COUVEIGNES et Guillaume HANROT en acceptant de juger ce travail et d'en être les rapporteurs. Veuillez accepter, Messieurs les professeurs, l'expression de ma profonde gratitude.

Je souhaite remercier chaleureusement Reynald LERCIER et Djiby SOW pour avoir accepté d'examiner ma dissertation doctorale et de faire partie de mon jury de thèse. Soyez assurés, Messieurs, de toute mon estime et de mon profond respect.

Je ne sais pas comment exprimer ma reconnaissance à tous les enseignants qui m'ont formé tout au long de mon parcours. Je pense particulièrement à Boubacar SECK du lycée Ngalandou DIOUF de Dakar, mon professeur de maths de terminale et au Professeur Mamadou SANGHARÉ de l'université de Dakar.

L'aboutissement d'une thèse n'aurait pu se faire sans un cadre de travail matériel et intellectuel favorable. C'est pourquoi, je tiens à remercier la Professeure Marie-Françoise ROY de m'avoir accueilli à l'Institut des Mathématiques Appliquées de Rennes. De même, j'associe ce remerciement à tout le personnel administratif de l'IRMAR, de l'école doctorale MATISSE et de l'université de Rennes 1 pour leur écoute, leur compétence, leur gentillesse et leur disponibilité.

La réalisation d'une thèse fut aussi l'occasion d'une aventure humaine merveilleuse au cours de la quelle j'ai croisé la route de nombreuses personnes. Je reconnais que chacune a apporté une contribution positive à ma vie personnelle et professionnelle. Un grand merci au Professeur Hervé pour son séminaire de psychologie, à Otto, à Demdah, à Moussa, aux deux Richard, à Mathieu, à Gabriel et à Christophe pour le partage d'un thé au 643.

Je remercie aussi tous les chercheurs du séminaire de cryptographie, tout le personnel du département de maths-info de la faculté des sciences et techniques de l'université de Dakar, tout le personnel et élèves des collèges Paul Féval, Montbarrot et Malifeu et à toutes les personnes que je n'ai pas citées et qui se reconnaîtront dans ces quelques lignes.

Je ne saurai terminer sans remercier mes amis, mes camarades des associations et surtout à toute ma famille pour leur irremplaçable et inconditionnel aide et soutien sans faille. Il m'est impossible d'exprimer toute ma reconnaissance et mon respect pour leurs

sacrifices. Et surtout les sacrifices de ma mère Gaye, Mère que Dieu te paie !

Merci à Mame Dialla Touré de supporter mes humeurs et de partager quotidiennement mes joies et peines.

Dédicace à ma fille, Kadiatou.

Table des matières

Remerciements **i**

Introduction **1**
Fondement de la cryptographie moderne 1
Discret Logarithm Problem (DLP) 1
Protocoles basés sur les couplages. 2
Arithmétiques hyperelliptiques 3
Organisaition du manuscrit 4
Notations 4

I Rappel sur l'arithmétique des courbes hyperelliptiques **7**

1 Généralités sur les courbes hyperelliptiques **9**
1.1 Courbes hyperelliptiques 9
1.2 Classification des courbes hyperelliptiques 10
1.2.1 Sur un corps fini 10
1.2.2 Sur un corps algébriquement clos 11
1.3 Corps de fonction d'une courbe hyperelliptique 11
1.4 Diviseurs d'une courbe 12

2 Jacobienne d'une courbe hyperelliptique **15**
2.1 Généralités 15
2.2 Points de torsion 16
2.3 Polynôme caractéristique du Frobenius 17
2.4 Courbes « pairing-friendly » 19

3 Arithmétique sur la jacobienne d'une courbe hyperelliptique **21**
3.1 Arithmétique sur une courbe elliptique 21
3.2 Addition et réduction de Cantor 22
3.2.1 Addition de Cantor 23
3.2.2 Réduction de Cantor 24
3.3 Formules explicites en genre 2 24
3.4 Quelques remarques pour finir 27

II Implémentation efficace des couplages en genre 2 **29**

4 Généralités sur les couplages **31**
4.1 Définition des couplages de Weil et de Tate 31

4.2 L'algorithme de Miller . . . 32
4.2.1 Fonction de Miller . . . 32
4.2.2 Fonction de Weil . . . 32
4.2.3 Evaluation d'une fonction en un diviseur . . . 35
4.2.4 Evaluation explicite de la fonction de Weil-Miller . . . 36
4.3 Application au calcul de couplages . . . 37

5 Quelques améliorations algorithmiques 39
5.1 Couplages de Tate et Eta . . . 40
5.2 Couplages Ate I et II . . . 40
5.2.1 Couplage Ate I . . . 41
5.2.2 Couplage Ate II . . . 42
5.3 Comparaison des différents couplages . . . 44
5.4 Elliptique vs hyperelliptique . . . 45
5.5 Implémentation cryptographique . . . 46
5.5.1 Construction de diviseurs . . . 46
5.5.2 Exponentiation finale . . . 46
5.5.3 Etude de cas . . . 47

III Modèles efficaces à base de fonctions thêta 49

6 Quelques rappels 51
6.1 Fonctions thêta de Riemann . . . 51
6.2 Quelques relations avec les fonctions thêta . . . 53
6.3 Nombres p-adiques . . . 54
6.3.1 Définitions et propriétés . . . 55
6.3.2 Extensions finies de $\mathbb{Q}_p$ . . . 56
6.3.3 Réduction et relèvement . . . 57

7 Calcul efficace sur les courbes elliptiques 59
7.1 Modèle d'Edwards en caractéristique impaire . . . 59
7.1.1 Modèle sur $\mathbb{C}$ . . . 60
7.1.2 Formules d'addition sur $\mathbb{C}$ . . . 61
7.1.3 En caractéristique impaire . . . 62
7.2 Courbe d'Edwards en caractéristique 2 . . . 63
7.2.1 Modèle de la courbe . . . 63
7.2.2 Formules d'addition . . . 65

8 Calcul efficace en genre 2 71
8.1 Variétés de Kummer . . . 71
8.2 Surfaces de Kummer en caractéristique impaire . . . 72
8.3 Surface de Kummer en caractéristique deux . . . 72
8.3.1 Cas des surfaces ordinaires . . . 73
8.3.2 Cas des surfaces non-ordinaires . . . 74
8.3.3 Surface de Kummer supersingulière . . . 75
8.3.4 Surface de Kummer de $p-$rang 1 . . . 79
8.3.5 Comparaison avec des études précédentes . . . 81
Conclusion . . . 81

Conclusion générale **82**

Index **83**

Bibliographie **85**

Introduction

Fondements de la cryptographie moderne. La cryptographie moderne se partage entre d'une part la cryptographie symétrique et d'autre part la cryptographie asymétrique. Dans le cas de la cryptographie symétrique les secrets qui permettent de chiffrer est de déchiffrer sont les mêmes. En cryptographie asymétrique ou à clef publique au contraire, la clef se compose d'une partie publique qui permet par exemple de chiffrer ou de vérifier une signature et d'une partie privée qui doit rester secrète. De fait, la cryptographie asymétrique bien que lente est bien adaptée à un usage sur un réseau comportant un grand nombre d'acteurs car elle permet entre autre un déploiement et une gestion simplifiée des secrets. Un exemple d'algorithme à clé secrète bien connu est l'**AES** (Advanced Encryption Standard) de Rijmen et Daemen [RD02] et l'algorithme à clé publique le plus utilisé actuellement est le **RSA** (Rivest Shamir Adleman) [RSA78] du nom de ses auteurs. L'objet principal de ce mémoire est l'étude de briques algorithmiques utiles à la cryptographie asymétrique. La sécurité des algorithmes asymétriques repose sur la notion de **fonctions à sens unique**, i.e. des fonctions "injectives" qui sont faciles à calculer, mais difficiles à inverser pour beaucoup de valeurs de l'ensemble d'arrivée. La sécurité des algorithmes à clés publiques est donc liée à la difficulté calculatoire de certains problèmes mathématiques. Ainsi le RSA repose sur la difficulté à factoriser un entier N formé du produit de deux grands nombres premiers p, q, et la fonction à sens unique utilisée est une fonction puissance dans le groupe multiplicatif de $\mathbb{Z}/N\mathbb{Z}$. De manière plus précise, on peut voir que si on sait factoriser rapidement, alors il est facile d'inverser toute fonction puissance dans $\mathbb{Z}/N\mathbb{Z}$ et on espère que réciproquement, si l'on sait inverser une fonction puissance alors on peut retrouver facilement la factorisation de l'entier N.

Une fois l'hypothèse calculatoire posée, la sécurité de RSA est fonction de la taille des clés utilisées. Cette taille doit être régulièrement revue à la hausse pour pouvoir suivre l'accroissement de la puissance des ordinateurs, et actuellement elle est usuellement de 2048 et voir même 4096 bits. Ces tailles de clés ne sont pas négligeables pour les équipements disposant de peu de ressource comme des cartes à puces ou des téléphones portables. Dès lors, il s'avère nécessaire de trouver d'autres algorithmes de clés publiques qui permettent pour un même niveau de sécurité de manipuler des objets plus compacts.

Discrete Logarithm Problem (DLP). En 1976, Diffie et Hellman [DH76] proposent une infrastructure générale permettant de construire des candidats de fonctions à sens unique à partir du **problème du logarithme discret** (DLP). Etant donné un groupe $(G, .)$ et deux éléments $g, h \in G$ tels que $h = g^k$ avec $k \in \mathbb{Z}$, le problème du logarithme discret sur G, consiste à trouver l'entier k connaissant g et h. Notons que le DLP est facile dans les $\mathbb{Z}$-modules additifs du fait de l'algorithme d'Euclide étendu. Afin d'utiliser le DLP, il est nécessaire de pouvoir fabriquer des familles de groupes de taille arbitrairement grande dans laquelle le problème DLP est réputé difficilé. En 1987 et 1989, Koblitz [Kob87, Kob89] proposa l'utilisation des groupes de points rationnels de courbes elliptiques et des jacobiennes

de courbes hyperelliptiques définies sur un corps fini. En fait, les meilleurs algorithmes connus à ce jour capables de calculer en général le DLP sur une courbe elliptique sont le "pas de géant-pas de bébé" [Sha71], le Pollard ρ [Pol78] et le Pohlig-Hellman [PH78] et ces algorithmes sont tous de complexité exponentielle en la taille du groupe. Ces algorithmes sont appelés algorithmes génériques car ils n'utilisent aucune autre information que celle donnée par la loi de groupe pour opérer.

Afin d'étudier le problème du logarithme discret sur les jacobiennes de courbes, il est important de concevoir des modèles de courbes avec une arithmétique particulièrement efficace ou ayant des propriétés de sécurité prouvées pour les applications cryptographiques. Il est aussi nécessaire d'étudier les structures supplémentaires sur les jacobiennes (dans un sens calculatoire) que l'on ne retrouve pas dans les groupes génériques. Un exemple partculièrement important de structure supplémentaire est le couplage qui donne lieu à des applications « constructives » et « destructives » en cryptographie.

Protocoles basés sur le couplage. Pour des courbes particulières, il existe des algorithmes plus rapides que les algorithmes génériques pour résoudre le DLP. Ces algorithmes utilisent donc des structures spécifiques (i.e. des structures qui n'existent pas dans un groupe générique) aux groupes des points rationnels d'une courbe elliptique. Par exemple, l'existence de couplages (formes bilinéaires non dégénérées) sur les courbes elliptiques calculables en temps polynomial a été mis à profit pour construire des attaques par transfert du problème de logarithme discret : l'idée est de se servir des couplages pour transporter le DLP depuis une courbe elliptique sur le groupe multiplicatif d'un corps fini pour lequel il existe des algorithmes de complexité sous-exponentielle pour résoudre le DLP. C'est le principe des attaques présentées d'une part par Menezes, Okamoto et Vanstone et d'autre part par Frey et Rûck (MOV [MOV93] en 1993 et FR [FR94] en 1994).

Il existe aussi des applications « constructives » des couplages sur les courbes elliptiques. La structure supplémentaire présente sur le groupe des points rationnels d'une courbe elliptique est utilisée pour construire des protocoles ayant des propriétés particulièrement intéressantes. On peut citer par exemple :

- le protocole Diffie-Hellman tripartite de Joux [Jou04] en 2000 et 2004,
- le schéma de signature de Sakai, Ohgishi et Kasahara [SOK00] en 2000,
- le système El-Gamal de Verheul [Ver01] en 2001,
- le schéma de signature de Boneh, Lynn et Shacham [BLS01] en 2001,
- le schéma d'échange de clé de Smart [Sma01b] en 2001,
- le schéma de signature de Paterson [Pat02] en 2002,
- le schéma de chiffrement de Boneh et Franklin [BF03] en 2003,

Cette liste n'est pas exhaustive. Nous voyons donc que le champ d'application de l'étude de couplages sur les courbes elliptiques et hyperelliptiques pour la cryptographie est très grand. Elle permet de concevoir des attaques nouvelles, mais aussi de construire des protocoles très rapides dont la sécurité repose sur un problème réputé difficile avec des tailles de clés de 4 à 20 fois plus petites que celles du RSA (voir [GPS06a, CBLM09] pour plus de détails sur la comparaison entre RSA et les courbes elliptiques). De nos jours, les cryptosystèmes basés sur des courbes elliptiques sont standardisés par beaucoup d'organismes comme l'IEEE [IEE00], le NIST [NIS02], le SEC, l'ANSI, etc.

Notons que la construction de protocoles avec des couplages dépend fortement du choix de la courbe. En effet, les attaques MOV et FR sont possibles sur des courbes elliptiques particulières : celles dont le cardinal des points rationnels est décomposable en de petits nombres premiers ou bien certaines courbes supersingulières de petit cardinal. Ce qui suggère l'existence de courbes idéales pour le couplage, ces courbes sont appelées « **courbes**

pairing-friendly ».

Arithmétique hyperelliptique. La construction de protocoles basés sur les courbes dépend fortement de l'arithmétique efficace sur les jacobiennes des courbes. Pour cela, il faut non seulement accélérer l'arithmétique sur les jacobiennes mais aussi faire un choix adéquat des corps finis. Pour les corps finis utilisés, selon le niveau de sécurité, on prend soit des grandes extensions de corps finis de caractéristique 2, soit de grands corps premiers. Par exemple, pour un niveau de sécurité égal à 80 bits, on utilise soit le corps fini $\mathbb{F}_{2^m}$ avec $m \approx 160$, soit le corps premier $\mathbb{F}_p$ avec p premier et $p \approx 2^{160}$. Pour améliorer les implémentations sur les corps finis, le polynôme de définition de $\mathbb{F}_{2^m}$ et le nombre premier p doivent être de poids de Hamming minimal.

Par ailleurs, l'efficacité de l'arithmétique dépend du cardinal de la Jacobienne de la courbe. Le théorème de Hasse sur les courbes elliptiques, généralisé par Weil sur les variétés abéliennes, donne une borne du cardinal de la jacobienne d'une courbe hyperelliptique entre $(\sqrt{q}-1)^{2g}$ et $(\sqrt{q}+1)^{2g}$. Le cardinal de la jacobienne est alors de l'ordre de q^g et la sécurité sur les courbes hyperelliptiques est de l'ordre de $q^{g/2}$. Cette remarque a une conséquence sur l'étude des courbes hyperelliptiques de genre supérieur. En effet, pour le genre 2 on peut choisir des courbes hyperelliptiques sur des corps plus petits que ceux nécessaires pour les courbes elliptiques. Par exemple, à un même niveau de sécurité, une courbe elliptique de taille $\approx 2^{360}$ correspond à une courbe hyperelliptique de genre 2 dont la taille de la jacobienne $\approx 2^{180}$. Cependant, les courbes hyperelliptiques de genre $g \geq 4$ sont moins sûres que les courbes de genre ≤ 3. En effet, Adleman, DeMarais et Huang d'une part [ADH94] et Gaudry [Gau00] d'autre part ont exhibé une attaque sous-exponentielle lorsque le genre de la courbe est grand.

Les considérations précédentes ont motivé d'importants travaux de recherche destinés à rendre plus efficace l'arithmétique des courbes elliptiques et des jacobiennes de courbes hyperelliptiques. L'algorithme de Cantor [Can87] permet de calculer la loi de groupe sur les jacobiennes des courbes hyperelliptiques. Lange [Lan01, Lan02a] donne une version efficace de l'algorithme de Cantor en genres 2 et 3. Pour améliorer l'arithmétique sur les courbes, on peut changer le système de représentations des diviseurs, ou bien changer le modèle de la courbe. Ceci suggère d'une part l'utilisation des coordonnées projectives ou des coordonnées jacobiennes pour la représentation des diviseurs des courbes et d'autre part l'utilisation des modèles d'Edwards [Edw07], de Jacobi ou de Hessian en genre 1 ou du modèle des surfaces de Kummer ou à base de fonctions thêta en genre 2.

Récemment sont apparues des attaques dites à canaux auxiliaires [ACD+06, chap. 29] qui exploitent le fait que les coûts de l'addition et de la duplication sont différents pour retrouver des informations sur la clé privée. Pour implémenter ces attaques, on mesure le temps d'exécution ou le rayonnement électromagnétique produit par le matériel lors de son utilisation pour calculer l'exponentation. Si on peut distinguer la complexité de l'addition et de la duplication, alors il est facile de retrouver la clé secrète utilisée lors de l'exponentation. Pour contrecarer ces attaques, il peut être intéressant de considérer des lois de groupes dites uniformes ce qui signifie que les formules d'addition et de duplication [BDJ04, BJ02] sont identiques. En genre 2, Lange et Mishra [LM05] proposent des formules pour uniformiser la loi de groupe. Une autre méthode pour parer aux attaques à canaux auxiliaires est l'utilisation d'algorithmes de type Montgomery [Duq04] qui calculent une exponentation en faisant à chaque étape une addition et une duplication quelle que soit la valeur du bit d'exposant. En 2007, Gaudry [Gau07] décrit une arithmétique efficace sur les surfaces de Kummer qui utilise la théorie des fonctions thêta et repose sur un algorithme de type Montgomery. En 2008, Gaudry et Lubicz [GL08] résolvent le cas des

courbes hyperelliptiques ordinaires définies sur un corps de caractéristique 2. Mais leurs formules ne sont pas valables pour des courbes non-ordinaires définies sur un corps fini de caractéristique 2. Dans ce mémoire, nous étudierons ces courbes non-ordinaires définies sur des corps de caractéristique 2.

Organisaition du manuscrit. Ce manuscrit est divisé en 3 parties et 9 chapitres (3 chapitres par partie) :

I. Rappel sur l'arithmétique des courbes hyperelliptiques.

II. Implémentation efficace des couplages en genre 2.

III. Modèle efficace à base de fonctions de thêta.

La première partie est consacrée aux rappels sur la théorie générale des courbes hyperelliptiques. Elle permet de comprendre la suite du présent manuscrit et ne comporte aucune démonstration. Dans le premier chapitre, nous rappelons les généralités sur les courbes hyperelliptiques. Dans le deuxième chapitre nous nous intéresserons aux jacobiennes et dans le troisième chapitre à leur arithmétique.

Les deux dernières parties constituent la partie centrale du présent manuscrit. La deuxième partie est entièrement consacrée à la théorie des couplages en petit genre tandis que la troisième est consacrée à l'arithmétique efficace en genres 1 et 2. Dans la deuxième partie, nous commencerons par rappeler l'algorithme de Miller qui manipule des fonctions dites de Miller. Le travail effectué dans cette partie est avant tout expérimental. Nous avons implémenté en Magma deux généralisations des couplages, d'une part le couplage optimal de [Ver08] pour le cas elliptique et d'autre part le couplage hyperelliptique de [GHV07]. Nous donnons une condition nécessaire et suffisante pour que le couplage de Ate soit plus rapide que celui de Tate. Nous avons implémenté tous les algorithmes et nous faisons une comparaison des performances pour un niveau de sécurité donné entre les genres 1 et 2.

La troisième partie de ce manuscrit constitue la partie la plus originale de ce mémoire. En effet, dans cette partie nous utilisons la théorie générale des fonctions thêta pour obtenir des modèles efficaces pour des jacobiennes de dimension 1 et 2. En genre 1, nous réinterpretons le modèle d'Edwards sur un corps de caractéristique impaire. Grâce au modèle d'Edwards en caractéristique impaire, nous allons déduire le modèle d'Edwards binaire. Ce lien justifie le modèle d'Edwards binaire et cela est crucial d'autant plus que nous montrons que notre modèle est une sous-famille du modèle d'Edwards binaire de [BLF08].

Nous rappelons d'abord la théorie générale des fonctions thêta. Puis nous donnons des formules efficaces obtenues pour l'arithmétique d'une courbe d'Edwards en caractéristique 2. De même, nous utilisons les fonctions thêta pour l'étude des surfaces de Kummer non-ordinaires sur des corps de caractéristique deux. Les cas de la caractéristique impaire et des courbes ordinaires sont bien connus. Pour les surfaces de Kummer non-ordinaires en caractéristique 2, nous utilisons en plus une technique de Laszlo, Pauly et Ducrochet [LP02, LP04, Duc08].

Notations. Sauf mention express du contraire, nous utiliserons les notations suivantes :
- a_λ : couplage Ate I de paramètre λ ;
- $a_{[c_0,...c_\ell]}$: couplage Ate II de paramètres $c_0, ..., c_\ell$;
- $\mathbb{A}^n$: espace affine de dimension n ;
- $C/\Bbbk$: une courbe hyperelliptique de genre g définie sur le corps $\Bbbk$;
- $\mathbb{C}$: corps des nombres complexes ;
- χ_C : le polynôme caractéristique du morphisme de Frobenius ;
- η_n : couplage Eta de paramètre $n \in \mathbb{N}$;

- $\mathbb{F}_p$: corps fini de cardinal un nombre premier p ;
- $\Phi_n(x) \in \mathbb{Z}[x]$: polynôme cyclotomique ;
- $\mathbb{H}_n$: demi-espace de Siegel de dimension n ;
- J_C : jacobienne de la courbe hyperelliptique C ;
- $J_C[r]$: les points de $r-$torsion de la jacobienne de C ;
- $J_C(K)$: les points de J_C qui sont rationnels sur le corps K ;
- $\Bbbk := \mathbb{F}_q$: corps fini de caractéristique p et de cardinal q ;
- $\mathcal{K}_A$: variété de Kummer de A (qui est soit une variété abélienne, soit une courbe) ;
- $\mathbb{M}_n$: anneau des matrices carrées d'ordre n ;
- $\mathbb{N}$: les entiers naturels ;
- p : nombre premier fixé ;
- $\mathbb{P}^n$: espace projectif de dimension n ;
- π_q ou π : le morphisme de Frobenius ;
- $\varphi(n)$: fonction indicatrice d'Euler ;
- q : une puissance d'un nombre premier ;
- $\mathbb{Q}$: les nombres rationnels ;
- $\mathbb{Q}_p$: les nombres $p-$adiques ;
- $\mathbb{R}$: les nombres réels ;
- T_n : couplage de Tate de paramètre $n \in \mathbb{N}$;
- $\theta(\cdot,\cdot)$: fonctions thêta de Riemann ;
- $\theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right](\cdot,\cdot)$: fonctions thêta de Riemann avec caractéristique $a, b \in \mathbb{Q}$;
- $v_p(\cdot)$: valuation discrète ;
- W_n : couplage de Weil de paramètre $n \in \mathbb{N}$;
- $\mathbb{Z}$: les entiers relatifs ;
- $\mathbb{Z}_p$: les entiers $p-$adiques ;

Première partie

Rappel sur l'arithmétique des courbes hyperelliptiques

Chapitre 1

Généralités sur les courbes hyperelliptiques

Dans ce chapitre, nous donnons des éléments essentiels pour la compréhension du présent document. Nous rappelons la définition des courbes hyperelliptiques qui sont classifiées par leur genre, puis nous donnons des équations pour des modèles plan affine en distinguant divers cas en fonction de la caractéristique du corps de base. Dès que le genre est plus grand que 2, en général, on ne peut pas munir la courbe d'une structure de groupe algébrique. Par contre, on peut toujours associer à une courbe, sa jacobienne qui est un groupe algébrique. Afin de pouvoir construire la jacobienne d'une courbe, nous rappelons dans ce chapitre, le corps de fonction associé à une courbe, le groupe des diviseurs ainsi que le groupe de Picard.

1.1 Courbes hyperelliptiques

Dans cette partie, nous donnons la définition formelle d'une courbe hyperelliptique. Nous remarquons que notre définition englobe le cas particulier des courbes elliptiques.

Définition 1.1 Soit $\Bbbk$ un corps fini de caractéristique p. On appelle courbe hyperelliptique définie sur $\Bbbk$ une courbe projective lisse dont un modèle plan affine est donné par une équation de la forme :

$$C : y^2 + h(x)y - f(x) = 0, \tag{1.1}$$

où :

- $f \in \Bbbk[x]$ est unitaire et de degré $2g+1$, avec g un entier positif qui est le genre de la courbe,
- $h \in \Bbbk[x]$ est de degré inférieur ou égal à g,
- la lissité de C signifie qu'il n'existe pas de point $P = (a, b)$ de C dans la clôture algébrique $\overline{\Bbbk}$ de $\Bbbk$ tel que : $2b + h(a) = 0,$ et $f'(a) - h'(a)b = 0.$

Le point à l'infini sera noté par P_∞ (ou bien parfois par O pour les courbes elliptiques). L'application $\iota : C \to C, (x, y) \mapsto \iota(x, y) = (x, -y - h(x))$ est appelée *l'involution hyperelliptique* de C. Les points de Weierstraβ de C sont les points invariants par ι, i.e. les points (x, y) vérifiant $y^2 + yh(x) = f(x)$ et $h(x)^2 + 4f(x) = 0$.

Exemple 1.2 Posons $p = 2003$, alors sur le corps $\mathbb{F}_p$, l'équation $y^2 = x^5 + 1184x^2 + 956x + 560$ définit une courbe hyperelliptique de genre $g = 2$.

Soient $C/\Bbbk$ une courbe hyperelliptique et $K/\Bbbk$ une extension algébrique de $\Bbbk$, alors un point P de la courbe C est dit K-rationnel (ou bien rationnel sur K) si ses coordonnées sont dans K. Si K est une extension galoisienne de $\Bbbk$ (ce qui est toujours le cas étant donné que l'on a supposé que $\Bbbk$ était un corps fini), on peut dire que P est K-rationnel si P est invariant par l'action du groupe de Galois $\mathrm{Gal}(\overline{\Bbbk}/K)$ sur ses coordonnées. L'ensemble des points K-rationnels de C est noté par $C(K)$ et les points $\Bbbk-$rationnels sont appelés les points rationnels de C. Soit $\pi : C \to C$ le morphisme de Frobenius défini sur les points de C par $\pi(x, y) := (x^q, y^q)$. Alors il est facile de voir que, pour toute extension finie $K/\Bbbk$ de degré d, un point $P = (x, y)$ est K-rationnel si et seulement si

$$\pi^d(P) = \underbrace{\pi \circ \ldots \circ \pi}_{d \text{ fois}}(P) = P.$$

En général, l'ensemble $C(K)$ n'a pas une structure de groupe, sauf pour $g = 1$ où C est une courbe elliptique que l'on confond avec sa jacobienne [Sil86, p. 66].

1.2 Classification des courbes hyperelliptiques

Dans cette section, nous classifions les modèles plans possibles pour une courbe hyperelliptique de genre $g \leq 2$ en fonction du corps de base. Les situations sur un corps fini $\Bbbk$ ou sur la clôture algébrique $\overline{\Bbbk}$ de $\Bbbk$ sont différentes. Sur $\Bbbk$, les classifications de [EMM02, CJ02, CJ03, DL06, BD04, GEM06] sont basées sur un changement de coordonnées locales de Lockhart [Loc94]. Tandis que sur $\overline{\Bbbk}$, les auteurs de [Anc43, Lan75, Bho90] se fondent sur les solutions du polynôme $h(x)$.

1.2.1 Sur un corps fini

En caractéristique impaire, en faisant le changement de variable, $x = x'$ et $y = y' - h(x)/2$, nous voyons que nous pouvons supposer que $h(x) = 0$ dans l'équation (1.1). Nous pouvons donc écrire l'équation (1.1) sous la forme :

$$C : y^2 = x^{2g+1} + \sum_{i=0}^{2g} f_i x^i \text{ avec } f_i \in \Bbbk. \tag{1.2}$$

En caractéristique deux, nous ne pouvons plus nous ramener à un modèle où $h(x) = 0$. Nous nous contentons de donner les modèles plans possibles en genre 2. La forme générale d'un modèle plan est alors

$$C : y^2 + (h_2x^2 + h_1x + h_0)y = x^5 + f_4x^4 + f_3x^3 + f_2x^2 + f_1x + f_0$$

que nous pouvons classer en 3 catégories :

1. $C : y^2 + (x^2 + h_1x + h_0)y = x^5 + f_1x + f_0$ (courbe ordinaire),
2. $C : y^2 + h_1xy = x^5 + f_3x^3 + f_2x^2 + f_0$, (courbe de $p-$rang 1),
3. $C : y^2 + y = x^5 + f_3x^3 + f_1x + f_0$ (courbe supersingulière).

Voir la section 2.2 pour les définitions de courbe ordinaire, courbe supersingulière et de p-rang.

1.2.2 Sur un corps algébriquement clos

Nous ne donnons que les modèles pour les corps algébriquement clos de caractéristique 2 en genre 2, étant donné que c'est le seul résultat que l'on utilisera par la suite. Dans ce cas, d'après [Lan75], on se ramener aux modèles suivants après un changement de variable rationnel :

1. $C : y^2 + (x^2 + x)y = f_5x^5 + f_3x^3 + f_1x$ (courbe ordinaire),
2. $C : y^2 + xy = f_5x^5 + f_3x^3 + x$ (courbe de p-rang 1),
3. $C : y^2 + y = x^5 + f_3x^3$ (courbe supersingulière).

1.3 Corps de fonction d'une courbe hyperelliptique

Dans cette partie, nous rappelons brièvement comment on peut associer à une courbe hyperelliptique un corps dit corps de fonctions qui caractérise la courbe à morphisme birationnel près.

Définition 1.3 Soit $C : y^2+h(x)y = f(x)$ une courbe hyperelliptique définie sur un corps fini $\Bbbk$, on appelle *anneau des coordonnées affines* de C, l'anneau quotient

$$\Bbbk[C] := \frac{\Bbbk[x, y]}{(y^2 + h(x)y - f(x))}.$$

L'anneau $\Bbbk[C]$ est un anneau intègre et il admet un corps de fractions rationnelles, noté $\Bbbk(C)$, appelé corps des fonctions rationnelles de C sur $\Bbbk$. De la même manière, on définit $K[C]$ et $K(C)$ pour toute extension algébrique $K/\Bbbk$, en remplaçant $\Bbbk$ par K dans la précédente définition.

Soit P un point K-rationnel de C, alors l'ensemble des fonctions $\psi \in \Bbbk[C]$ telles que $\psi(P) = 0$ forme un idéal maximal de $\Bbbk[C]$, noté M_P.

Définition 1.4 Soient C une courbe hyperelliptique définie sur $\Bbbk$ et P un point K-rationnel. L'anneau local de C en P, noté $\Bbbk[C]_P$, est le localisé de $\Bbbk[C]$ en M_P. En d'autres termes,

$$\Bbbk[C]_P := \left\{ \frac{\psi}{\phi} \in \Bbbk(C) : \phi(P) \neq 0 \right\}.$$

Proposition 1.5 *L'anneau $\Bbbk[C]_P$ est un anneau de valuation discrète où la valuation est donnée par l'application*

$$v_P : \Bbbk[C]_P \to \mathbb{N} \cup \{\infty\},\ v_P(\psi) = \max\{d \in \mathbb{N} : \psi \in M_P^d\}.$$

Remarque 1.6 On peut étendre l'application v_P au corps des fonctions rationnelles $\Bbbk(C)$ de C en posant $v_p(\psi/\phi) = v_P(\psi) - v_P(\phi)$.

Définition 1.7 On dit qu'une fonction $\psi \in K(C)$ est une uniformisante pour C en P si $v_P(\psi) = 1$ (alors ψ est un générateur de l'idéal maximal M_P).

Soit une fonction $\psi \in K(C)$, alors pour tout point K-rationnel P de C, l'entier $v_P(\psi)$ est appelé l'ordre de la fonction ψ en P. Si $v_P(\psi) > 0$, alors on dit que la fonction ψ a un *zéro* en P, et si $v_P(\psi) < 0$, on dit que la fonction ψ a un *pôle* en P.

Si $v_P(\psi) \geq 0$, alors on dit que la fonction ψ est régulière (ou définie) en P et on peut alors calculer $\psi(P)$ comme l'image de ψ dans $\Bbbk[C]/M_P$ par la projection canonique $\Bbbk[C] \to \Bbbk[C]/M_P$, sinon la fonction ψ a un pôle en P et on pose alors $\psi(P) = \infty$. Nous aurons besoin de la proposition suivante :

Proposition 1.8 *Soit C une courbe hyperelliptique définie sur $\mathbb{k}$ et $\psi \in \overline{\mathbb{k}}(C)$. Alors ψ admet un nombre fini de zéros et de pôles.*

Preuve : voir [Sil86, p. 22]. □

1.4 Diviseurs d'une courbe

On sait que pour une courbe C définie sur un corps fini $\mathbb{k}$, l'ensemble des points $\mathbb{k}$-rationnels ne peut pas être en général muni d'une structure de groupe. Par contre, on peut former naturellement le groupe commutatif libre sur les points de la courbe à savoir le groupe des diviseurs. Ce groupe est important car il permet de définir la jacobienne d'une courbe qui est un groupe que l'on peut munir d'une structure de variété algébrique.

Définitions 1.9 Soit C une courbe hyperelliptique définie sur $\mathbb{k}$. Le groupe libre engendré par les points de $C(\overline{\mathbb{k}})$ est appelé le groupe de diviseurs de C, et on le note par $Div_C(\overline{\mathbb{k}})$ ou simplement par Div_C. Un diviseur $D \in Div_C$ est une somme formelle de la forme

$$D = \sum_{P \in C(\overline{\mathbb{k}})} n_P.(P), \text{ avec } n_P \in \mathbb{Z} \text{ et } n_P = 0 \text{ sauf pour un nombre fini de points.}$$

Soient $D = \sum n_P.(P)$ et $D' = \sum n'_P.(P)$ des éléments de Div_C. La somme de D et D' est donnée par la formule suivante :

$$D + D' = \sum_{P \in C(\overline{\mathbb{k}})} (n_P + n'_P).(P).$$

On appelle le support d'un diviseur D, l'ensemble noté $\text{supp}(D) := \{P \in C, n_P \neq 0\}$.

Pour un diviseur $D = \sum n_P.(P)$ de Div_C, on appelle le degré de D, l'entier naturel donné par

$$\deg(D) = \sum_{P \in C(\overline{\mathbb{k}})} n_P.$$

L'ensemble des diviseurs de degré zéro forme un sous-groupe de Div_C, noté Div_C^0. Un diviseur $D = \sum_{P \in C} n_P(P)$ est dit effectif si $n_P \geq 0$ pour tout point P de $C(\overline{\mathbb{k}})$. On dit qu'un diviseur D_1 est supérieur à un diviseur D_2, et on note $D_1 \geq D_2$ si $D_1 - D_2$ est un diviseur effectif.

Soit K une extension algébrique de $\mathbb{k}$, alors le groupe de Galois $\text{Gal}(\overline{\mathbb{k}}/K)$ agit sur le groupe Div_C de la manière suivante :

$$\forall \sigma \in \text{Gal}(\overline{\mathbb{k}}/K), \text{ et } \forall D = \sum_{P \in C} n_p.(P), \text{ on a } \sigma(D) = \sum_{P \in C} n_P.(\sigma(P)).$$

On dit que le diviseur $D = \sum_{P \in C} n_P(P)$ est rationnel ou défini sur K si $\sigma(D) = D$ pour tout $\sigma \in \text{Gal}(\overline{\mathbb{k}}/K)$. Considérons le morphisme de Frobenius sur C, $\pi : (x, y) \mapsto (x^q, y^q)$, alors on peut faire agir π sur l'ensemble des diviseurs. Pour cela, à tout diviseur $D = \sum_{P \in C(\overline{\mathbb{k}})} n_P.(P)$, définissons l'action de π sur D par

$$\pi(D) = \sum_{P \in C(\overline{\mathbb{k}})} n_P.(\pi(P)).$$

Soit $K/\Bbbk$ une extension de $\Bbbk$ de degré d, alors D est K-rationnel si et seulement si

$$\pi^d(D) = D.$$

Attention : Pour $D = n_1(P_1) + ... + n_t(P_t)$ où tous les n_i sont non nuls, alors dire que le diviseur D est défini sur K ne signifie pas que tous les P_i sont $K-$rationnels.

L'ensemble des diviseurs K-rationnels (noté $Div_C(K)$) et des diviseurs K-rationnels de degré zéro (noté $Div_C^0(K)$) forment un sous-groupe de Div_C.
Soit une fonction $\psi \in \overline{\Bbbk}(C)$, alors on peut définir le diviseur de ψ noté $\mathrm{div}(\psi)$ (ou parfois par (ψ)) par :

$$\mathrm{div}(\psi) = \sum_{P \in C(\overline{\Bbbk})} v_P(\psi).(P).$$

Pour toute extension algébrique K de $\Bbbk$, si une fonction $\psi \in K(C)$, alors $\mathrm{div}(\psi) \in Div_C(K)$. On dit qu'un diviseur $D \in Div_C$ est principal si D est un diviseur d'une fonction. On dit que deux diviseurs D_1 et D_2 sont linéairement équivalents, et on note $D_1 \sim D_2$, si $D_1 - D_2$ est un diviseur principal. L'ensemble des diviseurs principaux de C, noté Prin_C, forme un sous-groupe de Div_C.

Proposition 1.10 *Soient C une courbe hyperelliptique définie sur $\Bbbk$ et une fonction non nulle $\psi \in \overline{\Bbbk}(C)$. Alors :*

(a) $\deg(\mathrm{div}(\psi)) = 0$, *donc* Prin_C *est un sous-groupe de* Div_C^0.

(b) $\mathrm{div}(\psi) = 0$ *si et seulement si la fonction ψ est une constante de* $\overline{\Bbbk}^*$

Preuve : voir [Sil86, p. 32] ou bien [Har77, p. 138]. □

Remarque 1.11 Soit $D \in Div_C^0$, alors il existe deux diviseurs effectifs D_0 et D_∞, de même degré tels que $D = D_0 - D_\infty$. Le degré de D_0 est appelé le **poids** du diviseur D.

Chapitre 2

Jacobienne d'une courbe hyperelliptique

Dans ce chapitre, nous abordons les notions de jacobienne, du polynôme caractéristique du Frobenius et des courbes « friendly-pairing ». Nous rappelons que $\mathbb{k}$ désigne un corps fini de caractéristique p et de cardinal q et que $C/\mathbb{k}$ est une courbe hyperelliptique de genre g.

2.1 Généralités

Définition 2.1 On appelle groupe des classes de diviseurs et l'on note Pic_C, le groupe quotient de Div_C^0 par le sous-groupe des diviseurs principaux Prin_C. Pour toute extension finie K de $\mathbb{k}$, le groupe des classes de diviseurs qui sont K-rationnels est par définition le sous-groupe $Pic_C(K)$ de Pic_C invariant par l'action de $\mathrm{Gal}(\overline{\mathbb{k}}/K)$. Notons que l'on a par définition $Pic_C = Pic_C(\overline{\mathbb{k}})$.

Posons $G = \mathrm{Gal}(\overline{\mathbb{k}}/K)$. D'après la précédente définition, nous avons la suite exacte suivante de G-modules :

$$0 \to Prin_C \to Div_C^0 \to Pic_C \to 0.$$

De la suite exacte longue de cohomologie associée à la précédente suite exacte, on déduit :

$$Prin_C(K) \to Div_C^0(K) \to Pic_C(K) \to H^1(G, Prin_C(K)).$$

On peut montrer que si C est une courbe hyperelliptique, alors $H^1(G, Prin_C(K)) = 0$ et on a donc :

$$Pic_C(K) = \frac{Div_C^0(K)}{Prin_C(K)}.$$

Définition 2.2 Soit C une courbe hyperelliptique, la jacobienne de C est la variété projective lisse J_C qui est caractérisée (à isomorphisme près) par la propriété suivante : pour tout extension algébrique K de $\mathbb{k}$ il existe une bijection $\phi_K : Pic_C(K) \to J_C(K)$ et les ϕ_K sont compatibles avec les injections naturelles $J_C(K) \to J_C(K')$ et $Pic_C(K) \to Pic_C(K')$ si K' est une extension algébrique de K.

En fait dans cette partie, nous n'aurons jamais besoin de considérer la structure de variété algébrique sur J_C et donc nous manipulerons les points de J_C comme des éléments de Pic_C.

Remarque 2.3 Toute classe de diviseur $D \in Pic_C$ peut être représentée par un *diviseur semi-réduit*, i.e. un diviseur de la forme

$$\sum_{i=1}^{m}(P_i) - m(P_\infty), \text{ avec } P_i \in C(\overline{\Bbbk}),\ P_i \neq P_\infty \text{ et } P_i \neq \iota(P_j) \text{ pour } i \neq j.$$

L'entier m est le poids du diviseur D, et D est dit *réduit* si $m \leq g$. Tout diviseur semi-réduit peut être représenté sous la forme unique d'un diviseur réduit (voir [Mum84, p. 18]).

Nous verrons comment réduire une classe de diviseur grâce à l'algorithme de réduction de Cantor. Cet algorithme repose sur une représentation agréable des diviseurs réduits appelée *représentation de Mumford*.

Théorème 2.4 (représentation de Mumford) *Soit $C : y^2 + h(x)y = f(x)$ une courbe hyperelliptique, de genre g, définie sur un corps fini $\Bbbk$. Soit K une extension algébrique de $\Bbbk$, alors tout élément D de J_C peut être représenté de façon unique par un couple $(u(x), v(x)) \in K[x]^2$ tel que :*

(i) u est un polynôme unitaire, avec $deg(u) \leq g$,

(ii) $deg(v) < deg(u)$, et

(iii) $u(x)$ divise $v(x)^2 + v(x)h(x) - f(x)$.

Preuve : [ACD+06].

Remarque 2.5 Pour passer de la représentation de Mumford d'un diviseur $D = (u(x), v(x))$ à la représentation naturelle $D = \sum_{i=1}^{m}(P_i) - m(P_\infty)$, on calcule les coordonnées des points $P_i = (x_i, v(x_i))$ avec x_i une racine de $u(x)$. Pour cela, on trouve les racines x_i de $u(x)$, ces racines sont les abscisses des points P_i dont les ordonnées sont les $v(x_i)$.

Le théorème 2.4 et la remarque précédente permettent de représenter des éléments de la jacobienne. En genre 2, la représentation de Mumford du diviseur de degré 0 dont la partie effective est la somme des points $P_1 = (x_1, y_1)$ et $P_2 = (x_2, y_2)$ s'obtient en une multiplication et une division par :

$$u(x) = x^2 - (x_1 + x_2)x + x_1x_2 \qquad \text{et} \qquad v(x) = \frac{y_1 - y_2}{x_1 - x_2}(x - x_1) + y_1.$$

2.2 Points de torsion

Soient n un entier relatif et D un élément de J_C, on définit :

$$\begin{aligned} [n]\,D &= \underbrace{D + D + ... + D}_{n \text{ fois}} && \text{si } n > 0, \\ [n]\,D &= -([-n]\,D) && \text{si } n < 0, \\ [0]\,D &= P_\infty. \end{aligned}$$

On dit que $D \in J_C$ est un diviseur de $n-$torsion si $[n]\,D = P_\infty$. L'ensemble des diviseurs de $n-$torsion est noté par $J_C\,[n]$ et si K est une extension algébrique de $\Bbbk$, l'ensemble des diviseurs de $n-$torsion qui sont rationnels sur le corps K est noté par $J_C\,[n]\,(K)$.

Proposition 2.6 *Soit p la caractéristique du corps fini $\Bbbk$, alors :*

1. *Si n est premier avec p, alors $J_C[n] = (\mathbb{Z}/n\mathbb{Z})^{2g}$.*
2. *Si $n = p^m$, alors $J_C[n] = (\mathbb{Z}/n\mathbb{Z})^t$ avec $t \in \mathbb{N}$ et $0 \leq t \leq g$.*

Preuve : voir [Mum74, p. 64]. □

L'entier t du deuxième cas est appelé le $p-$rang de la Jacobienne ou de la courbe.

Définition 2.7

1. Une courbe hyperelliptique est dite *ordinaire* si son $p-$rang est égal à g.
2. Une courbe elliptique est dite *supersingulière* si son $p-$rang est 0.
3. Une courbe hyperelliptique est dite *supersingulière* si sa jacobienne est *isogène* à un produit de g courbes elliptiques supersingulières.

Remarque 2.8 [ACD+06, p. 61] Une courbe hyperelliptique de genre ≤ 2 est supersingulière si et seulement si son $p-$rang est nul. Mais cela est faux en genre supérieur.

2.3 Polynôme caractéristique du Frobenius

Le morphisme de Frobenius, comme nous allons le voir, joue un rôle capital dans l'étude des courbes définies sur un corps fini. Il permet entre autre de calculer le cardinal de la jacobienne de la courbe. Au morphisme de Frobenius, nous allons associer son polynôme caractéristique qui est un invariant de la classe d'isogénie de la jacobienne de la courbe. Sur le plan pratique, il est classique d'utiliser le morphisme de Frobenius comme d'un moyen pour accélérer l'arithmétique sur les jacobiennes de courbes. Ainsi, nous verrons dans la partie II comment utiliser le morphisme de Frobenius pour calculer rapidement les couplages. Nous introduisons ici le matériel nécessaire pour la compréhension des algorithmes de la partie II.

Définition 2.9 Soit C une courbe définie sur $\mathbb{k}$ de jacobienne $J_C = J_C(\overline{\mathbb{k}})$. Le morphisme de Frobenius est l'application

$$\pi_q : J_C \to J_C,\ D := \sum_{P \in C} n_P(P) \mapsto \pi_q(D) = \sum_{P \in C} n_P(\pi_q(P)),$$

avec $\pi_q(P) = \pi_q(x, y) = (x^q, y^q)$. Si aucune ambiguïté n'est à craindre, on peut juste écrire π au lieu de π_q.

Proposition 2.10 (Propriétés du morphisme Frobenius)

1. π est une isogénie purement inséparable de degré q^g sur la variété J_C,
2. Pour tout entier positif d, on a $\pi_q^d = \pi_{q^d}$,
3. $J_C(\mathbb{k}) = \{D \in Pic_C,\ \pi(D) = D\} = \ker(\pi - [1])$,

3'. $D \in J_C(\mathbb{F}_{q^d}) \Leftrightarrow \pi_{q^d}(D) = D$.

Ces propriétés simples à démontrer montrent que l'on peut considérer l'ensemble des points de J_C rationnels sur une extension finie de $\mathbb{k}$ comme les points fixes de $J_C(\overline{\mathbb{k}})$ par l'action d'une puissance du morphisme de Frobenius. Une autre remarque importante est que le morphisme de Frobenius étant une isogénie est un automorphisme linéaire de $J_C[n]$ pour $n \in \mathbb{N}^*$. Ces faits sont à la base d'un ensemble de résultats qui relient, parfois de manière effective, le cardinal de $J_C(K)$ pour une extension finie K de $\mathbb{k}$ et le polynôme caractéristique du Frobenius agissant sur les éléments de $J_C[n]$.

Définition 2.11 Le polynôme caractéristique du morphisme de Frobenius π est le polynôme

$$\chi(\pi)_C(T) := T^{2g} + a_1 T^{2g-1} + ... + a_g T^g + a_{g-1} q T^{g-1} + ... + a_1 q^{g-1} T + q^g,$$

avec $a_i \in \mathbb{Z}$, $1 \leq i \leq g$ tel que pour tout élément $D \in J_C(\overline{\mathbb{k}})$, on ait :

$$\pi^{2g}(D) + [a_1]\,\pi^{2g-1}(D) + ... + [a_g]\,\pi^g(D) + ... + [q^g]\,(D) = (P_\infty).$$

Proposition 2.12 *Le polynôme caractéristique du morphisme de Frobenius vérifie les propriétés suivantes :*

1. *chaque coefficient a_i vérifie $|a_i| \leq \binom{2g}{i} q^{i/2}$,*
2. *la trace de $\chi(\pi)_C$ est la trace de la courbe C,*
3. *pour tout entier r premier avec q, la restriction de π à $J_C[r]$ a pour polynôme caractéristique $\chi(\pi)_C \pmod r$,*
4. *$\#J_C(\mathbb{k}) = \chi(\pi)_C(1)$,*

où $\binom{n}{p} = \dfrac{n!}{p!(n-p)!}$ représente les coefficients binomiaux.

Exemple 2.13 Soit E une courbe elliptique sur un corps fini $\mathbb{k}$, alors $\chi(\pi)_E(T) = T^2 - tT + q$, avec t la trace de $\chi(\pi)_E$.

Remarque 2.14 Soit $C/\mathbb{k}$ une courbe hyperelliptique définie sur un corps fini $\mathbb{k}$ de genre g et de jacobienne J_C et soit $E/\mathbb{k}$ une courbe elliptique. D'après le théorème de Hasse-Weil, on peut borner le cardinal de la jacobienne par :

$$(\sqrt{q} - 1)^g \leq \#(J_C(\mathbb{k})) \leq (\sqrt{q} + 1)^g.$$

Rappelons que les seules attaques connues pour résoudre le DLP sur les courbes hyperelliptiques sont les algorithmes génériques de coût $O(q^{g/2})$. La construction des courbes en genre supérieur nécessite alors des corps plus petits que ceux que l'on a besoin pour les courbes en genre 1. Par exemple, pour un même niveau de sécurité, une courbe elliptique de taille $\#(E(\mathbb{k})) \approx 2^{360}$ correspond à une courbe hyperelliptique de genre 2 de taille $\#(J_C(\mathbb{k})) \approx 2^{180}$ ou à une courbe hyperelliptique de genre 3 de taille $\#(J_C(\mathbb{k})) \approx 2^{120}$. Choisir d'implémenter les courbes sur des corps petits est déterminant pour certains appareils qui disposent de peu de ressources.

Le $2g$ racines du polynôme caractéristique du morphisme de Frobenius vérifient les propriétés suivantes :

Proposition 2.15 *Si on note par $\lambda_1, ..., \lambda_{2g}$ les racines de $\chi(\pi)_C$, alors :*

4. *Chaque λ_i est un nombre algébrique de degré $\leq 2g$,*
5. *le produit des λ_i donne $\prod \lambda_i = q^g$,*
6. *on peut réorganiser les racines λ_i pour $1 \leq i \leq g$ de façon à avoir $\lambda_i \lambda_{i+g} = q$.*
7. *Si on considère les λ_i comme des nombres complexes, alors leur valeur absolue est $|\lambda_i| = \sqrt{q}$.*

Preuve : voir le [ACD+06, théorème 5.76]. □

Pour calculer le polynôme caractéristique du morphisme de Frobenius, on peut calculer les coefficients a_i pour $1 \leq i \leq g$ en utilisant le procédé décrit par [ACD+06, théorème 14.17]. Cependant, le calcul efficace du polynôme caractéristique du Frobenius pour des tailles cryptographiques est une question difficile en genre 2 et 3.

La proposition suivante sera bien utile pour la définition du couplage de Ate :

Proposition 2.16 *Soient $C/\Bbbk$ une courbe hyperelliptique de genre g et de jacobienne J_C. Soit r un entier premier qui divise $\#J_C(\Bbbk)$, alors $1 \bmod r$ et $q \bmod r$ sont des valeurs propres de $\pi|_{J_C[r]}$, autrement dit, des racines de $\chi(\pi) \pmod r$.*

Preuve : Il est clair que $1 \bmod r$ est une valeur propre de $\chi(\pi) \pmod r$ car comme r divise $\sharp J_C(\Bbbk)$, il existe au moins un élément $D \in J_C(\Bbbk)$ et par définition on a $\pi(D) = D$. Et d'après la proposition 2.15, $q \bmod r$ est aussi une valeur propre de $\chi(\phi) \pmod r$. □

Remarque 2.17 La proposition précédente spécialisée au cas d'une courbe elliptique définie sur $\Bbbk$ donne que pour tout entier r premier avec q et qui divise $\#E(\Bbbk)$, il existe deux points $P, Q \in E[r]$ tels que $\pi(P) = P$ et $\pi(Q) = [q]\,Q$.

2.4 Courbes « pairing-friendly »

Les courbes « friendly-pairing » (i.e. des courbes idéales pour le couplage) sont des courbes dont le logarithme discret est difficile, mais dont le couplage reste facile. En effet, les protocoles que nous allons construire avec les couplages doivent résister aux attaques MOV [MOV93] et FR [FR94]. Nous allons nous restreindre aux courbes hyperelliptiques de genre 2.

Définitions 2.18 On dit que $C/\Bbbk$ est une courbe « friendly-pairing » si :

- $\#J_C(\Bbbk)$ est suffisamment grand,
- $\#J_C(\Bbbk)$ est divisible par un grand entier r premier avec q ($r \approx \#J_C(\Bbbk)$),
- le degré de plongement d relativement à r doit être petit.

Soit r un entier premier avec $q = \#\Bbbk$ et qui divise $\#J_C(\Bbbk)$. On appelle la ρ-valeur de C (relativement à r) le réel donné par

$$\rho(C) = g\frac{\log(q)}{\log(r)}.$$

Chapitre 3

Arithmétique sur la jacobienne d'une courbe hyperelliptique

Dans ce chapitre, nous faisons quelques rappels sur l'arithmétique des courbes hyperelliptiques. Nous commençons par le cas particulier bien connu des courbes elliptiques.

3.1 Arithmétique sur une courbe elliptique

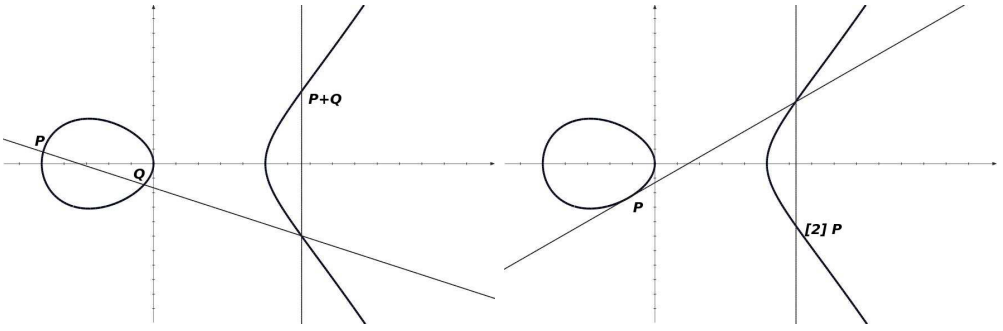

FIG. 3.1 – Additionner deux points - Doubler un point

Cette partie est consacrée aux rappels de l'arithmétique des courbes elliptiques $E/\Bbbk$. Soit K une extension algébrique de $\Bbbk$, alors $E(K)$ est un groupe abélien dont la loi d'addition est donnée par le théorème suivant :

Théorème 3.1 *[Sil86, III.2] On peut définir une loi de composition $+$ sur $E(K)$ de la manière suivante. Soit $P, Q \in E$, la droite ℓ_{PQ} passant par P et Q (qui est la tangente à la courbe si $P = Q$) rencontre la courbe E en un troisième point R. La droite ℓ_{RP_∞} passant par R et le point à l'infini P_∞ coupe la courbe E en un troisième point R' (qui est l'opposé de R) et on pose $P + Q = R'$.*

L'ensemble $E(K)$ muni de la loi de composition $+$ est un groupe.

Cette loi peut être décrite graphiquement comme dans la figure 3.1 (avec $E : y^2 = x^3 - x$ définie sur $\mathbb{R}$). La loi précédente s'exprime dans les coordonnées du modèle de Weierstraβ de la courbe avec des formules optimisées qui dépendent de la caractéristique de $\Bbbk$.

Caractéristique impaire : soient $\Bbbk$ un corps fini de caractéristique p, et une courbe elliptique donnée par son équation de Weierstraβ réduite $E : y^2 = x^3 + ax + b$ avec $a, b \in \Bbbk$.

Soit K une extension finie de $\Bbbk$, la loi de groupe de $E(K)$ est donné par : (voir [Sil86, p. 58]) :

1. $-(x, y) = (x, -y)$;
2. $(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$ avec $x_3 = \lambda^2 - x_1 - x_2,\ y_3 = \lambda(x_1 - x_3) - y_1$, et
   a. $\lambda = (y_1 - y_2)/(x_1 - x_2)$ si $(x_1, y_1) \neq \pm(x_2, y_2)$,
   b. $\lambda = (3x_1^2 + a)/(2y_1)$ si $(x_1, y_1) = (x_2, y_2)$.

L'addition nécessite 2 multiplications, 1 carré et une inversion dans K et la duplication 2 multiplications, 2 carrés et une inversion. Les attaques dites attaques à canaux cachés exploitent cette différence de coût de calcul entre l'addition et la duplication. Des contremesures existent (en genre 1, voir [BJ02, BDJ04] ou [BSS05, chap. 5]), mais dans ce mémoire nous nous intéresserons principalement aux techniques, en genre 2, qui permettent d'avoir une loi de groupe unifiée.

Caractéristique paire, nous avons deux possibilités pour l'équation de la courbe selon qu'elle soit ou non supersingulière :

$$E_1 : y^2 + xy = x^3 + a_2x^2 + a_6 \text{ ou bien } E_2 : y^2 + a_3y = x^3 + a_4x + a_6.$$

Cas 1 : avec la courbe $E_1 : y^2 + xy = x^3 + a_2x^2 + a_6$, on a :

a_1. $-(x, y) = (x, x + y)\ \forall\, (x, y) \in E_1$;

b_1. pour tout $(x_1, y_1), (x_2, x_2)$ de E_1, si $(x_3, y_3) = (x_1, y_1) + (x_2, y_2)$ alors
$x_3 = \lambda^2 + \lambda + x_1 + x_2 + a_2, y_3 = \lambda(x_1 + x_3) + x_3 + y_1$ et $\lambda = (y_1 + y_2)/(x_1 + x_2)$;

c_1. pour tout (x_1, y_1) de E_1, si $(x_3, y_3) = [2]\,(x_1, y_1)$ alors
$x_3 = \lambda^2 + \lambda + a_2$, $y_3 = \lambda(x_1 + x_3) + x_3 + y_1$ et $\lambda = x_1 + (y_1/x_1)$.

Cas 2 : avec la courbe $E_2 : y^2 + a_3y = x^3 + a_4x + a_6$, on a :

a_2. $-(x, y) = (x, y + a_3)\ \forall\, (x, y) \in E_2$;

b_2. pour tout $(x_1, y_1), (x_2, x_2)$ de E_2, si $(x_3, y_3) = (x_1, y_1) + (x_2, y_2)$ alors
$x_3 = \lambda^2 + x_1 + x_2,\ y_3 = \lambda(x_1 + x_3) + y_1 + a_3$ et $\lambda = (y_1 + y_2)/(x_1 + x_2)$;

c_2. pour tout (x_1, y_1) de E_2, si $(x_3, y_3) = [2]\,(x_1, y_1)$ alors
$x_3 = \lambda^2,\ y_3 = \lambda(x_1 + x_3) + y_1 + a_3$ et $\lambda = (x_1^2 + a_4)/a_3$.

Nous verrons dans la partie une représentation optimisée pour les courbes elliptiques ordinaires définies sur un corps de caractéristique deux.

3.2 Addition et réduction de Cantor

Soit $C : y^2 + h(x)y = f(x)$ une courbe hyperelliptique définie sur un corps fini $\Bbbk$, de genre g et de jacobienne J_C. Dans cette partie, nous allons calculer la somme de deux éléments de la jacobienne représentés par leur diviseurs réduits D_1 et D_2 grâce à l'algorithme de Cantor [Can87] publié en 1987 pour les corps de caractéristique impaire, et généralisé par Koblitz [Kob89] en 1989.

L'algorithme de Cantor prend en entrée deux diviseurs réduits D_1 et D_2 correspondants à des éléments de $J_C(\overline{\Bbbk})$ et se compose de deux parties :

- une partie addition qui permet de calculer un diviseur semi-réduit D_s de poids inférieur à $2g$ dans la classe de $D_1 + D_2$;

– une partie de réduction qui consiste à calculer l'unique diviseur réduit équivalent au diviseur semiréduit D_s.

L'unicité de la représentation de chaque élément de $J_C(\overline{\mathbb{k}})$ sous la forme d'un diviseur réduit assure alors que l'on peut par exemple tester l'égalité de deux éléments de $J_C(\overline{\mathbb{k}})$ et que l'on a donc bien défini une arithmétique sur $J_C(\overline{\mathbb{k}})$.

3.2.1 Addition de Cantor

Cantor donne des formules explicites pour calculer le diviseur semi-réduit correspondant à la somme de deux diviseurs réduits rationnels sur une extension K de $\mathbb{k}$.

Considérons deux diviseurs D_1 et D_2 de J_C rationnels sur K. La somme de D_1 et D_2 se fait grâce à l'algorithme d'addition de Cantor 3.2.1 qui utilise la représentation de Mumford $D_i = (u_i(x), v_i(x))$ pour $i = 1, 2$, tels que $u_i(x), v_i(x) \in K[x]$:

Algorithm 3.2.1 Algorithme d'addition de Cantor

`Entrée` : Deux diviseurs réduits $D_1 = (u_1, v_1)$ et $D_2 = (u_2, v_2) \in J_C(K)$
`Sortie` : Un diviseur semi-réduit $D_s = D_1 + D_2 \in J_C(K)$

1: **calculer** $d_1 \leftarrow \gcd(u_1, u_2) := e_1u_1 + e_2u_2$
2: **calculer** $d \leftarrow \gcd(d_1, v_1 + v_2 + h) := c_1d_1 + c_2(v_1 + v_2 + h)$
3: **calculer** $s_1 \leftarrow c_1e_1$, $s_2 \leftarrow c_1e_2$ et prendre $s_3 \leftarrow c_2$
4: **calculer** $u \leftarrow \frac{u_1u_2}{d^2}$ et $v \leftarrow \frac{s_1u_1v_2+s_2u_2v_1+s_3(v_1v_2+f)}{d} \bmod u$
5: **retourner** $D_s = (u, v)$

Dans le cas où $d_1 = \gcd(u_1, u_2) = 1$ c'est-à-dire quand les supports des diviseurs D_1 et D_2 sont disjoints, l'algorithme précédent s'explique très simplement :

– on a $u = u_1u_2$ car on souhaite que le support de D soit la somme des supports de D_1 et D_2 ;
– il est facile de voir que v est alors le polynôme qui interpole les valeurs de v_1 et de v_2 aux racines de u_1u_2.

Dans le cas, où le support de D_1 et de D_2 ne sont pas disjoints, il faut ajouter le diviseur d'une fonction de manière à rendre le diviseur calculé semi-réduit.

Remarque 3.2 Le diviseur semi-réduit D_s vérifie la relation suivante :

$$D_s = D_1 + D_2 - \mathrm{div}(d(x)).$$

Le diviseur $\mathrm{div}(d(x))$ joue un rôle fondamental dans le calcul des couplages, car il permet de calculer la fonction de Weil-Miller (voir section 4.2.1 et section 4.2.2).

Complexité de l'addition de Cantor. L'algorithme d'addition de Cantor nécessite 2 pgcd, 9 multiplications, un carré et 2 divisions de polynômes de $K[x]$ de degré inférieur ou égal à $2g$. Le calcul rapide du pgcd de deux polynômes peut s'effectuer en $O(M(g)\log g)$ opérations dans K [GG99, p. 301] où $M(g)$ est le temps de la multiplication de deux polynômes de degrés g. La fonction $M(g)$ dépend de l'algorithme choisi : Karatsuba coûte au plus $g^{1.59}$ multiplications dans K, et les méthodes rapides à base de transformations de Fourier rapide (FFT) descendent jusqu'à $O(g\log g\log\log g)$. Finalement l'algorithme d'addition de Cantor nécessite $O(g(\log g)^2\log\log g)$ opérations dans K.

Algorithm 3.2.2 Algorithme de réduction de Cantor

`Entrée` : Un diviseur semi-réduit $D_s = (u, v)$, avec $\deg(u) > g$.
`Sortie` : un diviseur réduit $D = (U, V)$

1: **tant que** $\deg(u) > g$ faire
2: **calculer** $U \leftarrow (f - vh - v^2)/u$
3: **calculer** $V \leftarrow -(v + h) \bmod U$
4: **prendre** $u \leftarrow U$ et $v \leftarrow V$
5: **fin tant que**
6: **rendre** u unitaire
7: **retourner** $D := (U, V)$

3.2.2 Réduction de Cantor

L'algorithme 3.2.1 donne un diviseur semi-réduit $D_s = (u(x), v(x))$ avec $\deg(u) > g$. On peut réduire D_s grâce à l'algorithme 3.2.2 qui fait baisser le degré de la partie effective (le poids) du diviseur semi-réduit D_s en ajoutant des diviseurs principaux. Chaque itération fait baisser ce poids de 2 (sauf la dernière qui ne le fait baisser que de 1). Comme, on part d'un diviseur semi-réduit de poids au plus $2g$, on voit qu'il y a au plus $\lceil g/2 \rceil$ itérations de la boucle $1 - 5$ de l'algorithme. Nous renvoyons le lecteur à [Can87] pour une preuve de l'algorithme. Comme nous travaillons généralement en genre petit, l'algorithme de Cantor est rapide, et nous allons le rendre plus explicite en genre 2 dans la section suivante.

Remarque 3.3 $D = D_s - \mathrm{div}\left(\frac{y - v(x)}{u'(x)}\right)$. En combinant l'algorithme d'addition et l'algorithme de réduction, on obtient l'algorithme de Cantor et aussi la fonction de Miller (voir les sections 4.2.1 et 4.2.2).

Complexité de la réduction de Cantor. Nous avons besoin de $O(g/2)$ itérations où chaque itération nécessite $O(M(2g))$ [GG99, §9.1] opérations dans K le corps de définition du diviseur D.

3.3 Formules explicites en genre 2

Dans cette section, nous donnons des formules explicites de l'algorithme de Cantor en genre 2 en se basant sur les formules explicites de Lange [Lan01, Lan02a]. L'idée est de dérouler la boucle de l'algorithme de Cantor et de regrouper les opérations de manière à optimiser l'algorithme résultant. Nous ajoutons une petite originalité à notre présentation en modifiant un peu l'algorithme obtenu de manière à le rendre résistant aux attaques par canaux auxiliaires les plus simples.

On représente les diviseurs réduits D_i pour $i = 1, 2$ sous la forme de Mumford $D_i = (u_i, v_i)$. Pour obtenir un diviseur semi-réduit linéairement équivalent à $D_s := D_1 + D_2$, on calcule le polynôme $u = u_1 u_2$ et le polynôme v de degré inférieur strictement au degré de u tel que

$$v \equiv v_i \pmod{u_i}, \text{ pour } i = 1, 2.$$

Pour calculer le polynôme v, nous distinguons deux cas qui correspondent aux cas les plus fréquents rencontrés dans une exponentiation :

1) les polynômes u_1 et u_2 sont premiers entre eux.

2) les polynômes u_1 et u_2 sont égaux (c'est le cas quand on fait une duplication).

Les cas résiduels étant très rares, on peut se contenter d'utiliser l'algorithme de Cantor standard sans que cela modifie vraiment la complexité de l'algorithme résultant ou sa qualité de résister à des attaques par canaux auxiliaires.

Addition : comme on souhaite que v soit tel que $v \equiv v_1 \bmod u_1$, alors il existe un unique polynôme s_1 tel que $v = s_1u_1 + v_1$, avec $\deg(s_1) = \deg(v) - \deg(u_1)$. Donc en calculant modulo u_2, on a :

$$\begin{aligned}(v_2 \bmod u_2 \equiv v) &\iff (v_2 \bmod u_2 \equiv s_1u_1 \bmod u_2 + v_1 \bmod u_2),\\ &\iff s_1u_1 \bmod u_2 \equiv (v_2 - v_1) \bmod u_2.\end{aligned}$$

Comme u_1 et u_2 sont premiers entre eux, on obtient dans ce cas

$$v = s_1u_1 + v_1 \text{ avec } s_1 = \frac{v_2 - v_1}{u_1} \bmod u_2.$$

Duplication : les polynômes u_1 et u_2 sont égaux et de même $v_1 = v_2$. Alors les polynômes u, v, u_1 et v_1 vérifient les formules suivantes :

$$\begin{aligned}u &= u_1^2,\\ v &\equiv v_1 \bmod u_1 \iff (v_1 = v - s_1u_1),\\ u &\mid f - vh - v^2,\\ u_1 &\mid f - v_1h - v_1^2 \iff (u_1t = f^2 - v_1h - v_1^2).\end{aligned}$$

En remplaçant l'expression de v_1 de la deuxième équation dans la quatrième équation et en divisant par u_1, on obtient

$$t = \frac{f - vh - v^2}{u_1} + s_1(h + 2v - s_1u_1).$$

La fraction $(f - vh - v^2)/u_1$ est exacte et est même encore divisible par u_1, donc quand on réduit modulo u_1, on obtient

$$t \equiv s_1(h + 2v_1) \bmod u_1 \quad \iff \quad s_1 = \frac{t}{h + 2v_1} \bmod u_1.$$

Réduction : après l'addition et la duplication, nous devons réduire les polynômes u et v sur le corps $\Bbbk(C)$. Suivant l'algorithme de Cantor, la propriété que nous utilisons est que le polynôme u divise $f - vh - v^2$. Comme $v = s_1u_1 + v_1$, alors

$$\frac{f - vh - v^2}{u_1} = \frac{f - v_1h - v_1^2}{u_1} - s_1(h + s_1u_1 + 2v_1).$$

On connaît la fraction exacte $t = (f - v_1h - v_1^2)/u_1$ et pour avoir la réduction du polynôme u on divise simplement par u_2, ce qui nous donne la fraction exacte suivante :

$$u' = \frac{f - vh - v^2}{u} = \frac{t - s_1(h + s_1u_1 + 2v_1)}{u_2}.$$

Il ne reste qu'à rendre u' unitaire et à calculer $v' = -(h + su_1 + v_1) \bmod u'$ pour avoir le résultat $D = [u', v'] = D_1 + D_2$.

Algorithme. Nous présentons ici un algorithme, en genre 2, résultant des considérations précédentes que nous modifions légèrement afin qu'il résiste aux attaques par canaux auxiliaires. L'idée est d'obtenir une formule unifiée pour l'addition et la duplication afin de les rendre indistinguables pour un observateur ayant par exemple accès à des traces de consommation de courant du processeur. Notons que Lange et Mishra [LM05], en supposant que le coût d'une multiplication et d'un carré sur le corps fini $\mathbb{k}$ sont les mêmes, ont déjà proposé des formules unifiées. Notre algorithme ne prétend pas être le plus efficace ni le plus résistant aux attaques par canaux auxiliaires, mais il illustre une technique classique de protection et le genre d'idée que doit avoir en tête un ingénieur qui souhaite implémenter soigneusement une arithmétique utilisable pour faire de la cryptographie.

Algorithm 3.3.1 Arithmétique en genre 2

`Entrée` : Les diviseurs $D_1 = (u_1, v_1)$ et $D_2 = (u_2, v_2)$
`Sortie` : Le diviseur $D = D_1 + D_2 = (u', v')$

1: $t_1 \leftarrow (f - v_1 h - v_1^2)/u_1$ et $t_2 \leftarrow t_1 \bmod u_2$
2: **si** $D_1 = D_2$ **alors** $s_1 \leftarrow t_2/(h + 2v_2) \bmod u_2$
3: **sinon** $s_1 \leftarrow (v_2 - v_1)/u_1 \bmod u_2$ **fin si**
4: $u' \leftarrow [t_1 - s_1(h + s_1 u_1 + 2v_1)]/(u_2)$
5: $v' \leftarrow -(h + s_1 u_1 + v_1) \bmod u'$
6: **retourner** $D = (u', v')$

Dans l'algorithme 3.3.1, le calcul de t_2 à la première ligne est indispensable pour que l'addition et la duplication soient indistinguables. Dans ce cas, les calculs effectués après **si** et **sinon** ont le même coût. Notons par $\mathbf{M_K}, \mathbf{S_K}$ et $\mathbf{I_K}$ les complexités respectives pour calculer une multiplication, un carré et une inversion dans une extension finie $K/\mathbb{k}$ de $\mathbb{k}$. Nous explicitons l'algorithme 3.3.1 pour des diviseurs définis dans K.

`Entrée` : Deux diviseurs $D_1 = (u_1, v_2)$, $D_2 = (u_2, v_2)$ avec $\deg(u_1) = \deg(u_2) = 2$
`Sortie` : Le diviseur somme $D = (u', v') = D_1 + D_2$

1. **Calculer** $\mathbf{t_1} := (\mathbf{f - v_1 h - v_1^2})/\mathbf{u_1} := \mathbf{x^3 + t_{12} x^2 + t_{11} x + t_{10}}$ $[\mathbf{3M_K + 1S_K}]$
   $t_{12} \leftarrow f_4 - u_{11}$; $w_1 \leftarrow u_{11} t_{21} + h_2 v_{11}$; $t_{11} \leftarrow f_3 - u_{10} - w_1$;
   $t_{10} \leftarrow u_{11}(u_{10} - t_{11}) - f_4 u_{10} - v_{11}(h_1 + v_{11}) - h_2 v_{10} + f_2$;
2. **Calculer** $\mathbf{t_2} := \mathbf{t_1} \bmod \mathbf{u_2} := \mathbf{t_{21} x + t_{20}}$ $[\mathbf{2M_K}]$
   $t_{21} \leftarrow u_{21}(u_{21} - t_{12}) + t_{11} - u_{20}$;
   $t_{20} \leftarrow u_{20}(u_{21} - t_{12}) + t_{10}$;
   si $D_1 = D_2$ **alors**
   $F_{11} \leftarrow t_{21}; F_{10} \leftarrow t_{20}; F_{21} \leftarrow (h_1 - h_2 u_{21} + 2v_{21}); F_{20} \leftarrow (h_0 - h_2 u_{20} + 2v_{20})$;
   sinon $F_{11} \leftarrow v_{21} - v_{11}; F_{10} \leftarrow v_{20} - v_{10}; F_{21} \leftarrow u_{11} - u_{21}; F_{20} \leftarrow u_{10} - u_{20}$;
   fin si
3. **Calculer** $\mathbf{s_2} := \mathrm{Monic}(\mathbf{F_1}/\mathbf{F_2} \bmod \mathbf{u_2}) := \mathbf{x + x_{20}}$ $[\mathbf{12M_K + 4S_K + 1I_K}]$
   $w_1 \leftarrow F_{20} - u_{21} F_{21}$; $r \leftarrow F_{20} w_1 + u_{20} F_{21}^2$;
   $s_{10} \leftarrow F_{10} w_1 + u_{20} F_{11} F_{21}$; $s_{11} \leftarrow F_{11} F_{20} - F_{21} F_{10}$;
   $w_1 \leftarrow 1/(r s_{11})$; $w_2 \leftarrow r^2 w_1$; $w_3 \leftarrow w_1 s_{11}^2$; $w_4 \leftarrow w_2^2$; $s_{20} \leftarrow s_{10} w_2$

4. **Calculer** $\ell := \mathbf{s_2 u_1} := \mathbf{x^3} + \ell_\mathbf{2}\mathbf{x^2} + \ell_\mathbf{1}\mathbf{x} + \ell_\mathbf{0}$ $[\mathbf{2M_K}]$
   $\ell_2 \leftarrow u_{11} + s_{20}$; $\ell_1 \leftarrow u_{10} + u_{11}s_{20}$; $\ell_0 \leftarrow u_{10}s_{20}$;
5. **Calculer** $\mathbf{u'} := (\mathbf{t_1} - \mathbf{s_1}(\mathbf{h} + \mathbf{v} + \mathbf{v_1}))/\mathbf{u_2} := \mathbf{x^2} + \mathbf{u'}_\mathbf{1}\mathbf{x} + \mathbf{u'}_\mathbf{0}$; $[\mathbf{3M_K}]$
   $z_1 \leftarrow u_{11} - u_{21}$; $u'_1 \leftarrow 2s_{20} + z_1 + h_2w_2 - w_4$;
   $u'_0 \leftarrow (s_{20} - u_{21})(s_{20} + z_1 + h_2w_2) - u_{20} + \ell_1$;
   $u'_0 \leftarrow u'_0 + (h_1 + 2v_{11})w_2 + (2u_{11} - z_1 - f_4)w_4$;
6. **Calculer** $\mathbf{v'} := -(\mathbf{h} + \ell + \mathbf{v}) \bmod \mathbf{u'} := \mathbf{v'}_\mathbf{1}\mathbf{x} + \mathbf{v'}_\mathbf{0}$ $[\mathbf{4M_K}]$
   $w_1 \leftarrow \ell_2 - u'_1$; $w_2 \leftarrow u'_1w_1 + u'_0 - \ell_1$;
   $v'_1 \leftarrow w_2w_3 - v_{11} - h_1 + h_2u'_1$; $w_2 \leftarrow u'_0w_1 - \ell_0$;
   $v'_0 \leftarrow w_2w_3 - v_{10} - h_0 + h_2u'_0$;
7. **retourner** $\mathbf{D} = [\mathbf{u'}, \mathbf{v'}]$ $[\mathbf{Total} : \mathbf{26M_K} + \mathbf{5S_K} + \mathbf{1I_K}]$

Bien que nos formules soient valables en toute caractéristique, nous avons indiqué seulement la complexité pour le cas de la caractéristique impaire où $h(x) = 0$.

3.4 Quelques remarques pour finir

Comme dans le cas des courbes elliptiques, notons qu'il existe des formules explicites pour d'autres systèmes de coordonnées que les coordonnées de Mumford, notamment les coordonnées projectives (voir [MDM+02, Lan02b] ou [ACD+06, section 14.4.1]) et les coordonnées Jacobiennes (voir [Lan02c] ou [ACD+06, section 14.4.2]). Ces systèmes de coordonnées permettent d'éliminer les calculs d'inversion présents dans le cas affine.

En coordonnées projectives, un diviseur réduit $D = (u, v)$ d'une jacobienne de genre 2 est représenté par un 5-uplet de la forme $(U_1, U_0, V_1, V_0, Z_1)$ tel que

$$u = x^2 + \frac{U_1}{Z_1}x + \frac{U_0}{Z_1} \quad \text{et} \quad v = \frac{V_1}{Z_1}x + \frac{V_0}{Z_1}.$$

En coordonnées Jacobiennes, un diviseur réduit $D = (u, v)$ d'une jacobienne de genre 2 est représenté par un 6-uplet de la forme $(U_1, U_0, V_1, V_0, Z_1, Z_2)$ tel que

$$u = x^2 + \frac{U_1}{Z_1^2}x + \frac{U_0}{Z_1^2} \quad \text{et} \quad v = \frac{V_1}{Z_1^3Z_2}x + \frac{V_0}{Z_1^3Z_2}.$$

Il existe des adaptations de l'algorithme de Cantor pour calculer avec les précédents systèmes de coordonnées.

Changement de modèle. D'autres techniques pour rendre efficace l'arithmétique sur une courbe hyperellitique de genre ≤ 2 utilisent un changement judicieux de modèle de la courbe. Pour le cas elliptique, nous avons les modèles d'Edwards [Edw07], de Jacobi [BJ03, FNW09], Hessien [Sma01a] (pour plus de détails voir [HWCD07]). Ces différents modèles sont des cas particuliers, fréquemment rencontrés, du modèle de Weierstraβ. En effet, pour une courbe elliptique E définie sur $\Bbbk$, le modèle d'Edwards suppose que $E(\Bbbk)$ admet un point de 4 torsion rationnel, le modèle de Jacobi suppose que $E(\Bbbk)$ admet un point de 2 torsion rationnel et le modèle de Hessian suppose que $E(\Bbbk)$ admet un point de 3 torsion rationnel. Pour le cas du genre 2, il existe une arithmétique efficace sur les surfaces de Kummer [Duq07, Duq08b, Gau07, GL08] qui étend dans le cas du genre 2 le classique algorithme de Montgomery.

Deuxième partie

Implémentation efficace des couplages en genre 2

Chapitre 4

Généralités sur les couplages

Un couplage est une application $c : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ de deux groupes (notés additivement) $\mathbb{G}_1, \mathbb{G}_2$ vers un groupe (noté multiplicativement) $\mathbb{G}_T$ qui est bilinéaire et non dégénérée :

$$\text{a)} \quad \textbf{bilinéaire} \quad \begin{cases} c(P_1 + P_2, Q) = c(P_1, Q)c(P_2, Q), \\ c(P, Q_1 + Q_2) = c(P, Q_1)c(P, Q_2), \end{cases}$$

$$\text{b)} \quad \textbf{non dégénérée} \quad \begin{cases} \forall\, P \in \mathbb{G}_1, \exists\, Y \in \mathbb{G}_2, c(P, Y) \neq 1, \\ \forall\, Q \in \mathbb{G}_2, \exists\, X \in \mathbb{G}_1, c(X, Q) \neq 1. \end{cases}$$

Par la suite, les groupes $\mathbb{G}_1$ et $\mathbb{G}_2$ seront des sous-groupes cycliques de points rationnels d'une jacobienne de courbe hyperelliptique définie sur le corps $\Bbbk$ de genre $g \leq 2$ tels que $\mathbb{G}_1 \cap \mathbb{G}_2 = \{0\}$ où 0 est l'élément neutre de la jacobienne.

Nous ne considérons que les couplages de *Tate*, de *Weil* et leurs améliorations cryptographiques, notamment les couplages *Eta* et *Ate*. L'objectif principal de cette partie est de décrire et de comparer diverses implémentations de calcul de couplages. Pour ces implémentations, nous utilisons le logiciel de calcul algébrique Magma [BCP97].

4.1 Définition des couplages de Weil et de Tate

Soit C une courbe hyperelliptique de genre g définie sur $\Bbbk$ et soit J_C sa jacobienne. Soit r un entier strictement positif. Si D est un diviseur réduit de C qui représente un élément de $J_C[r]$ alors on note f_D la fonction de C définie à un facteur multiplicatif près par $rD = (f_D)$. On note μ_r le sous-groupe de $\overline{\Bbbk}^*$ des racines $r^{\text{ièmes}}$ de l'unité et pour simplifier, nous supposons que μ_r est inclus dans une extension finie K de $\Bbbk$. On a alors la définition suivante :

Définition 4.1 Avec les notations précédentes, le couplage de Weil est l'application :

$$\begin{aligned} W_r : J_C[r] \times J_C[r] &\to \mu_r \subset K^* \\ (D_1, D_2) &\mapsto W_r(D_1, D_2) := \frac{f_{D_1}(D_2)}{f_{D_2}(D_1)}, \end{aligned}$$

où D_1 et D_2 sont des diviseurs réduits de supports disjoints.

On peut montrer que le couplage de Weil est une application bilinéaire non dégénérée.

Le couplage de Tate fut introduit par Tate [Tat95] sur les variétés abéliennes, puis Lichtenbaum [Lic69] l'applique pour des jacobiennes de courbes hyperelliptiques sur $\mathbb{C}$ et Frey et Rück [FR94] le définissent sur les corps finis.

Définition 4.2 En conservant les notations précédentes, le couplage de Tate est donné par l'application suivante :

$$\begin{array}{rccc} T_r : J_C(\Bbbk)\,[r] \times \dfrac{J_C(K)}{rJ_C(K)} & \to & \dfrac{K^*}{K^{*r}} \\ (D_1, D_2) & \mapsto & T_r(D_1, D_2) := f_{D_1}(D_2), \end{array}$$

où D_1 et D_2 sont des diviseurs réduits de supports disjoints.

Là encore, on peut montrer que le couplage de Tate est une application bilinéaire et qu'elle est non dégénérée si $J_C(K)$ ne contient pas un point de r^2-torsion.

Tous les algorithmes de calcul de couplage connus reposent sur l'algorithme de Miller [Mil86, Mil04] qui permet de calculer les fonctions f_D précédentes qui apparaissent dans la définition des couplages de Weil et Tate et de les évaluer en un diviseur D'.

4.2 L'algorithme de Miller

Dans cette section, nous décrivons les briques algorithmiques élémentaires sous-jacentes à tous les algorithmes de calcul de couplage. L'algorithme de Miller repose sur le principe de l'algorithme d'exponentiation rapide appliqué à des fonctions dites de Weil (voir la section 4.2.2).

4.2.1 Fonction de Miller

Dans un premier temps, nous nous intéressons au problème algorithmique suivant : étant donné deux diviseurs réduits D_1 et D_2 représentant des points de la jacobienne J_C, peut-on efficacement calculer une fonction h_{D_1,D_2} (dépendant de D_1 et D_2) telle que $\mathrm{div}(h_{D_1,D_2}) = D_1 + D_2 - \rho(D_s)$, avec $\rho(D_s)$ l'unique diviseur réduit équivalent à $D_s := D_1 + D_2$? La fonction h_{D_1,D_2}, déterminée à une constante multiplicative prés, est appelée fonction de Miller associée à D_1 et D_2.

Remarque 4.3 Pour le cas d'une courbe elliptique $E/\Bbbk$, la fonction de Miller est facile à obtenir : soient P_1 et P_2 deux points de E, on sait que $(P_1) + (P_2) + (h) = (P_1 + P_2)$ où $h_{P_1,P_2} = \frac{\ell_{P_1,P_2}}{v_{P_1,P_2}}$ est le rapport des fonctions qui s'annulent respectivement sur la droite ℓ_{P_1,P_2} passant par P_1 et P_2 et la droite verticale v_{P_1,P_2} passant par $P_1 + P_2$.

Dans le cas des courbes hyperelliptiques de genre plus grand que 1, nous allons voir que la fonction h_{D_1,D_2} peut se déterminer grâce à l'algorithme de Cantor.

4.2.2 Fonction de Weil

Pour tout diviseur $D \in Div_C^0$, notons toujours par $\rho(D)$ l'unique diviseur réduit équivalent à D.

Définition 4.4 Soient $n \in \mathbb{Z}$ et $D \in Div_C^0$ un diviseur réduit représentant un élément de $J_C(\overline{\Bbbk})$. On appelle fonction de Weil, toute fonction $f \in \overline{\Bbbk}(C)$ dont le diviseur vérifie

$$(f) = [n]\,D - \rho([n]\,D),$$

où $\rho([n]\,D)$ est l'unique diviseur réduit de $[n]\,D$. Cette fonction dépendant de n et de D sera notée $f_{n,D}$. Dans le cas d'une courbe elliptique, on écrit la fonction $f_{n,P}$ pour un point P de la courbe et on a : $(f_{n,P}) = n(P) - ([n]\,P) - (n-1)(O)$.

Notons que les fonctions de Weil sont déterminées à une constante près. Le lien entre les fonctions de Weil et le couplage de Weil est le suivant : si D représente un élément de $J_C[n]$ alors $f_{n,D}$ n'est autre que la fonction f_D qui est utilisée dans les définitions des couplages de Weil définition 4.1 et de Tate définition 4.2.

Le théorème suivant résume les principales propriétés des fonctions de Weil. On notera en particulier la première équation d'où découle immédiatement un algorithme de type exponentiation rapide pour calculer les couplages.

Théorème 4.5 *Soient des entiers n, $m \in \mathbb{Z}$ et un diviseur réduit $D \in Div_C^0$, alors, à un coefficient multiplicatif près, on a :*

$$\begin{aligned} f_{n+m,D} &= f_{n,D}.f_{m,D}.h_{\rho([n]D),\rho([m]D)}, && (4.1)\\ f_{mn,D} &= f_{m,D}^n.f_{n,\rho([m]D)} = f_{n,D}^m.f_{m,\rho([n]D)}, && (4.2)\\ f_{-n,D} &= \frac{1}{f_{n,D}h_{\rho([n]D),\rho([-n]D)}}. && (4.3) \end{aligned}$$

Preuve : Pour la première formule (4.1) (formule de l'addition), on a :

$$\begin{aligned} \mathrm{div}(f_{n,D}.f_{m,D}.h_{\rho([n]D),\rho([m]D)}) &= \mathrm{div}(f_{n,D}) + \mathrm{div}(f_{m,D}) + \mathrm{div}(h_{\rho([n]D),\rho([m]D)})\\ &= [n]\,D - \rho([n]\,D) + [m]\,D - \rho([m]\,D) + \rho([n]\,D)\\ &\quad +\rho([m]\,D) - \rho([n+m]\,D)\\ &= [n+m]\,D - \rho([n+m]\,D)\\ &= \mathrm{div}(f_{m+n,D}). \end{aligned}$$

Pour la seconde formule (4.2) (formule du produit), on a :

$$\begin{aligned} \mathrm{div}(f_{m,D}^n.f_{n,\rho([m]D)}) &= n.\mathrm{div}(f_{m,D}) + \mathrm{div}(f_{n,\rho([m]D)})\\ &= n\,([m]\,D - \rho([m]\,D)) + n(\rho([m]\,D)) - \rho(n\,[m]\,D)\\ &= [nm]\,D - \rho([nm]\,D)\\ &= \mathrm{div}(f_{mn,D}). \end{aligned}$$

Pour la dernière formule (4.3) (formule de l'opposée), on a :

$$\begin{aligned} \mathrm{div}(f_{n,D}.h_{[n]D,[-n]D}) &= \mathrm{div}(f_{n,D}) + \mathrm{div}(h_{\rho([n]D),\rho(-[n]D)})\\ &= [n]\,D - \rho([n]\,D) + \rho([n]\,D) + \rho([-n]\,D)\\ &= [n]\,D + \rho(-\,[n]\,D)\\ &= -\,([-n]\,D - \rho([-n]\,D))\\ &= -\mathrm{div}(f_{-n,D}). \end{aligned}$$

□

En prenant des valeurs particulières pour m et n dans les formules d'addition et de produit, nous avons le corollaire suivant :

Corollaire 4.6 *Pour tout entier $n \in \mathbb{Z}$ et tout diviseur $D \in J_C$, on a :*

$$\begin{aligned} f_{n+1,D} &= f_{n,D}.h_{\rho([n]D),D}, && (4.4)\\ f_{n^2,D} &= f_{n,D}^n.f_{n,\rho([n]D)}. && (4.5) \end{aligned}$$

Remarque 4.7 Il est facile de voir que $f_{0,D} = f_{1,D} = 1$ pour tout diviseur D et nous allons supposer que $f_{n,0} = 1$ pour tout entier n où 0 est le diviseur nul.

On peut généraliser le corollaire précédent avec les formules suivantes :

Corollaire 4.8 *Pour tous entiers $n \in \mathbb{Z}$, $\ell \in \mathbb{N}$, toute famille d'entier $(n_i)_{0\leq i\leq \ell}$ et pour tout diviseur réduit $D \in Div_C^0$, on a :*

$$f_{n^\ell,D} = \prod_{i=0}^{\ell-1} f_{n,\rho([n^i]D)}^{n^{\ell-1-i}}, \tag{4.6}$$

$$f_{\sum_{i=0}^{\ell} n_i,D} = \prod_{i=0}^{\ell} f_{n_i,D} \prod_{i=0}^{\ell-1} h_{\rho(\sum_{j=0}^{i}[n_j]D),\rho([n_{i+1}]D)}, \tag{4.7}$$

$$\prod_{i=0}^{\ell-1} h_{\rho(\sum_{j=0}^{i}[n_j]D),\rho([n_{i+1}]D)} = \prod_{i=0}^{\ell-1} h_{\rho(\sum_{j=i+1}^{\ell}[n_j]D),\rho([n_i]D)}. \tag{4.8}$$

Preuve : Toutes les formules se prouvent par récurrence suivant l'entier ℓ. Pour la formule de la puissance (4.6), on vérifie qu'elle est vraie pour $\ell = 1$. Supposons qu'elle soit vraie jusqu'à ℓ, établissons alors qu'elle est vraie jusqu'à $\ell + 1$. On a :

$$\begin{aligned}
f_{n^{\ell+1},D} &= f_{n^\ell.n,D} \\
&= f_{n^\ell,D}^n . f_{n,\rho([n^\ell]D)} \\
&= \left(\prod_{i=0}^{\ell-1} f_{n,\rho([n^i]D)}^{n^{\ell-1-i}}\right)^n . f_{n,\rho([n^\ell]D)} \\
&= \left(\prod_{i=0}^{\ell-1} f_{n,\rho([n^i]D)}^{n^{\ell-i}}\right) . f_{n,\rho([n^\ell]D)} \\
&= \prod_{i=0}^{\ell} f_{n,\rho([n^i]D)}^{n^{\ell-i}}.
\end{aligned}$$

Pour la relation (4.7), on voit qu'elle est valable pour $\ell = 1, 2$, en effet, pour $\ell = 1$, on a la formule suivante :

$$f_{n_.+n_1,D} = \prod_{i=0}^{1} f_{n_i,D} \prod_{i=0}^{0} h_{\rho([n_0]D),\rho([n_1]D)}.$$

Supposons que la formule (4.7) soit vraie jusqu'à ℓ. Pour $\ell + 1$, on a :

$$\begin{aligned}
f_{\sum_{i=0}^{\ell+1} n_i,D} &= f_{\sum_{i=0}^{\ell} n_i + n_{\ell+1},D} \\
&= f_{\sum_{i=0}^{\ell} n_i,D} . f_{n_{\ell+1},D} . h_{\rho(\sum_{i=0}^{\ell}[n_i]D),\rho([n_{\ell+1}]D)} \\
&= \left(\prod_{i=0}^{\ell} f_{n_i,D} \prod_{i=0}^{\ell-1} h_{\rho(\sum_{j=0}^{i} n_j D),\rho([n_{i+1}]D)}\right) . f_{n_{\ell+1},D} . h_{\rho(\sum_{i=0}^{l}[n_i]D),\rho([n_{\ell+1}]D)} \\
&= \prod_{i=0}^{\ell+1} f_{n_i,D} . \left(\prod_{i=0}^{\ell-1} h_{\rho(\sum_{j=0}^{i}[n_j]D),\rho([n_{i+1}]D)}\right) . h_{\rho(\sum_{i=0}^{\ell}[n_i]D),\rho([n_{\ell+1}]D)} \\
&= \prod_{i=0}^{\ell+1} f_{n_i,D} \prod_{i=0}^{\ell} h_{\rho(\sum_{j=0}^{i}[n_j]D),\rho([n_{i+1}]D)}.
\end{aligned}$$

Pour la dernière formule (4.8), il suffit de montrer par récurrence que

$$f_{\sum_{i=0}^{\ell} n_i,D} = \prod_{i=0}^{\ell} f_{n_i,D} \prod_{i=0}^{\ell-1} h_{\rho(\sum_{j=i+1}^{\ell}[n_j]D),\rho([n_i]D)}, \tag{4.9}$$

et de conclure avec la formule (4.7). En fait, on vérifie que la relation (4.9) est vrai pour $\ell = 0, 1$ et 2. Supposons que la relation (4.9) soit vraie jusqu'à ℓ et montrons qu'elle est vraie pour $\ell + 1$. On a :

$$\begin{aligned}
f_{\sum_{i=0}^{\ell+1} n_i, D} &= f_{n_0 + \sum_{i=1}^{\ell+1} n_i, D} \\
&= f_{n_0,D} . f_{\sum_{i=1}^{\ell+1} n_i, D} . h_{\rho(\sum_{i=1}^{\ell+1}[n_i]D), \rho([n_0]D)} \\
&= f_{n_0,D} . h_{\rho(\sum_{i=1}^{\ell+1}[n_i]D), \rho([n_0]D)} \cdot \left(\prod_{i=1}^{\ell+1} f_{n_i,D} \prod_{i=1}^{\ell} h_{\rho(\sum_{j=i+1}^{\ell+1} n_j D), \rho([n_i]D)} \right) \\
&= \prod_{i=0}^{\ell+1} f_{n_i,D} \cdot \left(\prod_{i=0}^{\ell-1} h_{\rho(\sum_{j=i+1}^{\ell+1}[n_j]D), \rho([n_i]D)} \right) . h_{\rho(\sum_{i=1}^{\ell+1}[n_i]D), \rho([n_0]D)} \\
&= \prod_{i=0}^{\ell+1} f_{n_i,D} \prod_{i=0}^{\ell} h_{\rho(\sum_{j=i+1}^{\ell+1}[n_j]D), \rho([n_i]D)} .
\end{aligned}$$

En écrivant l'égalité entre les formules (4.7) et (4.9), on prouve la relation (4.8). On peut aussi prouver (4.8) directement en utilisant les diviseurs des fonctions. □

Remarque 4.9 Dans [Ver08] Vercauteren utilise la formule (4.9) pour son couplage optimal dans le cas elliptique.

4.2.3 Evaluation d'une fonction en un diviseur

Des formules de la section précédente, nous déduisons immédiatement un algorithme permettant de calculer les fonctions qui apparaissent dans la définition des couplages. En fait, pour calculer les couplages, il faut savoir évaluer efficacement les fonctions de Weil en un diviseur ce qui est l'objet de cette section.

Cas du genre quelconque :

Définition 4.10 Soient $f \in \Bbbk(C)$ une fonction et $D = \sum_{P \in C} n_P(P) \in Div_C$ un diviseur tels que $\mathrm{supp}(D) \cap \mathrm{supp}(\mathrm{div}(f)) = \emptyset$. On a par définition :

$$f(D) := \prod_{P \in C} f(P)^{n_P}. \tag{4.10}$$

Remarquons que si le diviseur D est de degré zéro, alors $f(D)$ dépend seulement de $\mathrm{div}(f)$ et non de f. En effet, si $f_1 = \lambda f_2$ avec λ une constante, alors pour tout diviseur $D = \sum_i n_i(P_i)$ de degré zéro, on a :

$$f_1(D) := \prod_i f_1^{n_i}(P_i) = \prod_i (\lambda f_2)^{n_i}(P_i) = \prod_i \lambda^{n_i} f_2^{n_i}(P_i) = \prod_i f_2^{n_i}(P_i) = f_2(D).$$

La formule (4.10) de calcul de l'évaluation de la fonction f au diviseur D ne donne pas un algorithme optimal. Pour l'optimiser, on peut utiliser le lemme suivant :

Lemme 4.11 *Soit $f(x, y) \in \Bbbk[x, y]$ un polynôme, alors pour $D = (u, v) \in Div_C^0$, on a :*

$$f(D) = \text{Résultant}\Big(u(x), f(x, v(x))\Big) = \text{Résultant}\Big(u(x), f(x, v(x)) \bmod u(x)\Big).$$

Preuve : Ce résultat est immédiat avec [Cos09, théorème 5]. □

Alors pour calculer l'évaluation de $f = f_1/f_2 \in K(C)$ en $D = (u, v) \in Div_C^0$, on peut utiliser la formule :

$$f(D) = \frac{\text{Résultant}(u(x), \overline{f}_1(x))}{\text{Résultant}(u(x), \overline{f}_2(x))},$$

avec pour $i = 1, 2$ $\overline{f}_i(x) = f_i(x, v(x)) \bmod u(x)$. Pour normaliser, on divise par $\lambda^{\deg(u)}$, où λ est le coefficient dominant de f.

Cas du genre $g \leq 2$

Dans le cas du genre 1, les polynômes $f_i(x, v(x))$ intervenant dans les fonctions de Miller sont de degré 1, de même que le polynôme u et l'évaluation ne pose aucun problème particulier. Le genre 2 est plus intéressant. Dans ce cas, les polynômes $f_i(x, v(x))$ déduits des fonctions de Miller sont de degré 3 et le polynôme unitaire u est de degré 2. Alors, il nous suffit de donner le résultant de $u = x^2 + \mu_1 x + \mu_0 \in K[x]$ et d'un polynôme $H = \alpha_3 x^3 + \alpha_2 x^2 + \alpha_1 x + \alpha_0 \in K[x]$. Le calcul de $H \mod u$ est donné par :

$$\alpha_3 x^3 + \alpha_2 x^2 + \alpha_1 x + \alpha_0 \equiv \beta_1 x + \beta_0 \ \left[\bmod x^2 + \mu_1 x + \mu_0\right],$$

avec $\beta_1 = \alpha_1 + \mu_1\alpha_3 + \mathtt{c}\mu_0 - (\mu_1 + \mu_0)(\alpha_3 + \mathtt{c})$, $\beta_0 = \alpha_0 - \mathtt{c}\mu_0$, et $\mathtt{c} := \alpha_2 - \mu_1\alpha_3$. Par suite, on calcule le résultant de u et H avec la formule :

$$\text{Résultant}(u, H) = \beta_0(\beta_0 - \mu_1\beta_1) + \mu_0\beta_1^2.$$

Au total, ce calcul nécessite 6 multiplications et 1 carré dans K.

4.2.4 Evaluation explicite de la fonction de Weil-Miller

Soit $C/\Bbbk$ une courbe hyperelliptique de genre 2 et soient K et L deux extensions finies de $\Bbbk$ (pour calculer le couplage l'un des corps K et L est égal à $\Bbbk$). Notons par M_K, S_K, I_K respectivement le coût de la multiplication, du carré et de l'inversion dans K et par M_L, S_L, I_L les coûts correspondants pour le corps L. Soient $D_1 = (u_1, v_1)$ et $D_2 = (u_2, v_2)$ deux diviseurs rationnels sur K et $D = (u_D, v_D)$ un diviseur rationnel sur L tels que $\deg(u_1) = \deg(u_2) = \deg(u_D) = 2$ et soit $u_1 = u_2$ ou bien soit $\gcd(u_1, u_2) = 1$.

L'algorithme suivant permet de calculer le diviseur réduit $D' = D_1 + D_2$ et l'évaluation de la fonction de Weil-Miller h_{D_1,D_2} en D.

---

1. **Calculer $\mathbf{t_1} := (\mathbf{f} - \mathbf{v_1 h} - \mathbf{v_1^2})/\mathbf{u_1} := \mathbf{x^3} + \mathbf{t_{12}x^2} + \mathbf{t_{11}x} + \mathbf{t_{10}}$** $[\mathbf{3M_K} + \mathbf{1S_K}]$
   $t_{12} \leftarrow f_4 - u_{11}$; $w_1 \leftarrow u_{11}t_{21} + h_2v_{11}$; $t_{11} \leftarrow f_3 - u_{10} - w_1$;
   $t_{10} \leftarrow u_{11}(u_{10} - t_{11}) - f_4u_{10} - v_{11}(h_1 + v_{11}) - h_2v_{10} + f_2$;
2. **Calculer $\mathbf{t_2} := \mathbf{t_1} \bmod \mathbf{u_2} := \mathbf{t_{21}x} + \mathbf{t_{20}}$** $[\mathbf{2M_K}]$
   $t_{21} \leftarrow u_{21}(u_{21} - t_{12}) + t_{11} - u_{20}$; $t_{20} \leftarrow u_{20}(u_{21} - t_{12}) + t_{10}$;
   si $D_1 = D_2$ **alors**
   $F_{11} \leftarrow t_{21}; F_{10} \leftarrow t_{20}; F_{21} \leftarrow (h_1 - h_2u_{21} + 2v_{21}); F_{20} \leftarrow (h_0 - h_2u_{20} + 2v_{20})$;
   sinon $F_{11} \leftarrow v_{21} - v_{11}; F_{10} \leftarrow v_{20} - v_{10}; F_{21} \leftarrow u_{11} - u_{21}; F_{20} \leftarrow u_{10} - u_{20}$;
3. **Calculer $\mathbf{s_2} := \text{Monic}(\mathbf{F_1}/\mathbf{F_2} \bmod \mathbf{u_2}) := \mathbf{x} + \mathbf{s_{20}}$** $[\mathbf{12M_K} + \mathbf{4S_K} + \mathbf{1I_K}]$
   $w_1 \leftarrow F_{20} - u_{21}F_{21}$; $r \leftarrow F_{20}w_1 + u_{20}F_{21}^2$;

$s_{10} \leftarrow F_{10}w_1 + u_{20}F_{11}F_{21}$; $s_{11} \leftarrow F_{11}F_{20} - F_{21}F_{10}$;
$w_1 \leftarrow 1/(rs_{11})$; $w_2 \leftarrow r^2 w_1$; $w_3 \leftarrow w_1 s_{11}^2$; $w_4 \leftarrow w_2^2$; $s_{20} \leftarrow s_{10}w_2$

4. **Calculer** $\ell := \mathbf{s_2 u_1} := \mathbf{x^3} + \ell_\mathbf{2}\mathbf{x^2} + \ell_\mathbf{1}\mathbf{x} + \ell_\mathbf{0}$ $[\mathbf{2M_K}]$
   $\ell_2 \leftarrow u_{11} + s_{20}$; $\ell_1 \leftarrow u_{10} + u_{11}s_{20}$; $\ell_0 \leftarrow u_{10}s_{20}$;
5. **Calculer** $\mathbf{u'} := (\mathbf{t_1} - \mathbf{s_1}(\mathbf{h} + \mathbf{v} + \mathbf{v_1}))/\mathbf{u_2} := \mathbf{x^2} + \mathbf{u'_1 x} + \mathbf{u'_0}$; $[\mathbf{3M_K}]$
   $z_1 \leftarrow u_{11} - u_{21}$; $u'_1 \leftarrow 2s_{20} + z_1 + h_2 w_2 - w_4$;
   $u'_0 \leftarrow (s_{20} - u_{21})(s_{20} + z_1 + h_2 w_2) - u_{20} + \ell_1$;
   $u'_0 \leftarrow u'_0 + (h_1 + 2v_{11})w_2 + (2u_{11} - z_1 - f_4)w_4$;
6. **Calculer** $\mathbf{H_1} := \mathbf{Resultant}(\mathbf{u_D}, (\mathbf{v_D} - \mathbf{v}) \bmod \mathbf{u_D})$ $[\mathbf{3M_K} + \mathbf{6M_L} + \mathbf{1S_L}]$
   $z_0 \leftarrow v_{D0} - w_3\ell_0 - v_{10}$; $z_1 \leftarrow v_{D1} - w_3\ell_1 - v_{11}$; $z_2 \leftarrow -w_3\ell_2$; $z_4 \leftarrow z_2 + w_3 u_{D1}$;
   $\alpha_0 \leftarrow z_0 - z_4 u_{D0}$; $\alpha_1 \leftarrow z_1 - w_3 u_{D1} + z_4 u_{D0} - (u_{D1} + u_{D0})(z_4 - w_3)$
   $H_1 \leftarrow \alpha_0(\alpha_0 - \alpha_1 u_{D1}) + \alpha_1^2 u_{D0}$
7. **Calculer** $\mathbf{H_2} \leftarrow \mathbf{Resultant}(\mathbf{u_D}, \mathbf{u'} \bmod \mathbf{u_D})$ $[\mathbf{3M_L} + \mathbf{1S_L}]$
   $\beta_0 \leftarrow u'_0 - u_{D0}$; $\beta_1 \leftarrow u'_1 - u_{D1}$; $\beta_2 \leftarrow \beta_0 - \beta_1 u_{D1}$; $H_2 \leftarrow \beta_0\beta_2 + \beta_1^2 u_{D0}$;
8. **Calculer** $\mathbf{v'} := -(\mathbf{h} + \mathbf{v}) \bmod \mathbf{u'} := \mathbf{v'_1 x} + \mathbf{v'_0}$ $[\mathbf{4M_K}]$
   $w_1 \leftarrow \ell_2 - u'_1$; $w_2 \leftarrow u'_1 w_1 + u'_0 - \ell_1$; $v'_1 \leftarrow w_2 w_3 - v_{11} - h_1 + h_2 u'_1$;
   $w_2 \leftarrow u'_0 w_1 - \ell_0$; $v'_0 \leftarrow w_2 w_3 - v_{10} - h_0 + h_2 u'_0$;
9. **retourner** $\mathbf{D'} = [\mathbf{u'}, \mathbf{v'}]$ et $(\mathbf{H_1}, \mathbf{H_2}, \mathbf{w_3})$
   $[\mathbf{Total} : \mathbf{29M_K} + \mathbf{5S_K} + \mathbf{1I_K} + \mathbf{9M_L} + \mathbf{2S_L}]$

4.3 Application au calcul de couplages

Nous reprenons tous les résultats des précédentes sections pour donner l'algorithme de Miller dans le cas d'une courbe hyperelliptique. Considérons le couplage sur une courbe hyperelliptique $c : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ avec $\mathbb{G}_1$ et $\mathbb{G}_2$ des groupes cycliques de même ordre r. Soit D_1 un générateur de $\mathbb{G}_1$ et D_2 un élément de $\mathbb{G}_2$, alors l'algorithme de Miller est tout simplement un algorithme de "square-and-multiplied" (ou de "double and add") de la loi de groupe suivante :

$$\begin{array}{rcl} \Big(\mathbb{G}_1 \times \overline{\mathbb{k}}(C)\Big) \times \Big(\mathbb{G}_1 \times \overline{\mathbb{k}}(C)\Big) & \to & \Big(\mathbb{G}_1 \times \overline{\mathbb{k}}(C)\Big) \\ \Big(([m]\,D_1, f_{m,D_1}), ([n]\,D_1, f_{n,D_1})\Big) & \mapsto & \Big([m+n]\,D_1, f_{m+n,D_1}\Big), \end{array}$$

où f_{n,D_1} désigne la fonction de Weil. Le couplage correspond à calculer $f_{r,D_1}(D_2)$. L'algorithme de Miller pour le cas hyperelliptique est alors :

`Entrée` : Deux diviseurs $D_1 = (u_1, v_1)$ et $D_2 = (u_2, v_2)$ et un entier n

`Sortie` : $f_{n,D_1}(D_2)$

1. $D \leftarrow D_1$, $f \leftarrow 1$, $f_1 \leftarrow 1$, $f_2 \leftarrow 1$ et $f_3 \leftarrow 1$
2. $n = \sum_{i=0}^{\ell} n_i 2^i = (n_\ell, ..., n_0)_2$ en base 2.

3. **pour** $i = \ell - 1$ à 0 **faire**
4. $f_1 \leftarrow f_1^2 \bmod u_2$, $f_2 \leftarrow f_2^2 \bmod u_2$ et $f_3 \leftarrow f_3^2$
5. $D, (h_1, h_2, h_3) \leftarrow [2]\, D$
6. $f_1 \leftarrow f_1 h_1 \bmod u_2$, $f_2 \leftarrow f_2 h_2 \bmod u_2$ et $f_3 \leftarrow f_3 h_3$
7. **si** $n_i = 1$ **alors**
8. $D, (h_1, h_2, h_3) \leftarrow D + D_1$
9. $f_1 \leftarrow f_1 h_1 \bmod u_2$, $f_2 \leftarrow f_2 h_2 \bmod u_2$ et $f_3 \leftarrow f_3 h_3$
10. **fin si**
11. **fin pour**
12. **retourner** $f = \dfrac{\text{Résultant}(u_2, f_1)}{f_3^{\deg(u_2)} \text{Résultant}(u_2, f_2)}$.

Chapitre 5

Quelques améliorations algorithmiques

L'implémentation efficace des couplages en genre 1 et 2 a suscité un grand intêret au sein de la communauté scientifique. En témoigne, le nombre abondant de publications dont on peut citer les travaux de [BKLS02, Ver08, Mil04, HSV06, Hes08, GHO+07]. Ils reposent principalement sur deux idées :

- utiliser une représentation permettant une arithmétique particulièrement efficace de la jacobienne de la courbe [CMO98] ;
- réduire le nombre d'itérations de l'algorithme de Miller [HSV06].

Nous avons déjà discuté au précédent chapitre des différentes représentations possibles des éléments d'une jacobienne de courbe hyperelliptique. Nous reviendrons d'autre part sur l'arithmétique efficace des jacobiennes dans la troisième partie de ce mémoire.

Dans ce chapitre, nous allons avant tout nous concentrer sur les techniques permettant de réduire le nombre d'itérations de l'algorithme de Miller. Les couplages de Ate I et II (voir [JE08, chap. 2] pour le cas elliptique) sont des versions modifiées du couplage de Tate permettant de réduire le nombre de boucles de l'algorithme de Miller . Pour le couplage de Ate I, la réduction s'obtient grâce à l'utilisation de l'endomorphisme de Frobenius. Pour Ate II, on utilise la minimisation des coefficients de la décomposition en base q du nombre de boucles de l'algorithme de Miller dans le couplage Ate I. Le couplage Ate II est conjecturé optimal en terme de complexité dans le cas des courbes elliptiques [Ver08].

Conventions et notations. Nous aurons besoin de la définition suivante :

Définition 5.1 (Degré de plongement) Soit $\mathbb{k}$ un corps fini de caractéristique p et de cardinal q et soit r un entier premier avec q. On dit qu'un entier d est le degré de plongement de C relativement à r si les deux conditions suivantes sont réalisées :

i) J_C possède un point $\mathbb{k}$-rationnel d'ordre r,

ii) l'entier d est le plus petit entier tel que $\mu_r \subset K$ avec $K/\mathbb{k}$ l'extension de degré d (nous rappelons que nous avons supposé que $\mathbb{k}$ est fini),

où μ_r désigne l'ensemble des racines $r^{\text{ièmes}}$ de l'unité.

La deuxième condition n'implique pas que l'ensemble des points de r-torsions soit rationnel sur K (i.e. on n'a pas forcément $J_C[r] \subseteq J_C(K)$) sauf pour les courbes elliptiques. Ceci ne sera pas un problème vu que l'intersection des groupes $\mathbb{G}_1$ et $\mathbb{G}_2$ que l'on va construire se réduit à l'élément neutre de la jacobienne.

Notations. Dans toute la suite du chapitre,

- r désigne est un entier premier avec q,
- d désigne le degré de plongement relativement à r,
- K désigne la plus petite extension de $\Bbbk$ contenant μ_r.

5.1 Couplages de Tate et Eta

Le couplage Eta est un dérivé du couplage de Tate que l'on utilise dans les applications en cryptographie. Notons en effet que le couplage de Tate T_r est à valeurs dans l'espace quotient K^*/K^{*r}. Le fait que l'ensemble d'arrivée soit un quotient n'est pas pratique par exemple si l'on souhaite tester l'égalité entre deux valeurs. Pour avoir une représentation unique dans K^*, on peut élever le résultat de T_r à la puissance $(q^d-1)/r$. On obtient ainsi le couplage de Tate réduit [BGhS07], aussi appelé couplage Eta. On a la formule :

$$\eta_r(D_1, D_2) := T_r(D_1, D_2)^{\frac{q^d-1}{r}} = f_{r,D_1}(D_2)^{\frac{q^d-1}{r}}.$$

Remarque 5.2 Si on écrit $D_i = \sum_{j=1}^{m_i} P_j - m_i P_\infty$ avec $m_i \leq g$ pour $i = 1, 2$, alors

$$T_r(D_1, D_2) = f_{r,D_1}(D_2) = \frac{\prod_{j=1}^{m_2} f_{r,D_1}(P_j)}{f_{r,D_1}(P_\infty)^{m_2}}.$$

Donc il sera donc judicieux de normaliser les fonctions f_{r,D_1} en posant $f_{r,D_1}(P_\infty) = 1$

La propriété fondamentale du couplage Eta. Pour tout multiple N de r qui divise $q^d - 1$, et pour tout $D_1 \in J_C(\Bbbk)[r]$ et $D_2 \in \dfrac{J_C(K)}{rJ_C(K)}$, on a :

$$\eta_r(D_1, D_2) = \eta_N(D_1, D_2) = f_{D_1}(D_2)^{\frac{q^d-1}{N}}.$$

5.2 Couplages Ate I et II

Il s'agit de deux améliorations algorithmiques du couplage de Tate qui permettent de réduire le nombre d'itérations dans l'algorithme de Miller. L'idée, assez classique dans l'arithmétique des courbes, est d'utiliser l'existence d'un endomorphisme non trivial à savoir le Frobenius pour accélérer l'algorithme d'exponentiation. Dans le couplage de Tate, les deux groupes $\mathbb{G}_1$ et $\mathbb{G}_2$ ne jouent pas le même rôle d'un point de vue algorithmique. En effet, le groupe $\mathbb{G}_1$ est défini dans le petit corps $\Bbbk$ tandis que le groupe $\mathbb{G}_2$ est défini dans l'extension K et on choisit le couplage de manière a minimiser le nombre d'opérations dans le gros corps K car elles sont plus coûteuses. Pour pouvoir utiliser l'accélération liée à la structure d'extension de K, nous allons voir que l'on doit permuter le rôle de $\mathbb{G}_1$ et de $\mathbb{G}_2$. De ce fait, dans le couplage Ate, la diminution du nombre d'itérations de Miller est contrecarrée par le fait que l'on fait plus d'opérations sur le grand corps. Ainsi, les couplages Ate peuvent être plus lents que le couplage Eta. Notons par C_{Miller} la complexité d'une boucle de Miller, par ℓ_η et ℓ_a le nombre de boucles de l'algorithme de Miller pour respectivement les couplages Eta et Ate I, alors une condition nécessaire et suffisante pour que le couplage Ate I soit plus rapide que le couplage Eta est que :

$$\frac{\ell_a}{\ell_\eta} \leq \frac{C_{Miller}(\text{Eta})}{C_{Miller}(\text{Ate})}.$$

Nous allons expliciter cette formule dans le cas de courbes de genre 2 (voir formule (5.1)).

Dans les deux sections suivantes, nous abordons respectivement le couplage Ate I et le couplage Ate II en genre 2. Nous renvoyons le lecteur vers [HSV06, Ver08, MKHO07] pour le cas bien connu des courbes elliptiques.

5.2.1 Couplage Ate I

Introduit par Hess, Smart et Vercauteren dans [HSV06] en 2006 pour le cas elliptique, ce couplage repose sur le lemme suivant :

Lemme 5.3 *Soit λ un multiple de l'entier r, l'application a_λ suivante est bilinéaire*

$$\begin{aligned} a_\lambda : \mathbb{G}_2 \times \mathbb{G}_1 &\to \mu_r \subset K^* \\ (D_2, D_1) &\mapsto a_\lambda(D_2, D_1) := f_{\lambda, D_2}(D_1)^{\frac{q^d-1}{r}}, \end{aligned}$$

où f_{λ,D_2} est normalisée. De plus, elle est non dégénérée si $J_C(K)$ ne contient pas de point de r^2-torsion et si $\gcd(r, \lambda/r) = 1$.

Preuve : Posons $\lambda = cr$, alors le théorème 4.5 donne :

$$f_{\lambda,D_2} = f_{cr,D_2} = f_{r,D_2}^c . f_{s,[r]D_2} = f_{r,D_2}^c.$$

Ce qui permet d'écrire :

$$a_\lambda(D_2, D_1) = f_{\lambda,D_2}(D_1)^{\frac{q^d-1}{r}} = f_{r,D_2}(D_1)^{c\frac{q^d-1}{r}} = \eta_r(D_2, D_1)^c,$$

ce qui prouve la bilinéarité de a_λ. De plus, si $J_C(K)$ ne contient pas de point de r^2-torsion, alors le couplage de Tate est non dégénéré et il en est évidemment de même pour le couplage Ate si $\gcd(c, r) = 1$. □

Définition 5.4 Soient C une courbe hyperelliptique sur $\mathbb{k}$ et $P \in C(\overline{\mathbb{k}})$. On dit qu'une fonction $f \in \overline{\mathbb{F}}_q(C)$ est normalisée en P si $(u_P^n f)(P) = 1$ pour une uniformisante u_P en P et un entier n.

A partir de maintenant, nous supposons que $\mathbb{G}_1 = J_C[r] \cap (\ker(\pi) - [1])$ et $\mathbb{G}_2 = J_C[r] \cap (\ker(\pi) - [q])$ où π est le morphisme de Frobenius fixant $\mathbb{k}$. On suppose d'autre part, que $J_C(k)$ ne contient pas de point de r^2-torsion. La définition classique du couplage de Ate elliptique de [HSV06] donne dans le cas d'une courbe hyperelliptique [GHV07] :

Théorème 5.5 (Couplage Ate I) *Soit S un entier tel que $S \equiv q \pmod r$ et posons $\lambda = S^d - 1$ et $c = \lambda/r$. Alors l'application*

$$a_S : \mathbb{G}_2 \times \mathbb{G}_1 \to \mu_r \subset K^*,\ (D_2, D_1) \mapsto a_S(D_2, D_1) = f_{S,D_2}(D_1)^{\frac{q^d-1}{r}},$$

avec f_{S,D_2} normalisée, est bilinéaire. De plus elle est non dégénérée si $\gcd(c, r) = 1$.

Preuve : D'après les formules de la section 4.2.2, on a :

$$f_{\lambda,D_2} = f_{S^d-1,D_2} = f_{S^d,D_2} . f_{-1,D_2} . h_{[S^d]D_2,[-1]D_2}.$$

Or $f_{-1,D_2} = (f_{1,D_2} h_{D_2,-D_2})^{-1}$, et $f_{1,D_2} = 1$, comme $S^d \equiv 1 \bmod r$, D_1 et D_2 sont d'ordre r, et donc $h_{[S^d]D_2,[-1]D_2} = h_{D_2,-D_2}$. Par suite, on a :

$$f_{-1,D_2} h_{[S^d]D_2,[-1]D_2} = 1 \text{ ce qui permet d'écrire } f_{\lambda,D_2} = f_{S^d-1,D_2} = \prod_{i=0}^{d-1} f_{S,[S^i]D_2}^{S^{d-1-i}}.$$

Comme $S \equiv q \,(\bmod\, r)$ et $D_2 \in \mathbb{G}_2$ donc $[S^i]\, D_2 = [q^i]\, D_2 = \pi^i(D_2)$ (avec π le Frobenius). Par suite

$$f_{S,[S^i]D_2} = f_{S,\pi^i(D_2)} \Leftrightarrow f_{S,[S^i]D_2} \circ \pi^i = f_{S,D_2}^{q^i} \Leftrightarrow f_{S,[S^i]D_2}(D_1) = f_{S,D_2}^{q^i}(D_1),$$

car $\pi(D_1) = D_1$. Ce qui permet d'écrire

$$f_{\lambda,D_2}(D_1) = \prod_{i=0}^{d-1} f_{S,[S^i]D_2}^{S^{d-1-i}}(D_1) = \prod_{i=0}^{d-1} f_{S,D_2}^{q^i.S^{d-1-i}}(D_1) = f_{S,D_2}(D_1)^{\sum_{i=0}^{d-1} q^i.S^{d-1-i}}.$$

Les égalités précédentes montrent la bilinéarité de $a_S(D_2, D_1)$. Il est clair que $a_S(D_2, D_1)$ est non dégénérée avec les hypothèses du théorème. □

Remarque 5.6 On peut faire un choix judicieux des paramètres pour avoir une exponentielle finale adéquate. Par exemple $N = \gcd(q^d - 1, \lambda)$ et $c = \lambda/N$ alors

$$f_{\lambda,D_2} = f_{S,D_2}^{c_S \frac{q^d-1}{N}} \text{ avec } c_S = \gcd(N, \sum_{i=0}^{d-1} q^i.S^{d-1-i})$$

définit une application bilinéaire et qui est non-dégénérée si $\gcd(c, r) = 1$.

Remarque 5.7 Pour tout entier positif i, on note que r divise $(q^i)^d - 1$. Alors, on peut étendre le théorème 5.5 pour tout entier $S \equiv q^i \,(\bmod\, r)$.

On voit que l'avantage du couplage Ate est que l'entier S définissant le nombre de tours dans l'algorithme de Miller est plus petit que l'entier r qui intervient dans le nombre de tours du couplage de Tate.

5.2.2 Couplage Ate II

Avec les notations de la section précédente sur le couplage Ate I, nous pouvons écrire l'entier λ en base q, i.e $\lambda = \sum_{i=0}^{\ell} c_i q^i$. Alors le couplage a_λ du lemme 5.3 peut s'écrire

$$a_\lambda(D_2, D_1) = f_{\lambda,D_2}(D_1)^{(q^d-1)/r} = f_{\sum_{i=0}^{\ell} c_i q^i, D_2}(D_1)^{(q^d-1)/r}.$$

D'après les propriétés sur les fonctions de Weil (voir le corollaire 4.8), on a :

$$f_{\sum_{i=0}^{\ell} c_i q^i, D_2} = \prod_{i=0}^{\ell} f_{c_i q^i, D_2} \prod_{i=0}^{\ell-1} h_{\sum_{j=0}^{i} [c_j q^j] D_2, [c_{i+1} q^{i+1}] D_2}.$$

Or la formule du produit des fonctions de Weil donne :

$$f_{c_i q^i, D_2}(D_1) = f_{q^i, D_2}^{c_i}(D_1) f_{c_i, [q^i] D_2}(D_1) = f_{q^i, D_2}^{c_i}(D_1) f_{c_i, D_2}^{q^i}(D_1).$$

Et la formule de la puissance des fonctions de Weil donne :

$$f_{q^i,D_2}(D_1) = \prod_{j=0}^{i-1} f_{q,[q^j]D_2}^{q^{i-j-1}}(D_1) = \prod_{j=0}^{i-1} f_{q,D_2}^{q^{i-1}}(D_1) = f_{q,D_2}^{iq^{i-1}}(D_1).$$

Ce qui permet d'écrire

$$f_{c_iq^i,D_2}(D_1) = f_{q,D_2}^{ic_iq^{i-1}}(D_1) f_{c_i,D_2}^{q^i}(D_1).$$

Finalement

$$\begin{aligned} a_\lambda(D_2,D_1) &= \left(f_{q,D_2}^{\sum_{i=0}^{\ell} ic_iq^{i-1}}(D_1)\right)^{\frac{q^d-1}{r}} \left(\prod_{i=0}^{\ell} f_{c_i,D_2}^{q^i}(D_1)\right)^{\frac{q^d-1}{r}} \\ &\quad \times \left(\prod_{i=0}^{\ell-1} h_{\sum_{j=0}^{i}[c_jq^j]D_2,[c_{i+1}q^{i+1}]D_2}(D_1)\right)^{\frac{q^d-1}{r}}. \end{aligned}$$

Posons $a_q(D_2,D_1) = (f_{q,D_2}(D_1))^{\frac{q^d-1}{r}}$. Alors a_q définit une application bilinéaire d'après le théorème 5.5. On obtient :

$$\begin{aligned} a_\lambda(D_2,D_1) &= \left(a_q(D_2,D_1)^{\sum_{i=0}^{\ell} ic_iq^{i-1}}\right) \left(\prod_{i=0}^{\ell} f_{c_i,D_2}^{q^i}(D_1)\right)^{\frac{q^d-1}{r}} \\ &\quad \times \left(\prod_{i=0}^{\ell-1} h_{\sum_{j=0}^{i}[c_jq^j]D_2,[c_{i+1}q^{i+1}]D_2}(D_1)\right)^{\frac{q^d-1}{r}}. \end{aligned}$$

Posons

$$a_{[c_0,c_\ell]}(D_2,D_1) = \left(\prod_{i=0}^{\ell} f_{c_i,D_2}^{q^i}(D_1)\right)^{\frac{q^d-1}{r}} \left(\prod_{i=0}^{\ell-1} h_{\sum_{j=0}^{i}[c_jq^j]D_2,[c_{i+1}q^{i+1}]D_2}(D_1)\right)^{\frac{q^d-1}{r}},$$

alors $a_{[c_0,c_\ell]}(D_2,D_1) \neq 1$ si et seulement si $a_\lambda(D_1,D_2) \neq a_q\,(D_2,D_1)^{\sum_{i=0}^{\ell} ic_iq^{i-1}}$. Écrivons $a_\lambda(D_1,D_2)$ en fonction de a_q. On a :

$$a_\lambda(D_1,D_2) = f_{cr,D_2}(D_1)^{(q^d-1)/r} = f_{r,D_2}(D_1)^{c(q^d-1)/r} = f_{q^d-1,D_2}(D_1)^{c(\frac{q^d-1}{r})^{-1} \bmod r}.$$

La dernière égalité vient directement de la propriété fondamentale du couplage Eta. En utilisant les mêmes arguments que ceux de la preuve du théorème 5.5, on a :

$$\begin{aligned} a_\lambda(D_2,D_1) &= \left(f_{q^d,D_2}(D_1)\right)^{c(\frac{q^d-1}{r})^{-1} \bmod r} \\ &= \left(\prod_{i=0}^{d-1} f_{q,[q^i]D_2}^{q^{d-1-i}}\right)^{c(\frac{q^d-1}{r})^{-1} \bmod r} \\ &= \left(\prod_{i=0}^{d-1} f_{q,D_2}^{q^{d-1}}\right)^{c(\frac{q^d-1}{r})^{-1} \bmod r}. \end{aligned}$$

Donc,

$$\begin{aligned} a_\lambda(D_2, D_1) &= \left(f_{q,D_2}^{dq^{d-1}}(D_1)\right)^{c(\frac{q^d-1}{r})^{-1} \bmod r} \\ &= a_q(D_2, D_1)^{cdq^{d-1}(\frac{q^d-1}{r})^{-1} \bmod r}. \end{aligned}$$

Par suite,

$$a_\lambda(D_1, D_2) \neq \left(a_q(D_2, D_1)^{\sum_{i=0}^{\ell} ic_iq^{i-1}}\right) \Leftrightarrow cdq^{d-1}(\frac{q^d-1}{r})^{-1} \neq \sum_{i=0}^{\ell} ic_iq^{i-1} \bmod r.$$

Nous venons de démontrer le théorème suivant :

Théorème 5.8 (Couplage Ate II) *Soit $\lambda = cr$ avec $\gcd(r, c) = 1$ et écrivons $\lambda = \sum_{i=0}^{\ell} c_iq^i$ alors l'application*

$$\begin{aligned} a_{[c_0,c_\ell]} : \mathbb{G}_2 \times \mathbb{G}_1 &\to \mu_r \subset \mathbb{F}_{q^d}^* \\ (D_2, D_1) &\mapsto \left(\prod_{i=0}^{\ell} f_{c_i,D_2}^{q^i}(D_1)\right)^{\frac{q^d-1}{r}} \left(\prod_{i=0}^{\ell-1} h_{\sum_{j=0}^{i}[c_jq^j]D_2,[c_{i+1}q^{i+1}]D_2}(D_1)\right)^{\frac{q^d-1}{r}} \end{aligned}$$

est une application bilinéaire. Elle est non-dégénérée si et seulement si

$$cdq^{d-1} \neq (\frac{q^d-1}{r}) \sum_{i=0}^{\ell} ic_iq^{i-1} \bmod r.$$

En genre 1 où $D_1 := (P) - (P_\infty)$ et $D_2 := (Q) - (P_\infty)$ et la remarque 4.3 donne

$$h_{\sum_{j=0}^{i}[c_jq^j]Q,[c_{i+1}q^{i+1}]Q} := \frac{\ell_{\sum_{j=0}^{i}[c_jq^j]Q,[c_{i+1}q^{i+1}]Q}}{v_{\sum_{j=0}^{i}[c_jq^j]Q,[c_{i+1}q^{i+1}]Q}},$$

où pour tout point Q_1 et Q_2, la notation ℓ_{Q_1,Q_2} désigne l'équation de la droite passant par Q_1 et Q_2 et la notation v_{Q_1,Q_2} désigne l'équation de la droite verticale passant par Q_1+Q_2. Ce qui permet de voir que le théorème 1 de [Ver08] est un cas particulier du théorème 5.8.

Remarque 5.9 En pratique, pour utiliser le théorème 5.8, nous avons besoin de trouver des coefficients c_i petits dans la base q pour l'entier λ. Pour cela, il suffit de considérer les puissances q^i pour $1 \leq i \leq \varphi(d) - 1$ et de chercher grâce à LLL [LLL82] le plus petit vecteur de la matrice suivante :

$$M := \begin{pmatrix} r & 0 & 0 & \dots & 0 \\ -q & 1 & 0 & \dots & 0 \\ -q^2 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & & \ddots & \\ -q^{\varphi(d)-1} & 0 & \dots & 0 & 1 \end{pmatrix}.$$

5.3 Comparaison des différents couplages

Nous n'allons comparer que les complexités des couplages de Tate (ou plus précisément Eta qui est le plus utile pour les applications cryptographiques) et Ate I. Le calcul de ces différents couplages fait intervenir deux groupes $\mathbb{G}_1$ et $\mathbb{G}_2$ de même ordre r, mais dont les

éléments sont définis sur les corps $\Bbbk$ et K où K est l'extension de degré d (le degré de plongement relativement à r) de $\Bbbk$.

Pour simplifier, écrivons un couplage quelconque sous la forme de $c : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ avec $|\mathbb{G}_1| = |\mathbb{G}_2| = |\mathbb{G}_T| = r$. Alors le couplage Eta et Ate I s'écrivent respectivement $\eta_n(D_1, D_2) = c(D_1, D_2)$ et $a_n(D_2, D_1) = c(D_1, D_2)$. Soit $e = 1$ ou $e = d$ et notons par M_{q^e}, S_{q^e} et I_{q^e} la complexité de la multiplication, du carré et de l'inversion dans le corps fini $\mathbb{F}_{q^e}$.

Pour calculer un couplage, on effectue l'arithmétique dans $\mathbb{G}_1$ et on évalue la fonction de Miller en un élément de $\mathbb{G}_2$. Le tableau 5.1 donne les différentes complexités des couplages Eta et Ate où les entiers ℓ_η et ℓ_a représentent le nombre de boucles de l'algorithme de Miller avec $\ell_a \leq \ell_\eta = \log_2 r$.

Couplage	Coût
Eta	$\big(30M_q + 6S_q + I_q + 11M_{q^d} + 4S_{q^d}\big)\ell_\eta + 1I_{q^d}$
Ate I	$\big(30M_{q^d} + 6S_{q^d} + I_{q^d} + 11M_{q^d} + 4S_{q^d}\big)\ell_a + 1I_{q^d}$

TAB. 5.1 – Coût du couplage de Eta et de Ate I

On déduit du tableau 5.1 une condition nécessaire et suffisante pour que le couplage Ate soit plus efficace que la couplage Eta :

$$\ell_a \leq \frac{30M_q + 6S_q + I_q + 11M_{q^d} + 4S_{q^d}}{30M_{q^d} + 6S_{q^d} + I_{q^d} + 11M_{q^d} + 4S_{q^d}}\ell_\eta. \tag{5.1}$$

5.4 Elliptique vs hyperelliptique

Soient $\Bbbk$ et $\Bbbk'$ deux corps finis, $E/\Bbbk$ une courbe elliptique et $C/\Bbbk'$ une courbe hyperelliptique de genre 2. Soient r et r' deux nombres premiers divisant respectivement $|E(\Bbbk)|$ et $|J_C(\Bbbk')|$. Soient d et d' les degrés de plongement relativement à r et r' respectivement et notons par $L/\Bbbk$ et $L'/\Bbbk'$ les extensions de degrés d et d'.

Pour tout corps $K \in \{\Bbbk, \Bbbk', L, L'\}$, notons par M_K et $I_K = \alpha M_K$ les coûts d'une multiplication et d'une inversion dans le corps K, $1M_L = \beta M_\Bbbk$ et $1M_{L'} = \beta M_{\Bbbk'}$. Alors, en caractéristique impaire, les complexités des couplages (sans tenir compte de l'exponentiation finale) sont donnés dans le tableau 5.2

courbe elliptique	$\big((3 + \alpha + 3\beta)M_\Bbbk\big)\log_2 r$
courbe de genre 2	$\big((30 + \alpha + 11\beta)M_{\Bbbk'}\big)\log_2 r' + \alpha\beta M_{\Bbbk'}$

TAB. 5.2 – Coût des couplages elliptiques et hyperelliptiques

Pour pouvoir comparer les courbes $E/\Bbbk$ et $C/\Bbbk'$, il faut et il suffit qu'elles aient le même niveau de sécurité. Une condition vérifiée asymptotiquement pour cela est :

$$2\frac{d'}{d}\frac{\log_2 q'}{\log_2 q} = \frac{\log_2 r'}{\log_2 r}, \quad \text{avec} \quad q = \#\Bbbk \ \text{ et } \ q' = \#\Bbbk'. \tag{5.2}$$

L'égalité (5.2) signifie que les ρ-values des courbes E/L et C/L', définies sur les extensions, sont égaux. Clairement, dans le couplage hyperelliptique, ce qui coûte le plus est l'arithmétique sur la courbe et l'évaluation de la fonction de Miller.

5.5 Implémentation cryptographique

Dans cette partie, nous donnons quelques détails d'implémentation des algorithmes de calcul de couplage sur courbes hyperelliptiques. Nous avons fait les implémentations avec le logiciel MAGMA exécuté sous un système Linux Mandriva sur un PC 32 bits à 1.83 GHZ et avec 1 Go de RAM et nous donnons quelques temps de calcul afin de pouvoir faire des comparaisons.

Dans toutes les implémentations, nous prenons une courbe hyperelliptique C définie sur un corps $\Bbbk$, un entier r qui divise $\#J_C(\Bbbk)$, un entier d qui est le degré de plongement relativement à r. Deux groupes $\mathbb{G}_1 = J_C[r] \cap \ker(\pi - [1])$ et $\mathbb{G}_2 = J_C[r] \cap \ker(\pi - [q])$ engendrés par deux diviseurs réduits $D_1 \in J_C(\Bbbk)[r]$ et $D_2 \in J_C(K)[r]$. Nous prenons les exemples de courbes construites par Kawazoe et Takahashi [KT08], par Freeman [Fre07] et par Galbraith, Hess et Vercauteren [GHV07].

5.5.1 Construction de diviseurs

Contrairement au cas des courbes elliptiques, il est parfois difficile de trouver des éléments de $\mathbb{G}_1$ et $\mathbb{G}_2$. Pour résoudre cela, on prend deux points quelconques P_1 et P_2 définis sur $C(K)$ pour une extension finie K' de $\Bbbk$ (par la suite on prendra $K' = K$ ou $K' = \Bbbk$), puis on construit le diviseur $D = (P_1) + (P_2) - 2(P_\infty)$. Mais ce diviseur n'est pas forcément dans $\mathbb{G}_1$ ou dans $\mathbb{G}_2$.

Pour trouver un diviseur dans $\mathbb{G}_1$, on cherche d'abord le plus petit entier $e \geq 1$ tel que r^e divise $\#J_C(K')$ (pour $K' = \Bbbk$, alors l'entier $e = 1$). Par suite le diviseur

$$D' = \left[\frac{\#J_C(K')}{r^e}\right] D$$

est dans $J_C(K')[r]$ donc pour $K' := \Bbbk$, le diviseur D' est dans bien dans $\mathbb{G}_1$. Maintenant si $K' = K$, on doit trouver à partir de D' un élément de $\mathbb{G}_2$. Pour ce faire, on divise le polynôme caractéristique du Frobenius $\chi(\pi)(T) \bmod r$ par $(T - q) \bmod r$ et on utilise la formule suivante vérifiée par le Frobenius π :

$$\pi^4(D) + [a_1]\,\pi^3(D) + [a_2]\,\pi^2(D) + [a_1 q]\,\pi(D) + \left[q^2\right] D = (P_\infty).$$

5.5.2 Exponentiation finale

Pour calculer les couplages avec l'algorithme de Miller , nous effectuons une exponentiation finale d'un élément $\alpha \in K = \mathbb{F}_{q^d}$ à la puissance $m = (q^d - 1)/r$. Or

$$q^d - 1 = \prod_{n|d} \Phi_n(q),$$

avec $\Phi_n(x) \in \mathbb{Z}[x]$ le $n-$ième polynôme cyclotomique [GG99, p. 388]. Donc

$$m = \frac{q^d - 1}{r} = \frac{\Phi_d(q)}{r} \cdot \prod_{\substack{n|d \\ n \neq d}} \Phi_n(q) := m_1 m_2.$$

Les polynômes $\Phi_n(x)$ que nous utiliserons ont des coefficients égaux à -1 ou 1. Donc le produit m_2 peut s'écrire facilement en base q avec des coefficients égaux à -1 ou 1, i.e.

$m_2 = b_{d-\varphi(d)}q^{d-\varphi(d)} + ... + b_1 q + b_0$, avec $b_i \in \{-1, 0, 1\}$ où $\varphi(d)$ est la fonction indicatrice d'Euler. De même, on a $m_1 := \Phi_d(q)/r = a_{\varphi(d)-1}q^{\varphi(d)-1} + ... + a_1 q + c_0$. Donc

$$\alpha^m = \alpha^{m_1 m_2} = (\alpha^{m_2})^{m_1} = \left(\beta^{q^{\varphi(d)-1}}\right)^{a_{\varphi(d)-1}} ... \left(\beta^q\right)^{a_1} \beta^{a_0},$$

avec $\beta = \alpha^{m_2}$. Les termes β^{q^i} pour $0 \leq 1 \leq \varphi(d) - 1$ se calculent facilement grâce au morphisme de Frobenius. La partie difficile se calcule en utilisant l'exponentiation rapide [ACD+06].

Exemple 5.10 Considérons la famille BN de courbes elliptiques [BN06] où $d = 12$ et

$$\begin{aligned} q(x) &= 36x^4 + 36x^3 + 24x^2 + 6x + 1 \\ r(x) &= 36x^4 + 36x^3 + 18x^2 + 6x + 1 \end{aligned}$$

alors $q^{12} - 1 = \Phi_{12}(q).\Big(\Phi_1(q)\Phi_2(q)\Phi_3(q)\Phi_4(q)\Phi_6(q)\Big)$. Donc

$$\frac{q^{12}-1}{r} = \frac{q^4 - q^2 + 1}{r}(q^8 + q^6 - q^2 - 1) = (q^3 + a_2 q^2 + a_1 q + a_0)(q^8 + q^6 - q^2 - 1),$$

avec $a_2(x) = 6x^2 + 1$, $a_1(x) = 36x^3 - 18x^2 + 12x + 1$ et $a_0 = 36x^3 - 30x^2 + 18x - 2$ (cf [SBCP08]).

5.5.3 Etude de cas

Exemple 5.11 courbe hyperelliptique cyclotomique $C : y^2 = x^5 + 243x$ de Kawazoe et Takahashi [KT08] de type I donnée par les paramètres suivantes :

$d := 32$;
$r := 298271871767803247714167829477732515100314693637921$; (168 bits)
$c := 899265628387654982790712284926192804883 45$;
$d := 91102433828282221461546183306$;
$p := c^2 + 2d^2$; (273 bits)
$\pi_p(t) := t^4 - 4dt^3 + 8d^2t^2 - 4dpt + p^2$; (Frobenius)
$\#J_C(\mathbb{F}_p) \approx$ (621 bits)

Exemple 5.12 courbe hyperelliptique cyclotomique $C : y^2 = x^5 + 2x$ de Kawazoe et Takahashi [KT08] de type II donnée par les paramètres suivantes :

$d := 24$;
$t := 1049085$;
$c := -6665526863179228374181853184292218 75$;
$d := -3176822734034955749735700191 29$;
$r := 146718682892712893651454019963417202720820469 0001$; (161 bits)
$p := c^2 + 2d^2$; $(p \equiv 3 \bmod 8)$ (164 bits)
$\pi_p(t) := t^4 + (4c^2 - 2p)t^2 + p^2$; (Frobenius).

Exemple 5.13 courbe hyperelliptique à multiplication complexe de Freeman [Fre07] de la forme $y^2 = x^5 + a_3x^3 + a_2x^2 + a_1x + a_0$:

$d := 2$;
$r := 2^{160} + 7$;
$q := 795006611640170109396940876005774396116863415419758542983/$
$000866861998633580771739771859880604810428624690260906439/$

$$6966763836446430241565650794386330511522658711936072460 02/$$
$$1623269435928862304096161; \quad (651 \text{ bits})$$

$$s_1 := 24106522149194751442854131036844857413955837089165628335 7/$$
$$5130644533869547607329841035851103109025 24;$$

$$s_2 := 27359796173391521974641264798803491215724479159390071276 1/$$
$$3921708420371371770365655339687429984334911542250536630 74/$$
$$7540833278734962025912889995467452433290635909803745841 72/$$
$$1962697398843910255646496 6;$$

$$\pi(T) := t^4 - s_1 t^3 + s_2 t^2 - s_1 q t + p^2; \quad \text{(Frobenius)}$$

$$a_3 := 781556463828009280287360245134696723363334003262680019563/$$
$$3732466633994032830364805233918296724734157425944009119 80/$$
$$7179618084606363721356664947849828920635199536383165038 34/$$
$$9582750830436766970252305;$$

$$a_2 := 7582071544815219456170366446823922831149495107058780881 32/$$
$$2686089206261889334387948338188122777399118742240541369 92/$$
$$0781021614606618491386755769001513635702002583900328984 72/$$
$$4486510381446751384612338;$$

$$a_1 := 3818089517351649616063431378422557160370805668771261782 62/$$
$$4948661255611804031104728412516481837472216648106219404 75/$$
$$9483953015501490776665659662815927077156530942394435679 89/$$
$$0448998428239238224064322;$$

$$a_0 := 4517793113380355476036520985314738676697566971047952708 96/$$
$$0707773483032139181526019191380637561071045120827733864 05/$$
$$7302909106384439009009025246738012848274281139752085484 20/$$
$$4533726326846152147956130;$$

Couplage	Tate	Ate I	Ate I optimisé	Ate II
courbe KT, type I (exemple 5.11)	2800	4240	1600	4280
courbe KT, type II (exemple 5.12)	1440	2280	760	2360
courbe de Freeman (exemple 5.13)	100	90	90	100

TAB. 5.3 – Coût en millisecondes des différents exemples

On constate qu'en genre 2 les couplages Ate I et II ne sont pas plus efficaces que le couplage de Tate comme c'est le cas en genre 1. Cependant, la version optimisée du couplage Ate où le nombre de boucle est de la forme $q^i \bmod r$ est plus performante que le couplage de Tate. Ceci révèle l'importance du nombre de boucles de l'algorithme de Miller, mais aussi de l'arithmétique sur les corps $\mathbb{k}$ et K. En effet, pour que le couplage Ate soit plus performant que celui de Tate, il faut et il suffit que le nombre de boucles de l'algorithme de Miller vérifie l'inégalité (5.1)

Troisième partie

Modèles efficaces à base de fonctions thêta

Chapitre 6

Quelques rappels

Dans ce chapitre, nous rappelons quelques résultats sur les fonctions thêta . Ces fonctions thêta donnent une paramétrisation projective des variétés abéliennes et donc en particulier des jacobiennes de courbes hyperelliptiques. En fait, la jacobienne d'une courbe hyperelliptique C de genre g à coefficients dans $\mathbb{C}$ est isomorphe à un tore $\mathbb{C}^g/\Lambda$, où Λ est un réseau ayant certaines bonnes propriétés (voir [Gau00] pour la construction de Λ).

Bien que cette théorie, de nature analytique, utilise de manière cruciale le fait que les variétés abéliennes considérées soient à coefficients dans $\mathbb{C}$, les relations algébriques obtenues à partir des fonctions thêta gardent un sens pour tout corps de caractéristique zéro que l'on peut plonger dans $\mathbb{C}$. Nous expliquerons comment étendre ces résultats au corps fini de caractéristique impaire en utilisant les nombres $p-$adiques. Dans ce chapitre, nous commencerons par quelques rappels sur les fonctions thêta [Rit03, Mum83, RF74].

6.1 Fonctions thêta de Riemann

Soit g un entier positif et considérons $\mathbb{H}_g$ l'ensemble des matrices carrées $M \in \mathbb{M}_g(\mathbb{C})$ symétriques telles que la partie imaginaire de M soit définie positive ($\mathbb{H}_g$ est appelé demi-espace de Siegel). La fonction thêta de Riemann est donnée par la série de fonction de deux variables $(z, \Omega) \in \mathbb{C}^g \times \mathbb{H}_g$:

$$\theta(z, \Omega) = \sum_{n \in \mathbb{Z}^g} \exp\left(\pi i (n^t \Omega n + 2 n^t z)\right). \tag{6.1}$$

En tant que série de fonctions de deux variables, la fonction thêta est absolument et uniformément convergente sur tout compact de $\mathbb{C}^g \times \mathbb{H}_g$, et donc c'est une fonction holomorphe sur $\mathbb{C}^g \times \mathbb{H}_g$ [Mum83, page 118].

Pour $\Omega \in \mathbb{H}_g$, nous désignons par L_Ω le réseau de $\mathbb{C}^g$ donné par $L_\Omega = \mathbb{Z}^g + \mathbb{Z}^g\Omega$. Nous avons les propriétés suivantes :

Proposition 6.1 Pour tout $m \in \mathbb{Z}^g$

$$\begin{aligned} \theta(z + m, \Omega) &= \theta(z, \Omega), & (6.2)\\ \theta(z + m\Omega, \Omega) &= \exp(-\pi i (m^t \Omega m + 2 m^t z)\theta(z, \Omega), & (6.3)\\ \theta(-z, \Omega) &= \theta(z, \Omega). & (6.4) \end{aligned}$$

Preuve : voir [Mum83, page 120-121]. □

Pour $\Omega \in L_\Omega$ fixé, les relations (6.2) et (6.4) signifient que la fonction $\theta(., \Omega)$ est $L_\Omega-$quasi-périodique. On peut généraliser cette notion avec la définition suivante.

Définition 6.2 *On dit qu'une fonction complexe holomorphe $f : \mathbb{C}^g \to \mathbb{C}$ est $L_\Omega-$quasi-périodique de poids ℓ si elle vérifie les relations suivantes :*

(i) $f(z+m) = f(z)$ *pour tout* $m \in \mathbb{Z}^g$,

(ii) $f(z+m\Omega) = \exp(-\pi i\ell(m^t\Omega m + 2m^t z)f(z)$ *pour tout* $m \in \mathbb{Z}^g$.

Par exemple, la fonction $\theta(.,\Omega)$ est $L_\Omega-$quasi-périodique de poids 1. Notons par $\mathcal{R}_\ell^\Omega$ le $\mathbb{C}-$espace vectoriel des fonctions $L_\Omega-$quasi-périodiques de poids ℓ. Une base de l'espace vectoriel $\mathcal{R}_\ell^\Omega$ peut être donnée à l'aide des fonctions thêta avec caractéristique. Pour cela, nous posons la définition suivante :

Définition 6.3 Soient $a, b \in \mathbb{R}^g$ et $(z,\Omega) \in \mathbb{C}^g \times \mathbb{H}^g$, une fonction thêta avec caractéristique est donnée par :

$$\theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right](z,\Omega) = \sum_{n\in\mathbb{Z}^g} \exp\left(\pi i(n+\frac{1}{2}a)^t\Omega(n+\frac{1}{2}a) + 2\pi i(n+\frac{1}{2}a)^t(z+\frac{1}{2}b)\right). \tag{6.5}$$

Proposition 6.4 La matrice Ω étant fixée,

(i) pour tout $a, b \in \mathbb{R}^g$ et tout $z \in \mathbb{C}^g$, on a :

$$\theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right](z,\Omega) = \exp\left(\frac{\pi i}{4}a^t\Omega a + \pi i a^t(z+\frac{1}{2}b)\right)\theta\left(z+\frac{1}{2}a\Omega+\frac{1}{2}b\right). \tag{6.6}$$

(ii) pour tout $a, b \in \mathbb{Z}^g$ et tout $z \in \mathbb{C}^g$, on a :

$$\begin{aligned}\theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right](-z,\Omega) &= \theta\left[\begin{smallmatrix}-a\\-b\end{smallmatrix}\right](z,\Omega) &(6.7)\\ &= (-1)^{a^tb}\theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right](z,\Omega). &(6.8)\end{aligned}$$

(iii) pour tout $a, b \in \mathbb{R}^g$, $m, n \in \mathbb{Z}^g$ et tout $z \in \mathbb{C}^g$, on a :

$$\theta\left[\begin{smallmatrix}a+2n\\b+2m\end{smallmatrix}\right](z,\Omega) = \exp(\pi i a^t m)\theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right](z,\Omega). \tag{6.9}$$

Preuve : voir [Mum83, p. 123]. □

Remarquons que, pour tout $a, b \in \mathbb{Q}^g$, la fonction de Ω, $\theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right](0,\Omega)$ est holomorphe. Pour des entiers a et b fixés, les fonctions $\theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right](0,\Omega)$ sont appelés *thêta constantes*.

La principale propriété des fonctions thêta avec caractéristique est la propriété de quasi-périodicité.

Proposition 6.5 Pour tout $a, b, m \in \mathbb{Z}^g$ et tout $z \in \mathbb{C}^g$, on a :

$$\begin{aligned}\theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right](z+m,\Omega) &= \exp(\pi i a^t m)\theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right](z,\Omega), &(6.10)\\ \theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right](z+m\Omega,\Omega) &= \exp(-\pi i b^t m)\exp(-\pi i m^t\Omega m - 2\pi i m^t z)\theta\left[\begin{smallmatrix}a\\b\end{smallmatrix}\right](z,\Omega). &(6.11)\end{aligned}$$

Preuve : voir [Mum83, p. 120-121]. □

Le théorème suivant, qui se déduit aisément de la précédente proposition, donne une base de l'espace vectoriel $\mathcal{R}_\ell^\Omega$ en terme des fonctions thêta avec caractéristique.

Théorème 6.6 *Fixons $\Omega \in \mathbb{H}_g$, alors une base de $\mathcal{R}_\ell^\Omega$ est donnée par l'ensemble des fonctions holomorphes suivantes :*

1. $f_a(z) = \theta\left[\begin{smallmatrix}a/\ell\\0\end{smallmatrix}\right](\ell z, \ell\Omega)$, *avec* $a = (a_1, ..., a_g)$ *où* $0 \le a_i < \ell$,
2. $g_b(z) = \theta\left[\begin{smallmatrix}0\\b/\ell\end{smallmatrix}\right](z, \ell^{-1}\Omega)$, *avec* $b = (b_1, ..., b_g)$ *où* $0 \le b_i < \ell$.

Si de plus, l'entier ℓ est un carré, alors une troisième base est donnée par :

3. $h_{a,b}(z) = \theta \begin{bmatrix} a/\sqrt{\ell} \\ b/\sqrt{\ell} \end{bmatrix} (\sqrt{\ell} z, \Omega)$ *avec* $0 \leq a_i, b_i < \sqrt{\ell}$.

Ces différentes bases sont reliées par les relations suivantes :

$$\begin{aligned} g_b &= \sum_a \exp\left(2\pi i \ell^{-1} a^t b\right) f_a, \\ h_{a,b} &= \sum_{c \equiv a \bmod \sqrt{\ell}} \exp\left(2\pi i (\sqrt{\ell})^{-1} c^t b\right) f_c. \end{aligned}$$

Preuve : voir [Mum83, p. 124]. □

6.2 Quelques relations avec les fonctions thêta

Dans ce paragraphe, nous rappelons les formules de Riemann qui permettent d'obtenir beaucoup de relations algébriques entre les fonctions thêta.

Notation : Dans toute la suite, sauf mention du contraire, on fixera la matrice Ω et on notera respectivement les fonctions thêta et thêta avec caractéristique par $\theta(z)$ et $\theta \begin{bmatrix} a \\ b \end{bmatrix} (z)$ au lieu de $\theta(z, \Omega)$ et $\theta \begin{bmatrix} a \\ b \end{bmatrix} (z, \Omega)$. On a alors le théorème suivant :

Théorème 6.7 *Soient $a = (a_j)_{1 \leq j \leq 4}, b = (b_j)_{1 \leq j \leq 4}$, avec a_j, b_j des éléments de $\mathbb{R}^g$ et $z = (z_j)_{1 \leq j \leq 4}$ avec $z_j \in \mathbb{C}^g$. Posons*

$$T = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix},$$

et $aT = a'$, $bT = b'$, $zT = z'$ avec $a' = (a'_j)_{1 \leq j \leq 4}, b' = (b'_j)_{1 \leq j \leq 4}$ et $z' = (z'_j)_{1 \leq j \leq 4}$. Alors on a :

$$\prod_{j=1}^{4} \theta \begin{bmatrix} a_j \\ b_j \end{bmatrix} (z_j) = 2^{-g} \sum_{\alpha, \beta \in \mathbb{F}_2^g} \exp(-\pi i {a_1}^t \beta) \prod_{j=1}^{4} \theta \begin{bmatrix} {a'}_j + \alpha \\ {b'}_j + \beta \end{bmatrix} ({z'}_j). \tag{6.12}$$

Preuve : voir [Igu72, page 137]. □

Remarque 6.8 Dans le théorème précédent, si les thêta g-caractéristiques a_j et b_j sont des entiers, i.e. des éléments de $\mathbb{Z}^g$, alors la formule (6.12) s'écrit avec $(-1)^{{a_1}^t \beta}$ à la place de $\exp(-\pi i {a_1}^t \beta)$.

Remarque 6.9 Nous avons différents sous-cas du théorème 6.7 qui jouent sur l'écriture des z_i et ${z'}_i$. Notamment, soient $u_1, u_2, u_3, u_4 \in \mathbb{C}^g$ tels que

$$z_1 = u_1 + u_2,\ z_2 = u_1 - u_2,\ z_3 = u_3 + u_4 \text{ et } z_4 = u_3 - u_4,$$

alors il vient que

$${z'}_1 = u_1 + u_3,\ {z'}_2 = u_1 - u_3,\ {z'}_3 = u_2 + u_4 \text{ et } {z'}_4 = u_2 - u_4.$$

On obtient la formule :

$$\begin{aligned} \theta \begin{bmatrix} a_1 \\ b_1 \end{bmatrix} (u_1 + u_2)\ \theta \begin{bmatrix} a_2 \\ b_2 \end{bmatrix} (u_1 - u_2)\ \theta \begin{bmatrix} a_3 \\ b_3 \end{bmatrix} (u_3 + u_4)\ \theta \begin{bmatrix} a_4 \\ b_4 \end{bmatrix} (u_3 - u_4) = \\ 2^{-g} \sum_{\alpha, \beta \in \mathbb{F}_2^g} \exp(-\pi i {a_1}^t \beta)\ \theta \begin{bmatrix} {a'}_1 + \alpha \\ {b'}_1 + \beta \end{bmatrix} (u_1 + u_3)\ \theta \begin{bmatrix} {a'}_2 + \alpha \\ {b'}_2 + \beta \end{bmatrix} (u_1 - u_3) \\ \times \theta \begin{bmatrix} {a'}_3 + \alpha \\ {b'}_3 + \beta \end{bmatrix} (u_2 + u_4)\ \theta \begin{bmatrix} {a'}_4 + \alpha \\ {b'}_4 + \beta \end{bmatrix} (u_2 - u_4). \end{aligned} \tag{6.13}$$

Posons $u_3 = u_4 = 0$ et remplaçons u_1 par u et u_2 par v, alors la formule (6.13) devient

$$\theta \begin{bmatrix} a_1 \\ b_1 \end{bmatrix}(u+v)\ \theta \begin{bmatrix} a_2 \\ b_2 \end{bmatrix}(u-v)\ \theta \begin{bmatrix} a_3 \\ b_3 \end{bmatrix}(0)\ \theta \begin{bmatrix} a_4 \\ b_4 \end{bmatrix}(0) = 2^{-g} \sum_{\alpha,\beta \in \mathbb{F}_2^g} \exp(-\pi i {a_1}^t \beta) \times \theta \begin{bmatrix} {a'}_1+\alpha \\ {b'}_1+\beta \end{bmatrix}(u)\ \theta \begin{bmatrix} {a'}_2+\alpha \\ {b'}_2+\beta \end{bmatrix}(u)\ \theta \begin{bmatrix} {a'}_3+\alpha \\ {b'}_3+\beta \end{bmatrix}(v)\ \theta \begin{bmatrix} {a'}_4+\alpha \\ {b'}_4+\beta \end{bmatrix}(v). \tag{6.14}$$

Pour $v = 0$, la formule (6.14) devient

$$\theta \begin{bmatrix} a_1 \\ b_1 \end{bmatrix}(u)\ \theta \begin{bmatrix} a_2 \\ b_2 \end{bmatrix}(u)\ \theta \begin{bmatrix} a_3 \\ b_3 \end{bmatrix}(0)\ \theta \begin{bmatrix} a_4 \\ b_4 \end{bmatrix}(0) = 2^{-g} \sum_{\alpha,\beta \in \mathbb{F}_2^g} \exp(-\pi i {a_1}^t \beta) \times \theta \begin{bmatrix} {a'}_1+\alpha \\ {b'}_1+\beta \end{bmatrix}(u)\ \theta \begin{bmatrix} {a'}_2+\alpha \\ {b'}_2+\beta \end{bmatrix}(u)\ \theta \begin{bmatrix} {a'}_3+\alpha \\ {b'}_3+\beta \end{bmatrix}(0)\ \theta \begin{bmatrix} {a'}_4+\alpha \\ {b'}_4+\beta \end{bmatrix}(0). \tag{6.15}$$

Remarque 6.10

1. La formule (6.14) est appelée *formule d'addition* d'après [Igu72].
2. La transformation que nous avons effectuée à la remarque 6.9 pour avoir la formule d'addition s'applique aussi pour les caractéristiques a_i et b_i.

Par exemple, avec la formule (6.15), si l'on pose $a_1 = a_2$, $a_3 = a_4$, $b_1 = b_2$ et $b_3 = b_4$, alors $a'_1 = a_1 + a_3$, $a'_2 = a_1 - a_3$, $a'_3 = 0$ et $a'_4 = 0$ et $b'_1 = b_1 + b_3$, $b'_2 = b_1 - b_3$, $b'_3 = 0$ et $b'_4 = 0$. Par suite, la formule (6.15) s'écrit :

$$\theta^2 \begin{bmatrix} a_1 \\ b_1 \end{bmatrix}(u)\ \theta^2 \begin{bmatrix} a_3 \\ b_3 \end{bmatrix}(0) = 2^{-g} \sum_{\alpha,\beta \in \mathbb{F}_2^g} \exp(-\pi i {a_1}^t \beta) \times \theta \begin{bmatrix} a_1+a_3+\alpha \\ b_1+b_3+\beta \end{bmatrix}(u)\ \theta \begin{bmatrix} a_1-a_3+\alpha \\ b_1-b_3+\beta \end{bmatrix}(u)\ \theta^2 \begin{bmatrix} \alpha \\ \beta \end{bmatrix}(0). \tag{6.16}$$

Cette dernière formule peut s'écrire de façon simple, sous la forme :

$$\left[2^g - \exp(-\pi i (a_1+a_3)^t b_3\right] \theta^2 \begin{bmatrix} a_1 \\ b_1 \end{bmatrix}(u)\ \theta^2 \begin{bmatrix} a_3 \\ b_3 \end{bmatrix}(0) = \sum_{(\alpha,\beta) \neq (a_3,b_3)} \exp(-\pi i {a_1}^t \beta) \theta \begin{bmatrix} a_1+a_3+\alpha \\ b_1+b_3+\beta \end{bmatrix}(u)\ \theta \begin{bmatrix} a_1-a_3+\alpha \\ b_1-b_3+\beta \end{bmatrix}(u)\ \theta^2 \begin{bmatrix} \alpha \\ \beta \end{bmatrix}(0). \tag{6.17}$$

Remarque 6.11 Si les thêta g-caractéristiques a_j sont des éléments de $\mathbb{F}_2^g$, alors la formule (6.17) s'écrit simplement sous la forme de :

$$\left[2^g - (-1)^{(a_1+a_3)^t b_3}\right] \theta^2 \begin{bmatrix} a_1 \\ b_1 \end{bmatrix}(u) \theta^2 \begin{bmatrix} a_3 \\ b_3 \end{bmatrix}(0) = \sum_{(\alpha,\beta) \neq (a_3,b_3)} (-1)^{{a_1}^t \beta} \theta^2 \begin{bmatrix} a_1+a_3+\alpha \\ b_1+b_3+\beta \end{bmatrix}(u) \theta^2 \begin{bmatrix} \alpha \\ \beta \end{bmatrix}(0). \tag{6.18}$$

Et enfin si on pose $a_3 = b_3 = 0$, alors on obtient :

$$\left[2^g - 1\right] \theta^2 \begin{bmatrix} a_1 \\ b_1 \end{bmatrix}(u)\ \theta^2 \begin{bmatrix} 0 \\ 0 \end{bmatrix}(0) = \sum_{(\alpha,\beta) \neq (0,0)} (-1)^{{a_1}^t \beta} \theta^2 \begin{bmatrix} a_1+\alpha \\ b_1+\beta \end{bmatrix}(u)\ \theta^2 \begin{bmatrix} \alpha \\ \beta \end{bmatrix}(0). \tag{6.19}$$

6.3 Nombres p-adiques

Dans la littérature, il existe deux approches pour la définition des nombres p-adiques. L'une considère l'ensemble des nombres $p-$adiques comme le complété de $\mathbb{Q}$ pour une certaine norme $p-$adique (ultramétrique) et l'autre définit les $p-$adiques comme une certaine limite projective. Nous n'aborderons que la première approche, et pour plus de détails sur la seconde approche, voir l'excellent livre de Serre [Ser79].

6.3.1 Définitions et propriétés

Nous allons définir le corps des nombres p-adiques en se basant sur l'approche donnée par [Kob84, Gou97], comme le complété de $\mathbb{Q}$ pour une certaine norme.

Définition 6.12 Soit K un corps quelconque (fini ou non), on appelle *norme* ou *valeur absolue* sur K la donnée d'une application

$$|\cdot| : K \to \mathbb{R}_+,$$

vérifiant les conditions suivantes :

(i) pour tout $x \in K$, $|x| = 0$ si et seulement si $x = 0$,

(ii) pour tout $x, y \in K$, $|x.y| = |x|.|y|$,

(iii) pour tout $x, y \in K$, $|x + y| \leq |x| + |y|$,

Quelques exemples de normes :

1. la *norme usuelle* sur $\mathbb{Q}$, donnée par $\forall x \in \mathbb{Q}$, $|x| = \sup(x, -x)$,
3. la *norme triviale* sur tout corps K donnée par $|x| = 1$, $\forall\, x \neq 0$ et $|0| = 0$

Une norme sur un corps K est dite *non-archimidienne* ou bien *ultra métrique* si elle vérifie la condition suivante :

(iv) pour tout $x, y \in K$, $|x + y| \leq \max(|x|, |y|)$.

Nous allons définir une famille de normes non-archimidiennes sur $\mathbb{Q}$.

Définition 6.13 Soit p un nombre premier. Pour tout entier non nul $a \in \mathbb{Z}$, on appelle valuation en p de a et on note $n = v_p(a)$, la plus grande puissance de p divisant a.

Si $a = 0$, on écrit $v_p(0) = \infty$. Noter qu'on a alors une application $v_p : \mathbb{Z} \to \mathbb{Z}$ vérifiant

$$v_p(1) = 0 \qquad \text{et} \qquad v_p(ab) = v_p(a) + v_p(b).$$

On peut étendre cette fonction v_p sur $\mathbb{Q}$ en posant, pour tout nombre rationnel $r = a/b \in \mathbb{Q}$, $v_p(r) = v_p(a) - v_p(b)$. Alors $v_p(r)$ ne dépend pas de l'écriture fractionnaire de r, i.e. si $r = ac/bc$ alors $v_p(r) = v_p(ac) - v_p(bc)$. On a le lemme suivant.

Lemme 6.14 *Pour tout $x, y \in \mathbb{Q}$, on a :* $v_p(a + b) \geq \min(v_p(a), v_p(b))$.

On pose la définition suivante :

Définition 6.15 On appelle norme p-adique ou valeur absolue p-adique, l'application donnée par :

$$|x|_p = \begin{cases} p^{-v_p(x)} & \text{si} \quad x \neq 0, \\ 0 & \text{si} \quad x = 0. \end{cases} \tag{6.20}$$

La norme p-adique est une norme non-archimidienne sur $\mathbb{Q}$.

Pour construire le corps des nombres p-adiques, nous sommes amenés à définir la notion de complétion.

Définition 6.16 Soit K un corps et $|\,.\,|$ une norme sur K.

1. Une suite $(x_n)_{n\in\mathbb{N}}$ d'éléments de K est dite *suite de Cauchy* si elle vérifie :

$$\forall\, \epsilon > 0, \exists\, n_0 \in \mathbb{N} \text{ tel que } (n, n' \geq n_0 \Rightarrow |x_n - x_{n'}| < \epsilon).$$

2. K est dit complet si toute suite de Cauchy dans K admet une limite dans K.

Par exemple, pour la norme usuelle $\mathbb{Q}$ n'est pas complet alors que $\mathbb{R}$ et $\mathbb{C}$ sont complets. De même $\mathbb{Q}$ n'est pas complet pour la norme p-adique. Tout comme la construction de $\mathbb{R}$ à partir de $\mathbb{Q}$ par le complété de la valeur absolue usuelle, il est naturel de construire le complété de $\mathbb{Q}$ par la norme p-adique. Alors notons par $\mathcal{C}(\mathbb{Q})$ l'ensemble des suites de Cauchy sur $\mathbb{Q}$ et par I l'ensemble des suites de Cauchy tendant vers zéro. On peut munir de façon naturelle l'ensemble $\mathcal{C}(\mathbb{Q})$ d'une structure d'anneau unitaire (addition et multiplication de suites par l'addition et la multiplication des termes généraux) et I est alors un idéal maximal de $\mathcal{C}(\mathbb{Q})$. Donc l'ensemble quotient $\mathcal{C}(\mathbb{Q})/I$ est un corps normé qu'on appelle corps p-adique et que l'on note par $\mathbb{Q}_p$.

On appelle l'anneau des entiers p-adiques, l'ensemble des éléments de $\mathbb{Q}_p$ de norme p-adique inférieure à 1, on le note

$$\mathbb{Z}_p := \{x \in \mathbb{Q}_p : |x|_p \leq 1\}.$$

Proposition 6.17 *On a les propriétés suivantes :*

1. *L'anneau $\mathbb{Z}_p$ des entiers p-adiques est un anneau local d'idéal maximal*

$$p\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p < 1\}.$$

2. $\mathbb{Q}_p = \mathbb{Z}_p[1/p]$, *i.e. pour tout $x \in \mathbb{Q}_p$, il existe n tel que $p^n x \in \mathbb{Z}_p$.*
3. $\mathbb{Z} \subsetneq \mathbb{Z}_p$, $\mathbb{Q} \subsetneq \mathbb{Q}_p$ *et* $\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}$

Preuve : voir [Gou97, proposition 3.3.4]. □

Le corps obtenu en quotientant l'anneau $\mathbb{Z}_p$ par son idéal maximal $p\mathbb{Z}_p$ est appelé corps résiduel de $\mathbb{Q}_p$ qui est le corps fini $\mathbb{F}_p = \mathbb{Z}_p/p\mathbb{Z}_p$.

Corollaire 6.18 *Pour tout $x \in \mathbb{Q}_p$, il existe une unique suite d'entiers $(a_n)_n$ dont le terme général vérifie $0 \leq a_n \leq p-1$ telle que $x = \sum_{n \geq n_0} a_n p^n$ avec $n_0 = v_p(x)$.*

Comme nous devrons étudier le relèvement d'éléments d'un corps fini $\Bbbk$ avec q une puissance d'un nombre premier p, nous devons alors voir les extensions finies de $\mathbb{Q}_p$.

6.3.2 Extensions finies de $\mathbb{Q}_p$

Considérons dans cette partie que K une extension finie de $\mathbb{Q}_p$ de degré m définie par un polynôme unitaire irréductible $P(X) \in \mathbb{Q}_p[X]$. On peut écrire $K = \mathbb{Q}_p(\alpha)$, $\alpha \in K \setminus \mathbb{Q}_p$ et l'ensemble $\{1, \alpha, ..., \alpha^{m-1}\}$ est une base du $\mathbb{Q}_p-$espace vectoriel K. Considérons l'application $\mathbb{Q}_p$-linéaire suivante : $K \to K$, $x \mapsto \alpha x$. On définit la norme de α de K vers $\mathbb{Q}_p$, et on note par $N_{K/\mathbb{Q}_p}(\alpha)$, par le déterminant de cette application $x \mapsto \alpha x$. Cela permet d'étendre la valeur absolue p-adique de $\mathbb{Q}_p$ sur K de la façon suivante :

$$|.|_K : K \to \mathbb{R}_+, |x|_K = \sqrt[m]{|N_{L/\mathbb{Q}_p}(x)|_p}, \text{ avec } m = [K : \mathbb{Q}_p].$$

D'après [Kob84, III.2], l'application précédente est une norme qui permet d'étendre de façon unique la norme p-adique sur l'extension $K/\mathbb{Q}_p$.

Soit toujours K une extension finie de $\mathbb{Q}_p$. Considérons l'anneau des entiers de K donné par $\mathcal{O}_K = \{x \in K : |x|_K \leq 1\}$, alors $\mathcal{O}_K$ est un anneau local d'unique idéal maximal $\mathcal{M} = \{x \in L : |x|_L < 1\}$. Le corps résiduel de K est $\Bbbk := \mathcal{O}_K/\mathcal{M}$. Comme K est une extension finie, alors $\Bbbk$ est un corps fini qui est une extension du corps résiduel de $\mathbb{Q}_p$, i.e. $\Bbbk$ est une extension finie de $\mathbb{F}_p$ (voir [Kob84, p. 64] pour plus de détails). On dit qu'une extension finie K de $\mathbb{Q}_p$ est non-ramifiée si p est une uniformisante de $\mathcal{M}$, i.e. $\mathcal{M} = p\mathcal{O}_K$. Les extensions non-ramifiées jouent un rôle capitale comme le montre la remarque suivante.

Remarque 6.19 Réciproquement, soit un corps fini $\mathbb{k}$ de caractéristique p. On sait construire des extensions de $\mathbb{Q}_p$ ayant pour corps résiduel $\mathbb{k}$. Parmi les extensions de $\mathbb{Q}_p$ ayant pour corps résiduel $\mathbb{k}$, il existe une et une seule plus petite extension non-ramifiée (à isomorphisme près). La construction de cette extension non-ramifiée fait l'objet de la section suivante.

6.3.3 Réduction et relèvement

Soit K une extension non-ramifiée de $\mathbb{Q}_p$ de degré absolu d d'anneau des entiers $\mathcal{O}_K$ et de corps résiduel $\mathbb{k} = \mathcal{O}_K/\mathcal{M}$. La projection naturelle $\tau : \mathcal{O}_K \to \mathbb{k}, a \mapsto \overline{a}$ est appelée la réduction modulo l'idéal maximal $\mathcal{M}$. Tout antécédent a_0 d'un élément $\overline{a}_0 \in \mathbb{k}$ est appelé un relevé de $\overline{a}_0$.

Soit un polynôme $f(x_1, ..., x_n)$ de $\mathcal{O}_K[x_1, ..., x_n]$. On appelle la réduction de f et on note $\overline{f}$, le polynôme obtenu à partir de f en appliquant τ à chacun de ses coefficients.

Maintenant, partant d'un corps fini $\mathbb{k}$ de caractéristique p de degré absolu d, nous pouvons construire l'extension non-ramifiée de $\mathbb{Q}_p$ de degré d. Pour cela, soit $\overline{m}(x) \in \mathbb{F}_p[x]$ le polynôme minimal de l'extension $\mathbb{k}/\mathbb{F}_p$. Considérons un relevé $m(x) \in \mathbb{Z}_p[x]$ du polynôme $\overline{m}(x)$. Alors, $m(x)$ est un polynôme irréductible de $\mathbb{Z}_p[x]$ et donc $(m(x))$ est un idéal maximal de $\mathbb{Z}_p[x]$ et alors $\mathbb{Z}_p[x]/(m(x))$ est une extension finie de degré $d = \deg(m(x)) = \deg(\overline{m}(x))$ du corps $\mathbb{Q}_p$ des nombres $p-$adiques. D'où le corps $\mathbb{Z}_p[x]/(m(x))$ est non-ramifiée et :

$$\mathbb{Z}_p[x]/(m(x)) = \mathbb{Q}_{p^d} \qquad \text{et} \qquad \mathcal{O}_K = \mathbb{Q}_{p^d}.$$

Chapitre 7

Calcul efficace sur les courbes elliptiques

Dans ce chapitre et dans le prochain, nous allons utiliser la théorie générale des fonctions thêta du chapitre 6 pour obtenir des modèles pour les jacobiennes de dimension 1 ou 2. Ceci nous permet d'avoir respectivement une arithmétique efficace sur les courbes elliptiques et sur toutes les jacobiennes de courbes hyperelliptiques de genre 2 dans le chapitre 8.

Pour le cas de la dimension 1, nous réinterprétons le modèle d'Edwards [Edw07] sur le corps des complexes avec les fonctions thêta. Ensuite, nous expliquons comment cette interprétation se transfère aux corps finis via une technique de relèvement-réduction. Le cas des corps finis de caractéristique 2 se traite différemment car il y a des problèmes de mauvaise réduction. Nous levons ces obstacles et obtenons un modèle d'Edwards binaire. Notons que le lien entre le modèle d'Edwards sur $\mathbb{C}$ et le modèle binaire que l'on obtient est nouveau.

En genre 2, nous allons décrire une arithmétique efficace sur les surfaces de Kummer associées aux variétés abéliennes de dimension 2. Nous verrons en quoi les surfaces de Kummer peuvent se substituer aux variétés abéliennes dans beaucoup de cas d'applications en cryptographie. Dans le chapitre 8, nous rappelons d'abord les travaux de Gaudry [Gau07] en caractéristique impaire, puis ceux de Gaudry et Lubicz [GL08] sur les courbes ordinaires en caractéristique 2. Nous donnons enfin des formules efficaces pour des courbes non-ordinaires en caractéristique 2 en s'appuyant sur les travaux de [LP02, LP04, Duc08, Duq07, Duq08b].

7.1 Modèle d'Edwards en caractéristique impaire

Edwards [Edw07] montre qu'une courbe de la forme $x^2 + y^2 = a^2(1 + x^2y^2)$ définie sur un corps K est birationnellement équivalente sur la clôture algébrique $\overline{K}$ au modèle de Weierstraβ d'une courbe elliptique. Les formules d'addition obtenues sont très efficaces et résistent à certaines attaques par canaux auxiliaires (car la duplication et l'addition s'effectuent avec les mêmes formules).

En 2008, Bernstein et al. [BBJ+08] remarquent que l'équivalence birationnelle d'Edwards peut être généralisée sur tout corps de caractéristique impaire. Ils introduisent les courbes d'Edwards twistées qui généralisent le modèle d'Edwards. Bernstein, Lange et Farashashi [BLF08] proposent ensuite deux versions du modèle d'Edwards sur les corps de caractéristique 2. Dans ce dernier article, les auteurs ne montrent pas le lien formel qui existe entre le modèle d'Edwards binaire et le modèle d'Edwards général : leur approche

consiste à trouver un modèle ayant toutes les bonnes propriétés du modèle d'Edwards. Dans notre présentatioin nous comblons cette lacune en montrant que le modèle d'Edwards binaire s'obtient comme réduction modulo 2 du modèle d'Edwards général.

Dans cette section, en utilisant les relations thêta de Riemann pour $g = 1$, nous retrouvons le modèle d'Edwards ainsi que les formules d'additions de ce modèle sur $\mathbb{C}$. En utilisant le principe de Lefschetz, nous expliquerons pourquoi les résultats sur $\mathbb{C}$ sont valables sur tout corps fini k de caractéristique $p \geq 3$.

7.1.1 Modèle sur $\mathbb{C}$

Les fonctions thêta que nous considérons sont à valeurs dans $\mathbb{C}$. Ecrivons la formule (6.19) :

$$\theta^2 \left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](u)\, \theta^2 \left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right](0) = \sum_{(\alpha,\beta)\neq(0,0)} (-1)^{a\beta} \theta^2 \left[\begin{smallmatrix} a+\alpha \\ b+\beta \end{smallmatrix}\right](u)\, \theta^2 \left[\begin{smallmatrix} \alpha \\ \beta \end{smallmatrix}\right](0)$$

avec $a, b, \alpha, \beta \in \mathbb{F}_2$. Pour a, b parcourant $\mathbb{F}_2$, nous avons le système suivant :

$$(S) : \begin{cases} \theta^2 \left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right](u)\, \theta^2 \left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right](0) &= \theta^2 \left[\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right](u)\, \theta^2 \left[\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right](0) + \theta^2 \left[\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right](u)\, \theta^2 \left[\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right](0) & \text{si } (a,b) = (0,0) \\ \theta^2 \left[\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right](u)\, \theta^2 \left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right](0) &= \theta^2 \left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right](u)\, \theta^2 \left[\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right](0) + \theta^2 \left[\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right](u)\, \theta^2 \left[\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right](0) & \text{si } (a,b) = (0,1) \\ \theta^2 \left[\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right](u)\, \theta^2 \left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right](0) &= \theta^2 \left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right](u)\, \theta^2 \left[\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right](0) - \theta^2 \left[\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right](u)\, \theta^2 \left[\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right](0) & \text{si } (a,b) = (1,0) \\ \theta^2 \left[\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right](u)\, \theta^2 \left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right](0) &= \theta^2 \left[\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right](u)\, \theta^2 \left[\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right](0) - \theta^2 \left[\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right](u)\, \theta^2 \left[\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right](0) & \text{si } (a,b) = (1,1) \end{cases}$$

Pour simplifier l'écriture, posons $\theta_n = \theta \left[\begin{smallmatrix} n_1 \\ n_2 \end{smallmatrix}\right]$ avec n un entier dont l'écriture binaire s'écrit sous la forme de $n = (n_1 n_2)_2$. On a alors $\theta_0 = \theta \left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right]$, $\theta_1 = \theta \left[\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right]$, $\theta_2 = \theta \left[\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right]$ et $\theta_3 = \theta \left[\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right]$. Le système (S) s'écrit alors

$$(S) : \begin{cases} \theta_0^2(u)\, \theta_0^2(0) &= \theta_1^2(u)\, \theta_1^2(0) + \theta_2^2(u)\, \theta_2^2(0) \\ \theta_1^2(u)\, \theta_0^2(0) &= \theta_0^2(u)\, \theta_1^2(0) + \theta_3^2(u)\, \theta_2^2(0) \\ \theta_2^2(u)\, \theta_0^2(0) &= \theta_0^2(u)\, \theta_2^2(0) - \theta_3^2(u)\, \theta_1^2(0) \\ \theta_3^2(u)\, \theta_0^2(0) &= \theta_1^2(u)\, \theta_2^2(0) - \theta_2^2(u)\, \theta_1^2(0) \end{cases}.$$

Le système (S) est un système linéaire en $(\theta_0^2, \theta_1^2, \theta_2^2, \theta_3^2)$ et s'obtient par l'équation matricielle suivante :

$$(S) : \left[\begin{array}{cccc} \theta_0^2(u) & \theta_1^2(u) & \theta_2^2(u) & \theta_3^2(u) \end{array}\right] M = \left[\begin{array}{cccc} 0 & 0 & 0 & 0 \end{array}\right],$$

avec M la matrice symétrique suivante

$$M = \begin{bmatrix} \theta_0^2(0) & -\theta_1^2(0) & -\theta_2^2(0) & 0 \\ -\theta_1^2(0) & \theta_0^2(0) & 0 & -\theta_2^2(0) \\ -\theta_2^2(0) & 0 & \theta_0^2(0) & -\theta_1^2(0) \\ 0 & -\theta_2^2(0) & \theta_1^2(0) & \theta_0^2(0) \end{bmatrix}.$$

Le déterminant de M est égal à $\det(M) = \left(\theta_0^4(0) - \theta_1^4(0) - \theta_2^4(0)\right)\left(\theta_0^4(0) + \theta_1^4(0) - \theta_2^4(0)\right)$. D'après la relation thêta de Jacobi $\theta_0^4(0) = \theta_1^4(0) + \theta_2^4(0)$, le déterminant de M est nul, ce qui signifie que S est lié. Il est facile de montrer que le rang de M est égal à 2. Pour trouver la relation qui lie $\theta_0^2(u), \theta_1^2(u), \theta_2^2(u)$ et $\theta_3^2(u)$, effectuons le changement de variables suivant :

$$X(u) = \frac{\theta_0(u)}{\theta_2(u)} \qquad \text{et} \qquad Y(u) = \frac{\theta_3(u)}{\theta_1(u)},$$

alors les équations (3) et (1) de (S) donnent respectivement les formules :

$$\begin{array}{rcl} \left(X^2(u)\,\theta_2^2(0) - \theta_0^2(0)\right)\theta_2^2(u) &=& \theta_3^2(u)\,\theta_1^2(0) \\ \left(X^2(u)\,\theta_0^2(0) - \theta_2^2(0)\right)\theta_2^2(u) &=& \theta_1^2(u)\,\theta_1^2(0) \end{array}$$

Et le rapport de ces deux équations donne

$$\frac{X^2(u)\theta_2^2(0) - \theta_0^2(0)}{X^2(u)\theta_0^2(0) - \theta_2^2(0)} = \frac{\theta_3^2(u)}{\theta_1^2(u)} = Y^2(u)$$

ou bien de façon équivalente :

$$X^2(u) + Y^2(u) = \frac{\theta_0^2(0)}{\theta_2^2(0)}\left(1 + X^2(u)Y^2(u)\right). \tag{7.1}$$

Ceci est bien le modèle de la courbe d'Edwards [Edw07], avec comme paramètre $\theta_0(0)/\theta_2(0)$. La figure 7.1 donne un aperçu du modèle d'Edwards et du modèle de Weierstraβ d'une courbe elliptique sur $\mathbb{R}$.

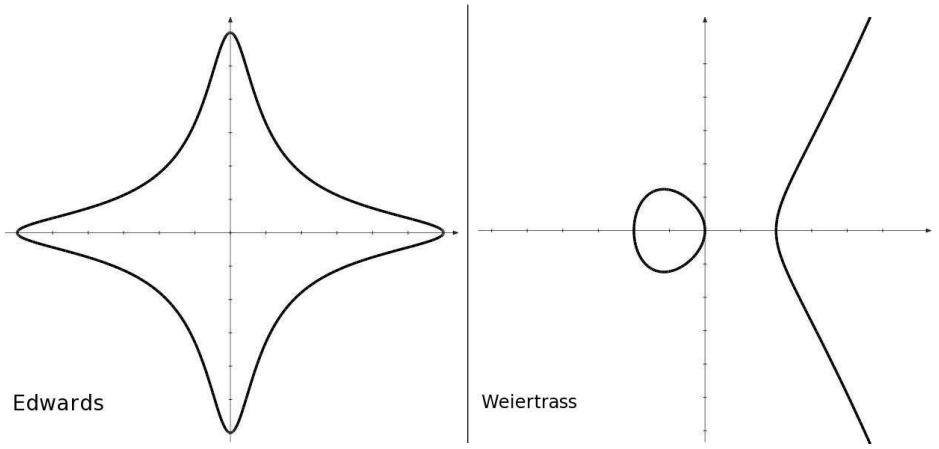

FIG. 7.1 – Modèles d'Edwards et de Weierstraβ d'une courbe elliptique sur $\mathbb{R}$

7.1.2 Formules d'addition sur $\mathbb{C}$

On sait désormais comment exprimer à l'aide des fonctions thêta le système de coordonnées donnant le modèle d'Edwards sur $\mathbb{C}$. En fait, nous avons

$$X(u) = \frac{\theta_0(u)}{\theta_2(u)} = \frac{\theta_{00}(u)}{\theta_{10}(u)} \qquad \text{et} \qquad Y(u) = \frac{\theta_3(u)}{\theta_1(u)} = \frac{\theta_{11}(u)}{\theta_{01}(u)}.$$

On rappelle la formule d'addition (6.14) des thêta 1-caractéristiques entières :

$$\begin{aligned} \theta\begin{bmatrix} a_1 \\ b_1 \end{bmatrix}(u+v)\;\theta\begin{bmatrix} a_2 \\ b_2 \end{bmatrix}(u-v)\;\theta\begin{bmatrix} a_3 \\ b_3 \end{bmatrix}(0)\theta\begin{bmatrix} a_4 \\ b_4 \end{bmatrix}(0) &= 2^{-g}\sum_{\alpha,\beta\in\mathbb{F}_2^g}(-1)^{{a_1}^t\beta} \\ &\times\theta\begin{bmatrix} a'_1+\alpha \\ b'_1+\beta \end{bmatrix}(u)\;\theta\begin{bmatrix} a'_2+\alpha \\ b'_2+\beta \end{bmatrix}(u)\theta\begin{bmatrix} a'_3+\alpha \\ b'_3+\beta \end{bmatrix}(v)\;\theta\begin{bmatrix} a'_4+\alpha \\ b'_4+\beta \end{bmatrix}(v). \end{aligned}$$

De cette formule, nous déduisons :

$$\theta_0(u+v)\,\theta_1(u-v)\,\theta_0(0)\,\theta_1(0) = \theta_0(u)\,\theta_1(u)\,\theta_0(v)\,\theta_1(v) - \theta_2(u)\,\theta_3(u)\,\theta_2(v)\,\theta_3(v), \tag{7.2}$$

$$\theta_2(u+v)\,\theta_1(u-v)\,\theta_1(0)\,\theta_2(0) = \theta_1(u)\,\theta_2(u)\,\theta_1(v)\,\theta_2(v) - \theta_0(u)\,\theta_3(u)\theta_0(v)\,\theta_3(v), \tag{7.3}$$

$$\theta_3(u+v)\,\theta_2(u-v)\,\theta_0(0)\,\theta_1(0) = \theta_0(u)\,\theta_1(u)\,\theta_2(v)\,\theta_3(v) + \theta_2(u)\,\theta_3(u)\,\theta_0(v)\,\theta_1(v), \tag{7.4}$$

$$\theta_1(u+v)\,\theta_2(u-v)\,\theta_1(0)\,\theta_2(0) = \theta_0(u)\,\theta_3(u)\,\theta_0(v)\,\theta_3(v) + \theta_1(u)\,\theta_2(u)\,\theta_1(v)\,\theta_2(v). \tag{7.5}$$

Divisons maintenant les formules (7.2), (7.3), (7.4) et (7.5) par le produit $\theta_2(u)\theta_2(v)\theta_1(u)\theta_1(v)$, on obtient alors

$$\begin{aligned}
\frac{\theta_0(u+v)\,\theta_1(u-v)\,\theta_0(0)\,\theta_1(0)}{\theta_2(u)\,\theta_2(v)\,\theta_1(u)\,\theta_1(v)} &= \frac{\theta_0(u)}{\theta_2(u)}\frac{\theta_0(v)}{\theta_2(v)} - \frac{\theta_3(u)}{\theta_2(u)}\frac{\theta_3(v)}{\theta_2(v)},\\
\frac{\theta_2(u+v)\,\theta_1(u-v)\,\theta_1(0)\,\theta_2(0)}{\theta_2(u)\,\theta_2(v)\,\theta_1(u)\,\theta_1(v)} &= 1 - \frac{\theta_0(u)}{\theta_2(u)}\frac{\theta_0(v)}{\theta_2(v)}\frac{\theta_3(u)}{\theta_1(u)}\frac{\theta_3(v)}{\theta_1(v)},\\
\frac{\theta_3(u+v)\,\theta_2(u-v)\,\theta_0(0)\,\theta_1(0)}{\theta_2(u)\,\theta_2(v)\,\theta_1(u)\,\theta_1(v)} &= \frac{\theta_0(u)}{\theta_2(u)}\frac{\theta_3(v)}{\theta_1(v)} + \frac{\theta_0(v)}{\theta_2(v)}\frac{\theta_3(u)}{\theta_1(u)},\\
\frac{\theta_1(u+v)\,\theta_2(u-v)\theta_1(0)\,\theta_2(0)}{\theta_2(u)\,\theta_2(v)\,\theta_1(u)\,\theta_1(v)} &= 1 + \frac{\theta_0(u)}{\theta_2(u)}\frac{\theta_3(u)}{\theta_1(u)}\frac{\theta_0(v)}{\theta_2(v)}\frac{\theta_3(v)}{\theta_1(v)}.
\end{aligned}$$

Faisons les rapports de la première sur la deuxième puis le rapport de la troisième sur la quatrième en se rappelant que

$$X(u) = \frac{\theta_0(u)}{\theta_2(u)} = \frac{\theta_{00}(u)}{\theta_{10}(u)} \qquad \text{et} \qquad Y(u) = \frac{\theta_3(u)}{\theta_1(u)} = \frac{\theta_{11}(u)}{\theta_{01}(u)}.$$

On obtient

$$X(u+v) = \frac{\theta_2(0)}{\theta_0(0)}\frac{X(u)X(v) - Y(u)Y(v)}{1 - X(u)X(v)Y(u)Y(v)} \tag{7.6}$$

$$Y(u+v) = \frac{\theta_2(0)}{\theta_0(0)}\frac{X(u)Y(v) + Y(u)X(v)}{1 + X(u)X(v)Y(u)Y(v)}. \tag{7.7}$$

Les formules (7.6) et (7.7) sont les formules d'addition de la courbe d'Edwards (7.1) [Edw07]. Nous avons utilisé la théorie des fonctions thêta sur $\mathbb{C}$ pour trouver le modèle de la courbe d'Edwards sur $\mathbb{C}$ et les formules d'addition de ce modèle. Dans le prochain paragraphe, nous allons utiliser des techniques de réduction et relèvement pour montrer la validité des résultats sur tout corps de caractéristique impaire.

7.1.3 En caractéristique impaire

Soit K une extension non-ramifiée de $\mathbb{Q}_p$ (avec p un entier premier impair), d'anneau des entiers $\mathcal{O}_K$ et de corps résiduel $\Bbbk$. Soit $\tau : \mathcal{O}_K \to \Bbbk$, $a \mapsto \overline{a}$ l'application de réduction modulo l'idéal maximal $\mathcal{M}$ de $\mathcal{O}_K$. Considérons $\psi : K \to \mathbb{C}$ un plongement de K dans $\mathbb{C}$ (cf [Rob00, p. 144-145]) que l'on fixe pour le reste de cette section.

Soit $\overline{E} : y^2 = x^3 + \overline{a}_2x^2 + \overline{a}_4x + \overline{a}_6$ une courbe elliptique définie sur $\Bbbk$. Considérons un relevé $E : y^2 = x^3 + a_2x^2 + a_4x + a_6$ de $\overline{E}$. La courbe E définie sur $\mathcal{O}_K$ peut être considérée via ψ comme une courbe à coefficients dans $\mathbb{C}$ ou plus exactement dans $\psi(K)$.

D'après les considérations qui précédent, E est birationnellement équivalente à un modèle d'Edwards donné par une équation :

$$E_{\mathrm{Ed}} : X^2 + Y^2 = \frac{\theta\begin{bmatrix}0\\0\end{bmatrix}^2(0)}{\theta\begin{bmatrix}1\\0\end{bmatrix}^2(0)}\left(1 + X^2Y^2\right).$$

Ce modèle se réduit modulo p à une courbe elliptique et l'application birationnelle entre E et E_{Ed} étant algébrique a aussi un sens modulo p. On en déduit que E_{Ed} est un modèle de E définie sur une extension de degré 4 de $\Bbbk$.

Cependant E_{Ed} se réduit modulo 2 en une courbe singulière sur tout corps de caractéristique 2. La résolution de ce problème en caractéristique 2 va constituer l'objet de notre prochaine section.

7.2 Courbe d'Edwards en caractéristique 2

En 2008, Bernstein, Lange et Farashashi [BLF08] donnent un modèle de la courbe d'Edwards en caractéristique 2 qui respecte une propriété de symétrie : (x, y) est un élément de la courbe si et seulement si (y, x) est un élément de la courbe.

L'objectif de cette section est de justifier le modèle d'Edwards binaire en montrant qu'il s'obtient naturellement par réduction modulo 2 du modèle d'Edwards habituel après avoir effectué un changement de coordonnées destiné à éviter les problèmes de mauvaise réduction. Le modèle que nous obtenons donne une sous-famille du modèle de [BLF08].

7.2.1 Modèle de la courbe

Soit $\Bbbk$ un corps fini de caractéristique 2 et de degré d'extension absolu d . On note par $\tau : \mathbb{Z}_{2^d} \to \Bbbk$ la réduction qui à $\mathbb{Z}_{2^d} \ni x \mapsto \overline{x} \in \Bbbk$. Considérons une courbe d'Edwards

$$E_{\mathrm{Ed}} : X^2(u) + Y^2(u) = \frac{\theta_0^2(0)}{\theta_2^2(0)} \left(1 + X^2(u)Y^2(u)\right),$$

à coefficients dans $\mathbb{Z}_{2^d}$. La courbe E_{Ed} est définie sur le corps des nombres 2−adiques $\mathbb{Q}_{2^d}$. Rappelons que la réduction de la courbe E_{Ed} donne une courbe $\mathcal{E}/\Bbbk$ singulière. Pour résoudre ce problème, nous allons faire un changement de variables en tennant compte des valuations sur les coefficients que l'on obtient à l'aide d'une certaine équation modulaire. Pour cela, nous avons besoin de la définition suivante :

Définition 7.1 Soit $\mathcal{E}/\Bbbk$ une courbe elliptique définie sur k. Un relevé $E/\mathbb{Z}_{2^d}$ de $\mathcal{E}/\Bbbk$ est dit *canonique* si les anneaux des endomorphismes de $E/\mathbb{Z}_{2^d}$ et de $\mathcal{E}/\Bbbk$ sont isomorphes (i.e. $\mathrm{End}(E/\mathbb{Z}_{2^d}) \equiv \mathrm{End}(\mathcal{E}/\Bbbk)$) via le morphisme de réduction.

Fixons un plongement $\psi : \mathbb{Q}_{2^d} \to \mathbb{C}$ et considérons $E/\mathbb{Z}_{2^d} \times_{\mathbb{Z}_{2^d}} \mathbb{Q}_{2^d}$ comme une courbe sur $\mathbb{C}$ via le plongement ψ. D'après la section 7.1.1, nous connaissons un modèle de la courbe E plongée dans le plan affine via les coordonnées

$$X(u) = \frac{\theta_{00}(u)}{\theta_{10}(u)} \qquad \text{et} \qquad Y(u) = \frac{\theta_{11}(u)}{\theta_{01}(u)}.$$

Dès lors, effectuons le changement de variables suivant [Mum66] :

$$\begin{cases} \theta_{00}(u) &= Z_0(u) + Z_2(u) \\ \theta_{01}(u) &= Z_1(u) + Z_3(u) \\ \theta_{10}(u) &= Z_0(u) - Z_2(u) \\ \theta_{11}(u) &= Z_1(u) - Z_3(u) \end{cases}. \tag{7.8}$$

Alors les thêta constantes s'obtiennent par les relations :

$$\begin{cases} \theta_{00}(0) &= Z_0(0) + Z_2(0) \\ \theta_{01}(0) &= Z_1(0) + Z_3(0) = 2Z_1(0) \\ \theta_{10}(0) &= Z_0(0) - Z_2(0) \\ \theta_{11}(0) &= Z_1(0) - Z_3(0) = 0 \end{cases}. \tag{7.9}$$

D'après [Car05], sur le relevé canonique, les $Z_i(0)$ pour $i = 0, 1, 2, 3$ vérifient la relation suivante

$$Z_i^2(0) = \sum_{j \in \mathbb{Z}/4\mathbb{Z}} \sigma(Z_{i+j}(0))\sigma(Z_j(0)), \tag{7.10}$$

où σ est le relèvement du morphisme de Frobenius sur $\mathbb{Z}_{2^d}$. Soit v_2 la valuation 2−adique sur l'anneau $\mathbb{Z}_{2^d}$. Alors la relation (7.10) permet de montrer que $v_2(Z_i(0)) \geq 1$ si $i \neq 0$ et $Z_0(0) \bmod 2 = 1$ (pour plus de détail voir [GL08]). Alors pour $i = 0, 1, 2, 3$, il existe des $c_i \in \mathbb{Z}_{2^d}$ tels que $Z_0(0) = 1 + 2c_0$ et $Z_i(0) = 2c_i$ pour $i \neq 0$. Dès lors, on peut calculer le paramètre de la courbe E_{Ed} en fonction des nouvelles coordonnées (Z_0, Z_1, Z_2, Z_3). On a :

$$\frac{\theta_{00}(0)}{\theta_{10}(0)} = \frac{Z_0(0) + Z_2(0)}{Z_0(0) - Z_2(0)} = \frac{1 + 2(c_0 + c_2)}{1 + 2(c_0 - c_2)}.$$

D'autres part, les formules (7.8) permettent d'écrire :

$$X(u) = \frac{\theta_{00}(u)}{\theta_{10}(u)} = \frac{Z_0(u) + Z_2(u)}{Z_0(u) - Z_2(u)} \qquad \text{et} \qquad Y(u) = \frac{\theta_{11}(u)}{\theta_{01}(u)} = \frac{Z_1(u) - Z_3(u)}{Z_1(u) + Z_3(u)}.$$

Posons les fonctions $x_u = \dfrac{Z_0(u)}{Z_2(u)}$ et $y_u = \dfrac{Z_3(u)}{Z_1(u)}$, alors

$$X(u) = \frac{x_u + 1}{x_u - 1} \qquad \text{et} \qquad Y(u) = \frac{1 - y_u}{1 + y_u}. \tag{7.11}$$

Remplaçons alors les expressions de $X(u)$ et $Y(u)$ dans l'équation de la courbe d'Edwards, on obtient alors

$$(2c_0c_2 + c_2)(x_u^2y_u^2 + x_u^2 + y_u^2) - 4(c_0^2 + c_2^2 + c_0)x_uy_u - x_uy_u + c_2 + 2c_0c_2 = 0.$$

En réduisant modulo 2 l'équation précédente, on obtient la forme de l'équation d'Edwards binaire. On peut alors donner la définition suivante :

Définition 7.2 Soit $\Bbbk$ un corps de caractéristique 2. Un modèle de la courbe d'Edwards binaire sur $\Bbbk$ peut s'écrire sous la forme de :

$$E_c : x^2 + y^2 + \frac{1}{c}xy = 1 + x^2y^2, \qquad \text{avec } c = c_2 \in \Bbbk^* := \Bbbk \setminus \{0\}. \tag{7.12}$$

Le genre de la courbe (7.12) est égal à 1 (cela se démontre en utilisant la formule générale de calcul du genre à partir de l'équation de la courbe, pour plus de détails voir Fulton [Ful69, p. 199] ou [Hac96, p. 35]).

Afin d'écrire l'addition sur les points de 4−torsion, nous avons besoin d'étudier les points de singularité de la courbe et de faire un éclatement en ses singularités.

Singularité. Une équation projective de la courbe E_c est donnée par :

$$c(X^2Y^2 + X^2Z^2 + Y^2Z^2 + Z^4) + XYZ^2 = 0. \tag{7.13}$$

Posons $f(X, Y, Z) = c(X^2Y^2 + X^2Z^2 + Y^2Z^2 + Z^4) + XYZ^2$, alors les dérivées partielles de f par rapport à X, Y et Z s'écrivent :

$$\frac{\partial f}{\partial X} = YZ^2, \quad \frac{\partial f}{\partial Y} = XZ^2 \quad \text{et} \quad \frac{\partial f}{\partial Z} = 0.$$

Les seuls points de singularité de la courbe d'Edwards sont les points à l'infini $[1 : 0 : 0]$ et $[0 : 1 : 0]$. Pour étudier la courbe au voisinage des points singuliers, nous allons faire une résolution de singularité en éclatant soit en $[1 : 0 : 0]$, soit en $[0 : 1 : 0]$.

Eclatement en $[1:0:0]$**.** Posons $X = 1$, alors l'équation (7.13) devient

$$c(Y^2 + Z^2 + Y^2Z^2 + Z^4) + YZ^2 = 0$$

qui est l'équation d'une courbe singulière en $(0,0)$. Posons, alors $Y = ZT$, et divisons par Z^2, on obtient alors la courbe

$$T^2 + Z^2 + \frac{1}{c}TZ = 1 + U^2Z^2$$

et pour $Z = 0$, on obtient $T = 1$, i.e. le point $(1,0)$ qui est un point non-singulier.
Pour le point $[0:1:0]$ de (7.13), on applique le même procédé et on trouve le même résultat.

Formules de transformations du modèle d'Edwards au modèle de Weierstraβ. Nous continuons d'appeler $\Bbbk$ une extension finie de $\mathbb{F}_2$ de degré absolu d. Une courbe elliptique ordinaire sur $\Bbbk$ admet une équation de Weierstraβ suivante :

$$z^2 + tz = t^3 + at^2 + b, \quad \text{avec} \quad b \neq 0. \tag{7.14}$$

Remarque 7.3 Seul le paramètre a apparaît dans les formules d'addition de la courbe (7.14) (voir la section 3.1).

Nous allons montrer que la courbe d'Edwards binaire (7.12) est birationnellement équivalente à la courbe elliptique ordinaire donnée par :

$$z^2 + tz = t^3 + c^4 \tag{7.15}$$

et de $j-$invariant égal à $1/c^4$. Pour cela, il faut juste considérer le changement de coordonnées suivant :

$$\varphi : \quad (x,y) \mapsto (t,z), \quad \begin{cases} t &= c/x \\ z &= c(y + cx(y+1))/(x(y+1)) \end{cases},$$
$$\varphi^{-1} : \quad (t,z) \mapsto (x,y), \quad \begin{cases} x &= c/t \\ y &= (z + c^2)/(t + z + c^2) \end{cases}.$$

L'application φ n'est pas définie au point $(0,1)$, et on pose $\varphi(0,1) = P_\infty$ (on montrera que le point de coordonnées $(0,1)$ est l'élément neutre de la loi de groupe sur la courbe (7.12)). D'après [Kob91, p. 161], les courbes d'Edwards que nous obtenons sont des courbes ordinaires dont la 4-torsion est rationnelle.

Pour retrouver le modèle de Bernstein, Lange et Farashahi [BLF08] donné par

$$d_1(T + Z) + d_2(T^2 + Z^2) = TZ(T + 1)(Z + 1), \text{ avec } d_1, d_2 \in \Bbbk,$$

il suffit de poser $d_2 = d_1^2$ et $d_1^6 = c^4$.

7.2.2 Formules d'addition

La loi d'addition sur la courbe d'Edwards est connue [Edw07, BBJ+08]. Nous allons réduire cette loi d'addition modulo 2 pour avoir la loi d'addition correspondant à notre modèle d'Edwards binaire.

Théorème 7.4 *Soient $P_1 = (x_1, y_1)$ et $P_2 = (x_2, y_2)$ deux points de la courbe $E_c/\mathbb{k}$ et posons $P_3 = (x_3, y_3) = P_1 + P_2$. Alors les coordonnées de P_3 sont données par les formules suivantes :*

$$x_3 = \frac{(x_1 + x_2)(1 + y_1 y_2)}{(y_1 + y_2)(1 + x_1 x_2)} \text{ et } y_3 = \frac{(x_1 + y_2)(y_1 + x_2)}{(1 + x_1 y_2)(1 + y_1 x_2)}. \tag{7.16}$$

Et si $P_1 = P_2$, alors les coordonnées de la duplication sont

$$x_3 = \frac{x_1(y_1 + 1)^2}{y_1(x_1 + 1)^2} \text{ et } y_3 = \frac{(x_1 + y_1)^2}{(x_1 y_1 + 1)^2}. \tag{7.17}$$

Ceci permet de définir sur la courbe $E_c/\mathbb{k}$, une loi d'addition dont l'élément neutre a pour coordonnées $(0, 1)$ et l'opposé de $P = (x, y)$ est $-P = (x, 1/y)$.

Preuve : Nous allons seulement démontrer les formules (7.16) et (7.17). Notons que ces formules s'obtiennent par le même procédé qui nous a permis d'obtenir le modèle. Soit $\mathcal{E}/\mathbb{Z}_{2^d}$ un relevé canonique de $E_c/\mathbb{k}$, on sait qu'un modèle d'Edwards de $\mathcal{E}/\mathbb{Z}_{2^d}$ s'écrit

$$X^2(u) + Y^2(u) = \frac{\theta_{00}^2(0)}{\theta_{10}^2(0)} \left(1 + X^2(u) Y^2(u)\right),$$

et que l'addition $(X(u+v), Y(u+v)) = (X(u), Y(u)) + (X(v), Y(v))$ est donnée par les formules suivantes :

$$\begin{aligned} X(u+v) &= \frac{\theta_{10}(0)}{\theta_{00}(0)} \frac{X(u)X(v) - Y(u)Y(v)}{1 - X(u)X(v)Y(u)Y(v)} \\ Y(u+v) &= \frac{\theta_{10}(0)}{\theta_{00}(0)} \frac{X(u)Y(v) + Y(u)X(v)}{1 + X(u)X(v)Y(u)Y(v)}. \end{aligned}$$

Or d'après la section 7.2.1, on sait que $\dfrac{\theta_{00}^2(0)}{\theta_{10}^2(0)} = \dfrac{1 + 2(c_0 + c_2)}{1 + 2(c_0 - c_2)}$ et que nous avons le changement de variables (7.11) suivant

$$X(u) = \frac{x_u + 1}{x_u - 1}, \ X(v) = \frac{x_v + 1}{x_v - 1}, \ Y(u) = \frac{1 - y_u}{1 + y_u} \quad \text{et} \quad Y(v) = \frac{1 - y_v}{1 + y_v}.$$

Alors,

$$\begin{aligned} X(u)X(v) - Y(u)Y(v) &= (1 + 2(c_0 - c_2)) \left[(x_v + y_v)(1 + x_u y_u) + (x_u + y_u)(1 + x_v y_v)\right] \\ X(u)X(v)Y(u)Y(v) - 1 &= (1 + 2(c_0 + c_2)) \left[(x_v - y_v)(1 - x_u y_u) + (x_u - y_u)(1 - x_v y_v)\right] \\ X(u)Y(v) + Y(u)X(v) &= (1 + 2(c_0 - c_2)) \left[(1 + x_u y_u)(1 + x_v y_v) - (x_u + y_u)(x_v + y_v)\right] \\ 1 + X(u)X(v)Y(u)Y(v) &= (1 + 2(c_0 + c_2)) \left[(1 - x_u y_u)(1 - x_v y_v) + (x_u - y_u)(x_v - y_v)\right] \end{aligned}$$

Donc on obtient $X(u+v) = \dfrac{x_{u+v} + 1}{x_{u+v} - 1} = \dfrac{A_1}{B_1}$ et $Y(u+v) = \dfrac{1 - y_{u+v}}{1 + y_{u+v}} = \dfrac{A_2}{B_2}$, avec

$$\begin{aligned} A_1 &= (1 + 2(c_0 - c_2))^2 \left[(x_v + y_v)(1 + x_u y_u) + (x_u + y_u)(1 + x_v y_v)\right] \\ -B_1 &= (1 + 2(c_0 + c_2))^2 \left[(x_v - y_v)(1 - x_u y_u) + (x_u - y_u)(1 - x_v y_v)\right] \\ A_2 &= (1 + 2(c_0 - c_2))^2 \left[(1 + x_u y_u)(1 + x_v y_v) - (x_u + y_u)(x_v + y_v)\right] \\ B_2 &= (1 + 2(c_0 + c_2))^2 \left[(1 - x_u y_u)(1 - x_v y_v) + (x_u - y_u)(x_v - y_v)\right] \end{aligned}$$

Alors, on en déduit x_{u+v} et y_{u+v} avec les formules suivantes

$$x_{u+v} = \frac{A_1 - B_1}{A_1 + B_1} \text{ et } y_{u+v} = \frac{B_2 - A_2}{B_2 + A_2}.$$

Les A_i et les B_i sont à valeurs dans le corps des nombres 2−adiques. En réduisant modulo 2, on obtient les formules d'addition. Les coordonnées de l'élément neutre et les coordonnées de l'opposé d'un élément peuvent être vérifiées facilement. □

Dans les formules de la loi de groupe de notre modèle, nous remarquons que le paramètre α n'apparait pas, ce qui n'est pas étonnant d'après la remarque 7.3 et la courbe (7.15). L'addition coûte 2 inversions et 8 multiplications, tandis que la duplication coûte 2 inversions, 3 multiplications et 3 carrés du corps de définition des points.

Formules en coordonnées projectives. Posons $x = X/Z$ et $y = Y/Z$, alors le modèle projectif de la courbe est

$$E_c : c(X^2Y^2 + X^2Z^2 + Y^2Z^2 + Z^4) + XYZ^2 = 0.$$

Addition. Soient $P_i = [X_i : Y_i : Z_i]$ pour $i = 1, 2, 3$ trois points de E_c tels que $P_3 = P_1 + P_2$, alors les coordonnées de P_3 sont données par les formules suivantes :

$$\begin{aligned}
&A = Z_1Z_2, \quad B = Z_1Y_2, \quad C = Y_1Z_2, \quad D = Z_1X_2, \quad E = X_1Z_2\\
&S_1 = (A + X_1Y_2)(A + Y_1X_2), \quad S_2 = (B + C)(A + X_1X_2),\\
&T_1 = (A + Y_1Y_2)(D + E), \quad T_2 = (B + E)(C + D),\\
&X_3 = S_1T_1, \qquad Y_3 = T_2S_2, \qquad Z_3 = S_1S_2.
\end{aligned}$$

Ces formules pour l'addition coûtent 16 multiplications.

Duplication : soit $P_1 = [X_1 : Y_1 : Z_1]$ un point de la courbe d'Edwards E_c, alors les coordonnées de $P_3 = 2P_1 = [X_3 : Y_3 : Z_3]$ sont données par les formules :

$$\begin{aligned}
&A = X_1 + Y_1, \quad B = X_1 + Z_1, \quad C = Y_1 + Z_1, \quad D = X_1Y_1,\\
&E = D + Z_1^2, \quad R = CE, \quad S = Z_1AB, \quad T = BE,\\
&X_3 = X_1R^2, \quad Y_3 = Y_1S^2, \quad Z_3 = Y_1T^2.
\end{aligned}$$

Ces formules pour la duplication coûtent 8 multiplications et 4 carrés.

Points de 4−torsion : on montre facilement que les points $[1 : 0 : 0]$, $[0 : 1 : 0]$, $[0 : 1 : 1]$ et $[1 : 0 : 1]$ sont des points de 4-torsion.

Nous allons vérifier directement que la loi d'addition sur la courbe d'Edwards binaire $c(x^2y^2 + x^2 + y^2 + 1) + xy = 0$ correspond à la loi d'addition sur la courbe elliptique ordinaire $z^2 + tz = t^3 + c^4$. Pour cela, nous utiliserons le changement de coordonnées $\varphi : (x, y) \mapsto (t, z)$. Nous utilisons aussi le lemme suivant :

Lemme 7.5 *Soit $E_c : c(x^2 + y^2 + x^2y^2 + 1) + xy = 0$ une courbe d'Edwards sur un corps $\Bbbk$ de caractéristique 2. Pour tout point $P = (x, y) \in E$, on a $\varphi(-P) = -\varphi(P)$.*

Preuve : Si $P = (0,1)$, on n'a rien à démontrer. Supposons que $P \neq (0,1)$, alors on a :

$$\begin{aligned}
\varphi(-P) &= \varphi(x, 1/y) = \left(\frac{c}{x}, \frac{c}{x(y+1)} + c\right) \\
-\varphi(P) &= -\left(\frac{c}{x}, \frac{cy}{x(y+1)} + c\right) \\
&= \left(\frac{c}{x}, \frac{c}{x} + \frac{cy}{x(y+1)} + c\right) \\
&= \left(\frac{c}{x}, \frac{c}{x(y+1)} + c\right).
\end{aligned}$$

Par identification, on voit que $\varphi(-P) = -\varphi(P)$. □

Théorème 7.6 *Soit* $\Bbbk$ *un corps de caractéristique* 2 *et soit* c *un élément non nul de* $\Bbbk$. *Soient* $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ *et* $P_3 = (x_3, y_3)$ *des points de la courbe* E_c *tels que* $P_3 = P_1 + P_2$, *alors*

$$\varphi(P_3) = \varphi(P_1) + \varphi(P_2).$$

Preuve : Si $P_1 = (0,1)$ (élément neutre de E_c), alors $P_2 = P_3$. Donc $\varphi(P_1) = \varphi(0,1) = P_\infty$ et $\varphi(P_2) = \varphi(P_3)$. D'où $\varphi(P_1) + \varphi(P_2) = P_\infty + \varphi(P_3) = \varphi(P_3)$. Si $P_2 = (0,1)$, on applique la même procédure.

Si $P_3 = (0,1)$, alors $P_2 = -P_1$. D'après le lemme 7.5, on a : $\varphi(-P_1) = -\varphi(P_1)$. Donc $\varphi(P_2) = -\varphi(P_1)$. D'où $\varphi(P_1) + \varphi(P_2) = P_\infty = \varphi(P_3)$.

Supposons dans la suite que les points $P_i \neq (0,1)$ et posons $\varphi(P_i) = Q_i = (t_i, z_i)$ pour $i = 1, 2, 3$. Nous distinguons alors deux cas :
Cas 1 : $P_1 \neq P_2$ i.e. $Q_1 \neq Q_2$. Si $t_1 = t_2$, alors $Q_2 = -Q_1$. Donc $Q_2 = \varphi(P_2) = -Q_1 = -\varphi(P_1)$ or $-\varphi(P_1) = \varphi(-P_1)$. Par suite $P_2 = -P_1$, d'où $P_1 + P_2 = (0,1)$ ce qui a été déjà traité. Supposons alors que $t_1 \neq t_2$. Les formules d'addition en coordonnées de Weierstraβ donnent $Q_1 + Q_2 = Q_4$ avec $t_4 = \lambda^2 + \lambda + t_1 + t_2$ et $z_4 = \lambda(t_1 + t_4) + t_4 + z_1$ où $\lambda = (z_1 + z_2)/(t_1 + t_2)$. Un calcul fastidieux permet de voir que $Q_3 = Q_4$; pour cela nous utilisons le code Sage [Ste09] suivant :

```
R.<a,x1,y1,x2,y2> = GF(2)[]
I1 = a*(x1^2*y1^2 + x1^2 + y1^2 + 1) + x1*y1
I2 = a*(x2^2*y2^2 + x2^2 + y2^2 + 1) + x2*y2
S = R.quotient([I1,I2])
# Addition sur Edwards
x3 = (x1*y1*y2 + y1*x2*y2 + x1 + x2)/(x1*y1*x2 + x1*x2*y2 + y1 + y2)
y3 = (x1*y1 + x1*x2 + y1*y2 + x2*y2)/(x1*y1*x2*y2 + y1*x2 + x1*y2 + 1)
t3 = a/x3
z3 = a*(y3 + a*x3*(y3+1))/(x3*(y3+1))

# Addition sur la courbe elliptique
t1 = a/x1
t2 = a/x2
z1 = a*(y1 + a*x1*(y1+1))/(x1*(y1+1))
z2 = a*(y2 + a*x2*(y2+1))/(x2*(y2+1))
l = (z1 + z2)/(t1 + t2)

t4 = l^2 + l + t1 + t2
```

```
z4 = l*(t1 + t4) + t4 + z1

# Comparaison
S(numerator(u3 - u4)) == 0 # True
S(numerator(v3 - v4)) == 0 # True
```

D'où $\varphi(P_3) = \varphi(P_1) + \varphi(P_2)$.
Cas 2 : $P_1 = P_2$, on utilise le même raisonnement que le cas 1. □

Remarque 7.7 Nous pouvons « twister » le modèle d'Edwards binaire en considérant l'application $(x, y) \mapsto (x\sqrt{a}, y\sqrt{b})$ pour tout a, b. On obtiendra une courbe d'Edwards définie sur une extension quadratique $\Bbbk(\sqrt{a}, \sqrt{b})$. On prendra a et b des éléments de $\Bbbk$ qui ne sont pas des carrés, car sinon $\Bbbk(\sqrt{a}, \sqrt{b}) = \Bbbk$.

Chapitre 8

Calcul efficace en genre 2

Dans ce chapitre, comme dans le chapitre précédant, nous donnerons des formules efficaces pour représenter les jacobiennes de courbes de genre 2, grâce aux fonctions thêta du chapitre 6. Pour cela, nous manipulerons des objets directement liés aux jacobiennes des courbes qui sont les surfaces de Kummer associées. Dans ce chapitre, nous commencerons par donner la construction générale d'une variété de Kummer, puis nous donnerons des formules donnant une arithmétique efficace sur les surfaces de Kummer.

L'étude des surfaces de Kummer n'est pas nouvelle comme en témoigne le livre de Hudson [Hud05]. Cependant, leur application en cryptographie est récente [SS99, Duq04, Gau07]. Les premières applications concernent les surfaces de Kummer en caractéristique impaire, le cas de la caractéristique 2 étant plus difficile à traiter. En caractéristique 2, Gaudry et Lubicz [GL08] trouvent le modèle et les formules de la loi sur les surfaces de Kummer ordinaires grâce à la théorie générale des fonctions thêta. Parallèlement, Duquesne [Duq07, Duq08b] utilise la méthode de Cassels et Flynn [CF96] pour retrouver le modèle et les formules de la loi sur les surfaces de Kummer en caractéristique 2. Cependant, les formules de [GL08], valables dans le cas ordinaire, sont plus efficaces que les formules de [Duq07, Duq08b].

8.1 Variétés de Kummer

Soit $(A, +)$ une variété abélienne de dimension g définie sur un corps quelconque $\Bbbk$. La variété de Kummer, notée $\mathcal{K}_A$ associée à A est définie par le quotient

$$\mathcal{K}_A := \frac{A}{\pm} := \{a \in A \,|\, a = -a\}.$$

La dimension de $\mathcal{K}_A$ est égale à g et si $g = 2$, on dit que $\mathcal{K}_A$ est la *surface de Kummer* associée à A. La loi d'addition de A n'induit pas une loi de groupe sur la variété de Kummer $\mathcal{K}_A$, mais une loi de semigroupe. En effet pour $a, b \in \mathcal{K}_A$, on ne peut pas décider entre $a + b = -(a + b)$ et $a - b = -a + b$ ce qui va représenter la somme de a et de b. Mais dès qu'on connait $a - b \in \mathcal{K}_A$, il est possible de calculer $a + b \in \mathcal{K}_A$ et vice-versa. La loi sur la variété de Kummer $\mathcal{K}_A$ permet ainsi d'utiliser l'algorithmique d'exponentiation : étant donné un entier n et un élément $a \in \mathcal{K}_A$, il est facile de calculer de proche en proche na. Ainsi, le problème du logarithme discret dans A a un équivalent algorithmique dans $\mathcal{K}_A$. Autrement dit, nous pouvons implémenter des protocoles cryptographiques en utilisant les variétés de Kummer $\mathcal{K}_A$.

8.2 Surfaces de Kummer en caractéristique impaire

Soit C une courbe hyperelliptique de genre g définie sur un corps fini $\Bbbk$ de caractéristique impaire, la surface de Kummer associée à la courbe C est la surface de Kummer associée à sa jacobienne J_C. Dans [Gau07], Gaudry utilise les fonctions thêta pour construire le modèle et la loi de semigroupe de la surface de Kummer associée à C.

Considérons les coordonnées $[x : y : z : t]$ de l'espace projectif $\mathbb{P}^3$, alors un modèle projectif d'une surface de Kummer sur $\Bbbk$ est donné par :

$$(x^4 + y^4 + z^4 + t^4) + 2\delta xyzt + \alpha(x^2t^2 + y^2z^2) + \beta(x^2z^2 + y^2t^2) + \gamma(x^2y^2 + z^2t^2) = 0. \tag{8.1}$$

avec les coefficients α, β, γ et δ dans $\Bbbk$ (voir [Gau07] pour plus de détails). Gaudry donne aussi les formules de la loi de semigroupe de (8.1) grâce aux formules d'addition et de duplication des fonctions thêta.

---

algorithme : **Duplication sur la surface de Kummer (8.1)**

Entrée Un point $P = [x : y : z : t]$ de (8.1)

Sortie : Le point $2P = [X : Y : Z : T]$ de (8.1)

1. $x' = (x^2 + y^2 + z^2 + t^2)^2/A^2$; $\quad y' = (x^2 + y^2 - z^2 - t^2)^2/B^2$;
2. $z' = (x^2 - y^2 + z^2 - t^2)^2/C^2$; $\quad t' = (x^2 - y^2 - z^2 + t^2)^2/D^2$;
3. $X = (x' + y' + z' + t')/a$; $\quad Y = (x' + y' - z' - t')/b$;
4. $Z = (x' - y' + z' - t')/c$; $\quad T = (x' - y' - z' + t')/d$;
5. Retourner $2P = [X : Y : Z : T]$.

---

algorithme : **Addition sur la surface de Kummer (8.1)**

Entrée $P_1 = [x_1 : y_1 : z_1 : t_1], P_2 = [x_2 : y_2 : z_2 : t_2]$ et $P - Q = [x_3 : y_3 : z_3 : t_3]$ de (8.1)

Sortie Le point $P_3 = P_1 + P_2 = [X : Y : Z : T]$

1. $x' = (x_1^2 + y_1^2 + z_1^2 + t_1^2)(x_2^2 + y_2^2 + z_2^2 + t_2^2)/A^2$;
2. $y' = (x_1^2 + y_1^2 - z_1^2 - t_1^2)(x_2^2 + y_2^2 - z_2^2 - t_2^2)/B^2$;
3. $z' = (x_1^2 - y_1^2 + z_1^2 - t_1^2)(x_2^2 - y_2^2 + z_2^2 - t_2^2)/C^2$;
4. $t' = (x_1^2 - y_1^2 - z_1^2 + t_1^2)(x_2^2 - y_2^2 - z_2^2 + t_2^2)/D^2$;
5. $X = (x' + y' + z' + t')/x_3$; $\quad Y = (x' + y' - z' - t')/y_3$;
6. $Z = (x' - y' + z' - t')/z_3$; $\quad T = (x' - y' - z' + t')/t_3$;
7. Retourner $P_3 = [X : Y : Z : T]$.

Les coefficients a, b, c, d, A, B, C et D ne dépendent que des coefficients α, β, γ et δ de la surface (8.1). Nous renvoyons le lecteur à [Gau07] pour plus de détails.

8.3 Surface de Kummer en caractéristique deux

Le cas de la caractéristique deux est très difficile à traiter car la réduction modulo 2 du schéma (8.1) sur une extension non ramifiée de $\mathbb{Z}_2$ donne une variété singulière en tout point. Pour traiter ce problème de mauvaise réduction, Gaudry et Lubicz [GL08] utilisent

des techniques de résolution des singularités arithmétiques. Ils obtiennent ainsi le modèle et la loi de semigroupe pour des surfaces de Kummer ordinaires. Le cas des surfaces de Kummer non-ordinaires étant plus difficile. Pour résoudre ce problème, nous allons plonger les courbes non-ordinaires dans une famille de courbes ordinaires comme dans [LP02, LP04], c'est le problème de la théorie des courbes modulaires. Il s'agit de considérer la surface de Kummer sur un anneau de séries formelles défini sur un corps fini de caractéristique 2 dont la fibre générique est ordinaire mais la fibre spéciale est non-ordinaire. On peut alors construire un système de coordonnées qui par réduction sur le fibre spéciale donne un modèle pour une surface de Kummer non-ordinaire. La loi de semigroupe s'obtient de la même manière par réduction sur la fibre spéciale.

Notons que Ducrohet [Duc08] exhibe en plus le modèle de la surface de Kummer supersingulière (qui est le même que celui de Duquesne [Duq07, Duq08b]) même si Duquesne [Duq07, Duq08b] retrouve le modèle et les formules de la loi de semigroupe en utilisant la technique de Cassels et Flynn [CF96, chapitre 3]. Les formules de Duquesne ont été généralisées par Müller [Mul10]. Nous n'allons pas utiliser les formules de la loi de semigroupe de Duquesne, mais juste ses modèles de surfaces de Kummer non-ordinaires en caractéristique 2.

8.3.1 Cas des surfaces ordinaires

Gaudry et Lubicz [GL08] donnent un modèle et la loi de semigroupe pour les surfaces de Kummer ordinaires définies sur un corps de caractéristique deux.

Soit J une surface abélienne définie sur un corps fini $\Bbbk$ de caractéristique 2 et de degré d'extension absolue d. Considérons le relevé canonique $\mathcal{J}$ de J sur le corps de caractéristique zéro $\mathbb{Q}_{2^d}$ que l'on peut plonger dans $\mathbb{C}$ (voir [Rob00, p. 144-145]). On peut alors construire la surface de Kummer $\mathcal{K}_{\mathcal{J}}$ de $\mathcal{J}/\mathbb{C}$. La réduction modulo 2 de $\mathcal{K}_{\mathcal{J}}$ donne une surface non réduite. Pour résoudre les problèmes de mauvaise réduction de la fibre spéciale de $\mathcal{K}_{\mathcal{J}}$, on utilise un changement de variables adéquat dans l'équation (8.1), comme dans la section 7.2 (pour plus de détails, voir [GL08]).

Modèle. Le modèle de Weierstraβ d'une courbe ordinaire C définie sur la clôture algébrique $\overline{\Bbbk}$ peut s'écrire sous la forme de

$$C : y^2 + x(x+1)y \;=\; x(x+1)\left[ax^3 + (a+b)x^2 + cx + c\right] \text{ avec } abc \in \overline{\Bbbk} \smallsetminus \{0\}.$$

Soit $[x : y : z : t]$ le vecteur des coordonnées de l'espace projectif $\mathbb{P}^3$, le modèle projectif de la surface de Kummer associée à la courbe C est alors

$$\mathcal{K}_C \;:\; c(x^2z^2 + y^2t^2) + b(x^2y^2 + z^2t^2) + a(x^2t^2 + y^2z^2) + xyzt \;=\; 0.$$

Arithmétique. Soient $P = [x_1 : y_1 : z_1 : t_1]$ et $Q = [x_2 : y_2 : z_2 : t_2]$ deux points projectifs de la surface de Kummer ordinaire $\mathcal{K}_C$. Posons $P - Q = [x_3 : y_3 : z_3 : t_3]$. Alors les coordonnées de $2P = [X_3 : Y_3 : Z_3 : T_3]$ et de $P + Q = [X'_3 : Y'_3 : Z'_3 : T'_3]$ sont données par les formules suivantes (cf [GL08]) :

$$\begin{array}{l|l}
X_3 = \alpha_0(x_1^2 + y_1^2 + z_1^2 + t_1^2)^2 & X'_3 = (x_1x_2 + y_1y_2 + z_1z_2 + t_1t_2)^2/x_3 \\
Y_3 = \alpha_1(x_1y_1 + z_1t_1)^2 & Y'_3 = (x_1y_2 + y_1x_2 + z_1t_2 + t_1z_2)^2/y_3 \\
Z_3 = \alpha_2(x_1z_1 + y_1t_1)^2 & Z'_3 = (x_1z_2 + y_1t_2 + z_1x_2 + t_1y_2)^2/z_3 \\
T_3 = \alpha_3(x_1t_1 + y_1z_1)^2 & T'_3 = (x_1t_2 + y_1z_2 + z_1y_2 + t_1x_2)^2/t_3 \\
\textbf{Duplication} & \textbf{Addition}
\end{array} . \tag{8.2}$$

avec $\alpha_0 = \sqrt{abc}, \alpha_1 = \sqrt{b}, \alpha_2 = \sqrt{c}$ et $\alpha_3 = \sqrt{a}$ des constantes ne dépendant que de l'équation de la surface $\mathcal{K}_C$. La duplication et l'addition peuvent être représentées par la figure 8.1.

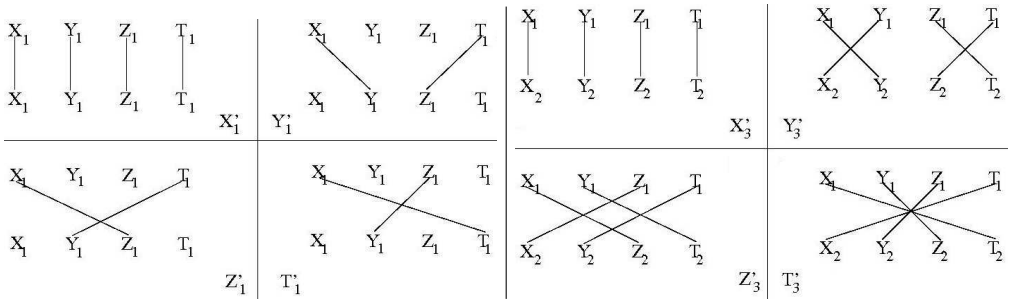

FIG. 8.1 – Duplication et addition de la surface de Kummer ordinaire

8.3.2 Cas des surfaces non-ordinaires

Dans cette partie, nous faisons des calculs sur une surface de Kummer non-ordinaire en caractéristique 2. Soient $\mathbb{k}$ un corps fini de caractéristique 2 et C une courbe non-ordinaire de genre 2 définie sur $\mathbb{k}$, mais que nous considérons sur la clôture algébrique $\overline{\mathbb{k}}$. Comme nous aurons à traiter le cas de courbes de p-rang 0 ou 1, nous aurons à considérer deux équations de la courbe C dont les modèles de Weierstraβ sont données par les équations (voir la section 1.2) :

$$y^2 + y = x^5 + \mu^2 x^3 \text{ avec } \mu \in \overline{\mathbb{k}} - \{0\}; \tag{8.3}$$

$$y^2 + xy = \lambda x^5 + \mu x^3 + x, \text{ avec } \lambda, \mu \in \overline{\mathbb{k}} \text{ et } \lambda \neq 0. \tag{8.4}$$

La courbe (8.3) est supersingulière, i.e. de $p-$rang 0, tandis que la courbe (8.4) est de $p-$rang 1. Comme la clôture algébrique est de degré infini, nous allons juste nous placer dans une extension finie de $\mathbb{k}$ contenant tous les coefficients. Les surfaces de Kummer des courbes (8.3) et (8.4) ont été étudiées respectivement par Ducrohet [Duc08] et Laszlo et Pauly [LP04].

En fait, pour chacune des courbes (8.3) et (8.4), on peut construire sur une extension finie de l'anneau des séries formelles $\mathbb{k}[[s]]$ (que l'on munit de sa valuation $s-$adique naturelle), une courbes de genre 2 telle que : la fibre générique soit ordinaire et que la fibre spéciale soit isomorphe respectivement à la courbe (8.3) [Duc08] ou (8.4) [LP04]. Pour la théorie générale des schémas et des fibres voir le livre de Hartshorne [Har77].

Ducrohet [Duc08] utilise en plus une variable $\varepsilon \in \mathbb{k}[[s]]$ différente de 0 et 1, de valuation nulle. Les deux courbes sur $\mathbb{k}[[s]]$ qu'ils construisent sont données par :

(1) Pour la courbe (8.3) de $p-$rang zéro, on pose

$$\mathcal{C}_s : y^2 + (s^2x + 1)(s^2\varepsilon^2 x + 1)y = x^5 + \mu^2 x^3.$$

(2) Pour la courbe (8.4) de $p-$rang égal à 1, suivant [LP04], on pose

$$\mathcal{C'}_s : y^2 + (sx^2 + x)y = \lambda x^5 + \mu x^3 + x.$$

Pour $s = 0$, les fibres spéciales $\mathcal{C}_0/\mathbb{k}$ et $\mathcal{C'}_0/\mathbb{k}$ sont égales respectivement aux courbes (8.3) et (8.4), et les fibres génériques $\mathcal{C}_s$ et $\mathcal{C'}_s$ sont isomorphes à des courbes ordinaires

sur une extension quadratique de $\mathbb{k}((s))$ (en fait, $\mathcal{C}_s$ et $\mathcal{C}'_s$ sont des twistes d'une courbe ordinaire définie sur $\mathbb{k}$).

Nous allons décrire des modèles ainsi que l'arithmétique des surfaces de Kummer associées à chacune des courbes (8.3) et (8.4).

8.3.3 Surface de Kummer supersingulière

Modèle. Nous considérons la courbe supersingulière $\mathcal{C} : y^2+y = x^5+\mu^2x^3$ définie sur $\overline{\mathbb{k}}$ comme la fibre spéciale de la courbe ordinaire $\mathcal{C}_s : y^2+(s^2x+1)(s^2\varepsilon^2x+1)y = x^5+\mu^2x^3$ définie sur l'anneau $\overline{\mathbb{k}}[[s]]$.

La fibre générique de $\mathcal{C}_s$ est isomorphe à un twist de courbe ordinaire sur $\mathbb{k}((s))$ donnée par l'équation $C : w^2 + z(z+1)y = z(z+1)\left[a_sz^3 + (a_s+b_s)z^2 + c_sz + c_s\right]$, avec

$$\begin{cases} a_s &= \dfrac{1+\varepsilon^2}{s^{10}\varepsilon^6}, \\ b_s &= \dfrac{1+\nu_1^6}{s^{10}\varepsilon^6(1+\varepsilon)^6}, \quad \text{avec } \nu_1 = \mu^2s^4\varepsilon^4 + s^5\varepsilon^3(1+\varepsilon^2)(1+\mu s^2\varepsilon^2) \\ c_s &= \dfrac{\varepsilon^2(1+\nu_0^6)}{s^{10}(1+\varepsilon)^6}, \quad \text{avec } \nu_0 = \mu^2s^4 + s^5(1+\varepsilon^2)(1+\mu s^2). \end{cases} \tag{8.5}$$

Posons $\tau_0 = \dfrac{1}{\sqrt{1+\nu_0}}$ et $\tau_1 = \dfrac{1}{\sqrt{1+\nu_1}}$. Désormais, nous confondons les points de la courbe C et les points de la fibre générique $\mathcal{C}_s$, ce que l'on représente en mettant l'indice s sur les points de C. Comme les points de Weierstraβ sont les points invariants par l'involution hyperelliptique, alors la projection canonique $\varphi : C \to \mathbb{P}^1(\overline{\mathbb{k}})$, $\varphi(x_s, y_s) = x_s$ admet trois points de Weierstraβ que l'on peut noter par $0_s, 1_s$ et ∞_s.

Notons par $\mathrm{Sym}(C)$, l'ensemble des fonctions de $C \times C$ invariantes par permutation des copies de C dans $C \times C$ et considérons l'application birationnelle d'Abel-Jacobi :

$$\begin{array}{rccl} AJ : & \mathrm{Sym}(C) & \to & J_C \\ & P+Q & \mapsto & (P)+(Q)-(\omega), \end{array}$$

où ω est le diviseur canonique de degré 2 (d'après le théorème de Riemann-Roch). Les points non-nuls de 2−torsion de $J_C[2]$ sont images par l'application d'Abel-Jacobi des diviseurs

$$(0_s) := AJ(1_s + \infty_s), \quad (1_s) := AJ(0_s + \infty_s) \quad \text{et} \quad (\infty_s) := AJ(0_s + 1_s).$$

On peut associer à cette paramétrisation de la 2−torsion de J_C, une base canonique des fonctions thêta que l'on note X_B, X_0, X_1, X_∞. On peut calculer les pullbacks des fonctions rationnelles $\dfrac{X_B}{X_\infty}, \dfrac{X_0}{X_\infty}$, et $\dfrac{X_1}{X_\infty}$ par l'application d'Abel-Jacobi AJ ce qui donne :

$$\begin{aligned}
F_B := AJ^*\left(\frac{X_B}{X_\infty}\right) &= \tau_0\tau_1\frac{1}{q(x_{1,s})q(x_{2,s})}\left[s^6\varepsilon^2(1+\varepsilon^2)\left(\frac{q(x_{1,s})y_{2,s}+q(x_{2,s})x_{1,s}}{x_{1,s}+x_{2,s}}\right)^2\right.\\
&\quad +s^8\left(\frac{1+\varepsilon^{10}}{1+\varepsilon^2}+\mu^2s^4\varepsilon^4\frac{1+\varepsilon^6}{1+\varepsilon^2}\right)(x_{1,s}x_{2,s})^2\\
&\quad \left.+\,s^4\left(\frac{1+\varepsilon^6}{1+\varepsilon^2}+\mu^2s^4\varepsilon^4\right)(x_{1,s}+x_{2,s})^2+(1+\mu^2s^4\varepsilon^2)\right],\\
F_0 := AJ^*\left(\frac{X_0}{X_\infty}\right) &= \tau_0\left[1+s^2(x_{1,s}+x_{2,s})+s^4x_{1,s}x_{2,s}\right],\\
F_1 := AJ^*\left(\frac{X_1}{X_\infty}\right) &= \tau_1\left[1+s^2\varepsilon^2(x_{1,s}+x_{2,s})+s^4\varepsilon^4x_{1,s}x_{2,s}\right].
\end{aligned}$$

Il est facile de voir que les trois précédentes fonctions se réduisent à l'unité 1 sur la fibre spéciale et donc ne forment pas une $\overline{\mathbb{k}}[[s]]$-base d'un système de coordonnées projectives de J_C.

Par ailleurs, on peut construire les pullback par AJ d'une $k[[s]]$-base des section globales de $J_{\mathcal{C}_s}$ en considérant des fonctions symétriques. En effet, les trois fonctions symétriques $1, x_{1,s}+x_{2,s}$ et $x_{1,s}x_{2,s}$ sont linéairement indépendantes. On peut alors compléter ces trois fonctions par une fonction symétrique f pour avoir une base $\{1, x_{1,s}+x_{2,s}, x_{1,s}x_{2,s}, f\}$ de coordonnées homogènes de l'espace projectif $\mathbb{P}^3(\mathbb{k}[[s]])$. Notons $u_{1,s}, u_{2,s}, u_{3,s}$ et $u_{4,s}$ la base canonique des fonctions thêtas. Cette base est liée à la base des coordonnées homogènes grâce au lemme suivant :

Lemme 8.1 *[Duc08, prop. 3.7] Considérons les coordonnées homogènes $\{x,y,z,t\}$ de l'espace projectif $\mathbb{P}^3(\mathbb{k}[[s]])$, et la base thêta canonique $\{u_{1,s},u_{2,s},u_{3,s},u_{4,s}\}$. La transformation suivante donne un changement de base entre les coordonnées thêta et les coordonnées homogènes :*

$$\left\{\begin{array}{lcl}
u_{1,s} &=& x\\
u_{2,s} &=& \tau_1^2(x+s^4\varepsilon^4y+s^8\varepsilon^8z)\\
u_{3,s} &=& \tau_0^2(x+s^4y+s^8z)\\
u_{4,s} &=& (\tau_0\tau_1)^2\left[(1+\mu^2s^4\varepsilon^2)^2x+s^4(1+\varepsilon^2)^2y+s^8(1+\varepsilon^4)^2z+s^{12}\varepsilon^{12}(1+\varepsilon^2)^2t\right]
\end{array}\right. \tag{8.6}$$

et l'inverse est donné par :

$$\left\{\begin{array}{lcl}
x &=& u_{1,s}\\
y &=& \dfrac{1}{(s^2\varepsilon^2\tau_0\tau_1(1+\varepsilon^2))^2}\left[(1+\varepsilon^4)^2\tau_0^2\tau_1^2u_{1,s}+\tau_0^2u_{2,s}+\varepsilon^8\tau_1^2u_{3,s}\right]\\
z &=& \dfrac{1}{(s^4\varepsilon^2\tau_0\tau_1(1+\varepsilon^2))^2}\left[(1+\varepsilon^2)^2\tau_0^2\tau_1^2u_{1,s}+\tau_0^2u_{2,s}+\varepsilon^4\tau_1^2u_{3,s}\right]\\
t &=& \dfrac{1}{(s^6\varepsilon^2\tau_0\tau_1(1+\varepsilon^2))^2}\left[(1+\mu^2s^4\varepsilon^2)^2\tau_0^2\tau_1^2u_{1,s}+\tau_0^2u_{2,s}+\tau_1^2u_{3,s}+u_{4,s}\right]
\end{array}\right. . \tag{8.7}$$

Le lemme précédent permet d'obtenir un modèle pour les surfaces de Kummer supersingulières en réduisant modulo s l'équation obtenue sur la $k[[s]]$-base $\{x,y,z,t\}$. On obtient qu'un modèle projectif de la surface de Kummer associée à la courbe supersingulière est :

$$\mathcal{K}_C \;:\; \mu^2x^3y+x^3t+x^2yz+\mu^4x^2z^2+xy^3+y^2t^2+z^4=0.$$

Arithmétique. Nous allons montrer que $\mathcal{K}_C$ est un semigroupe. Pour cela, soient $P = [x_1 : y_1 : z_1 : t_1]$ et $Q = [x_2 : y_2 : z_2 : t_2]$ deux points de la surface de Kummer supersingulière $\mathcal{K}_C$. Posons $P - Q = [x_3 : y_3 : z_3 : t_3] \in \mathcal{K}_C$. Alors les coordonnées de $2P = [X_3 : Y_3 : Z_3 : T_3]$ et de $P + Q = [X'_3 : Y'_3 : Z'_3 : T'_3]$ sont données par les formules suivantes :

$$\textbf{Duplication} \begin{cases} X_3 = (\mu x_1 + y_1)^4 \\ Y_3 = x_1^4 \\ Z_3 = (x_1 z_1 + y_1 t_1)^2 \\ T_3 = (\mu^2 z_1^2 + \mu x_1^2 + x_1 y_1 + t_1^2)^2 \end{cases}$$

$$\textbf{addition} \begin{cases} A &= (x_1 t_2 + y_1 z_2 + z_1 y_2 + t_1 x_2)^2 \\ B &= (x_1 y_2 + y_1 x_2)^2 \\ C &= \mu^4 (t_1 x_2 + x_1 z_2)^2 + (t_1 y_2 + y_1 t_2)^2 \\ D &= (\mu x_2 + y_2)(\mu x_1 + y_1) \\ E_1 &= y_3^2 + x_3 z_3 \\ E_2 &= y_3^3 + x_3^2 t_3 \\ X'_3 &= A/x_3 \\ Y'_3 &= (y_3 A + x_3 B)/x_3^2 \\ Z'_3 &= (E_1 A + x_3 y_3 B + x_3^2 C)/x_3^3 \\ T'_3 &= (A E_2 + x_3 E_1 B + x_3^2 y_3 C + x_3^3 D^2)/x_3^4 \end{cases} .$$

L'élément neutre de la loi de semigroupe est $[1 : 0 : 0 : 0]$.

Complexité. La duplication coûte 5 multiplications et 7 carrés. Pour l'addition, on peut utiliser les formules suivantes :
$L_1 = x_1 x_2,\ L_2 = y_1 y_2,\ L_3 = z_1 z_2,\ L_4 = t_1 t_2,$
$T_1 = (x_1 + y_1)(x_2 + y_2),\ T_2 = (x_1 + z_1)(x_2 + z_2)$
$M_1 = (y_1 + z_1 + t_1)(y_2 + z_2 + t_2),\ M_2 = (x_1 + y_1 + t_1)(x_3 + y_3 + t_2),$
$M_3 = (x_1 + z_1 + t_1)(x_1 + z_1 + t_1),\ N = (x_1 + y_1 + z_1 + t_1)(x_2 + y_2 + z_2 + t_2),$
$A = (L_1 + L_4 + M_2 + M_3 + N)^2,\ B = (L_1 + L_2 + T_1)^2,$
$C = (L_2 + L_4 + M_1 + M_2 + N + (\mu^2 + 1)(T_3 + L_1 + L_3))^2,$
$D = ((\mu + 1)(\mu L_1 + L_2) + \mu T_1)^2,$
et les coordonnées de la somme sont données par :

$$\begin{cases} X'_3 &= A/x_3 \\ Y'_3 &= (y_3 X'_3 + B)/x_3 \\ Z'_3 &= (z_3 X'_3 + y_3 Y'_3 + C)/x_3 \\ T'_3 &= (t_3 X'_3 + z_3 Y'_3 + y_3 Z'_3 + D)/x_3 \end{cases} .$$

Alors l'addition coûte 20 multiplications et 4 carrés (comme on est en coordonnées projectives). Si $\mu = 1$, cette complexité descend jusqu'à 16 multiplications et 4 carrés.

Vérification de l'addition. Le code `sagemath` [Ste09] suivant permet de vérifier que l'addition est une loi interne.

```
R.<mu,x1,y1,z1,t1,x2,y2,z2,t2,x3,y3,z3,t3> = GF(2)[]
EqP = mu^4*x1^2*z1^2 + mu^2*x1^3*y1 + x1*y1^3 + x1^2*y1*z1\
    + z1^4 + x1^3*t1 + y1^2*t1^2
EqQ = mu^4*x2^2*z2^2 + mu^2*x2^3*y2 + x2*y2^3 + x2^2*y2*z2\
    + z2^4 + x2^3*t2 + y2^2*t2^2
EqR = mu^4*x3^2*z3^2 + mu^2*x3^3*y3 + x3*y3^3 + x3^2*y3*z3\
```

```
    + z3^4 + x3^3*t3 + y3^2*t3^2
A = (x1*t2 + y1*z2 + z1*y2 + t1*x2)^2
B = (x1*y2 + y1*x2)^2
C = mu^4*(t1*x2 + x1*z2)^2 + (t1*y2 + y1*t2)^2
D = (mu*x2 + y2)*(mu*x1 + y1)
E = (y3^2 + x3*z3)
X3 = A/x3
Y3 = (z2*A + x3*B)/x3^2
Z3 = (E*A + x3*y3*B + x3^2*C)/x3^3
T3 = (A*(y3^3 + x3^2*t3) + x3*E*B + x3^2*y3*C + x3^3*D^2)/x3^4
EqS = mu^4*X3^2*Z3^2 + mu^2*X3^3*Y3 + X3*Y3^3 + X3^2*Y3*Z3\
    + Z3^4 + X3^3*T3 + Y3^2*T3^2
EqS%(EqP*EqQ*EqR) == 0
```

Preuve de la loi de semigroupe. La preuve de la duplication de la proposition 8.3.3 est faite par Ducrohet [Duc08], nous n'allons prouver que la loi d'addition du semigroupe.

Considérons les points $U = [u_{1,s} : u_{2,s} : u_{3,s} : u_{4,s}], V = [v_{1,s} : v_{2,s} : v_{3,s} : v_{4,s}]$ et $W = [w_{1,s} : w_{2,s} : w_{3,s} : w_{4,s}]$ de la surface ordinaire $\mathcal{K}_{\mathcal{C}_s}$ les antécédents des points P, Q et R donnés par le changement de variables (8.6). Sur la surface de Kummer ordinaire $\mathcal{K}_{\mathcal{C}_s}$, nous avons les formules d'addition (8.2) suivantes (attention aux changement de notation) :

$$\left\{\begin{array}{lcl} u'_{3,s} & = & (u_{1,s}v_{1,s} + u_{2,s}v_{2,s} + u_{3,s}v_{3,s} + u_{4,s}v_{4,s})^2/w_{1,s} \\ u'_{3,s} & = & (u_{1,s}v_{2,s} + u_{2,s}v_{1,s} + u_{3,s}v_{4,s} + u_{4,s}v_{3,s})^2/w_{2,s} \\ u'_{3,s} & = & (u_{1,s}v_{3,s} + u_{2,s}v_{4,s} + u_{3,s}v_{1,s} + u_{4,s}v_{2,s})^2/w_{3,s} \\ u'_{3,s} & = & (u_{1,s}v_{4,s} + u_{2,s}v_{3,s} + u_{3,s}v_{2,s} + u_{4,s}v_{1,s})^2/w_{4,s} \end{array}\right. .$$

Alors, il suffit de calculer les $u'_{i,s}$ pour $i = 1, 2, 3, 4$. Soient $S_{i,s}$, pour $i = 1, 2, 3, 4$, les images des $u'_{i,s}$ par l'application (8.7), alors

$$\left\{\begin{array}{lcl} S_{1,s} & = & u'_{1,s} \\ S_{2,s} & = & \dfrac{1}{(s^2\varepsilon^2\tau_0\tau_1(1+\varepsilon^2))^2}\left[(1+\varepsilon^4)^2\tau_0^2\tau_1^2u'_{1,s} + \tau_0^2u'_{2,s} + \varepsilon^8\tau_1^2u'_{3,s}\right] \\ S_{3,s} & = & \dfrac{1}{(s^4\varepsilon^2\tau_0\tau_1(1+\varepsilon^2))^2}\left[(1+\varepsilon^2)^2\tau_0^2\tau_1^2u'_{1,s} + \tau_0^2u'_{2,s} + \varepsilon^4\tau_1^2u'_{3,s}\right] \\ S_{4,s} & = & \dfrac{1}{(s^6\varepsilon^2\tau_0\tau_1(1+\varepsilon^2))^2}\left[(1+\mu^2s^4\varepsilon^2)^2\tau_0^2\tau_1^2u'_{1,s} + \tau_0^2u'_{2,s} + \tau_1^2u'_{3,s} + u's_{4,s}\right] \end{array}\right. .$$

Après calcul et factorisation de chaque $S_{i,s}$, on trouve les formules d'addition en spécialisant $s = 0$, i.e. en calculant $S_{i,0}$ pour $i = 1, 2, 3, 4$. Les calculs peuvent se faire grâce au script `sagemath` [Ste09] suivant :

```
R.<s,mu,e,x1,y1,z1,t1,x2,y2,z2,t2,x3,y3,z3,t3> = GF(2)[]
v0 = mu^2*s^4+s^5*(1+e^2)*(1+mu*s^2)
v1 = mu^2*s^4*e^4 + s^5*e^3*(1+e^2)*(1+mu*s^2*e^2)
Tau0 = 1/(1+v0)
Tau1 = 1/(1+v1)

u1 = x1
u2 = Tau1*(x1 + (s^2*e^2)^2*y1 + (s^4*e^4)^2*z1)
u3 = Tau0*(x1 + (s^2)^2*y1 + (s^4)^2*z1)
```

```
u4 = (Tau0*Tau1)*((1+mu^2*s^4*e^2)^2*x1 + (s^2*(1+e^2))^2*y1\
     + (s^4*(1+e^4))^2*z1 + (s^6*e^2*(1+e^2))^2*t1)

v1 = x2
v2 = Tau1*(x2 + (s^2*e^2)^2*y2 + (s^4*e^4)^2*z2)
v3 = Tau0*(x2 + (s^2)^2*y2 + (s^4)^2*z2)
v4 = (Tau0*Tau1)*((1+mu^2*s^4*e^2)^2*x2 + (s^2*(1+e^2))^2*y2\
      + (s^4*(1+e^4))^2*z2 + (s^6*e^2*(1+e^2))^2*t2)

w1 = x3
w2 = Tau1*(x3 + (s^2*e^2)^2*y3 + (s^4*e^4)^2*z3)
w3 = Tau0*(x1 + (s^2)^2*y3 + (s^4)^2*z3)
w4 = (Tau0*Tau1)*((1+mu^2*s^4*e^2)^2*x3 + (s^2*(1+e^2))^2*y3 \
      + (s^4*(1+e^4))^2*z3 + (s^6*e^2*(1+e^2))^2*t3)

u_1=(u1*v1 + u2*v2 + u3*v3 + u4*v4)^2/w1
u_2=(u1*v2 + u2*v1 + u3*v4 + u4*v3)^2/w2
u_3=(u1*v3 + u2*v4 + u3*v1 + u4*v2)^2/w3
u_4=(u1*v4 + u2*v3 + u3*v2 + u4*v1)^2/w4

# Utilisation de l'inverse
S1 = u_1
S2 = (u_1*((e^4 + 1)^2*Tau0*Tau1) + u_2*Tau0\
      + (e^4)^2*u_3*Tau1)/((s^2*e^2*(e^2 + 1))^2*Tau0*Tau1)
S3 = (u_1*((e^2 + 1)^2*Tau0*Tau1) + u_2*Tau0\
      + (e^2)^2*u_3*Tau1)/((s^4*e^2*(e^2 + 1))^2*Tau0*Tau1)
S4 = (u_1*((mu^2*s^4*e^2 + 1)^2*Tau0*Tau1) + u_2*Tau0\
      + u_3*Tau1 + u_4)/((s^6*e^2*(e^2 + 1))^2*Tau0*Tau1)
```

Ce qui permet de déduire les formules de la loi de semigroupe. □

8.3.4 Surface de Kummer de $p-$rang 1

Modèle. Le modèle de Weierstraβ de la courbe hyperelliptique de $p-$rang 1 est donné par l'équation $\mathcal{C}' : y^2 + xy = \lambda x^5 + \mu x^3 + x$, avec $\lambda, \mu \in \overline{\mathbb{k}}$ et $\lambda \neq 0$. On peut considérer la courbe $\mathcal{C}'$ comme la fibre spéciale de la courbe $\mathcal{C}'_s$ sur l'anneau de séries formelles $\overline{\mathbb{k}}[[s]]$, donnée par l'équation $\mathcal{C}'_s : y^2 + (sx^2 + x)y = \lambda x^5 + \mu x^3 + x$. Comme pour le modèle supersingulier, la courbe $\mathcal{C}'_s$ est un twist d'une courbe ordinaire (8.2) avec

$$a_s = \lambda/s^3, \quad b_s = \alpha^2 + \alpha, \quad c_s = s \quad \text{et} \quad \alpha^2 = a_s + c_s + \mu/s. \tag{8.8}$$

Considérons la base canonique des fonctions thêta $[u_{1,s}, u_{2,s}, u_{3,s}, u_{4,s}]$ de la courbe $\mathcal{C}'_s$ et la base des coordonnées homogènes $[x, y, z, t]$ sur $\mathbb{P}^3(\mathbb{k}[[s]])$. Les formules suivantes donnent l'application de changement de bases ([LP04, section 4.4])

$$\begin{cases} u_{1,s} &= (1 + s'^3 + s'^4 + s'^5)^2 x \\ u_{2,s} &= (1 + s'^3 + s'^4 + s'^5)^2 y \\ u_{3,s} &= x + s'^8 z \\ u_{4,s} &= y + s'^8 t \end{cases}, \tag{8.9}$$

avec $s = s'^4$. Nous pouvons alors utiliser la même technique que celle de la sous-section 8.3.3 avec le changement de variables (8.9) et des relations (8.8). Ceci nous permet de donner un modèle projectif de la surface de Kummer associée à la courbe de $p-$rang 1 :

$$\mathcal{K}_{\mathcal{C}'} \quad : \quad x^4 + x^2yt + \mu^2x^2y^2 + \lambda xy^2z + \lambda^2y^4 + z^2t^2 = 0.$$

Arithmétique. Comme dans la section précédente, nous allons montrer que la surface de Kummer $\mathcal{K}_{\mathcal{C}'}$ est un semigroupe. Pour cela, soient $P = [x_1 : y_1 : z_1 : t_1]$ et $Q = [x_2 : y_2 : z_2 : t_2]$ deux points de la surface de Kummer supersingulière $\mathcal{K}_{\mathcal{C}'}$. Posons $P - Q = [x_3 : y_3 : z_3 : t_3]$ un point de $\mathcal{K}_{\mathcal{C}'}$. Alors les coordonnées de $2P = [X_3 : Y_3 : Z_3 : T_3]$ et de $P + Q = [X'_3 : Y'_3 : Z'_3 : T'_3]$ sont données par les formules suivantes :

$$\textbf{Duplication} \begin{cases} X_3 &= \lambda_1(x_1 + y_1)^4 \\ Y_3 &= \lambda_2(x_1 + y_1 + z_1 + t_1)^4 \\ Z_3 &= \lambda_3(x_1t_1 + y_1z_1)^2 \\ T_3 &= \lambda_4(x_1y_1)^2 \end{cases}$$

$$\textbf{Addition} \begin{cases} A &= (x_1z_2 + y_1t_2 + z_1x_2 + t_1y_2)^2 \\ B &= (x_1t_2 + y_1z_2 + z_1y_2 + t_1x_2)^2 \\ C &= (x_1y_2 + y_1x_2)^2 \\ D &= (x_1x_2 + y_1y_2)^2 \\ X'_3 &= A/x_3 \\ Y'_3 &= B/y_3 \\ Z'_3 &= (D + z_3X'_3)/x_3 \\ T'_3 &= (C + t_3Y'_3)/y_3 \end{cases}.$$

L'élément neutre de la loi de semigroupe est $[0 : 0 : 1 : 0]$.

Complexité. La duplication coûte 6 multiplications et 6 carrés comme on peut prendre $\lambda_0 = 1$. Pour l'addition, on peut utiliser les formules suivantes :

$$\begin{cases} L_0 = x_1x_2,\ L_1 = y_1y_2,\ L_2 = z_1z_2,\ L_3 = t_1t_2, \\ T = (x_1 + y_1)(x_2 + y_2),\ M_1 = (y_1 + z_1 + t_1)(y_2 + z_2 + t_2), \\ M_2 = (x_1 + y_1 + t_1)(x_3 + y_3 + t_2),\ M_3 = (x_1 + z_1 + t_1)(x_1 + z_1 + t_1), \\ N = (x_1 + y_1 + z_1 + t_1)(x_2 + y_2 + z_2 + t_2),\ A = (L_1 + L_3 + M_1 + M_2 + N)^2, \\ B = (L_0 + L_3 + M_2 + M_3 + N)^2,\ C = (L_0 + L_1 + T)^2,\ D = (L_0 + L_1)^2, \end{cases}$$

donc l'addition coûte 11 multiplications, 4 carrés et 2 inversions.

Vérification de la loi de semigroupe. Le code `sagemath` [Ste09] suivant permet de vérifier la loi de semigroupe :

```
R.<lamb,mu,x1,y1,z1,t1,x2,y2,z2,t2,x3,y3,z3,t3> = GF(2)[]
EqP = x1^4 + x1^2*y1*t1 + mu^2*x1^2*y1^2 + lamb*x1*y1^2*z1\
    + lamb^2*y1^4 + z1^2*t1^2
EqQ = x2^4 + x2^2*y2*t2 + mu^2*x2^2*y2^2 + lamb*x2*y2^2*z2\
    + lamb^2*y2^4 + z2^2*t2^2
EqR = x3^4 + x3^2*y3*t3 + mu^2*x3^2*y3^2 + lamb*x3*y3^2*z3\
    + lamb^2*y3^4 + z3^2*t3^2

L0 = x1*x2;L1 = y1*y2;L2 = z1*z2;L3 = t1*t2
M0 = (x1 + y1)*(x2 + y2);M1 = (y1 + z1 + t1)*(y2 + z2 + t2)
```

```
M2 = (x1 + y1 + t1)*(x3 + y3 + t2);M3 = (x1 + z1 + t1)*(x1 + z1 + t1)
N = (x1 + y1 + z1 + t1)*(x2 + y2 + z2 + t2)
A = (L1 + L3 + M1 + M2 + N)^2;D = (L0 + L1)^2
B = (L0 + L3 + M2 + M3 + N)^2;C = (L0 + L1 + M0)^2

X3 = A/x3;  Y3 = B/y3
Z3 = (D + z3*X3)/x3;
T3 = (C + t3*Y3)/y3

EqS = X3^4 + X3^2*Y3*T3 + mu^2*X3^2*Y3^2 + lamb*X3*Y3^2*Z3\
    + lamb^2*Y3^4 + Z3^2*T3^2

EqS % (EqP*EqQ*EqR) == 0
```

Preuve de la loi de semigroupe. La preuve de cette loi de semigroupe est semblable à la preuve 8.3.3 dans le cas de la surface supersingulière.

Considérons les points $U = [u_{1,s} : u_{2,s} : u_{3,s} : u_{4,s}], V = [v_{1,s} : v_{2,s} : v_{3,s} : v_{4,s}]$ et $W = [w_{1,s} : w_{2,s} : w_{3,s} : w_{4,s}]$ de la surface ordinaire $\mathcal{K}_{\mathcal{C}_s}$ comme les antécédents des points P, Q et R donnés par le changement de variables (8.9). Il suffit alors d'utiliser les formules d'addition sur la surface ordinaire, d'utiliser l'inverse et de spécialiser $s = 0$.

8.3.5 Comparaison avec des études précédentes

Nous allons comparer notre étude à celle de Duquesne [Duq07, Duq08b] ; principalement, nous utilisons les formules qu'il donne sur le web http://www.math.univ-montp2.fr/~duquesne/articles/kummer2 [Duq08a]. Rappelons les notations suivantes :

$$\begin{aligned} C &: y^2 + x(x+1)y = x(x+1)\left[ax^3 + (a+b)x^2 + cx + c\right] \text{ avec } abc \in \overline{\mathbb{k}} - \{0\} \\ \mathcal{C} &: y^2 + y = x^5 + \mu^2 x^3 \text{ avec } \mu \in \overline{\mathbb{k}} - \{0\} \\ \mathcal{C}' &: y^2 + xy = \lambda x^5 + \mu x^3 + x, \text{ avec } \lambda, \mu \in \overline{\mathbb{k}} \text{ et } \lambda \neq 0. \end{aligned}$$

Le tableau 8.1 donne les différents coûts de calcul, en nombre de multiplications (M) et de carrés (S), sur les surfaces de Kummer $\mathcal{K}_C, \mathcal{K}_{\mathcal{C}}$ et $\mathcal{K}_{\mathcal{C}'}$ correspondantes. Le symbole $\gg 1$ signifie que la constante est grande et on peut compter la multiplication par la constante et le symbole ≈ 1 signifie que la multiplication par la constante est négligeable. Comme le carré est une opération linéaire sur les corps fini de caractéristique 2, alors nous allons prendre au maximum $S = 0,3M$ comme indiqué dans le tableau 8.1.

On remarque que le coût de la duplication est le même sauf pour les surfaces ordinaires ; d'ailleurs, on trouve les mêmes formules de duplication pour la surface supersingulière. Pour l'addition, on obtient globalement des gains de calculs par rapport aux formules de Duquesne et le gain maximum est de 16% (le cas de la surface supersingulière où $\mu \approx 1$ et $S = 0.3M$).

Conclusion

Dans cette partie, nous avons d'abord rappelé la théorie générale des fonctions thêta au chapitre 6, puis aux chapitres 7 et 8 nous avons donner deux applications de cette théorie à l'arithmétique efficace des courbes elliptiques et des courbes en genre 2 respectivement.

En genre 1, nous réinterprétons le modèle d'Edwards en caractéristique impaire grâce aux fonctions thêta. Ce qui nous permet d'en déduire le modèle d'Edwards binaire grâce à

Type	Duplication		Addition	
	Formules de **Duquesne**	Formules de **thêta**	Formules de **Duquesne**	Formules de **thêta**
$\mathcal{K}_C$ (ordinaire)	$10M + 6S$	$7M + 4S$	$14M + S$	$11M + 4S$
$S = 0,3M$	$11,8M$	$8,2M$	$14,3M$	$12,2M$
$\mathcal{K}_\mathcal{C}$ (supersingulière)	$5M + 7S$	$5M + 7S$	$20M + 5S$	$20M + 4S$
$\mu \gg 1$ et $S = 0,3M$	$7,1M$	$7,1M$	$21,5M$	$21,2M$
$\mu \approx 1$	$5M + 7S$	$5M + 7S$	$19M + 5S$	$16M + 4S$
$\mu \approx 1$ et $S = 0.3M$	$7,1M$	$7,1M$	$20,5M$	$17,2M$
$\mathcal{K}_{\mathcal{C}'}$ ($p-$rang 1)	$6M + 6S$	$6M + 6S$	$13M + 2S$	$11M + 4S$
$\lambda \gg 1$ et $S = 0,3M$	$7,8M$	$7,8M$	$13,6M$	$12,2M$
$\lambda \approx 1$	$6M + 6S$	$6M + 6S$	$12M + 2S$	$11M + 4S$
$\lambda \approx 1$ et $S = 0,3M$	$7,8M$	$7,8M$	$12,6M$	$12,2M$

TAB. 8.1 – Coût de l'arithmétique sur les surfaces de Kummer en caractéristique 2

une résolution de mauvaise réduction. En genre 2, nous obtenons des modèles et formules sur les surfaces de Kummer non-ordinaires, i.e. des surfaces de Kummer de $p-$rang 0 ou de $p-$rang 1. Comparativement aux formules connues, nous obtenons ainsi des gains de temps de calcul allant jusqu'à 16% pour les courbes de genre 2 en caractéristique deux.

Conclusion générale

Dans ce mémoire, nous avons tout d'abord implémenté les différents couplages en genre deux. Nous avons aussi utilisé les fonctions thêta pour faire le lien entre le modèle d'Edwards binaire et le modèle d'Edwards général. Nous avons enfin utilisé des techniques de déformation pour avoir de l'arithmétique efficace sur les surfaces de Kummer non-ordinaires. Ainsi, nous dégageons ici quelques perspectives :

- l'utilisation des mêmes techniques de déformation pour avoir le modèle et l'arithmétique sur le modèle d'Edwards supersingulier.
- L'étude du modèle et de l'arithmétique sur les lignes de Kummer supersingulières en utilisant les formules de [GL08] sur les lignes de Kummer ordinaires.
- Récemment les fonctions thêta [LR10] sont utiliséés pour améliorer l'implémentation des couplages en caractéristique impaire, cette étude devrait être faite en caractéristique deux.
- Un problème plus difficile est l'étude du modèle d'Edwards en genre deux.

Index

algorithme
  de Cantor, 22–24, 26
  de Miller, 32, 36, 37, 39, 46
anneau
  de valuation discrète, 11
  des coordonnées affines, 11
  des entiers p-adiques, 56
arithmétique
  courbe elliptique, 21
  efficace
    courbe elliptique, 59
    genre 2, 59, 71–73, 76, 80
  jacobienne, 26, 27, 39
attaques
  à canaux auxiliaires, 3, 22, 24, 26
  MOV et FR, 2, 19

Cantor
  addition, 23
  algorithme, 23, 24
  formules explicites, 24, 26
  réduction, 24
complexité, 22, 23, 40, 45, 77, 80, 81
coordonnée
  affine, 16
  jacobienne, 27
  projective, 27
corps
  algébriquement clos, 11
  de fonctions, 11
  extension non-ramifiée, 56
  fini, 10, 56
  nombres p-adiques, 55
  résiduel, 56
couplage, 31
  Ate I, 41
  Ate II, 42
  Eta, 40
  Tate, 31
  Weil, 31
courbe
  $p-$rang, 10, 17
  « friendly-pairing », 19
  elliptique, 9
  genre de la courbe, 9
  hyperelliptique, 9, 10
  modèle
    de Hessian, 27
    Edwards, 27, 59, 61
    Edwards binaire, 63
    Jacobi, 27
    Weierstraβ, 9
    Weierstraβ, 21, 27, 59
  ordinaire, 10, 17
  supersingulière, 10, 17
  twist, 69, 75, 79

degré
  d'un diviseur, 12
  d'une extension, 57
  de plongement, 19
diviseur, 12
  canonique, 75
  de fonction, 13
  degré -, 12
  effectif, 12
  poids -, 13, 16
  principal, 13

Eclatement, 65
Edwards (modèle -), 27, 59, 61

fonction
  Miller - Weil, 32, 36
  quasi-périodique, 52
  thêta, 51, 60, 72, 79
    formule d'addition, 54, 61
  thêta avec caractéristique, 52
  thêta constantes, 52, 63
  zéros et pôles, 11

groupe
  de Picard (Pic_C), 9, 15
  des diviseurs, 12

Hasse-Weil (théorème de), 18
Hessian (modèle), 27

involution hyperelliptique, 9

Jacobi (modèle -), 27
jacobienne, 15–18, 22

logarithme discret, 1, 2, 18

Miller (algorithme), 32, 36
morphisme de Frobenius, 10, 17, 41, 64
Mumford (représentation de), 16

norme, 55
    p-adique, 55, 56
    non-archimidienne, 55

point
    à l'infini, 9, 64
    de torsion, 16, 67
    rationnel, 10
    singulier, 64
polynôme caractéristique, 17, 46

réduction et relèvement, 57, 62

surface de Kummer, 71
    de $p-$rang 1, 79
    en caractéristique impaire, 72
    en caractéristique paire, 72
    ordinaire, 73
    supersingulière, 75

uniformisante, 11, 56

valuation, 11, 55, 64
variété de Kummer, 71

Weierstraβ
    modèle -, 22, 27, 59
    point de -, 9

Bibliographie

[Abh66] S.S. Abhyankar. *Resolution of singularities of embedded algebraic surfaces.* Academic Press - New York, 1966.

[ACD+06] R. Avanzi, H. Cohen, C. Doche, G. Frey, T. Lange, K. Nguyen, and F. Vercauteren. *Handbook of elliptic and hyperelliptic curve cryptography.* Chapman and Hall, 2006.

[ADH94] L. M. Adleman, J. DeMarrais, and M.-D. Huang. A subexponential algorithm for discrete logarithms over the rational subgroup of the jacobians of large genus hyperelliptic curves over finite fields. *ANTS-I (L. Adleman and M.-D. Huang, eds.), Lecture Notes in Comput. Sci. vol. 877, Springer Verlag*, 1994.

[AG01] J. Arledge and D. Grant. An explicit theorem of the square for hyperelliptic Jacobians. *Michigan Math. J. 49*, 2001.

[Anc43] M. Ancochea. Corps hyperelliptiques abstraits de caracteristique deux. *Portugaliae Math. 4*, 1943.

[BBJ+08] D. J. Bernstein, P. Birkner, M. Joye, T. Lange, and Peters C. Twisted Edwards curves. *in AFRICACRYPT 2008*, 2008.

[BCP97] W. Bosma, J. Cannon, and C. Playoust. The magma algebra system I : The User Language. *J. Symbolic Comp.* http:// magma.maths.usyd.edu.au/ magma/, 1997.

[BD04] B. Byramjee and S. Duquesne. Classification of genus 2 curves over $\mathbb{F}_{2^n}$ and optimization of their arithmetic. *Cryptography ePrint Archive 2004/107*, 2004.

[BDJ04] E. Brier, I. Déchène, and M. Joye. Unified addition formulae for elliptic curve cryptosystems. *Embedded Cryptography Hardware : Methodologies and Architectures. Nova Science Publisher*, 2004.

[Ber06] D. Bernstein. Curve25519 : new Diffie-Hellman speed records. *in Int. Conf. on theory and practice in PKC - New York. Lecture Notes in Comp. Science*, 2006.

[BF03] D. Boneh and M. Franklin. Identity-based encryption from Weil pairing. *SIAM Journal of Computing*, 2003.

[BGhS07] P.S.L.M. Barreto, S.D. Galbraith, C.O hEigeartaigh, and M. Scott. Efficient pairing computation on supersingular abelian varieties. *In Designs, Codes and Cryptography*, 42(3), 2007.

[Bho90] U. Bhosle. Pencils of quadrics and hyperelliptic curves in characteristic two. *J. Reine Angew. Math.*, 1990.

[BJ02] E. Brier and M. Joye. Weierstrass elliptic curves and side channels attacks. *Public Key Cryptography - PKC 02, Lect. Notes in Comp. Sci.*, 2274, Springer-Verlag, Berlin, 2002.

[BJ03] O. Billet and M. Joye. The Jacobi model of an elliptic curve and side channels analysis. *Applied Algebra, Algebraic Algorithms and Errors-Correcting Codes, LNCS 2643 - Springer-Verlag*, 2003.

[BKLS02] P.S.L.M. Barreto, H.Y. Kim, B. Lynn, and M. Scott. Efficient algorithms for pairings-based cryptosystems. *In Crypto 2002, vol 2442 of Lecture Notes in Computer Science - Springer*, 2002.

[BLF08] D.J. Bernstein, T. Lange, and R.R. Farashahi. Binary Edwards curves. *Cryptology ePrint Archive, 2008/171*, 2008.

[BLR90] S. Bosh, W. Lutkebohmert, and M. Raynaud. *Néron models.* Springer-Verlag, 1990.

[BLS01] D. Boneh, B. Lynn, and H. Shacham. Short signatures from the Weil pairing. *In Advances in Cryptology - ASIACRYPT 2001, ser. Lecture Notes in Computer Science*, 2001.

[BLS02] P.S.L.M. Barreto, B. Lynn, and M. Scott. Constructing elliptic curves with prescribed embedding degrees. *Preprint*, 2002.

[BN06] P.S.L.M. Barreto and M. Naehrig. Pairing-friendly elliptic curves of prime order. *In Selected Areas in Cryptography - SAC'2005, v. 3897 of LNCS Springer-Verlag*, 2006.

[BPR01] S. Basu, R. Pollack, and M.-F. Roy. *Algorithms in real algebraic geometry.* Springer-Verlag, 2001.

[BSS05] U. Blake, G. Seroussi, and N. Smart. *Advances in Elliptic Curves in Cryptography.* London Math. Society LN 317 - Cambridge University Press, 2005.

[Can87] D. Cantor. Computing in the Jacobian of a hyperelliptic curve. *Math. Comp.*, 1987.

[Car05] R. Carls. Theta null points of 2-adic canonical lifts. *A preprint is available at http://arxiv.org/math.NT/0509092*, 2005.

[CBLM09] T. Cheneau, A. Boudguiga, and M. Laurent-Maknavicius. Amélioration des performances des adresses CGA et du protocole SEND : étude comparée de RSA et d'ECC/ECDSA. *7ième conférence sur la sécurité et Architectures Réseaux SAR-SSI*, 2009.

[CF96] J.W.S. Cassels and E.V. Flynn. *Prolegomena to a middlebrow arithmetic of curves of genus 2.* London Math. Society - Cambridge University Press, 1996.

[CJ02] Y. Choie and E. Jeong. Isomosrphism classes of hyperelliptic curves of genus 2 over $\mathbb{F}_q$. *ACISP'02,pp.190-202 LNCS - Springer Verlag*, 2002.

[CJ03] Y. Choie and E. Jeong. Isomorphism classes of hyperellipic curves of genus 2 over $\mathbb{F}_{2^n}$. *Cryptography ePrint Archive 2003/213*, 2003.

[CMO98] H. Cohen, A. Miyaji, and T. Ono. Efficient elliptic curve exponentiation using mixed coordinates. *Asiacrypt 98. URL : http://www.math.u-bordeaux.fr/~cohen/asiacrpt98.dvi*, 1998.

[Con99] I. Connell. *Elliptic curve handbook.* Lecture notes, Web draft, available http://www.math.mcgill.ca/connell/, 1999.

[Coq02] R. Coquereaux. *Espaces fibrés et connexions : Une introduction aux géométries classiques et quantiques de la physique théorique.* available at http://www.cpt.univ-mrs.fr/~coque/linkxtoxbook.html, 2002.

[Cos09] M. Coste. Elimination, résultant. discriminant. *Agrégation mathématique de l'université de Rennes 1. URL http://agreg-maths.univ-rennes1.fr/documentation/docs/Revelim.pdf*, 2001 (consulté le 1 septembre 2009).

[DH76] W. Diffie and M. E. Hellman. New directions in cryptography. *IEEE Trans. Inform. Theory*, 1976.

[DL06] Y. Deng and M. Liu. Isomorphism classes of hyperelliptic curves of genus 2 over finite fields with characteristic 2. *ISS, Chinese Academy of Mathematics and Systems Science, Beijing, China*, 2006.

[Duc08] L. Ducrohet. The action of Frobenius map on rank 2 vector bundles over a supersingular genus 2 curves in characteristic 2. *Advances Mathematics*, 2008.

[Duq04] S. Duquesne. Montgomery scalar multiplication for genus 2 curves. *Algorithmic Number Theory Symposium - ANTS VI. Lect. Notes in Comp. Sci.*, 2004.

[Duq07] S. Duquesne. Traces of the group law on the Kummer surface of a curve of genus 2 in characteristic 2. *Preprint*, 2007.

[Duq08a] S. Duquesne. Formulas for traces of the group law on the Kummer surface of a curve of genus 2 in characteristic 2. *available at http://www.math.univ-montp2.fr/~duquesne/articles/kummer2*, 2008.

[Duq08b] S. Duquesne. Montgomery ladder for all genus 2 curves in characteristic 2. *Algorithmic Number Theory Symposium - ANTS VI. Lect. Notes in Comp. Sci.*, 2008.

[Edw07] H. M. Edwards. A normal form for elliptic curves. *Bulletin of the American Mathematical Society 44(2007)*, 2007.

[EMM02] L. H. Encinas, A. J. Menezes, and J. M. Masqué. Isomorphism classes of genus-2 hyperelliptic curves over finite fields. *Appl. Algebra Engrg. Comm. Comput.*, 2002.

[FNW09] R. Feng, M. Nie, and H. Wu. Twisted Jacobi intersections curves. *Cryptology ePrint Archive 2009/597*, 2009.

[FR94] G. Frey and H. Rück. A remark concerning m-divisibility and the discrete logarithm in divisor class group of curves. *Mathematics of Computation*, 1994.

[Fre07] D. Freeman. Constructing pairing-friendly genus 2 curves over prime fields with ordinary Jacobians. *Cryptyology ePrint Archive 2007/057*, 2007.

[Ful69] W. Fulton. *Algebraic Curves : An Introduction to Algebraic Geometry.* W.A. Benjamin, Inc - New York, 1969.

[Gal01] S. D. Galbraith. Supersingular curves in cryptography. *in C. Boyd - ASIACRYPT 2001 - Springer LNCS*, 2001.

[Gal05] S. D. Galbraith. Pairings. advances in elliptic curve cryptography. *London Math. Soc. Lecture Note Ser. 317, 183-213, Cambridge Univ. Press*, 2005.

[Gau00] P. Gaudry. Algorithme des courbes hyperelliptiques et applications à la cryptologie. *PhD thesis, Ecole Polytechnique*, 2000.

[Gau07] P. Gaudry. Fast genus 2 arithmetic based on theta functions. *Journal of Mathematical Cryptology*, 2007.

[GEM06] J.E. Garcia, L.H. Encinas, and J.M. Masqué. A review on the isomosrphism classes of hyperelliptic curves of genus 2 over finite fields admitting a weierstrass point. *Acta Appl. Math*, 2006.

[GG99] J.V.Z. Gathen and J. Gerhard. *Modern Computer Algebra*. Cambridge University Press, 1999.

[GHO+07] R. Granger, F. Hess, R. Oyono, N. Thériault, and F. Vercauteren. Ate pairing on hyperelliptic curves. *In EUROCRYPT 2007, vol. 4515 of Lecture Notes in Computer Science*, 2007.

[GHS02] S. D. Galbraith, K. Harrison, and D. Soldera. Implementing Tate pairing. *Algo. Number Theory Symposium - ANTS V, Lect. Notes in Comp. Sci.*, 2002.

[GHV07] S. D. Galbraith, F. Hess, and F. Vercauteren. Hyperelliptic pairings. *Springer Berlin - Lect. Notes in Comp. Sci.*, 2007.

[GL08] P. Gaudry and D. Lubicz. The arithmetic of characteristic 2 Kummer surfaces and of elliptic Kummer lines. *Accepté pour publication dans Finite Fields and Their Applications.*, 2008.

[Gou97] F. Q. Gouvêa. *p-adic Numbers - An Introduction*. Springer-Verlag, second edition, 1997.

[GPS06a] S. D. Galbraith, K. Paterson, and N. Smart. Pairings for cryptpgraphers. *Cyrptography ePrint Archive 2006/165*, 2006.

[GPS06b] R. Granger, D. Page, and N.P. Smart. High security pairing-based cryptography revisited. *LNCS vol. 4076*, 2006.

[Hac96] G. Haché. Construction effective de codes géométriques. *Ph.D. thesis, Universit de Paris VI*, 1996.

[Har77] R. Hartshorne. *Algebraic Geometry*. Springer-Verlag, 1977.

[Har00] R. Harley. Fast arithmetic on genus 2 curves. *http://cristal.inria.fr/~harley/hyper pour le code source en C*, 2000.

[Hes08] F. Hess. Pairings lattices. *Cryptology eprint archive, report 2008/125*, 2008.

[HMV04] D. Hankerson, A. Menezes, and S. Vanstone. *Guide to Elliptic Curve Cryptography*. Springer-Verlag New York, 2004.

[HSV06] F. Hess, N. P. Smart, and F. Vercauteren. The Eta pairing revisited. *IEEE Trans. Inform. Theory*, 2006.

[Hud05] R.W.H.T. Hudson. *Kummer's quartic surface*. Cambridge University Press, 1905.

[HWCD07] H. Hisil, K. Wong, G. Carter, and E. Dawson. Faster group operations on elliptic curves. *Cryptology ePrint Archive, 2007/441*, 2007.

[IEE00] IEEE. P.1363, Standard Specifications for Public-Key Cryptography. *Institute of Electrical and Electronics Engineers*, 2000.

[Igu72] J.-I. Igusa. *Theta functions*. vol. 194 of Die Grundlehren der mathematischen Wissenschaften. Springer, 1972.

[JA04] N. Jansma and B. Arredondo. Performance comparison of elliptic curve and RSA digital signatures. *Technical report, University of Michigan College of Engineering*, 2004.

[JE08] M. Joye and G. Neven (Eds.). *Identity-Based Cryptography*. IOS Press, 2008.

[Jou04] A. Joux. A one round protocol for tripartite Diffie-Hellman. *Journal of Cryptography*, 2004.

[Kob84] N. Koblitz. *p-adic Numbers, p-adic Analysis, and Zeta-functions*. Springer-Verlag, second edition, 1984.

[Kob87] N. Koblitz. Elliptic curve cryptosystems. *Math. Comp.*, 1987.

[Kob89] N. Koblitz. Hyperelliptic cryptosystems. *Journal of Cryptography*, 1989.

[Kob91] N. Koblitz. Constructing elliptic curve cryptosystems in characteristic 2. *In Advances in Cryptology - Crypto 90. LNCS, vol 537. Springer-Berlin.*, 1991.

[KT08] M. Kawazoe and T. Takahashi. Pairing-friendly hyperelleptic curves with ordinary Jacobian of type $y^2 = x^5 + ax$. *Cryptology ePrint Archive 2008/026*, 2008.

[Lan75] Von H. Lange. Uber die modulschemata der kurven vom geschlecht 2 mit 1, 2 oder 3 weierstrasspunkten. *J. Reine Angew. Math.*, 1975.

[Lan01] T. Lange. Efficient arithmetic on hyperelliptic curves. *PhD. Thesis Université Gesamthochschule Essen*, 2001.

[Lan02a] T. Lange. Efficient arithmetic on genus 2 hyperelliptic curves over finite fields via explicit formulae. *Cryptology ePrint Archive 2002/121*, 2002.

[Lan02b] T. Lange. Inversion-free arithmetic on genus 2 hyperelliptic curves. *Cryptography ePrint Archive 2002/147*, 2002.

[Lan02c] T. Lange. Weighted coordinates on genus 2 hyperelliptic curves. *Cryptography ePrint Archive 2002/153*, 2002.

[Ler97] R. Lercier. Finding good random elliptic curves for cryptosystems defined over $\mathbb{F}_{2^n}$. *Advances in Cryptology - EUROCRYPT 97. Springer-Verlag*, 1997.

[Ler04] R. Lercier. Courbes elliptiques et cryptographie. *Direction des Centres d'Expertise et d'Essais*, 2004.

[Lic69] S. Lichtenbaum. Duality theorem for curves over p-adic fields. *Inventiones mathematicae*, 1969.

[LLL82] A.K. Lenstra, H.W. Lenstra, and L. Lovàsz. Factoring polynomials with rational coefficients. *Math. Ann. 261*, 1982.

[LLL08] E. Lee, H-S Lee, and Y. Lee. Eta pairing computation on general divisors over hyperelliptic curve $y^2 = x^7 - x \pm 1$. *a voir*, 2008.

[LM05] T. Lange and P.K. Mishra. SCA resistant parallel explicit formula for addition and doubling of divisors in the Jacobian of hyperelliptic curves of genus 2. *LNCS v. 3797/2005. Springer Berlin/Heidelberg*, 2005.

[Loc94] P. Lockhart. On the discriminant of a hyperelliptic curve. *Trans. Ame. Math. Soc. 342*, 1994.

[LP02] Y. Laszlo and C. Pauly. The action of Frobenius map on rank 2 vector bundles in characteristic 2. *Journal of Alg. Geom. vol 11*, 2002.

[LP04] Y. Laszlo and C. Pauly. The Frobenius map, rank 2 vector bundles and Kummer's quartic surface in characteristics 2 and 3. *Advances Mathematics*, 2004.

[LR10] D. Lubicz and D. Robert. Efficient pairing computation with Theta functions. *Preprint*, 2010.

[MDM+02] Y. Miyamoto, H. Doi, K. Matsuo, J. Chao, and S. Tsuji. A fast addition algorithm of genus two hyperelliptic curve. *Symposium on Cryptography and Information Security - SCIS*, 2002.

[Mil86] V. S. Miller. Short programs for functions on curves. *Umpublished manuscript Available at http://crypto.stanford.edu/miller/miller.pdf*, 1986.

[Mil04] V. S. Miller. The Weil pairing, and its efficient calculation. *Journal of Cryptology*, 2004.

[MKHO07] S. Matsuda, N. Kanayama, F. Hess, and E. Okamoto. Optimised versions of ate and twisted ate pairings. *In The 11th IMA International Conference on Crytography and Coding*, 2007.

[MOV93] A.J. Menezes, T. Okamoto, and S.A. Vanstone. Reducing elliptic curve logarithms to logarithms in finite field. *IEEE Transactions on Information Theory volume 39, num 5*, 1993.

[Mul10] J.S. Muller. Explicit Kummer surface theory for arbitrary characteristic. *London Math. Soc. J. of Comp. and Math.*, 2010.

[Mum66] D. Mumford. On the equations defining abelian varieties I. *Invent. Math.*, 1966.

[Mum74] D. Mumford. *Abelian Varieties.* Oxford University Press, 1974.

[Mum83] D. Mumford. *Tata lectures on theta I.* Birkhäuser Boston Inc., Boston, MA, 1983.

[Mum84] D. Mumford. *Tata lectures on theta II.* Birkhäuser Boston Inc., Boston, MA, 1984.

[NIS02] NIST. Elliptic curves for digital signature algorithm (ECDSA) FIPS 186-2. *National Institute of Standards and Technology recommended for US Government's*, 2002.

[Pat02] K.G. Paterson. ID-based signature from pairings on elliptic curves. *Electronics Letters, Vol.38, No.18*, 2002.

[PH78] S. Pohlig and M. Hellman. An improved algorithm for computing logarithms over GF(p) ans its cryptographic significance. *IEEE Transactions on Information Theory*, 1978.

[PKS09] L. J. D. Perez, E. J. Kachisa, and M. Scott. Implementing cryptographic pairings : a magma tutorial. *Cryptology ePrint Archive, 2009/072*, 2009.

[Pol78] J. M. Pollard. Monte carlo methox for index computation (mod p). *Math. Comp.*, 1978.

[RD02] V. Rijmen and J. Daemen. *The Design of Rijndael.* Springer-Verlag, 2002.

[RF74] H.E. Rauch and H.M. Farkas. *Theta Functions with Applications to Riemann Surfaces.* Baltimore, Williams & Wilkins Comp., 1974.

[Rit03] C. Ritzenthaler. Problèmes arithmétiques relatifs à certaines familles de courbes sur les corps finis. *thèse de doctorat Université Denis Diderot - Paris VII*, 2003.

[Rob00] A.M Robert. *A course in p-adic analysis.* Springer - Graduate Texts in Mathematics, 2000.

[RSA78] R. L. Rivest, A. Shamir, and L. M. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Comm. ACM*, 1978.

[SBCP08] M. Scott, N. Benger, M. Charlemagne, and L.J.D. Perez. On the final exponentiation for calculating pairings on ordinary elliptic curves. *ePrint Archive Cryptography, 2008/490*, 2008.

[Ser79] J.-P Serre. *Local Fields.* Graduate Texts in Mathematics, vol. 67, Springer-Verlag, 1979.

[Sha71] D. Shanks. Class number, a theory of factorisation, and genera. *In Proc. Symp. Pure Math. vol 20*, 1971.

[Sho08] V. Shoup. *A computational Introduction to Number Theory and Algebra*. Cambridge University Press, 2008.

[Sil86] J. Silvermann. *The Arithmetic of Elliptic Curves*. Springer, 1986.

[Sma01a] N. P. Smart. The Hessian form of an elliptic curve. *CHES - LNCS 2162*, 2001.

[Sma01b] N. P. Smart. An identity based authentification key agreement protocol based on pairing. *Electronics Letters, Vol.38, No.13*, 2001.

[SOK00] R. Sakai, K. Ohgishi, and M. Kasahara. Cryptosystems based on pairings. *In 2000 Symposium on Cryptography and Information Security, Okinawa, Japan*, 2000.

[SS99] N. Smart and S. Siksek. A fast Diffie-Hellman protocol in genus 2. *Journal of Cryptology 12*, 1999.

[Ste09] William Stein. Sage mathematics software (version 3.4). *The Sage Group http://www.sagemath.org*, 2009.

[Tat95] J. Tate. WC-groups over p-adic fields. *Séminaire Bourbaki, volume 4, Société mathématique de France, Exposé no. 156 (1957/58)*, 1995.

[Ver99] F. Vercauteren. $\#EC(GF(2^{1999}))$. *E-mail message to the NMBRTHRY list*, 1999.

[Ver01] E. Verheul. Evidence that XTR is more secure than supersingular elliptic curve cryptosystems. *In B. Pfitzmann, editor, EUROCRYPT, volume 2045* Lecture Notes in Computer Science *Springer*, 2001.

[Ver08] F. Vercauteren. Optimal pairings. *Cryptology ePrint Archive 2008/096*, 2008.

[Wal35] R. J. Walker. Reduction of the singularities of an algebraic surface. *The Annals of Mathematics, Second Series*, 1935.

[Wen03] A. Weng. Constructing hyperelliptic curves of genus 2 suitable for cryptography. *Math. Comp. 72*, 2003.

[Zé00] G. Zémor. *Cours de cryptographie*. Paris : Cassini, 2000.