UNIVERSITÉ DE VERSAILLES
SAINT-QUENTIN-EN-YVELINES

Laboratoire PRISM

Algorithmique des couplages et cryptographie

THÈSE

présentée et soutenue publiquement le 14 mai 2010

pour l'obtention du

Doctorat de l'université de Versailles Saint-Quentin-en-Yvelines
(spécialité informatique)

Sorina IONICĂ

Composition du jury

Jean-Marc Couveignes	Rapporteur
Louis Goubin	Examinateur
Antoine Joux	Directeur de thèse
David Kohel	Rapporteur
Tanja Lange	Examinateur
Ariane Mézard	Examinateur
Benjamin Smith	Examinateur

Remerciements

Ce travail n’aurait probablement pas vu le jour sans l’aide et la direction de mes professeurs. Je remercie Antoine Joux, mon directeur de thèse, d’avoir guidé mes pas vers le monde de la recherche. Il m’est très difficile de le remercier en une seule phrase pour tout ce qu’il a su me transmettre. J’essaie quand même : « Les idées simples sont aussi les plus belles ».
Je dois énormement à Ariane Mézard, pour les mathématiques que j’ai apprises d’elle, pour son enthousiasme envers la recherche, pour ses encouragements. Merci à elle pour tout le temps qu’elle a investit dans cette thèse.

J’ai une pensée toute particulière pour Marcel Tena, qui fut mon professeur de mathématiques au lycée, et grâce à qui j’ai decouvert l’algèbre. J’espère, Monsieur le professeur, ne pas vous avoir trop déçu et que vous trouverez dans ces pages, malgré le grand nombre de lignes de pseudocode, des maths aussi belles que celles que vous m’aviez apprises.

Je tiens à remercier Louis Goubin et Michael Quisquater de m’avoir proposé de travailler sur le projet Secure Algorithm, ainsi que pour nos collaborations lors des enseignements. Merci à mes co-auteurs, Nadia El Mrabet et Nicolas Guillermin, ainsi qu’à Jean-Claude Bajard et Sylvain Duquesne d’avoir suivi notre travail. Je remercie Tanja Lange pour la lecture de mes articles et pour ses remarques. Je suis reconnaisante à mes collègues qui ont lu et corrigé des parties de ce manuscrit : Anja Becker, Peter Birkner, Nadia El Mrabet, Malika Izabachène, Bastien Vayssière, Vanessa Vitse. Merci à Cris car sans son aide les courbes dans ma thèse ne seraient pas aussi belles !

Le tour des thèsards maintenant, ou devrais-je dire le tour des cryptogirls... ? Merci à Aurélie de m’avoir accueillie à mon arrivé au laboratoire, d’avoir corrigé les fautes d’orthographe de mon rapport de stage. Je remercie Joana, ma co-bureau, pour son enthousiasme et sa bonne humeur habituelle, pour avoir rempli le bureau de toutes les langues du monde (l’espagnol, l’allemand, le portugais, l’alsacien, le roumain et même le français). Je remercie Vanessa pour nos discussions qui m’ont fait me sentir moins seule (dans un monde cruellement envahi par les bases de Gröbner), et aussi pour une certaine implémentation que je n’aurais jamais eu le courage de faire. Mais, malgré les rumeurs, le Prism n’est pas une école de femmes. Merci à Jean-Michel de faire face, à Sebastien de m’avoir fait rire (et pleurer) tant de fois ! Un grand merci à Stéphane, le « responsable » Linux de toutes mes machines, pour sa disponibilité permanente ainsi que pour avoir eu une réponse à toute question. Merci à tous les « archi » que j’ai eu l’occasion de croiser.
Ce que je garderai vif à l’esprit ? Les Tds en L1 soigneusement rédigés avec des stylos Barbie, les cadeaux d’Aurélie pour le 1er mars, les photos de Thierry (merci à Thierry pour les perruques), la rump session d’Eurocrypt, la poudre de craie cachée sous le bureau de L., les pamplemousses de Seb, les histoires de Stéphane...

Merci à mes amis d’ici et de très loin pour leur soutien permanent, sans lequel je ne serais peut être pas arrivée au bout de ce chemin. Merci à Miru, Iuli et toute la bande de faire mes retours à Bucarest plus beaux, de me rappeler constamment d’où je viens. Merci à Adi de m’avoir encouragée à partir et finir mes études à l’étranger.
Quant à ceux d’ici, merci de m’avoir adoptée, à Villeneuve-sur-Lot, au sein d’une bande de futurs ingénieurs un peu fous (born in Regie). Le temps s’est écoulé très vite : au campus gris de l’X, en passant après par la rue de Tolbiac, où je trainais plus de temps que chez moi, pour arriver enfin à la maison de Chantiers, toujours très animée (je n’oublierai pas la musique !). Merci à eux d’avoir fait de Paris ma deuxième maison. DistrusX rulz !

Mes derniers mots sont pour ma famille, à Bucarest et à Craiova. Je leur remercie pour leur soutien inconditionnel tout au long de mes années d’études. Qu’ils sachent que, malgré ces moments d’absence, je pense fort à eux.

A mes grandparents
Bunicilor mei

Table des matières

Chapitre 1

Introduction

En cryptographie moderne, nous distinguons deux principales techniques de chiffrement. La plus ancienne est la cryptographie symétrique, ou encore à clé secrète, qui repose sur le principe que deux parties doivent détenir un secret commun pour pouvoir échanger de l'information chiffrée. La deuxième, la cryptographie asymétrique, est parue en 1976, quand Diffie et Hellman [30] proposent pour la première fois un schéma de chiffrement ne nécessitant pas la connaissance préalable d'un même secret. Aujourd'hui, dans un système sécurisé, la cryptographie à clé secrète et celle à clé publique sont utilisées conjointement, afin d'offrir un chiffrement rapide de l'information. Dans un premier temps, un schéma à clé publique est utilisé pour échanger une clé commune secrète. Ensuite, cette clé secrète est utilisée pour sécuriser, à l'aide d'un schéma symétrique, la communication entre l'émetteur et le destinataire.

Nous décrivons le protocole d'échange de clef proposé par Diffie et Hellman, pour un groupe abstrait G, noté additivement, qui est engendré par un élément P. Deux parties Alice (A) et Bob (B) détiennent les paramètres publics $(G, +, P)$ et veulent se mettre d'accord sur une clé commune, qui est un élément du groupe. A choisit $a \in \mathbb{N}$ et calcule $P_A = aP$, tandis que B choisit $b \in \mathbb{N}$ et calcule $P_B = bP$. Ils échangent publiquement ces valeurs. Ayant reçu P_B, A calcule

$$P_k = aP_B = abP.$$

De la même manière, B reçoit P_A et calcule

$$P_k = bP_A = abP.$$

La sécurité de ce protocole repose sur la difficulté du problème du logarithme discret dans le groupe G. Cette difficulté signifie qu'étant donné un point P et xP, un multiple scalaire du point P, il est calculatoirement difficile de retrouver x. La difficulté de ce problème dépend évidemment du choix du groupe $(G, +)$. En effet, si le problème du logarithme discret était facile dans le groupe G, un attaquant Charlie, réussissant à intercepter P_A ou P_B, pourrait calculer a ou b et retrouver P_k.

Afin de pouvoir développer des cryptosystèmes comme celui de Diffie et Hellman, il est donc indispensable de trouver des groupes dans lesquels le problème du logarithme discret semble difficile. Notons qu'il existe des attaques, dites génériques, qui fonctionnent dans tous les groupes. Les meilleures attaques génériques contre le logarithme discret sont les attaques de Shanks [85] et de Pollard [79]. Leur complexité est $O(\sqrt{r})$, où r est le plus grand facteur premier de la cardinalité de la courbe. Diffie et Hellman [30] ont proposé le groupe multiplicatif d'un corps fini. Néanmoins, dans ces groupes, il existe des méthodes dites de ”calcul d'indice”, qui résolvent le problème du logarithme discret avec une complexité sous-exponentielle [52, 53]. Pour améliorer la sécurité, le logarithme discret sur les courbes elliptiques ou sur les jacobiennes des courbes hyperelliptiques a été ensuite proposé [58, 59, 69]. Cependant, dans le cas des courbes de genre supérieur à 3, des attaques contre le logarithme discret avec une complexité sous-exponentielle ont été trouvées [2, 41, 42].

Les premières attaques spécifiques contre le logarithme discret sur les courbes elliptiques ont été données par Menezes, Okamoto et Vanstone [1] et Frey et Rück [37]. Ces attaques utilisent les couplages de Weil ou de Tate pour réduire le problème du logarithme discret sur la courbe elliptique au problème du logarithme discret dans un corps fini, où des attaques plus efficaces de type calcul d'indice sont connues. Ces résultats sont aussi la première utilisation des couplages en cryptographie. Par ailleurs, il existe des attaques utilisant le descente de Weil qui réduisent le problème du logarithme discret sur la courbe elliptique au problème du logarithme discret sur une courbe de genre supérieur. Ces attaques [29, 39] s'appliquent seulement à des courbes définies sur des corps composées $\mathbb{F}_{q^k}$, avec $q = p^d$. Les courbes de trace 1 sont elles, plus que déconseillées [81].

Malgré ces attaques, il n'existe aujourd'hui aucun algorithme sous-exponentiel pour résoudre le problème du logarithme discret sur une courbe elliptique générique.

La réduction MOV/Frey-Ruck contre le logarithme discret sur les courbes elliptiques. Cette attaque représente aussi la première utilisation des couplages en cryptographie. Supposons P, Q deux points sur une courbe elliptique E, d'ordre r, tels que $Q = \lambda P$, avec $\lambda \in \mathbb{N}$. Supposons qu'il existe un couplage sur la courbe elliptique, calculable en un temps polynômial, et que ce couplage soit non-dégénéré, c'est à dire qu'il existe un point R sur la courbe E tel que

$$e(P, R) \neq 1.$$

Alors, un attaquant peut calculer

$$\zeta_1 = e(P, R) \text{ et } \zeta_2 = e(Q, R).$$

Pour retrouver λ il suffit de résoudre l'équation

$$\zeta_1^\lambda = \zeta_2,$$

en utilisant un algorithme de calcul d'indice dans le corps fini $\mathbb{F}_{q^k}$.

1.1 Couplages et cryptographie

Soient $\mathbb{G}_1$ et $\mathbb{G}_2$ deux sous-groupes cycliques d'ordre r sur une courbe elliptique. A l'aide des couplages de Weil ou de Tate, applications bilinéaires définies sur la courbe elliptique, nous considérons le couplage cryptographique

$$e : \mathbb{G}_1 \times \mathbb{G}_2 \to H \tag{1.1}$$

où H est un sous-groupe multiplicatif d'ordre r dans un corps fini $\mathbb{F}_{q^k}$. Nous appelons k le degré de plongement relativement à r et nous verrons au chapitre 6 que k est un paramètre important de la sécurité du système.

Le premier schéma à base de couplages est l´échange tripartite Diffie-Hellman, proposé par Joux en 2000 [51]. Un an plus tard, Boneh et Franklin [16] proposent leur schéma de chiffrement à base d'identité utilisant des couplages. Ce schéma répond à une question posée par Shamir [84] à la conférence CRYPTO'84, concernant un système de chiffrement où la clé publique est obtenue à partir de l'identité. De nos jours, la cryptographie à base de couplages est un domaine très vaste, qui comprend des centaines de schémas. Cependant, le chiffrement à base d'identité de Boneh et Franklin [16] reste sans doute l'application la plus remarquable des couplages en cryptographie.

Dans un première temps, la sécurité de ces systèmes repose sur la difficulté du logarithme discret sur la courbe elliptique et dans le corps fini $\mathbb{F}_{q^k}$. Dans un deuxi/'eme temps, d'autres hypothèses de sécurité sont étudi'ees, comme les problèmes Diffie-Hellman calculatoire (CDH) et Diffie-Hellman décisionnel (DDH).

Le problème Diffie-Hellman calculatoire (CDH) : Etant donné un groupe $\mathbb{G}$ et un élément $P \in \mathbb{G}$ il est difficile, à partir de aP et bP, de calculer abP.

Le problème Diffie-Hellman décisionnel (DDH) : Étant donné un groupe $\mathbb{G}$, $P \in \mathbb{G}$, et un triplet (aP, bP, cP), il est difficile de décider si $cP = abP$.

Enfin, l'étude de la sécurité des schémas à base de couplages a permis l'introduction d'autres variantes de ces problèmes, comme le Diffie-Hellman calculatoire bilinéaire (CBDH) et Diffie-Hellman décisionnel bilinéaire (DBDH).

Le protocole de Diffie Hellman à trois parties. Soit P le générateur de $\mathbb{G}$ et $e : \mathbb{G} \times \mathbb{G} \to H$. Supposons que nous ayons $e(P, P) \neq 1$. Les paramètres publics sont $(\mathbb{G},P,H,e)$.
L'utilisateur A choisit $a_A \in N$ et calcule $P_A = [a_A]P$, qu'il envoie à B et C. De la même manière, B et C choisissent a_B et a_C et envoient aux deux autres $P_B = [a_B]P$ et $P_C = [a_C]P$. Alors, A, B et C obtiennent la clé commune K de H car

$$K = e(P_B, P_C)^{a_A} = e(P_A, P_C)^{a_B} = e(P_A, P_B)^{a_C} = e(P, P)^{a_A a_B a_C}.$$

Chiffrement à base d'identité. En règle générale, les algorithmes existants pour des systèmes de type logarithme discret demandent que le destinataire d'un message chiffré ait établi sa clé publique par avance. Le concept de cryptographie à base de l'identité introduit par Shamir [84] permettrait de résoudre le problème de d'envoyer un message chiffré à une personne qui n'est pas encore dans le système. Dans le schéma à base d'identité de Boneh et Franklin, la clé publique est calculée de manière déterministe à partir des paramètres de l'identité de l'utilisateur, mais pour déchiffrer le message ce dernier doit faire appel à une autorité de confiance, le centre de génération de clef (CGC), qui à partir d'une clé maître peut calculer la clé secrète de chaque utilisateur. Ce schéma est décrit par quatre algorithmes.

Initialisation. Le CGC choisit un groupe $\mathbb{G}$ avec une application bilinéaire e vers H et calcule la clé publique $P_{TA} = sP$. Il choisit aussi deux fonctions de hachage $h_1 : \{0, 1\}^* \to \mathbb{G}^*$, $h_2 : H \to \{0, 1\}^n$. Les paramètres $(\mathbb{G}, H, P, P_{TA}, h_1, h_2)$ sont publics, l'entier s est la clé secrète du CGC.
Génération de clef. Étant donnée l'identité $Id \in \{0, 1\}^*$, le CGC calcule $Q_{Id} = h_1(Id)$ et aussi la clé secrète de Id, soit $Q = sQ_{Id}$.
Chiffrement. Pour chiffrer on message m que l'on veut envoyer à Id, on choisit $r \in N$. On calcule

$Q_{Id} = h_1(Id)$. Alors le chiffré est

$$C = (rP, m \oplus h_2(e(Q_{Id}, P_{CGC})^r)).$$

Déchiffrement. Pour déchiffrer un message $C = (C_1, C_2)$, Id utilise sa clé secrète Q pour calculer

$$C_2 \oplus h_2(e(Q, C_1)) = m.$$

En effet, si C est le chiffré du message m avec la clé publique Id, alors

$$e(Q, C_1) = e(sQ_{Id}, rP) = e(Q_{Id}, sP)^r = e(Q_{Id}, P_{CGC})^r.$$

Cela montre que l'algorithme de déchiffrement renvoie bien m.

1.2 Motivation des travaux et objectifs de la thèse

Le problème du logarithme discret est difficile sur une courbe elliptique générique, mais il faut tout de même s'assurer que la cardinalité du groupe de la courbe n'est pas friable pour résister à la réduction de Polhig et Hellman [78]. Il est donc nécessaire de calculer le nombre de points d'une courbe elliptique. Le premier algorithme qui calcule la cardinalité d'une courbe elliptique en temps polynômial a été donné par R. Schoof [82] en 1985. Schoof utilise l'équation caractéristique de l'endomorphisme de Frobenius π

$$\pi^2 - t\pi + q = 0,$$

et, en conséquence, l'action de l'endomorphisme π sur le sous-groupe de ℓ-torsion d'une courbe pour déterminer la trace du Frobenius t modulo ℓ. En répétant ce procédé pour plusieurs nombres premiers petits ℓ, il peut ensuite utiliser le théorème du reste chinois pour déterminer la valeur de la trace du morphisme de Frobenius t et donc la cardinalité de la courbe, grâce à la formule

$$\#E(\mathbb{F}_q) = q + 1 - t. \tag{1.2}$$

Des améliorations importantes à cet algorithme ont été trouvées ultérieurement par Elkies [33] et Atkin [5].

Le problème du calcul de l'anneau d'endomorphismes d'une courbe elliptique est naturellement lié au problème du calcul du nombre de points. Par (1.2), connaître le nombre de points sur une courbe elliptique est équivalent au fait de connaître l'équation caractéristique de l'endomorphisme de Frobenius π et donc à la détermination de $\mathbb{Z}[\pi]$, qui est un sous-anneau de l'anneau $\mathrm{End}(E)$. De plus, H. Lenstra [55] établit un isomorphisme de $\mathrm{End}(E)$-modules entre le groupe défini sur la courbe elliptique ordinaire, noté $E(K)$, et le quotient de $\mathrm{End}(E)$ par $\pi - 1$:

$$\mathrm{End}(E)/(\pi - 1) \cong E(K). \tag{1.3}$$

Ainsi, le fait de connaître l'anneau d'endomorphismes de la courbe permettrait de déterminer ensuite la structure du groupe de la courbe elliptique.

Notons que deux courbes ont le même nombre de points si et seulement si elles sont isogènes, donc la cardinalité de la courbe est un invariant par isogénies. Elle détermine en fait une classe de courbes isogènes, que nous notons $Ell_t(E)$. Pour un nombre ℓ, Kohel [61] décrit la structure du graphe de ℓ-isogénies défini sur $Ell_t(\mathbb{F}_q)$. L'étude de cette structure permet d'une part de déterminer l'anneau d'endomorphismes de chaque courbe dans ce graphe, mais aussi de connaître la relation entre deux courbes isogènes et leurs anneaux d'endomorphismes. En utilisant les polynômes modulaires pour le parcours du graphe de ℓ-isogénies et en supposant la cardinalité de la courbe connue, Kohel montre qu'il est possible de calculer la valuation ℓ-adique du conducteur f de l'anneau d'endomorphismes pour des petits valeurs de ℓ. Il utilise cette méthode dans un algorithme déterministe permettant de calculer l'anneau d'endomorphismes d'une courbe elliptique.

Fouquet et Morain [35] appellent les graphes d'isogénies *volcans d'isogénies*. Ayant comme motivation l'optimisation de l'algorithme de Schoof, Fouquet et Morain montrent qu'il est possible de déterminer la valuation ℓ-adique de f sans connaître la cardinalité de la courbe.

Cette thèse s'inscrit dans la continuation des travaux de Kohel et de Fouquet-Morain. Nous nous sommes intéressés à la structure du groupe de ℓ-torsion des courbes sur un volcan de ℓ-isogénies. Cette approche était déjà proposée par Miret et al. [71, 72], qui ont montré que dans de nombreux cas, en étudiant la structure de la ℓ-torsion sur deux courbes E et E' reliées par une arrête $I : E \to E'$ dans le graphe d'isogénies, il est possible de savoir si nous sommes monté ou descendu dans le volcan, ou si nous avons fait un pas sur le cratère. Cela était très intéressant car, en utilisant seulement les polynômes modulaires, il n'était pas possible, après avoir fait un pas sur le volcan, de connaître simplement la direction de ce pas. Du coup, dans les algorithmes de Kohel et de Fouquet-Morain, afin de déterminer la direction prise, il est nécessaire de faire de nombreux pas successifs. Neanmoins, même utilisant l'information supplémentaire venant de la structure du groupe de la ℓ-torsion, le coût de ces algorithmes n'est pas réduit de manière significative. Le désavantage de la méthode de Miret et al. est que lorsqu'on veut prendre une certaine direction sur le volcan en partant d'un noeud E, nous sommes obligés de calculer tous les voisins de E, et de déterminer la structure du groupe pour chacun d'entre eux, avant de se décider sur le noeud qui se trouve dans la bonne direction.

Nous nous sommes alors proposés d'étudier un modèle plus complexe, en construisant un couplage sur la ℓ-torsion des courbes sur un volcan de ℓ-isogénies. Dans ce cadre, nous avons observé que le comportement du couplage sur les courbes du volcan diffère d'un niveau à l'autre et est strictement lié au type d'isogénies qui apparaissent dans le graphe. En utilisant le couplage définit sur la ℓ-torsion de la courbe, nous avons montré qu'il est possible de déterminer la direction d'une isogénie dont le noyau est engendré par un point de ℓ-torsion fixé. Notre objectif était alors de donner des nouveaux algorithmes, permettant de parcourir les graphes d'isogénies de manière très efficace.

Dans un second temps, nous nous sommes intéressés aux algorithmes qui calculent le couplage sur une courbe elliptique. La motivation de ce travail est donné en partie par le fait que nos algorithmes de parcours de graphes utilisent les couplages, mais surtout par l'intérêt d'avoir, en cryptographie à base de couplages, des algorithmes rapides pour le calcul de ces applications bilinéaires.

L'algorithme le plus utilisé pour le calcul des couplages de Weil et de Tate a été donné par Miller [70] en 1985. Cet algorithme est en fait une extension de la méthode égyptienne (double-and-add) pour le calcul du multiple scalaire d'un point sur la courbe elliptique. Depuis l'apparition de la cryptographie à base de couplages, un des objectifs majeurs de la recherche dans le domaine est l'optimisation de l'algorithme de Miller. Nos travaux s'inscrivent dans cette voie de recherche.

Le point de départ est donné par les résultats sur le raccourcissement de la boucle de l'algorithme de Miller, obtenus par Barreto et al. [6] et par Hess et al. [47]. Cette technique, qui a comme résultat un algorithme de calcul du couplage de type double-and-add mais avec une boucle très courte, utilise le fait que l'endomorphisme du Frobenius a un noyau trivial. Notre idée est d'étudier d'autres endomorphismes, de petit degré, qui auront eux un noyau d'ordre petit.

1.3 Contributions et organisation de cette thèse

L'objectif de ce manuscrit est de donner un aperçu de l'algorithmique des couplages, en présentant à la fois les aspects constructifs et calculatoires de ces applications bilinéaires. Afin de rendre ce texte plus accessible, nous commençons par rappeler dans la Partie I l'arithmétique classique des courbes elliptiques ainsi que des notions de théorie des nombres élémentaire. Cette partie s'articule en trois chapitres. Le deuxième chapitre présente la loi de groupe sur une courbe elliptique. Le chapitre 3 présente brièvement quelques résultats importants de la théorie de la multiplication complexe. Au chapitre 4, nous donnons quelques algorithmes importants dans la cryptographie à base de couplages, notamment l'algorithme de Miller et les algorithmes construisant des courbes à multiplication complexe.

La Partie II est dédiée à l'étude du modèle de volcans d'isogénies. Nous commençons par présenter d'abord les techniques de Kohel et de Fouquet-Morain pour le parcours des volcans d'isogénies. Nous étudions ensuite la structure de la ℓ-torsion sur les différents niveaux du volcan, ce qui nous mène à considérer des couplages non-dégénérés sur cette structure de groupe. Nous étudions le couplage d'un point par lui même et nous montrons que les points ayant des couplages non-dégénérés engendrent les noyaux des isogénies descendantes, tandis que les points dont le couplage est dégénéré engendrent les noyaux des isogénies ascendantes ou horizontales. Dans certains cas, qu'on appelle des *volcans irréguliers*, notre modèle est complètement dégénéré et l'étude de la ℓ-torsion sur le corps de base $\mathbb{F}_q$ ne suffit pas pour déterminer les directions des isogénies. Dans ce cas, nous devons considérer la courbe dans une extension de degré ℓ du $\mathbb{F}_q$. On conclût cette partie par nos algorithmes de parcours des volcans d'isogénies.

Enfin, la Partie III porte sur l'implémentation de l'algorithme de Miller sur des courbes elliptiques offrant une mise en oeuvre sécurisée des protocoles cryptographiques à base de couplages. Dans cette partie, nous proposons l'utilisation des isogénies pour le calcul efficace de couplages.

Le chapitre 6 regroupe plusieurs aspects de l'implémentation efficace des couplages sur les courbes elliptiques. Nous donnons d'abord les formules pour le calcul de couplages en coordonnées jacobiens. Nous nous attardons particulièrement sur le cas des courbes elliptiques ayant un degré de plongement pair. Nous expliquons que, grâce à l'existence des tordues, dans ce cas une bonne partie des calculs se fait dans $\mathbb{F}_q$ et dans un sous-corps de $\mathbb{F}_{q^k}$. Nous avons donné, dans ce cas, des formules rapides pour le calcul de la partie doublement de l'algorithme de Miller, pour des courbes ayant un degré de plongement pair [50]. Une fois la problématique sur l'implémentation du couplage expliquée, nous donnons un algorithme efficace pour le calcul du couplage sur des courbes dont le discriminant de l'anneau d'endomorphismes est petit. Nous montrons que notre algorithme est plus rapide que l'algorithme de Miller, si la courbe a un degré de plongement $2, 3$ ou 4. Nous donnons aussi une construction de courbes à multiplication complexe ayant degré du plongement 1 et un couplage non-dégénéré d'un point par lui même.

Au chapitre 7, nous étudions l'implémentation des couplages sur les courbes d'Edwards. Les courbes d'Edwards ont été introduites en cryptographie par Bernstein et Lange [12] en 2007, qui ont donné ainsi des formules très efficaces pour l'addition et le doublement des points sur une courbe elliptique. Cette loi d'addition est complète, i.e. s'applique dans tous les cas, si le paramètre d de la courbe n'est pas un carré dans le corps fini. Ces courbes permettent à une implémentation très efficace de la multiplication scalaire d'un point de la courbe, qui se montre aussi résistante aux attaques par canaux cachés. C'est dans ce contexte que nous nous sommes intéressés à l'implémentation efficace du couplage sur les courbes d'Edwards, ce qui permettrait l'implémentation des protocoles en cryptographie à base de couplages entièrement en coordonnées d'Edwards. En utilisant une isogénie de degré 4 d'une courbe d'Edwards vers une autre courbe de genre 1, nous avons donné la première implémentation efficace du couplage sur des courbes génériques en coordonnées d'Edwards [50]. Notre méthode a des performances comparables à celles d'une implémentation du couplage sur la forme Weierstrass d'une courbe elliptique. Nous donnons aussi un algorithme efficace pour la multiplication scalaire dans le cas des courbes d'Edwards dont le paramètre d est un carré dans le corps fini.

Notations

Throughout this work, we use the standard notations

$$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$$

to represent integers, rational numbers, real numbers and complex numbers. We denote by K a perfect field (i.e. every algebraic extension of K is separable) and by $\overline{K}$ its algebraic closure. We denote by $\mathbb{F}_p$ a finite field, with p a prime number and by $\mathbb{F}_q$ a finite field with $q = p^r$.

Part I

Preliminaries

Chapter 2

Arithmetic of elliptic curves

In this chapter we define elliptic curves, which are the main object of study in this dissertation. We first give some the basic notions of algebraic geometry and then introduce elliptic curves and present their arithmetic. Finally, we study algebraic maps for these curves and define the Weil pairing and the Tate pairing. We assume that the reader is familiar with basic concepts in commutative algebra such as rings, ideals, fields, modules. All these notions are given, for example, in Lang's *Algebra* [62] or in Atiyah and Macdonald's book [4]. Our *algebraic geometry* dictionary follows the exposition of Silverman [86] and Hartshorne [45]. For the proofs of results, we refer to these two books.

2.1 Algebraic varieties

Let K be a field and $\bar{K}$ its algebraic closure. For some positive integer n, we define the *affine n-space* $\mathbb{A}^n$ as the set of n-tuples $(x_1, x_2, \ldots, x_n)$ with $x_i \in \bar{K}$. We denote by $\mathbb{A}^n(K)$ the set of *K-rational points in* $\mathbb{A}^n$:

$$\mathbb{A}^n(K) = \{P = (x_1, \ldots, x_n) \in \mathbb{A}^n | x_i \in K\}.$$

The *projective n-space* $\mathbb{P}^n$ is the set of all $(n+1)$-tuples $(x_0, x_1, \ldots, x_n) \in \mathbb{A}^{n+1}$ such that at least one x_i is non-zero, modulo the equivalence relation given by

$$(x_0, x_1, \ldots, x_n) \sim (y_0, y_1, \ldots, y_n),$$

if there is a $\lambda \in \bar{K}^*$ with $x_i = \lambda y_i$ for all i. We denote the equivalence class of $(x_0, \ldots, x_n)$ by $[x_0, \ldots, x_n]$. The affine n-space $\mathbb{A}^n$ can be embedded into the projective n-space $\mathbb{P}^n$ by identifying $(x_1, \ldots, x_n)$ with $[x_1, \ldots, x_n, 1]$.
We also denote by $\mathbb{P}^n(K)$ the set of *K-rational points in* $\mathbb{P}^n$:

$$\mathbb{P}^n(K) = \{P = [x_0, \ldots, x_n] \in \mathbb{P}^n | x_i \in K\}.$$

An element σ of the Galois group $G_{\bar{K}/K}$ acts on $\mathbb{P}^n$ as follows

$$[x_0, \ldots, x_n]^\sigma = [x_0^\sigma, \ldots, x_n^\sigma].$$

Let $\bar{K}[X_1, \ldots, X_n]$ be a polynomial ring in n variables and let $I \subset \bar{K}[X_1, \ldots, X_n]$ be an ideal. We denote by V_I the subset

$$V_I = \{P \in \mathbb{A}^n | f(P) = 0 \text{ for all } f \in I\}.$$

We call a set of the form V_I an affine *algebraic set*. To any algebraic set V we associate the *ideal* of V by

$$I(V) = \{f \in \bar{K}[X] | f(P) = 0 \text{ for all } P \in V\}.$$

We say that an algebraic set is *defined over* K if its ideal can be generated by polynomials in $K[X]$. If V is defined over K, the *set of K-rational points of* is the set

$$V(K) = V \cap \mathbb{A}^n(K)$$

We may now define an affine variety.

Definition 2.1. An affine algebraic set V is called an affine variety if the ideal $I(V)$ associated to it is prime.

For a variety V defined over K, we also define its *function field*.

Definition 2.2. Let V be a variety defined over K. Then the affine coordinate ring of V is defined by

$$K[V] = \frac{K[X_1, \ldots, X_n]}{(I(V))}.$$

$K[V]$ is an integral domain and its quotient field, denoted $K(V)$, is called the function field of V.

The *dimension* of a variety is actually its dimension as a topological space. For details on the topology of a variety, the reader is referred to [45]. We give here an algebraic definition of the dimension.

Definition 2.3. Let V be a variety. The dimension of V is the transcendence degree of $\bar{K}(V)$ over $\bar{K}$.

We denote the dimension of a variety V by $\dim V$.

Example 2.1. The dimension of $\mathbb{A}^n$ is n, since $\bar{K}(\mathbb{A}^n) = \bar{K}(X_1, \ldots, X_n)$. $V \subset \mathbb{A}^n$ has dimension $n-1$ if and only if it is given by a single non-constant polynomial equation $f(X_1, \ldots, X_n) = 0$ (see [45, I.1.3]).

We shall now define the notion of *smooth* or *non-singular* algebraic variety. This notion corresponds to the notion of manifold in topology. It is thus natural to introduce this notion in terms of the derivatives defining the variety. But before doing that, note that by the Hilbert basis theorem (see [4, Theorem 7.6]) all ideals in $\bar{K}[X_1, \ldots, X_n]$ and $K[X_1, \ldots, X_n]$ are finitely generated, which explains the fact that we may consider a finite number of generators in the following definition.

Definition 2.4. Let V be a variety, $P \in V$, and $f_1, \dots, f_m \in \bar{K}$ a set of generators for $I(V)$. We say that V is non-singular (or smooth) at P if the $m \times n$ matrix

$$(\partial f_i / \partial X_j(P))_{1 \le i \le m, 1 \le j \le n}$$

has rank $n - \dim V$. If V is non-singular at every point, then we say that V is non-singular.

Example 2.2. Let V be the following variety in $\mathbb{A}^2$

$$V : Y^2 = X^3.$$

The singular points on V satisfy

$$Y = X = 0.$$

Thus V has one singular point, namely $(0, 0)$.

One can easily show that this definition of the notion of non-singular variety is independent of the set of generators of the ideal of V chosen. However, this definition apparently depends on the embedding of V in the affine space $\mathbb{A}^n$. We will now show that the notion of non-singular variety can be described intrinsically in terms of functions on the variety V. We first define the ideal M_P of $\bar{K}[V]$ by

$$M_P = \{f \in \bar{K}[V] | f(P) = 0\}.$$

It is easy to see that M_P is a maximal ideal, due to the fact that the map

$$\begin{array}{ccc} \bar{K}[V]/M_P & \to & \bar{K} \\ f & \to & f(P) \end{array}$$

is an isomorphism.

Proposition 2.1. Let V be a variety. A point $P \in V$ is non-singular if and only if

$$\dim_{\bar{K}} M_P / M_P^2 = \dim V.$$

Proof. See [45], Theorem I.5.1. □

Definitions similar to those we have presented for affine spaces can be given for projective spaces. But before doing that, we need to explain what it means that a projective point is a zero of a polynomial. Let us first introduce the notion of *homogeneous polynomials*.

Definition 2.5. A polynomial $P(x_1, \dots, x_n)$ is homogeneous of degree d if for all $\lambda \in K$,

$$P(\lambda x_1, \dots, \lambda x_n) = \lambda^d P(x_1, \dots, x_n).$$

Note that for a homogeneous polynomial f, it makes sense to say that $f(P) = 0$ for a point $P \in \mathbb{P}^n$. An ideal of $K[X]$ is called *homogeneous* if it is generated by homogeneous polynomials. To any homogeneous ideal I, we associate

$$V_I = \{P \in \mathbb{P}^n \mid f(P) = 0 \text{ for all homogeneous } f \in I\}.$$

A set of the form V_I is called a *projective algebraic set*. To any projective algebraic set V we associate $I(V)$, the homogeneous ideal of $\overline{K}[X_1, \ldots, X_n]$ generated by

$$\{f \in \overline{K}[X_1, \ldots, X_n] \mid f \text{ is homogeneous and } f(P) = 0 \text{ for all } P \in V\}.$$

We say that V is *defined over* K if its ideal can be generated by homogeneous polynomials in $K[X]$. If V is defined over K, the set of *K-rational points of* V is the set

$$V(K) = V \cap \mathbb{P}^n.$$

Just like in the affine case, we define *varieties*.

Definition 2.6. A projective algebraic set is a projective variety if its homogeneous ideal $I(V)$ is a prime ideal in $\overline{K}[X]$.

For $1 \leq i \leq n$, we define the following inclusion

$$\begin{array}{rcl} \varphi_i : \mathbb{A}^n & \to & \mathbb{P}^n \\ (y_1, \ldots, y_n) & \to & [y_1, y_2, \ldots, y_{i-1}, 1, y_i, \ldots, y_n] \end{array}$$

and we also denote $U_i = \{(x_0, \ldots, x_n) \in \mathbb{P}^n | x_i \neq 0\}$. Note that $\mathbb{P}^n = \cup_{1 \leq i \leq n} U_i$. Now there is also a natural bijection

$$\begin{array}{rcl} \varphi_i^{-1} : U_i & \to & \mathbb{A}^n \\ {[x_0, \ldots, x_n]} & \to & \left(\dfrac{x_0}{x_i}, \dfrac{x_1}{x_i}, \ldots, \dfrac{x_{i-1}}{x_i}, \dfrac{x_{i+1}}{x_i}, \ldots, \dfrac{x_n}{x_i}\right). \end{array}$$

If V is a projective algebraic set defined by an homogenous ideal $I(V)$, we designate by $V \cap \mathbb{A}^n$ any of the sets $\varphi_i^{-1}(V \cap U_i)$. This set is actually an affine algebraic set, whose ideal is given by

$$I(V \cap \mathbb{A}^n) = \{f(Y_1, \ldots, Y_{i-1}, 1, Y_i, \ldots, Y_n) \mid f(X_0, \ldots, X_n) \in I(V)\}.$$

Since $U_1, \ldots, U_n$ cover all $\mathbb{P}_n$, it follows that a projective variety is covered by the affine varieties $V \cap U_0, \ldots, V \cap U_n$, via the corresponding maps ϕ_i^{-1}.

In reverse, given an affine algebraic set V and its ideal $I(V)$, we may associate to it a projective algebraic set, in the following way. For all $f \in I(V)$, we consider polynomials of the form

$$f^*(X_0, \ldots, X_n) = X_i^d f\left(\frac{X_0}{X_i}, \frac{X_1}{X_i}, \ldots, \frac{X_{i-1}}{X_i}, \frac{X_{i+1}}{X_i}, \ldots, \frac{X_n}{X_i}\right),$$

where $d = \deg(f)$ is the smallest integer for which f^* is a polynomial. We call the *projective closure of* V, denoted $\overline{V}$, the projective algebraic set whose homogenous ideal is generated by the set

$$\{f^*(X) | f \in I(V)\}.$$

The following result allows us to define the properties of projective varieties in terms of properties of affine varieties.

Proposition 2.2. (a) Let V be an affine variety. Then $\overline{V}$ is a projective variety, and

$$V = \overline{V} \cap \mathbb{A}^n.$$

(b) Let V be a projective variety. Then $V \cap \mathbb{A}^n$ is an affine variety, and either

$$V \cap \mathbb{A}^n = \emptyset \quad \text{or} \quad V = \overline{V \cap \mathbb{A}^n}.$$

Proof. See [45, I.2.3]. □

Consequently, we call the function field of V, denoted by $K(V)$, the function field of $V \cap \mathbb{A}^n$. For some point $P \in V$, take $\mathbb{A}^n \subset \mathbb{P}^n$ with $P \in \mathbb{A}^n$. We say that V is *non-singular* (or *smooth*) at P if $V \cap \mathbb{A}^n$ is non-singular at P. We end this section by defining algebraic maps between projective varieties, i.e. maps defined by rational functions.

Definition 2.7. Let V_1 and $V_2 \subset \mathbb{P}^n$ be two projective varieties. A rational map from V_1 to V_2 is a map of the form

$$\phi : V_1 \to V_2$$

$$\phi = [f_0, \ldots, f_n],$$

where $f_0, \ldots, f_n \in \overline{K}(V_1)$ verify the property that for every point $P \in V_1$ at which $f_0, ..., f_n$ are defined,

$$\phi(P) = [f_0(P), \ldots, f_n(P)] \in V_2.$$

If there is $\lambda \in \overline{K}$ such that $\lambda f_0, ..., \lambda f_n \in K(V_1)$, we say that ϕ is *defined over K*.

Definition 2.8. A rational map $\phi = [f_0, \ldots, f_n]$ is *regular* (or *defined*) at a point $P \in V_1$ if there is a function $g \in \overline{K}(V_1)$ such that

(a) gf_i is defined at point P, for all i

(b) there is a j such that $gf_j(P) \neq 0$.

If such a g exists, we set

$$\phi(P) = [(gf_0)(P), \ldots, (gf_n)(P)].$$

A rational map which is regular at every point is called a *morphism*.

2.2 Algebraic curves

A *curve* is a projective smooth variety of dimension 1. In this section we describe local rings of curves and then study rational maps on curves and their local properties.

Example 2.3. Consider the variety C in $\mathbb{P}^3$ given by the zeros of the polynomial equation

$$y^2 = x^3 + x$$

(with the convention that $C \in \mathbb{P}^3$ is actually given by the homogenization of the polynomial $y^2 - x^3 - x$). Then C is a curve.

The local ring of C at P, denoted $\bar{K}[C]_P$, is the localization of $\bar{K}[C]$ at M_P. It can be described as follows

$$\bar{K}[C]_P = \{F \in \bar{K}(C) | F = f/g \text{ for some } f, g \in \bar{K}[C] \text{ with } g(P) \neq 0\}.$$

This ring is a discrete valuation ring. We briefly remind that a *discrete valuation ring R* is a principal ideal domain with only one non-zero maximal ideal. On the fraction field K of such a ring, we usually define a function $v : K \to \mathbb{Z} \cup \{\infty\}$ such that $R = \{x |\ x \in K, v(x) \geq 0\}$. This function is called a *discrete valuation*. For details on discrete valuation rings, we refer the reader to [62].

Proposition 2.3. $\bar{K}[C]_P$ is a discrete valuation ring, whose the valuation is given by:

$$\text{ord}_P : \bar{K}[C]_P \to \{0, 1, 2, ...\} \cup \{\infty\}$$

$$\text{ord}_P(f) = \max\{d \in \mathbb{Z} | f \in M_P^d\}.$$

Proof. See [86], Prop. II.1.1. □

Using $\text{ord}_P(f/g) = \text{ord}_P(f) - \text{ord}_P(g)$, we extend ord_P to $\bar{K}(C)$,

$$\text{ord}_P | \bar{K}(C) \to \mathbb{Z} \cup \{\infty\}.$$

A *uniformizer* of C at P is a function $t \in \bar{K}(C)$ such that $\text{ord}_P(t) = 1$ (i.e. a generator of M_P). If $f \in \bar{C}$ is as above, then the valuation at P, $\text{ord}_P(f)$, is called the *order of f at P*. If $\text{ord}_P(f) > 0$, we say that *f has a zero at P*; if $\text{ord}_P < 0$ we say that *f has a pole at P*.

Proposition 2.4. Let C be a smooth curve and $f \in \bar{K}(C)$. Then there are only finitely many points of C at which f has a zero or a pole. Further, if f has no poles, then $f \in \bar{K}$.

Proof. [45, I.6.5] and [45, I.3.4a] □

We will now give some important results about rational maps on smooth curves.

Theorem 2.1. (a) Let $\phi : C_1 \to C_2$ a rational map between two curves. Suppose, moreover, that C_1 is smooth. Then ϕ is a morphism.

(b) If $\phi : C_1 \to C_2$ is a non-constant morphism of curves, then it is surjective.

Proof. See [86, Prop. II.2.1] for (a) and [45, Prop. II.6.8] for (b). □

Now consider a non-constant rational map $\phi : C_1 \to C_2$ defined over K. Then composition with ϕ induces an injection of function fields:

$$\begin{array}{rcl} \phi^* : K(C_2) & \to & K(C_1) \\ f & \mapsto & f \circ \phi. \end{array}$$

Theorem 2.2. If $\phi : C_1 \to C_2$ is a morphism defined over K, then $K(C_1)$ is a finite extension of $K(C_2)$.

Proof. [45, Prop. II.6.8]. □

Definition 2.9. Let $\phi : C_1 \to C_2$ be a map of curves defined over K. If ϕ is constant, we define its degree to be 0. Otherwise, the degree of ϕ is given by

$$\deg \phi = [K(C_1) : \phi^* K(C_2)].$$

We say that ϕ is *separable* (*inseparable, purely inseparable*) if the extension $K(C_1)/\phi^* K(C_2)$ has the corresponding property.

We denote the separable and inseparable degrees of the extension $K(C_1)/\phi^* K(C_2)$ by $\deg_s \phi$ and $\deg_i \phi$, respectively. We shall now take a look at the behavior of a map of smooth curves locally, in the neighborhood of a point.

Definition 2.10. Let $\phi : C_1 \to C_2$ be a non-constant map of smooth curves and let $P \in C_1$. The ramification index of ϕ at P, denoted $e_\phi(P)$, is given by

$$e_\phi(P) = \mathrm{ord}_P(\phi^* t_{\phi(P)}),$$

where $t_{\phi(P)} \in K(C_2)$ is a uniformizer at point $\phi(P)$.

Note that $e_\phi(P) \geq 1$. We say that ϕ is *unramified at point P* if $e_\phi(P) = 1$ and that ϕ is *unramified* if it is unramified at every point of C_1.

2.3 Divisors

In this section we shall associate an abelian group to each non-singular curve. For elliptic curves, which are the main object of study in this thesis, one can attach a group structure to the set of points of the curve. However, this is not possible for all smooth curves. In the general case, the way out is to consider formal finite sums of points, called *divisors*, as group elements. We present this construction here, and explain later that for elliptic curves, this group structure coincides with the one obtained considering points as elements. Nevertheless, in the following sections it will become clear that divisors are important tools in studying of the geometry of elliptic curves.

Let C be a smooth curve. The *divisor group* of C, denoted by Div(C) is the free abelian group generated by the points of the curve. This means that a *divisor* $D \in \mathrm{Div}(C)$ is a formal sum of points

$$D = \sum_{P \in C} n_P (P)$$

with $n_P \in Z$ and $n_P = 0$, for all but finitely many $P \in C$. The *degree* of the divisor D is defined by

$$\deg D = \sum_{P \in C} n_P.$$

It follows that the divisors of degree 0 form a subgroup of Div(C), that we denote by

$$\mathrm{Div}^0(C) = \{D \in \mathrm{Div}(C) | \deg D = 0\}.$$

If $f \in \bar{K}(C)^*$, then we associate to f the following divisor

$$\mathrm{div}(f) = \sum_{P \in C} \mathrm{ord}_P(f)(P).$$

Note that this makes sense, as the sum of points above is finite by Proposition 2.4. We say that a divisor D is *principal* if it is of the form $\operatorname{div}(f)$, for some $f \in \overline{K}(C)$. It is a fact that if $f \in \overline{K}(C)^*$, then $\deg(\operatorname{div}(f)) = 0$ (see [86, Prop. II.3.1]). Hence, the set of principal divisors is a subgroup of $\operatorname{Div}^0(C)$. The quotient of $\operatorname{Div}^0(C)$ by the subgroup of principal divisors is called the *divisor class group* $\operatorname{Pic}^0(C)$.

If C is defined over K, we let the Galois group of $\overline{K}/K$ act on $\operatorname{Div}(C)$ in an obvious way, given that $G_{\bar{K}/K}$ acts on points:

$$D^\sigma = \sum_{P \in C} n_p (P^\sigma).$$

We say that D is *defined over* K if $D^\sigma = D$ for all $\sigma \in G_{\bar{K}/K}$. In particular, it is obvious that if $f \in K(C)$, then $\operatorname{div}(f)$ is defined over K. The following example is taken from [86] and will be useful in the remainder of this dissertation:

Example 2.4. Assume that $\operatorname{char}(K) \neq 2$. Let $e_1, e_2, e_3 \in \overline{K}$ be distinct, and consider the curve

$$C : y^2 = (x - e_1)(x - e_2)(x - e_3).$$

This curve has only one point with $Z = 0$ that we denote by $O = (0, 1, 0)$. Note that the function $Z = 0$ intersects the curve at point O with multiplicity 3. We denote by $P_i = (e_i, 0) \in C$. Then

$$\begin{aligned} \operatorname{div}\left(\frac{X - e_i Z}{Z}\right) &= 2(P_i) - 2(O) \\ \operatorname{div}\left(\frac{Y}{Z}\right) &= (P_1) + (P_2) + (P_3) - 3(O). \end{aligned}$$

Let $\phi : C_1 \to C_2$ be a non-constant map of smooth curves. We saw that ϕ induces the map:

$$\phi^* : \overline{K}(C_2) \to \overline{K}(C_1).$$

Similarly, we define maps for the divisor groups. We denote

$$\begin{aligned} \phi^* : \operatorname{Div}(C_2) &\to \operatorname{Div}(C_1) \\ (Q) &\to \sum_{P \in \phi^{-1}(Q)} e_\phi(P)(P), \end{aligned}$$

which we extend $\mathbb{Z}$-linearly to $\operatorname{Div}(C_2)$.

Proposition 2.5. Let C_1 and C_2 be two smooth curves and $\phi : C_1 \to C_2$ a rational map.

(a) $\deg(\phi^* D) = (\deg \phi)(\deg D)$, for all $D \in \operatorname{Div}(C_2)$;

(b) $\phi^*(\operatorname{div} f) = \operatorname{div}(\phi^* f) \quad$ for $\quad f \in \overline{K}(C_2)^*$;

(c) If $\psi : C_2 \to C_3$ is another such map, then $(\psi \circ \phi)^* = \phi^* \circ \psi^*$.

Proof. See [86, II.3.6] □

2.4 Elliptic curves and Weierstrass equations

An *elliptic curve* is a smooth curve of *genus* 1, with a specified basepoint. In order to simplify our exposition, we give a definition of elliptic curves, which is in fact a consequence of the Riemann-Roch theorem for curves of genus 1. For details on the genus of a curve and the Riemann-Roch theorem, the reader should refer to [86].

Definition 2.11. An elliptic curve E is a non-singular projective curve whose equation is a Weierstrass equation, i.e. an equation of the form:

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

with $a_1, a_2, a_3, a_4, a_6 \in \bar{K}$.

The curve is defined over K if $a_1, a_2, a_3, a_4, a_6 \in K$. The only point on the curve with $Z = 0$ is $O = [0 : 1 : 0]$. We call it the point at infinity. By using non-homogeneous coordinates $x = X/Z$ and $y = Y/Z$, the other points can be identified with points on the affine Weierstrass curve

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Now suppose that $\mathrm{char}(K) \neq 2$. We may then substitute (x, y) for $(x, y + \frac{1}{2}(a_1x + a_3))$. We obtain a new equation for the curve

$$E : y^2 = x^3 + \frac{b_2}{4}x^2 + \frac{b_4}{2}x + \frac{b_6}{4},$$

where $b_2 = a_1^2 + 4a_2$, $b_4 = 2a_4 + a_1a_3$, $b_6 = a_3^2 + 4a_6$. If further $\mathrm{char}(K) \neq 2, 3$, we may replace (x, y) by $(\frac{x-3b_2}{36}, \frac{y}{108})$ and we get a simple equation for the curve

$$E : y^2 = x^3 - 27c_4x - 54c_6,$$

called the short Weierstrass form. We also define

$$b_8 = a_1^2a_6 - a_1a_3a_4 + 4a_2a_6 + a_2a_3^2 - a_4^2,$$
$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \text{ and } j = c_4^3/\Delta.$$

The constant Δ is called the *discriminant* of the Weierstrass equation. We will see that the constant j is actually an invariant of the curve that we call the *j-invariant* of the curve. Note that the definitions of Δ and j are also correct for $\mathrm{char}(K) = 2, 3$. The proofs of the following two propositions are essentially given in Section III.1 and Appendix A of [86].

Proposition 2.6. (a) The curve given by a Weierstrass equation is non-singular if and only if $\Delta \neq 0$.

(b) Two elliptic curves are isomorphic (over $\bar{K}$) if and only if they have the same j-invariant.

(c) Let $j_0 \in \bar{K}$. Then there exists an elliptic curve (defined over $K(j_0)$) with j-invariant equal to j_0.

Proposition 2.7. Let E be an elliptic curve defined over K, with $\mathrm{char}(K) \neq 2, 3$ and j-invariant j. Then E is isomorphic to a curve given by the following equation

(a) $y^2 = x^3 + a$, for some $a \in K$ if $j = 0$.

(b) $y^2 = x^3 + ax$, for some $a \in K$ if $j = 1728$.

(c) $y^2 = x^3 - \frac{36}{j-1728}x - \frac{1}{j-1728}$, up to a quadratic twist, if $j \neq 0, 1728$.

2.5 The Group Law

Let E be an elliptic curve given by a Weierstrass equation. As stated in Section 2.3, we attach to the elliptic curve a group, whose set of elements is the set of points of the elliptic curve. We then show that this group is actually isomorphic to $\mathrm{Pic}^0(E)$.

Definition 2.12. Let $P, Q \in E$, L the line connecting P and Q (tangent line to E if $P = Q$), and R the third point of intersection of L with E. Let $L^{'}$ be the line connecting R and O. Let $P + Q$ be the point such that $L^{'}$ intersects E at R, O, and $P + Q$.

This rule is illustrated in Figure 2.5. The fact that $L \cap E$, taken with multiplicities, consists of three points, is a special case of Bezout's theorem (see [45, I.7.8]). The addition law defined above makes E into an abelian group (see [86, III.2.2] for the proof). We give below a description of this addition law for curves defined over a field K with $\mathrm{char}(K) \neq 2, 3$, having a the Weierstrass equation of the form $y^2 = x^3 + ax + b$.

Proposition 2.8. Let E be an elliptic curve defined over a field K with $\mathrm{char}(K) \neq 2, 3$, given in short Weierstrass form. The addition law in definition 2.12 has the following properties:

(a) We have $P + O = O + P = P$, for all $P \in E$, i.e. O is the neutral element of the addition law.

(b) If $P = (x_P, y_P)$, then its inverse with respect to the addition law is $-P = (-x_P, y_P)$.

(c) If $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$ with $Q \neq -P$, we denote by

$$\lambda = \begin{cases} \frac{y_Q - y_P}{x_Q - x_P} & \text{if } P \neq Q, \\ \frac{3x_P^2 + a}{2y_P} & \text{if } P = Q. \end{cases}$$

The coordinates of $P + Q$ are then

$$\begin{aligned} x_{P+Q} &= \lambda^2 - x_P - x_Q, \\ y_{P+Q} &= \lambda(x_{P+Q} - x_P) + y_P. \end{aligned}$$

Proof. See [86, III.2.2] and [86, III.2.3]. □

Notation 2.1. For $P \in E$ and $m \in \mathbb{Z}$, we denote

$$mP = P + \cdots + P \text{ (m terms), for } m > 0, \ 0P = O, \text{ and } mP = (-m)(-P) \text{ for } m < 0.$$

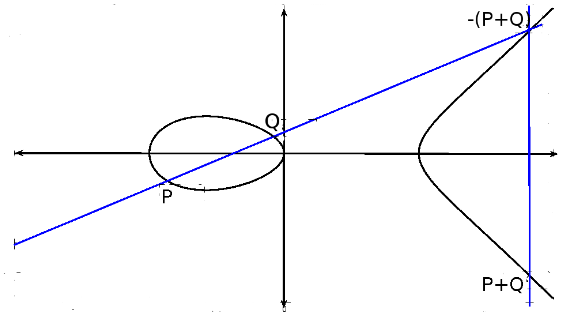


Figure 2.1: Addition on an elliptic curve

Proposition 2.9. Let E be an elliptic curve over a field K and O its point at infinity. For every divisor $D \in \mathrm{Div}^0(E)$ there exists a unique point $P \in E$ so that $D \sim (P) - (O)$. Let $\Lambda : \mathrm{Div}^0(E) \to E$ be the map given with this association. This map is surjective. Moreover, if $D_1, D_2 \in \mathrm{Div}^0(E)$, then

$$\Lambda(D_1) = \Lambda(D_2) \text{ if and only if } D_1 \sim D_2.$$

Thus Λ induces a bijection of sets (which we also denote by Λ)

$$\sigma : \mathrm{Pic}^0(E) \to E.$$

The group law on E defined in definition 2.12 and the group law induced from $\mathrm{Pic}^0(E)$ by using Λ are the same.

Proof. [86, III.3.4]. □

An important consequence of this proposition is the following corollary.

Corollary 2.1. Let E be an elliptic curve and $D = \sum n_P(P) \in \mathrm{Div}(E)$. Then D is principal if and only if $\sum n_P = 0$ and $\sum n_P P = 0$.

Proof. [86, III.3.5] □

2.6 Isogenies

Definition 2.13. Let E_1 and E_2 two elliptic curves. An *isogeny* between E_1 and E_2 is a morphism $\phi : E_1 \to E_2$ satisfying $\phi(O) = O$. E_1 and E_2 are *isogenous* if there is an isogeny ϕ between them with $\phi(E_1) \neq \{O\}$.

From Theorem 2.1 we have that ϕ satisfies either $\phi(E_1) = \{O\}$ or $\phi(E_1) = E_2$. Since there is a group structure on an elliptic curve, it is natural to investigate isogenies that are also group homomorphisms. It turns out that all isogenies are group homomorphisms.

Theorem 2.3. Let $\phi : E_1 \to E_2$ be an isogeny. Then

$$\phi(P + Q) = \phi(P) + \phi(Q) \text{ for all points } P, Q \in E_1$$

Proof. [86, III.4.8] □

We denote by $\mathrm{Hom}(E_1, E_2)$ the set of all isogenies from E_1 to E_2. The *endomorphism ring* of E is defined as $\mathrm{End}(E) = \mathrm{Hom}(E, E)$. The invertible elements of $\mathrm{End}(E)$ are called *automorphisms* and the set of automorphisms is denoted by $\mathrm{Aut}(E)$. We also denote by $\mathrm{Hom}_K(E_1, E_2)$ the set of isogenies from E_1 to E_2 defined over K and $\mathrm{End}_K(E)$ the set of endomorphisms of E defined over K. An isogeny defined over K is called *K-rational* or simply *rational*. We give now some important properties of isogenies.

Theorem 2.4. Let $\phi : E_1 \to E_2$ be a non-constant isogeny.

(a) For every point $Q \in E_2$, $\#\phi^{-1}(Q) = \deg_s \phi$. Further, for every $P \in E_1$, $e_\phi(P) = \deg_i(\phi)$.

(b) If ϕ is separable, then ϕ is unramified and $\#\mathrm{Ker}\ \phi = \deg\ \phi$.

Proof. [86, III.4.10] □

Example 2.5. Let K be a perfect field of characteristic $p > 0$, $q = p^r$, E an curve defined over K given by the Weierstrass equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

We define $E^{(q)}$ the elliptic curve given by the following equation

$$E^{(q)} : y^2 + a_1^q xy + a_3^q y = x^3 + a_2^q x^2 + a_4^q x + a_6^q.$$

We define the Frobenius morphism

$$\begin{array}{rcl} \pi : E & \to & E^{(q)} \\ (x, y) & \mapsto & (x^q, y^q). \end{array}$$

If $K = \mathbb{F}_q$, then π is an endomorphism $\pi : E \to E$, which commutes with all elements of $\mathrm{End}_K(E)$.

Proposition 2.10. The Frobenius endomorphism has the following properties

(a) ϕ is purely inseparable.

(b) $\deg\ \phi = q$.

(c) If $K = \mathbb{F}_q$, then π is an endomorphism $\pi : E \to E$ and $1 - \pi$ is a separable isogeny.

Proof. [86, II.2.11 and III.5.5] □

Corollary 2.2. Every map $\psi : E_1 \to E_2$ of elliptic curves over a field of characteristic $p > 0$ factors as

$$E_1 \xrightarrow{\pi} E_1^{(q)} \xrightarrow{\lambda} E_2,$$

where $q = \deg_i(\psi)$, π is the q^{th}-power Frobenius map and λ is separable.

Proof. Also [86, Cor. II.2.12]. □

Example 2.6. Let E be an elliptic curve. For each $m \in \mathbb{Z}$ we can define the *multiplication by m* map

$$\begin{aligned} [m] : E &\to E \\ P &\mapsto mP. \end{aligned}$$

It can be shown (see [86, III.4.1] and [86, III.4.2]) that $[m]$ is a non-constant isogeny. Moreover, $\deg[m] = m^2$ and $\widehat{[m]} = [m]$.

An important property of an isogeny is the existence of its dual.

Theorem 2.5. Let $\phi : E_1 \to E_2$ be a non-constant isogeny of degree m. Then there exists a unique isogeny $\hat{\phi} : E_2 \to E_1$ such that $\hat{\phi} \circ \phi = [m]$ and $\phi \circ \hat{\phi} = [m]$.

Proof. [86, III.6.1] □

If $\phi : E_1 \to E_2$ is an isogeny, we call the isogeny $\hat{\phi} : E_2 \to E_1$ given in Theorem 2.5 its *dual isogeny*.

Theorem 2.6. Let $\phi, \psi : E_1 \to E_2$ be two isogenies.

(a) $\widehat{\phi \circ \psi} = \hat{\psi} \circ \hat{\phi}$.

(b) $\widehat{\phi + \psi} = \hat{\phi} + \hat{\psi}$.

(c) $\deg \hat{\phi} = \deg \phi$.

(d) $\hat{\hat{\phi}} = \phi$.

Proof. See [86, Theorem III.6.2]. □

We call Ker$[m]$ the *m-torsion group* of E. We denote this group by $E[m]$. More precisely, we have

$$E[m] = \{P \in E(\overline{K}) | [m]P = O\}$$

Using *division polynomials*, that we define below, we derive explicit formulae for the computation of $[m]$.

Definition 2.14. Using the notations from Section 2.4, the m-th division polynomial of an elliptic curve, that we note by f_m, is given by:

$$f_0(X) = 0,\ f_1(X) = 1,\ f_2(X) = 1,\ f_3(X) = 3X^4 + b_2X^3 + 3b_4X^2 + 3b_6X + b_8,$$
$$f_4(X) = 2X^6 + b_2X^5 + 5b_4X^4 + 10b_6X^3 + 10b_8X^2 + (b_2b_8 - b_4b_6)X + (b_4b_8 - b_6^2),$$

and, by letting $F(X) = 4X^3 + b_2X^2 + 2b_4X + b_6$,

$$\begin{aligned} f_{2m} &= f_m(f_{m+2}f_{m-1}^2 - f_{m-2}f_{m+1}^2), \\ f_{2m+1} &= \begin{cases} F^2 f_{m+2}f_m^3 - f_{m-1}f_{m+1}^3 & \text{if } m \text{ is pair,} \\ f_{m+2}f_m^3 - f_{m-1}f_{m+1}^3F^2 & \text{otherwise.} \end{cases} \end{aligned}$$

The degree of the polynomial f_m is $(m^2 - 1)/2$ if m is odd and smaller than $(m^2 - 2)/2$, if m is even.

Theorem 2.7. Let E be an elliptic curve defined over a field K, P a point of E and $m \in \mathbb{N}^*$. Then

$$[m](P) = \begin{cases} O & \text{if } P \in E[m], \\ \left(\frac{\phi_m(x,y)}{\psi_m^2(x,y)}, \frac{\omega_m(x,y)}{\psi_m^3(x,y)}\right) & \text{if } P = (x, y) \in E(\overline{K})\backslash E[m], \end{cases}$$

where the polynomials ϕ_m, ψ_m and ω_m are given by

$$\psi_m = \begin{cases} (2Y + a_1X + a_3)f_m & \text{if } m \text{ is pair,} \\ f_m & \text{otherwise,} \end{cases}$$

and

$$\phi_m = X\psi_m^2 - \psi_{m-1}\psi_{m+1},\ 2\psi_m\omega_m = \psi_{2m} - \psi_m^2(a_1\phi_m + a_3\psi_m^2).$$

If the characteristic of K is different from 2, this theorem gives an explicit construction of $[m]$. Moreover, an important consequence of theorem 2.7 is that the x-coordinates of non-trivial m-torsion points of the curve are actually zeros of the m-division polynomial.

Theorem 2.8. Let $P \in E(\overline{K})$. Then $P \in E[m]$ if and only if $P = O$ or the x-coordinate of the point P verifies $f_m(x) = 0$

From the computation of $\deg[m]$ we deduce immediately the group structure of $E[m]$.

Corollary 2.3. Let E be an elliptic curve and $m \in \mathbb{Z}$, $m \neq 0$.

(a) If $\mathrm{char}(K) = 0$ or if m is prime to $\mathrm{char}(K)$, then

$$E[m] \cong (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z}).$$

(b) If $\mathrm{char}(K) = p$, then either

$$\begin{aligned} E[p^e] &\cong \{O\} \text{ or all } e = 1, 2, 3, \ldots, \text{ or} \\ E[p^e] &\cong \mathbb{Z}/p^e\mathbb{Z} \text{ for all } e = 1, 2, 3, \ldots \end{aligned}$$

2.7 Endomorphisms and automorphisms of an elliptic curve

It is obvious that the multiplication by $m \in \mathbb{Z}$ gives an injective ring homomorphism:

$$[] : \mathbb{Z} \to \mathrm{End}(E).$$

It follows that the endomorphism ring of an elliptic curve always contains $\mathbb{Z}$.

Definition 2.15. An elliptic curve E has *complex multiplication* if $\mathrm{End}(E)$ is larger than $\mathbb{Z}$.

Automorphisms of the curve E are very rare. Actually, we can easily check that an automorphism is necessarily of the form $(x, y) \to (u^2x, u^3y)$, with $u \in \overline{K}^*$. Further, this observation determines the group structure of $\mathrm{Aut}(E)$.

Theorem 2.9. Let E be an elliptic curve defined over a field K, with $\mathrm{char}(K) \neq 2, 3$. Then

$$\mathrm{Aut}(E) \cong \mu_n,$$

where μ_n is the group of n-th roots of unity and

$$n = \begin{cases} 2 \text{ if } & j(E) \notin \{0, 1728\}, \\ 4 \text{ if } & j(E) = 1728, \\ 6 \text{ if } & j(E) = 0. \end{cases}$$

2.8 Twists of elliptic curves

Let E, E' be elliptic curves defined over K and ϕ an isomorphism $\phi : E \to E'$, in the sense of definition 2.13, i.e. $\phi(O) = O'$. Then E' is called *the twist* of E. The degree d of the minimal extension field of K over which ϕ is defined is called *the degree of the twist* E'. We denote the set of twists of E by $\mathrm{Twist}((E, O)/K)$.

Theorem 2.10. Assume $\mathrm{char}(K) \neq 2, 3$ and that E is an elliptic curve given by a Weierstrass equation

$$E : y^2 = x^3 + ax + b.$$

Let n be given by

$$n = \begin{cases} 2 \text{ if } & j(E) \notin \{0, 1728\}, \\ 4 \text{ if } & j(E) = 1728, \\ 6 \text{ if } & j(E) = 0. \end{cases}$$

Then $\mathrm{Twist}((E, O)/K)$ is isomorphic to K^*/K^{*n} and for every $D \in K^*$ the corresponding elliptic curve $E_D \in \mathrm{Twist}(E, O)/K)$ is given by the following equation

(a) $E_D : y^2 = x^3 + D^2ax + D^3b$ if $j(E) \neq 0, 1728$;

(b) $E_D : y^2 = x^3 + Dax$ if $j(E) = 1728$;

(c) $E_D : y^2 = x^3 + Db$ if $j(E) = 0$.

The corresponding isomorphisms are $\phi_D : E \to E_D$ are:

$$\begin{aligned} (x, y) &\mapsto (D^{-1}x, D^{-3/2}y) && \text{if } j(E) \neq 0, 1728, \\ (x, y) &\mapsto (D^{-1/2}x, D^{-3/4}y) && \text{if } j(E) = 1728, \\ (x, y) &\mapsto (D^{-1/3}x, D^{-1/2}y) && \text{if } j(E) = 0. \end{aligned}$$

2.9 The Weil pairing

Let E be an elliptic curve defined over a field K and $l \in \mathbb{Z}$ such that l is prime to $p = \mathrm{char}(K)$ ($p > 0$). Let P and Q be two l-torsion points on the curve and D_P and D_Q two divisors with disjoint supports such that

$$D_P \sim (P) - (O) \text{ and } D_Q \sim (Q) - (O).$$

From Corollary 2.1 we deduce that there are two functions $f_{l,P}$ and $f_{l,Q}$ such that

$$\mathrm{div}(f_{l,P}) = lD_P \text{ and } \mathrm{div}(f_{l,Q}) = lD_Q.$$

We denote by $\mu_l \subset \bar{K}$ the group of l-th roots of unity. Given a function f and a divisor $D = \sum a_i(P_i)$, we denote by $f(D) = \prod_i f(P_i)^{a_i}$. The Weil pairing is a map

$$e_l : E[l] \times E[l] \to \mu_l$$

given by

$$e_l(P, Q) = \frac{f_{l,P}(D_Q)}{f_{l,Q}(D_P)}.$$

Note that the functions $f_{l,P}$ and $f_{l,Q}$ are unique up to a constant. It is easy to check that the value of the pairing does not depend on the choice of these functions. The fact that the Weil pairing is well defined, i.e. it does not depend on the choice of divisors, follows easily from the following result.

Proposition 2.11. (Weil's reciprocity) If C is a curve and $0 \neq f, g \in K(C)$ have disjoint supports, then

$$f(\mathrm{div}(g)) = g(\mathrm{div}(f)).$$

Proof. See Exercice 2.11 from [86]. □

Suppose that D'_Q is a divisor such that $D'_Q \sim D_Q$, i.e. there is a function f such that $D'_Q = D_Q + \mathrm{div}(f)$. We denote by $f'_{l,Q}$ the function such that $\mathrm{div}(f'_{l,Q}) = lD'_Q$. Then we have

$$\frac{f_{l,P}(D'_Q)}{f'_{l,Q}(D_P)} = \frac{f_{l,P}(D_Q) f_{l,P}(\mathrm{div}(f))}{f_{l,Q}(D_P) f(lD_P)} = \frac{f_{l,P}(D_Q)}{f_{l,Q}(D_P)}.$$

This proves that the Weil pairing is well defined, independently of the choice of representatives of the divisor classes. Using Weil's reciprocity, we also check that the Weil pairings has values in μ_l.

Proposition 2.12. The Weil pairing has the following properties:

(a) Bilinear:

$$\begin{aligned} e_l(P_1 + P_2, Q) &= e_l(P_1, Q)e_l(P_2, Q), \\ e_l(P, Q_1 + Q_2) &= e_l(P, Q_1)e_l(P, Q_2). \end{aligned}$$

(b) Alternating: $e_l(P, Q) = e_l(Q, P)^{-1}$. In particular, $e_l(P, P) = 1$.

(c) Non-degenerate: If $e_l(P,Q) = 1$ for all $Q \in E[l]$, then $P = O$.

(d) Galois invariant: For all $\sigma \in G_{\bar{K}/K}$, $e_l(P,Q)^\sigma = e_l(P^\sigma, Q^\sigma)$.

(e) Compatible: If $P \in E[ll']$ and $Q \in E[l]$, then

$$e_{ll'}(P,Q) = e_l([l']P, Q).$$

Proof. See [86, III.8.1]. □

Definition 2.16. A non-zero function f on E is normalized if the leading coefficient in the expression of f as a Laurent series in u_O, a uniformizer at O, is 1.

Remark 2.1. There are two equivalent definitions for the Weil pairing. We presented here the one that is used most in cryptography. For the other, we refer the reader to [86].

In [70], it was shown that by choosing normalized functions $f_{l,P}$ and $f_{l,Q}$ such that $\mathrm{div}(f_{l,P}) = l(P) - l(O)$ and $\mathrm{div}(f_{l,Q}) = l(Q) - l(O)$, the computation of the Weil pairing can be simplified.

Proposition 2.13. Let E/K be an elliptic curve, let $P, Q \in E(K)[l]$, and let $P \neq Q$. Then

$$e_l(P,Q) = (-1)^l \frac{f_{l,P}(Q)}{f_{l,Q}(P)}.$$

2.10 The Tate pairing

The Tate pairing was introduced by Tate in [92] as a pairing on abelian varities over local fields. Lichtenbaum gave in [66] an interpretation in the case of Jacobians of curves over local fields which gives an explicit computation of the pairing. In this dissertation, we are only interested in pairings over elliptic curves defined over finite fields. We will therefore introduce directly the Tate pairing for these curves. For more details on the Tate pairing on Jacobians of curves of higher genus, we refer the reader to [31].

Let E be an elliptic curve defined over some finite field $\mathbb{F}_q$ and l a number prime to q such that $l | \#E(\mathbb{F}_q)$ and $k \in \mathbb{N}$ minimal with $l | (q^k - 1)$. We call *k the embedding degree with respect to l*. Let $P \in E[l](\mathbb{F}_{q^k})$ and $Q \in E(\mathbb{F}_{q^k})/lE(\mathbb{F}_{q^k})$. Let $f_{l,P}$ be the function whose divisor is $\mathrm{div}(f_{l,P}) = l(P) - l(O)$. Take R a random point in $E(\mathbb{F}_q)$ such as the support of the divisor $D = (Q+R) - (R)$ is disjoint from the support of $f_{l,P}$. Then we define the Tate pairing as follows

$$\begin{array}{rcl} t_l : E(\mathbb{F}_{q^k})[l] \times E(\mathbb{F}_{q^k})/lE(\mathbb{F}_{q^k}) & \to & \mathbb{F}_{q^k}/(\mathbb{F}_{q^k})^l \\ (P,Q) & \to & f_{l,P}(Q+R)/f_{l,P}(R) \end{array}$$

Theorem 2.11. Let E be an elliptic curve defined over some finite field $\mathbb{F}_q$, l a number prime to q, such that $l | \#E(\mathbb{F}_q)$ and k the embedding degree with respect to l. The Tate pairing satisfies the following properties:

(a) Bilinearity: For all $P, P_1, P_2 \in E(\mathbb{F}_{q^k})[n]$ and for all $Q, Q_1, Q_2 \in E(\mathbb{F}_{q^k})/lE(\mathbb{F}_{q^k})$,

$$\begin{array}{rcl} t_l(P_1 + P_2, Q) & = & t_l(P_1,Q)t_l(P_2,Q) \\ t_l(P, Q_1 + Q_2) & = & t_l(P,Q_1)t_l(P,Q_2). \end{array}$$

(b) Non-degeneracy: For all $P \in E(\mathbb{F}_{q^k})[l]$, $P \neq O$, there is some $Q \in E(\mathbb{F}_{q^k})/lE(\mathbb{F}_{q^k})$ such that $t_l(P,Q) \neq 1$. Similarly, for all $Q \in E(\mathbb{F}_{q^k})/lE(\mathbb{F}_{q^k})$, there is a $P \in E(\mathbb{F}_{q^k})$ such that $t_l(P,Q) \neq 1$.

(c) Galois invariance: If $\sigma \in \mathrm{Gal}(\overline{\mathbb{F}}_{q^k}/\mathbb{F}_{q^k})$, $t_l(P^\sigma, Q^\sigma) = t_l(P,Q)^\sigma$.

Proof. While the proofs of (a) and (c) are easy and can be found for instance in [15], the proof of non-degeneracy is more complicated and implies either Galois cohomology (see [37]) or Kummer theory on function fields over finite fields (see [46]). □

The following result has important consequences in cryptography.

Theorem 2.12. (Balasubramanian, Koblitz) Let E be an elliptic curve defined over $\mathbb{F}_q$ such that $E(\mathbb{F}_q)$ contains a point of order l, with l prime with q. Let $k > 1$ be the embedding degree with respect to l. Then $E[l] \subset E(\mathbb{F}_{q^k})$.

Remark 2.2. From theorem 2.12 it follows that if $k > 1$ and no l^2-torsion point is defined over $\mathbb{F}_{q^k}$, we can actually define the Tate pairing as a bilinear non-degenerate map

$$t_l : E[l] \times E[l] \to \quad \mathbb{F}_{q^k}/(\mathbb{F}_{q^k})^l$$

Note that, if $k > 1$, $t_l(P,P) \in (\mathbb{F}_{q^k})^l$, for all points $P \in E[l]$. However, if $k = 1$, the value of $t_l(P,P)$ is not necessarily a l-th power of an element in $\mathbb{F}_q$. If only one subgroup of order l is defined over $\mathbb{F}_q$, then due to the non-degeneracy of the pairing $t_l(P,P) \notin (\mathbb{F}_q)^l$. Otherwise, if $E[l] \subset E(\mathbb{F}_q)$, both cases can occur. The case of curves with embedding degree 1 and $E[l] \subset E(\mathbb{F}_q)$ will be explained in chapter 5.

For cryptographic purposes, we prefer working with a pairing whose value is unique. We therefore introduce the *reduced Tate pairing* of two l-torsion points P and Q:

$$T_l(P,Q) = t_l(P,Q)^{\frac{q^k-1}{l}}.$$

Proposition 2.14. Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$, $P \in E[l]$, k the embedding degree with respect to l and $Q \in E(\mathbb{F}_{q^k})$. If the function $f_{l,P}$ is normalized, then the reduced Tate pairing is given by

$$T_l(P,Q) = f_{l,P}(Q)^{\frac{q^k-1}{l}}.$$

Proof. See [43, Lemma 1]. □

Chapter 3

Complex Multiplication

Most elliptic curves over $\mathbb{C}$ have endomorphism ring isomorphic to $\mathbb{Z}$. An elliptic curve with *complex multiplication*, i.e. with extra endomorphisms, has interesting properties. The endomorphism ring of an elliptic curve with complex multiplication is an order in a quadratic imaginary field, and via Deuring's reduction theorem [27], this structure is preserved over the finite field. In cryptography, this property is heavily exploited, as we will show in the following chapters.

In this chapter, we briefly review some concepts from the complex multiplication theory. To begin, in section 3.1 we review some basic facts on number fields, factorization of ideals and orders in quadratic imaginary fields. A key role in the study of elliptic curves with complex multiplication is played by the equivalence between elliptic curves over $\mathbb{C}$ and lattices over $\mathbb{C}$, which is explained in section 3.2. This leads us to consider in section 3.3 the j-invariant of a lattice and hence the j-invariant of an order in a quadratic imaginary field. In section 3.3, we show that if O is an order in a quadratic imaginary field, the j-invariant of O is an algebraic number. In section 3.4 we give the analytic properties of the j-function and we define the modular equation. Finally, in section 3.6.2 we give Deuring's reduction theorems, which are the basis for all algorithms constructing elliptic curves with complex multiplication over finite fields.

Our exposition is strongly based on results presented in Silverman's books [86] [87] and in Cox's book [25]. Some notions, such as Dedekind domains or ring class fields, are not defined. For a more complete treatment of the subject the reader is referred to the books of Lang [63] or Cox [25].

3.1 Orders in quadratic imaginary fields

A *number field* is a subfield of $\mathbb{C}$ which has a finite degree over $\mathbb{Q}$. We usually denote a number field by K and the degree of the extension $K/\mathbb{Q}$ by $[K:\mathbb{Q}]$. Given K, we may consider O_K *the ring of algebraic integers* of K, i.e. numbers $\alpha \in K$ which are roots of monic integer polynomials. We briefly recall that the field of fractions of O_K is K and that O_K is a free $\mathbb{Z}$-module of rank $[K:\mathbb{Q}]$ (see [19] for more details).

Suppose now that K is a quadratic field, i.e. $K = \mathbb{Q}(\sqrt{N})$, where $N \neq 0, 1$ is a squarefree integer. We define the *discriminant* of K, denoted by d_K, to be

$$d_K = \begin{cases} N & \text{if } N \equiv 1 \pmod 4, \\ 4N & \text{otherwise.} \end{cases}$$

Note that $d_K \equiv 0, 1 \pmod 4$ and that $K = \mathbb{Q}(\sqrt{d_K})$. The ring of integers O_K of K is given by

$$O_K = \begin{cases} \mathbb{Z}[\sqrt{N}] & \text{if } N \not\equiv 1 \bmod 4, \\ \mathbb{Z}\left[\frac{1+\sqrt{N}}{2}\right] & \text{if } N \equiv 1 \bmod 4. \end{cases}$$

(as shown in [25, Ex. II.E.5.7.]). Using the discriminant we may also write $O_K = \mathbb{Z}\left[\frac{d_K+\sqrt{d_K}}{2}\right]$. The following result tells us how prime numbers decompose in quadratic fields.

Proposition 3.1. Let K be a quadratic field of discriminant d_K and p a prime in $\mathbb{Z}$.

(a) If $\left(\frac{d_K}{p}\right) = 0$, then $pO_K = \mathfrak{p}^2$, for some prime ideal $\mathfrak{p}$ of O_K.

(b) If $\left(\frac{d_K}{p}\right) = 1$, the $pO_K = \mathfrak{p}\mathfrak{p}'$, where $\mathfrak{p} \neq \mathfrak{p}'$ are prime ideals in O_K.

(c) If $\left(\frac{d_K}{p}\right) = -1$, then pO_K is prime in O_K.

Proof. See [25, Prop. II.B.5.16]. □

If p satisfies the condition in (a), we say that it is *ramified*. Otherwise, we say that p is *split* if it satisfies the condition in (b) and *inert* if it is like in case (c). We now introduce orders in quadratic imaginary fields, which constitute our object of study in this chapter.

Definition 3.1. An order O in a quadratic field is a subset $O \subset K$ such that

(a) O is a subring of K.

(b) O is a free $\mathbb{Z}$-module of rank 2.

The ring O_K of integers is obviously an order. Moreover, if $\alpha \in O$, where O is an order of K, then α is an algebraic integer of K. Hence $\alpha \in O_K$. It follows that for every order O, $O \subset O_K$. In order to describe orders in quadratic fields, we write O_K as follows

$$O_K = [1, \omega_K], \quad \omega_K = \frac{d_K + \sqrt{d_K}}{2}, \tag{3.1}$$

where $[1, \omega_K]$ represents a basis for the $\mathbb{Z}$-module.

Lemma 3.1. Let O be an order in a quadratic field K of discriminant d_K. Then O has a finite index in O_K, and if we set $f = [O_K : O]$, then

$$O = \mathbb{Z} + fO_K = [1, f\omega_K],$$

where ω_K is as in equation (3.1).

Proof. See [25, Lemme 7.7.2]. □

Given an order O as above, the index $f = [O_K : O]$ is called the *conductor* of the order. We also define the *discriminant* of the order O, which is another important invariant of the order.

Let $\alpha \to \alpha'$ be the nontrivial automorphism of K and take $[\alpha, \beta]$ a basis for the order. Then the *discriminant* is given by

$$D = \det \begin{pmatrix} \alpha & \beta \\ \alpha' & \beta' \end{pmatrix}^2 .$$

The discriminant is independent from the basis used; by computing the discriminant in the basis $[1, f\omega_K]$ we get

$$D = f^2 d_K.$$

The discriminant of $\mathcal{O}_K$, d_K, is called a *fundamental discriminant*.
We will now study the properties of ideals of an order $\mathcal{O}$.

Lemma 3.2. Let $\mathcal{O}$ be an order of K. If $\mathfrak{a}$ is a nonzero ideal of $\mathcal{O}$, then the quotient ring $\mathcal{O}/\mathfrak{a}$ is finite.

We can therefore define the *norm* of the ideal $\mathfrak{a}$ as the cardinal of the quotient ring $\mathcal{O}/\mathfrak{a}$

$$N(\mathfrak{a}) = |\mathcal{O}/\mathfrak{a}|.$$

However, orders with the conductor $f > 1$ are not Dedekind domains. This means that ideals of $\mathcal{O}$ do not have unique factorization, and consequently the theory of ideals of orders is more complicated (see [25] for more details). While in the case of the ring of integers $\mathcal{O}_K$ we work directly with ideals, in the case of orders of K we need to restrain to a smaller class of ideals. Consequently, we define *proper* ideals.

Definition 3.2. An ideal $\mathfrak{a}$ of an order $\mathcal{O}$ is called *proper* if

$$\mathcal{O} = \{\beta \in K \,|\, \beta\mathfrak{a} \subset \mathfrak{a}\}.$$

A *fractional ideal* of $\mathcal{O}$ is a subset of K which is a nonzero finitely generated $\mathcal{O}$-module. We can show that a fractional ideal is of the form $\alpha\mathfrak{a}$, where $\alpha \in K^*$ and $\mathfrak{a}$ is an $\mathcal{O}$-ideal. Extending the terminology, we also say that a fractional ideal $\mathfrak{b}$ is *proper* if

$$\mathcal{O} = \{\beta \in K \,|\, \beta\mathfrak{b} \subset \mathfrak{b}\}.$$

A fractional ideal $\mathfrak{a}$ is *invertible* if there is another fractional ideal $\mathfrak{b}$ such that $\mathfrak{a}\mathfrak{b} = \mathcal{O}$. Principal fractional ideals, i.e. ideals of the form $\alpha\mathcal{O}$, $\alpha \in K^*$, are obviously invertible. The basic result is that for orders in quadratic fields, the notions of proper and invertible coincide.

Lemma 3.3. Let $\mathcal{O}$ be an order in a quadratic field K, and let $\mathfrak{a}$ be a fractional $\mathcal{O}$-ideal. Then $\mathfrak{a}$ is proper if and only if $\mathfrak{a}$ is invertible.

Given an order $\mathcal{O}$, let $I(\mathcal{O})$ be the set of proper fractional $\mathcal{O}$-ideals. Using Lemma 3.3, it is easy to show that $I(\mathcal{O})$ is a group under the multiplication law. The principal $\mathcal{O}$-ideals form a subgroup $P(\mathcal{O}) \subset I(\mathcal{O})$. We may consequently define the *ideal class group*

$$C(\mathcal{O}) = I(\mathcal{O})/P(\mathcal{O}).$$

The cardinal of $C(\mathcal{O})$ is called the *class number* of the order $\mathcal{O}$ and is usually denoted by $h(\mathcal{O})$.
The following result will be useful in this dissertation.

Proposition 3.2. Let $\mathcal{O}$ be an imaginary quadratic field. Given a nonzero integer M, then every ideal class in $C(\mathcal{O})$ contains a proper $\mathcal{O}$-ideal whose norm is relatively prime to M.

3.2 Lattices over $\mathbb{C}$ and the Weierstrass $\wp$-function

We define a *lattice* to be an additive subgroup L of $\mathbb{C}$ which is generated by two complex numbers ω_1 and ω_2, which are linearly independent over $\mathbb{R}$. The scope of this section is to establish an equivalence of categories between elliptic curves over $\mathbb{C}$ and lattices over $\mathbb{C}$. We show that both the algebraic and analytic study of elliptic curves over $\mathbb{C}$ is reduced to the study of lattices.

For every lattice Λ and $z \in \mathbb{C}$, we define the Weierstrass $\wp$ function as follows

$$\wp(z, \Lambda) = z^{-2} + \sum_{\omega \in \Lambda - \{0\}} ((z-\omega)^{-2} - \omega^{-2}).$$

The Weierstrass $\wp$-function is an *elliptic function*, i.e. a meromorphic function defined on $\mathbb{C}$, invariant to translation with all $\omega \in \Lambda$. When the lattice Λ is fixed, we simply denote the Weierstrass function by $\wp(z)$.

Theorem 3.1. Let $\wp(z)$ be the Weierstrass $\wp$-function for the lattice Λ.

(a) $\wp(z)$ is an elliptic function for Λ whose singularities consist of double poles at the points of Λ.

(b) $\wp(z)$ satisfies the differential equation

$$\wp'(z)^2 = 4\wp(z)^3 - g_2(\Lambda)\wp(z) - g_3(\Lambda), \tag{3.2}$$

where the constants $g_2(\Lambda)$ and $g_3(\Lambda)$ are defined by

$$g_2(\Lambda) = 60 \sum_{\omega \in \Lambda - \{0\}} \frac{1}{\omega^4}, \tag{3.3}$$

$$g_3(\Lambda) = 140 \sum_{\omega \in \Lambda - \{0\}} \frac{1}{\omega^6}. \tag{3.4}$$

Proof. See [25, Theorem 10.1]. □

Remark 3.1. The series defined at equations (3.3) and (3.4) are absolutely convergent. This means that we may define the constants $g_2(\Lambda)$ and $g_3(\Lambda)$.

We also define

$$\Delta(\Lambda) = g_2(\Lambda)^3 - 27g_3(\Lambda)^2.$$

We can show that $\Delta(\Lambda) \neq 0$ ([25, Prop.10.7]), hence we may also define the *j-invariant* of the lattice Λ as the complex number

$$j(\Lambda) = 1728\frac{g_2(\Lambda)^3}{g_2(\Lambda)^3 - 27g_3(\Lambda)^2} = 1728\frac{g_2(\Lambda)^3}{\Delta(\Lambda)}.$$

Thus Theorem 3.1 shows that $(\wp(z), \wp(z)')$ are the coordinates of a point on an elliptic curve E_Λ given by the Weierstrass equation

$$y^2 = x^3 - g_2(\Lambda)x - g_3(\Lambda).$$

Let $E/\mathbb{C}$ be an elliptic curve. Since the group law $E \times E \to E$ is given by locally defined rational functions (as seen in Section 2.5), we conclude that E is a *complex Lie group*, i.e. a complex manifold with a group law given locally by complex analytic functions. Similarly, if $\Lambda \subset \mathbb{C}$ is a lattice, then $\mathbb{C}/\Lambda$ with the natural addition from $\mathbb{C}$ is a complex Lie group.

Theorem 3.2. Let g_2 and g_3 be the quantities associated to a lattice Λ. and $E/\mathbb{C}$ be an elliptic curve given by the equation

$$E : y^2 = x^3 - g_2 x - g_3.$$

Then there is a complex analytic isomorphism

$$\phi : \mathbb{C}/\Lambda \to E, \quad \phi(z) = [\wp(z,\Lambda), \wp'(z,\Lambda), 1]$$

of complex Lie groups.

Proof. See [86, Prop. VI.3.6] □

Let Λ_1 and Λ_2 be lattices in $\mathbb{C}$. If $\alpha \in \mathbb{C}$ is such that $\alpha\Lambda_1 \subset \Lambda_2$, the scalar multiplication by α

$$\begin{aligned} \phi_\alpha : \mathbb{C}/\Lambda_1 &\to \mathbb{C}/\Lambda_2, \\ z \pmod{\Lambda_1} &\to \alpha z \pmod{\Lambda_2}. \end{aligned}$$

is obviously a holomorphic homomorphism. The following theorem shows that these are essentially the only holomorphic maps.

Theorem 3.3. (a) With notation as above, the association

$$\begin{aligned} \{\alpha \in \mathbb{C} \,|\, \alpha\Lambda_1 \subset \Lambda_2\} &\to \{\text{holomorphic maps } \phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2 \text{ with } \phi(0) = 0\} \\ \alpha &\to \phi_\alpha \end{aligned}$$

is a bijection.

(b) Let E_1 and E_2 be the elliptic curves corresponding to lattices Λ_1 and Λ_2 as in Theorem 3.2. Then the map ϕ_α induces a map of elliptic curves

$$\begin{aligned} E_1 &\to E_2 \\ [\wp(z,\Lambda_1), \wp'(z,\Lambda_1), 1] &\to [\wp(\alpha z,\Lambda_2), \wp'(\alpha z,\Lambda_2), 1]. \end{aligned}$$

which gives a bijection

$$\{\text{holomorphic maps } \phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2 \text{ with } \phi(0) = 0\} \to \{\text{isogenies } \phi : E_1 \to E_2\}$$

Proof. See [86, Thm. VI.4.1]. □

The *uniformization theorem* for elliptic curves states that every elliptic curve over $\mathbb{C}$ is parameterized by elliptic functions.

Theorem 3.4. Let $A, B \in \mathbb{C}$ satisfy $A^2 - 27B^2 \neq 0$. Then there exists a unique lattice $\Lambda \in \mathbb{C}$ such that $g_2(\Lambda) = A$ and $g_3(\Lambda) = B$.

Proof. See [86, Theorem VI.5.1]. □

In other words, Theorem 3.4 states that every elliptic curve over $\mathbb{C}$ is parameterized by elliptic functions, via a lattice Λ. In this dissertation, we denote by E_Λ the elliptic curve corresponding to a given lattice Λ, up to an isomorphism.

To sum up, in this section we have shown that the following categories are equivalent [86, Corollary VI.5.3]:

(a) The category of elliptic curves over $\mathbb{C}$ with morphisms given by isogenies.

(b) The category of lattices $\Lambda \subset \mathbb{C}$, with the morphism set

$$\mathrm{Mor}(\Lambda_1, \Lambda_2) = \{\alpha \in \mathbb{C} | \alpha\Lambda_1 \subset \Lambda_2\}.$$

(c) The category of complex tori $\mathbb{C}/\Lambda$ with holomorphic maps taking 0 to 0 for morphisms.

3.3 The j-invariant and the class equation

We say that two lattices are *homothetic* if there is a nonzero complex number λ such that $\Lambda' = \lambda\Lambda$. The j-invariant $j(\Lambda)$ defined in Section 3.2 allows us to characterize lattices up to homothety.

Theorem 3.5. If Λ and Λ' are lattices in $\mathbb{C}$, then $j(\Lambda) = j(\Lambda')$ if and only if Λ and Λ' are homothetic.

Proof. See [25, Theorem 10.9] □

Consider now $\mathcal{O}$ an order in a imaginary quadratic field K and let $\mathfrak{a}$ be a proper fractional ideal of $\mathcal{O}$. It follows from 3.1 that $\mathfrak{a} = [\alpha, \beta]$ for some $\alpha, \beta \in K$. Since α and β are linearly independent over $\mathbb{R}$ (because K is imaginary quadratic), we have that $\mathfrak{a} = [\alpha, \beta]$ is a lattice in $\mathbb{C}$; therefore we may define the j-invariant $j(\mathfrak{a})$.

If $\mathfrak{a}$ is an ideal in the ring of integers $\mathcal{O}_K$, the main result of complex multiplication theory states that the extension field $K(j(\mathfrak{a}))$ is the maximal abelian extension of the field K (we briefly recall that in Galois theory, an extension is abelian if its Galois group is abelian). We also call this field *the Hilbert class field of K*. If $\mathcal{O}$ is an order, different from the maximal order $\mathcal{O}_K$, it is also possible to associate to it an abelian extension of K, by generalizing the construction of the Hilbert class field. The field obtained in this way is called the *the ring class field of $\mathcal{O}$*. For the construction of the ring class field, which is beyond the scope of the present dissertation, we refer the reader to the book of Cox [25]. We state here the result relating $j(\mathfrak{a})$ to the ring class field of $\mathcal{O}$.

Theorem 3.6. Let $\mathcal{O}$ be an order in an imaginary quadratic field K, and let $\mathfrak{a}$ be a proper fractional ideal of $\mathcal{O}$. Then the j-invariant $j(\mathfrak{a})$ is an algebraic integer and $K(j(\mathfrak{a}))$ is the ring class field of the order $\mathcal{O}$. Moreover, if we denote by $\mathfrak{a}_i$, $i = 1, \ldots, h$ the ideal class representatives (so that h is the class number of *mathcal*(O)), the minimal polynomial of $j(\mathfrak{a})$ is given by the formula

$$H_{\mathcal{O}}(X) = \prod_{i=1}^{h} (X - j(\mathfrak{a}_i)).$$

Proof. See [25, Theorem 11.1, Proposition 13.2]. □

We call the minimal polynomial of $j(\mathfrak{a})$ *the class equation* or *the Hilbert class polynomial*. Since an order in a quadratic imaginary field is given by its discriminant, we often denote the class equation by $H_D(X)$, where D is the discriminant of the order. We also denote by $h(D)$ the degree of the polynomial H_D, which is also the class number of $\mathcal{O}$.

Example 3.1. We give as an the example the class equation for the discriminant -56.

$$\begin{aligned} H_{-56} \quad = \quad & X^4 - 2^8 \cdot 19 \cdot 937 \cdot 3559X^3 + 2^{13} \cdot 251421776987X^2 + \\ & 2^{20} \cdot 3 \cdot 11^6 \cdot 19 \cdot 21323X + (2^8 \cdot 11^2 \cdot 17 \cdot 41)^3. \end{aligned}$$

In this dissertation we also need the following result.

Theorem 3.7. Let $\mathcal{O}$ be an order of discriminant $-n$ in a quadratic imaginary field K and p a prime number such that $(p, n) = 1$. Then p is a norm of an element in $\mathcal{O}$, i.e. $4p = x^2 + ny^2$, if and only if the class polynomial $H_{-n} \pmod p$ has only simple roots and they are all in $\mathbb{Z}/p\mathbb{Z}$.

Proof. See [25, Theorem 9.4] □

3.4 The j-function and the modular equation

We saw that an elliptic curve $E/\mathbb{C}$ is given by a lattice $\Lambda = [\omega_1, \omega_2]$. We may suppose that the imaginary part of $\tau = \omega_2/\omega_1$ is positive (by interchanging ω_1 and ω_2 if necessary). We may therefore consider the j-invariant of the curve as $j(\tau) = j([1, \tau])$. We will study this function on the upper half plane $\mathcal{H} = \{\tau \,|\, \mathrm{Im}(\tau) > 0\}$.
We denote by

$$SL_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} | \, a, b, c, d \in \mathbb{Z} \text{ such that } ad - bc = 1 \right\}.$$

Moreover, we denote by $\Gamma_0(m)$ the subgroup of $SL_2(\mathbb{Z})$ defined as follows:

$$\Gamma_0(m) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) | \, a, b, c, d \in \mathbb{Z} \text{ such that } c \equiv 0 \pmod m \right\}.$$

We will now introduce modular functions. We will be interested in modular functions defined over $\Gamma_0(m)$ (even though they can be defined for any subgroup of $SL_2(\mathbb{Z})$).

Definition 3.3. A *modular function* for $\Gamma_0(m)$ is a function f defined on $\mathcal{H}$ with values in $\mathbb{C}$, which satisfies three conditions:

(a) $f(\tau)$ is meromorphic on $\mathcal{H}$.

(b) $f(\tau)$ is invariant under $\Gamma_0(m)$.

(c) For every $\gamma \in SL_2(\mathbb{Z})$, the $e^{2\pi i \tau}$-Laurent expansion has only finitely many nonzero coefficients for negative exponents.

We state that $j(\tau)$ is a modular function for $SL_2(\mathbb{Z}) = \Gamma_0(1)$. The reader is referred to Theorem 11.9 in [25] for the details of the proof of this fact. Moreover, modular functions for $\Gamma_0(m)$ can be described in function of the j-function. We consider the function j_m given by $\tau \to j(m\tau)$ for all $\tau \in \mathcal{H}$.

Theorem 3.8. The modular functions for $\Gamma_0(m)$ form a field. This field is $\mathbb{C}(j, j_m)$.

Proof. See [25, Theorem 11.9]. □

There exists a polynomial $\Phi_m(X, Y)$ such that

$$\Phi_m(j, j_m) = 0.$$

This polynomial is called *the modular polynomial*.

Theorem 3.9. Let m be a positive integer.

(a) $\Phi_m(X, Y) \in \mathbb{Z}[X, Y]$.

(b) $\Phi_m(X, Y)$ is irreducible when regarded as a polynomial in X.

(c) $\Phi_m(X, Y) = \Phi_m(Y, X)$ if $m > 1$.

(d) If m is not a perfect square, then $\Phi_m(X, X)$ is a polynomial of degree > 1 whose leading coefficient is 1.

(e) If m is a prime p, then $\Phi_p(X, Y) = (X^p - Y)(X - Y^p) \mod p\mathbb{Z}[X, Y]$.

Proof. See [25, Theorem 11.18]. □

Example 3.2. We give here two examples of modular equations.

$$\begin{aligned}
\Phi_2(X, Y) &= (X + Y)^3 - X^2Y^2 + 1485XY(X + Y) - 162000(X + Y)^2 \\
&+ 41097375XY + 8748000000(X + Y) - 157464000000000, \\
\Phi_3(X, Y) &= X^4 - X^3Y^3 + Y^4 + 2232(X^3Y^2 + X^2Y^3) - 1069956(X^3Y + XY^3) \\
&\quad +36864000(X^3 + Y^3) + 2587918086X^2Y^2 + 8900222976000(X^2Y + XY^2) + \\
&\quad 452984832000000(X^2 + Y^2) - 770845966336000000XY \\
&\quad +1855425871872000000000(X + Y).
\end{aligned}$$

The size of coefficients of modular polynomials increases exponentially with m, so computing these polynomials is a difficult task.

In order to use modular polynomials for curves with complex multiplication, we need to understand these polynomials in terms of j-invariants of lattices. If Λ is a lattice, the roots of $\Phi_m(X, j(\Lambda)) = 0$ are given by the j-invariants of those sublattices $\Lambda' \subset \Lambda$ which satisfy the following properties:

1. Λ' is a sublattice of index m in Λ, i.e. $[\Lambda : \Lambda'] = m$.

2. The quotient Λ/Λ' is a cyclic group.

If these conditions are satisfied, we say that Λ' is a *cyclic sublattice* of index m.

Theorem 3.10. Let m be a positive integer. If $u, v \in \mathbb{C}$, then $\Phi_m(u, v) = 0$ if and only if there is a lattice Λ and a cyclic sublattice $\Lambda' \subset \Lambda$ of index m such that $u = j(\Lambda')$ and $v = j(\Lambda)$.

Proof. See [25, Theorem 11.23]. □

As a consequence of the equivalence between elliptic curves over $\mathbb{C}$ and lattices, we have the following corollary.

Corollary 3.1. Let E and E' be two elliptic curves over $\mathbb{C}$. The two curves are isogenous via an isogeny of degree m if and only if $\Phi_m(j(E), j'(E)) = 0$.

3.5 Elliptic curves over $\mathbb{C}$

Let O be an order in a quadratic imaginary field. We denote by $Ell(O)$ the set of isomorphism classes of elliptic curves, with endomorphism ring $\mathrm{End}(E) \cong O$. By applying results in Section 3.2, we have

$$Ell(O) = \frac{\{\text{elliptic curves } E/\mathbb{C} \text{ with } \mathrm{End}(E) \cong O\}}{\text{isomorphism over } \mathbb{C}} = \frac{\{\text{lattices } \Lambda \text{ with } \mathrm{End}(E_\Lambda) \cong O\}}{\text{homothety}}.$$

Suppose that we want to construct an elliptic curve with complex multiplication by O. If $\mathfrak{a}$ is a nonzero fractional proper ideal of O, consider $E_\mathfrak{a}$, the elliptic curve whose endomorphism ring is

$$\mathrm{End}(E_\mathfrak{a}) \cong \{\alpha \in \mathbb{C} \mid \alpha\mathfrak{a} \subset \mathfrak{a}\} = \{\alpha \in K \mid \alpha\mathfrak{a} \subset \mathfrak{a}\} = O.$$

Note that if Λ is a lattice with $Ell(O)$, and $\mathfrak{a}$ is a nonzero fractional proper ideal of O, we can form the product

$$\mathfrak{a}\Lambda = \{\alpha_1\lambda_1 + \ldots + \alpha_r\lambda_r | \ \alpha_i \in \mathfrak{a}, \ \ \lambda_i \in \Lambda\}.$$

The following result shows that there is a simply transitive action of the ideal class group $C(O)$ on $Ell(O)$.

Proposition 3.3. (a) Let Λ be a lattice with $E_\Lambda \in Ell(O)$, and let $\mathfrak{a}$ and $\mathfrak{b}$ be nonzero fractional proper ideals of O.

(1) $\mathfrak{a}\Lambda$ is a lattice in $\mathbb{C}$.

(2) The elliptic curve $E_{\mathfrak{a}\Lambda}$ satisfies $\mathrm{End}(E_{\mathfrak{a}\Lambda}) \cong O$.

(3) $E_{\mathfrak{a}\Lambda} \cong E_{\mathfrak{b}\Lambda}$ if and only if $\hat{\mathfrak{a}} = \hat{\mathfrak{b}}$ in $C(O)$.

Hence there is a well-defined action of $C(O)$ on $Ell(O)$ determined by

$$\hat{\mathfrak{a}} * E_\Lambda = E_{\mathfrak{a}^{-1}\Lambda}.$$

(b) The action of $C(O)$ on $Ell(O)$ described at (a) is simply transitive. In particular,

$$\#C(O) = \#Ell(O).$$

Proof. See [87, Prop. II.1.2]. □

Let E be an elliptic curve with endomorphism ring $\mathcal{O}$. For an ideal $\mathfrak{a}$ of $\mathcal{O}$, we define the *group of* $\mathfrak{a}$*-torsion points of E.*

$$E[\mathfrak{a}] = \{P \in E | [\alpha]P = 0 \text{ for all } \alpha \in \mathfrak{a}\}.$$

Note that we have $\Lambda \subset \mathfrak{a}^{-1}\Lambda$, because $\mathfrak{a} \subset \Lambda$. This means that there is a natural homomorphism

$$\mathbb{C}/\Lambda \to \mathbb{C}/\mathfrak{a}^{-1}\Lambda, \ \ z \mapsto z,$$

which induces naturally an isogeny

$$E_\Lambda \to \hat{\mathfrak{a}} * E_\Lambda$$

Proposition 3.4. Let $E \in Ell(\mathcal{O})$, and let $\mathfrak{a}$ be an ideal of $\mathcal{O}$.

(a) $E[\mathfrak{a}]$ is the kernel of the natural map $E \to \hat{\mathfrak{a}} * E$.

(b) $E[\mathfrak{a}]$ is a free $\mathcal{O}/\mathfrak{a}$-module of rank 1.

Proof. See [87, Proposition II.1.4]. □

We can use Proposition 3.4 to compute the degree of the isogeny $E \to \hat{\mathfrak{a}} * E$ and, in particular, the degree of an endomorphism $[\alpha] : E \to E$.

Corollary 3.2. Let $E \in Ell(\mathcal{O})$.

(a) For all integral ideals $\mathfrak{a} \subset \mathcal{O}$, the natural map $E \to \hat{\mathfrak{a}} * E$ has degree $N(\mathfrak{a})$.

(b) For all $\alpha \in \mathcal{O}$, the endomorphism $[\alpha] : E \to E$ has degree $|N(\alpha)|$.

Proof. See [87, Corollary II.1.5]. □

3.6 Elliptic curves over finite fields

3.6.1 Hasse's theorem and the endomorphism ring

Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$, for $q = p^n$, with p prime and $n \in \mathbb{Z}$. Then the Frobenius morphism is an endomorphism and its characteristic equation is $\pi^2 - t\pi + q = 0$ (see [86, Section V.2]). We call t the *trace* of the Frobenius endomorphism. Then t is related to the cardinality of the curve. The following result, due to Hasse, gives bounds on the cardinality of the curve.

Theorem 3.11. (Hasse) Let $E/\mathbb{F}_q$ be an elliptic curve defined over $\mathbb{F}_q$. Then

$$\#E(\mathbb{F}_q) = q + 1 - t, \ \text{ where } |t| \leq 2\sqrt{q}.$$

Theorem 3.12. Let $\mathbb{F}_q$ be a (perfect) field of characteristic p and $E/\mathbb{F}_q$ an elliptic curve.

(a) The following properties are equivalent:

(i) $E[p^r] = 0$ for one (all) $r \geq 1$.

(ii) $\hat{\pi}$ is (purely) inseparable.

(iii) The trace of π is divisible by p.

(iv) The endomorphism ring End(E) is an order in a quaternion algebra.

(b) If the equivalent conditions in (a) do not hold, then

(a) $E[p^r] \cong \mathbb{Z}/p^r\mathbb{Z}$ for all $r \geq 1$,

(b) $\hat{\pi}$ is separable.

(c) The trace of π is prime to p.

(iv) The endomorphism ring End(E) is an order in a quadratic imaginary field.

Proof. [86, V.3.1] □

If E has the properties in case (a) of the theorem, we say that it is a *supersingular* curve. Otherwise, we say that E is *ordinary*. The following result relates the structure of the abelian group on the elliptic curve to the structure of the ring of endomorphisms.

Theorem 3.13. (Lenstra) Let E be an elliptic curve defined over $\mathbb{F}_q$. Let π be the Frobenius endomorphism of E.

(a) Let $\pi \notin \mathbb{Z}$. Then for all finite fields of the form $\mathbb{F}_{q^r}$, $\mathrm{End}_{\mathbb{F}_{q^r}}(E)$ is a $\mathbb{Z}$-module of rank 2 and there is an isomorphism of $\mathbb{Z}$-modules

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

(b) Suppose that $\pi \in \mathbb{Z}$. Then $\mathrm{End}_{\mathbb{F}_{q^r}}(E)$ is a $\mathbb{Z}$-module of rank 4 and we have

$$E(\mathbb{F}_{q^r}) \cong \frac{\mathbb{Z}}{\mathbb{Z}(\pi^r - 1)} \oplus \frac{\mathbb{Z}}{\mathbb{Z}(\pi^r - 1)}.$$

Proof. [55, Theorem 1]. □

As a consequence, we get the following result on the group structure of an elliptic curve.

Theorem 3.14. The abelian group $E(\mathbb{F}_q)$ has rank 1 or 2. It is isomorphic to $\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$, where n_2 divides n_1 and moreover n_2 divides $q - 1$.

3.6.2 Reduction and lifting of curves

Let H be a number field and let E be an elliptic curve defined by

$$y^2 = 4x^3 - g_2 x - g_3, \quad , where\ g_2, g_3 \in H.$$

If $\mathfrak{p}$ is a prime in O_H lying over some prime p (i.e. $\mathbb{Z} \cap O_H = p\mathbb{Z}$), we are interested in reducing the curve modulo $\mathfrak{p}$. If g_2 and g_3 can be written as α/β, with $\alpha, \beta \in O_H$ and $\beta \notin \mathfrak{p}$, we can define $\overline{g}_2$ and $\overline{g}_3$ in $O_H/\mathfrak{p}$ and we obtain the equation of a curve defined over a finite field:

$$\overline{E} : y^2 = 4x^3 - \overline{g}_2 x - \overline{g}_3.$$

Assume that we also have

$$\Delta = \overline{g_2}^3 - 27\overline{g_3}^2 \neq 0 \in O_H/\mathfrak{p}.$$

Then $\overline{E}$ is an elliptic curve defined over $O_H/\mathfrak{p}$ and we say that E has *good reduction* modulo $\mathfrak{p}$. When E has complex multiplication and good reduction, Deuring [27] showed that there is a relation between the complex multiplication of E and the number of points of $\overline{E}$ over $O_H/\mathfrak{p} \cong \mathbb{F}_p$.

Theorem 3.15. Let $E/\overline{\mathbb{Q}}$ be an elliptic curve with endomorphism ring $\mathrm{End}(E) = O$, where O is an order in an imaginary quadratic field K. Let $\mathfrak{p}$ be a prime of $\overline{\mathbb{Q}}$, over a prime number p, at which E has good reduction $\overline{E}$. The curve $\overline{E}$ is supersingular if and only if p has only one prime of K above it. Assume that p splits in K as $p = \pi\overline{\pi}$ and denote by f the conductor of O. If $(f, p) = 1$ then we have

(a) $\mathrm{End}(\overline{E}) \cong \mathrm{End}(E)$ and the isomorphism is given by the reduction morphism.

(b) $\#\overline{E}(\mathbb{F}_p) = p + 1 - (\pi + \overline{\pi})$.

Proof. See [62, Theorem 13.4.12]. □

Theorem 3.16. Let E_0 be an elliptic curve defined over a finite field $\mathbb{F}_q$, of characteristic p and ϕ_0 an endomorphism of E. Then there exists an elliptic curve E defined over a number field H, an endomorphism ϕ of E and a prime $\mathfrak{p}$ over p in H such that E_0 is isomorphic to the reduction $\overline{E}$ of E at $\mathfrak{p}$ and ϕ_0 corresponds, under this isomorphism, to the reduction $\overline{\phi}$ of ϕ.

Proof. See [62, Theorem 13.5.14]. □

3.6.3 Modular polynomials over finite fields

Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$. There are $l + 1$ isogenies of degree l whose kernels correspond to the $l + 1$ subgroups of order l of $E[l]$. As explained in Section 3.4, the j-invariants of the $l + 1$ curves isogenous to E are roots of the polynomial $\Phi_l(X, j(E)) = 0$. The following proposition relates the factorization of this polynomial to the degree of the extension field over which the l-torsion points are defined.

Proposition 3.5. Let E be an elliptic curve over $\mathbb{F}_q$ with j-invariant $j \neq 0, 1728$. Then

(a) The polynomial $\Phi_l(X, j)$ has a zero $j' \in \mathbb{F}_{q^r}$ if and only if the kernel F of the corresponding isogeny is a one-dimensional eigenspace of π^r in $E[l]$.

(b) The polynomial $\Phi_l(X, j)$ splits completely in $\mathbb{F}_{q^r}[X]$ if and only if π^r acts as a scalar matrix on $E[l]$.

Atkin [5] showed that only certain factorizations can occur for the modular polynomial.

Theorem 3.17. (Atkin) Let E be an ordinary elliptic curve defined over $\mathbb{F}_q$ with j-invariant $j \neq 0, 1728$. Let $\Phi_l(X, j) = f_1 f_2 \dots f_s$ be the factorization of $\Phi_l(X, j) \in \mathbb{F}_q$ as a product of irreducible polynomials. Then there are the following possibilities for the degrees of $f_1, \dots, f_s$:

(a) $(1, l)$ or $(1, 1, \dots, 1)$. In either case we have $t^2 - 4q \equiv 0 \mod l$.

(b) $(1, 1, r, r, \dots r)$. In this case $t^2 - 4q$ is a square modulo l, r divides $l - 1$ and π acts on $E[l]$ as a diagonal matrix $\begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}$, with $\lambda, \mu \in \mathbb{F}_l^*$.

(c) $(r, r, \dots, r)$ for some $r > 1$. In this case $t^2 - 4q$ is not a square modulo l, r divides $l + 1$ and the restriction of π to $E[l]$ has an irreducible characteristic polynomial over $\mathbb{F}_l$.

Let E be an elliptic curve and suppose we have a curve l-isogenous to E, denoted by $\tilde{E}$, given by its j-invariant $\tilde{j}$. Elkies [33] proved the following theorem, which provides a Weierstrass equation for $\tilde{E}$.

Theorem 3.18. Let E be an ordinary elliptic curve over a large prime finite field $\mathbb{F}_q$ with j-invariant j different from $0, 1728$. Assume that E is given by the Weierstrass equation $E : y^2 = x^3 + a_4 x + a_6$ and that $\tilde{E}$ is l-isogenous to E over $\mathbb{F}_q$. Let $\tilde{j}$ be the j-invariant of $\tilde{E}$. The Weierstrass equation of $\tilde{E}$ is given by

$$\tilde{E} : y^2 = x^3 + \tilde{a}_4 x + \tilde{a}_6,$$

with

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

where $\tilde{j}' \in \mathbb{F}_q$ is given by

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

and $\Phi_{l,X}$ (resp. $\Phi_{l,Y}$) denotes the partial derivative of $\Phi_l(X, Y)$ with respect to X (resp. Y).

Chapter 4

Computational preliminaries

In this chapter we present a small number of algorithms, of great importance for elliptic curve cryptography. In Section 4.1, we present Miller's algorithm to compute the Weil and the Tate pairings on elliptic curves. Since its discovery in 1985, this algorithm has been heavily utilized in the implementation of pairings on elliptic curves. In Section 4.2 we present a generic method to construct curves with complex multiplication over a finite field $\mathbb{F}_q$. Sections 4.3 and 4.4 illustrate this method, by presenting two algorithms which construct curves with almost prime group order and curves with a subgroup of large prime order and small embedding degree, respectively. Section 4.5 presents formulae to compute an isogeny over $\mathbb{F}_q$ whose kernel is known. Finally, in Section 4.6, we give a brief account of Schoof's algorithm for counting the number of points on an elliptic curve over $\mathbb{F}_q$.

4.1 Miller's algorithm

The first algorithm for pairing computation was given by Miller [70]. Miller presented his method for the computation of the Weil pairing, but a similar idea gives an algorithm computing the Tate pairing. Since it is generally acknowledged that in cryptographic applications, the Tate pairing is to be preferred to the Weil pairing, we present Miller's method for the Tate pairing. Let E be an elliptic curve given by a Weierstrass equation:

$$y^2 = x^3 + ax + b, \tag{4.1}$$

defined over a finite field $\mathbb{F}_q$. Consider r a large prime dividing $\#E(\mathbb{F}_q)$ and k the corresponding embedding degree. Let P be an r-torsion point and for any integer i, denote by $f_{i,P}$ the function with divisor

$$\operatorname{div}(f_{i,P}) = i(P) - (iP) - (i-1)(O).$$

Note that $f_{r,P}$ is such that $\operatorname{div}(f_{r,P}) = r(P) - r(O)$, hence the notation is consistent with the one in Section 2.10. Miller's algorithm heavily relies on the double and add method for finding a point multiple.

Suppose we want to compute the sum of iP and jP for $i, j \geq 1$. Let l be the line through iP and jP. Then l intersects the cubic curve E at one further point that we denote by R. We take v the line between R and O (which is a vertical line when R is not O). The line v intersects E at one more point which is defined to be the sum of iP and jP, that is $(i+j)P$. The lines l and v are functions on the curve and the corresponding divisors are:

$$\begin{aligned} \operatorname{div}(l) &= (iP) + (jP) + (R) - 3(O), \\ \operatorname{div}(v) &= (R) + ((i+j)P) - 2(O). \end{aligned}$$

One can then easily check the following relation

$$f_{i+j,P} = f_{i,P} f_{j,P} \frac{l}{v}. \tag{4.2}$$

In the sequel, we will call this relation *Miller's equation*. Turning back to Miller's algorithm, suppose that we want to compute $f_{r,P}(Q)$. We compute at each step i of the algorithm on one side mP, where m is the integer with binary expansion given by the i topmost bits of the binary expansion of r, and on the other side $f_{m,P}$ evaluated at Q, by exploiting the formula above. The complexity of this algorithm is $O(\log r)$.

Algorithm 1 Miller's algorithm

```
INPUT: An elliptic curve $E$ defined over a finite field $\mathbb{F}_q$, $P$ an $r$-torsion point on the curve and
  $Q \in E(\mathbb{F}_{q^k})$.
OUTPUT: the Tate pairing $t_r(P,Q)$.
  Let $i = [\log_2(r)]$, $K \leftarrow P$, $f \leftarrow 1$
  while $i \geq 1$ do
    Compute equations of $l$ and $v$ arising in the doubling of $K$
    $K \leftarrow 2K$ and $f \leftarrow f^2 l(Q)/v(Q)$
    if the $i$-th bit of $r$ is 1 then
      Compute equations of $l$ and $v$ arising in the addition of $K$ and $P$
      $K \leftarrow P + K$ and $f \leftarrow f l(Q)/v(Q)$
    end if
    Let $i \leftarrow i - 1$
  end while
  return $f$
```

4.2 The Complex Multiplication Method for Elliptic Curves

Using the results presented in chapter 3, we derive a method to construct elliptic curves with complex multiplication (CM) over finite fields. In this section, our exposition is restricted to the case of a finite field $\mathbb{F}_p$, with p a prime number. If $E/\mathbb{F}_p$ is an elliptic curve with complex multiplication by an order O, there is an element $\pi \in O$ such that $p = \pi\overline{\pi}$ and $t = \pi + \overline{\pi}$, i.e. π corresponds to the Frobenius endomorphism on the curve. We denote by $-n$ the discriminant of O. By Deuring's theorems 3.15 and 3.16 and Theorem 3.7, in order to obtain the j-invariant of this curve, it suffices to factorize $H_{-n}(X) \pmod p$. If j is a root of this polynomial ($j \neq 0, 1728$), the curve with $p + 1 - t$ points is given by:

$$E_j : y^2 = x^3 - \frac{36}{j-1728}x + \frac{1}{j-1728},$$

or by a twist of this curve. Suppose now we want to construct an elliptic curve whose number of points has a fixed property Pr. Common examples in cryptography of such a property are the fact that E has a subgroup of large prime order r or that the number of points is a prime number. In pairing based cryptography, we are looking for curves whose embedding degree with respect to r is small. The fact that $p = \pi\overline{\pi}$ means that we need to look for primes that satisfy the equation $t^2+ny^2 = 4p$. The number of points of the curve will be either $p+1-t$ or $p+1+t$. The pseudocode of the algorithm is given in Algorithm 2.

Algorithm 2 Construction of elliptic curves via complex multiplication

```
INPUT: $n$, $H_{-n}(X)$, and the property $Pr$.
OUTPUT: A prime $p$ and a curve $E$ defined over $\mathbb{F}_p$
repeat
    Choose $p$ a prime satisfying $4p = t^2 + ny^2$, for $t, y \in \mathbb{Z}$
    $N_1 \leftarrow p + 1 - t$ and $N_2 \leftarrow p + 1 + t$
until $N_1$ or $N_2$ satisfies property $Pr$
Compute a root $j$ of $H_{-n}(X) \pmod{p}$
Compute $E_j/\mathbb{F}_p$ and its twist $\tilde{E}_j/\mathbb{F}_p$.
while true do
    Take $P \in E_j(\mathbb{F}_p)$ and compute $Q \leftarrow [N_1]P$
    if $Q = O$ and $[N_2]P \neq O$ then
        return $p$ and $E_j$.
        else
        if $Q \neq O$ then
            return $p$ and $\tilde{E}_j$
        end if
    end if
end while
```

The algorithm terminates if the condition Pr is satisfied. This method works also for discriminants -3 and -4, with the only difference that in these cases all the twists need to be examinated in order to find the curve with the good number of points. The formulae computing the number of points for twists in these cases are given in [47, Proposition 2].

4.3 A method to construct curves with almost prime group order

For use in cryptography we need curves with almost prime order, i.e. whose number of points is of the form cr, with c small and r a large prime number. In this section we explain how to find a curve having a prescribed number of points N. We only give a solution for certain values of N. For algorithms in the general case, the reader is referred to [22] and to R. Bröker's thesis [21].

Consider $n \equiv 1 \pmod 4$, and $n > 0$. Our objective is to find a curve defined over a finite field having exactly N points, where N is a number with a large prime factor r. Assume that the following equation has roots in $\mathbb{Z}$

$$x^2 - 2x + 1 + n = N.$$

Then by letting $p = x^2 + n$ and $t = 2x$, we get

$$4p - t^2 = 4n.$$

This means that, for p is prime, there is an elliptic curve over $\mathbb{F}_p$ of discriminant $-4n$ and having group order $N = p + 1 - t$. Algorithm 3 finds values of x for which $p = x^2 + n$ is a prime number and $x^2 - 2x + 1 + n = 2r$, with r a large prime number.

Algorithm 3 Finding curves with almost prime group order

```
INPUT:  A discriminant $-4n$, integers $a$ and $b$, with $a < b$.
OUTPUT:  A prime number $p$ and an elliptic curve having $2r$ points, with $r$ prime.
 1: for $x = a$ to $b$ do
 2:     if $x^2 + n$ is prime then
 3:         $N \leftarrow x^2 - 2x + 1 + n$;
 4:         if $N/2$ is prime then
 5:             return $p$;
 6:         end if
 7:     end if
 8: end for
 9: Compute a root $j$ of $H_{-4n}(X) \pmod{p}$
10: Compute $E_j/\mathbb{F}_p$ and its twist $\tilde{E}_j/\mathbb{F}_p$.
11: Return $p$ and $E_j$ or its twist.
```

Example 4.1. With the notations above, our computations with PARI/GP [77] produced the following example of curve:

$$\begin{aligned} n &= 13; \\ x &= 1208925819614629174706204; \\ p &= 1461501637330902918203752532562181438889716089629; \\ r &= 730750818665451459101875057355271104815683338611. \end{aligned}$$

The equation of the curve is

$$\begin{aligned} y^2 + xy = x^3 &+ 697259408412535233735138061329584168410027227826x \\ &+ 912508206380344428728269271602710439555105033324 \end{aligned}$$

and its number of points is $2r$.

Suppose now that $n \equiv 3 \pmod 4$. Our search produces values of x such that $4x^2 - 4x + 1 + n = 4r$, with r large. We let $p = 4x^2 + n$, $t = 4x$ and $N = 4r$. The following equations are then verified

$$\begin{cases} 4p = & t^2 + 4n \\ N = & p + 1 - t \end{cases}$$

The lines of the pseudocode for this algorithms are similar to those of Algorithm 3. Indeed, it suffices to replace the condition in line 2 by ”**if** $4x^2 + n$ is prime” and the condition in line 4 by

”**if** $N/4$ is prime”. The j-invariant of the curve E is given by a root of $H_{-n} \pmod{p}$. Our search with PARI/GP for values of x satisfying the conditions mentioned before produced easily a large number of curves.

Example 4.2. Our computations with PARI/GP found the following example

$$\begin{aligned} n &= 3; \\ x &= 65674; \\ p &= 17252297107; \\ r &= 4313008603. \end{aligned}$$

The equation of the curve is

$$y^2 = x^3 + 5.$$

4.4 The Cocks-Pinch method

An ordinary curve is suitable for pairing based cryptography if the elliptic curve group over the ground field has a subgroup of large prime order and an efficiently computable pairing. Pairing implementation is efficient if the embedding degree k is not too large. Unfortunately, picking just any curve with a large prime order subgroup will not work, since generally such a curve has very large embedding degree. Since the invention of first pairing based protocols, the problem of finding curves with small embedding degree has had several different approaches. In this section we present the method of Cocks and Pinch [15] to construct curves with a large prime order subgroup and a small value of the embedding degree. Chronologically, this method is one of the first algorithms on this subject. For a survey of all existing methods to construct such curves, the reader is referred to [36]. To begin, we look for suitable values of the following parameters

- p, the cardinality of the ground field,
- r, the order of the elliptic curve subgroup,
- k, its embedding degree.

Given the fact that curve must have a subgroup of large order r and that the number of points on the curve is $\#E(\mathbb{F}_q) = p + 1 - t$ we write

$$p + 1 - t = hr.$$

Furthermore, the fact that the Frobenius is an element of an order in a quadratic imaginary field $\mathbb{Q}(\sqrt{-n})$ $(n > 0)$ gives:

$$ny^2 = 4p - t^2 = 4hr - (t-2)^2.$$

To sum up, in order to generate a pairing friendly curve, we are looking for p, r, k, d, t and y verifying the following conditions

$$\begin{cases} r| & ny^2 + (t-2)^2 \\ r| & p^k - 1 \\ t^2 + & ny^2 = 4p \end{cases}$$

Cocks and Pinch gave an algorithm which finds, given r and a small k, parameters p prime and t satisfying the equations above. The pseudocode of their algorithm is detailed in Algorithm 4.

Algorithm 4 The Cocks Pinch algorithm

```
INPUT: $k$, $r$ a prime number, a discriminant $n$ and $k|(r-1)$
OUTPUT: $p$, $t$ such that there is a curve over $\mathbb{F}_p$ with $p+1-t$ points where $r|(p+1-t)$ and
    $r|(p^k-1)$
Choose a primitive $k$th root of unity $g$ in $\mathbb{F}_r$
Choose an integer $t \equiv g+1 \pmod{r}$
if gcd$(t, n) \neq 1$ then
    exit (or choose another $g$)
end if
Choose an integer $y_0 = \pm(t-2)/\sqrt{-n} \pmod{r}$
$j \rightarrow 0$
repeat
    $p \leftarrow (t^2 + n(y_0 + jr)^2)/4$
    $j \leftarrow j+1$
until $p$ is prime
return $p$ and $t$
```

Example 4.3. A toy example

We take n=19 and

$$r = 79811;$$

Our implementation of the Cocks-Pinch method in MAGMA [68] found the following curve

$$y^2 + xy = x^3 + 141312404721642x + 30297319882664$$

over the prime field $\mathbb{F}_p$, with

$$p = 158231851842377$$

This method produces ordinary curves over $\mathbb{F}_p$, where the prime p is too large compared to r. More precisely, the ratio $\frac{\log p}{\log r}$ is close to 2. This does not give an optimal implementation of the pairing. We will further detail this idea in chapter 6. We only note that Brezing and Weng [20] generalized this method, by parameterizing t, r and p as polynomials. They obtained an algorithm which produces curves with small embedding degree and also smaller ratio $\frac{\log p}{\log r}$.

4.5 Vélu's formulae

Let E be an elliptic curve defined over a field K and suppose the Weierstrass equation of the curve is

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

In this section we explain how to compute an isogeny whose kernel is a fixed subgroup F of finite order. In his article [93], Vélu gave the following isogeny which obviously has kernel F

$$\begin{array}{rcl} I : E & \to & E/F \\ P & \to & \left\{ \begin{array}{ll} O_{E/F} & \text{if } P \in F, \\ (x_P + \sum_{Q \in F - \{O_E\}} (x_{P+Q} - x_Q), y_P + \sum_{Q \in F - \{O_E\}} (y_{P+Q} - y_Q)) & \text{if } P \notin F. \end{array} \right. \end{array}$$

We denote by $F_2 = (E[2] \cap F) \backslash \{O_E\}$ and by R a subset of $F \backslash (\{O_E\} \cup F_2)$ such that $F \backslash (\{O_E\} \cup F_2) = R \cup (-R)$ and $-R$ is the set of inverses of the points of R with respect to the addition law such that $R \cap (-R) = \emptyset$. We denote by $S = R \cup F_2$. By applying the addition law formulae for points on the elliptic curve, we obtain algebraic expressions for the isogeny.

Theorem 4.1. (Vélu) An isogeny $I : E \to E/F$ maps $P = (x_P, y_P) \notin F$ to the point $I(P)$ whose coordinates are

$$\begin{array}{rcl} x_{I(P)} & = & x_P + \sum_{Q \in S} \left(\frac{t_Q}{x_P - x_Q} + \frac{u_Q}{(x_P - x_Q)^2} \right) \\ y_{I(P)} & = & x_P + \sum_{Q \in S} \left(u_Q \frac{2y_P + a_1 x_P + a_3}{(x_P - x_Q)^3} + t_Q \frac{a_1(x_P - x_Q) + (y_P - y_Q)}{(x_P - x_Q)^2} + \frac{a_1 u_Q - g_Q^x g_Q^y}{(x_P - x_Q)^2} \right), \end{array}$$

with the following notations

$$\begin{array}{rcl} g_Q^x & = & 3x_Q^2 + 2a_2 x_Q + a_4 - a_1 y_Q, \\ g_Q^y & = & -2y_Q - a_1 x_Q - a_3, \\ t_Q & = & \left\{ \begin{array}{ll} g_Q^x & \text{if } Q \in F_2, \\ 2g_Q^x - a_1 g_Q^y = 6x_Q^2 + b_2 x_Q + b_4 & \text{if } Q \notin F_2, \end{array} \right. \\ u_Q & = & (g_Q^y)^2 = 4x_Q^3 + b_2 x_Q^2 + 2b_4 x_Q + b_6. \end{array}$$

The b_i are those defined at Section 2.4. Letting

$$t = \sum_{Q \in S} t_Q, \ w = \sum_{Q \in S} (u_Q + x_Q t_Q),$$

the equation of E/F is

$$y^2 + A_1 xy + A_3 y = X^3 + A_2 x^2 + A_4 x + A_6,$$

with

$$A_1 = a_1, A_2 = a_2, A_3 = a_3, A_4 = a_4 - 5t, A_6 = a_6 - b_2 t - 7w.$$

Suppose now that I is an isogeny of degree odd ℓ and denote $d = (\ell - 1)/2$. Dewaghe [28] and, independently, Kohel [61] rewrote these formulae in a more useful way. We define

$$H(X) = \Pi_{Q \in R}(X - x_Q) = X^d - h_1 X^{d-1} + h_2 X^{d-2} + \cdot + (-1)^d h_d.$$

and the following quantities

$$S_1 = \sum_{Q \in R} x_Q, \ S_2 = \sum_{Q \in R} x_Q^2, \ S_3 = \sum_{Q \in R} x_Q^3.$$

With these notations, it follows easily that

$$\begin{aligned} t &= 6S_2 + b_2 S_1 + b_4 d = 6(h_1^2 - 2h_2) \\ w &= 10S_3 + 2b_2 S_2 + 3b_4 S_1 + b_6 d = 10(h_1^3 - 3h_1 h_2 + 3h_3) + 2b_2(h_1^2 - 2h_2) + 3b_4 h_1 + b_6 d, \end{aligned}$$

which gives us the coefficients of E/F.

In the case of isogenies of degree 2, the isogeny can be easily computed by a simple application of Vélu's formulae. The computation is detailed, for example, in [64]. See also [61].

4.6 Counting the number of points on an elliptic curve

In 1985, Schoof [82] gave the first polynomial time algorithm allowing to count the number of points on an elliptic curve. Let E be an elliptic curve over $\mathbb{F}_q$, with $q > 3$, given by the equation

$$E : y^2 = x^3 + ax + b.$$

We know that $\#E(\mathbb{F}_q) = q + 1 - t$, with t the trace of the Frobenius and that $t \leq 2\sqrt{q}$, by Theorem 3.11. Schoof's idea is to determine t modulo many small prime numbers $\ell_1, \dots, \ell_r$ such that $\prod_{i=1}^r \ell_i > 4\sqrt{q}$, and to use the Chinese Remainder Theorem to compute t afterwards. More precisely, for the computation of t modulo some prime number ℓ, we use division polynomials and the fact that the Frobenius morphism verifies the equation $\pi^2 - t\pi + q = 0$. So for any point $P \in E[\ell]$ we have

$$\pi^2(P) - [t_\ell]P + [q_\ell]P = O,$$

where $t_\ell \equiv t \pmod{\ell}$ and $q_\ell \equiv q \pmod{\ell}$. It follows that the equation

$$(X^{q^2}, Y^{q^2}) + [p_\ell](X, Y) = [t_\ell](X^q, Y^q) \tag{4.3}$$

holds modulo the division polynomial $f_\ell(X)$ and modulo the polynomial $F_E(X, Y) = Y^2 - X^3 - aX - b$. Hence we check all possible values of t_ℓ in $\{0, \dots, \ell - 1\}$ to find the unique value such that equality (4.3) holds modulo $\gcd(f_\ell(X), F_E(X, Y))$. The complexity of this algorithm critically depends on the degree of division polynomial f_ℓ, which is $\frac{\ell^2-1}{2}$.

Elkies [33] found a method to replace the division polynomial by a factor of f_ℓ, of degree $\frac{\ell-1}{2}$. Depending on whether the discriminant $d_\pi = t^2 - 4q$ is a square or a non-square in $\mathbb{F}_\ell^*$, the roots of the polynomial $F(X) = X^2 - tX + q$ are defined over $\mathbb{F}_\ell$ or over $\mathbb{F}_{\ell^2}$. In the former case, we say that ℓ is an *Elkies prime*, and in the latter case, that it is an *Atkin prime*. Of course, since we do not know t, we cannot decide whether t is an Elkies or an Atkin prime. By Theorem 3.17,we have a criterion to decide whether a prime is of the Elkies or of the Atkin type. Indeed, if $\Phi_\ell(X, j)$ factorizes as in cases (a) and (b) of Theorem 3.17, ℓ is an Elkies prime. If the factorization of $\Phi_\ell(X, j)$ is like in case (c) of the theorem, then ℓ is an Atkin prime.

If ℓ is an Elkies prime, there is a subgroup $\mathbb{G}$ of order ℓ that is stable under π, i.e. $\phi(P) = \lambda P$ for all $P \in \mathbb{G}$. Elkies determines an elliptic curve E_1 which is ℓ-isogenous to E. This gives a polynomial h_ℓ

$$h_\ell = \prod_{\pm P \in \mathbb{G} \setminus \{O\}} (X - x_P),$$

where x_P is the x-coordinate of P. Note that h_ℓ has degree $(\ell - 1)/2$ and that h_ℓ is a factor of the division polynomial f_ℓ. We do not detail the computation of h_ℓ, which is given, for example, in [65]. Elkies computes an eigenvalue of π which verifies

$$(X^q, Y^q) = [\lambda](X, Y) \bmod \gcd(h_\ell(X), F_E(X, Y)).$$

He then computes $t \equiv \lambda + q/\lambda \pmod{\ell}$. If, on the other hand, ℓ is an Atkin prime, we limit the number of possibilities for $t \pmod{\ell}$ by computing r. We compute

$$\gcd(\Phi_\ell, X^{q^i} - X),$$

for $i = 1, 2, 3, \ldots$ until the computation gives $\Phi_\ell(X, j)$. We set r to i and look for θ such that $\left(\frac{\theta^2 - 4q}{\ell}\right) = -1$ and such that the ratio of the roots of the polynomial $X^2 - \theta X + q = 0$ in $\mathbb{F}_{\ell^2}$ is a root of unity of order r. For a complete description of the SEA algorithm, the reader is referred to [65].

Part II

Pairings and Isogeny Volcanoes

Chapter 5

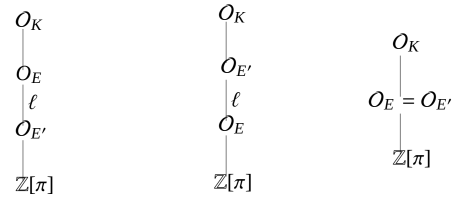
Isogeny Volcanoes

An isogeny volcano is a graph whose vertices are elliptic curves and whose edges are ℓ-isogenies. In his thesis [61], Kohel explains how this graph is related to orders in a quadratic imaginary field. Moreover, he shows that a depth-first search in this graph determines the ℓ-adic valuation of the conductor of $\mathrm{End}(E)$, for small values of ℓ. In view of optimizing point counting, Fouquet and Morain [35] give other algorithms for traveling on isogeny volcanoes. Other more recent applications of isogeny volcanoes are: the computation of the Hilbert class polynomial [8,91], that of modular polynomials [90] and that of the endomorphism ring of the curve [14]. More precisely, the methods enumerated above make use of algorithms that aim at traveling efficiently on the volcano by either walking on the crater, descending from the crater to the floor or, conversely, ascending from the floor to the crater.

As explained in [71, 72], the structure of the ℓ-Sylow subgroup of the elliptic curve may, in many cases, help deciding whether we have taken a step on the crater, or we have descended or ascended in the volcano. However, no known method can predict, before taking a step on the volcano, the direction of this step. In this chapter, we describe a method to determine, given a point P of order ℓ, the type of the isogeny whose kernel is generated by P. The immediate consequences of this method are very simple algorithms to travel on the volcano. In Section 5.1, we give definitions and main theorems about isogeny volcanoes. Section 5.2 presents algorithms to travel on the volcano using modular polynomials. Section 5.3 presents our method using pairings to determine the direction of an isogeny whose kernel is generated by a point of order ℓ and concludes by showing efficient algorithms to travel on the volcano. In Section 5.4 we compare the complexities of our methods to the complexities of algorithms using modular polynomials to walk through the volcano. Section 5.5 presents two volcano-based algorithms, computing the Hilbert polynomial and the modular polynomial, respectively.

5.1 Isogeny volcanoes

Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$, where $q = p^r$ is a prime power. Let π be the Frobenius endomorphism, i.e. $\pi(x, y) \mapsto (x^q, y^q)$ and denote by t its trace. We further assume that E is an ordinary curve, and its endomorphism ring, which we denote by $\mathcal{O}_E$, is an order in a quadratic imaginary field K (Theorem 3.12). Let $d_\pi = t^2 - 4q$ be the discriminant of π. We can write $d_\pi = g^2 d_K$, where d_K is the discriminant of the quadratic field K and g is the conductor of



descending ascending horizontal

Figure 5.1: Types of Isogenies

$\mathbb{Z}[\pi]$. There are only a finite number of possibilities for O_E, since

$$\mathbb{Z}[\pi] \subset O_E \subset O_{d_K}.$$

This also means that the conductor of O_E divides g.
In his thesis, Kohel shows that the computation of the endomorphism ring of an elliptic curve E is closely related to the computation of ℓ-isogenies starting from E. The following lemma explains the relation between the endomorphism rings of two ℓ-isogenous curves.

Lemma 5.1. Let $I : E \to E'$ an isogeny of degree ℓ. Then either $[O_E : O'_E] = \ell$, or $[O'_E : O_E] = \ell$, or $O_E = O'_E$.

Proof. See [61, Proposition 21]. □

If O_E is properly contained in $O_{E'}$, we say that I is a *descending* isogeny. Otherwise, if O_E is properly contained in $O_{E'}$, we say that I is a *ascending* isogeny. If O_E and $O_{E'}$ are equal, then we call the isogeny *horizontal*. Figure 5.1 illustrates this classification. Note that if an isogeny is descending, its dual is ascending and vice-versa.
The following proposition follows essentially from Proposition 23 in [61].

Proposition 5.1. Let E be an elliptic curve defined over $\mathbb{F}_q$ with endomorphism ring O_E with discriminant $D \neq -3, -4$. Let ℓ a prime number, different from the characteristic of the field $\mathbb{F}_q$.

(a) If $\ell \nmid [O_K : O_E]$, then there are $\left(\frac{D}{\ell}\right) + 1$ horizontal isogenies defined over $\mathbb{F}_q$.

(b) If $\ell \mid [O_K : O_E]$, then there are no horizontal isogenies.

(c) If there exist more than $\left(\frac{D}{\ell}\right) + 1$ isogenies defined over $\mathbb{F}_q$, then all ℓ-isogenies are defined over $\mathbb{F}_q$ and among them, there are exactly $\ell - \left(\frac{D}{\ell}\right)$ descending isogenies.

Proof. See [61, Prop. 23]. □

For technical reasons, we exclude the cases of discriminants $D = -3, -4$, even though similar results hold in these cases (see [61]).

Suppose ℓ is such that $\ell \mid [O_K : \mathbb{Z}[\pi]]$. Then there are three possible cases.

1. If O_E is such that $\ell \nmid [O_E : \mathbb{Z}[\pi]]$, then there cannot be any descending isogenies defined over $\mathbb{F}_q$ and, by Proposition 5.1, there are no horizontal ones. Hence there is exactly one isogeny defined over $\mathbb{F}_q$, which is ascending.

2. Suppose now ℓ divides both $[O_K : O_E]$ and $[O_E : \mathbb{Z}[\pi]]$. Then there are ℓ descending isogenies and the remaining one is ascending. We pick one of the descending isogenies, that we denote by I. The dual $\hat{I}$ of this isogeny is ascending and is necessarily defined over $\mathbb{F}_q$. This implies that I is defined over $\mathbb{F}_q$. We conclude that all descending isogenies from E are defined over $\mathbb{F}_q$.

3. When $\ell \nmid [O_K : O_E]$ and $\ell \mid [O_E : \mathbb{Z}[\pi]]$, there are at most 2 horizontal isogenies (depending on the value of $\left(\frac{D}{\ell}\right)$), and the remaining ones are descending isogenies.

This leads to the following definition.

Definition 5.1. An ℓ-volcano is a connected undirected graph with vertices partitioned into levels $V_0, \dots, V_h$, in which a subgraph on V_0 (the *crater*) is a regular connected graph whose vertices have all degree at most 2 and:

(a) For $i > 0$, each vertex in V_i has exactly one edge leading to a vertex in V_{i-1}, and every edge not on the crater is of this form.

(b) For $i < h$, each vertex in V_i has degree $\ell + 1$.

We call the level V_h *the floor* of the volcano.
We denote by $Ell_t(\mathbb{F}_q)$ the set of elliptic curves defined over $\mathbb{F}_q$ with trace t. Using this definition, Proposition 5.1 can be then reformulated as follows.

Proposition 5.2. Let p be a prime number, $q = p^r$, and $d_\pi = t^2 - 4q$. Take $\ell \neq p$ another prime number. Let G be the undirected graph with vertex set $Ell_t(\mathbb{F}_q)$ and edges ℓ-isogenies defined over $\mathbb{F}_q$. Suppose that $Ell_t(\mathbb{F}_q)$ does not contain curves with j-invariant 0 or 1728. We denote by ℓ^{2h} the largest power of ℓ dividing the conductor of d_π. Then the connected components of G are ℓ-volcanoes of height h and for each component V:

(a) The elliptic curve whose j-invariants lie in V_0 have endomorphism rings isomorphic to some $O_{d_0} \supseteq O_{d_\pi}$ whose conductor is not divisible by ℓ.

(b) The elliptic curve whose j-invariants lie in V_i have endomorphism rings isomorphic to O_{d_i}, where $d_i = \ell^{2i} d_0$.

We call the connected components of the graph defined in Proposition 5.2 *ℓ-isogeny volcanoes*. We will refer to a vertex of an isogeny volcano either by naming the curve or its j-invariant. The degree of a vertex E on the volcano is denoted by $\deg(E)$ or $\deg(j(E))$.

The number of horizontal isogenies of curves on the crater depends on the value of $\left(\frac{d_0}{\ell}\right)$. This also determines the shape of the crater, as described in Figure 5.1. By showing that to each level on the volcano we can associate an order in O_K, Proposition 5.2 shows that determining the ℓ-adic valuation endomorphism ring of an elliptic curve E is equivalent to determining the level of E in the ℓ-volcano. In the following section, we will give algorithms allowing to compute this level.

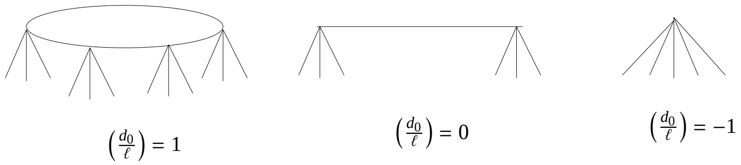

$\left(\frac{d_0}{\ell}\right) = 1$
$\left(\frac{d_0}{\ell}\right) = 0$
$\left(\frac{d_0}{\ell}\right) = -1$

Figure 5.2: Crater shape

5.2 The modular polynomial approach

5.2.1 Using modular polynomials to travel on volcanoes

In Section 3.5 (Corollary 3.1), we saw that given two elliptic curves E and E', there is a ℓ-isogeny defined over $\mathbb{F}_q$ if and only if $\#E(\mathbb{F}_q) = \#E'(\mathbb{F}_q)$ and $\Phi_\ell(j(E), j(E')) = 0$ ($j(E)$ and $j(E')$ are the j-invariants of curves E and E'). Hence in order to find the curves related to E via a ℓ-isogeny, we need to solve the equation $\Phi_\ell(X, j(E)) = 0$. As stated in Theorem 3.17, this polynomial may have 1, 2 or $\ell + 1$ roots in $\mathbb{F}_q$. So in order to find an edge on the volcano, it suffices to find a root j' of this polynomial. Note that the j-invariant determines the curve up to a twist. In order to compute the equation of the curve $E' \in Ell_t(\mathbb{F}_q)$, we use the formula in Theorem 3.18.

Remark 5.1. As explained in Section 3.4, classical modular polynomials $\Phi_\ell(X, Y)$ have some important drawbacks: the size of their coefficients increases badly as ℓ increases and their degree in Y is too high. In practice we use polynomials with fewer and smaller coefficients, which have been obtained as minimal polynomials of different modular functions. One possibility is the canonical modular polynomial $\Phi^c_\ell(X, Y)$ (see [65] for more details). To illustrate the difference between the classical modular polynomial and the canonical one, we give below $\Phi_3(X, Y)$ and $\Phi^c_5(X, Y)$:

$$\begin{aligned}
\Phi_3(X, Y) \quad = \quad & X^4 - X^3Y^3 + Y^4 + 2232(X^3Y^2 + X^2Y^3) - 1069956(X^3Y + XY^3) \\
& +36864000(X^3 + Y^3) + 2587918086X^2Y^2 + 8900222976000(X^2Y + XY^2) \\
& +452984832000000(X^2 + Y^2) - 770845966336000000XY \\
& +1855425871872000000000(X + Y) \\
\Phi^c_5(X, Y) \quad = \quad & X^6 + 30X^5 + 315X^4 + 1300X^3 + 1575X^2 + (-Y + 750)X + 125.
\end{aligned}$$

5.2.2 Walking the volcano

In this section we present algorithms that use modular polynomials to travel on the graph of isogenies. More precisely, we show algorithms allowing to descend to the floor of the volcano, to ascend one level in the volcano or to walk on the crater. As explained in Section 5.2.1 modular polynomials are difficult to handle and the algorithms presented in this section may be applied only for small values of ℓ.

We present first an algorithm given by Kohel [61] which, given a curve E in a ℓ-volcano of height h, finds a path descending to the floor, determining in this way the level of E in the volcano. This gives the ℓ-adic valuation of the conductor of E.

If $\deg(E) \neq \ell + 1$, then we are already on the floor and the level is h. Otherwise we start walking two paths, that we extend as far as possible, but whose respective lengths, k_1 and k_2, will not be greater than h. Moreover, $k_2 \leq k_1$. If E is on the surface, these paths have both length h, otherwise at least one of them is a descending path of length k_2. In both cases, E is on the level $h - k_2$. The number of visited vertices is $O(2h)$. The pseudocode for this algorithm is detailed in Algorithm 5.

Algorithm 5 Finding the level of a curve in a volcano of height h

```
INPUT: An vertex $E$ in a $\ell$-volcano of height $h$ and its $j$-invariant, $j$.
OUTPUT: The level of $E$ in the $\ell$-volcano.
if $\deg(j) \neq l + 1$ then
    return $h$.
    else let $j_1 \neq j_2$ be neighbours of $j$.
end if
Walk a path of length $k_1 \leq h$ extending $(j, j_1)$
Walk a path of length $k_2 \leq k_1$ extending $(j, j_2)$
return $h - k_2$.
```

There is a second approach to this problem given by Fouquet and Morain [35]. The idea is to start walking three paths in parallel and extend them as far as possible. Since at least one of them is descending, we stop when we have reached the floor for the first time and return $h - k$, where k is the length of the path that descended to the floor. The number of visited vertices, in the worst case, is $O(3h)$. This algorithm is obviously slower, but it has the advantage that it works for volcanoes whose height is not necessarily known. The pseudocode for this algorithm is given in Algorithm 6.

Algorithm 6 Finding the level

```
INPUT: A vertex $E$ in a $\ell$-volcano and its $j$-invariant $j$
OUTPUT: The level of $E$ in the $\ell$-volcano
$j_1 \leftarrow j$, $j_2 \leftarrow j$, $j_3 \leftarrow j$ and $k \leftarrow 0$
while $\deg(j_1) \neq 1$ and $\deg(j_2) \neq 1$ and $\deg(j_3) \neq 1$ do
    Extend paths starting from $j_1$, $j_2$ and $j_3$ by adding edges $(j_1, j_1')$, $(j_2, j_2')$ and $(j_3, j_3')$
    Let $j_1 \leftarrow j_1'$, $j_2 \leftarrow j_2'$, $j_3 \leftarrow j_3'$
    $k \leftarrow k + 1$
end while
return $h - k$.
```

In view of application to point counting, Fouquet and Morain give an algorithm allowing to ascend one level in the volcano or to take one step on the crater. Following [91], we present an algorithm allowing to ascend one level in the volcano. If we are on the floor (i.e. $\deg(E) \neq \ell + 1$), we take the curve given by the only rational ℓ-isogeny. Otherwise, we start walking descending paths for each of the $\ell + 1$ curves isogenous to E. We then compare all lengths and pick among the neighbours of E the curve which gave the longest path. The number of visited vertices is, in the worst case, $O(\ell h)$. This is Algorithm 7.

Note that alternatively, one could walk in parallel all of the $\ell + 1$ paths starting from the initial curve and keep the (two) longest as horizontal or ascending. As far as we know, this has not been

Algorithm 7 Ascending/walking on the crater

```
INPUT: A vertex $E$ in a volcano $V$ and its $j$-invariant $j$
OUTPUT: A curve $E'$ lying one level up or on the same level if $E$ is on the crater
if $\deg(j) = 1$ then
    return $E'$ whose $j$-invariant is $j_1$, the neighbour of $j$
    else
    Extend the path $j, j_1$ as far as possible and compute $l_1$ the length of the path and max$\leftarrow l_1$
end if
Take $j_2, \ldots, j_{\ell+1}$ the other neighbours of $j$
for $i = 2$ to $\ell + 1$ do
    Walk a path of length $l_i$ extending as far as possible $(j, j_i)$
    if $l_i > max$ then
        return a curve $E'$ whose $j$-invariant is $j' = j_i$
    end if
end for
return $E'$ whose $j$-invariant is $j_1$
```

proposed in the literature, but this variant of existing algorithms offers a slightly better asymptotic time complexity. For completeness, we give an pseudo-code description of this parallel variant of Kohel and Fouquet-Morain algorithms as Algorithm 8.

5.3 Our approach

5.3.1 The group structure of the elliptic curve on the volcano

Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$. Given P a point of order ℓ on E, the ℓ-isogeny $I : E \to E'$ whose kernel G is generated by P can be found by using Vélu's formulae (Section 4.5)). It follows that we can use these formulae in order to travel on the volcano. If we want to use this approach, we are interested in explicitly computing the coordinates of points of order ℓ on E.

We denote by G_i, $1 \leq i \leq g$, the g subgroups of order ℓ of E that represent the kernels of the g isogenies of degree ℓ defined over $\mathbb{F}_q$. In [72] Miret and al. computed the degree r_i of the smallest extension field of $\mathbb{F}_q$ such that $G_i \subset E(\mathbb{F}_{q^{r_i}})$, for all i, $1 \leq i \leq g$. The value of r_i is related to the order of q in the group $\mathbb{F}_\ell^*$, that we denote by $\mathrm{ord}_\ell(q)$.

Proposition 5.3. Let E defined over $\mathbb{F}_q$ be an elliptic curve with exactly g ℓ-isogenies defined over $\mathbb{F}_q$. Assume that $\ell > 2$. Let G_i, $1 \leq i \leq g$, be the kernels of the g isogenies, and let r_i be the minimum value for which $G_i \subset E(\mathbb{F}_{q^{r_i}})$.

(a) If $g = 1$ then $r_1 = \mathrm{ord}_\ell(q)$ or $r_1 = 2\mathrm{ord}_\ell(q)$.

(b) If $g = \ell + 1$ then either $r_i = \mathrm{ord}_\ell(q)$ for all i, or $r_i = 2\mathrm{ord}_\ell(q)$ for all i.

(c) If $g = 2$ then $r_i | (\ell - 1)$, $i = 1, 2$.

Algorithm 8 Parallel variant of ascending/horizontal step (using modular polynomials)

```
INPUT: A $j$-invariant $j_0$ in $\mathbb{F}_q$, a prime $\ell$, the modular polynomial $\Phi_\ell(X, Y)$.
OUTPUT: The $j$-invariants lying on the same level/upper level of a $\ell$-volcano
Let $f(x) = \Phi_\ell(X, j_0)$
Compute $J_0$ the list of roots of $f(x)$ in $F_q$
if $\#J_0 = 0$ return: “Trivial volcano”exit
if $\#J_0 = 1$ return: “On floor, step leads to:”, $J_0[1]$ exit
if $\#J_0 = 2$ return: “On floor, two horizontal steps to:”, $J_0[1]$ and $J_0[2]$ exit
Let $J = J_0$. Let $J'$ and $K$ be empty lists. Let Done = false.
repeat
  Perform multipoint evaluation of $\Phi_\ell(X, j)$, for each $j \in J$. Store in list $F$.
  for $i$ from 1 to $\ell + 1$ do
    Perform partial factorization of $F[i]$, computing at most two roots $r_1$ and $r_2$.
    if $F[i]$ has less than two roots then
      Let Done = true. Append $\perp$ to $K$ (Reaching floor)
      else
      if $r_1 \in J'$ then
        append $r_1$ to $K$
        else
        Append $r_2$ to $K$. (Don’t backtrack)
      end if
    end if
  end for
  Let $J' = J$, $J = K$ and $K$ be the empty list.
until Done
for each $i$ from 1 to $\ell + 1$ such that $J[i] \neq \perp$ append $J_0[i]$ to $K$
return “Possible step(s) lead to:” $K$ (One or two outputs)
```

Proof. See [72, Prop. 2]. □

The following corollary [72] shows that in some situations, if possible, it is more efficient to replace E with its twist, which has points of order ℓ over an extension field of smaller degree.

Corollary 5.1. Let $E/\mathbb{F}_q$ be an elliptic curve over $\mathbb{F}_q$ and denote by $\tilde{E}$ its quadratic twist. If $E/\mathbb{F}_q$ has 1 or $\ell + 1$ rational ℓ-isogenies, then $\#E(\mathbb{F}_{q^{\mathrm{ord}_\ell q}})$ or $\#\tilde{E}(\mathbb{F}_{q^{\mathrm{ord}_\ell q}})$ is a multiple of ℓ. Moreover, if $E/\mathbb{F}_{q^{\mathrm{ord}_\ell q}}$ has $\ell + 1$ rational isogenies, then it is also a multiple of ℓ^2.

Proof. See [72, Cor. 4].

Proposition 5.4. On a ℓ-volcano the structure of the elliptic curve group is the same for all curves in a given level.

Proof. Proposition 3.13 relates the structure of the curve to the endomorphism ring by giving the following isomorphism of O_E-modules

$$E(\mathbb{F}_q) \simeq O_E/(\pi - 1). \tag{5.1}$$

We write $\pi = a + g\omega$, with:

$$a = \begin{cases} (t-g)/2 \\ t/2 \end{cases} \quad \text{and } \omega = \begin{cases} \frac{1+\sqrt{d_K}}{2} & \text{if } d_K \equiv 1 \pmod 4 \\ \frac{\sqrt{d_K}}{2} & \text{if } d_K \equiv 0 \pmod 4 \end{cases} \tag{5.2}$$

where d_K is the discriminant of the quadratic imaginary field containing O_E, t is the trace of the curve E and g is the conductor of $\mathbb{Z}[\pi]$. Note that N is maximal such that $E[N] \subset E(\mathbb{F}_q)$ and by [80, Lemma 1] we get that $N = \gcd(a-1, g/f)$, where f is the conductor of O_E. This shows that the value of N is the same at a given level in the volcano. Due to the fact that isogenous curves have the same cardinality, we deduce that curves at the same level also have the same m and consequently the same group structure. □

In the sequel, we denote by v_ℓ the ℓ-adic valuation. The following lemma was given by Miret et al. [72] in the case $\ell = 2$. We state the same result in the general case.

Lemma 5.2. Let E be an elliptic curve over $\mathbb{F}_q$. We consider a as in equation 5.2. Then we have

$$v_\ell(a-1) \geq \min\{v_\ell(g), v_\ell(\#E(\mathbb{F}_q))/2\}.$$

Proof. If $d_K \equiv 0 \pmod 4$, then $a = t/2$ and we have $4(a-1)^2 = g^2 d_K + 4A$, where by $A = \#E(\mathbb{F}_q)$. Otherwise, $a = (t-g)/2$ and, since $(t-2)^2 - g^2 d_K = 4A$ we have $4(a-1)^2 = 4A + g^2(d_K - 1) - g(a-1)$. We consider the ℓ-adic valuation of these expressions and we get the claimed inequality. □

Notations. Let $n \geq 0$. In the sequel, we denote by $E[\ell^n](K)$ the subgroup of points of order ℓ^n defined over K and by $E[\ell^\infty](K)$ the ℓ-Sylow subgroup of $E(K)$.

Let E be a curve whose group structure is $E(\mathbb{F}_q) = \mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$. This curve lies on an ℓ-isogeny volcano and two cases may occur for the ℓ-torsion subgroup of E.

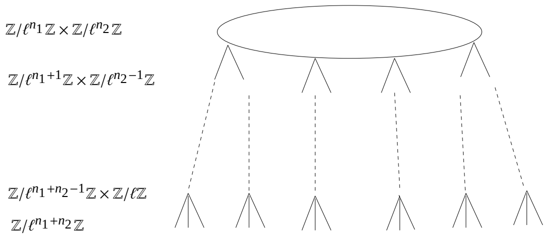

$\mathbb{Z}/\ell^{n_1}\mathbb{Z}\times\mathbb{Z}/\ell^{n_2}\mathbb{Z}$
$\mathbb{Z}/\ell^{n_1+1}\mathbb{Z}\times\mathbb{Z}/\ell^{n_2-1}\mathbb{Z}$
$\mathbb{Z}/\ell^{n_1+n_2-1}\mathbb{Z}\times\mathbb{Z}/\ell\mathbb{Z}$
$\mathbb{Z}/\ell^{n_1+n_2}\mathbb{Z}$

Figure 5.3: An irregular volcano

In the first case, we have $v_\ell(N) < v_\ell(M)$. Note that in this case $v_\ell(N) < v_\ell(\#E(\mathbb{F}_q))/2$. As we descend from E down to the floor, the structure of $E[\ell^\infty](\mathbb{F}_q)$ changes. More precisely, the valuation of the corresponding N decreases by 1 at every level, while the valuation of M increases by 1. Note that N is maximal such that $E[N] \subset E(\mathbb{F}_q)$ and by [80, Lemma 1] we get that $N = \gcd(a-1, g/f)$. Suppose now that $\min\{v_\ell(g), v_\ell(\#E(\mathbb{F}_q))/2\} = v_\ell(g)$. Then $v_\ell(a-1) \geq v_\ell(g)$ and since $N = \gcd(a-1, g/f)$, we get $v_\ell(N) = v_\ell(g/f)$. Otherwise, if $\min\{v_\ell(g), v_\ell(\#E(\mathbb{F}_q))/2\} = v_\ell(\#E(\mathbb{F}_q))/2$, we get

$$v_\ell(a-1) \geq v_\ell(\#E(\mathbb{F}_q))/2 > v_\ell(N).$$

From $N = \gcd(a-1, g/f)$, it follows again that $v_\ell(N) = v_\ell(g/f)$. As we descend, the valuation at ℓ of the conductor f increases by 1 at each level (by Proposition 5.2b). This implies that the ℓ-valuation of N for curves at each level decreases by 1 and is equal to 0 for curves lying on the floor.

In the second case, $v_\ell(\#E(\mathbb{F}_q))$ is even and $v_\ell(M) = v_\ell(N)$. Then the structure of the ℓ-torsion group $E[\ell^\infty](\mathbb{F}_q)$ may be unaltered from the crater down to a certain level. From that level down, the structure of the ℓ-torsion group starts changing as explained above. In the sequel we call the lowest level at which $v_\ell(M) = v_\ell(N)$ the *first stability level*[1]. The volcanoes whose ℓ-torsion is different at each level are called *regular* volcanoes (see Figure 2.5). Their first stability level is on the crater. This terminology is taken from [72].

In the remainder of this chapter, we will work with points of order a power of a prime number ℓ. Let $n \geq 0$. Given a point $P \in E[\ell^n](\mathbb{F}_q)$, we also need to determine the degree of the extension field in which there is a ℓ^{n+1}-torsion point such that $\ell\tilde{P} = P$. The following result is taken from [34].

Proposition 5.5. Let $E/\mathbb{F}_q$ be an elliptic curve which lies on a ℓ-volcano whose height $h(V)$ is different from 0. Then the height of V', the ℓ-volcano of the curve $E/\mathbb{F}_{q^s}$ is

$$h(V') = h(V) + v_\ell(s).$$

From this proposition, it follows easily that if the structure of subgroup $E[\ell^\infty](\mathbb{F}_q)$ on the curve E is $\mathbb{Z}/\ell^{n_1}\mathbb{Z}\times\mathbb{Z}/\ell^{n_2}\mathbb{Z}$, then the smallest extension K of $\mathbb{F}_q$ such that $E[\ell^\infty](K)$ is not isomorphic to $E[\ell^\infty](\mathbb{F}_q)$ is $\mathbb{F}_{q^\ell}$. First of all, note that E lies on a ℓ-volcano $V/\mathbb{F}_q$ of height at least n_2. We consider

[1] Miret et al. [72] call it the stability level.

a curve E' lying on the floor of $V/\mathbb{F}_q$ such that there is a descending path of isogenies between E and E'. Obviously, we have $E'[\ell^\infty](\mathbb{F}_q) \simeq \mathbb{Z}/\ell^{n_1+n_2}\mathbb{Z}$. By Proposition 5.5, $V/\mathbb{F}_{q^\ell}$ has one extra down level, which means that the curve E' is no longer on the floor, but on the level just above the floor. Consequently, we have that $E'[\ell] \subset E'(\mathbb{F}_{q^\ell})$ and, moreover, $E'[\ell^\infty](\mathbb{F}_{q^\ell}) \simeq \mathbb{Z}/\ell^{n_1+n_2+\Delta}\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$. We now show that $\Delta = 1$. Note first that $\ell^{n_2}|q-1$ and that $v_\ell(q^\ell - 1) = v_\ell(q-1)+1$. Suppose now that $\Delta = 0$. We denote by P a point of order ℓ^{n_1} on the curve E'. Then, without restraining the generality, we may assume that

$$T_{\ell^{n_2}}(\ell^{n_1}P, P) = f_{\ell^{n_2},\ell^{n_1}P}(P)^{\frac{q-1}{\ell^{n_2}}} \in \mu_{\ell^{n_2}}, \tag{5.3}$$

and

$$T^{(\mathbb{F}_{q^\ell})}_{\ell^{n_2+1}}(\ell^{n_1-1}P, P) = f_{\ell^{n_2+1},\ell^{n_1-1}P}(P)^{\frac{q^\ell-1}{\ell^{n_2+1}}} \in \mu_{\ell^{n_2+1}} \backslash \mu_{\ell^{n_2}}.$$

By using the bilinearity of the pairing and the fact that $f_{\ell^{n_2+1},P} = f^{\ell}_{\ell^{n_2},P}$ (up to a constant), we get

$$f_{\ell^{n_2},\ell^{n_1}P}(P)^{\ell\frac{q^\ell-1}{\ell^{n_2+1}}} \in \mu_{\ell^{n_2}},$$

which contradicts Equality (5.3). A similar reasoning leads to a contradiction if $\Delta \geq 1$. Hence $\Delta = 1$. By ascending on the volcano from E' to E, we deduce that the structure of the ℓ-torsion of E over $\mathbb{F}_{q^\ell}$ is necessarily

$$E[\ell^\infty](\mathbb{F}_{q^\ell}) \simeq \mathbb{Z}/\ell^{n_1+1}\mathbb{Z} \times \mathbb{Z}/\ell^{n_2+1}\mathbb{Z}.$$

5.3.2 Preliminary results. Determining directions on the volcano

In this section, we describe a model using pairings, allowing to predetermine the direction of an isogeny constructed using Vélu's formulae. Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$ and assume that $E[\ell^n] \subseteq E(\mathbb{F}_q)$, and that $E[\ell^{n+1}] \nsubseteq E[\mathbb{F}_q]$. Now let P and Q be two ℓ^n-torsion points on E. We define the following symmetric pairing [54]

$$S(P, Q) = (T_{\ell^n}(P, Q)\, T_{\ell^n}(Q, P))^{\frac{1}{2}}. \tag{5.4}$$

Note that for any point P, $T_{\ell^n}(P, P) = S(P, P)$. In the sequel, we call $S(P, P)$ *the self-pairing* of P. We focus on the case where the pairing S is non-constant. Suppose now that P and Q are two linearly independent ℓ^n-torsion points. Then all ℓ^n-torsion points R can be expressed as $R = aP + bQ$. Using bilinearity and symmetry of the S-pairing, we get

$$\log(S(R, R)) = a^2 \log(S(P, P)) + 2ab\ \log(S(P, Q)) + b^2 \log(S(Q, Q)) \pmod{\ell^n},$$

where log is a discrete logarithm function in μ_{ℓ^n}. We denote by k the largest integer such that the polynomial

$$\mathcal{P}(a, b) = a^2 \log(S(P, P)) + 2ab\ \log(S(P, Q)) + b^2 \log(S(Q, Q)) \tag{5.5}$$

is identically zero modulo ℓ^k and nonzero modulo ℓ^{k+1}. Obviously, since S is non-constant we have $0 \leq k < n$. Dividing by ℓ^k, we may thus view $\mathcal{P}$ as a polynomial in $\mathbb{F}_\ell[a, b]$. When we want to emphasize the choice of E and ℓ^n, we write $\mathcal{P}_{E,\ell^n}$ instead of $\mathcal{P}$.

Since $\mathcal{P}$ is a non-zero quadratic polynomial, it has at most two homogeneous roots, which means that that from all the $\ell + 1$ subgroups of $E[\ell^n]/E[\ell^{n-1}] \simeq (\mathbb{Z}/\ell\mathbb{Z})^2$, at most 2 have self-pairings in μ_{ℓ^k} (see also [54]). In the sequel, we denote by N_{E,ℓ^n} the number of zeros of $\mathcal{P}_{E,\ell^n}$. Note that this number does not depend on the choice of the two generators P and Q of the ℓ^n-torsion subgroup $E[\ell^n]$. Moreover, we say that an ℓ^n-torsion point R has *degenerate self-pairing* if $T_{\ell^n}(R,R)$ is a ℓ^k-th root of unity and that R has *non-degenerate self-pairing* if $T_{\ell^n}(R,R)$ is a primitive ℓ^{k+1}-th root of unity. Also, if $T_{\ell^n}(R,R)$ is a primitive ℓ^n-th root of unity, we say that R has *primitive self-pairing*.

Note that it is also possible to have $T_{\ell^n}(R,R) = 1$, for all points $R \in E[\ell^n]$. This happens if and only if the polynomial $\mathcal{P}_{E,\ell^n}$ is zero, which implies that

$$S(P,Q) = 1,$$

for every two points P and Q generating $E[\ell^n]$. Equivalently, all self-pairings are degenerate if the Tate pairing T_{ℓ^n} and the Weil pairing W_{ℓ^n} are equal.
We give some lemmas, meant to explain the relations between pairings on two curves, whenever there exists an isogeny between the two curves.

Lemma 5.3. Suppose $E/\mathbb{F}_q$ is an elliptic curve and P, Q are points in $E(\mathbb{F}_q)$ of order ℓ^n, $n \geq 1$. Suppose there are $\tilde{P}, \tilde{Q} \in E[\overline{\mathbb{F}}_q]$ such that $\ell\tilde{P} = P$ and $\ell\tilde{Q} = Q$. Then we have the following relation for the Tate pairing:

(a) If $\tilde{P}, \tilde{Q} \in E[\mathbb{F}_q]$, then

$$T_{\ell^{n+1}}(\tilde{P}, \tilde{Q})^{\ell^2} = T_{\ell^n}(P, Q).$$

(b) Suppose $\ell \geq 3$. If $\tilde{Q} \in E[\overline{\mathbb{F}}_q] \backslash E[\mathbb{F}_q]$, then

$$T_{\ell^{n+1}}(\tilde{P}, \tilde{Q})^{\ell} = T_{\ell^n}(P, Q).$$

Proof. (a) By writing down the divisors of the functions $f_{\ell^{n+1},\tilde{P}}$, $f_{\ell^n,\tilde{P}}$, $f_{\ell^n,P}$, one can easily check that

$$f_{\ell^{n+1},\tilde{P}} = (f_{\ell,\tilde{P}})^{\ell^n} \cdot f_{\ell^n,P}.$$

We evaluate these functions at some points $Q + R$ and R (where R is carefully chosen) and raise the equality to the power $(q-1)/\ell^n$.
(b) Due to the equality on divisors $\mathrm{div}(f_{\ell^{n+1},P}) = \mathrm{div}(f^{\ell}_{\ell^n,P})$, we have

$$T_{\ell^{n+1}}(\tilde{P}, \tilde{Q})^{\ell} = T^{(\mathbb{F}_{q^\ell})}_{\ell^n}(P, \tilde{Q}),$$

where $T^{(\mathbb{F}_{q^\ell})}_{\ell^n}$ is the ℓ^n-Tate pairing for E defined over $\mathbb{F}_{q^\ell}$. It suffices then to show that

$$T^{(\mathbb{F}_{q^\ell})}_{\ell^n}(P, \tilde{Q}) = T_{\ell^n}(P, Q).$$

We have

$$\begin{aligned} T^{(\mathbb{F}_{q^\ell})}_{\ell^n}(P, \tilde{Q}) &= f_{\ell^n,P}([\tilde{Q} + R] - [R])^{\frac{(1+q+\cdots+q^{\ell-1})(q-1)}{\ell^n}} \\ &= f_{\ell^n,P}((\tilde{Q} + R) + (\pi(\tilde{Q}) + R) + (\pi^2(\tilde{Q}) + R) + \ldots \\ &+ (\pi^{\ell-1}(\tilde{Q}) + R) - \ell(R))^{\frac{(q-1)}{\ell^n}} \end{aligned} \tag{5.6}$$

where R is a random point defined over $\mathbb{F}_q$. It is now easy to see that for $\ell \geq 3$,

$$\tilde{Q} + \pi(\tilde{Q}) + \pi^2(\tilde{Q}) + \ldots + \pi^{\ell-1}(\tilde{Q}) = \ell\tilde{Q} = Q,$$

because $\pi(\tilde{Q}) = \tilde{Q} + T$, where T is a point of order ℓ. By applying Weil's reciprocity law (2.11), it follows that the equation (5.6) becomes:

$$T_{\ell^n}^{(\mathbb{F}_{q^\ell})}(P, \tilde{Q}) \quad = \quad \left(\frac{f_{\ell^n,P}(Q+R)}{f_{\ell^n,P}(R)}\right)^{\frac{q-1}{\ell^n}} f((P)-(O))^{q-1},$$

where f is such that $\mathrm{div}(f) = (\tilde{Q}+R)+(\pi(\tilde{Q})+R)+(\pi^2(\tilde{Q})+R)+...+(\pi^{\ell-1}(\tilde{Q})+R)-(Q+R)-(\ell-1)(R)$. Note that this divisor is $\mathbb{F}_q$-rational, so $f((P)-(O))^{q-1} = 1$. This concludes the proof. □

Lemma 5.4. (a) Let $\phi : E \to E'$ be a separable isogeny of degree d defined over $\mathbb{F}_q$, P an ℓ-torsion on the curve E such that $\phi(P)$ is a ℓ-torsion point on E', and Q a point on E. Suppose, moreover, that $\mathrm{Ker}\phi \subset E[\mathbb{F}_q]$. Then we have:

$$T_\ell(\phi(P), \phi(Q)) = T_\ell(P, Q)^d.$$

(b) Let $\phi : E \to E'$ be a separable isogeny of degree ℓ defined over $\mathbb{F}_q$, P an $\ell\ell'$-torsion point such that $\mathrm{Ker}\ \phi =< \ell' P >$ and Q a point on the curve E. Then we have:

$$T_{\ell'}(\phi(P), \phi(Q)) = T_{\ell\ell'}(P, Q)^\ell.$$

Proof. (a) We have

$$(\phi)^*(f_{\ell,\phi(P)}) = \ell \sum_{K\in\mathrm{Ker}\phi} ((P+K)-(K)) = \ell \sum_{K\in\mathrm{Ker}\phi} ((P)-(O)) + \mathrm{div}\left(\left(\prod_{K\in\mathrm{Ker}\phi} \frac{l_{K,P}}{v_{K+P}}\right)^\ell\right),$$

where $l_{K,P}$ is the straight line passing through K and P and v_{K+P} is the vertical line passing through $K+P$. It follows that for some point S on E

$$f_{\ell,\phi(P)} \circ \phi(S) = f_{\ell,P}^d(S) \left(\prod_{K\in\mathrm{Ker}\phi} \frac{l_{K,P}(S)}{v_{K+P}(S)}\right)^\ell .$$

We obtain the desired formula by evaluating the equality above at two carefully chosen points $Q+R$ and R, and then by raising to the power $\frac{q-1}{\ell}$.
(b) This time we have

$$(\phi)^*(f_{\ell',\phi(P)}) = \ell' \sum_{K\in\mathrm{Ker}\phi} ((P+K)-(K)) = \ell' \sum_{K\in\mathrm{Ker}\phi} ((P)-(O)) + \mathrm{div}\left(\left(\prod_{K\in\mathrm{Ker}\phi} \frac{l_{K,P}}{v_{K+P}}\right)^{\ell'}\right),$$

Since $\#\mathrm{Ker}\phi = \ell$, we get

$$f_{\ell',\phi(P)} \circ \phi(Q) = f_{\ell\ell',P}(Q) \left(\prod_{K\in\mathrm{Ker}\phi} \frac{l_{K,P}(Q)}{v_{K+P}(Q)}\right)^{\ell'} .$$

We raise this equality to the power $\frac{q-1}{\ell'}$ and get the announced result. □

Remark 5.2. Actually the statement at (a) holds for all isogenies, as shown in Theorem IX.9.4 of [15]. We kept our proof because a similar technique can be applied to prove (b). Of course, we could also extend our result to all isogenies by using Lemma 5.3.

Proposition 5.6. Let E be an elliptic curve defined a finite field $\mathbb{F}_q$ and assume that $E[\ell^\infty](\mathbb{F}_q)$ is isomorphic to $\mathbb{Z}/\ell^{n_1}\mathbb{Z} \times \mathbb{Z}/\ell^{n_2}\mathbb{Z}$ (with $n_1 \geq n_2$). Suppose that there is a ℓ^{n_2}-torsion point P such that $T_{\ell^{n_2}}(P,P)$ is a primitive ℓ^{n_2}-th root of unity. Then the ℓ-isogeny whose kernel is generated by $\ell^{n_2-1}P$ is descending. Moreover, the curve E does not lie above the first stability level of the corresponding ℓ-volcano.

Proof. Consider $I_1 : E \to E_1$ the isogeny whose kernel is generated by $\ell^{n_2-1}P$ and suppose this isogeny is ascending or horizontal. This means that $E_1[\ell^{n_2}]$ is defined over $\mathbb{F}_q$. Take Q another ℓ^{n_2}-torsion point on E, such that $E[\ell^{n_2}] =< P, Q >$ and denote by $Q_1 = I_1(Q)$. One can easily check that the dual of I_1 has kernel generated by $\ell^{n_2-1}Q_1$. It follows that there is a point $P_1 \in E_1[\ell^{n_2}]$ such that $P = \hat{I}_1(P_1)$. By Lemma 6.1 this means that $T_{\ell^{n_2}}(P,P) \in \mu_{\ell^{n_2-1}}$, which is false. This proves not only that the isogeny is descending, but also that the structure of the ℓ-torsion is different at the level of E_1, so E cannot be above the first stability level. □

Proposition 5.7. Let $\ell \geq 3$ be a prime number and suppose that $E/\mathbb{F}_q$ is a curve which lies in an ℓ-volcano and on the first stability level. Suppose $E[\ell^\infty](\mathbb{F}_q) \simeq \mathbb{Z}/\ell^{n_1}\mathbb{Z} \times \mathbb{Z}/\ell^{n_2}\mathbb{Z}$, $n_1 \geq n_2$. Then there is at least one ℓ^{n_2}-torsion point on $R \in E(\mathbb{F}_q)$ whose pairing $T_{\ell^{n_2}}(R,R)$ is a primitive ℓ^{n_2}-th root of unity.

Proof. Let P be an ℓ^{n_1}-torsion point and Q be an ℓ^{n_2}-torsion point such that $\{P, Q\}$ generates $E[\ell^\infty](\mathbb{F}_q)$.
Case 1. Suppose $n_1 \geq n_2 \geq 2$. Let

$$E \xrightarrow{I_1} E_1$$

be a descending ℓ-isogeny and denote by P_1 and Q_1 the ℓ^{n_1+1} and ℓ^{n_2-1}-torsion points generating $E_1[\ell^\infty](\mathbb{F}_p)$. Moreover, without loss of generality, we may assume that $I_1(P) = \ell P_1$ and $I_1(Q) = Q_1$. If $T_{\ell^{n_2-1}}(Q_1, Q_1)$ is a primitive ℓ^{n_2-1}-th root of unity, $T_{\ell^{n_2}}(Q,Q)$ is a primitive ℓ^{n_2}-th root of unity by Lemma 6.1. If not, from the non-degeneration of the pairing, we deduce that $T_{\ell^{n_2-1}}(Q_1, P_1)$ is a primitive ℓ^{n_2-1}-th root of unity, which means that $T_{\ell^{n_2-1}}(Q_1, \ell P_1)$ is a ℓ^{n_2-2}-th primitive root of unity. By applying Lemma 6.1, we get $T_{\ell^{n_2}}(Q,P) \in \mu_{\ell^{n_2-1}}$ at best. It follows that $T_{\ell^{n_2}}(Q,Q) \in \mu_{\ell^{n_2}}$ by the non-degeneracy of the pairing.
Case 2. If $n_2 = 1$, then consider the volcano defined over the extension field $\mathbb{F}_{q^\ell}$. There is a ℓ^2-torsion point $\tilde{Q} \in E(\mathbb{F}_{q^\ell})$ with $Q = \ell\tilde{Q}$. We obviously have $\ell^2 | q^\ell - 1$ and from Lemma 5.3, we get $T_{\ell^2}(\tilde{P}, \tilde{P})^\ell = T_\ell(P,P)$. By applying Case 1, we get that $T_{\ell^2}(\tilde{P}, \tilde{P})$ is a primitive ℓ^2-th root of unity, so $T_\ell(P,P)$ is a primitive ℓ-th root of unity. □

Two stability levels. Remember that in any irregular volcano, $v_\ell(\#E(\mathbb{F}_q))$ is even and the height h of the volcano is greater than $v_\ell(\#E(\mathbb{F}_q))$. Moreover, all curves at the top of the volcano have $E[\ell^\infty](\mathbb{F}_q) \simeq \mathbb{Z}/\ell^{n_2}\mathbb{Z} \times \mathbb{Z}/\ell^{n_2}\mathbb{Z}$ with $n_2 = v_\ell(\#E(\mathbb{F}_q))$. The existence of a primitive self-pairing of a ℓ^{n_2}-torsion point on any curve lying on the first stability level implies that the polynomial

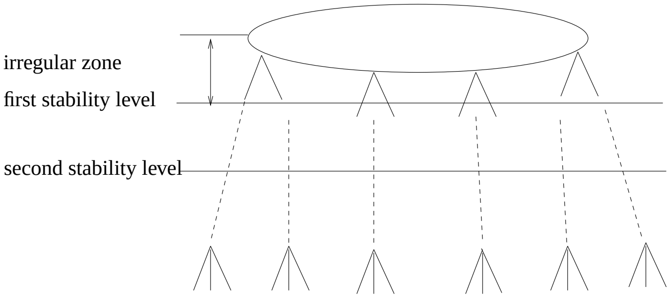


Figure 5.4: An irregular volcano

$\mathcal{P}$ is non-zero at every level from the first stability level up to the level $\max(h+1-2n_2, 0)$ (by Lemma 6.1). We call this level *the second level of stability*. On the second stability level there is at least one point of order ℓ^{n_2} with pairing equal to a primitive ℓ-th root of unity. At every level above the second stability level all polynomials $\mathcal{P}_{E,\ell^{n_2}}$ may be zero[2]. Consider now E a curve on the second stability level and $I : E \to E_1$ an ascending isogeny. Let P be a ℓ^{n_2}-torsion point on E and assume that $T_{\ell^{n_2}}(P,P) \in \mu_\ell^*$. We denote by $\tilde{P} \in E(\mathbb{F}_{q^\ell}) \backslash E(\mathbb{F}_q)$ the point such that $\ell\tilde{P} = P$. By Lemma 5.3 we get $T_{\ell^{n_2+1}}(\tilde{P}, \tilde{P})$ is a primitive ℓ^2-th root of unity. It follows by Lemma 6.1 that $T_{\ell^{n_2}}(I(P), I(P))$ is a primitive ℓ-th root of unity. We deduce that $\mathcal{P}_{E_1,\ell^{n_2+1}}$ corresponding to $E_1/\mathbb{F}_{q^\ell}$ is non-zero. Applying this reasoning repeatedly, we conclude that for every curve E above the second stability level there is an extension field $\mathbb{F}_{q^{s\ell}}$ such that the polynomial $\mathcal{P}_{E,\ell^{n_2+s}}$ associated to the curve defined over $\mathbb{F}_{q^{s\ell}}$ is non-zero. When the second stability level of a volcano is 0, we say that the volcano is *almost regular*.

Proposition 5.8. We use the notations and assumptions from Proposition 5.2. Furthermore, we assume that for all curves E lying at a fixed level i in V the group structure of $E[\ell^\infty](\mathbb{F}_q)$ is $\mathbb{Z}/\ell^{n_1}\mathbb{Z}\times\mathbb{Z}/\ell^{n_2}\mathbb{Z}$, with $n_1 \geq n_2$. The value of $N_{E,\ell^{n_2}}$, the number of zeros of the polynomial defined at 5.3.2, is constant for all curves lying at level i in the volcano.

Proof. Let E_1 and E_2 be two curves lying at level i in the volcano V. Then by Proposition 5.2 they both have endomorphism ring isomorphic to some order $\mathcal{O}_{d_i}$. We denote by $\mathcal{E}\ell\ell_{d_i}(\mathbb{F}_q)$ the set of elliptic curves defined over $\mathbb{F}_q$ with endomorphism ring isomorphic to $\mathcal{O}_{d_i}$. Now by taking into account the fact that the action of $C(\mathcal{O}_{d_i})$ on $\mathcal{E}\ell\ell_{d_i}(\mathbb{F}_q)$ is transitive, we consider an isogeny $\phi : E_1 \to E_2$ of degree ℓ_1. By applying Proposition 3.2, we may assume that $(\ell_1, \ell) = 1$. Take now P and Q two independent ℓ^{n_2}-torsion points on E_1 and denote by $\mathcal{P}_{E_1,\ell^{n_2}}$ the quadratic polynomial corresponding to the ℓ^{n_2}-torsion on E_1 as in . We use Lemma 6.1 to compute $S(\phi(P), \phi(P))$, $S(\phi(P), \phi(Q))$ and $S(\phi(Q), \phi(Q))$ and deduce that a polynomial $\mathcal{P}_{E_2,\ell^{n_2}}(a,b)$ on the curve E_2 computed from $\phi(P)$ and $\phi(Q)$ is such that

$$\mathcal{P}_{E_1,\ell^{n_2}}(a,b) = \mathcal{P}_{E_2,\ell^{n_2}}(a,b).$$

[2] In all the examples we considered for this case, $\mathcal{P}$ is always 0.

This means that $N_{E_1,\ell^{n_2}}$ and $N_{E_2,\ell^{n_2}}$ coincide, which concludes the proof. Moreover, we have showed that the value of k for two curves lying on the same level of a volcano is the same. □

Proposition 5.9. Let E be an elliptic curve defined a finite field $\mathbb{F}_q$ and let $E[\ell^\infty](\mathbb{F}_q)$ be isomorphic to $\mathbb{Z}/\ell^{n_1}\mathbb{Z} \times \mathbb{Z}/\ell^{n_2}\mathbb{Z}$ with $\ell \geq 3$ and $n_1 \geq n_2 \geq 1$. Suppose $N_{E,\ell^{n_2}} \in \{1, 2\}$ and let P be a ℓ^{n_2}-torsion point with degenerate self-pairing. Then the ℓ-isogeny whose kernel is generated by $\ell^{n_2-1}P$ is either ascending or horizontal. Moreover, for any ℓ^{n_2}-torsion point Q whose self-pairing is non-degenerate, the isogeny with kernel spanned by $< \ell^{n_2-1}Q >$ is descending.

Proof. *Case 1.* Suppose $T_{\ell^{n_2}}(P, P) \in \mu_{\ell^k}$, $k \geq 1$ and that $T_{\ell^{n_2}}(Q, Q) \in \mu_{\ell^{k+1}} \backslash \mu_{\ell^k}$. Denote by $I_1 : E \to E_1$ the isogeny whose kernel is generated by $\ell^{n_2-1}P$ and $I_2 : E \to E_2$ the isogeny whose kernel is generated by $\ell^{n_2-1}Q$. By repeatedly applying lemmas 5.3 and 6.1, we get the following relations for points generating the ℓ^{n_2-1}-torsion on E_1 and E_2:

$$\begin{aligned} T_{\ell^{n_2-1}}(I_1(P), I_1(P)) &\in \mu_{\ell^{k-1}},\ T_{\ell^{n_2-1}}(\ell I_1(Q), \ell I_1(Q)) \in \mu_{\ell^{k-2}} \backslash \mu_{\ell^{k-3}} \\ T_{\ell^{n_2-1}}(\ell I_2(P), \ell I_2(P)) &\in \mu_{\ell^{k-3}},\ T_{\ell^{n_2-1}}(I_2(Q), I_2(Q)) \in \mu_{\ell^k} \backslash \mu_{\ell^{k-1}}. \end{aligned}$$

with the convention that $\mu_{\ell^e} = \emptyset$ whenever $e \leq 0$. From the relations above, we deduce that on the ℓ-volcano having E, E_1 and E_2 as vertices, E_1 and E_2 do not lie at the same level. Given the fact that there are at least $\ell - 1$ descending rational ℓ-isogenies parting from E and that Q is any of the $\ell - 1$ (or more) ℓ^{n_2}-torsion points with non-degenerate self-pairing, we conclude that I_1 is horizontal or ascending and that I_2 is descending.

Case 2. Suppose now that $k = 0$. Note that the case $n_2 = 1$ was already treated in Proposition 5.6. Otherwise, consider the curve E defined over $\mathbb{F}_{q^\ell}$. By Lemma 5.3 we have $k = 1$ for points on $E/\mathbb{F}_{q^\ell}$, so we may apply Case 1. □

Remark 5.3. The statement at point (b) of Lemma 5.3 is not true for $\ell = 2$. The statements in Propositions 5.6 and 5.8 are also true for $\ell = 2$. Note also that all statements in the proof of *Case* 1 of Proposition 5.9 are true for $\ell = 2$ also. The only case that is not clear is the one when $k = 0$ and $n_2 \geq 1$. We did not find a proof for the statement in Proposition 5.7 for $\ell = 2$, but in our computations with MAGMA [68] we did not find any counterexamples either.

A special case. If E is a curve lying under the first stability level and such that

$$E[\ell^\infty](\mathbb{F}_q) \simeq \mathbb{Z}/\ell^{n_1}\mathbb{Z} \times \mathbb{Z}/\ell^{n_2}\mathbb{Z},$$

with $n_1 > n_2$, then it suffices to find a point P_1 of order ℓ^{n_1} and the point $\ell^{n_1-1}P_1$ generates the kernel of an horizontal or ascending isogeny (P_1 has degenerate self-pairing).

Crater detection. Note that when ℓ is split in $\mathcal{O}_E$, there are two horizontal isogenies from E and this is equivalent, by Propositions 5.8 and 5.9, to $N_{E,\ell^{n_2}} = 2$. Similarly, when ℓ is inert in $\mathcal{O}_E$, there are neither ascending nor horizontal isogenies and $N_{E,\ell^{n_2}} = 0$. In these two cases, we easily detect that the curve E is on the crater. These results are summarized in Table 5.1.

Remark 5.4. The results presented in this section hold for all curves, regardless of the value of the discriminant of the endomorphism ring. In particular, they hold for discriminants $-3, -4$.

Table 5.1: Number of roots of $P_{E,\ell^{n_2}}$ on the volcano

$N_{E,\ell^{n_2}}$	Types of isogenies	Level
2	$2 \rightarrow$ $\ell - 1 \downarrow$	0
1	$1 \rightarrow$ or $1 \uparrow$ $\ell \downarrow$	$i,\ 0 \leq i \leq h - 1$
0	$\ell + 1 \downarrow$	0
$\ell + 1$	undecided	> second stability level

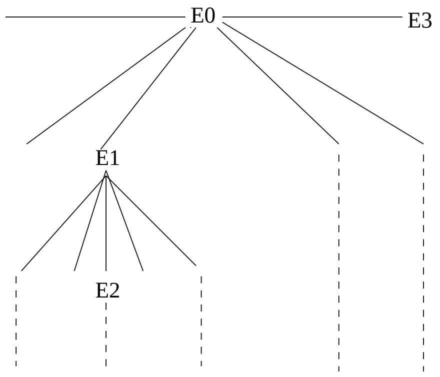
5.3.3 Numeric examples

In this section we give some examples in order to illustrate the results obtained in the previous section. We do not sketch volcanoes entirely, but we give only a descending path in each case. In our tables the notation $[a, b]$ stands for an equation of the type $y^2 = x^3 + ax + b$. For each curve, we give values of self-pairings for three points. Two of these points generate the ℓ^{n_2}-torsion, the third one is a linear combination of the first two.

Example 5.1. Let E be the elliptic curve whose Weierstrass equation is given by

$$y^2 = x^3 + 521631762x + 248125891$$

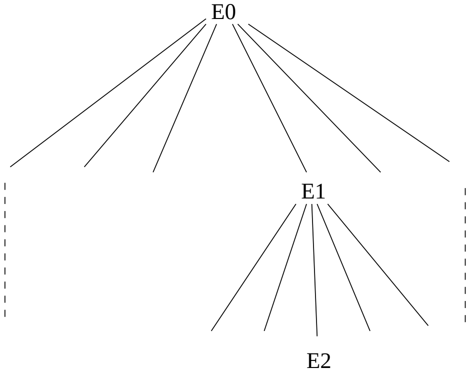
defined over $\mathbb{F}_{1992187501}$. The 5^5-torsion is entirely defined over $\mathbb{F}_{1992187501}$. Our computations using pairings and Vélu's formulae gave the following volcano:



Example 5.2. This example of 5-volcano that is not regular is taken from [34]. The curves are defined over $\mathbb{F}_{5081}$. The polynomial $P_{E_0,5}$ is zero. Our computation showed that by considering E_0 over $\mathbb{F}_{5081^5}$ we get a non-zero polynomial $P_{E_0,5^2}$ and give the following volcano structure:

Example 5.3. This is an example from [71] of a 2-volcano that is non-regular. Note that on a 2-volcanoes, if two self-pairings are degenerate, then any polynomial $P_{E,2^{n_2}}$ is actually zero. We therefore make use of Kohel's and Fouquet-Morain's techniques to build the volcano until we reach the stability level 2. Then we may use pairings and Vélu's formulae to descend to the floor.

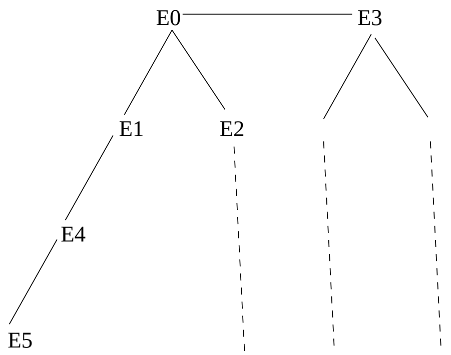
Level	Curve	Equation	ℓ^{n_2}	ℓ^{n_2}-self-pairings	isogeny type
0	E_0	$[521631762, 248125891]$	5^5	$P = (1913305198, 8982844016)$, $T_{5^5}(P, P) \in \mu_{5^5} \backslash \mu_{5^4}$ $Q = (476410925, 1792947402)$, $T_{5^5}(Q, Q) \in \mu_{5^4}$ $R = (1833840623, 747120419)$, $T_{5^5}(R, R) \in \mu_{5^4}$	$\downarrow$ $\rightarrow$ $\rightarrow$
0	E_3	$[1154518985, 1671760359]$	5^5	$P = (1193992046, 1078004656)$, $T_{5^5}(P, P) \in \mu_{5^5} \backslash \mu_{5^4}$ $Q = (1888999464, 1539567655)$, $T_{5^5}(Q, Q) \in \mu_{5^4}$ $R = (1049479475, 786278403)$, $T_{5^5}(R, R) \in \mu_{5^4}$	$\downarrow$ $\rightarrow$ $\rightarrow$
1	E_1	$[13045695, 1561617081]$	5^4	$P = (1498339142, 899662653)$, $T_{5^4}(P, P) \in \mu_{5^2}$ $Q = (537818240, 209505883)$, $T_{5^4}(Q, Q) \in \mu_{5^4} \backslash \mu_{5^3}$ $R = (303596911, 620007624)$, $T_{5^4}(R, R) \in \mu_{5^4} \backslash \mu_{5^3}$	$\uparrow$ $\downarrow$ $\downarrow$
2	E_2	$[951374589, 1320401943]$	5^3	$P = (881997308, 908148660)$, $T_{5^3}(P, P) = 1$ $Q = (1032634348, 321607146)$, $T_{5^3}(Q, Q) \in \mu_{5^3} \backslash \mu_{5^2}$ $R = (1027305622, 1924912950)$, $T_{5^3}(R, R) \in \mu_{5^3} \backslash \mu_{5^2}$	$\uparrow$ $\rightarrow$ $\rightarrow$



Level	Curve	Equation	ℓ^{n_2}	ℓ^{n_2}-self-pairings	isogeny type
0	E_0	$[1355, 2505]$	5	$P = (4036, 3650)$, $T_5(P, P) = 1$ $Q = (3811, 2838)$, $T_5(Q, Q) = 1$ $R = (1470, 2065)$, $T_5(R, R) = 1$	undetermined undetermined undetermined
1	E_1	$[3688, 3542]$	5	$P = (4675, 4827)$, $T_5(P, P) \in \mu_5 \backslash \{1\}$ $Q = (2005, 4622)$, $T_5(Q, Q) \in \mu_5 \backslash \{1\}$ $R = (4681, 3860)$, $T_5(R, R) = 1$	$\downarrow$ $\downarrow$ $\uparrow$
2	E_2	$[3332, 4679]$	–	–	–

5.3.4 Walking on the volcano: new algorithms

In our algorithms, we first need to choose an extension field of $\mathbb{F}_q$ to guarantee that the kernels of all required isogenies are spanned by ℓ-torsion points defined on this extension field. As explained in Corollary 5.1, the degree of this extension field is the order of q modulo ℓ and it can be computed very quickly after factoring $q - 1$. Once this is done, assuming that we are starting from a curve below the second level of stability, we use Algorithms 9 and 10 to find all ascending or horizontal isogenies from the initial curve. In order to walk a descending path, it suffices to choose any other isogeny. Note that, in the subsequent steps of a descending path, in the cases where the group



Level	Curve	Equation	ℓ^{n_2}	ℓ^{n_2}-self-pairings	ℓ-torsion
0	E_0	$y^2 = x^3 + 206x^2 + 144x$	2	$P = (3, 0)$, $T_2(P, P) = 1$ $Q = (48, 0)$, $T_2(Q, Q) = 1$ $R = (0, 0)$, $T_2(R, R) = 1$	undetermined undetermined undetermined
0	E_3	$y^2 = x^3 + 206x^2 + 195x + 78$	2	$P = (51, 0)$, $T_2(P, P) = 1$ $Q = (24, 0)$, $T_2(Q, Q) = 1$ $R = (233, 0)$, $T_2(R, R) = 1$	undetermined undetermined undetermined
1	E_1	$y^2 = x^3 + 206x^2 + 48x + 224$	2	$P = (45, 0)$, $T_2(P, P) = 1$ $Q = (108, 0)$, $T_2(Q, Q) = 1$ $R = (155, 0)$, $T_2(R, R) = 1$	undetermined undetermined undetermined
1	E_2	$y^2 = x^3 + 206x^2 + 138x + 150$	2	$P = (10, 0)$, $T_2(P, P) = 1$ $Q = (212, 0)$, $T_2(Q, Q) = 1$ $R = (86, 0)$, $T_2(R, R) = 1$	undetermined undetermined undetermined
2	E_4	$y^2 = x^3 + 206x^2 + 221x + 33$	2	$P = (121, 0)$, $T_2(P, P) \in \mu_2 \backslash \{1\}$ $Q = (31, 0)$, $T_2(Q, Q) = 1$ $R = (156, 0)$, $T_2(R, R) \in \mu_2 \backslash \{1\}$	$\downarrow$ $\uparrow$ $\downarrow$
3	E_5	$y^2 = x^3 + 206x^2 + 37x + 66$	–	–	–

structure satisfies $n_1 > n_2$, it is not necessary to run Algorithm 10 as a whole. Indeed, since we know that we are not on the crater, there is a single ascending isogeny and it is spanned by $\ell^{n_1-1}P_1$. In order to walk an ascending or horizontal path, it suffices to choose one of the isogenies found by Algorithm 10, taking care not to backtrack.

5.4 Complexities and efficiency comparison

Before analyzing the complete algorithms, we first compare the costs of taking a single step on a volcano by using the two methods existing in the literature: modular polynomials and classical Vélu's formulae. Suppose that we wish to take a step from a curve E. With the modular polynomial approach, we have to evaluate the polynomial $f(X) = \Phi_\ell(X, j(E))$ and find its roots in $\mathbb{F}_q$. Assuming that the modular polynomial (modulo the characteristic of $\mathbb{F}_q$) is given as input and using asymptotically fast algorithms to factor $f(X)$, the cost of a step in terms of arithmetic

Algorithm 9 Computing the structure of the ℓ^∞-torsion of E over $\mathbb{F}_q$
(assuming volcano height ≥ 1)

```
INPUT: A curve $E$ defined over $\mathbb{F}_q$, a prime $\ell$
OUTPUT: Structure $\mathbb{Z}/\ell^{n_1}\mathbb{Z} \times \mathbb{Z}/\ell^{n_2}\mathbb{Z}$, generators $P_1$ and $P_2$
 1: Check that $q \equiv 1 \pmod{\ell}$ (if not need to move to extension field: abort)
 2: Let $t$ be the trace of $E(\mathbb{F}_q)$.
 3: Check $q + 1 - t \equiv 0 \pmod{\ell}$ (if not consider twist or abort)
 4: Let $d_\pi = t^2 - 4q$, let $z$ be the largest integer such that $\ell^z | d_\pi$ and $h = \lfloor \frac{z}{2} \rfloor$
 5: Let $n$ be the largest integer such that $\ell^n | q + 1 - t$ and $N = \frac{q+1-t}{\ell^n}$
 6: Take a random point $R_1$ on $E(\mathbb{F}_q)$, let $P_1 = N \cdot R_1$
 7: Let $n_1$ be the smallest integer such that $\ell^{n_1} P_1 = 0$
 8: if $n_1 = n$ then
 9:     return Structure is $\frac{\mathbb{Z}}{\ell^n \mathbb{Z}}$, generator $P_1$
        ($E$ is on the floor, ascending isogeny with kernel $\langle \ell^{n-1} P_1 \rangle$)
10: end if
11: Take a random point $R_2$ on $E(\mathbb{F}_q)$, let $P_2 = N \cdot R_2$ and $n_2 = n - n_1$
12: Let $\alpha = \log_{\ell^{n_2} P_1}(\ell^{n_2} P_2) \pmod{\ell^{n_1 - n_2}}$
13: if $\alpha$ is undefined then
14:     Goto 6 ($\ell^{n_2} P_2$ does not belong to $\langle \ell^{n_2} P_1 \rangle$)
15: end if
16: Let $P_2 = P_2 - \alpha P_1$
17: If WeilPairing$_\ell(\ell^{n_1 - 1} P_1, \ell^{n_2 - 1} P_2) = 1$ goto 6 (This checks linear independence)
18: return Structure is $\frac{\mathbb{Z}}{\ell^{n_1} \mathbb{Z}} \times \frac{\mathbb{Z}}{\ell^{n_2} \mathbb{Z}}$, generators $(P_1, P_2)$.
```

Algorithm 10 Finding the kernel of ascending or horizontal isogenies
(Assuming curve not on floor and below the second stability level)

```
INPUT: A curve $E$, its structure $\frac{\mathbb{Z}}{\ell^{n_1}\mathbb{Z}} \times \frac{\mathbb{Z}}{\ell^{n_2}\mathbb{Z}}$ and generators $(P_1, P_2)$.
OUTPUT: The kernels of horizontal/ascending isogenies starting from $E$.
if $n_1 > n_2$ then
    The isogeny with kernel $\langle \ell^{n_1-1} P_1 \rangle$ is ascending or horizontal
    To check whether there is another, continue the algorithm
end if
Let $g$ be a primitive $\ell$-th root of unity in $\mathbb{F}_q$. Let Count = 0
Let $Q_1 = \ell^{n_1-n_2} P_1$
Let $a = T_{\ell^{n_2}}(Q_1, Q_1)$, $b = T_{\ell^{n_2}}(Q_1, P_2) \cdot T_{\ell^{n_2}}(P_2, Q_1)$ and $c = T_{\ell^{n_2}}(P_2, P_2)$
if $(a, b, c) = (1, 1, 1)$ abort (Above the second stability level)
repeat
    Let $a' = a$, $b' = b$ and $c' = c$
    Let $a = a^\ell$, $b = b^\ell$ and $c = c^\ell$
until $a = 1$ and $b = 1$ and $c = 1$
Let $L_a = \log_g(a')$, $L_b = \log_g(b')$ and $L_c = \log_g(c') \pmod{\ell}$.
Let $\mathcal{P}(x, y) = L_a x^2 + L_b xy + L_c y^2 \pmod{\ell}$
if $\mathcal{P}$ has no roots modulo $\ell$ return No isogeny (implies single point crater)
if single root $(x_1, x_2)$ return One isogeny with kernel $\langle \ell^{n_2-1}(x_1 Q_1 + x_2 P_2) \rangle$
if $\mathcal{P}$ has two roots $(x_1, x_2)$ and $(y_1, y_2)$ return Two isogenies with kernels $\langle \ell^{n_2-1}(x_1 Q_1 + x_2 P_2) \rangle$
    and $\langle \ell^{n_2-1}(y_1 Q_1 + y_2 P_2) \rangle$
```

Table 5.2: Number of steps performed on the volcano

	Descent	Ascent/Crater walking
Kohel [61]	$2h$	-
Fouquet and Morain [35]	$3h$	ℓh
Ionica and Joux [49]	1	1

operations in $\mathbb{F}_q$ is $O(\ell^2 + M(\ell)\log q)$, where $M(\ell)$ denotes the operation count of multiplying polynomials of degree ℓ. In this formula, the first term corresponds to evaluation of $\Phi_\ell(X, j(E_{i-1}))$ and the second term to root finding[3].

With Vélu's formulae, we need to take into account the fact that the required ℓ-torsion points are not necessarily defined over $\mathbb{F}_q$, but over an extension field of $\mathbb{F}_q$. Let r denotes the smallest integer such that the required points are all defined over $\mathbb{F}_{q^r}$. We know that $1 \leq r \leq \ell - 1$. Using asymptotically efficient algorithms to perform arithmetic operations in $\mathbb{F}_{q^r}$, multiplications in $\mathbb{F}_{q^r}$ cost $M(r)$ $\mathbb{F}_q$-operations. Given an ℓ-torsion point P in $E(\mathbb{F}_{q^r})$, the cost of using Vélu's formulae is $O(\ell)$ operations in $\mathbb{F}_{q^r}$. As a consequence, in terms of $\mathbb{F}_q$ operations, each isogeny costs $O(\ell M(r))$ operations. As a consequence, when q is not too large and r is close to ℓ, using Vélu formulae is more expensive by a logarithmic factor.

Computing an ascending or horizontal path. With the classical algorithms, each step in an ascending or horizontal path requires to try $O(\ell)$ steps and test each by walking descending paths of height bounded by h. The cost of each descending path is $O(h(\ell^2 + M(\ell)\log q))$ and the total cost is $O(h(\ell^3 + \ell M(\ell)\log q))$ (see [61, 91]). When $\ell >> \log q$, this cost is dominated by the evaluations of the polynomial Φ_ℓ at each j-invariant. Thus, by walking in parallel $\ell + 1$ paths from the original curve, we can amortize the evaluation of $\Phi_\ell(X, j)$ over many j-invariants using fast multipoint evaluation, see [74, Section 3.7] or [95], thus replacing ℓ^3 by $\ell\, M(\ell)\log\ell$ and reducing the complexity of a step to $O(h\ell\, M(\ell)(\log\ell + \log q))$. However, this increases the memory requirements.

With our modified algorithms, we need to find the structure of each curve, compute some discrete logarithms in ℓ-groups, perform a small number of pairing computations (usually five) and compute the roots of $\mathcal{P}_{E,\ell^{n_2}}$. Except for the computation of discrete logarithms, it is clear that all these additional operations are polynomial in n_2 and $\log\ell$ and they take negligible time in practice (see Section 5.4.2). Using generic algorithms, the discrete logarithms cost $O(\sqrt{\ell})$ operations, and this can be reduced to $\log\ell$ by storing a sorted table of precomputed logarithms. After this is done, we have to compute at most two isogenies, ignoring the one that backtracks. Thus, the computation of one ascending or horizontal step is dominated by the computation of isogenies and costs $O(\ell M(r))$.

For completeness, we also mention the complexity analysis of Algorithm 9. The dominating step here is the multiplication by N of randomly chosen points. When we consider the curve over an extension field $\mathbb{F}_{q^r}$, this costs $O(r\log q)$ operations in $\mathbb{F}_{q^r}$, i.e. $O(rM(r)\log q)$ operations in $\mathbb{F}_q$.

Finally, comparing the two approaches on a regular volcano, we see that even in the less favorable case, we gain a factor h compared to the classical algorithms. More precisely, the two

[3] Completely splitting $f(X)$ to find all its roots would cost $O(M(\ell)\log\ell\log q)$, but this is reduced to $O(M(\ell)\log q)$ because we only need a constant number of roots for each polynomial $f(X)$.

Table 5.3: Walking the volcano: Order of the cost per step

	Descending path		Ascending/Horizontal
	One step	Many steps	
[35, 61] Parallel evaluation	$h(\ell^2 + M(\ell)\log q)$ –	$(\ell^2 + M(\ell)\log q)$ –	$h(\ell^3 + \ell\, M(\ell)\log q)$ $h\ell\, M(\ell)(\log \ell + \log q)$
Regular volcanoes	Structure determination		
Best case Worst case $r \approx \ell/2$	$\log q$ $r\, M(r)\log q$		$\log q$ $r\, M(r)\log q$
Regular volcanoes	Isogeny construction		
Best case Worst case $r \approx \ell/2$	ℓ $r\, M(r)$		ℓ $r\, M(r)$
Irregular volcanoes (worst case)	No improvement		

are comparable, when the height h is small and r is close to ℓ. In all the other cases, our modified algorithms are more efficient. This analysis is summarized in Table 5.3. For compactness $O(\cdot)$s are omitted from the table.

5.4.1 Irregular volcanoes

Consider a fixed value of q and let $s = v_\ell(q-1)$. First of all, note that all curves lying on irregular volcanoes satisfy $\ell^{2s}|q+1-t$ and $\ell^{2s+2}|t^2-4q$. For traces that satisfy only the first condition, we obtain a regular volcano. We estimate the total number of different traces of elliptic curves lying on ℓ-volcanoes by $\#\{t \text{ s.t. } \ell^{2s}|q+1-t \text{ and } t \in [-2\sqrt{q}, 2\sqrt{q}]\} \sim \frac{4\sqrt{q}}{\ell^{2s}}$.

Next, we estimate traces of curves lying on irregular volcanoes by

$$\#\{t \text{ s.t. } \ell^{2s}|q+1-t\,,\, \ell^{2s+2}|t^2-4q \text{ and } t \in [-2\sqrt{q}, 2\sqrt{q}]\} \sim \frac{4\sqrt{q}}{\ell^{2s+2}}.$$

Indeed, by writing $q = 1 + \gamma\ell^s$ and $t = 2 + \gamma\ell^s + \mu\ell^{2s}$, and imposing the condition $\ell^{2s+2}|t^2 - 4q$, we find that $t \cong t_0(\gamma, \mu)(\text{mod } \ell^{2s+2})$.

Thus, we estimate the probability of picking a curve whose volcano is not regular, among curves lying on volcanoes of height greater than 0, by $\frac{1}{\ell^2}$. This is not negligible for small values of ℓ. However, since our method also works everywhere on almost regular volcano, the probability of finding a volcano where need to combine our modified algorithm with the classical algorithms is even lower. Furthermore, in some applications, it is possible to restrict ourselves to regular volcanoes.

Remark 5.5. This estimate is very crude because the number of different curves for each value of the trace is close to the Hurwitz class number $H(4q - t^2)$ (see [91, Section 3.1]).

5.4.2 Practical examples

In order to demonstrate the potential of the modified algorithm, we present two examples in which our algorithms walk the crater of an ℓ-volcano for large values of ℓ. We have chosen values of ℓ

for which the modular polynomial approach is expensive, in both time and memory (see [88] for precomputations of modular polynomials).

A favorable case. We consider the favorable case of a volcano of height 2, where all the necessary ℓ-torsion points are defined over the base field $\mathbb{F}_p$, where $p = 619074283342666852501391$ is prime. We choose $\ell = 100003$.
Let E be the elliptic curve whose Weierstrass equation is

$$y^2 = x^3 + 198950713578094615678321\,x + 320441332159698071077747.$$

The group $E[\ell^\infty]$ over $\mathbb{F}_p$ has structure $\frac{\mathbb{Z}}{\ell^4 Z}$. It is spanned by the point

$$P = (110646719734315214798587, 521505339992224627932173).$$

Taking the ℓ-isogeny I_1 with kernel $\langle \ell^3 P\rangle$, we obtain the curve

$$E_1 : y^2 = x^3 + 476298723694969288644436\,x + 260540808216901292162091,$$

with structure of the ℓ^∞-torsion $\frac{\mathbb{Z}}{\ell^3} \times \frac{\mathbb{Z}}{\ell}$ and generators

$$P_1 = (226300457529970756040 69, 207694187789705800930332) \text{ and}$$

$$Q_1 = (304782745358080727058129, 193904829837168032791973).$$

The ℓ-isogeny I_2 with kernel $\langle \ell^2 P_1\rangle$ leads to the curve

$$E_2 : y^2 = x^3 + 212075995763000386527 90\,x + 471086215466928725193841,$$

on the volcano's crater and with structure $\frac{\mathbb{Z}}{\ell^2\mathbb{Z}} \times \frac{\mathbb{Z}}{\ell^2\mathbb{Z}}$ and generators

$$P_2 = (545333002760803067576755, 367548280448276783133614) \text{ and}$$

$$Q_2 = (401515368371004856400951, 225420044066280025495795).$$

Using pairings on these points, we construct the polynomial:

$$\mathcal{P}(x, y) = 97540\,x^2 + 68114\,x\,y + 38120\,y^2,$$

having homogeneous roots $(x, y) = (26568, 1)$ and $(72407, 1)$. As a consequence, we have two horizontal isogenies with kernels $\langle \ell(26568\,P_2 + Q_2)\rangle$ and $\langle \ell(72407\,P_2 + Q_2)\rangle$. We can continue and make a complete walk around the crater which contains 22 different curves. Using a crude implementation under Magma 2.15-15, a typical execution takes about 154 seconds[4] on a single core of an Intel Core 2 Duo at 2.66 GHz. Most of the time is taken by the computation of Vélu's formulas (138.3 seconds) and the computation of discrete logarithms (15.2 seconds) which are not tabulated in the implementation. The computation of pairings only takes 40 milliseconds.

[4] This timing varies between executions. The reason that we first try one root of $\mathcal{P}$, if it backtracks on the crater, we need to try the other one. On average, 1.5 root is tried for each step, but this varies depending on the random choices.

A larger example. We have also implemented the computation for $\ell = 1009$ using an elliptic curve with j-invariant $j = 34098711889917$ in the prime field defined by $p = 953202937996763$. The ℓ-torsion appears in a extension field of degree 84. The ℓ-volcano has height two and the crater contains 19 curves. Our implementation walks the crater in 20 minutes. More precisely, 750 seconds are needed to generate the curves' structures, 450 to compute Vélu's formulas, 28 seconds for the pairings and 2 seconds for the discrete logarithms.

5.5 Two volcano-based algorithms

In this section we present two applications of isogeny volcanoes: an algorithm computing the Hilbert polynomial and another one computing modular polynomials. We explain how these algorithms could be modified in order to use our algorithms for walking the volcano.

5.5.1 Computing the Hilbert polynomial via isogeny volcanoes

The algorithm for computing the Hilbert polynomial via isogeny volcanoes was proposed by Belding et al. [8] and optimized recently by Sutherland [91]. Let $\mathcal{O}_D$ be an order of discriminant D in a quadratic imaginary field K. We consider only primes in the set

$$\mathcal{P}_d = \{p > 3 \text{ prime}: \ 4p = t^2 - v^2 D \text{ for some } t, v \in \mathbb{N}^*\}.$$

This algorithm computes first $H_D(X)$ mod p, for many prime numbers p in $\mathcal{P}$ and then uses the Chinese Remainder Theorem to determine H_D. A prime $p \in \mathcal{P}$ splits in K, which means that $H_D(X)$ splits completely over $\mathbb{F}_p$ by Theorem 3.7. We denote by $\mathcal{E}\ell\ell_D(\mathbb{F}_p)$ the set of elliptic curves having endomorphism ring isomorphic to $\mathcal{O}_D$. Then H_D has $h(D)$ roots, each of them corresponding to the j-invariant of a curve in $\mathcal{E}\ell\ell_D(\mathbb{F}_p)$. Moreover, by Proposition 3.3, there is a free transitive action of $\mathrm{C}(\mathcal{O}_D)$ on $\mathcal{E}\ell\ell_D(\mathbb{F}_p)$. Consequently, Sutherland's algorithm computes H_D mod p by determining its roots and then forming the product of the corresponding linear factors. If one element of $\mathcal{E}\ell\ell_D(\mathbb{F}_p)$ is known, we may use the action of $\mathrm{C}(\mathcal{O}_D)$ to find the entire set $\mathcal{E}\ell\ell_D(\mathbb{F}_p)$. Suppose p verifies the equation $4p = t^2 - v^2 D$. We sketch here the steps of the algorithm ([91, Algorithm 1])

1. Search for a curve E with $j(E) \in Ell_t(\mathbb{F}_p)$.
2. Find an isogenous curve E' with $j(E') \in \mathcal{E}\ell\ell_D(\mathbb{F}_p)$.
3. Enumerate $\mathcal{E}\ell\ell_D(\mathbb{F}_p)$ from $j(E')$ via the action of $\mathrm{C}(\mathcal{O}_D)$.
4. Compute H_D mod p as $H_D(X) = \prod_{j \in \mathcal{E}\ell\ell_D(\mathbb{F}_p)} (X - j)$.

The curve in step 1 is found by randomly testing curves over $\mathbb{F}_p$, until a curve with trace t is found (there are some optimizations on the random search of a curve, but we do not get into the details). We may then use algorithm 7 to find a curve E' with endomorphism ring given by $\mathcal{O}_D$ (step 2). We then choose primes $\ell_1, \ldots, \ell_r$ such that $C(\mathcal{O}_D)$ is generated by ideals of norm ℓ_i, $1 \le i \le r$ and

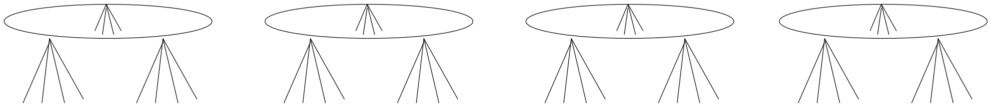


Figure 5.5: Four isogeny volcanoes of height 1

E' lies on the crater of a ℓ_i-volcano, for any ℓ_i. Consequently, we use algorithm **??** in step 3 to enumerate all curves having endomorphism ring $\mathcal{O}_D$.

Since pairing-based algorithms for ascending and for walking on the crater are faster than previous methods, our intuition is that Sutherland's algorithm may be optimized by using our pairing-based algorithms to travel on the volcano.

5.5.2 Modular polynomials via isogeny volcanoes

Bröker, Lauter and Sutherland [90] gave an algorithm using isogeny volcanoes to compute the modular equation. The idea is similar to the one used to compute the Hilbert polynomial in Section 5.5.1. The algorithm computes Φ_ℓ mod p for sufficiently many values of p, and then uses the Chinese Remainder Theorem to compute $\Phi_\ell(X, Y) \in \mathbb{Z}[X, Y]$.

We give a short outline of the algorithm using an example taken from [90]. Figure 5.5.2 depicts a set of four ℓ-volcanoes, each with two levels, the crater and the floor. Each vertex j on the crater has $\ell + 1$ neighbours, which are roots of $\Phi_\ell(X, j) \in \mathbb{F}_p[X]$. If there are at least $\ell + 2$ such j on the craters, it suffices to compute $\ell + 2$ polynomials $\Phi_\ell(X, j)$ and then to interpolate in order to get $\Phi_\ell \in \mathbb{F}_p[X, Y]$.

The curves on the crater of the 4 volcanoes are all roots of the class equation $H_D(X)$, where D is the discriminant of curves lying on the crater. We may then find a root j of H_D and then enumerate the other curves by using the action of $C(\mathcal{O}_D)$.

Similarly, the vertices on the floor are the roots of $H_{\ell^2 D}$ and we may use the action of $C(\mathcal{O}_{\ell^2 D})$ to enumerate them. So we use Vélu's formulae to descend to the floor, we find a curve on the floor and then use the action of $C(\mathcal{O}_{\ell^2 D})$ to find the other curves on the floor. To identify children of a common parent (siblings), we exploit the fact that the siblings lie in a cycle of ℓ^2-isogenies.

We give below a sketch of the algorithm that given ℓ, p and the discriminant D computes Φ_ℓ mod p.

1. Find a root of H_D over $\mathbb{F}_p$.

2. Enumerate the roots j_i of H_D and identify the ℓ-isogeny cycles.

3. For each j_i find an ℓ-isogenous j on the floor.

4. Enumerate the roots of $H_{\ell^2 D}$ and identify the ℓ^2-isogeny cycles.

5. For each j_i compute $\Phi_\ell(X, j_i) = \prod_{(j_i, j_k) \in V}(X - j_k)$.

6. Interpolate $\Phi_\ell \in (\mathbb{F}_p[Y])[X]$ using the j_i and the polynomials $\Phi_\ell(X, j_i)$.

We explain how this algorithm could be modified in order to use our pairing-based algorithms. First of all, instead of precomputing $H_D(X)$ and then factorizing this polynomial mod p in step 1, we could simply search of for a curve of trace t and then use algorithm 10 to ascend to the crater. Note that we can easily recognize a curve on the crater, since the polynomials $P_{E,\ell^{n_2}}$ have two roots if and only if we have reached the crater.

All volcanoes are regular, hence we could Vélu's formulae to enumerate all curves lying on craters and, at the same time, compute the siblings for each of these curves. This is easy since our pairing-based algorithms can distinguish between points spanning kernels of horizontal isogenies and points spanning kernels of descending ℓ-isogenies. This method produces, for each curve j on the crater, the polynomial Φ_ℓ. In order to enumerate all the curves in $\mathcal{E}\ell\ell(\mathbb{F}_p)$ we also need a way to switch from one volcano to another. We may use, for example, the action of $C(\mathcal{O}_D)$. Note that no identification of ℓ-cycles or ℓ^2-cycles is needed in this way and that each curve in $Ell_t(\mathbb{F}_p)$ is only considered once.

Since evaluating complexities of these algorithms is an elaborated task, we do not pretend this method would give a faster algorithm. Further work is necessary to make the most of our approach with pairings.

5.6 Conclusion

In this chapter, we have proposed a method which allows, in the regular part of an isogeny volcano, to determine, given a curve E and a ℓ-torsion point P, the type of the ℓ-isogeny whose kernel is spanned by P. In addition, this method also permits, given a system of generators for the ℓ-torsion, to find the ascending isogeny (or horizontal isogenies) from E. Finally, our study of volcanoes shows that it is possible to determine the level of a curve on the volcano by simply computing a small number of pairings. In particular, we can easily determine if the curve lies on the crater of the volcano. We expect that our algorithms can be used to improve the performance of several volcano-based algorithms, such as the computation of the Hilbert's [91] or modular [90] polynomials.

Part III

Pairings and Cryptography

Chapter 6

Efficient Implementation of Cryptographic Pairings

In this chapter, we study the implementation of cryptographic pairings on elliptic curves. We show that an efficient implementation of the pairing depends on both the choice of the curve and its parameters and on the efficient representation of points on the elliptic curve. We start by presenting in Section 6.2 our formulae for pairing computation in Jacobian coordinates [50]. We explain that for curves with even embedding degrees, pairing computation is most efficient when points are represented as points on the twisted curve. Further, we study endomorphisms on curves with small embedding degree. Section 6.3 gives a brief survey on *distortion maps* on ordinary curves. Distortion maps are used in cryptography to construct non-degenerate self-pairings. First, we show that due to results obtained in our study of isogeny volcanoes in Chapter 5, it is possible to construct curves with non-degenerate self-pairings without using distortions (Section 6.4). Secondly, we implicitly obtain subgroups on the elliptic curve which are invariant under the action of endomorphisms. In Section 6.5 we show that in such subgroups, it is possible to use the action of the endomorphism in order to compute the pairing efficiently. Our method applies to *pairing friendly curves* constructed by the Cocks-Pinch method presented in Chapter 4.

6.1 Pairings in cryptography

A secure pairing-based cryptosystem needs to be implemented in elliptic curve subgroups $\mathbb{G}_1$ and $\mathbb{G}_2$ with a pairing

$$e : \mathbb{G}_1 \times \mathbb{G}_2 \to H,$$

such that the discrete logarithm problem is computationally difficult in $\mathbb{G}_1$, $\mathbb{G}_2$ and in $H \in \mathbb{F}_{q^k}^*$. The best known algorithm for computing discrete logarithms on elliptic curves is the Pollard-rho method [76, 79], which has complexity $O(\sqrt{r})$, where r is the order of the groups $\mathbb{G}_1$ and $\mathbb{G}_2$. Meanwhile, the best known algorithm for solving the discrete logarithm problem in the multiplicative group of a finite field is the index calculus algorithm, which has sub-exponential running time [52, 53]. Consequently, in order to achieve the same level of security in both the elliptic curve subgroups and in the finite field subgroup, we need to choose a q^k which is significantly larger than r. It is therefore interesting to consider the ratio of these sizes:

$$\frac{k \log\ q}{\log\ r}.$$

As the efficiency of the implementation will depend critically on the so-called ρ-value

$$\rho = \frac{\log q}{\log r},$$

it is preferable to keep this value as small as possible and increase the value of the embedding degree k, whenever we want a higher level of security the finite field. The following definition is given by Teske et al. [36].

Definition 6.1. Let E be a curve defined over a finite field $\mathbb{F}_q$. We say that E is *pairing friendly* if the following two conditions hold:

(a) there is a prime r dividing $E(\mathbb{F}_q)$ such that $r \geq \sqrt{q}$;

(b) the embedding degree with respect to r is less than $(\log\ r)/8$.

Teske et al. justify the bound on the size of r in this definition by giving a result due to Luca and Shparlinski [67], who showed that curves having small embedding degree are abundant if $r < \sqrt{q}$ and rare if $r > \sqrt{q}$. The bound on k is based on the requirements for different desired security levels (see [36] for details).

In Chapter 4, we have presented the Cocks-Pinch method to construct curves with small embedding degree and ρ-value 2. Research in pairing-based cryptography during the past few years, has focussed on finding pairing-friendly curves whose ρ-value is closer to 1. Up to now, a small number of examples are known. Miyaji, Nakabayashi and Takano [73] found examples of curves with embedding degrees $3, 4, 6$ and $\rho \approx 1$, but such curves are very rare. In an exhaustive search for such curves, the value of the discriminant of the endomorphism ring of the curve grows very quickly (see [57] and [67]). Barreto and Naehrig [7] gave an example of curves with ρ-value 1 and embedding degree 12. Other examples of families of curves with small ρ-value were found by Kachisa et al. [56] for embedding degrees 16 and 18. The reader should refer to [36] for a survey of all families of pairing friendly curves with ρ-value close to 1. However, note that Vercauteren [36] showed recently that for some discriminants there are no ordinary curves with ρ-value smaller than 2.

Proposition 6.1. Let E be an elliptic curve over $\mathbb{F}_q$ with a subgroup of prime order $r > 3$ and embedding degree $k > 1$ with respect to r. If E has a twist $E'/\mathbb{F}_q$ of degree k and $r \geq 4\sqrt{q}$, then E is supersingular.

Proof. See [36, Prop. 7.1]. □

In particular, this means that there are no ordinary curves with embedding degree 2 and ρ-value smaller than 2. Moreover, ordinary curves with discriminant -4 and embedding degree 4 and those with discriminant -3 and embedding degree 6 have ρ-value at least 2.

6.2 Formulas for pairing computation

One of the most efficient ways of computing pairings on an elliptic curve given by a Weierstrass equation is to use Jacobian coordinates [60] [44]. A point $[X, Y, Z]$ in Jacobian coordinates represents the affine point $(X/Z^2, Y/Z^3)$ on the elliptic curve. We give formulae for the computation of the doubling step of Algorithm 1, using formulae for point doubling on elliptic curves in Jacobian coordinates from [10]. The computation of the addition step is based on results in [3], with the only difference that all our computations are made in $\mathbb{F}_q$ and denominator elimination is not possible.

We first present the computation in a general context, without taking into account the fact that a part of the operations can be done in subfields. This approach is to be considered when implementing pairings on curves with embedding degree 1, such as the self-pairings on isogeny volcanoes introduced in Chapter 5 or the ordinary curves having $k = 1$ for protocols requiring composite order subgroups (see [18, 36]). This computation can be a starting point for pairings on curves with higher embedding degrees.

Finally, in Section 6.2.1, we give simplified computations on curves with even embedding degrees. In the remainder of this chapter, we denote by **s** and **m** the costs of squaring and multiplication in $\mathbb{F}_q$ and by **S** and **M** the costs of these operations in the extension field $\mathbb{F}_{q^k}$, if $k > 1$. Sometimes, if q is a sparse prime (such a generalized Mersenne prime), we may assume that $\mathbf{s}/\mathbf{m} = 0.8$. However, when constructing pairing friendly curves, it is difficult to obtain such primes. Hence, we generally have $\mathbf{s}/\mathbf{m} \approx 1$. Since inversions are expensive, we slightly modify Algorithm 1 in order to perform only one inversion in the end. See Algorithm 11.

Algorithm 11 Computing one inversion in Miller's algorithm

```
Let $i = [\log_2(r)]$, $K \leftarrow P$, $f_1 \leftarrow 1$, $f_2 \leftarrow 1$
while $i \geq 1$ do
   Compute equations of $l$ and $v$ arising in the doubling of $K$.
   $K \leftarrow 2K$ and $f_1 \leftarrow f_1^2 l_1(Q) v_2(Q)$ and $f_2 \leftarrow f_2^2 l_2(Q) v_1(Q)$
   if the $i$-th bit of $l$ is 1 then
      Compute equations of $l$ and $v$ arising in the addition of $K$ and $P$.
      $K \leftarrow P + K$ and $f_1 \leftarrow f_1 l_1(Q) v_2(Q)$ and $f_2 \leftarrow f_2 l_2(Q) v_1(Q)$
   end if
   Let $i \leftarrow i - 1$.
end while
$f \leftarrow f_1/f_2$
return $f$
```

The doubling step

We write the normalized functions l and v that appear in Algorithm 11 as $l = l_1/l_2$ and $v = v_1/v_2$. In the double and add method, after initially setting $K = P$ and $f_1 = f_2 = 1$, we have to do the

Table 6.1: Operations of the doubling part of a Miller operation

$A \leftarrow W_1^2,\ B \leftarrow X_1^2,\ C \leftarrow Y_1^2,\ D \leftarrow C^2$	(4**s**)
$E \leftarrow (X_1 + C)^2 - B - D,\ F \leftarrow 3B + aA,\ G \leftarrow F^2$	(2**s**)
$X_3 \leftarrow -4E + G,\ Y_3 \leftarrow -8D + F \cdot (2E - X_3),\ Z_3 \leftarrow (Y_1 + Z_1)^2 - C - W_1$	(1**m**+1**s**)
$W_3 \leftarrow Z_3^2,\ H \leftarrow (Z_3 + W_1)^2 - W_3 - A,\ I \leftarrow H \cdot y$	(1**m**+2**s**)
$J \leftarrow F \cdot T_1,\ T_3 \leftarrow W_3 \cdot x - X_3,\ L \leftarrow (Z_3 + Z_1)^2 - W_3 - W_1$	(2**m**+1**s**)
$l_1 \leftarrow I - 4C - 2J$	
$f_1 \leftarrow f_1^2 \cdot l_1 \cdot Z_3$	(2**m**+1**s**)
$f_2 \leftarrow f_2^2 \cdot T_3 \cdot L$	(2**m**+1**s**)

following evaluations for the i-th bit of r

$$\begin{aligned} K &\leftarrow 2K, \\ f_1 &\leftarrow f_1^2 l_1(Q) v_2(Q), \\ f_2 &\leftarrow f_2^2 l_2(Q) v_1(Q). \end{aligned} \tag{6.1}$$

We compute $2K = (X_3, Y_3, Z_3)$ as

$$\begin{aligned} X_3 &= (3X_1^2 + Z_1^4)^2 - 8X_1Y_1^2, \\ Y_3 &= (3X_1^2 + aZ_1^4)(4X_1Y_1^2 - X_3) - 8Y_1^4, \\ Z_3 &= 2Y_1Z_1. \end{aligned}$$

The normalized functions l and v, corresponding to the tangent line to the curve at K and the vertical line through the point $2K$, respectively, have the following equations:

$$l(x,y) = l_1(x,y)/l_2 = (Z_3Z_1^2y - 2Y_1^2 - (3X_1^2 + aZ_1^4)(Z_1^2x_Q - X_1))/(Z_3Z_1^2) \tag{6.2}$$

$$v(x,y) = v_1(x,y)/v_2 = (Z_3^2x_Q - X_3)/Z_3^2. \tag{6.3}$$

We represent the point K as $K = [X_1, Y_1, Z_1, W_1, T_1]$, where $[X_1, Y_1, Z_1]$ are the Jacobian coordinates of the point on the Weierstrass curve, $W_1 = Z_1^2$ and $T_1 = Z_1^2x_Q - X_1$. If the intermediate storage is not expensive, then this representation is to be preferred, because it allows some squaring-multiplication trade-offs and it also saves 2 operations. The operation count for the doubling step presented in table 6.1 gives 8**m** + 12**s** + 1**a**.

The mixed addition step

In the implementation of pairing-based protocols, it is often possible to choose the point P such that its Z-coordinate is 1, in order to save some operations. The addition of two points $K = [X_1, Y_1, Z_1]$ and $P = [X_2, Y_2, 1]$ is called *mixed addition*. In Algorithm 11 a mixed addition step implies the following operations

$$\begin{aligned} K &\leftarrow K + P, \\ f_1 &\leftarrow f_1 l_1(Q) v_2(Q), \\ f_2 &\leftarrow f_2 l_2(Q) v_1(Q). \end{aligned} \tag{6.4}$$

Table 6.2: Operations of the addition part of a Miller operation for $k > 2$

$B \leftarrow X_2 \cdot W_1,\ D \leftarrow ((Y_2 + Z_1)^2 - R_2 - W_1) \cdot W_1,\ H \leftarrow B - X_1,\ I \leftarrow H^2$	(2**m**+2**s**)
$E \leftarrow 4I,\ J \leftarrow H \cdot E,\ L_1 \leftarrow (D - 2Y_1),\ V \leftarrow X_1 \cdot E,\ K \leftarrow (Y_2 + Z_3)^2 - R_2 - T_3$	(2**m**+1**s**)
$X_3 \leftarrow L_1^2 - J - 2V;\ Y_3 \leftarrow L_1 \cdot (V - X_3) - 2Y_1 \cdot J$	(2**m**+1**s**)
$Z_3 \leftarrow (Z_1 + H)^2 - W_1 - I,\ W_3 \leftarrow Z_3^2,\ T_3 \leftarrow W_3 \cdot x_Q - X_3,\ l_1 \leftarrow 2Z_3 \cdot y_Q - K - 2L_1 \cdot (x_Q - X_2)$	(3**m**+2**s**)
$f_1 \leftarrow f_1 \cdot l_1$	(1**m**)
$f_2 \leftarrow f_2 \cdot 2Z_3$	(1**m**)

The result of the addition of $K = [X_1, Y_1, Z_1, W_1, T_1]$ and $P = [X_2, Y_2, 1, 1, x_Q - X_2]$ is $K + P = [X_3, Y_3, Z_3, W_3, T_3]$ with

$$\begin{aligned}
X_3 &= (X_1 + X_2Z_1^2)(X_1 - X_2Z_1^2)^2 + (Y_2Z_1^3 - Y_1)^2,\\
Y_3 &= (Y_2Z_1^3 - Y_1)(X_1(X_1 - X_2Z_1^2)^2 - X_3) + Y_1(X_1 - X_2Z_1^2)^2,\\
Z_3 &= Z_1(X_2Z_1^2 - X_1),\\
W_3 &= Z_3^2,\\
T_3 &= W_3x_Q - X_3.
\end{aligned}$$

The lines l and v have the following equations

$$\begin{aligned}
l &= l_1/l_2 = Z_3y - Y_2Z_3 - (2Y_2Z_1^3 - 2Y_1)(x_Q - X_2)/Z_3,\\
v &= (W_3x_Q - X_3)/W_3.
\end{aligned}$$

We precompute $R_2 = Y_2^2$ and $A = x_Q - X_2$. Efficient mixed addition formulas were given by Arène et al. [3]. We slightly modified their operation count in order to adapt it to the general case. Detailed operations are presented in table 6.2 and the total cost is 11**m** + 6**s**.

6.2.1 The Case of Curves with Even Embedding Degree

Pairing computation for curves with embedding degree greater than 1 is different from the computation presented in the previous section, due to the fact that many computations are done in subfields of $\mathbb{F}_{q^k}$. For efficiency reasons, the point P can be chosen such that $\langle P \rangle$ is the unique subgroup of order r in $E(\mathbb{F}_q)$. We may thus describe this subgroup as

$$\mathbb{G}_1 = E[r] \cap \mathrm{Ker}(\pi - [1]). \tag{6.5}$$

In order to get a non-degenerate pairing, we need to define $\mathbb{G}_2$ as a subgroup of order r in $E(\mathbb{F}_{q^k}) \backslash E(\mathbb{F}_q)$. In this section we show that by taking

$$\mathbb{G}_2 = E[r] \cap \mathrm{Ker}(\pi - [q]), \tag{6.6}$$

we get a non-degenerate pairing, as well as an efficient implementation of Miller's algorithm. The following result and its proof are taken from [47].

Theorem 6.1. Let E be an ordinary elliptic curve over $\mathbb{F}_q$ admitting a twist of degree e. Assume that $r > 6$ satisfies $r \| \#E(\mathbb{F}_q)$ and $r^2 \| \#E(\mathbb{F}_{q^e})$. Then there is a unique twist E' of degree e such that

$r \| \#E'(\mathbb{F}_q)$. Furthermore, if we denote by $\mathbb{G}_2'$ the unique subgroup of order r of E' over $\mathbb{F}_q$ and by $\phi : E' \to E$ the twisting isomorphism, the subgroup $\mathbb{G}_2$ described at equation (6.6) is given by

$$\mathbb{G}_2 = \phi(\mathbb{G}_2').$$

Proof. Let E_i for $i = 0, \ldots, e-1$ be the twists of E of degree dividing e. We first show that

$$\#E(\mathbb{F}_{q^e}) = \prod_{i=0}^{e-1} \#E_i(\mathbb{F}_q).$$

For every i, consider the twisting isomorphism $\phi_i : E_i \to E$. This isomorphism of curves gives an isomorphism of endomorphism rings

$$\begin{array}{rcl} \Phi_i : \mathrm{End}(E_i) & \to & \mathrm{End}(E) \\ f & \mapsto & \phi_i \circ f \circ \phi_i^{-1}. \end{array}$$

If we denote by $\pi_{q,i}$ the Frobenius morphism on E_i, we observe that $\Phi_i(\pi_{q,i}) = \phi_i \circ \pi_{q,i} \circ \phi_i^{-1} = \phi_i \circ (\phi_i^{-1})^\sigma \circ \pi_q$. Since the degree of the twist ϕ_i divides e, we conclude that $\phi_i \circ (\phi_i^{-1})^\sigma$ is an automorphism of E of degree dividing e, i.e. a e-th root of unity. Since we have an isomorphism $[] : \mu_e \to \mathrm{Aut}(E)$, we can label the twists of E_i by $\Phi_i(\pi_{q,i}) = [\xi_i]\pi_q$, with ξ_i a e-th root of unity. Therefore we have

$$E_i(\mathbb{F}_q) \simeq \mathrm{Ker}([\xi_i]\pi_q - 1).$$

Moreover, we can factor $\pi_q^e - 1$ as

$$\pi_q^e - 1 = (-1)^{e-1} \prod_{i=0}^{e-1} ([\xi_i]\pi_q - 1).$$

Since $\pi_q^e - 1$ is separable (as explained in Section 2.6) and $\#E(\mathbb{F}_{q^e}) = \#\mathrm{Ker}(\pi_q^e - 1)$, we take degrees of separability and get $\#E(\mathbb{F}_{q^e}) = \prod_{i=0}^{e-1} \#E_i(\mathbb{F}_q)$. Since $r \| \#E(F_q)$ and $r^2 \| \#E(\mathbb{F}_{q^e})$, it follows that there is a twist E' of degree e such that $r \| \#E'(\mathbb{F}_q)$. We denote by $\phi : E' \to E$ the twisting isomorphism and by $\mathbb{G}'$ the unique subgroup of order r in $E(\mathbb{F}_q)$. Note that $E'(\mathbb{F}_q) \simeq \mathrm{Ker}([\xi]\pi_q - 1)$ (for some e-th root of unity ξ) and that $\mathrm{Ker}([\xi]\pi_q - 1)$ is stable under π_q. We conclude that $\mathbb{G}_2 = \phi(\mathbb{G}_2')$. □

In the remainder of this section, we suppose that the embedding degree is even and that E has a twist of order 2 defined over $\mathbb{F}_{q^{k/2}}$. From theorem 6.1 and by using the equations of twists given in Section 2.8, we derive an efficient representation of points in $\mathbb{G}_2$. In the remainder of this section, we consider a twist of degree 2 of the curve E defined over $\mathbb{F}_{q^{k/2}}$, whose cardinality is divisible by r. It follows that the subgroup $\mathbb{G}_2 = \langle Q \rangle \subset E(\mathbb{F}_{q^k})$ can be chosen such that the x-coordinates of all its points lie in $\mathbb{F}_{q^{k/2}}$ and the y-coordinates are products of elements of $\mathbb{F}_{q^{k/2}}$ with $\sqrt{\beta}$, where β is not a square in $\mathbb{F}_{q^{k/2}}$ and $\sqrt{\beta}$ is a fixed square root in $\mathbb{F}_{q^k}$.

We look at the doubling step of the Miller operation detailed in equation (6.1). Since k is the multiplicative order of q modulo r, $(q^k - 1)/r$ is a multiple of $q^{k'} - 1$ for any proper divisor k' of k. We observe that the terms $l_2(Q)$, $v_2(Q)$ and $v_1(Q)$ in equations (6.2) and (6.3) can be ignored,

Table 6.3: Cost of one step in Miller's algorithm for even embedding degree

	Doubling		Mixed addition
	$k = 2$	$k \geq 4$	
$\mathcal{J}$ [50], [3]	3**m** + 10**s** + 1**a** + 1**M** + 1**S**	(1+k)**m**+11**s**+1**a**+1**M**+1**S**	(6+k)**m**+6**s**+1**M**
$\mathcal{J}$,$y^2 = x^3 + b$ $e = 2, 6$ [23]	(2k/e+2)**m**+7**s**+1**a**+1**M**+1**S**	(2k/e+2)**m**+7**s**+1**a**+1**M**+1**S**	(2k/e+9)**m**+2**s**+1**M**
$\mathcal{J}, y^2 = x^3 + ax$ $e = 2, 4$ [23]	(2k/e+2)**m**+8**s**+1**a**+ 1**M**+1**S**	(2k/e+2)**m**+8**s**+1**a**+ 1**M**+1**S**	(2k/e+12)**m**+4**s**+1**M**

because they lie in proper subfields of $\mathbb{F}_{q^k}$ and would give 1, after the final exponentiation step (the computation of the reduced Tate pairing). Consequently, the doubling part of Miller's algorithm at equation (6.1) becomes

$$\begin{aligned} K &\leftarrow 2K, \\ f_1 &\leftarrow f_1^2 l_1(Q). \end{aligned}$$

We represent the point K as $K = [X_1, Y_1, Z_1, W_1]$, where $[X_1, Y_1, Z_1]$ are the Jacobian coordinates of the point K on the Weierstrass curve and $W_1 = Z_1^2$.
For $k = 2$ we have $x_Q \in \mathbb{F}_q$, hence we compute the function l_1 as follows

$$l_1(x_Q, y_Q) = Z_3 W_1 y_Q - 2Y_1^2 - (3X_1^2 + aW_1^2)(W_1 x_Q - X_1).$$

For $k > 2$, x_Q is in $\mathbb{F}_{q^{k/2}}$, hence the computation is slightly different

$$l_1(x_Q, y_Q) = Z_3 W_1 y_Q - 2Y_1^2 - W_1(3X_1^2 + aW_1^2)x_Q + X_1(3X_1^2 + aW_1^2).$$

We no longer detail the computations, which are similar to those in table 6.1. Our count gives 10**s** + 3**m** + 1**a** + 1**S** + 1**M** for $k = 2$ and 11**s** + $(k + 1)$**m** + 1**a** + 1**S** + 1**M** if $k > 2$ (see also [50]). Due to the fact that we ignore terms lying in proper subfields of $\mathbb{F}_{q^k}$, the mixed addition step in equation (6.4) is

$$\begin{aligned} K &\leftarrow K + P, \\ f_1 &\leftarrow f_1 l_1(Q). \end{aligned}$$

The line l_1 is given by the equation

$$l_1 = Z_3 y_Q - Y_2 Z_3 - (2Y_2 Z_1^3 - 2Y_1)Z_2^3 x_Q + X_2 Z_2(2Y_2 Z_1^3 - 2Y_1).$$

The operation count, detailed in [3], gives 6**s** + 6**m** + k**m** + 1**M**.

In Table 6.3 we summarize all these results, and we also give the operation count for pairing computation on curves allowing twists of higher degree (i.e. 4 and 6). The computation in these special cases can be found in [23].

6.3 Self-pairings and distortion maps

We say that an endomorphism $\phi : E \to E$ is a *distortion map* on E with respect to a point P on E if $\phi(P) \notin \langle P \rangle$.

Example 6.1. We consider the curve given by the equation

$$y^2 = x^3 + ax, \tag{6.7}$$

where $q \equiv 3 \pmod 4$. The latter condition ensures that -1 is not a square in $\mathbb{F}_q$. A distorsion map for points (x, y) defined over $\mathbb{F}_q$ is given by $\phi(x, y) = (-x, iy)$, with $i^2 = -1$.

The curve in Example 6.7 is supersingular. Verheul [94] showed that on supersingular curves all points have distortion maps.

In cryptography, special attention has been paid to distortion maps because they enable the construction of non-degenerate self-pairings. Indeed, in the case of the Tate pairing, if $T_r(P, P) = 1$, then $T_r(P, \phi(P)) \neq 1$ if $\phi(P) \notin \langle P \rangle$. This is due to the non-degeneracy of the pairing. First of all, this can be used in the implementation of protocols which require pairings with $\mathbb{G}_1 = \mathbb{G}_2$. Secondly, this property can be used to solve the DDH hypothesis on some order r groups. Indeed, given a 4-uple (P, aP, bP, cP), we can decide whether $ab \equiv c \pmod r$ by verifying if

$$T_r(aP, \phi(bP)) = T_r(P, \phi(cP)).$$

Since in this dissertation we focus on ordinary curves, we survey results on distortion maps on these curves. The following result is due to Charles [24].

Theorem 6.2. Let E be an ordinary elliptic curve defined over a finite field $\mathbb{F}_q$ and denote by $\mathcal{O}$, the endomorphism ring of E. $\mathcal{O}$ is an order in a quadratic imaginary field with maximal order $\mathcal{O}_K$ and discriminant d_K. Suppose r is a prime such that $E[r] \subset \mathbb{F}_q$, but no point of order r is defined over a smaller extension field.

(a) If $r | [\mathcal{O}_K : \mathcal{O}]$, then there are no distortion maps.

(b) If $r \nmid [\mathcal{O}_K : \mathcal{O}]d_K$ and

  (i) r is inert in $\mathcal{O}_K$, then there are distortion maps for every (order r) subgroup of $E[r]$;

  (ii) r is split in $\mathcal{O}_K$, then all but two subgroups of $E[r]$ have distortion maps.

(c) If $r \nmid [\mathcal{O}_K : \mathcal{O}]$ and $r | d_K$, so that r is ramified in $\mathcal{O}_K$, then all (except one) subgroups of $E[r]$ have distortion maps.

Proof. It is easy to see that if $r | [\mathcal{O}_K : \mathcal{O}]$ there are no distortion maps, because the reduction modulo r of every endomorphism is the multiplication by a scalar. Suppose now that $r \nmid [\mathcal{O}_K : \mathcal{O}]$. We have

$$\mathcal{O}_K/(r) \cong \mathcal{O}/(r).$$

If $r \nmid d_K$ and r is inert in $\mathcal{O}_K$, then $\mathcal{O}/(r) \cong \mathbb{F}_{r^2}$. We take $\alpha \in \mathcal{O}$ such that $\alpha \pmod r$ does not lie in $\mathbb{F}_r$. Then the action of α on $E[r]$ is irreducible over $\mathbb{F}_r$, since the characteristic equation is irreducible. It follows that no subgroup of order r is stabilized by α, hence α is a distortion map for all points in $E[r]$. If $r \nmid d_K$ and r is split in $\mathcal{O}_K$, then $\mathcal{O}/(r) \cong \mathbb{F}_r[X]/(X-a)(X-b) \cong (\mathbb{Z}/r\mathbb{Z})^2$ (where $a \neq b$). The action of any $\alpha \in \mathcal{O}_K$ corresponds to X in $\mathbb{F}_r(X)/(X-a)(X-b)$ and is conjugate to a matrix of the form

$$\begin{pmatrix} \gamma & 0 \\ 0 & \delta \end{pmatrix}$$

Distortion maps exist for all but two subgroups of $E[r]$. Finally, if r is ramified, $\mathcal{O}/(r) \cong \mathbb{F}_r[X]/(X-a)^2$. Consider the map $\alpha \in \mathcal{O}$ that corresponds to X in the ring $\mathbb{F}_r[X]/(X-a)^2$. Then the action of α on $E[r]$ is given by the matrix

$$\begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix}$$

with $\beta \neq 0$. We conclude that there are distortion maps for all but one subgroup of $E[r]$. □

Suppose now that the embedding degree k with respect to r is greater than 1. For any point $P \in E(\mathbb{F}_{q^k})$, we define the trace map as

$$Tr(P) = \sum_{i=0}^{k-1} \pi^i(P).$$

This map was proposed as a distortion map in [16] and [17]. We consider two points $P \in \mathbb{G}_1$ and $Q \in \mathbb{G}_2$, where $\mathbb{G}_1$ and $\mathbb{G}_2$ are the subgroups defined at equations (6.5) and (6.6). It is easy to check that for $R = aP + bQ$, with $ab \neq 0$, then $Tr(R) = kaP$. This means that the trace is a distortion map for all points of order r that are neither in $\mathbb{G}_1$, nor in $\mathbb{G}_2$. Verheul [94] shows that there are no distortion maps for points in $\mathbb{G}_1$ and $\mathbb{G}_2$.

Theorem 6.3. Let E be an ordinary curve defined over $\mathbb{F}_q$ and let P be a point over E of prime order $r \neq \text{char}(\mathbb{F}_q)$. Suppose the embedding degree k is greater than 1 and denote by Q the point defined over $\mathbb{F}_{q^k}$, such that $\pi(Q) = qQ$. Then there are no distorsion maps for P and Q.

Proof. Suppose there is a distortion ϕ of $\langle P \rangle$. Then we have

$$\phi(\pi(P)) = \pi(\phi(P)) \text{ and } \phi(\pi(P)) = \phi(P). \tag{6.8}$$

The first equality comes from the fact that the ring $\text{End}(E)$ is commutative, while the second one is due to the fact that $P \in E(\mathbb{F}_q)$. It follows that $\pi(\phi(P)) = \phi(P)$, hence $\phi(P)$ is an eigenvector for the eigenvalue 1 of π. This means that $\phi(P) \in \langle P \rangle$. The proof for Q is similar. □

The conclusion is that by choosing to implement the pairing on $\mathbb{G}_1 \times \mathbb{G}_2$, we get efficient pairing implementation and also work in subgroups for which the DDH problem is difficult.

6.4 Constructing non-degenerate self-pairings on ordinary curves

As explained in the previous section, in some pairing-based protocols we need a non-degenerate self-pairing

$$e : \mathbb{G} \times \mathbb{G} \to H.$$

On ordinary curves, a first way to construct such pairings is to use theorem 6.2. One may choose a large prime r and an order O in a quadratic imaginary field K. Suppose that the discriminant D of O is such that $\left(\frac{D}{r}\right) = -1$. We construct a curve with embedding degree 1 and discriminant D by the complex multiplication method (for example using the Cocks Pinch method). In this case, $E[r] \subseteq E(\mathbb{F}_q)$ and any endomorphism is a distortion map for all points of order r on the curve. Hence we can build non-degenerate self-pairings using the distortion. If D is small, we can efficiently compute endomorphisms and use this method.

A second possibility is to use the trace map defined at (6.8) on curves with $k > 1$, but the implementation of the pairing is very expensive, since we use a subgroup $\mathbb{G}$ which is different from $\mathbb{G}_1$ and $\mathbb{G}_2$. More precisely, all the operations during the pairing computation are performed in $\mathbb{F}_{q^k}$, since we do not have an efficient representation for points in $\mathbb{G}$.

Suppose now that r is a prime such that E has embedding degree 1 with respect to r and that $E[r] \subseteq E(\mathbb{F}_q)$. Proposition 5.7 shows that if E is on the crater of a regular volcano and there is no point of order r^2 in $E(\mathbb{F}_q)$, there will be at least point of order r with non-degenerate self-pairing on E. The number of subgroups with non-degenerate self-pairings on a curve is in fact given by the shape of the crater. More precisely, we have

1. If r is inert in O_K, then all subgroups of order r have non-degenerate self-pairing.
2. If r is split in O_K, then all but two subgroups have non-degenerate self-pairings.
3. If r is ramified in O_K, then all (except one) subgroups of order r have non-degenerate self-pairings.

Note that our result is similar to the one given in theorem 6.2. We choose r and the discriminant D such that $\left(\frac{D}{r}\right) = -1$. We use the Cocks-Pinch method to construct curves with embedding degree 1 with respect to r and discriminant D. The algorithm will produce a prime number of the form $p = (4 + 4sr - D(vr)^2)/4$. If r is large enough, v will not be divisible by r and the r-volcano has height 1. Since $\#E(\mathbb{F}_p) = p - 1$, we have $r^2 \| \#E(\mathbb{F}_p)$. Note that the curve constructed by the CM method lies on the crater of the volcano, hence the structure of the r-torsion is

$$E[r] \simeq \mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/r\mathbb{Z}.$$

Since the volcano is regular, any point of order r on E will have non-degenerate self-pairing.

Example 6.2. A toy example:

$$\begin{aligned}
D &= -4 \cdot 5,\\
r &= 1048613,\\
p &= 19792606027842001,\\
E &: y^2 + xy = x^3 + 18940287523734171x + 5474270604842005,\\
P &= (13679054837080486 : 14162470055178600 : 1),\\
T_r(P, P) &= 11431087027967778 \in \mu_r^*.
\end{aligned}$$

We have given a method to to find non-degenerate self-pairings on curves with embedding degree 1. Since our curves are such that the group of points of order r is defined over $\mathbb{F}_p$, they have ρ-value 2. Thus pairing implementation on these curves will be less efficient than implementation of self-pairings obtained using distortion maps on supersingular curves with $k = 2$. Moreover, for $k > 1$, hashing to points on the elliptic curve is possible due to the properties of the Frobenius endomorphism. Hence, we do not know whether it is possible to hash to points on our curves with embedding degree 1.

6.5 Speeding up pairing computation using isogenies

To our knowledge, the first time isogenies were proposed to speed up pairing computation was in a paper by Barreto, Galbraith, O'HEigeartaigh and Scott [6]. They introduced the Eta pairing and showed how the Tate pairing can be calculated from it using a loop of only half the size of the loop in Miller's algorithm. This idea was extended by Hess, Smart and Vercauteren in [47]. We present the main result in [47], without giving the proof.

Theorem 6.4. Let E be an elliptic curve defined over $\mathbb{F}_q$ and r a large prime with $r|\#E(\mathbb{F}_q)$. We denote by k the embedding degree and by t the trace of the Frobenius.

(a) For $T = t - 1$, $Q \in \mathbb{G}_2 = E[r] \cap \mathrm{Ker}(\pi - [q])$, and $P \in \mathbb{G}_1 = E[r] \cap \mathrm{Ker}(\pi - [1])$ we have

  (i) $f_{T,Q}(P)$ defines a bilinear pairing, which we call *the Ate pairing*.

  (ii) Let $N = \gcd(T^k - 1, q^k - 1)$ and $T^k - 1 = LN$. Then

$$t_r(Q, P)^L = f_{T,Q}(P)^{c(q^k-1)/N},$$

  where $c = \sum_{i=0}^{k-1} T^{k-1-i} q^i \equiv kq^{k-1} \pmod r$. For $r \nmid L$, the Ate pairing is non-degenerate.

(b) Assume that E has a twist of degree e and set $m = \gcd(k, e)$ and $f = k/m$. We denote by $c = \sum_{i=0}^{m-1} T^{f(m-1-i)} q^{fi} \equiv mq^{f(m-1)} \bmod r$. We have

  (i) $f_{T^f,P}(Q)$ defines a bilinear pairing, which we call *the twisted Eta pairing*.

  (ii) $t_r(P, Q)^L = f_{T^f,P}(Q)^{c(q^k-1)/N}$ and the twisted Eta pairing is non-degenerate if $r \nmid L$.

The loop in Miller's algorithm for computing the Ate (twisted Eta) pairing has length $\log t$ ($\log t^f$). When the trace t is small, this gives an algorithm that is more efficient than the one computing the Tate pairing. Many families of pairing friendly curves have small trace and give efficient implementations of the Ate pairing (see [47] for details).

Notation 6.1. In the sequel we denote the correction of two points R_1 and R_2 as follows:

$$\mathrm{corr}_{R_1,R_2} = \frac{l_{R_1,R_2}}{v_{R_1+R_2}},$$

where l_{R_1,R_2} is the line passing through R_1 and R_2 and $v_{R_1+R_2}$ is the vertical line through $R_1 + R_2$.

Our starting idea is a method to exploit efficiently computable endomorphisms in pairing computation suggested by Scott [83], for a family of curves called NSS. These curves are defined over $\mathbb{F}_q$ with $q \equiv 1 \bmod 3$ and given by an equation of the form $y^2 = x^3 + B$. Since they have $k = 2$ and $\rho \sim 2$, the Eta and Ate pairings will not bring any improvement to pairing computation. However, these curves admit an endomorphism $\phi : (x, y) \to (\beta x, y)$, where β is a non-trivial cube root of unity. Its characteristic equation is $\phi^2 + \phi + 1 = 0$. If P is an eigenvalue of ϕ such that $\phi(P) = \lambda P$, then λ verifies the equation

$$\lambda^2 + \lambda + 1 = cr.$$

We obtain

$$f^c_{r,P}(Q) = f_{\lambda^2+\lambda,P}(Q) = f_{\lambda(\lambda+1),P}(Q) = f^{\lambda+1}_{\lambda,P}(Q) \cdot f_{\lambda+1,[\lambda]P}(Q) \cdot \frac{l_{[\lambda]P,P}}{v_{[\lambda+1]P}}.$$

Since for $P = (x, y)$, λP is given by $(\beta x, y)$, we can easily compute $f_{\lambda,\lambda P}(Q)$ and $f_{\lambda,P}(Q)$ at the same time when running Miller's algorithm, by replacing x with βx when computing doublings, additions and line equations. Note that pairing computation on these curves has been recently improved by Zhao and al. [96].

We apply similar techniques to curves with endomorphisms that verify a characteristic equation $x^2 + ax + b = 0$, with a, b small. In all cases, we use the Cocks-Pinch method to construct curves such that there is a $\lambda \sim \sqrt{r}$ which verifies $\lambda^2 + a\lambda + b = cr$. This can be done by exhaustive search on λ. Thanks to the density of prime numbers, we are able to produce couples (λ, r) within seconds with MAGMA.

We obtain a new algorithm for pairing computation, whose loop is shorter than that of the algorithm computing the Tate pairing.

Lemma 6.1. Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$ and ϕ an endomorphism of E whose degree is b. Let P, Q be two points on the curve E. Then for any integer λ the following equality is true up to a constant:

$$f_{\lambda,\phi(P)}(\phi(Q)) = f^b_{\lambda,P}(Q)\left(\prod_{K\in \mathrm{Ker}\,\phi\backslash\{P_\infty\}} corr_{P,K}(Q)\right)^{\lambda}\left(\prod_{K\in \mathrm{Ker}\,\phi\backslash\{P_\infty\}} corr_{\lambda P,K}(Q)\right)^{-1}$$

Proof. We have

$$\begin{aligned}
\phi^*(f_{\lambda,\phi(P)}) &= \lambda \sum_{K\in\mathrm{Ker}\phi}(P+K) - \sum_{K\in\mathrm{Ker}\phi}(\lambda P + K) - (\lambda - 1)\sum_{K\in\mathrm{Ker}\phi}(K)\\
&= \lambda \sum_{K\in\mathrm{Ker}\phi}((P+K) - (K)) - \sum_{K\in\mathrm{Ker}\phi}((\lambda P + K) - (K))\\
&= \lambda \sum_{K\in\mathrm{Ker}\phi}((P) - (O)) - \sum_{K\in\mathrm{Ker}\phi}(\lambda P) - (O) + \mathrm{div}\left(\left(\prod_{K\in\mathrm{Ker}\,\phi}\frac{l_{K,P}}{v_{K+P}}\right)^{\lambda}\right)\\
&-\mathrm{div}\left(\prod_{K\in\mathrm{Ker}\,\phi}\frac{l_{K,\lambda P}}{v_{K+\lambda P}}\right) = \mathrm{div}(f_{\lambda,P}) + \mathrm{div}\left(\prod_{K\in\mathrm{Ker}\,\phi\backslash\{P_\infty\}} corr_{\lambda P,K}\right)\\
&-\mathrm{div}\left(\prod_{K\in\mathrm{Ker}\,\phi\backslash\{P_\infty\}} corr_{\lambda P,K}\right).
\end{aligned}$$

Using the fact that $\phi^*(f_{\lambda,\phi(P)}) = f_{\lambda,\phi(P)} \circ \phi$, we obtain the equality we have announced. □

In the sequel, we make use of the following relation which holds for all $m, n \in \mathbb{Z}$ and any point P on the elliptic curve

$$f_{mn,P} \quad = \quad f^{n}_{m,P} \cdot f_{n,mP}. \tag{6.9}$$

This equality can be easily checked using divisors.

Theorem 6.5. Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$, r a prime number such that $r|\#E(\mathbb{F}_q)$ and k the embedding degree with respect to r. Let ϕ be an efficiently computable separable endomorphism of E, whose characteristic equation is $X^2 + aX + b = 0$. Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be the the subgroups of order r whose elements are eigenvectors of ϕ defined over $\mathbb{F}_q$ and $\mathbb{F}_{q^k}$, respectively. Let λ be the eigenvalue of ϕ on $\mathbb{G}_1$, verifying $\lambda^2 + a\lambda + b = cr$, with $r \nmid bc$. Then the map $a_\phi(\cdot,\cdot) : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{F}^*_{q^k}/(\mathbb{F}^*_{q^k})^r$ given by

$$\begin{aligned} a_\phi(P,Q) \quad = \quad & f^{\lambda+a}_{\lambda,P}(bQ) f^{b}_{\lambda,P}(\hat{\phi}(Q)) f_{a,\lambda P}(bQ) f_{b,P}(bQ) \left(\prod_{K \in \mathrm{Ker}\phi \setminus \{P_\infty\}} corr_{P,K}(\hat{\phi}(Q)) \right)^{\lambda} \\ & \cdot \left(\prod_{K \in \mathrm{Ker}\phi \setminus \{P_\infty\}} corr_{\lambda P,K}(\hat{\phi}(Q)) \right)^{-1} corr_{\lambda^2 P, a\lambda P}(bQ) \ l_{\lambda^2 P + a\lambda P, bP}(bQ) \end{aligned}$$

is a bilinear non-degenerate pairing.

Proof. The following equality is obtained by repeatedly applying the equality at (6.9)

$$\begin{aligned} f_{\lambda^2+a\lambda+b,P} \quad = \quad & (f^{\lambda}_{\lambda,P}) \cdot (f_{\lambda,\lambda P}) \cdot (f^{a}_{\lambda,P}) \cdot (f_{a,\lambda P}) \cdot (f_{b,P}) \\ & \cdot corr_{\lambda^2 P, a\lambda P} \cdot l_{\lambda^2 P + a\lambda P, bP} \end{aligned} \tag{6.10}$$

By applying Lemma 6.1, we obtain

$$\begin{aligned} f_{\lambda,\lambda P}(bQ) \quad = \quad & f^{b}_{\lambda,P}(\hat{\phi}(Q)) \left(\prod_{K \in \mathrm{Ker}\phi \setminus \{P_\infty\}} corr_{P,K}(\hat{\phi}(Q)) \right)^{\lambda} \\ & \cdot \left(\prod_{K \in \mathrm{Ker}\phi \setminus \{P_\infty\}} corr_{\lambda P,K}(\hat{\phi}(Q)) \right)^{-1} \end{aligned}$$

By replacing this term in equation (6.10), we derive that $a_\phi(P,Q)$ is a power of $t_r(P,Q)$. Since $(bc, r) = 1$, we conclude that a_ϕ defines a non-degenerate pairing on $\mathbb{G}_1 \times \mathbb{G}_2$. □

If the value of λ is close to $\sqrt{r}$ and a and b are small, Theorem 6.5 gives an efficient algorithm to compute the Tate pairing (actually a small power of the Tate pairing). This is Algorithm 12. The complexity of the new algorithm is $O(\log ab\lambda)$.

Algorithm 12 Our algorithm for pairing computation for curves with an efficiently computable endomorphism

```
INPUT: An elliptic curve $E$, $P, Q$ points on $E$ and $\phi$ such that $\phi(P) = \lambda P$, $Q' = \hat{\phi}(Q)$.
OUTPUT: A power of the Tate pairing $T_r(P, Q)$.
 1: Let $i = [\log_2(\lambda)]$, $K \leftarrow P$, $f \leftarrow 1$, $g \leftarrow 1$
 2: while $i \geq 1$ do
 3:    Compute equation of $l$ arising in the doubling of $K$
 4:    $K \leftarrow 2K$ and $f \leftarrow f^2 l(bQ)$ and $g \leftarrow g^2 l(Q')$
 5:    if the $i$-th bit of $\lambda$ is 1 then
 6:       Compute equation of $l$ arising in the addition of $K$ and $P$
 7:       $K \leftarrow P + K$ and $f \leftarrow f l(bQ)$ and $g \leftarrow g l(Q')$
 8:    end if
 9:    Let $i \leftarrow i - 1$
10: end while
11: Compute $A \leftarrow f^{\lambda+a}$
12: Compute $B \leftarrow g^b$
13: Compute $C \leftarrow \left(\prod_{K\in\mathrm{Ker}\phi\backslash\{P_\infty\}} corr_{P,K}(Q')\right)^{\lambda} \left(\prod_{K\in\mathrm{Ker}\phi\backslash\{P_\infty\}} corr_{\lambda P,K}(Q')\right)^{-1}$
14: Compute $D \leftarrow f_{a,\lambda P}(bQ) f_{b,P}(bQ)$
15: $F \leftarrow corr_{\lambda^2 P, a\lambda P}(bQ) l_{\lambda^2 P + a\lambda P, bP}(bQ)$
16: Return $A \cdot B \cdot C \cdot D \cdot F$
```

6.6 Computational costs

Suppose we use an endomorphism ϕ whose characteristic equation is

$$\phi^2 + a\phi + b = 0,$$

with a and b small. We also neglect the cost of computing the dual of ϕ at Q, $\hat{\phi}(Q)$, because $\hat{\phi}$ can be precomputed by Vélu's formulae in Section 4.5 and is given by polynomials of small degree. Note that in some protocols Q is a fixed point, so all the precomputations on this point may be done before the computation of the pairing.

We also note that the endomorphism is defined over $\mathbb{F}_q$, because the curve E is ordinary. Moreover, the points in $\mathrm{Ker}\,\phi$ are eigenvectors for the Frobenius endomorphism. Indeed, since $\mathrm{End}(E)$ is a commutative ring, we have $\phi(\pi(K)) = \pi(\phi(K)) = O$, for all $K \in \mathrm{Ker}\,\phi$. It follows that $\pi(K) \in \mathrm{Ker}\,\phi$. Thus the points of $\mathrm{Ker}\,\phi$ are defined over an extension field of $\mathbb{F}_q$ of degree smaller than b. Furthermore, if $\mathrm{Ker}\,\phi$ is cyclic, we have

$$\left(\prod_{K\in\mathrm{Ker}\,\phi\backslash\{P_\infty\}} corr_{P,K}(\hat{\phi}(Q))\right) \in \mathbb{F}_{q^k}.$$

Consequently, given that the degree of ϕ is small, we assume that the number of operations needed to compute the correction $\prod_{K\in\mathrm{Ker}\,\phi} corr_{P,K}(\hat{\phi}(Q))$ is negligible. Since a and b are small, we also assume that the costs of the exponentiation at line 12 and that of the computation of functions at line 14 of Algorithm 12 are negligible.

Table 6.4: Our method versus the Tate pairing

bit length of r	$k = 2$		$k \geq 4$ and $D \neq 4$	
	Tate pairing	This work	Tate pairing	This work
160 bits	3040	2400	5120	4880

Since in practice we usually consider curves with even embedding degree, we present only results for these curves. We assume that the curves have an efficiently computable endomorphism and eigenvalues of size $\sqrt{r}$. In our evaluation, we only counted the number of operations performed in the doubling part of Miller's algorithm, because we suppose that λ and r have low Hamming weight (which is possible if the curve is constructed with the Cocks-Pinch method). For operations in extension fields of degree 2, we use tower fields. For example, to construct an extension field of degree 4 we have

$$\mathbb{F}_q \subset \mathbb{F}_{q^2} \subset \mathbb{F}_{q^4}.$$

With Karatsuba's method the cost of an operation in the extension field of degree 2 is three times the cost of the same operation in the base field, while with Toom-Cook a multiplication in an extension field of degree 3 costs 5 multiplications in the base field. Using the formulas in Table 6.3 the total cost of the doubling step in Algorithm 12 and of the exponentiation at line 11 is

$$(11\mathbf{s} + (1 + 2k)\mathbf{m} + 2\mathbf{M} + 2\mathbf{S}) \log \lambda + \log \lambda \mathbf{M} \quad \text{if } D \neq 3, 4.$$

Our computations showed that our method gives better performances than the Tate pairing for some families of ordinary curves with embedding degree 2, 3 and 4. Indeed, using the complexity estimations above and making the assumption that $\mathbf{s} \approx \mathbf{m}$, our algorithm is faster than the Tate pairing if and only if

$$(12 + 2k)\mathbf{m} + 5\mathbf{M} > 2((12 + k)\mathbf{m} + 2\mathbf{M}).$$

A simple computation shows that this is true if and only if $k \leq 4$. In Table 6.4, we compare the performances of our method to those of Miller's algorithm, for curves with embedding degree 2 and 4 constructed via the Cocks-Pinch method. Note that for $k = 2$, the Eta pairing algorithm (and its variants) is not faster than the Tate pairing algorithm, because $t \approx r$. We assume that for curves with embedding degree 4 the CM discriminant is not -4, because for such curves the Tate and the twisted Ate pairing have comparable costs. Note that for $D = -4$ the twisted Ate pairing computation has complexity $O(\log t)$ and is thus faster than the Tate pairing and also faster than our method if t is careffully chosen of small size.

6.7 Conclusion

In this chapter we have presented an efficient implementation of Miller's algorithm on the Weierstrass form of an elliptic curve. We have explained that by making use of twists, we reduce the costs of the pairing computation on $\mathbb{G}_1 \times \mathbb{G}_2$, when $\mathbb{G}_1$ and $\mathbb{G}_2$ are generated by eigenvectors of the Frobenius map. We have also shown that endomorphisms of small degree can be used to speed up pairing computation for curves with small embedding degree, whenever loop shortening techniques do not work.

Chapter 7

Pairings on Edwards curves

In 2007, H. Edwards found a new form for elliptic curves and showed that on this form the addition law on the elliptic curve had a surprisingly simple, symmetric form. Little later, Bernstein and Lange introduced this addition in cryptography, by proving that it provided very efficient formulae for addition and doubling on elliptic curves. Moreover, this formulae were unified, which meant that they worked for both addition and doubling. The Edwards coordinates were thus also offering protection against side-channel attacks. This provided enough motivation to implement pairing based protocols entirely in Edwards coordinates. Using isogenies, we have given the first formulae for efficient computation of pairings in Edwards coordinates [50].

In Section 7.2, we present an algorithm for pairing computation in Edwards coordinates and compare our complexities to those of algorithms computing pairings on Weierstrass curves. Section 7.3 briefly presents another recent algorithm computing pairings on Edwards curves. Section 7.4 gives an algorithm which performs efficient scalar multiplication on Edwards curves for which the addition law is not defined for all points.

7.1 Edwards curves

H. Edwards gave a new normal form for elliptic curves defined over algebraic number fields. More precisely, he showed in [32] that every elliptic curve E defined over an algebraic number field is birationally equivalent over some extension of that field to a curve given by the equation

$$x^2 + y^2 = c^2(1 + x^2y^2). \tag{7.1}$$

Bernstein and Lange stated a similar result in the context of finite fields [12]. The following theorem was given in [11].

Theorem 7.1. Fix a finite field $\mathbb{F}_q$ with char$(\mathbb{F}_q) \neq 2$ and let E be an elliptic curve over $\mathbb{F}_q$. E is birationally equivalent over $\mathbb{F}_q$ to a curve $E_d : x^2 + y^2 = 1 + dx^2y^2$ if and only if the group $E(\mathbb{F}_q)$ has an element of order 4.

In this dissertation, we call the curve E_d given by $x^2 + y^2 = 1 + dx^2y^2$ an Edwards curve. In this chapter, we denote by d the parameter giving the equation of an Edwards curve.

Suppose now that E is an elliptic curve given by a Weierstrass equation, having a point of order 4, that we denote by $P = (u_4, v_4)$ of E. We may assume, without loss of generality, that $(0, 0)$ is a point on the curve, so the Weierstrass equation of E is

$$E : y^2 = x^3 + a_2x^2 + a_4x.$$

We may also assume, without restraining the generality, that $2P = (0, 0)$. This means that the tangent line to E at P passes through $(0, 0)$. This gives $3u_4^3 + 2a_2u_4^2 + a_4u_4 = 2v_4^2$. Further, we have $2u_4^3 + 2a_2u_4^2 + 2a_4u_4 = 2v_4^2$. Subtracting one equation from another we get $u_4^3 = u_4a_4$, hence $u_4^2 = a_4$. Moreover, $a_2 = (v_4^2 - u_4^3 - a_4u_4)/u_4^2 = v_4^2/u_4^2 - 2u_4$. We define $d = 1 - 4u_4^3/v_4^2$ and consider the corresponding Edwards curve E_d. We obtain the rational map

$$\begin{aligned} \psi : E &\rightarrow E_d \\ (u, v) &\mapsto (x, y) = (v_4u/u_4v, (u - u_4)/(u + u_4)). \end{aligned} \tag{7.2}$$

This map has a finite number of exceptional cases, i.e. points where $u_4v = 0$ or $u = -u_4$. Its inverse is

$$\psi^{-1} : E_d \rightarrow E \tag{7.3}$$

$$(x, y) \mapsto (u_4(1 + y)/(1 - y), v_4(1 + y)/(1 - y)x). \tag{7.4}$$

This map has a finite number of exceptional cases $y = 1$ or $x = 0$. Hence ψ is a birational equivalence between E and E_d.

Edwards showed that on an Edwards curve, the addition law has the following symmetric form

$$(x_1, y_1), (x_2, y_2) \rightarrow \left(\frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}\right). \tag{7.5}$$

The neutral element of this addition law is $O = (0, 1)$. For every point $P = (x, y)$ the inverse element is $-P = (-x, y)$. The curve has a 4-torsion subgroup defined over $\mathbb{F}_q$. We note $T_2 = (0, -1)$ the point of order 2 and $T_4 = (1, 0)$, $-T_4 = (-1, 0)$ the two points of order 4. There are two singular points on the Edwards curve: $\Omega_1 = [0, 1, 0]$ and $\Omega_2 = [1, 0, 0]$. Resolving them produces four points defined over $\mathbb{F}_q(\sqrt{d})$ on the desingularization of the curve (the reader is referred to [45] for a definition of desingularization).

In [12], Bernstein and Lange showed that the Edwards addition law is *complete* when d is not a square. This means it is defined for all pairs of input points on the Edwards curve with no exceptions for doublings, neutral element etc. Moreover, this addition law is the same as the one induced by the birational map described above, i.e. $P_1 + P_2 = \psi^{-1}(\psi(P_1) + \psi(P_2))$, where the first + stands for the addition law on the Edwards curve E_d and the last + stands for the standard addition law on the curve E.

Edwards curves in cryptography

Bernstein and Lange [12] showed that by using projective coordinates to represent points on the Edwards curve, they obtained formulae faster than all addition and doubling formulae known at that time. A point $[X, Y, Z]$ in projective Edwards coordinates corresponds to the affine point

Table 7.1: Performance evaluation: Edwards versus Jacobian

	Edwards coordinates	inverted Edwards coordinates	Jacobian coordinates
addition	10**m**+1**s**+1**d**	9**m**+1**s**+1**d**	11**m**+5**s**
doubling	3**m**+4**s**	3**m**+4**s**+1**d**	1**m**+8**s**+1**a** or 3**m**+5**s** for $a = -3$
mixed addition	9**m**+1**s**+1**d**	8**m**+1**s**+1**d**	7**m**+4**s**

$(X/Z, Y/Z)$ on the curve $x^2+y^2 = 1+dx^2y^2$. Table 7.1 gives a cost comparison between operations of addition, doubling and mixed addition on the Edwards curve and on the Weierstrass curve in Jacobian coordinates. We assume that the Weierstrass curve is given by an equation $y^2 = x^3+ax+b$, with $a, b \in \mathbb{F}_q$. For Edwards curves, we present costs in projective Edwards coordinates and in *inverted Edwards coordinates* [13]. In inverted Edwards coordinates, a point $[X, Y, Z]$ stands for $(Z/X, Z/Y)$ on the affine Edwards curve. We denote by **m** the cost of a field multiplication, by **s** the cost of a field squaring in $\mathbb{F}_q$ and by **a** and **d** the costs of multiplication by the constants a and d, respectively. Results are taken from [10].

Moreover the addition formulae at (7.5) are unified formulae, i.e. they work for both addition and doubling, offering protection against side-channel attacks (see also [12]).

7.2 Pairing computation in Edwards coordinates

Given that addition on the elliptic curve was faster on Edwards curves than on curves in Weierstrass form, it is natural that Edwards curves were proposed for pairing based cryptography. Examples of pairing friendly Edwards curves were given in [26] and [3].

Example 7.1. The following example is given in [26]. Consider $E : y^2 = x^3 + x$ over $\mathbb{F}_q$, with $q \equiv 3 \bmod 4$. This curve is supersingular and its corresponding Edwards form is $x^2+y^2 = 1-(xy)^2$, hence $d = -1$. One may choose for instance $q = 2^{520} + 2^{363} - 2^{360} - 1$, $r = 2^{160} + 2^3 - 1$ or $q = 2^{1582} + 2^{1551} - 2^{1326} - 1, r = 2^{256} + 2^{225} - 1$. These curves have embedding degree 2.

Example 7.2. This example was given by Arène et al. [3] and is based on the construction from [40]. We consider the Edwards curve E_d defined over $\mathbb{F}_q$, with q and d given by:

$$\begin{aligned} q &= 2051613663768129606093583432875887398415301962227490187508801 \\ d &= 1100661309421493056836745159318889208210931380459417578976626. \end{aligned}$$

This is an elliptic curve with discriminant -7230 and embedding degree 6. It has $\rho \approx 1.22$.

However, computing pairings on Edwards curves efficiently was proven to be a complex problem. The main difficulty when trying to express Miller's algorithm in Edwards coordinates was that it was hard to find the equations of rational functions that needed to be evaluated at each addition step. On a curve in Weierstrass form, these equations correspond to straight lines. For curves in Edwards form matters are more complex. The natural approach was to use the map ψ and compute the equations of these functions as pullbacks of lines on a Weierstrass curve. This gave complicated equations, which resulted in a highly inefficient algorithm. However, Das and Sarkar [26] managed to simplify these equations in the case of supersingular curves given in example 7.1 and obtained a fast algorithm. In this section we present our approach to pairing computation in Edwards curves, which uses an isogeny of small degree.

7.2.1 An isogeny of degree 4

Let E_d denote an Edwards curve defined over some finite field $\mathbb{F}_q$ of odd characteristic. Let us take a look at the action of the 4-torsion subgroup defined over $\mathbb{F}_q$ on a fixed point on the Edwards curve $R = (x, y)$ with $xy \neq 0$. A simple computation shows that $R + T_4 = (y, -x)$, $R + T_2 = (-x, -y)$ and $R - T_4 = (-y, x)$. We notice then that by letting $p = (xy)^2$ and $s = x/y - y/x$, the pair (p, s) characterizes the point P up to an addition with a 4-torsion point. This leads us to consider the following morphism from the Edwards curve to a curve given by the equation $E_{s,p} : s^2 p = (1 + dp)^2 - 4p$

$$\begin{aligned} \phi : E_d &\rightarrow E_{s,p} \\ (x, y) &\rightarrow ((xy)^2, \frac{x}{y} - \frac{y}{x}). \end{aligned} \tag{7.6}$$

We will study the arithmetic of the curve $E_{s,p}$, our objective being to establish Miller's equation on this curve. By taking the pullback of this equation on the Edwards curve, we derive Miller's equation on the Edwards curve. This yields all the tools needed to apply Miller's algorithm on the Edwards curve.

The equation of $E_{s,p}$ in homogeneous coordinates $(\overline{P}, \overline{S}, \overline{Z})$ is given by $\overline{S}^2\overline{P} = (\overline{Z} + d\overline{P})^2\overline{Z} - 4\overline{P}\overline{Z}^2$. If we dehomogenize this equation by setting P to 1, we get the Weierstrass equation of an elliptic curve

$$s^2 = z^3 + (2d - 4)z^2 + d^2 z. \tag{7.7}$$

We denote by $O_{s,p} = [0, 1, 0]$ the point at infinity and $T_{2,s,p} = [1, 0, 0]$ which is a two torsion point on the curve $E_{s,p}$. The following definition is simply another way to write the addition law on an elliptic curve in (p, s) coordinates.

Definition 7.1. Let $S, T \in E_{s,p}$, L the line connecting S and T (tangent line to $E_{s,p}$ if $S = T$), and R the third point of intersection of L with E. Let L' be the vertical line through R (of equation $p = p_R$). Then $S + T$ is the point such that L' intersects $E_{s,p}$ at R and $S + T$ (the point symmetric to R with respect to the p-axis).

Figure 7.2.1 illustrates this definition.
Note that we can extend the map ϕ to the 4-torsion points by $\phi(O) = \phi(T_2) = \phi(T_4) = \phi(-T_4) = O_{s,p}$.

Theorem 7.2. Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be two points on the Edwards curve and $P + Q$ their sum. Then $\phi(P + Q)$ is the sum of $\phi(P)$ and $\phi(Q)$ in the addition law of definition 7.1.

Proof. Consider $\psi : E \rightarrow E_d$ the map defined in equation (7.2). By using Theorem 2.1 one can easily see that $\phi \circ \psi$ is a morphism from E to the elliptic curve $E_{s,p}$. As $\phi \circ \psi(O') = O_{s,p}$ (where O' is the point at infinity of E), we deduce that $\phi \circ \psi$ is an isogeny. Moreover, the Edwards addition law on E_d is the same as the addition law induced by ψ. It follows that the addition law induced by ϕ is the same as the standard addition law on the elliptic curve, so it corresponds to the addition law described at definition 7.1. □

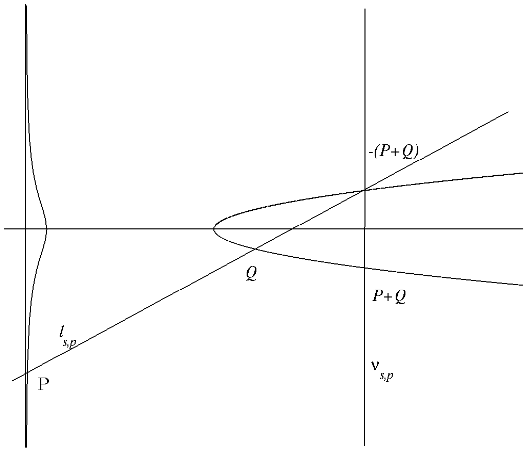


Figure 7.1: Addition law on the $E_{s,p}$ curve

In the sequel we need to compute the pullback of certain functions on the curve $E_{s,p}$. Before that, we compute the degree of ϕ.

Proposition 7.1. The map $\phi : E_d \to E_{s,p}$ is separable of degree 4.

Proof. Let $P = (x, y)$ be a point on the Edwards curve. The doubling formula gives

$$2P \;=\; \left(\frac{2xy}{1+d(xy)^2}, \frac{y^2-x^2}{1-d(xy)^2}\right) = \left(\frac{2xy}{x^2+y^2}, \frac{y^2-x^2}{2-(x^2+y^2)}\right).$$

If $xy \neq 0$ then by letting $p = (xy)^2$ and $s = x/y - y/x$, we can write

$$4P \;=\; \left(\frac{4ps(1-d^2p^2)}{(1-d^2p^2)^2-4dp^2s^2}, \frac{4p(1+dp)^2-ps^2}{(1-d^2p^2)^2+4dp^2s^2}\right).$$

This means that by defining

$$\begin{array}{rccl} \theta: & E_{s,p} & \to & E \\ & (p,s) & \to & \left(\dfrac{4ps(1-d^2p^2)}{(1-d^2p^2)^2-4dp^2s^2}, \dfrac{4p(1+dp)^2-ps^2}{(1-d^2p^2)^2+4dp^2s^2}\right), \end{array}$$

we get a rational map ψ such that $\phi \circ \theta = [4]$ on E. It follows that $\deg\phi$ divides 16. As the inseparable degree $\deg_i \phi$ is a power of the characteristic of $\mathbb{F}_q$, we deduce that ϕ is a separable map (we have supposed that $\mathrm{char}(\mathbb{F}_q) \neq 2$). By putting $\phi(P) = Q$ we easily get $\phi^{-1}(Q) = \{P, P + T_2, P + T_4, P - T_4\}$. We conclude that $\deg\phi = 4$. □

7.2.2 Miller's algorithm on the Edwards curve

Let P be an r-torsion point on the Edwards curve. We consider slightly modified functions $f_{i,P}^{(4)}$:

$$\begin{aligned} f_{i,P}^{(4)} &= i((P) + (P + T_4) + (P + T_2) + (P - T_4)) - ((iP) + (iP + T_4) \\ &\quad +(iP + T_2) + (iP - T_4)) - (i - 1)((O) + (T_4) + (T_2) + (-T_4)). \end{aligned}$$

Then $f_{r,P}^{(4)} = r((P) + (P + T_4) + (P + T_2) + (P - T_4)) - r((O) + (T_4) + (T_2) + (-T_4))$, which means that we can compute the Tate pairing up to a 4-th power:

$$T_r(P, Q)^4 = f_{r,P}^{(4)}(Q)^{\frac{q^k-1}{r}}.$$

We also get the following Miller equation

$$f_{i+j,P}^{(4)} = f_{i,P}^{(4)} f_{j,P}^{(4)} \frac{l}{v}, \tag{7.8}$$

where l/v is the function of divisor

$$\begin{aligned} \operatorname{div}(l/v) &= ((iP) + (iP + T_4) + (iP + T_2) + (iP - T_4)) \\ &\quad +((jP) + (jP + T_4) + (jP + T_2) + (jP - T_4)) \\ &\quad -(((i + j)P) + ((i + j)P + T_4) + ((i + j)P + T_2) + ((i + j)P - T_4))) \\ &\quad -((O) + (T_4) + (T_2) + (-T_4)). \end{aligned}$$

Let $P^{'} = \phi(P)$ and let $l_{s,p}$ and $v_{s,p}$ be functions on the $E_{s,p}$ curve such that div $(l_{s,p}) = (iP^{'}) + (jP^{'}) + (-(i + j)P^{'}) - 2(T_{2,s,p}) - (O_{s,p})$ and div $(v_{s,p}) = ((i + j)P^{'}) + (-(i + j)P^{'}) - 2(T_{2,s,p})$.

We observe that we have $l/v = \phi^*(l_{s,p}/v_{s,p})$ up to constants in $\mathbb{F}_q$. It is easy to find the equations of lines $l_{s,p}$ and $v_{s,p}$ that appear in the definition of the sum $iP^{'} + jP^{'}$, namely $l_{s,p}$ is the line connecting $iP^{'}$ and $jP^{'}$, and $v_{s,p}$ is the vertical line through $(i + j)P^{'}$. As we will see in the next section, we can compute their pullback via the map ϕ without any significant computational cost.

7.2.3 Pairing computation in Edwards coordinates

Just like in Chapter 6, we denote by $\mathbf{m}, \mathbf{s}$ the costs of multiplication and squaring in the field $\mathbb{F}_q$ and by $\mathbf{M}, \mathbf{S}$ the costs of these operations in the extension field $\mathbb{F}_{q^k}$. We take a look into the details of the computation of a Miller iteration. We first detail the computation for the doubling step, and then the one for the mixed addition step.

Doubling step

We note $K = [X_1, Y_1, Z_1]$. Following [12], the doubling formulas for $2K = [X_3, Y_3, Z_3]$ are:

$$\begin{aligned} X_3 &= 2X_1Y_1(2Z_1^2 - (X_1^2 + Y_1^2)), \\ Y_3 &= (X_1^2 + Y_1^2)(Y_1^2 - X_1^2), \\ Z_3 &= (X_1^2 + Y_1^2)(2Z_1^2 - (X_1^2 + Y_1^2)). \end{aligned}$$

On the curve $E_{s,p}$, let $l_{s,p}$ be the tangent line to the curve at $\phi(K) = (p_1, s_1)$ and $v_{s,p}$ the vertical line passing through $\phi(2K) = (p_3, s_3)$. These lines have the following equations:

$$\begin{aligned} l_{s,p}(s,p) &= 2p_1^2 s_1(s - s_1) - p_1(2d(1 + dp_1) - (s_1^2 + 4))(p - p_1), \\ v_{s,p}(s,p) &= p - p_3. \end{aligned}$$

Using the equation of the curve $E_{s,p}$ and then the expressions for s and p we get

$$\begin{aligned} l_{s,p} &= 2p_1^2 s_1(s - s_1) - (2d(1 + dp_1)p_1 - (1 + dp_1)^2)(p - p_1) \\ &= 2p_1^2 s_1(s - s_1) + (1 - dp_1)(1 + dp_1)(p - p_1) \\ &= (x_1y_1)^2(x_1^2 - y_1^2)(2x_1y_1(x/y - y/x) - 2(x_1^2 - y_1^2)) \\ &+(2 - x_1^2 - y_1^2)(x_1^2 + y_1^2)((xy)^2 - (x_1y_1)^2). \end{aligned}$$

Consequently, making use of the Edwards curve equation, we get the following equations of normalized functions l and v defined at equation (7.8)

$$\begin{aligned} l(x,y) = l_1(x,y)/l_2 &= ((X_1^2 + Y_1^2 - Z_1^2)(X_1^2 - Y_1^2)(2X_1Y_1(x/y - y/x) \\ &\quad -2(X_1^2 - Y_1^2)) + Z_3(dZ_1^2(xy)^2 - (X_1^2 + Y_1^2 - Z_1^2)))/ \\ &\quad (2X_1Y_1(X_1^2 + Y_1^2 - Z_1^2)(X_1^2 - Y_1^2)), \\ v(x,y) = v_1(x,y)/v_2 &= (dZ_3^2(xy)^2 - (X_3^2 + Y_3^2 - Z_3^2))/(X_3^2 + Y_3^2 - Z_3^2). \end{aligned}$$

We establish the following equation

$$v_2/l_2 = 4Z_1^2(Y_1^2 - X_1^2)/2X_1Y_1.$$

Therefore we may write the doubling part given in equation 6.1 as follows

$$\begin{aligned} K &\leftarrow 2K, \\ f_1^{(4)} &\leftarrow (f_1^{(4)})^2 l_1(Q)4I, \\ f_2^{(4)} &\leftarrow (f_2^{(4)})^2 l_2(Q)C. \end{aligned}$$

We represent the point K as $K = [X_1, Y_1, Z_1, U_1, V_1, W_1, T_1]$, where $[X_1, Y_1, Z_1]$ are the projective coordinates of the point K on the Edwards curve, $U_1 = X_1^2$, $V_1 = Y_1^2$, $W_1 = Z_1^2$ and $T_1 = dZ_1^2(xy)^2 - (X_1^2 + Y_1^2 - Z_1^2)$. The operation count is presented in Table 7.2; the doubling part costs $8\mathbf{s} + 11\mathbf{m} + 1\mathbf{d}$.

Mixed addition

Next, we take a look at the mixed addition step in a Miller iteration. We count the number of operations that must be executed when adding $K = [X_1, Y_1, Z_1]$ and $P = [X_0, Y_0, 1]$. The result is $K + P = (X_3, Y_3, Z_3)$ with

$$\begin{aligned} X_3 &= Z_1(X_0Y_1 + Y_0X_1)(Z_1^2 - dX_0X_1Y_0Y_1), \\ Y_3 &= Z_1(Y_0Y_1 - X_0X_1)(Z_1^2 + dX_0X_1Y_0Y_1), \\ Z_3 &= (Z_1^2 + dX_0X_1Y_0Y_1)(Z_1^2 - dX_0X_1Y_0Y_1). \end{aligned}$$

Table 7.2: Operations of the doubling part of the Miller operation

$C \leftarrow (X_1 + Y_1)^2,\ D \leftarrow U_1 + V_1,$	(1**s**)
$E \leftarrow C - D,\ F \leftarrow V_1 - U_1,\ H \leftarrow 2W_1 - D,$	
$X_3 \leftarrow E \cdot H,\ Y_3 \leftarrow D \cdot F,\ Z_3 \leftarrow D \cdot H,\ U_3 \leftarrow X_3^2,\ V_3 \leftarrow Y_3^2,\ W_3 \leftarrow Z_3^2,$	(3**s**+3**m**)
$I \leftarrow W_1 \cdot F,\ J \leftarrow I - Y_3,\ K \leftarrow E \cdot (x/y - y/x),\ L \leftarrow J \cdot (K - 2F),$	(3**m**)
$T_3 \leftarrow dW_3 \cdot (xy)^2 - (U_1 + V_1 - W_1),\ P \leftarrow 2Z_3 \cdot T_3,\ l_1 \leftarrow L - P,$	(2**m**)
$f_1^{(4)} \leftarrow (f^{(4)})^2 \cdot l_1 \cdot (4I)$	(2**m**+1**s**)
$f_2^{(4)} \leftarrow (f^{(4)})^2 \cdot l_2 \cdot C$	(2**m**+1**s**)

On the curve $E_{s,p}$, we consider $l_{s,p}$ the straight line passing through $\phi(K) = (p_1, s_1)$ and $\phi(P) = (p_0, s_0)$ and $v_{s,p}$ the vertical line passing through the point $\phi(K) + \phi(P) = (p_3, s_3)$. We get

$$\begin{aligned} l_{s,p}(s,p) &= (p_0 - p_1)(s - s_1) - (s_0 - s_1)(p - p_1), \\ v_{s,p}(s,p) &= p - p_3. \end{aligned}$$

Replacing p_0, p_1, s_0, s_1 by their expressions and multiplying the equation above by $(x_1 y_1)$ we have

$$\begin{aligned} l_{s,p}(s,p) &= ((x_1y_1)^2 - (x_0y_0)^2)(x_1y_1(x/y - y/x) - (x_1^2 - y_1^2)) \\ &\quad -(x_1^2 - y_1^2 - x_1y_1(x_0^2 - y_0^2))((xy)^2 - (x_1y_1)^2). \end{aligned}$$

We obtain normalized functions l and v with equations

$$\begin{aligned} l(x,y) = l_1(x,y)/l_2 &= ((X_1^2 + Y_1^2 - Z_1^2 - dZ_1^2(X_0Y_0)^2)\left(X_1Y_1(\frac{x}{y} - \frac{y}{x}) - (X_1^2 - Y_1^2)\right) \\ &\quad -\left(X_1^2 - Y_1^2 - X_1Y_1\left(\frac{X_0}{Y_0} - \frac{Y_0}{X_0}\right)\right) \\ &\quad \cdot(dZ_1^2(xy)^2 - (X_1^2 + Y_1^2 - Z_1^2))) \\ &\quad /(X_1Y_1(X_1^2 + Y_1^2 - Z_1^2 - dZ_1^2(X_0Y_0)^2)); \\ v(x,y) = v_1(x,y)/v_2 &= (dZ_3^2(xy)^2 - (X_3^2 + Y_3^2 - Z_3^2))/(X_3^2 + Y_3^2 - Z_3^2). \end{aligned}$$

Therefore we may write the mixed addition part as follows

$$\begin{aligned} K &\leftarrow K + P, \\ f_1^{(4)} &\leftarrow f_1^{(4)} l_1(Q) v_2(Q), \\ f_2^{(4)} &\leftarrow f_2^{(4)} l_2(Q) v_1(Q). \end{aligned}$$

The steps of the computation are detailed in Table 7.3. We count $4\mathbf{s} + 19\mathbf{m} + 1\mathbf{d}$. In the beginning, we precompute expressions such as $2X_0Y_0$, dX_0Y_0, $(X_0Y_0)^2$ and $\frac{X_0}{Y_0} - \frac{Y_0}{X_0}$. In Table 7.4 we present a comparison between costs of pairings computed in Edwards coordinates and those of pairings computed in Jacobian coordinates.

Table 7.3: Operations of the mixed addition step of a Miller operation

$C \leftarrow (X_1 + Y_1)^2 - U_1 - V_1, D \leftarrow C \cdot (dX_0Y_0)$	(1**m**+1**s**)
$E \leftarrow 2(X_1 + X_0) \cdot (Y_0 + Y_1) - C - 2X_0Y_0,$	(1**m**)
$F \leftarrow 2(X_1 + Y_0) \cdot (Y_1 - X_0) - C + 2X_0Y_0$	(1**m**)
$X_3 \leftarrow Z_1 \cdot E \cdot (2W_1 + D), Y_3 \leftarrow Z_1 \cdot F \cdot (2W_1 - D), Z_3 \leftarrow (2W_1 - D) \cdot (2W_1 + D)$	(5**m**)
$U_3 \leftarrow X_3^2,\ V_3 \leftarrow Y_3^2,\ W_3 \leftarrow Z_3^2,\ H \leftarrow dW_1 \cdot (X_0Y_0)^2$	(1**m**+3**s**)
$J \leftarrow C \cdot (x/y - y/x),\ K \leftarrow (U_1 + V_1 - W_1 - H) \cdot (J - 2(U_1 - V_1))$	(2**m**)
$L \leftarrow C \cdot (X_0/Y_0 - Y_0/X_0),\ M \leftarrow T_1 \cdot (2U_1 - 2V_1 - L),$	(2**m**)
$T_3 \leftarrow dW_3 \cdot (xy)^2 - (U_3 + V_3 - T_3),\ l_1 \leftarrow K - M,$	(1**m**)
$l_2 \leftarrow C \cdot (U_1 + V_1 - W_1 - H),$	(1**m**)
$f_1^{(4)} \leftarrow f_1^{(4)} \cdot l_1 \cdot (U_3 + V_3 - W_3),$	(2**m**)
$f_2^{(4)} \leftarrow f_2^{(4)} \cdot l_2 \cdot T_3.$	(2**m**)

Table 7.4: Comparison of costs for the Miller operation in the general case

	doubling	mixed addition
Edwards coordinates	11**s** + 8**m** + 1**d**	4**s** + 19**m** + 1**d**
Jacobian coordinates	12**s** + 8**m** + 1**a**	6**s** + 11**m**

The case of even embedding degree

For efficiency reasons, we take subgroups $\mathbb{G}_1$ and $\mathbb{G}_2$ on the Weierstrass equivalent form, as explained in Section 6.2.1

$$\begin{aligned} \mathbb{G}_1 &= E[r] \cap \mathrm{Ker}(\pi - [1]) \\ \mathbb{G}_2 &= E[r] \cap \mathrm{Ker}(\pi - [q]). \end{aligned}$$

We recall that the curve $E_d : x^2 + y^2 = 1 + dx^2y^2$ is birationally equivalent to the curve E, via the rational map $\psi : E \to E_d$. We choose $P^{'} \in \mathbb{G}_1$ and $Q^{'} \in \mathbb{G}_2$ on the E_d curve as explained above and then take $P = \psi(P^{'})$ and $Q = \psi(Q^{'})$. It follows that the coordinates of elements of $\langle P \rangle$ are in $\mathbb{F}_q$. The subgroup $\langle Q \rangle \in \mathbb{F}_{q^k}$ is such that its elements have y-coordinates in the quadratic subextension $\mathbb{F}_{q^{k/2}}$ and x-coordinates that can be written as products of elements of $\mathbb{F}_{q^{k/2}}$ with $\sqrt{\beta}$, for some element β of $\mathbb{F}_{q^{k/2}}$.

Doubling step

We show that the computational cost of the doubling part in Miller's algorithm is significantly lower than in the general case because we can ignore terms that lie in a proper subfield of $\mathbb{F}_{q^k}$. These terms will become 1 after the final exponentiation. We can ignore l_2 and v_2 because they depend only on the coordinates of P, which lie in $\mathbb{F}_q$. Since $(xy)^2 \in \mathbb{F}_{q^{k/2}}$ and hence $v_1(Q) \in \mathbb{F}_{q^{k/2}}$, it follows that we can also ignore $v_1(Q)$. Hence the function evaluation step in the doubling part of Miller's algorithm becomes

$$f_1^{(4)} \leftarrow (f_1^{(4)})^2 l_1(Q). \tag{7.9}$$

Note that multiplications by $(xy)^2$ and $x/y - y/x$ cost $(k/2)\mathbf{m}$ each ($x/y - y/x$ is the product of some element in $\mathbb{F}_{q^{k/2}}$ with $\sqrt{\beta}$). Also note that computing $x/y - y/x$ once at the beginning costs one inversion in $\mathbb{F}_{q^{k/2}}$. In some protocols Q is a fixed point, so we can precompute $x/y - y/x$.
If $k = 2$, we actually have $(xy)^2 \in \mathbb{F}_q$ and we compute l_1 as

$$\begin{aligned} l_1(x,y) \quad = \quad & ((X_1^2 + Y_1^2 - Z_1^2)(X_1^2 - Y_1^2)) \cdot 2X_1Y_1(x/y - y/x) - ((X_1^2 + Y_1^2 - Z_1^2) \\ & \cdot(X_1^2 - Y_1^2)) \cdot 2(X_1^2 - Y_1^2) - Z_3 \cdot (dZ_1^2 \cdot (xy)^2 - (X_1^2 + Y_1^2 - Z_1^2)), \end{aligned}$$

For $k > 2$ some operations are done in $\mathbb{F}_{q^k}$ and others in $\mathbb{F}_q$, hence we compute l_1 as

$$\begin{aligned} l_1(x,y) \quad = \quad & ((X_1^2 + Y_1^2 - Z_1^2)(X_1^2 - Y_1^2)) \cdot 2X_1Y_1(x/y - y/x) - ((X_1^2 + Y_1^2 - Z_1^2) \\ & \cdot(X_1^2 - Y_1^2)) \cdot 2(X_1^2 - Y_1^2) - Z_3 \cdot dZ_1^2 \cdot (xy)^2 + Z_3 \cdot (X_1^2 + Y_1^2 - Z_1^2), \end{aligned}$$

Computations do not differ much from those in Table 7.2 and we do not detail them. Results are summarized in Table 7.5.

Table 7.5: Comparison of costs for the doubling step of the Miller operation in the case of k even

	$k = 2$	$k \geq 4$
Jacobian coordinates	$10\mathbf{s} + 3\mathbf{m} + 1\mathbf{a} + \mathbf{S} + \mathbf{M}$	$11\mathbf{s} + (k+1)\mathbf{m} + 1\mathbf{a} + \mathbf{S} + \mathbf{M}$
Das/Sarkar Edwards coordinates (supersingular curves)	$6\mathbf{s} + 9\mathbf{m} + \mathbf{S} + \mathbf{M}$	-
Das/Sarkar Edwards inverted coordinates (supersingular curves)	$6\mathbf{s} + 9\mathbf{m} + \mathbf{S} + \mathbf{M}$	-
Edwards coordinates	$4\mathbf{s} + 9\mathbf{m} + 1\mathbf{d} + \mathbf{S} + \mathbf{M}$	$4\mathbf{s} + (k+8)\mathbf{m} + 1\mathbf{d} + \mathbf{S} + \mathbf{M}$

Mixed addition

Following a similar technique as the one for the doubling case, we obtain the mixed addition step for even k

$$f_1^{(4)} \leftarrow (f_1^{(4)})^2 l_1(Q). \tag{7.10}$$

The detailed computations are similar to those in Table 7.3. Since computing $\frac{X_0}{Y_0} - \frac{Y_0}{X_0}$ costs one inversion in $\mathbb{F}_q$, in some cases it will be less expensive to work with $l_1^{'} = (X_0Y_0)l_1$ instead of l_1. For protocols in which Q is a fixed point, we may precompute $\frac{x}{y} - \frac{y}{x}$. This would give an inversion free algorithm. Results and performance comparison are summarized Table 7.6.

Comparison

By looking at tables 7.5 and 7.6, one can see that in the case of curves with even embedding degree the cost of an implementation of Miller's algorithm in Edwards coordinates will be slightly more expensive than an implementation in Jacobian coordinates. We also checked performances of our method in inverted Edwards coordinates, but we did not obtain better results. We underline the idea that, independently of the representation of curves and points chosen in an implementation

Table 7.6: Comparison of costs for the mixed addition step of the Miller operation in the case of k even

	$k = 2$	$k \geq 4$
Jacobian coordinates	$3\mathbf{s} + 11\mathbf{m} + \mathbf{M}$	$3\mathbf{s} + (k + 9)\mathbf{m} + 1\mathbf{M}$
Das/Sarkar Edwards coordinates (supersingular curves)	$1\mathbf{s} + 18\mathbf{m} + \mathbf{M}$	-
Das/Sarkar Edwards inverted coordinates (supersingular curves)	$1\mathbf{s} + 17\mathbf{m} + \mathbf{M}$	-
Edwards coordinates	$4\mathbf{s} + 15\mathbf{m} + 1\mathbf{d} + \mathbf{M}$	$4\mathbf{s} + (k + 14)\mathbf{m} + 1\mathbf{d} + 1\mathbf{M}$

of Miller's algorithm, it would be impossible to avoid the expensive computation of updates in the Miller loop. These cost $1\mathbf{M} + 1\mathbf{S}$ for the doubling step (equation (7.9)) and $1\mathbf{M}$ for the mixed addition (equation (7.10)). Significant speed up can be obtained by using curves with parameter r with low Hamming weight. This will avoid performing the mixed addition step. In such cases, our proposal for an implementation in Edwards coordinates has performances comparable to those of an implementation in Jacobian coordinates, if $\mathbf{s}/\mathbf{m}$ is close to 1.

It is clear that when Edwards coordinates are preferred for the implementation of a protocol for certain reasons (scalar multiplication is faster, resistant to side channel attacks), a solution would be to switch to Jacobian coordinates and to compute the pairing on the Weierstrass form. Even though pairing implementation is faster in Jacobian coordinates, this approach will cost at least one field inversion. Consequently, on restricted devices, it is preferable to use our approach and avoid implementing inversions.

7.3 A recent approach to pairing computation in Edwards coordinates

In [3], Aréne et al. provide a geometric interpretation for the addition law on Edwards curves (actually the original contribution is given on twisted Edwards curves, but these are beyond the scope of this dissertation). Let P_1 and P_2 be two points on the Edwards curve E_d. Define $P_3 = P_1 + P_2$ the sum of P_1 and P_2. Let C be the conic passing through Ω_1, Ω_2, T_2, P_1 and P_2. The equation of C is of the form:

$$C : c_{Z^2}(Z^2 + YZ) + c_{XY}XY + c_{XZ}XZ = 0,$$

where c_{Z^2}, c_{XY} and c_{XZ} are elements of $\mathbb{F}_q$. We also denote by l_1 the vertical line through P_3 and by l_2 the vertical line through O. The equations of these lines are

$$\begin{aligned} l_1 : Z_3Y - Y_3Z &= 0 \\ l_2 : X &= 0. \end{aligned}$$

where $P_3 = [X_3, Y_3, Z_3]$. Arène et al. established the following equality on divisors

$$\mathrm{div}\left(\frac{C}{l_1 l_2}\right) = (P_1) + (P_2) - (P_3) - (O).$$

Table 7.7: Comparison of costs for the mixed addition step of the Miller operation in the case of even k

	doubling	mixed addition
$\mathcal{E}$ [50]	$4\mathbf{s} + (8 + k)\mathbf{m} + 1\mathbf{d} + 1\mathbf{S} + 1\mathbf{M}$	$4\mathbf{s} + (k + 14)\mathbf{m} + 1\mathbf{d} + 1\mathbf{M}$
$\mathcal{E}$ [3]	$5\mathbf{s} + 6\mathbf{m} + 1\mathbf{S} + 1\mathbf{M}$	$(12 + k)\mathbf{m} + 1\mathbf{M}$
$\mathcal{J}$ [50] [3]	$11\mathbf{s} + (1 + k)\mathbf{m} + 1\mathbf{a} + 1\mathbf{S} + 1\mathbf{M}$	6**s**+(6+k)**m**+1**M**
$\mathcal{J}$,$y^2 = x^3 + b$ $e = 2, 6$ [23]	(2k/e+2)**m**+7**s**+1**a**+1**M**+1**S**	(2k/e+9)**m**+2**s**+1**M**
$\mathcal{J}, y^2 = x^3 + ax$ $e = 2, 4$ [23]	(2k/e+2)**m**+8**s**+1**a**+ 1**M**+1**S**	(2k/e+12)**m**+4**s**+1**M**

This gives the Miller equation on the Edwards curve and, consequently, an efficient algorithm for pairing computation. We present in Table 7.7 the cost of their algorithm, in terms of the number of operation in the doubling and the mixed addition steps of the Miller loop, in the case of curves with even embedding degree. The case $k = 1$ is not evaluated in their paper.

To sum up, the Algorithm in [3] for pairing computation in Edwards coordinates is faster than then the method described in Section 7.2.3. However, if $\mathbf{s} = 0.8\mathbf{m}$, a simple computation shows that pairing computation is still fastest in Jacobian coordinates. Otherwise, when $\mathbf{s}/\mathbf{m}$ is close to 1, Edwards coordinates are to be preferred. Moreover, in the case of curves allowing twists of degree 4 or 6, it is not known whether we can represent the points in $\mathbb{G}_2$ as points over $\mathbb{F}_{q^{k/e}}$, in order to save multiplications.

7.4 An algorithm for scalar multiplication on incomplete Edwards curves

Suppose E_d is an Edwards curve over $\mathbb{F}_q$ given by the equation

$$x^2 + y^2 = 1 + d(xy)^2,$$

with d a square in $\mathbb{F}_q$. As explained in Section 7.1, this curve is not *complete*, i.e. the Edwards addition law is not complete. We denote by α a square root of $1/d$. We consider the map:

$$\begin{array}{rcl} \tau : E_d & \rightarrow & E_d \\ [x, y, 1] & \mapsto & [\frac{\alpha}{x}, \frac{\alpha}{y}, 1]. \end{array} \qquad (7.11)$$

One can easily check that $\tau([x, y, 1])$ is a point on the Edwards curve. On special points we extend this map as follows:

$$\begin{array}{rcl} \tau[0, 1, 1] & = & [1, 0, 0] \text{ and } \tau[1, 0, 0] = [0, 1, 1] \\ \tau[1, 0, 1] & = & [0, 1, 0] \text{ and } \tau[0, 1, 0] = [1, 0, 1] \end{array}$$

We show that the map τ is in fact a translation map by a point of order 2, with respect to the addition law on the elliptic curve.

Proposition 7.2. Let E_d be an Edwards curve defined over a finite field $\mathbb{F}_q$ such that -1 and $d-1$ are not square roots in $\mathbb{F}_q$. The map $\tau : E_d \to E_d$ defined by equation (7.11) has the following properties

(a) Given P_1 and P_2 two points on the curve E_d we have:

$$\begin{aligned} \tau(P_1+P_2) &= \tau(P_1)+P_2 \\ \tau(P_1) &+ \tau(P_2) = P_1+P_2. \end{aligned}$$

(b) If P is a point on E_d, then $\tau(\tau(P)) = P$.

(c) τ is a translation by a point of order 2.

Proof. We denote $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$. By applying the formulae for the Edwards addition law we have that the coordinates of $\tau(P_1) + P_2$ are

$$\left(\frac{\alpha(x_1x_2+y_1y_2)}{x_1y_1+x_2y_2}, \frac{\alpha(x_1y_2-y_1x_2)}{x_1y_1-x_2y_2}\right)$$

Now by using the curve equation we get the following equalities:

$$\begin{aligned} (x_1x_2+y_1y_2)(x_1y_2+y_1x_2) &= x_1y_1(x_2^2+y_2^2)+x_2y_2(x_1^2+y_1^2) = x_1y_1(1+d(x_2y_2)^2)+x_2y_2(1+d(x_1y_1)^2) \\ &= x_1y_1+x_2y_2+dx_1x_2y_1y_2(x_1y_1+x_2y_2) = (x_1y_1+x_2y_2)(1+dx_1x_2y_1y_2) \\ (x_1y_2-y_1x_2)(y_1y_2-x_1x_2) &= x_1y_1(x_2^2+y_2^2)-x_2y_2(x_1^2+y_1^2) = x_1y_1(1+d(x_2y_2)^2)-x_2y_2(1+d(x_1y_1)^2) \\ &= (x_1y_1-x_2y_2)(1-dx_1x_2y_1y_2). \end{aligned}$$

It follows that the coordinates of $\tau(P_1) + P_2$ can also be written as

$$\left(\frac{\alpha(1+dx_1y_1x_2y_2)}{x_1y_2+y_1x_2}, \frac{\alpha(1-dx_1y_1x_2y_2)}{y_1y_2-x_1x_2}\right).$$

We conclude that $\tau(P_1) + P_2 = \tau(P_1 + P_2)$. The second formula at (a) can be checked easily by applying addition formulae. The equality at (b) is obvious. To prove (c), we observe that, if P_1 and P_2 are two points on the Edwards curve, we have that

$$\psi^{-1}(\tau(P_1+P_2)) - \psi^{-1}(\tau(P_1)) = \psi^{-1}(P_1+P_2) - \psi^{-1}(P_1),$$

where ψ^{-1} is the map defined in equation (7.3) and the + stands for the addition law on the Weierstrass equivalent curve. We conclude that τ is a translation for the addition law on the elliptic curve. By applying the second equality at point (a), we deduce that it is a translation by a point of order 2. □

Remark 7.1. Point (a) in Theorem 7.2 can also be proven by using Hisil and al.'s addition law for Edwards curves [48]. Indeed, note that by applying addition formulae in [48], we get that the coordinates of the point in equation (7.12) are the coordinates of the point $\tau(P_1 + P_2)$.

Algorithm 13 Scalar multiplication on incomplete Edwards curves

INPUT: An Edwards curve $E_d/\mathbb{F}_q$, with d a square root in $\mathbb{F}_q$, a point P on E and $\lambda \in \mathbb{Z}$.
OUTPUT: The point λP.

```
Let $i = [\log_2(\lambda)]$, $K \leftarrow P,\ f \leftarrow 1$, $l \leftarrow 0$.
while $i \geq 1$ do
  if $2K$ is defined then
    $K \leftarrow 2K$
  end if
  else $K \leftarrow \tau(K) + K$; $l \leftarrow l + 1$.
  if the $i$-th bit of $\lambda$ is 1 then
    if $K + P$ is defined then
      $K \leftarrow K + P$.
    end if
    else $K \leftarrow \tau(K) + P$; $l \leftarrow l + 1$.
  end if
end while
if $l \ mod\ 2 = 1$ then
  $K \leftarrow \tau(K)$.
end if
return $K$.
```

The correctness of Algorithm 13 is transparent from Proposition 7.2. The conditions that -1 and $d-1$ are not squares ensure that whenever the Edwards addition $P_1 + P_2$ is not defined, the modified addition $\tau(P_1) + P_2$ is defined (we no longer detail the computations). Hence Algorithm 13 works for all points on the curve. The algorithm is based on the square-and-multiply method, hence its complexity is $O(\log \lambda)$ in time. The cost of an addition of two points during the process is of 10**m** + 1**s** + 1**d**, if performed in projective coordinates. We now evaluate the cost of performing the addition $\tau(P_1) + P_2$, instead of $P_1 + P_2$.

Suppose $P_1 = (X_1, Y_1, Z_1)$ and $P_2 = (X_2, Y_2, Z_2)$ two points we want to add. In projective coordinates, the formulae for computing $\tau(P_1) + P_2$ are as follows

$$\begin{aligned} X_3 &= \alpha(Z_1^2 Z_2^2 + dX_1X_2Y_1Y_2)(Y_1Y_2 - X_1X_2) \\ Y_3 &= \alpha(Z_1^2 Z_2^2 - dX_1X_2Y_1Y_2)(X_1Y_2 + Y_1X_2) \\ Z_3 &= Z_1Z_2(X_1Y_2 + Y_1X_2)(Y_1Y_2 - X_1X_2) \end{aligned}$$

This computation is performed as shown in Table 7.8. The operation count gives $9\mathbf{m}+1\mathbf{s}+1\mathbf{d}+2\alpha$ for one addition. This is faster than addition in projective coordinates and as fast as addition in inverted Edwards coordinates.

Table 7.8: Complete addition for incomplete Edwards curves

$A \leftarrow Z_1 \cdot Z_2,\ B \leftarrow A^2,\ C \leftarrow X_1 \cdot X_2,\ D \leftarrow Y_1 \cdot Y_2$	(1**s**+3**m**)
$E \leftarrow dC \cdot D,\ F \leftarrow B - E,\ G \leftarrow B + E,\ X_3 \leftarrow \alpha \cdot G \cdot (D - C),\ H \leftarrow (X_1 + Y_1) \cdot (X_2 + Y_2) - C - D$	(3**m**)
$Y_3 \leftarrow \alpha \cdot F \cdot H,\ Z_3 \leftarrow A \cdot H \cdot (D - C)$	(3**m**)

We have given an efficient algorithm for scalar multiplication for Edwards curves whose addi-

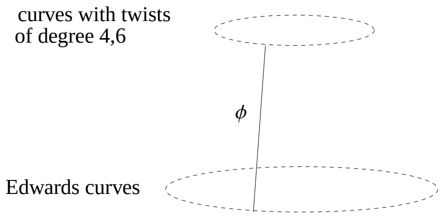


Figure 7.2: A 2-volcano

tion law is incomplete. Other complete addition laws for incomplete Edwards curves were recently proposed by Bernstein and Lange [9].

7.5 Future work. Computing the Ate pairing on Edwards curves

Theorem 7.1 states that an elliptic curve is in Edwards form if the group that is associated to it has a subgroup of order 4. Galbraith [38] shows that for curves with twists of degree larger than 2, the curve and its twist cannot be simultaneously in Edwards form. This becomes a problem in pairing computation, especially when we want to compute the Ate pairing defined on $\mathbb{G}_2 \times \mathbb{G}_1$. As explained in Section 6.2.1, the group $\mathbb{G}_2$ on the elliptic curve in Weierstrass form is given by

$$\phi(\mathbb{G}_2'),$$

where $\mathbb{G}_2'$ is a subgroup of order r on the twisted curve. Hence most operations in pairing computation are performed on $\mathbb{F}_{q^{k/e}}$, where e is the degree of the twist.

In [23], Costello et al. present a solution to this problem: they suppose that the twisted curve is in Edwards form and show that the Ate pairing (actually a small power of the Ate pairing) can be computed entirely on the twisted curve. Even though this solution allows us to compute a pairing with a shorter loop, this approach has several important drawbacks. Before explaining the disadvantages of the proposal in [23], we give a recent result of Morain [75].

Theorem 7.3. A complete Edwards curve lies on the floor of a 2-volcano.

This result implies that curves whose discriminants are fundamental are not complete Edwards curves. In particular, curves with j-invariants 0 and 1728 do not allow a complete Edwards addition law. Hence, the approach presented in [23] could only work on incomplete Edwards curves. Moreover, in a cryptographic implementation, one rarely needs to compute only the pairing. In most protocols, there is a scalar multiplication to perform on the curve, before computing the pairing. The main reasons one might have for implementing protocols in Edwards coordinates are that the scalar multiplication is faster and that these coordinates offer resistance to side-channel attacks (see [12]). Obviously, we cannot perform the scalar multiplication on the twisted curve, because it would be very expensive.

Using the two curves to exploit their respective advantages would be the ideal solution to this problem. But how can we do that? Since the Edwards curve E_d lies on the floor of its 2-volcano, the isogeny $\phi : E_d \to E_{s,p}$ described at Section 7.2.1 is of the ascending type. If the 2-volcano had height 2, we could use this isogeny to switch from the Edwards curve to a curve on the crater of the volcano. However, this approach implies performing some inversions in the finite field. We have found another isogeny of degree 4 from the Edwards curve to a curve in Weierstrass form, whose equation gives a method to switch between the two representations without performing inversions. We define the following isogeny from an Edwards curve E_d to the curve $E'_{s,p}$ of equation $E'_{s,p} : s^2 = d^2 p^3 + 2(d - 2)p^2 + p$

$$\begin{array}{rcl} \varphi : E_d & \to & E'_{s,p} \\ (x, y) & \mapsto & (xy(x^2 - y^2), (xy)^2) \end{array}$$

Suppose that $\sqrt[3]{d} \in \mathbb{F}_q$. Then we substitute (s, p) for $(s, \frac{p}{\sqrt[3]{d^2}})$. We obtain a new equation for the curve $E'_{s,p}$:

$$s^2 = p^3 + \frac{2(d - 2)}{d\sqrt[3]{d}} p^2 + \frac{p}{\sqrt[3]{d^2}}.$$

The kernel of φ is the 4-torsion subgroup $\{O, T_2, T_4, -T_4\}$. It follows that φ is not a new isogeny, the curve $E'_{s,p}$ being actually isomorphic to $E_{s,p}$.

Remark 7.2. We have tried to use φ to give an algorithm computing a 4-th power of the Tate pairing, using similar techniques to those in Section 7.2.3. Unfortunately, we have obtained an algorithm which is slower than the one in Section 7.2.3.

We believe that this isogeny may be the solution to efficiently computing the Ate pairing in Edwards coordinates on curves with discriminants −4 and −3. Moreover, this could also represent a solution to the problem of using twists of high degree to compute the Tate pairing. Further investigation is needed to make sure we can actually employ the twists in these algorithms.

7.6 Conclusion

Efficiently implementing pairings on Edwards curves is a difficult problem. Some questions in this research area remain open. For example, it is not possible to implement protocols using the Ate pairing entirely in Edwards coordinates. Moreover, many families of pairing friendly curves cannot be given in Edwards form, because they do not fulfill the condition on the curve group order.

Chapter 8

Conclusion

At a first glance, this thesis treats two different subjects. The first one is a study of isogeny volcanoes using pairings, while the second one refers to the efficient implementation of cryptographic pairings using isogenies. In fact, the starting idea of our work is the following observation. Given P and Q two ℓ-torsion points on the elliptic curve, the value of the pairing $e_\ell(P, Q)$ and an isogeny $I : E \to E'$, we have

$$e_\ell(\phi(P), \phi(Q)) = e_\ell(P, Q)^{\deg \phi}.$$

Part two of this dissertation relates this result to the isogeny class $Ell_t(\mathbb{F}_q)$. To every curve E in $Ell_t(\mathbb{F}_q)$ we associate a quadratic form $P_{E,\ell^{n_2}}$ which is an invariant of the set of curves having the same endomorphism ring as E. We show that the zeros of this quadratic form correspond to points of order ℓ generating the kernel of horizontal or vertical isogenies in the ℓ-isogeny volcano of E. The remaining points of order ℓ generate the kernels of descending isogenies.

This discovery has important consequences on algorithms used to travel on the isogeny volcano. First of all, by evaluating the number of zeros of the quadratic form $P_{E,\ell^{n_2}}$, we give a method to decide whether the curve E is on the crater of the ℓ-volcano or not. Secondly, we give a method to decide in advance, when taking a step on the volcano, whether this step is horizontal or descending, ascending or descending. Our method is very efficient, because it involves only the computation of a small number of pairings. The immediate consequence is that we have found very simple algorithms, allowing to travel on the graph from one point to another.

In the third part, the approach is completely different. This time our goal is to make use of the isogeny in order to speed up the computation of the pairing value $e(P, Q)$. A first result is obtained by considering endomorphisms of small degree for pairing friendly elliptic curves. Endomorphisms were already used before in pairing computation [83] [47] [96]. However, until now, only endomorphisms with trivial kernel, such as the Frobenius endomorphism or automorphisms, were proposed. We propose endomorphisms having a kernel of small order. This gives a small correction factor in the computation of the pairing, but the cost of the computation of this factor is negligible. Our algorithm has better performances than Miller's algorithm for curves with embedding degree $2, 3$ and 4.

The second contribution in this area is an efficient algorithm to compute pairings on Edwards curves. We used an isogeny of degree 4 between the Edwards curve and another curve of genus 1 and derived formulae for efficient pairing computation on the Edwards curve.

8.1 Limitations of our methods and open problems

Isogeny volcanoes. Unfortunately, on some volcanoes, our method for determining the direction of an isogeny is very expensive in the upper part of the volcano, above the second stability level. Given a curve E lying on a level above the second stability level, all self-pairings of ℓ-torsion points of $E/\mathbb{F}_q$ may be degenerate. Consequently, if we restrain to the volcano defined over the base field, we cannot distinguish between a point spanning the kernel of an horizontal isogeny from the point spanning the kernel of a descending isogeny, or the point spanning the kernel of the ascending isogeny from the point spanning the kernel of the descending isogeny. However, we have shown that by considering the curve defined over an extension field $\mathbb{F}_q$, with degree a multiple of ℓ, we find non-degenerate self-pairings of ℓ-torsion points. The only problem is that computing these pairings may be very expensive, and the algorithms derived in this way will be highly inefficient. The question of how to predict directions of isogenies in the irregular part of the volcano remains thus open. We only note that the non-degenerate pairings obtained over the extension field $\mathbb{F}_{q^{s\ell}}$ have values over the base field $\mathbb{F}_q$. This rises the question whether it would be possible to compute these pairings more efficiently.

Isogeny volcanoes and cryptography. In Section 5.5.1, we presented a volcano-based algorithm to compute the Hilbert polynomial. Apart from the theoretical importance of this computation, advances in this area also have quickly found application in cryptography. Interest in algorithms allowing to compute this polynomial has arisen because of the key role this polynomial plays in methods to construct pairing friendly curves.

As explained in section 6.1, some families of pairing friendly curves are very rare, and finding curves in such families depends drastically on our ability to compute $H_D(X)$ for large discriminants D. We explain this idea by an example. For MNT curves with embedding degree 6, Sutherland's computations [89] gave 500 discriminants D, with $D < 10^{12}$ which provide pairing friendly curves at 80 bits security level (according to [36]).

Consequently, a logical continuation of the work in this thesis would be to adapt Sutherland's algorithm to our methods and see whether this results into obtaining the class equations for larger discriminants.

The same considerations are valid for the algorithm computing modular polynomials [90], which are needed in cryptography since certain algorithms (such as Schoof's algorithm) use precomputations of this polynomial.

Cryptographic non-degenerate self pairings. We explained in Chapter 6 that non-degenerate self-pairings have many cryptographic applications. While on supersingular curves, constructing such pairings is rather easy thanks to distortion maps, on ordinary curves matters are more complicated. In Section 6.4 we have given a method to construct ordinary curves having non-degenerate self-pairings for all points of order r. Our construction is the first construction of this kind which does not use distortion maps.

The curves have embedding degree 1 and ρ-value is approximately 2. Unfortunately, because of the high ρ-value, we estimate that pairing computation is less efficient on these curves than on supersingular curves with embedding degree 2. The questions of how to implement these pairings efficiently and how to hash to these curves efficiently remain open.

Pairing implementation using endomorphisms. In Chapter 6 we have given a method to use endomorphisms to speed up pairing computation on curves with small discriminant. We have surveyed many existing constructions of pairing friendly curves with small discriminant to see whether our method applies to these constructions. More precisely, we were interested in finding curves for which the size of the eigenvalue λ of the endomorphism is approximately $\sqrt{r}$. We have found that our method works on curves constructed with the Cocks-Pinch method, which is very flexible in choosing the value of r. Unfortunately, because of the high value of the parameter ρ, these curves are far from being optimal for pairing based cryptography. We raise the question whether it would be possible to construct by complex multiplication curves having eigenvalues $\lambda \approx \sqrt{r}$ and better ρ-value.

Pairing on Edwards curves. We have given an isogeny of degree 4 from the Edwards curve to a curve in Weierstrass form. F. Morain [75] showed recently that complete Edwards curves lie on the floor of 2-volcanoes. This result implies that on a 4-volcano, our isogeny is ascending. In the case of curves with discriminant -4 and -3 lying on a 2-volcano of height 2, this allows us to transport points from the Edwards curve lying on the floor to a curve lying on the crater. This gives an inversion free algorithm to compute the Ate pairing on the Weierstrass curve, by making use of twists of degree 4 and 6. However, we do not know whether it is possible, by using the isogeny or its dual, to find an algorithm which computes the Ate pairing (or a small power of the Ate pairing) entirely in the Edwards form.

Bibliography

[1] T. Okamoto A. Menezes and S.A. Vanstone. Reducing elliptic curve logarithms to logarithms in the finite field. In *Proceedings 23rd Annual ACM Symposium on Theory of Computing (STOC)*, pages 80–89. ACM Press, 1991.

[2] L.M. Adleman, J. DeMarrais, and M.-D. Huang. A subexponential algorithm for discrete logarithms over hyperelliptic curves of large genus over GF (q). *Theoretical Computer Science*, 226(1-2):7–18, 1999.

[3] C. Arène, T. Lange, M. Naehrig, and C. Ritzenthaler. Faster Computation of the Tate Pairing. http://eprint.iacr.org/2009/155.

[4] M. Atiyah and I. Macdonald. *Introduction to Commutative Algebra*. Addison-Wesley, 1969.

[5] A.O.L. Atkin. The number of points on an elliptic curve modulo a prime. E-mail on the Number Theory Mailing List, 1988.

[6] P. Barreto, S. Galbraith, C. Héigeartaigh, and M. Scott. Efficient Pairing Computation on Supersingular Abelian Varieties. *Des. Codes Cryptography*, 42(3):239–271, 2007.

[7] P. Barreto and M. Naehrig. Pairing-friendly elliptic curves of prime order. In B. Preneel and S. Tavares, editors, *Selected Areas in Cryptography - SAC 2005*, volume 3897 of *Lecture Notes in Computer Science*, pages 319 –331. Springer, 2006.

[8] J. Belding, R. Broker, A. Enge, and K. Lauter. Computing Hilbert class polynomials. In A.J. van der Poorten and A. Stein, editors, *Algorithmic Number Theory Symposium-ANTS VIII*, volume 5011 of *Lecture Notes in Computer Science*, pages 282–295. Springer Verlag, 2008.

[9] D. Bernstein and T. Lange. A complete set of addition laws for incomplete Edwards curves. http://eprint.iacr.org/2009/580.

[10] D. Bernstein and T. Lange. Explicit formulas-database. http://www.hyperelliptic.org/EFD, 2007.

[11] D. J. Bernstein, P. Birkner, M. Joye, T. Lange, and C. Peters. Twisted Edwards curves. In S. Vaudenay, editor, *AFRICACRYPT*, volume 5023 of *Lecture Notes in Computer Science*, pages 389–405. Springer Verlag, 2008.

[12] D. J. Bernstein and T. Lange. Faster addition and doubling on elliptic curves. In K. Kurosawa, editor, *Advances in Cryptology – ASIACRYPT 2007*, volume 4833 of *Lecture Notes in Computer Science*, pages 29–50. Springer Verlag, 2007.

[13] D. J. Bernstein and T. Lange. Inverted Edwards coordinates. In S. Boztas and H.F. Lu, editors, *AAECC 2007*, volume 4851 of *Lecture Notes in Computer Science*, pages 20–27. Springer Verlag, 2007.

[14] G. Bisson and A. Sutherland. Computing the endomorphism ring of an ordinary elliptic curve over a finite field. http://eprint.iacr.org/2009/100, 2009.

[15] I. F. Blake, G. Seroussi, and N. P. Smart. *Advances in Elliptic Curve Cryptography*, volume 317 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, 2005.

[16] D. Boneh and M. K. Franklin. Identity-based encryption from the Weil pairing. In J. Kilian, editor, *Advances in Cryptology – CRYPTO 2001*, volume 2139 of *Lecture Notes in Computer Science*, pages 213–229. Springer Verlag, 2001.

[17] D. Boneh, B. Lynn, and H. Shacham. Short signatures from the Weil pairing. In C. Boyd, editor, *Advances in Cryptology – ASIACRYPT 2001*, volume 2248 of *Lecture Notes in Computer Science*, pages 514–532. Springer Verlag, 2001.

[18] D. Boneh, K. Rubin, and A. Silverberg. Finding composite order ordinary elliptic curves using the Cocks-Pinch method. to appear in Journal of Number Theory.

[19] Z.I. Borevitch and I.R. Chafarevitch. *Théorie des nombres*. Gauthiers-Villars, Paris, 1967.

[20] F. Brezing and A. Weng. Elliptic curves suitable for pairing based cryptography. *Des Codes Cryptography*, 37(1):133–141, 2005.

[21] R. Broker. *Constructing elliptic curves of prescribed order*. PhD thesis, Universiteit Leiden, 2006.

[22] R. Broker and P. Stevenhagen. Constructing elliptic curves of prime order. *Contemporary Mathematics*, (463):17–28, 2008.

[23] T. Lange C. Costello and M. Naehrig. Faster Pairing Computations on Curves with High-Degree Twists. In P. Q. Nguyen and D. Pointcheval, editors, *Public Key Cryptography-PKC 2010*, Lecture Notes in Computer Science, pages 224–242. Springer, 2010.

[24] D. Charles. On the existence of distortion maps on ordinary curves. http://eprint.iacr.org/2006/128.

[25] D. A. Cox. *Primes of the Form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication*. John Wiley & Sons, Inc, 1989.

[26] M. Prem Laxman Das and P. Sarkar. Pairing computation on twisted Edwards form elliptic curves. In S. Galbraith and K. Paterson, editors, *Pairing*, volume 5209 of *Lecture Notes in Computer Science*, pages 192–210. Springer Verlag, 2008.

[27] M. Deuring. *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper*. Abh. Math. Sem. Hansischen Univ. 14, 1941.

[28] L. Dewaghe. Un corollaire aux formules de Vélu. Draft, 1995.

[29] C. Diem. The GHS attack in odd characteristic. *Journal of Ramanujan Mathematical Society*, 18(1):1–32, 2003.

[30] W. Diffie and M. Hellman. New Directions in Cryptography. *IEEE Transcations on Informatics Theory*, IT-22(6):644–654, 1976.

[31] S. Duquesne and G. Frey. Background on pairings, Chapter 6. In *Handbook of elliptic and hyperelliptic curve cryptography*, pages 115–132. Chapman and Hall/CRC, Taylor and Francis Group, 2006.

[32] H. M. Edwards. A normal form for elliptic curves. *Bull. AMS*, 44:393–422, 2007.

[33] N.D. Elkies. Explicit isogenies. Draft, 1991.

[34] M. Fouquet. *Anneau d'endomorphismes et cardinalité des courbes elliptiques: aspects algorithmiques*. PhD thesis, Ecole Polytechnique, 2001.

[35] M. Fouquet and F. Morain. Isogeny volcanoes and the SEA algorithm. In C. Fieker and D. R. Kohel, editors, *ANTS-V*, volume 2369 of *Lecture Notes in Computer Science*, pages 276–291. Springer, 2002.

[36] D. Freeman, M. Scott, and E. Teske. A taxonomy of pairing-friendly elliptic curves. *Journal of Cryptology*, (23):224–280, 2006.

[37] G. Frey and H.-G. Rück. A remark concerning m-divisibility and the discrete logarithm problem in the divisor class group of curves. *Math.Comp.*, 62:865–874, 1994.

[38] S. Galbraith. Twists of Edwards curves. Draft, 2009.

[39] S. Galbraith, F. Hess, and N. Smart. Extending the GHS Weil-descent attack. In L. R. Knudsen, editor, *EUROCRYPT02*, volume 2332 of *Lecture Notes in Computer Science*, pages 29–44. Springer, 2002.

[40] S. Galbraith, J.F McKee, and P.C. Valenca. Ordinary abelian varieties having small embedding degree. *Finite Fields and their Applications*, (13):800–814, 2007.

[41] P. Gaudry. An algorithm for solving the discrete log probleme on hyperelliptic curves. In B. Preneel, editor, *EUROCRYPT00*, volume 1807 of *Lecture Notes in Computer Science*, pages 19–34. Springer, 2000.

[42] P. Gaudry, E. Thomé, N. Thériault, and C. Diem. A double large prime variation for small genus hyperelliptic index calculus. *Mathematics of Computation*, 76(257):475–492, 2007.

[43] R. Granger, F. Hess, R. Oyono, N. Thériault, and F. Vercauteren. Ate pairing on hyperelliptic curves. In M. Naor, editor, *EUROCRYPT07*, Lecture Notes in Computer Science, pages 430–447. Springer, 2007.

[44] R. Granger, D. Page, and N. P. Smart. High security pairing-based cryptography revisited. In F. Hess, S. Pauli, and M. E. Pohst, editors, *ANTS*, volume 4076 of *Lecture Notes in Computer Science*, pages 480–494, 2006.

[45] R. Hartshorne. *Algebraic Geometry*, volume 52 of *Graduate Texts in Mathematics*. Springer, 1977.

[46] F. Hess. A note on the Tate pairing of curves over finite fields. *Arch. Math*, 82:28–32, 2004.

[47] F. Hess, N. P. Smart, and F. Vercauteren. The Eta pairing revisited. *IEEE Transactions on Information Theory*, 52:4595–4602, 2006.

[48] Huseyin Hisil, Kenneth Koon-Ho Wong, Gary Carter, and Ed Dawson. Twisted edwards curves revisited. In *ASIACRYPT '08: Proceedings of the 14th International Conference on the Theory and Application of Cryptology and Information Security*, pages 326–343. Springer-Verlag, 2008.

[49] S. Ionica and A. Joux. Pairing the volcano. In *Algorithmic Number Theory*. 9th International Symposium, Nancy, France, ANTS-IX, July 19-23, 2010, Proceedings, To appear.

[50] S. Ionica and A. Joux. Another approach to pairing computation in Edwards coordinates. In D. R. Chowdhury, V. Rijmen, and A. Das, editors, *Progress in Cryptography- Indocrypt 2008*, volume 5365 of *Lecture Notes in Computer Science*, pages 400–413. Springer, 2008.

[51] A. Joux. A one round protocol for tripartite Diffie-Hellman. *Journal of Cryptology*, 17(4):263–276, September 2004.

[52] A. Joux and R. Lercier. The Function Field Sieve in the Medium Prime Case. In *Advances in Cryptology: Eurocrypt 2006*.

[53] A. Joux, R. Lercier, N. Smart, and F. Vercauteren. The Number Field Sieve in the Medium Prime Case. In Cynthia Dwork, editor, *Advances in Cryptology- CRYPTO 2006*, volume 4117 of *Lecture Notes in Computer Science*, pages 326–344, 2006.

[54] A. Joux and K. Nguyen. Separating Decision Diffie Hellman from Computational Diffie Hellman in Cryptographic Groups. *Journal of Cryptology*, 16(4):239–247, 2003.

[55] H.W. Lenstra Jr. Complex multiplication structure of elliptic curves. *Journal of Number Theory*, 56(2):227–241, 1996.

[56] E. Kachisa, E. Schaefer, and M. Scott. Constructing Brezing-Weng pairing friendly elliptic curves using elements in the cyclotomic field. In S. Galbraith and K. Paterson, editors, *Pairing Based Cryptography-Pairing 2008*, volume 5209 of *Lecture Notes in Computer Science*, pages 126–135, 2008.

[57] K. Karabina and E. Teske. On prime order elliptic curves with embedding degrees $3, 4$ and 6. In A.J. van der Poorten and A. Stein, editors, *Algorithmic Number Theory Symposium-ANTS-VIII*, volume 5011 of *Lecture Notes in Computer Science*, pages 102–117. Springer, 2008.

[58] N. Koblitz. Elliptic curve cryptosystems. *Mathematics of Computation*, 48(177):203–209, 1987.

[59] N. Koblitz. Hyperelliptic curve cryptosystems. *Journal of Cryptology*, 1:139–150, 1989.

[60] N. Koblitz and A. Menezes. Pairing-based cryptography at high security levels. In N. P. Smart, editor, *Proceedings of Cryptography and Coding 2005*, volume 3796 of *Lecture Notes in Computer Science*, pages 13–36, 2005.

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

[62] S. Lang. *Elliptic Functions*, volume 112 of *Graduate Texts in Mathematics*. Springer Verlag, 1987.

[63] S. Lang. *Algebraic Number Theory*, volume 110 of *Graduate Texts in Mathematics*. Springer Verlag, 1994.

[64] R. Lercier. *Algorithmique des Courbes Elliptiques dans les Corps Finis*. PhD thesis, École polytechnique, Palaiseau, 1997.

[65] R. Lercier, D. Lubicz, and F. Vercauteren. Point counting on elliptic and hyperelliptic curves, Chapter 17. In *Handbook of elliptic and hyperelliptic curve cryptography*, pages 407–454. Chapman and Hall/CRC, Taylor and Francis Group, 2006.

[66] S. Lichtenbaum. Duality theorems for curves over p-adic fields. *Invent.Math.7*, pages 120–136, 1969.

[67] F. Luca and I. Shparlinski. Elliptic curves with small embedding degree. *Journal of Cryptology*, (19):553–562, 2006.

[68] MAGMA Computational Algebra System. *MAGMA version V2.16-5*, 2010. http://magma.maths.usyd.edu.au/magma.

[69] V. Miller. Use of elliptic curves in cryptography. In A. M. Odlyzko, editor, *Advances in Cryptology – CRYPTO'86*, volume 263, pages 417–426. Springer Verlag, 1986.

[70] V. Miller. The Weil pairing, and its efficient calculation. *Journal of Cryptology*, 17(4):235–261, September 2004.

[71] J. Miret, R. Moreno, D. Sadornil, J. Tena, and M. Valls. An algorithm to compute volcanoes of 2-isogenies on elliptic curves over finite fields. *Applied Mathematics and Computation*, 176(2):736–750, 2006.

[72] J. Miret, R. Moreno, D. Sadornil, J. Tena, and M. Valls. Computing the height of volcanoes of l-isogenies of elliptic curves over finite fields. *Applied Mathematics and Computation*, 196(1):67–76, 2008.

[73] A. Miyaji, M. Nakabayashi, and S. Takano. New explicit of elliptic curve traces for FR-reduction. *IEICE Transactions on Fundamentals*, E84-A5(5):1234–1343, 2001.

[74] P.L. Montgomery. *A FFT extension of the elliptic curve method of factorization*. PhD thesis, University of California, 1992.

[75] F. Morain. Edwards curves and CM multiplication. http://hal.inria.fr/inria-00375427/fr.

[76] P.C.van Oorschot and M.J.Wiener. Parallel collision search with cryptanalytic applications. *Journal of Cryptology*, (12):1–18, 1999.

[77] The PARI Group, Bordeaux. *PARI/GP, version 2.1.5*, 2005. http://pari.math.u-bordeaux.fr.

[78] S. Pohlig and M. Hellmann. An improved algorithm for computing logarithms over GF(p) and its cryptographic significance. *IEEE Transactions in Information Theory*, IT-24:106–110, 1978.

[79] J. Pollard. Monte Carlo methods for index computation (mod p). *Mathematics of Computation*, (32):918–924, 1978.

[80] H.-G. Rück. A note on elliptic curves over finite fields. *Mathematics of Computation*, 179:301–304, 1987.

[81] T. Satoh and K. Araki. Fermat quotients and the polynomial time discrete log algorithm for anomalous curves. *Comm. Math. Univ. Sancti Pauli*, 47:81–92, 1998.

[82] R. Schoof. Counting points on elliptic curves over finite fields. *Journal de Theorie des Nombres de Bordeaux*, 7:219–254, 1995.

[83] M. Scott. Faster pairings using an elliptic curve with an efficient endomorphism. In S. Maitra, C. E. V. Madhavan, and R. Venkatesen, editors, *INDOCRYPT 2005*, volume 3797 of *Lecture Notes in Computer Science*, pages 258–269. Springer, 2005.

[84] A. Shamir. Identity-based cryptosystems and signature schemes. In G. R. Blakley and D. Chaum, editors, *CRYPTO84*, volume 196 of *Lecture Notes in Computer Science*, pages 47–53. Springer, 1985.

[85] D. Shanks. Class number, a theory of factorization, and genera. In *Proceedings of Symposium of Pure Mathematics*, volume 20, pages 415–440. American Mathematical Society, 1971.

[86] J. H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, 1986.

[87] J.H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*, volume 151 of *Graduate Texts in Mathematics*. Springer, 1994.

[88] A. Sutherland. Pairing-friendly curves suitable for cryptography. http://www-math.mit.edu/ drew/WeberModPolys.html.

[89] A. Sutherland. Pairing-friendly curves suitable for cryptography. http://www-math.mit.edu/ drew/MNTCurves.

[90] A. Sutherland. Modular polynomials via isogeny volcanoes. http://arxiv.org/abs/1001.0402, 2009.

[91] Andrew Sutherland. Computing Hilbert Class Polynomials with the CRT. http://arxiv.org/abs/0903.2785, 2009.

[92] J. Tate. WC-groups over p-adic fields. In *Séminaire Bourbaki; 10e année: 1957/1958. Textes des conférences;Exposés 152 à 168; 2e éd. corrigée,Exposé 156*, volume 13. Sécretariat mathématique, Paris, 1958.

[93] J. Vélu. Isogenies entre courbes elliptiques. *Comptes Rendus De Academie Des Sciences Paris, Serie I-Mathematique, Serie A.*, 273:238–241, 1971.

[94] E.R. Verheul. Evidence that XTR is more secure that supersingular elliptic curve cryptosystems. In B. Pfitzmann, editor, *Advances in Cryptography: EUROCRYPT 2001*, volume 2045 of *Lecture Notes in Computer Science*, pages 195–201. Springer, 2001.

[95] J. von zur Gathen and V. Shoup. Computing Frobenius maps and factoring polynomials. *Computational Complexity*, 2:187–224, 1992.

[96] C. Zhao and F. Zhang. Computing the Bilinear Pairings on Elliptic Curves with Automorphisms. http://eprint.iacr.org/2008/209.

Résumé

Les couplages sont utilisés en cryptographie pour mener des attaques contre le logarithme discret sur certaines courbes elliptiques, ainsi que pour la construction des schémas cryptographiques. Depuis 2000, la cryptographie à base des couplages a connu un grand essor.

Dans cette thèse, nous nous intéressons dans un premier temps à l'implémentation des couplages en utilisant des isogénies. Ces travaux incluent une méthode pour le calcul du couplage sur des courbes elliptiques ayant des endomorphismes de petit degré. Nous proposons par ailleurs un algorithme qui calcule le couplage sur la courbe d'Edwards, à l'aide d'une isogénie de degré 4 entre la courbe d'Edwards et une autre courbe de genre 1.

Dans un deuxième temps, nous proposons les couplages pour l'étude des volcans d'isogénies. Les volcans d'isogénies sont des graphes dont les noeuds sont des courbes elliptiques et les arêtes sont des l-isogénies entre les courbes. En 1996, Kohel propose l'utilisation du parcours en profondeur de ces graphes dans un algorithme qui calcule l'anneau d'endomorphismes d'une courbe elliptique. Fouquet et Morain (2001) ont proposé d'autres algorithmes pour le parcours de ces graphes. Cependant, jusqu'à présent, il n'était pas possible de prédire la direction d'un pas sur le volcan; de fait, un grand nombre de pas successifs était nécessaire avant de déterminer la direction prise. Nous introduisons une méthode qui permet de calculer, pour une courbe elliptique E, les points d'ordre l qui engendrent les noyaux des isogénies descendantes, ascendantes ou horizontales. Notre méthode, basée sur le calcul de quelques couplages, est très efficace et donne, dans beaucoup de cas, des algorithmes plus rapides que les méthodes existantes pour le parcours des volcans d'isogénies.

Abstract

Pairings are used in cryptography to attack the discrete logarithm problem on some curves and also in building cryptosystems. Since 2000, pairing based cryptography has been an active area of research.

In this thesis, we first study algorithms for pairing computation combined with isogenies. We give an algorithm for pairing computation using endomophisms of small degree and an efficient implementation of pairings on an Edwards curve, by making use of an isogeny of degree 4 between the Edwards curve and another genus one curve.

Secondly, we propose pairings in the study of isogeny volcanoes. Isogeny volcanoes are graphs whose vertices are elliptic curves and whose edges are l-isogenies. Algorithms allowing to travel on these graphs were developed by Kohel in his thesis (1996) and later on, by Fouquet and Morain (2001). However, up to now, no method was known, to predict, before taking a step on the volcano, the direction of this step. To solve this issue, we develop a method to determine on an elliptic curve the points of order l that generate kernels of descending, ascending and horizontal isogenies. Our method, based on the computation of a few pairings, is very efficient and gives, in most cases, simple algorithms, allowing to either walk on the crater, descend from the crater to the floor or ascend from the floor to the crater.