Habilitation à diriger des recherches

UNIVERSITÉ PARIS 6

Courbes elliptiques, arithmétique et corps finis

Document de synthèse de l'activité scientifique de

François Morain

Soutenue le 17 octobre 1997 devant le jury composé de :

Henri Cohen	Rapporteur
Philippe Flajolet	
Daniel Lazard	Président
Jean-François Mestre	Rapporteur
Jean-Louis Nicolas	
Jean-Jacques Quisquater	Rapporteur

LABORATOIRE D'INFORMATIQUE
UMR CNRS n°7650
École polytechnique 91128 Palaiseau Cedex FRANCE

Remerciements

Le premier à remercier est naturellement D. Lazard, qui a accepté la lourde tâche de président de jury, après m'avoir aidé à comprendre le cheminement administratif nécessaire à une soutenance d'habilitation. Je le remercie aussi pour son intérêt géométrique porté aux courbes elliptiques.

H. Cohen a été mon premier guide dans le domaine de la primalité, et son influence sur la communauté française et mondiale de théorie algorithmique des nombres – par ses écrits ou le logiciel `pari` – a été prédominante aussi bien sur le domaine que dans mes travaux.

On ne peut pas travailler sur les courbes elliptiques sans croiser un jour ou l'autre les travaux de J.-F. Mestre. Ses articles ciselés et son enthousiasme à faire partager ses travaux a toujours été très enrichissant pour moi.

J.-J. Quisquater s'est intéressé à mes travaux depuis mes débuts. Je me souviendrai longtemps du congrès EUROCRYPT'89 qu'il organisa et qui marqua ma première participation active à cette longue liste de congrès.

Depuis fort longtemps, je dois beaucoup à P. Flajolet, pour son accueil au projet ALGO pendant ma thèse, pour la qualité de son écoute et sa façon synthétique de présenter des résultats de recherche en en extrayant la quintessence.

Ma dette envers J.-L. Nicolas est immense. Non content d'avoir été un directeur de thèse de première classe, il m'a aussi impliqué dans de nombreux coups audacieux, comme ces trois années passées à apprendre à rédiger des problèmes de math-info pour l'épreuve éponyme de l'ENS.

Une habilitation ne se fait pas toute seule, n'importe où, avec n'importe qui ou dans n'importe quelles conditions.

Je remercie la DGA, qui m'a permis de faire de la recherche dans de bonnes conditions, et ce depuis le début de ma thèse. En m'affectant à l'École polytechnique et plus précisément au Laboratoire d'Informatique (LIX), j'ai pu continuer à travailler sur les sujets qui me passionnent. J'espère avoir remboursé une partie de la dette contractée en formant une grande majorité des Ingénieurs de l'Armement intéressés par la cryptologie, que ce soit en DEA (IMA puis ALGO), ou encore en thèse.

Après ma thèse, J.-M. Steyaert m'a accueilli à l'École polytechnique, dans l'équipe ALGO. Grâce à lui, j'ai continué ma formation de chercheur aussi bien que de futur directeur de recherches, et j'ai débuté ma carrière d'enseignant. Non content de tout cela, il me soutient également dans les moments difficiles. Je ne le remercierai jamais assez de ses efforts.

On ne fait de bonne recherche que dans une bonne ambiance. Celle du LIX m'a été profitable, en commençant par celle qui règne au sein de l'équipe ALGO ; merci en particulier à P. Chassignet pour sa complicité. Merci à M. Weinfeld pour assurer la cohésion du laboratoire contre vents et marées. Merci à Évelyne et Catherine pour leur compétence et leurs sourires. Et puis, merci aux autres membres du labo pour leur gentillesse. Je n'oublierai pas non plus mes collègues de toujours du projet ALGO de l'INRIA, ni l'incomparable Virginie.

La recherche ne se fait pas de manière isolée. Merci donc à tous mes collègues de la spécialité, et en premier lieu à mes différents co-auteurs, qui m'ont tous appris quelque chose sur leur domaine respectif : A. O. L. Atkin depuis mes débuts, D. Guillaume, A. Joux, J.-M. Couveignes, F. Leprévost.

On dit souvent que la seule façon de comprendre un domaine de recherche consiste à enseigner celui-ci, à différents niveaux. Je remercie donc mes collègues enseignants, qui m'ont fait l'honneur de m'associer à leur enseignement, R. Cori, J.-J. Lévy, J. Stern, J. Vuillemin.

Les échanges avec les élèves permettent d'améliorer la compréhension de la chose exposée. Que soient donc ici remerciés tous mes élèves passés et présents, à l'École polytechnique (en Tronc Commun, Majeure ou Option), en DEA ou en thèse, et parmi eux R. Lercier, P. Gaudry, E. Thomé, M. Fouquet.

La rédaction du présent mémoire a bénéficié des réponses aux questions souvent indiscrètes posées aux différents chercheurs de la spécialité. Merci donc à R. Anderson pour m'avoir invité au Newton Institute dans lequel une bonne partie du mémoire a été écrite ; B. Kaliski et V. Miller pour la cryptologie ; H. W. Lenstra et R. Schoof pour les débuts historiques des courbes elliptiques ; R. Pinch, M. A. Shokrollahi pour leurs travaux ou des pointeurs utiles ; J. Wolfmann, D. Lebrigand, J.-F. Michon et le projet CODES de l'INRIA (P. Charpin, N. Sendrier, D. Augot) pour avoir répondu à mes questions naïves sur les codes algébriques.

Pour finir, n'oublions pas les relecteurs de ce mémoire, à différents stades d'achèvement, à commencer par J.-M. Steyaert et Ph. Dumas.

Merci à mon épouse adorée pour m'avoir forcé à rédiger au moins une de mes thèses, m'empêchant ainsi de céder à la tentation de me contenter de quelques pages qui ne m'auraient pas semblé à la hauteur de ce diplôme ultime, quand bien même celui-ci ne serait que l'ombre des thèses d'État de nos grands-mères.

Table des matières

Chapitre 1

Introduction

§1. L'essor de la théorie algorithmique des nombres

La notion d'expérimentation en théorie des nombres est intrinsèque au domaine. En effet, nombre d'hypothèses peuvent être testées sur des exemples accessibles aux calculs. Dans certains cas, ces expériences conduisent à formuler des conjectures : c'est le cas de la célèbre conjecture de Birch et Swinnerton-Dyer.

Plusieurs phénomènes ont provoqué l'essor de ce domaine dans les vingt dernières années. Tout d'abord l'accès à des moyens de calculs peu onéreux s'est répandu. D'autre part, l'apparition de la cryptographie à clefs publiques en 1976 [DH76, ARS78] a provoqué la résurgence de problèmes anciens comme la primalité et la factorisation des entiers. Aux méthodes parfois artisanales, des méthodes systématiques ont succédé, dont on a pu quantifier l'effet grâce à l'apport de la théorie de la complexité.

Le domaine commence à acquérir ses lettres de noblesse, comme le montre la qualité des congrès ANTS [AH94, Coh96, Buh98] ainsi que l'ouvrage de H. Cohen [Coh93] ou celui de M. Pohst et H. Zassenhaus [PZ89]. L'algorithmisation de deux grands thèmes dominent les débats : celle de la théorie algébrique des nombres et celle de la théorie des courbes algébriques. Du premier thème je ne dirai rien, renvoyant aux références que je viens de citer. Pour le second, je me concentrerai dans ce mémoire sur le cas des courbes elliptiques, essentiellement définies sur des corps finis. Le cas des courbes de genre supérieur sera évoqué au chapitre 10 traitant des codes correcteurs (chapitre 10).

§2. Brève histoire de la théorie des courbes elliptiques

2.1 Courbes elliptiques sur $\mathbb{Q}$

La théorie des courbes elliptiques est riche et ancienne. Motivée par la résolution d'équations cubiques en nombres entiers, et en particulier la paramétrisation de solutions de telles équations, elle s'est enrichie d'une approche analytique, en relation avec le calcul d'intégrales (voir à ce propos l'excellent article de C. Houzel [Hou78]), puis d'une approche arithmétique.

L'approche arithmétique commence au moment où la notion de groupe des points sur une courbe elliptique est reconnue comme fondamentale. Bien que de nombreux chercheurs (à commencer par Newton[1] – voir [Sch90]) aient empiriquement découvert les propriétés de groupe de l'ensemble des solutions d'une équation cubique – la fameuse loi de la tangente et de la corde permet de trouver de nouvelles solutions à partir d'une solution déjà connue – il a fallu attendre les travaux de Mordell [Mor22] pour que la notion de groupe commence à s'imposer dans l'étude des courbes elliptiques.

[1] **Diophante ?**

Le théorème principal, appelé désormais théorème de Mordell-Weil (suite à la généralisation de ce résultat par Weil au cas des courbes algébriques quelconques sur un corps quelconque [Wei28]), dit que le groupe des points rationnels de E est engendré par un nombre fini de points. Autrement dit

$$E(\mathbb{Q}) \sim E_{\text{tors}} \oplus \mathbb{Z}^r$$

où E_{tors} est l'ensemble des points de torsion et r est le *rang* de la courbe. Poincaré [Poi01] avait déjà considéré cette quantité, mais sans référence au groupe des points. Les groupes de torsion ont commencé à être étudiés à peu près à la même époque et ils ont été classifiés complètement sur $\mathbb{Q}$ par Mazur [Maz77] (voir [Mer96] pour le cas des corps de nombres).

De nombreux objets sont attachés aux courbes elliptiques : fonctions ζ, fonctions L, formes modulaires. Les succès de ces connexions sont fameux, comme le montrent par exemple les travaux de Wiles sur la conjecture de Taniyama-Weil [Wil95a, TW95] (impliquant le théorème de Fermat). L'une des conjectures les plus importantes concernant le rang des courbes sur $\mathbb{Q}$ est celle de Birch et Swinnerton-Dyer [BSD63, BSD65], qui relie le rang de la courbe E à l'ordre en 1 de la fonction L de la courbe. Cette conjecture a été prouvée dans certains cas particuliers. Nous renvoyons à [Coh93, ch. 7] pour des précisions supplémentaires.

2.2 Courbes elliptiques sur un corps finis

Dans sa thèse [Art24], Artin conjecture que le nombre m de points d'une courbe hyperelliptique $C\ : y^2 = f(x)$ de genre g modulo p satisfait $|m-(p+1)| \leqslant 2g\sqrt{p}$.

En genre 1, Davenport [Dav31] prouve que $m-p = O(p^{3/4})$ dans le cas où f est de degré 3 et a trois racines dans $\mathbb{Z}/p\mathbb{Z}$. Mordell [Mor93] montre que $m-p = O(p^{2/3})$ pour tout f de degré 3. C'est Hasse qui démontre la conjecture d'Artin, toujours en genre 1, en utilisant deux méthodes différentes [Has33, Has34b] ; il introduit également la notion de courbe elliptique supersingulière [Has34a]. Viennent ensuite les travaux fondamentaux de Deuring [Deu41] classifiant les anneaux d'endomorphismes possibles pour les courbes elliptiques définies sur un corps fini, théorie qui a ensuite été raffinée par Waterhouse [Wat69].

La conjecture d'Artin a été démontrée dans toute sa généralité par Weil [Wei48] et dans le cas des variétés abéliennes par Deligne (voir par exemple [Kat76]).

§3. Algorithmique des courbes elliptiques

3.1 Algorithmes sur $\mathbb{Q}$

La résolution algorithmique des problèmes que posent les courbes définies sur $\mathbb{Q}$ a beaucoup progressé dans les trente dernières années. Les premières idées sont présentes dans [BSD63, BSD65]. Le calcul du rang est désormais possible d'un point de vue numérique, en se basant sur les formules explicites de Mestre par exemple [Mes83]. Les programmes de Cremona [Cre92] permettent d'accomplir cette tâche. On peut désormais envisager de trouver toutes les solutions de certaines équations diophantiennes elliptiques en utilisant des minorations de forme linéaires de logarithmes [GPZ94, ST94]. Nous renvoyons là encore à [Coh93, ch. 7] pour de plus amples informations.

3.2 Algorithmes dans les corps finis

Présentation du contexte

Le premier algorithme de primalité déterministe ayant un temps de calcul quasi-polynomial est apparu en 1978 (dans [Adl80], voir aussi [APR83]). Il faisait appel à la théorie des sommes de Gauss et des lois de réciprocité d'ordre supérieur. Des tentatives de simplification de cet algorithme ont conduit à raffiner et décrire en termes modernes les algorithmes de primalité utilisés [Len81]. Là aussi, la notion de groupe s'est révélée fondamentale. En primalité comme en factorisation, les groupes (ou pseudo-groupes) utilisés provenaient tous de corps finis ou d'extensions de l'anneau $\mathbb{Z}/N\mathbb{Z}$.

L'extension de ces idées aux courbes elliptiques – en d'autres termes le remplacement de $\mathbb{Z}/N\mathbb{Z}$ par le groupe des points sur une courbe elliptique – s'est faite en plusieurs étapes. Dès 1981, motivé par une question de H. Cohen, R. Schoof avait mis au point un algorithme de calcul du nombre de points d'une courbe elliptique dans un corps fini. Vers 1982, il avait trouvé une application au calcul déterministe polynomial de racines carrés modulo p (voir [Sch85]). Vers 1985, H. W. Lenstra (Jr.) a l'idée d'utiliser les courbes elliptiques pour factoriser des entiers à la Pollard ; Bosma [Bos85] étudie des tests de primalité avec des courbes elliptiques à multiplication complexe. L'approche de Lenstra a un succès immédiat. Celle-ci représente en effet une idée résolument nouvelle dans le domaine. Testée dès 1985, la méthode de factorisation montre rapidement ses qualités, en fournissant des facteurs plus grands que ceux trouvés par les algorithmes probabilistes classiques (voir le chapitre 7 pour plus de détails).

En 1986, Goldwasser et Kilian combinent l'approche de Lenstra et celle de Schoof et mettent au point le premier algorithme de primalité exacte permettant de tester la primalité de presque tous les nombres en temps polynomial. La même année, Adleman et Huang généralisent cette méthode au cas des courbes de genre 2 et donnent le premier algorithme exact de primalité en temps polynomial probabiliste [AH86, AH92]. La même année encore, Atkin met au point un algorithme pratique de primalité basé lui aussi sur les courbes elliptiques, ne reposant pas sur l'algorithme de Schoof, mais sur les propriétés de multiplication complexe. Il semble que la méthode soit plus puissante que la méthode des sommes de Jacobi et cela d'autant plus qu'elle fournit un certificat de primalité qu'il est aisé de vérifier.

Résumé de ma participation

La recherche d'algorithmes performants sur les courbes elliptiques dans les corps finis est ainsi en train de prendre son essor, lorsqu'en 1987, je commence à travailler sur l'algorithme d'Atkin. J'écris très rapidement une première implantation qui me permet, dès 1988, de certifier tous les nombres probablement premiers contenus dans les tables du projet Cunningham [BLS$^+$88] et qui n'avaient pu être certifiés par l'algorithme des sommes de Jacobi. En 1989, je rends visite à Atkin et nous comparons nos idées sur son test de primalité. Suite à cette visite, j'entreprends de mettre au point de meilleurs algorithmes pour construire le corps de classe de Hilbert des corps quadratiques imaginaires, un des points les plus critiques de l'algorithme. Ces travaux m'amènent à mettre au point des algorithmes spécifiques pour la factorisation de polynômes sur des extensions quadratiques de $\mathbb{Q}$. Cela me conduit également à utiliser la théorie de Galois pour résoudre par radicaux certaines équations algébriques modulo p. Ces travaux constituent une part importante de l'article [AM93a].

Lors du congrès EUROCRYPT'89, je présente l'application de mon programme à la génération de nombres premiers utiles en cryptographie (100 à 200 chiffres décimaux), qui semble alors plus rapide que l'algorithme des sommes de Jacobi [Mor90a]. Lors de ce même congrès, Bosma et van der Hulst (qui à l'époque optimisent l'algorithme des sommes de Jacobi [BvdH90a]) me lancent un défi, celui d'être le premier à certifier le premier *nombre Titanic*[2] ordinaire, à savoir $(2^{3539}+1)/3$ (nombre qui a 1065 chiffres décimaux). Pour relever le défi de Bosma et van der Hulst, je commence l'implantation distribuée de l'algorithme de primalité. Le record est établi le 11 novembre 1989 (le 10, le mur de Berlin est tombé), après de multiples péripéties relatées dans [Mor91b]. Je détiens toujours le record actuel avec un nombre de 1505 chiffres décimaux[3] [Mor92b]. Après ma thèse [Mor90b], je réalise une seconde implantation de l'algorithme, qui s'appelle désormais ECPP (pour Elliptic Curve Primality Proving algorithm). Cette version `C` est mise en ftp anonyme et est encore utilisée actuellement.

L'une des retombées de l'implantation d'ECPP concerne la fabrication de bonnes courbes utilisables dans les cryptosystèmes fondés sur des courbes elliptiques. En effet, dès 1986, les courbes elliptiques ont été employées comme substitut au groupe $\mathbb{Z}/N\mathbb{Z}$ dans les schémas de cryptographie publique [Mil87, Kob87]. Pour pouvoir utiliser des courbes elliptiques, il faut en connaître la cardinalité ; compte tenu de la difficulté d'implanter l'algorithme de Schoof à l'époque, les seules courbes utilisables sont très particulières (en majorité supersingulières). En 1991, je montre dans [Mor91a] qu'une variante d'ECPP fournit une méthode de construction d'une classe de courbes plus générales que les courbes supersingulières.

Vers 1992, il semble soudain raisonnable de s'intéresser à l'implantation efficace de l'algorithme de Schoof. Revenons un peu en arrière. Dès 1986, Atkin pense à utiliser des équations modulaires pour implanter de façon efficace l'algorithme de Schoof. En 1988, une première méthode est décrite [Atk88]. Vers 1989–1990, Elkies apporte une amélioration décisive à l'algorithme de Schoof, construite en partie sur les idées d'Atkin. Celui-ci voit immédiatement le parti à tirer de cette idée et il en donne une version très efficace [Atk92]. En 1993, je commence à étudier et implanter les idées d'Atkin et d'Elkies. J'obtiens rapidement un programme efficace qui permet de travailler dans un corps premier de grande caractéristique. Outre la possibilité de battre des records, ce programme sert de plateforme de tests pour des améliorations ultérieures. Conjointement avec Couveignes [CM94], nous apportons une amélioration quantitative à l'algorithme, ce qui nous a permis de battre le record de la spécialité, en passant de 200 à 350 chiffres décimaux. Aiguillonné par la concurrence [LMMS94, Mül95], je profite d'une amélioration importante due à Dewaghe [Dew98] pour porter finalement le record à 500 chiffres décimaux [Mor95].

Le cas le plus utile pour la cryptographie est sans nul doute celui de la caractéristique 2, cas pour lequel les techniques d'Elkies et d'Atkin ne s'appliquent que partiellement. En 1994, Couveignes donne un algorithme résolvant ces problèmes dans sa thèse [Cou94]. Avec Lercier, qui a fait ses premières armes dans l'implantation de la méthode ECM (voir chapitre 7), et qui devient mon premier "élève", nous décortiquons cet algorithme. Un transfert de mon programme écrit pour la caractéristique p grande vers la caractéristique 2 s'opère très rapidement et Lercier peut alors se concentrer sur l'algorithme de Couveignes, puis sur l'élaboration de son propre algorithme. Les résultats sont saisissants et ont fait l'objet de [LM95c, LM95b]. Nous renvoyons au chapitre 6 pour plus de détails.

[2] À l'époque, un nombre Titanic désignait tout nombre premier de plus de 1000 chiffres décimaux [Yat84, Yat85]. On dit de quelqu'un qui découvre un tel nombre qu'il a *coulé le Titanic*. Suite à mon record, la définition a été portée à 2000 chiffres. Voir par exemple la page `http ://www.utm.edu/research/primes/`.

[3] Record porté à 2196 chiffres début 1998 juste avant d'être battu par le retour des sommes de Jacobi [Mih98].

§4. Présentation du mémoire

Le mémoire reprend les thèmes abordés ci-dessus dans un ordre logique et se veut un panorama de la théorie des courbes elliptiques sur un corps fini et de ses applications à différents domaines.

Nous commençons par une présentation rapide des courbes elliptiques, comprenant entre autres un rappel des propriétés des courbes sur $\mathbb{C}$. Cela nous permet d'introduire la théorie des équations modulaires et de la multiplication complexe. Ces deux thèmes sont récurrents dans le reste du mémoire. Nous passerons ensuite à la théorie sur les corps finis, puis aux algorithmes spécifiques aux corps finis, réservant une place importante à l'algorithme de Schoof. Suivront le chapitre sur la factorisation, puis celui sur la primalité. Les applications à la cryptologie sont données ensuite. Pour compléter le panorama du domaine, nous terminons par un chapitre sur l'utilisation de courbes algébriques (dont les courbes elliptiques) dans la théorie des codes correcteurs d'erreurs, et le dernier chapitre présentera quelques applications marginales des courbes elliptiques.

Nous avons tenté de donner le maximum de références, les plus à jour possibles.

CHAPITRE 2

Théorie générale

Ce chapitre a pour but de rappeler une partie de la théorie des courbes elliptiques définies sur un corps quelconque et de fixer les notations qui seront employées par la suite. Ce qui suit est repris du livre de référence de J. Silverman [Sil86]. Un autre livre de référence est celui de A. W. Knapp [Kna92].

On se place sur un corps $\mathbb{K}$ de caractéristique carac($\mathbb{K}$) et on appelle $\overline{\mathbb{K}}$ une clôture algébrique de $\mathbb{K}$.

§1. Définition

Nous suivons [Sil86, ch. III]. Une courbe de genre 1 est une cubique projective lisse. On note $\mathbb{P}^2(\mathbb{K})$ le plan projectif de $\mathbb{K}$. La forme la plus générale de l'équation d'une telle courbe est $\mathcal{F}(X,Y,Z)=0$ avec

$$\mathcal{F}(X,Y,Z) = Y^2Z + a_1XYZ + a_3YZ^2 - (X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3) \tag{2.1}$$

où les a_i sont dans $\mathbb{K}$. La condition de lissité s'exprime par le fait que le système

$$\frac{\partial F}{\partial X} = \frac{\partial F}{\partial Y} = \frac{\partial F}{\partial Z} = 0$$

n'a pas de solutions non triviales dans le plan projectif. Ceci est équivalent au fait qu'une certaine quantité Δ, appelé le *discriminant* de la courbe, est non nul. On pose

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

$$c_4 = b_2^2 - 24b_4, c_6 = b_2^3 + 36b_2b_4 - 216b_6.$$

Le discriminant de la courbe est alors

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$$

et la condition annoncée est simplement $\Delta \neq 0$. La quantité $j(E) = c_4^3/\Delta$ est appelé *invariant* de la courbe. Nous noterons également :

$$\mathcal{F}(X,Y) = Y^2 + a_1XY + a_3Y - (X^3 + a_2X^2 + a_4X + a_6).$$

Si carac($\mathbb{K}$) est différente de 2 et 3, on se ramène au modèle classique de Weierstrass $y^2 = x^3 + ax + b$.

On note $E(\mathbb{K})$ l'ensemble des points du plan projectif de $\mathbb{K}$ vérifiant (2.1). La courbe E possède un seul point à l'infini $O_E = (0,1,0)$. La partie affine de E est constituée des points $(X,Y,1)$ où $\mathcal{F}(X,Y)=0$.

§2. Loi de groupe

On peut munir l'ensemble $E(\mathbb{K})$ d'une loi de groupe abélien, que l'on note traditionnellement additivement. La loi associée, dite *loi de la corde et de la tangente*, s'exprime au moyen de fractions rationnelles. La donnée de E et de Ω constitue une *courbe elliptique*.

Pour définir la loi de groupe, on choisit arbitrairement un point Ω de $E(\mathbb{K})$ qui servira d'élément neutre. On calcule la somme P_3 de deux points P_1 et P_2 de $E(\mathbb{K})$, en appliquant les deux formules :

$$P_1 + P_2 + S = O_E,$$

$$S + P_3 + \Omega = O_E.$$

Dans la plupart des cas, on choisit $\Omega = O_E$, ce qui simplifie les calculs. Les équations dans ce cas se trouvent dans [Sil86, chap. III] et nous les rappelons pour mémoire. Si $P = (x, y)$ est un point non nul de $E(\mathbb{K})$, alors $-P = (x, -y - a_1x - a_3)$. Si P_1 et P_2 sont deux points, $P_i = (x_i, y_i)$, on calcule leur somme $P_3 = (x_3, y_3)$ de la façon suivante. Si $x_1 = x_2$ et $y_1 + y_2 + a_1x_2 + a_3 = 0$, alors $P_3 = O_E$. Sinon, on calcule l'équation de la droite $\mathcal{D}$ d'équation $y = \lambda x + \nu$ passant par P_1 et P_2 (si $P_1 = P_2$, on prend la tangente) ; on calcule ainsi :

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}, \quad \nu = \frac{y_1x_2 - y_2x_1}{x_2 - x_1}$$

si $x_2 \neq x_1$ et

$$\lambda = \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}, \quad \nu = \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}$$

sinon. On termine alors en intersectant cette droite $\mathcal{D}$ avec la courbe E, pour trouver :

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2,$$

$$y_3 = -(\lambda + a_1)x_3 - \nu - a_3.$$

On définit la multiplication par un entier positif m sur E de la façon suivante : $[0]P = O_E$ et si $m \neq 0$:

$$[m]P = \underbrace{P + P + \cdots + P}_{m \text{ fois}}.$$

On prolonge par $[-m]P = -([m]P)$.

Des considérations algorithmiques sur le calcul de la loi de groupe sont rassemblées dans le chapitre 6.

§3. Polynômes de division et points de torsion

Soit m un entier positif. Comme l'équation de la loi de groupe s'exprime à l'aide de fractions rationnelles, il est facile de voir qu'il existe des polynômes ϕ_m, ψ_m et ω_m de $\mathbb{Z}[a_1, a_2, a_3, a_4, a_6, X, Y]$ tels que

$$[m](X, Y) = \left(\frac{\phi_m(X, Y)}{\psi_m^2(X, Y)}, \frac{\omega_m(X, Y)}{\psi_m^3(X, Y)}\right)$$

Le polynôme ψ_m, appelé *polynôme de m-division*, satisfait les formules :

$$\psi_0 = 0, \psi_1 = 1, \psi_2 = 2Y + a_1X + a_3;$$

$$\psi_3 = 3X^4 + b_2X^3 + 3b_4X^2 + 3b_6X + b_8;$$
$$\psi_4 = \psi_2\left(2X^6 + b_2X^5 + 5b_4X^4 + 10b_6X^3 + 10b_8X^2 + (b_2b_8 - b_4b_6)X + (b_4b_8 - b_6^2)\right);$$

$$\psi_2\psi_{2m} = \psi_m(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2), m \geqslant 2; \tag{2.2}$$

$$\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3, m \geqslant 2. \tag{2.3}$$

Le polynôme ϕ_m est donné par

$$\phi_m = X\psi_m^2 - \psi_{m-1}\psi_{m+1}.$$

En caractéristique différente de 2, on a

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

En caractéristique 2, et pour des paramétrisations simplifiées, Koblitz [Kob90] donne des formules pour ces polynômes.

Le polynôme ψ_m joue un rôle particulier. Soit $\psi_m'(X)$ la réduction de $\psi_m(X,Y)$ dans

$$\mathbb{K}[X,Y]/(\mathcal{F}(X,Y)).$$

On définit les polynômes f_m de la façon suivante : si m est pair, on pose $f_m = \psi_m'/\psi_2'$ et si m est impair, on pose $f_m = \psi_m'$. Si m est pair, f_m est de degré $(m^2-4)/2$ et de coefficient dominant $m/2$; si m est impair, f_m est de degré $(m^2-1)/2$ et de coefficient dominant m. Notons qu'on peut calculer rapidement le polynôme f_m, i.e., en temps $O(\log m)$, grâce aux formules (2.2) et (2.3). Une autre approche est utilisée dans [McK94] où l'auteur utilise une équation différentielle due à Fricke pour calculer f_m.

On désigne par $E[m]$ l'ensemble

$$\{P \in \overline{\mathbb{K}}, [m]P = O_E\}$$

des points de m-torsion de $E(\overline{\mathbb{K}})$.

Théorème 2.1 *Soit $P = (X,Y) \in E(\overline{\mathbb{K}})$ tel que $2P \neq O_E$. Alors $P \in E[m]$ si et seulement si $f_m(X) = 0$.*

La structure du groupe $E[m]$ est connue précisément.

Théorème 2.2 *Si $\mathbb{K}$ est de caractéristique 0 ou m premier avec* carac$(\mathbb{K})$*, alors $E[m] \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. Si* carac$(\mathbb{K}) = p$*, alors pour tout e, $E[p^e]$ est soit réduit au point O_E (et E sera dite* supersingulière*), soit isomorphe à $\mathbb{Z}/p^e\mathbb{Z}$.*

§4. Isogénies et endomorphismes

Les isogénies sont de première importance dans l'étude de la multiplication complexe (chapitre 4), ainsi que dans les améliorations de l'algorithme SEA (voir chapitre 6). Nous rappelons ici brièvement quelques-unes des propriétés les plus importantes.

Définition 2.1 *On appelle* isogénie *entre deux courbes E_1 et E_2 tout morphisme ϕ de E_1 dans E_2 envoyant O_{E_1} sur O_{E_2}. Les deux courbes seront dites* isogènes *s'il existe une isogénie ϕ vérifiant $\phi(E_1) \neq \{O_{E_2}\}$.*

Si ϕ est une isogénie non constante, elle induit une injection ϕ^* entre $\overline{\mathbb{K}}(E_2)$ et $\overline{\mathbb{K}}(E_1)$ définie par $\phi^*(f) = f \circ \phi$. On appelle *degré* de ϕ le degré de l'extension $[\overline{\mathbb{K}}(E_1) : \phi^*\overline{\mathbb{K}}(E_2)]$. On montre que ce degré est fini, et on pose par convention $\deg(0) = 0$.

Exemple. La multiplication par un entier m est une isogénie de degré m^2.

L'un des résultats importants est le suivant.

Théorème 2.3 *Soit ϕ une isogénie de degré m. Alors il existe une unique isogénie $\hat{\phi}$, appelée* isogénies duale *entre E_2 et E_1 telle que $\hat{\phi} \circ \phi = [m]$.*

Il est naturel de s'intéresser aux isogénies entre E et elle-même. Ces isogénies forment l'anneau des endomorphismes de E, noté $\mathrm{End}(E)$. Cet ensemble contient toutes les multiplications $[m]$. Les différents types d'anneau possible sont donnés dans le théorème suivant.

Théorème 2.4 *L'anneau* $\mathrm{End}(E)$ *est soit $\mathbb{Z}$, soit un ordre dans un corps quadratique imaginaire, soit un ordre dans une algèbre de quaternion.*

Si $\mathbb{K} = \mathbb{C}$, seuls les deux premiers cas peuvent se produire. Si $\mathbb{K}$ est un corps fini, on est dans l'un des deux derniers (voir chapitre 5). Si $\mathrm{End}(E)$ est plus grand que $\mathbb{Z}$, on dit que E est à multiplication complexe. C'est le cas de certaines courbes définies sur $\mathbb{C}$ – théorie que nous résumons au chapitre qui suit – et pour la majorité des courbes définies sur un corps fini. Les liens entre ces deux théories, multiplication complexe sur $\mathbb{C}$ et dans les corps finis, forment le cœur de la théorie des courbes sur les corps finis.

CHAPITRE 3

Courbes définies sur $\mathbb{C}$: le cas classique

Le cas complexe est le cas classique par excellence, cadre de la théorie des fonctions elliptiques développée au XIX^{e} siècle et de la célèbre paramétrisation de Weierstrass.

L'identification d'une courbe elliptique avec un réseau nous donne la clef de nombreuses propriétés satisfaites par des courbes définies dans n'importe quel corps. Ce passage est possible parce que les objets que l'on construit sont algébriques et définis sur $\mathbb{Q}$. C'est le cas des polynômes modulaires et des courbes modulaires associées.

Ces courbes modulaires sont utilisées dans beaucoup de domaines de la théorie des nombres. Les courbes $X_0(m)$ et $X_1(m)$, que nous allons présenter dans ce chapitre, permettent de décrire certaines propriétés des courbes elliptiques. La courbe $X_0(m)$ est l'objet central des idées d'Atkin et d'Elkies présentées au chapitre 6, car elle permet de construire les isogénies de degré m. Elle sert également d'exemple dans le chapitre sur les codes algébriques.

L'implantation des améliorations de l'algorithme SEA (voir chapitre 6) nécessite le calcul d'équations explicites pour $X_0(m)$, m premier $\leqslant 1000$, calculs que j'ai effectués en m'appuyant sur [Atk88] et qui a fait l'objet de [Mor95].

La courbe $X_1(m)$ permet de paramétrer les courbes elliptiques ayant un point d'ordre m défini sur $\mathbb{K}$. Cette courbe est utilisée dans l'analyse de la méthode ECM au chapitre 7. De façon explicite, elle permet de construire des courbes définies sur $\mathbb{Q}$ et ayant des groupes de torsion maximaux avec un rang non nul, ce qui est fait dans mon article avec Atkin [AM93b].

§1. Courbes elliptiques et réseaux

On sait que toute courbe elliptique E sur $\mathbb{C}$ est isomorphe à un quotient $\mathbb{C}/L$ où L est un réseau : $L = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ avec $\tau = \omega_1/\omega_2$ un élément du demi plan de Poincaré $\mathcal{H} = \{z \in \mathbb{C}, \Im(z) > 0\}$. La fonction de Weierstrass de E définie par la somme

$$\wp(z) = \frac{1}{z^2} + \sum_{\substack{\omega\in L\\ \omega\neq 0}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right) = \frac{1}{z^2} + \sum_{k=1}^{\infty} G_{2k}(L) z^{2k} = \sum_{\substack{\omega\in L\\ \omega\neq 0}} \frac{1}{\omega^{2k}}$$

permet de paramétrer la courbe E. En effet, le couple $(\wp(z), \wp'(z))$ est un point de $E \ : y^2 = 4x^3 - g_2 x - g_3$ où l'on a posé $g_2 = 60G_4(L)$, $g_3 = 140G_6(L)$. On définit la quantité

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

qui est appelée *invariant* du réseau (ou de la courbe), en raison du fait qu'elle reste invariante par homothétie par rapport à L, c'est-à-dire que pour tout $\alpha \in \mathbb{C}^*$, $j(\alpha L) = j(L)$.

§2. Formes et fonctions modulaires

Les résultats de cette section sont tirés de [Ser70]. Pour $\tau \in \mathcal{H}$, on note $q = \exp(2i\pi\tau)$.

2.1 Définitions

On pose

$$\Gamma = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix}, a, b, c, d \in \mathbb{Z}, ad - bc = 1 \right\}.$$

Si $M \in \Gamma$, son action sur $\mathcal{H}$ est notée

$$M\tau = M(\tau) = \frac{a\tau + b}{c\tau + d}.$$

On définit encore $\hat{\mathbb{C}}$ le compactifié de $\mathbb{C}$ et $\mathcal{H}^* = \mathcal{H} \cup \mathbb{Q} \cup \{i\infty\}$. Les éléments de $\mathbb{Q} \cup \{i\infty\}$ sont appelés “pointes” ; $i\infty$ est la “pointe à l'infini”.

Définition 3.1 *Soit k un entier naturel. Une fonction $f : \mathcal{H}^* \to \hat{\mathbb{C}}$ est dite* modulaire de poids k *si et seulement si*

1. *f est méromorphe sur $\mathcal{H}$ (holomorphe sauf en les pôles) ;*
2. *$f(M\tau) = (c\tau + d)^k f(\tau)$ pour tout $M \in \Gamma$ et tout $\tau \in \mathcal{H}^*$;*
3. *il existe $a > 0$ tel que pour $\Im(\tau) > a$, $f(\tau)$ a un développement du type*

$$f(\tau) = \sum_{v \geqslant h} b_v e^{2\pi i v \tau}$$

avec $h \in \mathbb{Z}$ et $b_h \neq 0$. Par suite $f(i\infty) = 0$ si $h > 0$, $f(i\infty) = b_0$ si $h = 0$ et $f(i\infty) = \infty$ si $h < 0$.

Définition 3.2 *On appelle* forme modulaire *toute fonction modulaire qui est holomorphe à l'infini. Donc $f(\tau) = \sum_{n \geqslant 0} a_n x^n$. Si $a_0 = 0$, on dit que f est* parabolique.

L'exemple le plus classique de formes modulaires est celui des séries d'Eisenstein. Soit k un entier positif plus grand que 1. Reprenons la quantité $G_{2k}(\mathbb{Z} + \tau\mathbb{Z})$ introduite à la section précédente et récrivons la :

$$G_{2k}(\tau) = \sum_{(n,m) \neq (0,0)} \frac{1}{(m\tau + n)^{2k}}.$$

Proposition 3.1 *La série G_{2k} est une forme modulaire de poids $2k$ avec de plus $G_{2k}(i\infty) = 2\zeta(2k)$ où ζ désigne la fonction ζ de Riemann.*

On introduit alors une autre série classique, de poids 12, est donnée par

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

Enfin, l'invariant modulaire $j(\tau)$, qui correspond à l'invariant de la courbe, vaut $12^3 g_2(\tau)^3 / \Delta(\tau)$.

Théorème 3.1 *La fonction j est une fonction modulaire de poids 0. Elle est holomorphe dans $\mathcal{H}$ et a un pôle simple à l'infini. Elle s'écrit :*

$$j(q) = j(\tau) = \frac{1}{q} + 744 + \sum_{n \geqslant 1} c_n q^n \tag{3.1}$$

où les c_n sont des entiers positifs satisfaisant des propriétés arithmétiques remarquables [Ser70].

La fonction j permet de caractériser toutes les fonctions modulaires de poids 0 :

Proposition 3.2 *Soit f une fonction méromorphe sur $\mathcal{H}$. Alors les propriétés suivantes sont équivalentes :*

1. *f est une fonction modulaire de poids 0 ;*
2. *f est quotient de deux formes modulaires de même poids ;*
3. *f est une fonction rationnelle en j.*

§3. Isogénies et équations modulaires

Le but de cette section est d'introduire le plus naturellement possible les polynômes modulaires et les propriétés qui en découlent. Pour cela, les propriétés des réseaux sont une nouvelle fois essentielles.

Soient L un réseau, E la courbe elliptique $\mathbb{C}/L$, M un autre réseau et $E' = \mathbb{C}/M$. On sait (voir par exemple [Lan73]) que les isogénies entre E et E' sont les homomorphismes analytiques entre E et E', et que ceux-ci s'identifient aux nombres complexes α tels que $\alpha M \subset L$. Pour étudier ces isogénies, il suffit de considérer le cas où M et un sous-réseau de L, puisque $j(\alpha M) = j(M)$.

Sans perte de généralité, on peut se contenter d'étudier les cas où L/M est cyclique, ce qui nous conduit à étudier les sous-réseaux de L de la forme

$$M = (a\omega_1 + b\omega_2)\mathbb{Z} + (c\omega_1 + d\omega_2)\mathbb{Z}$$

avec

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

une matrice à coefficients entiers positifs de déterminant m et $\mathrm{pgcd}(a, b, c, d) = 1$. L'ensemble des matrices 2×2 à coefficients positifs et premiers entre eux forme le groupe Δ_m^*.

Proposition 3.3 *Soient f et g deux éléments de Δ_m^*. On note $f \sim g$ si et seulement s'il existe γ dans Γ tel que $g = \gamma \circ f$. Les classes d'équivalence de cette relation forment l'ensemble*

$$\mathcal{S}_m = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}, ad = m, \mathrm{pgcd}(a, b, d) = 1, a > 0, d > b \geqslant 0 \right\}$$

dont le cardinal est $\mu_0(m) = m \prod_{p|m}(1 + 1/p)$.

Soit A une matrice de $\mathcal{S}_m$:

$$A = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}.$$

La matrice A agit sur $\mathcal{H}$ par $\tau \mapsto A\tau = (a\tau + b)/d$. On pose

$$\Psi_m(X, q) = \prod_{A \in \mathcal{S}_m} (X - j(A\tau))$$

où Ψ_m est un polynôme en X et $q = \exp(2i\pi\tau)$. Les coefficients de Ψ_m sont en fait des fonctions modulaires, donc des polynômes en $j(q)$, d'après la proposition 3.2. On considère alors Ψ_m comme étant un polynôme bivarié $\Psi_m(X, Y)$ vérifiant $\Psi_m(j(A\tau), j(\tau)) = 0$. Ce polynôme est appelé *polynôme modulaire*.

On démontre alors les résultats suivants :

Théorème 3.2 *Le polynôme $\Psi_m(X,Y)$ est à coefficients dans $\mathbb{Z}$, symétrique en X et Y, unitaire si m est sans facteur carré.*

Rassemblons les résultats obtenus sous une forme compacte :

Théorème 3.3 *Il existe $\alpha \in \mathbb{C}$ tel que $\alpha M \subset L$ si et seulement s'il existe m tel que*

$$\Psi_m(j(L), j(M)) = 0.$$

Ou encore : il existe une isogénie de noyau cyclique d'indice m (de degré m) entre E et E' si et seulement si $\Psi_m(j(E), j(E')) = 0$.

Plus généralement [Igu59, Igu68] :

Théorème 3.4 *Soit $\mathbb{K}$ un corps quelconque, $E/\mathbb{K}$ et $E^*/\mathbb{K}$ deux courbes elliptiques. Il existe une isogénie cyclique de degré m entre E et E^* si et seulement si $\Psi_m(j(E), j(E^*)) = 0$.*

Nous verrons dans le chapitre 4 que ce théorème est de première importance dans la théorie de la multiplication complexe. Il sert de base aux améliorations de l'algorithme de Schoof (voir chapitre 6).

L'équation $\Psi_m(X,Y) = 0$ définit la courbe $X_0(m)$, qui est un cas particulier de courbe modulaire. Nous allons détailler les propriétés de ces courbes au chapitre suivant.

§4. Courbes modulaires

On pourra consulter par exemple [Shi71, Sch74, TV91] pour la théorie de ces courbes. Les propriétés qui suivent raffinent celles introduites pour le groupe Γ tout entier. L'idée générale est d'associer à tout sous-groupe Γ_1 d'indice fini μ de Γ, une courbe, dite *modulaire*, notée $X(\Gamma_1)$.

4.1 Théorie

On note S_v les classes de Γ/Γ_1 :

$$\Gamma = \bigcup_{v=1}^{\mu} \Gamma_1 S_v.$$

On dit alors que deux points τ et τ' de $\mathcal{H}^*$ sont *équivalents* si et seulement s'il existe $M \in \Gamma_1$ tel que $\tau' = M\tau$. On note $\mathcal{H}^*/\Gamma_1$ l'ensemble des classes d'équivalence pour cette relation. On montre que l'ensemble $\mathcal{H}^*/\Gamma_1$ est un espace de Haussdorf compact et connexe. Il forme une surface de Riemann compacte, notée $X(\Gamma_1)$.

Une *fonction modulaire* pour un sous-groupe Γ_1 est alors essentiellement une fonction f sur $\mathcal{H}^*$ invariante par les matrices de Γ_1, c'est-à-dire que, outre des conditions techniques de régularité, on a

$$f(M(\tau)) = f(\tau)$$

pour tout $M \in \Gamma_1$ et $\tau \in \mathcal{H}^*$.

On peut trouver une équation de $X(\Gamma_1)$ en utilisant des propriétés de théorie de Galois des fonctions modulaires.

Théorème 3.5 *Toute fonction modulaire f pour Γ_1 satisfait une équation de degré μ :*

$$G(f) = \sum_{v=0}^{\mu} R_v(J) f^v = 0$$

où les coefficients $R_v(J)$ sont des fonctions rationnelles en J sur $\mathbb{C}$. Les conjugués de f sont les fonctions $f|S_v$ définies par $(f|S_v)(\tau) = f(S_v\tau)$.

4.2 Exemples : les courbes $X_0(m)$ et $X_1(m)$

La courbe $X_0(m)$

La courbe $X_0(m)$ correspond au sous-groupe

$$\Gamma_0(m) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix}, ad - bc = 1, c \equiv 0 \bmod m \right\}.$$

Les classes de $\Gamma/\Gamma_0(m)$ forment l'ensemble $\mathcal{S}_m$ défini à la section §3..

Théorème 3.6 *Le genre de $X_0(m)$ est*

$$g_0(m) = 1 + \frac{\mu_0(m)}{12} - \frac{\epsilon_\rho}{3} - \frac{\epsilon_i}{4} - \frac{\sigma_\infty}{2}$$

où

$$\epsilon_\rho = \begin{cases} 0 & \text{si } 9 \mid m \\ \prod_{p \mid m} \left(1 + \left(\frac{-3}{p}\right)\right) & \text{sinon;} \end{cases}$$

$$\epsilon_i = \begin{cases} 0 & \text{si } 4 \mid m \\ \prod_{p \mid m} \left(1 + \left(\frac{-1}{p}\right)\right) & \text{sinon;} \end{cases}$$

et

$$\sigma_\infty = \sum_{t \mid m} \varphi((t, m/t))$$

où φ désigne la fonction d'Euler.

La courbe $X_1(m)$

Nous renvoyons à [HBJ92] pour les propriétés de cette courbe. La courbe $X_1(m)$ correspond au sous-groupe

$$\Gamma_1(m) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix}, ad - bc = 1, a \equiv d \equiv 1 \bmod m, c \equiv 0 \bmod m, \right\}$$

d'indice $\mu_1(m) = \varphi(m)\mu_0(m)$. Soit $g_1(m)$ le genre de $X_1(m)$.

Théorème 3.7 *Si $m \leqslant 4$, $g_1(m) = 0$. Sinon*

$$g_1(m) = 1 + \frac{\mu_1(m)}{24} - \frac{1}{4} \sum_{t \mid m} \varphi(t)\varphi(m/t).$$

Cette courbe paramétrise les courbes elliptiques ayant un point d'ordre m sur $\mathbb{K}$. On peut calculer une équation de $X_1(m)$ de la façon suivante. Pour simplifier, on se donne une courbe elliptique sur $\mathbb{K}$ définie par deux coefficients indéterminés a et b :

$$E \ : Y^2 = X^3 + aX + b$$

et on suppose connu un point particulier $P = (x_0, y_0)$ de $E(\mathbb{K})$. On calcule alors les coordonnées du point $[m]P$ en fonction de a et b. L'annulation de ce point fournit des relations algébriques pour a et b, qui caractérisent les courbes E ayant P pour point de m-torsion.

Cette approche a été utilisée par exemple dans [Kub76, Rei86] et qui est reprise dans [AM93b] (voir chapitre 7).

4.3 Calcul d'équations pour $X_0(m)$

Calcul de Ψ_m

Fixons un entier m et expliquons comment calculer Ψ_m. L'idée de base est simple. Comme on connait les racines de Ψ_m, on peut calculer ses coefficients par l'intermédiaire des sommes de Newton. Les sommes des puissances r-ièmes des racines sont en fait des formes modulaires, qui admettent un développement en q, qu'il suffit de calculer, puis de récrire en fonction de $j(q)$.

Les sommes des puissances r-ièmes des racines de Ψ_m sont données par

$$\Sigma_r = \sum_{A \in \mathcal{S}_m} j(A\tau)^r.$$

Pour simplifier, écrivons le développement de j^r sous la forme :

$$j(q)^r = \sum_{n \geqslant -r} C(n,r) q^n$$

avec les $C(n,r)$ des entiers. On introduit les variables $\zeta_m = \exp(2i\pi/m)$ et $w = q^{1/m}$, ce qui permet d'écrire

$$\exp(2i\pi(a\tau + b)/d) = \zeta_m^{ab} w^{a^2}.$$

On calcule alors les sommes Σ_r avec cette variable w, comme

$$\Sigma_r = \sum_{a,b} \sum_{n \geqslant -r}^{\infty} C(n,r)(\zeta_m^{ab} w^{a^2})^n = \sum_{n \geqslant -r}^{\infty} C(n,r)\alpha_n$$

où

$$\alpha_n = \sum_{a,b} (\zeta_m^{ab} w^{a^2})^n.$$

Ces derniers coefficients peuvent être calculés une fois pour toutes (ils ne dépendent pas de r, mais seulement de m et n). Par la théorie de Galois, les sommes Σ_r sont à coefficients en q. Notons que ces formules se simplifient dans le cas où m est premier (cf. [Mor95]).

Le calcul efficace de ces équations se fait par le calcul de $\Psi_m(X,Y)$ modulo de petits nombres premiers p, en utilisant la FFT pour calculer le produit de séries, puis en remontant par le théorème Chinois. Notons que la hauteur des coefficients de Ψ_m est donnée dans [Coh84].

Donnons deux exemples numériques, calculés à l'aide du système de calcul formel Maple, suivant les algorithmes de [Mor95]. Écrivons

$$\Psi_m(X,Y) = \sum_{r,s=0}^{\mu_0(m)} a_{r,s} X^r Y^s.$$

Commençons par le cas $m = 2$:

$$\Psi_2(X,Y) = X^3 + X^2\left(-Y^2 + 1488\,Y - 162000\right) + X\left(1488\,Y^2 + 40773375\,Y + 8748000000\right)$$
$$+Y^3 - 162000\,Y^2 + 8748000000\,Y - 157464000000000.$$

Dans la littérature, on trouve peu d'exemples de valeurs de Ψ_m pour m composé. On trouvera les coefficients de Ψ_4 dans le tableau 3.1.

Remarque : On peut vérifier les calculs sur Ψ_ℓ, où ℓ premier, en utilisant la relation de Kronecker

$$\Psi_\ell(X,Y) \equiv (X^\ell - Y)(Y^\ell - X) \bmod \ell.$$

$a_{0,0}$	$=$			$2^{12} \times 3^{27} \times 5^{18} \times 11^{9}$
$a_{0,1}$	$=$	$a_{1,0}$	$=$	$-2^{12} \times 3^{25} \times 5^{16} \times 11^{6} \times 389$
$a_{0,2}$	$=$	$a_{2,0}$	$=$	$2^{8} \times 3^{19} \times 5^{12} \times 11^{3} \times 71 \times 127 \times 181243$
$a_{0,3}$	$=$	$a_{3,0}$	$=$	$-2^{9} \times 3^{16} \times 5^{10} \times 389 \times 1669 \times 163199$
$a_{0,4}$	$=$	$a_{4,0}$	$=$	$2^{4} \times 3^{10} \times 5^{6} \times 71 \times 127 \times 181243$
$a_{0,5}$	$=$	$a_{5,0}$	$=$	$-2^{4} \times 3^{7} \times 5^{4} \times 389$
$a_{0,6}$	$=$	$a_{6,0}$	$=$	1
$a_{1,1}$	$=$			$-2^{4} \times 3^{19} \times 5^{13} \times 11^{3} \times 19 \times 164207213$
$a_{1,2}$	$=$	$a_{2,1}$	$=$	$3^{16} \times 5^{10} \times 439 \times 96195947 \times 10627$
$a_{1,3}$	$=$	$a_{3,1}$	$=$	$2^{4} \times 3^{10} \times 5^{7} \times 641 \times 264616561831$
$a_{1,4}$	$=$	$a_{4,1}$	$=$	$2^{5} \times 3^{8} \times 5^{4} \times 41 \times 179 \times 1240081$
$a_{1,5}$	$=$	$a_{5,1}$	$=$	$3 \times 11 \times 17013473$
$a_{2,2}$	$=$			$2^{12} \times 3^{11} \times 5^{6} \times 7 \times 11 \times 107 \times 282653083$
$a_{2,3}$	$=$	$a_{3,2}$	$=$	$-2^{8} \times 3^{7} \times 5^{5} \times 13 \times 787 \times 3769 \times 13553$
$a_{2,4}$	$=$	$a_{4,2}$	$=$	$2^{10} \times 3 \times 5 \times 41 \times 311 \times 7276903$
$a_{2,5}$	$=$	$a_{5,2}$	$=$	$-2^{4} \times 3^{4} \times 5 \times 17 \times 23$
$a_{3,3}$	$=$			$2^{10} \times 5 \times 10729 \times 2441 \times 20359$
$a_{3,4}$	$=$	$a_{4,3}$	$=$	$2^{4} \times 3^{4} \times 5 \times 12495001$
$a_{3,5}$	$=$	$a_{5,3}$	$=$	$2^{5} \times 3 \times 31$
$a_{4,4}$	$=$			$2^{4} \times 3 \times 5 \times 31$
$a_{4,5}$	$=$	$a_{5,4}$	$=$	-1

TAB. 3.1: Coefficients de $\Psi_4(X, Y)$.

Autres approches

Les coefficients des polynômes Ψ_m ont tendance à être énormes et ces polynômes sont donc difficiles à utiliser en pratique. Pour remédier à ce problème, il convient de remplacer la fonction $j(q^m) = q^{-m} + \cdots$ par une fonction f sur $\Gamma_0(m)$, qui ait le plus petit ordre possible à l'infini. C'est ce que décrit Atkin dans [Atk88] (voir également [Mor95, Mül95]). Grâce aux techniques indiquées, il est possible de calculer des modèles de $X_0(\ell)$ pour ℓ premier $\leqslant 1000$. De telles équations sont utilisées dans l'algorithme SEA (voir chapitre 6).

Chapitre 4

Courbes elliptiques sur $\mathbb{C}$ et multiplication complexe

Nous présentons ici les résultats principaux de la théorie de la multiplication complexe. Cette théorie est au cœur d'ECPP (voir chapitre 8). Le calcul d'invariants singuliers (au sens de Weber) a constitué une part importante de ma thèse (voir [AM93a]). J'ai utilisé les formules explicites dans l'article [JM95] pour évaluer certaines sommes de caractères en utilisant les points de $\sqrt{-D}$-division.

Les références pour la théorie présentée ci-dessous sont par exemple [Web02, BCH$^+$66, Lan73, Cox89]. Un excellent exposé historique et synthétique de la théorie et de ses extensions fait l'objet de [Vlă91]. Notons pour l'anecdote que ces résultats sont à la base de formules rapides pour le calcul de π, comme montré d'abord par Ramanujan [Ram14] (voir [BB87, BB88, CC88b, CC89, BB93] pour une présentation moderne et des résultats récents).

Pour démystifier certains des résultats de cette théorie élaborée, nous donnons quelques-unes des démonstrations clefs faciles.

§1. Les théorèmes fondamentaux

Nous conservons les notations du chapitre 3. Fixons un réseau $L = \mathbb{Z} + \tau\mathbb{Z}$ avec $\tau \in \mathcal{H}$. Le réseau L, et par extension la courbe elliptique E associée, sont dits à *multiplication complexe* si le stabilisateur de L, c'est-à-dire l'ensemble $\Sigma(L) = \{\alpha \in \mathbb{C}, \alpha L \subset L\}$ est strictement plus grand que $\mathbb{Z}$ (il contient $\mathbb{Z}$ trivialement). Une caractérisation immédiate d'un tel réseau est la suivante :

Proposition 4.1 *Le réseau L est à multiplication complexe si et seulement si τ est quadratique.*

Démonstration : dire que L est à multiplication complexe revient à dire qu'il existe un nombre complexe $\alpha \notin \mathbb{Z}$ tel que $\alpha L \subset L$. Autrement dit, il existe une matrice

$$\mathcal{M} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

dans $\mathrm{SL}_2(\mathbb{Z})$ telle que

$$\begin{cases} \alpha & = & a + b\tau \\ \alpha\tau & = & c + d\tau. \end{cases}$$

Éliminant α entre ces deux équations, on trouve que τ est algébrique de degré 2

$$b\tau^2 + (a - d)\tau - c = 0$$

puisque $b \neq 0$. On note $K = \mathbb{Q}(\sqrt{-D})$ le corps quadratique correspondant. Il est facile de voir que α appartient au même corps K et que son polynôme minimal est

$$X^2 - (a + d)X + ad - bc = 0$$

ce qui en fait un entier algébrique. □

On note $\mathcal{O}_K$ l'anneau des entiers de K. Rappelons que cet anneau est de la forme $\mathbb{Z}[\omega]$ avec

$$\omega = \begin{cases} \sqrt{-D/4} & \text{si } D \equiv 0 \bmod 4 \\ (1+\sqrt{-D})/2 & \text{si } D \equiv 3 \bmod 4. \end{cases}$$

Corollaire 4.1 *Si L est à multiplication complexe, le stabilisateur $\Sigma(L)$ est un ordre (sous-anneau unitaire) de $\mathcal{O}_K$.*

Théorème 4.1 *La courbe $E = \mathbb{C}/L$ est à multiplication complexe si et seulement s'il existe $m > 1$ tel que $\Psi_m(j(\tau), j(\tau)) = 0$.*

Démonstration : Supposons d'abord que $\Psi_m(j(\tau), j(\tau)) = 0$. Alors, il existe une matrice

$$\mathcal{M} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

tel que $\mathcal{M}\tau = \tau$, ou encore il existe α dans $\mathbb{C}$ tel que

$$\begin{cases} \alpha & = & a + b\tau \\ \alpha\tau & = & c + d\tau. \end{cases}$$

Le nombre α est quadratique et L a multiplication complexe.

Réciproquement, si L est à multiplication complexe par un ordre $\mathcal{O}_K$ d'un corps quadratique imaginaire, on peut trouver $\alpha \in \mathcal{O}_K$ tel que $\mathrm{N}(\alpha) = n > 1$ et tel que $\alpha \notin k\mathcal{O}_K$ pour tout k. Alors $\Psi_m(j(\tau), j(\tau)) = 0$. □

Théorème 4.2 *Si $E = \mathbb{C}/L$ est à multiplication complexe par un ordre $\mathcal{O}_K$ d'un corps quadratique imaginaire $K = \mathbb{Q}(\sqrt{-D})$, alors $j(\tau)$ est un entier algébrique.*

Démonstration : Il suffit de trouver comme précédemment un nombre α dans $\mathcal{O}_K$ tel que $\mathrm{N}(\alpha) = m > 1$ et soit sans facteur carré. C'est toujours possible : si $D = 4$, on prend $\alpha = 1 + i$; si D est sans facteur carré, on prend $\alpha = \sqrt{-D}$. Alors $\Psi_m(j(\tau), j(\tau)) = 0$ et comme m est sans facteur carré, $\Psi_m(X, X)$ est unitaire et donc $j(\tau)$ est un entier algébrique. □

Le théorème le plus important concernant j est le suivant.

Théorème 4.3 *Soit E une courbe elliptique à multiplication complexe par l'anneau des entiers $\mathcal{O}_K$ du corps quadratique imaginaire $K = \mathbb{Q}(\sqrt{-D})$. Soit $\mathcal{CL}$ le groupe des classes de K : $\mathcal{CL} = \{\mathfrak{i}_1, \mathfrak{i}_2, \ldots, \mathfrak{i}_h\}$. Alors pour tout r, $j(\mathfrak{i}_r)$ est algébrique de degré h. Les conjugués de $j(\mathfrak{i}_r)$ sont les $j(\mathfrak{i}_s^{-1}\mathfrak{i}_r)$ pour $s \neq r$. Ces nombres génèrent le corps de classe de Hilbert de K, noté K_H. L'extension K_H/K est galoisienne.*

On pose

$$H_D(X) = \prod_{r=1}^{h} (X - j(\mathfrak{i}_r))$$

que l'on appelera le polynôme de Hilbert de D.

§2. Calcul de $H_D(X)$

La référence pour cette section est [AM93a]. Le calcul de $j(\mathfrak{i}_r)$ se fait de la façon suivante. On peut établir une correspondance entre idéaux du groupe de classes et formes quadratiques primitives réduites (a, b, c) de discriminant $-D = \mathrm{Disc}(K) = b^2 - 4ac$. Rappelons qu'une forme réduite est telle que $|b| \leqslant a \leqslant c$ et $|b| = a$ ou $c = a$ implique $b \geqslant 0$. À une telle forme, on associe le nombre

$$\tau_Q = \frac{-b + \sqrt{-D}}{2a}.$$

On calcule ainsi les $j(\mathrm{i}_r) = j(\tau_{Q_r})$, puis on en déduit les coefficients de $H_D(X)$. Un calcul flottant fait avec assez de précision permet de retrouver des entiers relatifs.

Donnons quelques exemples numériques. On sait qu'il existe seulement 9 corps quadratiques de nombre de classes 1, associés à

$$D \in \{4, 8, 3, 7, 11, 19, 43, 67, 163\}.$$

Dans chacun de ces cas, la seule forme quadratique est la forme principale correspondant à $\tau = \omega$. Il est facile de voir que si $D = 4$, alors E a pour équation $y^2 = x^3 + ax$ et donc $j = 1728$; de même si $D = 3$, l'équation est $y^2 = x^3 + b$ et $j = 0$.

En utilisant `PARI-gp`, on trouve par exemple :

```
? jell(sqrt(-2))
%1 = 7999.9999999999999999999999999999999997 +  0.E-34*i
? jell((-1+sqrt(-7))/2)
%2 = -3374.9999999999999999999999999999999997 + 4.7607521208302644066985565O0 E-35*i
? jell((-1+sqrt(-11))/2)
%3 = -32767.999999999999999999999999999999997 + 3.024317221267492650834535217 E-34*i
? jell((-1+sqrt(-19))/2)
%4 = -884735.99999999999999999999999999999992 + 8.790252716773658870491603423 E-33*i
? jell((-1+sqrt(-43))/2)
%5 = -884735999.99999999999999999999999999995 - 6.855494955875882822065453536 E-29*i
? jell((-1+sqrt(-67))/2)
%6 = -147197951999.99999999999999999999999997 + 1.389874253236849191124949176 E-27*i
? jell((-1+sqrt(-163))/2)
%7 = -262537412640767999.99999999999999999994 + 2.811015236183202207998974020 E-21*i
```

et on peut factoriser les valeurs correspondantes :

D	j_D
8	$(2^2 \times 5)^3$
7	$(-3 \times 5)^3$
11	$(-2^5)^3$
19	$(-2^5 \times 3)^3$
43	$(-2^6 \times 3 \times 5)^3$
67	$(-2^5 \times 3 \times 5 \times 11)^3$
163	$(-2^6 \times 3 \times 5 \times 23 \times 29)^3$

Le fait que ces valeurs soient des cubes d'entiers n'est pas un hasard [GZ85].

L'évaluation rapide de $j(\tau)$ se fait à l'aide des fonctions de Weber. Une approche complémentaire et « orthogonale » consiste à factoriser les polynômes de Weber sur le corps de genre de K. Voir [AM93a] pour ce point. Notons que des améliorations au calcul des invariants de Weber se trouvent dans [YZ97, Haj93b, Haj93a, HV96].

Nous verrons à la section suivante une autre manière de procéder.

§3. Utilisation des polynômes modulaires

On peut identifier certaines valeurs de $j(\tau)$ à l'aide des polynômes modulaires, en appliquant le théorème 4.1 sous la forme :

Proposition 4.2 *Soit E à multiplication complexe par $\mathcal{O}_K$. Si α est un élément de norme m dans $\mathcal{O}_K$, alors $\Psi_m(j(E), j(E)) = 0$.*

Notons un résultat analogue, peu connu (voir par exemple [Sch95a]).

Théorème 4.4 *Soit δ_m le discriminant de $\Psi_m(X,Y)$ par rapport à Y. Les racines de δ_m sont les invariants des courbes E à multiplication complexe par un ordre $\mathcal{O}_K$ dans lequel existe un élément de norme m^2.*

Il est facile de voir que δ_m est de la forme $m^*\mathcal{D}_m(J)$ où m^* est un entier dépendant des facteurs premiers de m et $\mathcal{D}_m(J)$ un polynôme en J. On peut montrer que si m est un nombre premier impair, alors $m^* = (-1)^{(m-1)/2}m$ et $\mathcal{D}_m$ le carré d'un polynôme. Les premières valeurs de δ_m sont :

$$\delta_2(X) = 4\,X^2\,(X-1728)\,(X+3375)^2\left(X^2+191025\,X-121287375\right)^2;$$

$$\begin{aligned}\delta_3(X) = &-27\,X^2\,(X-8000)^2\,(X-1728)^2\,(X+32768)^2\left(X^2-1264000\,X-681472000\right)^2\\ &\times\left(X^2+117964800\,X-134217728000\right)^2\left(X^2-52250000\,X+12167000000\right)^2;\end{aligned}$$

$$\begin{aligned}\delta_4(X) = &-256\,X^4\,(X-54000)^2\,(X-16581375)^2\,(X-1728)^3\,(X+3375)^4\left(X^2+191025\,X-121287375\right)^4\\ &\times\left(X^2-37018076625\,X+153173312762625\right)^2\\ &\times\left(X^4+67515199875\,X^3-193068841781250\,X^2+4558451243295023437500\,X\right.\\ &\left.-6256903954262253662109375\right)^2\\ &\times\left(X^4+13136684625\,X^3-20948398473375\,X^2+172576736359017890625\,X\right.\\ &\left.-1857798902503278435937 5\right)^2\\ &\times\left(X^4+331531596\,X^3-429878960946\,X^2+109873509788637459\,X+20919104368024767633\right)^2.\end{aligned}$$

3.1 Le cas $h = 1$

Considérons maintenant le cas de la multiplication complexe par $\mathbb{Z}[\sqrt{-2}]$. Si E est à multiplication complexe par $\mathbb{Z}[\sqrt{-2}]$, alors il existe une isogénie de degré $\mathrm{N}(\sqrt{-2}) = 2$ entre E et elle-même. Autrement dit l'invariant de E satisfait $\Psi_2(X,X) = 0$. Or

$$\Psi_2(X,X) = -\,(X-1728)\,(X-8000)\,(X+3375)^2.$$

Toutes les racines de $\Psi_2(X,X)$ sont des invariants $j(\tau)$ avec τ un élément de norme 2 dans le corps quadratique associé.

Cherchons quels corps quadratiques imaginaires possèdent des éléments de norme 2. Supposons d'abord $D \equiv 0 \bmod 4$. On doit résoudre

$$u^2 + D/4v^2 = 2$$

ce qui n'est possible que pour $(D/4, u, v) \in \{(1, \pm 1, \pm 1), (2, 0, \pm 1)\}$. Si maintenant $D \equiv 3 \bmod 4$, on trouve que $(D, u, v) \in \{(7, \pm 1, \pm 1)\}$.

Ayant identifié $j = 1728$ comme correspondant à $D = 4$, nous pouvons trouver $j(\sqrt{-2})$ de la façon suivante. L'invariant $j(\sqrt{-2})$ peut se calculer à l'aide du développement (3.1). Posant $q = \exp(2i\pi\sqrt{-2})$, on a

$$j(\sqrt{-2}) = \frac{1}{q} + 744 + \sum_{n \geqslant 1} c_n q^n$$

où les c_n sont des entiers positifs. Mais $q = \exp(-2\pi\sqrt{2}) > 0$ et par suite $j(q) > 0$ et donc $j(\sqrt{-2}) = 8000$.

On retrouve finalement que $j((-1 + \sqrt{-7})/2) = -3375$.

3.2 Quelques cas où $h = 2$

Dans ce cas, on sait que j est de degré 2 et la théorie de la factorisation sur le corps de genre nous indique que j appartient à un corps quadratique réel dont le discriminant est un facteur de D que l'on peut expliciter. Cherchons les invariants des courbes à multiplication complexe par K de discriminant $-D = -15$. On constate qu'il existe une isogénie de degré 4 pour $D = 15$ puisque $1^2 + 15 \times 1^2 = 4 \times 4$. Par suite, en utilisant la factorisation de

$$\Psi_4(X, X) = -2\,(X - 287496)\,(X - 54000)^2\,(X + 3375)^2\,\left(X^2 + 191025\,X - 121287375\right)^2$$

on trouve que le polynôme minimal de $j(\omega)$ est

$$X^2 + 191025\,X - 121287375.$$

Cette méthode d'identification est raisonnable dans les cas les plus simples (D petit). Quand D est grand, elle est clairement inapplicable et l'approche brutale consistant à évaluer numériquement les différents conjugués est la meilleure possible.

§4. Formules explicites pour la multiplication complexe

Soit $L = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ avec $\tau = \frac{\omega_2}{\omega_1} = \omega$ et $\Im(\tau) > 0$. Soit $E = \mathbb{C}/L$ une courbe elliptique à multiplication complexe par $\mathcal{O}_K$. On a [Cox89, §10, C]

Théorème 4.5 *Soit α dans $\mathcal{O}_K$. Alors*

$$\wp(\alpha z) = \frac{F_\alpha(\wp(z))}{G_\alpha(\wp(z))}$$

où F_α et G_α sont deux polynômes de degré respectifs $\mathrm{N}(\alpha)$ et $\mathrm{N}(\alpha) - 1$, à coefficients dans K.

On déduit de cela que

Corollaire 4.2 *La multiplication par α sur E est donnée par*

$$[\alpha](X, Y) = \left(\frac{F_\alpha(X)}{G_\alpha(X)}, \frac{Y}{\alpha}\left(\frac{F_\alpha}{G_\alpha}\right)(X)'\right).$$

La détermination de F_α et G_α peut se faire de plusieurs façons. La méthode de Stark [Sta73] consiste à développer $\wp(\alpha z)$ en fraction continue en $\wp(z)$. On peut aussi utiliser les formules de Vélu à la Dewaghe [Dew95] pour exprimer F_α en fonction de G_α et calculer les coefficients par interpolation.

Une autre approche consiste à deviner les zéros de G_α. Par exemple, si $\alpha = \omega$, on a le résultat suivant.

Théorème 4.6 *Posons $\mathcal{N} = \mathrm{N}(\omega)$. Si $\mathcal{N}$ est impair (i.e., $D \equiv 4 \bmod 8$ ou $D \equiv 3 \bmod 8$), alors*

$$G_\omega(X) = \left(\prod_{s=1}^{(\mathcal{N}-1)/2} \left(X - \wp\left(\frac{s\omega_2}{\omega}\right)\right)\right)^2.$$

Si $\mathcal{N}$ est pair (i.e., $D \equiv 0 \bmod 8$ ou $D \equiv 7 \bmod 8$), alors

$$G_\omega(X) = \left(X - \wp\left(\frac{(\mathcal{N}/2)\omega_2}{\omega}\right)\right)\left(\prod_{s=1}^{\mathcal{N}/2-1} \left(X - \wp\left(\frac{s\omega_2}{\omega}\right)\right)\right)^2.$$

Exemples. Dans le cas $D = 3$, on a $\mathcal{N} = 1$ et par suite $G_\omega = 1$. Dans ce cas, sur $E\ : y^2 = x^3 + 1$, on a

$$[\omega](X, Y) = (\omega X, Y).$$

De même, sur $E\ : y^2 = x^3 + x$, on a

$$[i](X, Y) = (-X, iY).$$

Pour $D = 7$ et $E\ : y^2 = x^3 - 35x - 98$

$$[\omega](X,Y) = \left[\frac{\left(X^2 + (4+\omega)\,X + 21\,\omega + 7\right)(-1+\omega)}{4\,X + 16 + 4\,\omega}, \frac{Y\left(X^2 + (8+2\,\omega)\,X + 7 - 14\,\omega\right)(3+\omega)}{8\,X^2 + 8\,(8+2\,\omega)\,X + 56\,\omega + 112}\right].$$

J'ai utilisé un théorème analogue dans [JM95] pour évaluer des sommes de caractères. Si $h(-D) = 1$ et $D \equiv 3 \bmod 8$, on peut montrer que le corps de décomposition de $G_{\sqrt{-D}}$ est $\mathbb{Q}(\cos(2\pi/D))$, le plus grand sous-corps réel du corps de racines D^{e} de l'unité. Pour d'autres exemples du même type, voir par exemple [DM96]. On renvoie à la section 2.2 du chapitre 8 pour des informations complémentaires.

CHAPITRE 5

Courbes elliptiques sur un corps fini

Les propriétés des courbes elliptiques sur les corps finis sont des propriétés de multiplication complexe. Rappelons que l'endomorphisme de Frobenius ϕ_E associe au point $P = (X, Y)$ de $E(\overline{\mathbb{K}})$ le point (X^q, Y^q), et envoie donc $E(\overline{\mathbb{K}})$ dans lui-même. Cet endomorphisme est inséparable, et donc ne peut être égal à la multiplication par un entier relatif m sur la courbe. D'après le théorème 2.4, l'anneau $\mathrm{End}(E)$ est donc soit un ordre dans un corps quadratique imaginaire, soit un ordre dans une algèbre de quaternion.

Il revient à Hasse d'avoir identifié ces différents cas et à Deuring d'avoir décrit très précisément les deux cas possibles. Le cas le plus courant est celui de l'ordre dans un corps quadratique ; l'autre cas est celui des courbes supersingulières.

Notations : les notations suivantes sont utilisées constamment dans la suite du mémoire : $\mathbb{K}$ est un corps fini de caractéristique p et de cardinalité $q = p^n$. Le cardinal de $E(\mathbb{K})$ s'écrit $m = q + 1 - t$.

§1. Cardinalité de $E(\mathbb{K})$

Les résultats suivants sont très importants. Ils permettent entre autres de classifier les courbes elliptiques à isogénie près sur les corps finis. En effet, deux courbes sont isogènes sur $\mathbb{K}$ si et seulement si elles ont même cardinalité. C'est un cas particulier des résultats de Tate [Tat66].

1.1 Le théorème de Hasse

À l'aide de considérations sur les modules de Tate, on montre que le Frobenius de la courbe E satisfait une équation du type

$$\pi^2 - t\pi + q = 0 \tag{5.1}$$

où t est un entier relatif vérifiant $t^2 - 4q \leqslant 0$. Comme ϕ_E est inséparable, $1 - \phi_E$ est séparable et $\#E(\mathbb{K}) = \#\mathrm{Ker}(\phi_E - 1) = q + 1 - t$. En résumé, on trouve le théorème de Hasse :

Théorème 5.1 *Le nombre de points de $E(\mathbb{K})$ s'écrit $\#E(\mathbb{K}) = q + 1 - t$ avec $|t| \leqslant 2\sqrt{q}$.*

La première démonstration de ce résultat dans [Has33] repose sur l'utilisation de la théorie de la multiplication complexe analytique, l'idée étant de transformer birationnellement la courbe de départ en une courbe définie sur une extension de $\mathbb{K}$, que l'on puisse paramétrer par des fonctions elliptiques particulières. Par la suite Hasse [Has34b] donne une autre démonstration de ce théorème, purement algébrique et utilisant les propriétés du Frobenius. Cette démonstration est reprise par exemple dans [Sil86, Chap. V].

L'équation (5.1) se traduit par le fait que le polynôme $X^2 - tX + q$ a deux racines α et β de module $\sqrt{q}$. Il est facile d'en déduire que le polynôme minimal de ϕ_E^n, c'est-à-dire le Frobenius de

$E/\mathbb{K}_n$, où $\mathbb{K}_n$ est une extension de degré n de $\mathbb{K}$, est alors $(X-\alpha^n)(X-\beta^n)$. On définit alors la fonction dzêta de $E/\mathbb{K}$ par

$$\log Z(E/\mathbb{K},T) = \sum_{n=1}^{\infty}(\#(E/\mathbb{K}_n))T^n/n.$$

Théorème 5.2 *La fonction Z est donnée par :*

$$Z(E/\mathbb{K},T) = \frac{1-tT+qT^2}{(1-T)(1-qT)}.$$

C'est un cas particulier de l'hypothèse de Riemann pour les courbes algébriques, qui a été prouvée par Weil [Wei49], et généralisée par Deligne [Del74].

1.2 Les travaux de Deuring

Le théorème de Hasse représente le premier pas dans la compréhension des propriétés des courbes elliptiques définies sur les corps finis. La connection avec les propriétés du Frobenius montre que l'étude des endomorphismes de E est primordiale.

Faisant suite aux travaux de Hasse, Deuring [Deu41] a décrit complètement les différents types d'anneaux possibles dans le cas des corps finis, en fonction de la séparabilité de l'isogénie duale du Frobenius (voir par exemple [Sil86, V. §3]) :

Théorème 5.3 *Soit $\hat{\phi}_E : E^p \to E$ l'isogénie duale du Frobenius de E. Si $\hat{\phi}_E$ est séparable,* End(E) *est un ordre dans un corps quadratique imaginaire. Si au contraire, elle est inséparable, alors c'est un ordre dans une algèbre de quaternion et la courbe est dite* supersingulière*.*

Une des conséquences de ce théorème est que la p^k-torsion des courbes supersingulières est réduite à $\{O_E\}$, ce qui implique que $p \mid t$.

Deuring ne s'arrête pas là, mais relie les propriétés des courbes elliptiques sur les corps finis aux propriétés des courbes elliptiques à multiplication complexe définies sur $\overline{\mathbb{Q}}$. Deuring établit d'abord des propriétés de réduction de l'anneau des endomorphismes d'une courbe à multiplication complexe dans un corps fini, puis des propriétés de *lifting* d'une courbe elliptique définie sur un corps fini. Expliquons les choses de façon élémentaire (voir par exemple [Lan73, 13, §4] pour une présentation plus rigoureuse).

On a vu au chapitre 4 qu'une courbe E à multiplication complexe par l'anneau des entiers $\mathcal{O}_K$ d'un corps K est définie sur une extension de degré h de $\mathbb{K}$. Si p est un nombre premier, il existe une extension finie de $\mathbb{F}_p$ sur laquelle on peut définir la réduction $\tilde{E}$ de E. Deux cas se présentent : si p est inerte ou ramifié dans $\mathbb{K}$, alors $\tilde{E}$ est supersingulière ; par contre, si p est scindé dans $\mathbb{K}$, alors l'anneau des endomorphismes de $\tilde{E}$ est exactement celui de E.

Deuring montre ensuite que toute courbe elliptique définie sur $\mathbb{F}_q$ peut en fait se remonter (*lifting*) en une courbe à multiplication complexe définie sur $\overline{\mathbb{Q}}$.

De ces travaux, on déduit par exemple le théorème fondamental pour ECPP (voir chapitre 8) :

Théorème 5.4 *Soit p un nombre premier se scindant dans le corps de classe de Hilbert K_H de K. Soit $\mathfrak{P}$ un idéal premier au-dessus de p dans K_H. Alors la courbe E a bonne réduction modulo $\mathfrak{P}$ et de plus $\#(E/\mathfrak{P}) = \mathrm{N}(\pi - 1)$.*

Exemple. Donnons un exemple simple illustrant ce qui précède. La courbe $E : y^2 = x^3 + x$ est à multiplication complexe par $\mathbb{Z}[i]$. Elle se réduit, coefficient par coefficient modulo tout nombre premier p, en une courbe $\tilde{E}$. Si $p \equiv 3 \bmod 4$, p est inerte dans $\mathbb{Z}[i]$ et la courbe $\tilde{E}$ est supersingulière, ce qui implique notamment que son nombre de points est $p+1$. Par contre, si $p \equiv 1 \bmod 4$, p est scindé dans $\mathbb{Q}(i)$, ce qui équivaut à $p = a^2 + b^2$ avec a et b entiers relatifs et la courbe $\tilde{E}$ a $p+1 \pm a$ ou $p+1 \pm b$ points.

1.3 Classes d'isomorphismes de courbes elliptiques

Les travaux de Deuring ont été rafinés et complétés par Waterhouse [Wat69] (voir également [Sch87]). Un des apports importants de cette théorie est la caractérisation des classes d'isomorphismes de courbes elliptiques. On trouve dans [Sch87] cette classification sur tout corps fini $\mathbb{K}$.

Désignons par $H(-D)$ le nombre de classes de Kronecker :

$$H(-D) = \sum_{\substack{d>0 \\ d^2 \mid D \\ -D/d^2 \equiv 0 \text{ } ou \text{ } 1 \bmod 4}} h(-D/d^2).$$

On note $\mathcal{Q}(p) = (p + 6 - 4(-3/p) - 3(-4/p))/12$ le nombre d'ordres maximaux dans l'algèbre de quaternion $\mathbb{Q}_{\infty,p}$, la seule algèbre définie sur $\mathbb{Q}$ et ramifiée seulement en p et ∞.

Soit $N(t)$ le nombre de classes d'isomorphismes de courbes définies sur $\mathbb{K}$ ayant $q+1-t$ points. Si $p \nmid t$, alors la courbe n'est pas supersingulière et se remonte en une courbe à multiplication complexe par un ordre de $\mathbb{Q}(\sqrt{t^2 - 4q})$, et par suite $N(t) = H(t^2 - 4q)$. Dans le cas où $p \mid t$, la courbe est supersingulière, et on connait les valeurs de t permises, ainsi que la structure de $E(\mathbb{K})$ (voir table 5.1). Dans le cas $(*)$, si $q \not\equiv -1 \bmod 4$, toutes les courbes ayant $t = 0$ sont cycliques ; si

n	t	p	$N(t)$	$E(\mathbb{K})$
impair	0		$H(-4p)$	$(*)$
	$\pm\sqrt{3q}$	3	1	cyclique
pair	0		$1-(-4/p)$	cyclique
	$\pm\sqrt{q}$		$1-(-3/p)$	cyclique
	$\pm 2\sqrt{q}$		$\mathcal{Q}(p)$	$\mathbb{Z}/(\sqrt{q} \mp 1)\mathbb{Z} \oplus \mathbb{Z}/(\sqrt{q} \mp 1)\mathbb{Z}$

TAB. 5.1: Classes d'isomorphismes de courbes supersingulières

$q \equiv 1 \bmod 4$, $h(-4p)$ sont cycliques et $h(-p)$ sont isomorphes à $\mathbb{Z}/((q+1)/2)\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

1.4 Compléments sur les courbes supersingulières

On trouvera dans [Sil86, ch. V., §3] les preuves des propriétés que nous énonçons maintenant. On doit à Hasse l'introduction de l'invariant qui porte son nom et qui permet de classifier les courbes supersingulières. Cet invariant $c_p(E)$, qui est proportionnel à un polynôme $S_p(J)$ en $j(E)$, est nul si et seulement si la courbe est supersingulière. On montre alors que $j(E)$ appartient nécessairement à $\mathbb{F}_{p^2}$.

Les racines de ce polynôme $S_p(J)$ sont appelés *invariants supersinguliers*. Le calcul de c_p (ou plutôt de $S_p(J)$) se fait très facilement à l'aide de formules dues à Atkin [Atk88] (voir également [KZ98]). Ces formules utilisent des liens entre invariant de Hasse et séries hypergéométriques (voir par exemple [Hus87] dans le cas de courbes sous la forme de Legendre). Cette connection semble avoir été remarquée pour la première fois par Igusa [Igu58]. Une table des polynômes $S_p(J)$ se trouve dans [BK75, pp. 143–144]. Notons également qu'une autre méthode de calcul est celle de la méthode des graphes [Mes86] (voir également [MO19] pour des compléments à la fois sur la méthode et les propriétés des courbes supersingulières).

Partant de la liste des t possibles de Waterhouse, par exemple, on peut donner des représentants de chaque classe de façon explicite, dans le cas où p est petit. Le cas $p = 2$ est traité dans [MV90a]. Motivé par l'implantation efficace de l'algorithme SEA (voir section suivante), j'ai expliqué dans [Mor97] comment trouver ces équations dans le cas $p \geqslant 3$.

Kohel [Koh96], a donné deux algorithmes qui permettent de trouver quatre endomorphismes indépendants dans $\mathrm{End}(E)$, l'un en temps déterministe $O(p^{3/2+\varepsilon})$ et l'autre probabiliste $O(p^{1+\varepsilon})$ pour tout $\varepsilon > 0$.

§2. Structure de $E(\mathbb{K})$

On déduit du théorème 2.2 que

Proposition 5.1 *Le groupe $E(\mathbb{K})$ est isomorphe au produit de deux sous-groupes cycliques $E_1 \times E_2$, d'ordres n_1 et n_2 tels que $n_2 \mid n_1$.*

On peut en fait démontrer que

Théorème 5.5 *Avec les notations précédentes, on a $n_2 \mid q - 1$.*

La démonstration classique de ce résultat se fait en utilisant le *couplage de Weil* (voir par exemple [Sil86, Ch. III, §8] et chapitre 6). Un entier m étant fixé premier à p, il existe une fonction bilinéaire $e_m : E[m] \times E[m] \to \mu_m$ (l'ensemble des racines m-ièmes de l'unité dans $\overline{\mathbb{K}}$) qui vérifie les propriétés suivantes :

- $\forall P \in E[m]$, $e_m(P, P) = 1$.
- $\forall P, Q \in E[m]$, $e_m(P, Q) = e_m(Q, P)^{-1}$.
- Si $P \in E[m]$, alors $e_m(P, O_E) = 1$. De plus, si pour tout Q dans $E[m]$, $e_m(P, Q) = 1$, alors $P = O_E$.
- Si $E[m] \subset E(\mathbb{K})$, alors $\mu_m \subset \mathbb{K}^*$.

La dernière propriété fournit immédiatement le théorème. Le couplage de Weil peut se calculer assez aisément, voir par exemple [Mil86, Kal88, Men93], ainsi que les chapitres 9 et 6.

Les résultats précédents donnent une caractérisation de tous les groupes possibles. Réciproquement, on peut montrer que tous ces groupes peuvent être effectivement réalisés [Rüc87, Vol88].

§3. Quelques résultats de réduction

Les résultats de Deuring sur la théorie de la réduction des endomorphismes permettent d'analyser la variation de certains paramètres liés aux courbes elliptiques définies sur $\mathbb{Q}$ et réduites modulo p.

3.1 Variation du nombre de points

La courbe E étant fixée, on peut mesurer comment varie $\#E(\mathbb{F}_p)$ quand p premier tend vers l'infini. On pose classiquement $t(p) = 2\sqrt{p}\cos\theta_p$ avec $0 < \theta_p < \pi$. Si E est à multiplication complexe, la distribution de θ_p est uniforme. Si E n'est pas à multiplication complexe, Tate a conjecturé [Tat65] (voir également [LT76]) que pour $0 \leqslant c < d \leqslant \pi$, la densité de nombres premiers p pour lesquels $c \leqslant \theta_p \leqslant d$ existe et vaut

$$\frac{2}{\pi}\int_c^d \sin^2 t \,\mathrm{d}\,t.$$

Des subtilités concernant cette distribution sont décrites dans [McK96]. Birch [Bir68] a étudié un problème voisin, en fixant p et en faisant varier E.

3.2 Réduction supersingulière

On peut s'intéresser à la fréquence avec laquelle la réduction modulo p d'une courbe $E/\mathbb{Q}$ est supersingulière. On appelle $\pi_0(x, E)$ le nombre de nombres premiers $\leqslant x$ ayant cette propriété.

Si $E/\mathbb{Q}$ est à multiplication complexe par un ordre dans $\mathbb{Q}(\sqrt{-D})$, alors

$$\pi_0(x, E) \sim \frac{1}{2} \frac{x}{\log x}$$

puisque E a réduction supersingulière modulo p dès que $(-D/p) = -1$.

Lang et Trotter [LT76] ont conjecturé que si $E/\mathbb{Q}$ n'est pas à multiplication complexe, alors il existe une constante $C_E > 0$ dépendant de E pour laquelle :

$$\pi_0(x, E) \sim C_E \frac{\sqrt{x}}{\log x}.$$

Le premier résultat dans cette direction est dû à Elkies [Elk87] :

Théorème 5.6 *Soit $E/\mathbb{Q}$ une courbe elliptique. Alors il existe une infinité de nombres premiers p pour lesquels E a réduction supersingulière.*

Les nombres premiers p pour lesquels E a réduction supersingulière sont les facteurs des numérateurs des $H_D(j(E))$ où $H_D(X)$ est un polynôme de Weber introduit au chapitre 4. Elkies a montré que pour p fixé, un tel D satisfait $D \leqslant 2p^{2/3}$. Kaneko [Kan89] a montré qu'on pouvait prendre $D \leqslant 4\sqrt{p}/\sqrt{3}$.

La meilleure borne supérieure pour $\pi_0(x, E)$ est due à Elkies [Elk92] et donne $\pi_0(x, E) = O_E(x^{3/4})$. Fouvry et Murty [FM96] (voir également [FM95]) ont prouvé que

$$\pi_0(x, E) > \frac{\log_3 x}{(\log_4 x)^{1+\delta}}$$

pour tout $\delta > 0$ et x assez grand ($\log_k x$ désigne le logarithme itéré k fois de x).

3.3 Résultats sur l'exposant de $E(\mathbb{K})$

Compte tenu des contraintes fortes sur la structure de $E(\mathbb{K})$, on peut se demander quelle est la taille de l'exposant du groupe. Dans cette direction, notons [Sch91b]

Théorème 5.7 *Soit $E/\mathbb{Q}$ une courbe sans multiplication complexe. Il existe une constante $c_E > 0$ telle que*

$$\frac{\operatorname{Exp}(E(\mathbb{F}_p))}{\sqrt{p}} > c_E \frac{\log p}{(\log \log p)^2}$$

pour tout p nombre premier p de bonne réduction.

Ce résultat est faux pour les courbes elliptiques à multiplication complexe. Par exemple, si E est à multiplication complexe par $\mathbb{Z}[i]$ et $p = n^2 + 1$, $n \equiv 0 \bmod 4$, alors $\operatorname{Exp}(E(\mathbb{F}_p)) = n$.

3.4 Cyclicité

On peut se demander quand une courbe est cyclique. Commençons par [Mur83] :

Théorème 5.8 *Si $E/\mathbb{Q}$ est à multiplication complexe, alors le nombre de nombres premiers $p \leqslant x$ tel que $E(\mathbb{F}_p)$ soit cyclique est équivalent à $c_E x/\log x$.*

On trouve des résultats complémentaires dans [GM86]. Le meilleur résultat est le suivant [GM90] :

Théorème 5.9 *Soit $E/\mathbb{Q}$ une courbe elliptique. Le groupe $E(\mathbb{F}_p)$ est cyclique pour une infinité de p si et seulement si E a un point d'ordre 2 non rationnel. Dans ce cas, le nombre de $p \leqslant x$ pour lequel le groupe est cyclique est $\gg x/\log^2 x$.*

CHAPITRE 6

Algorithmes pour les courbes elliptiques sur un corps fini

Ce chapitre rassemble des algorithmes adaptés aux courbes elliptiques sur les corps finis. En dehors de quelques rappels sur le calcul de la loi de groupe, le cœur du chapitre est la présentation de l'algorithme de Schoof, qui permet de calculer la cardinalité de $E(\mathbb{K})$. Ce premier pas accompli, nous évoquons les algorithmes qui déterminent la structure du groupe ou bien celui de l'anneau des endomorphismes de la courbe.

Outre l'application de ces résultats à la primalité (chapitre 8), mon intérêt dans l'algorithme de Schoof vient de son utilisation en cryptographie. Le calcul de $\#E(\mathbb{K})$ est en effet la première tâche à accomplir quand on veut fabriquer un cryptosystème (voir chapitre 9). Mes contributions au sujet sont [CM94, CDM96, Mor95, LM95c, LM95b, LM98].

§1. Calcul de la loi de groupe

En fonction des contextes, il est parfois préférable d'utiliser des paramétrisations différentes d'une courbe elliptique.

Pour la méthode de factorisation ECM (voir chapitre 7), on utilise de nombreuses courbes définies sur $\mathbb{Q}$ et ayant un groupe de torsion le plus gros possible (d'ordre 12 ou 16). Cela conduit à des paramétrisations particulières. On se reportera à [CC86, Mon87] pour de plus amples précisions.

En primalité ou pour faire du chiffrement, on opère sur une courbe elliptique donnée et ces mêmes astuces ne sont en général plus possible. En fonction des machines, on peut soit utiliser la loi de groupe sous sa forme affine (si l'on dispose d'un pgcd rapide) ou bien sous sa forme homogène (si l'on dispose d'une arithmétique modulaire rapide). Notons que l'on utilise rarement la loi de groupe sous forme de fractions en les polynômes de division, sauf dans le cas de l'algorithme de Müller [Mül94].

L'évaluation de $[m]P$ se fait par des méthodes d'exponentiation classiques [Knu81], auquelles on peut ajouter des variantes utilisant le concept de chaînes d'addition-soustraction (voir par exemple mon article avec Olivos [MO90] et ses successeurs [KT92]).

§2. Calcul de la cardinalité : algorithme de Schoof

Nous allons d'abord donner un algorithme simple, puis passer à l'algorithme de Schoof et à ses variantes. En dehors de l'algorithme des pas de bébé et des pas de géant, qui fournit une méthode de temps de calcul $O(q^{1/4})$, il existe un seul algorithme polynomial pour déterminer la cardinalité, celui de Schoof. Les références sur le sujet sont [Sch85, Atk88, Elk91, Sch95a, Mor95, Elk98].

2.1 Présentation

L'algorithme de Schoof [Sch85] utilise les propriétés du Frobenius de la courbe. Supposons que ℓ est un nombre premier impair. La restriction de ϕ_E à $E[\ell]$ satisfait

$$\pi^2 - t\pi + q \equiv 0 \bmod \ell. \tag{6.1}$$

On cherche alors l'unique entier τ, $0 \leqslant \tau < \ell$ tel que

$$(X^{q^2}, Y^{q^2}) \oplus [q](X, Y) = [\tau](X^q, Y^q) \tag{6.2}$$

dans l'anneau $\mathbb{K}[X, Y]/(\mathcal{F}(X, Y), f_\ell(X))$.

Connaissant $t \bmod \ell$ pour suffisamment de ℓ, c'est-à-dire si

$$\prod \ell > 4\sqrt{q}$$

alors on peut reconstruire t par le théorème chinois. Le temps de calcul est clairement polynomial en $\log q$, puisque toutes les opérations à effectuer portent sur des polynômes.

Cependant, les calculs utilisent f_ℓ qui est un polynôme de degré $O(\ell^2)$, et ceci est le point faible de cette approche.

2.2 Les premières améliorations d'Atkin

Dès 1986, Atkin [Atk88] a envisagé d'utiliser les propriétés du polynôme modulaire $\Psi_\ell(X, Y)$ introduit au chapitre 4. Les racines du polynôme $\Phi(X) = \Psi_\ell(X, j(E))$ dans $\overline{\mathbb{K}}$ sont les invariants des courbes elliptiques E/F où F est un sous-groupe cyclique de $E[\ell]$. Le groupe de Galois de Ψ_ℓ étant $\Gamma_0(\ell)$, le polynôme Φ ne peut avoir en général que deux types de factorisation : soit $(11r \ldots r)$ avec $\ell - 1 = rs$, soit $(r \ldots r)$ avec $\ell + 1 = rs$ (il existe deux autres cas assez rares que nous omettons par souci de simplicité). Ces deux cas ont reçu *a posteriori* les noms suivants : dans le premier, ℓ est dit *nombre premier d'Elkies* et dans le second, ℓ est dit *nombre premier d'Atkin*.

Dans les deux cas, r est l'ordre de α/β où α et β sont les racines de l'équation caractéristique

$$\pi^2 - t\pi + q \equiv 0 \bmod \ell$$

et appartiennent donc à $\mathbb{F}_\ell$ si ℓ est d'Elkies (et donc $t^2 - 4q$ doit être un carré modulo ℓ) et dans $\mathbb{F}_{\ell^2}$ sinon (ce qui veut dire que $t^2 - 4q$ n'est pas un carré modulo ℓ). La valeur de r étant connue, il y a $\varphi(r)$ valeurs possibles de $t \bmod \ell$ et dans de nombreux cas, ce nombre est beaucoup plus petit que ℓ. Il reste à combiner ces valeurs de r de façon intelligente, en utilisant un programme de type *match and sort* décrit dans [Atk88].

D'un point de vue pratique, on détermine r en trouvant le plus petit entier tel que

$$X^{q^r} \equiv X \bmod \Phi(X).$$

On peut pour cela utiliser certaines des idées de Shoup [Sho95].

Toujours d'un point de vue pratique, on remplace le polynôme modulaire par des polynômes à coefficients plus petits, comme expliqué au chapitre 3.

2.3 Les améliorations d'Elkies et d'Atkin

L'idée d'Elkies [Elk91] consiste à utiliser de façon plus raffinée les propriétés de l'équation modulaire. En effet, dans le cas où $\Psi_\ell(X, j(E))$ a des racines dans $\mathbb{K}$, cela veut dire qu'il existe une courbe isogène $E^* = E/F$ ainsi qu'une isogénie $I \ : E \to E^*$, de degré ℓ, toutes les deux définies sur $\mathbb{K}$. Une telle isogénie est de la forme :

$$I(X) = \frac{h_\ell(X)}{g_\ell(X)^2}$$

où $h_\ell(X)$ et $g_\ell(X)$ sont des polynômes de $\mathbb{K}[X]$ de degrés respectifs ℓ et $(\ell-1)/2$. Soit $\hat{I}$ l'isogénie duale, qui vérifie $\hat{I} \circ I = [\ell]$. Il est clair que le noyau de I est inclus dans celui de $[\ell]$ est par suite g_ℓ est un facteur de f_ℓ, de degré $O(\ell)$ et non $O(\ell^2)$.

Elkies montre également que les deux sous-groupes cycliques rationnels de $E[\ell]$ sont des sous-espaces propres de la restriction de ϕ_E. Autrement dit, il existe un entier k, valeur propre de ϕ_E, tel que

$$(X^q, Y^q) = [k](X, Y) \bmod (\mathcal{F}(X, Y), g_\ell(X)) \tag{6.3}$$

donnant $t = k + q/k \bmod \ell$. Ce calcul est beaucoup plus rapide à tester que la relation originelle (6.2).

Restent à calculer E^* et I. Dans les cas $\ell \ll p$, Elkies a montré comment utiliser les formules de Vélu [Vél71] et les fonctions de Weierstrass, en exploitant l'interprétation modulaire des courbes elliptiques définies sur $\mathbb{C}$. En bref, on peut trouver l'équation de E^* ainsi que I en utilisant des formules algébriques liant les quantités connues, comme E, $j(E)$, etc. On pourra consulter également [CCR91] pour une autre présentation de ces travaux.

Atkin a amélioré ces idées en utilisant des propriétés plus profondes des fonctions modulaires [Atk92], le conduisant à trouver des formules algébriques dépendant de l'équation modulaire utilisée. Bien que délicates à programmer, ces idées donnent des programmes extrêmement rapides. On pourra consulter [Mor95] pour des compléments aux idées d'Atkin, [Sch95a] pour l'utilisation des équations modulaires standards et [Mül95] pour des formules liées aux opérateurs de Hecke.

Dès que les idées d'Atkin furent publiées, ce fut dès lors la course aux calculs sur des corps premiers de caractéristique de plus en plus grande. Outre l'implantation d'Atkin, on dispose maintenant des travaux [LMMS94, Mor95, Mül95]. Je détiens toujours le record actuel avec le calcul de la cardinalité d'une courbe modulo un nombre premier de 500 chiffres décimaux [Mor95].

2.4 Les améliorations récentes

Quand ℓ augmente, le coût de la recherche de la valeur propre du Frobenius tend à devenir prépondérant. C'est pourquoi Müller a proposé une amélioration significative dans [Mül94]. Notons que cette amélioration est d'autant plus mesurable qu'elle est combinée avec les idées de Dewaghe [Dew98]. Ce sont ces idées qui ont permis mon plus récent record [Mor95].

Nous avons supposé jusqu'à présent que ℓ était premier impair différent de p. Le cas $\ell = 2$ se traite de manière analogue, la seule différence notable étant qu'une isogénie de degré 2 est de la forme $I(X) = h_2(X)/g_2(X)$ avec g_2 de degré 1. Le cas $\ell = p$ est traité dans [LM95b]. De même, une partie de la théorie peut être généralisée au cas des puissances de nombres premiers. Bien que d'importance négligeable dans le coût asymptotique de lálgorithme, cette idée accélère notablement les calculs. La théorie et la pratique des "cycles d'isogénies" est décrite dans [CM94, CDM96].

Une grande partie de la théorie est encore valide dans le cas où p est petit, ce qui est le cas pour les applications cryptographiques qui utilisent $p = 2$. La seule difficulté est liée au calcul de l'isogénie, qui ne peut plus se faire en utilisant les fonctions de Weierstrass. La première solution est due à Couveignes [Cou94] et utilise les groupes formels (voir [Blu98a, Blu98b] pour des compléments sur la méthode). Lercier et moi avons été les premiers à implanter ces idées et cela forme les articles [LM95c, LM95b]. Lercier a développé à partir de cela un nouvel algorithme utilisant des idées différentes qui l'ont conduit à gagner un facteur considérable dans le temps de calcul [Ler96]. Nous détenons ainsi le record[1] pour la caractéristique 2, avec le corps $\mathbb{F}_{2^{1301}}$ (cf. [LM98, Ler97b]). Récemment, Couveignes [Cou96, Cou97] a donné un deuxième algorithme qui évite toute référence explicite au groupe formel, mais utilise les propriétés de la p-torsion en caractéristique p et les extensions d'Artin-Schreier. L'étude et l'implantation de cet algorithme sont encore en cours actuellement, mais les résultats sont prometteurs [Ler97a]. Ces trois algorithmes sont décrits et comparés dans [LM98].

Il reste à comprendre parfaitement où se situe la frontière entre les deux classes d'algorithmes (Elkies-Atkin comparé à Couveignes-Lercier) quand ℓ, p et $q = p^n$ varient. Quelques indications pour cela se trouvent dans [Ler97a].

§3. Algorithmes complémentaires

3.1 Détermination de la structure de $E(\mathbb{K})$

Une fois la cardinalité de $E(\mathbb{K})$ connue, on peut tenter de trouver la structure du groupe $E(\mathbb{K})$. Si la factorisation de $\mathrm{pgcd}(m, q-1)$ est connue, Miller a montré comment on peut déterminer n_1 en temps polynomial probabiliste en utilisant le *couplage de Weil*, introduit au chapitre 5. Notons que si ne l'on ne dispose pas de la factorisation complète de m, il n'est pas possible de trouver un générateur de $E(\mathbb{K})$.

On pourra consulter [Sch95a] pour quelques finesses concernant la détermination exacte de la structure du groupe.

3.2 Détermination de $\mathrm{End}_{\mathbb{K}}(E)$

L'algorithme de Schoof permet de trouver l'équation caractéristique du Frobenius, mais il ne nous donne pas de renseignements sur la classe d'isomorphisme de $\mathrm{End}_{\mathbb{K}}(E)$. Kohel [Koh96], en utilisant des idées proches de celles ces cycles d'isogénies, a donné un algorithme déterministe pour accomplir cette tâche (quand E n'est pas supersingulière), mais dont le temps de calcul est non polynomial et repose sur la véracité d'une hypothèse de Riemman. Notons pour finir que la connaissance de $\mathrm{End}_{\mathbb{K}}(E)$ permet d'obtenir des résultats sur le groupe $E(\mathbb{K}_1)$ si $\mathbb{K}_1$ est une extension finie de $\mathbb{K}$ (voir [Len96]).

[1] Record amélioré par Lercier avec un calcul dans $\mathbb{F}_{2^{1663}}$ en juin 1998 [JL98].

Chapitre 7

Factorisation d'entiers

La méthode de factorisation ECM basée sur les courbes elliptiques a été présentée par H. W. Lenstra, Jr. en 1985 (le 11 février[1]). L'idée s'est répandue comme une trainée de poudre et de nombreuses présentations ont été faites de l'algorithme la même année dans plusieurs contextes, la première communément disponible étant [Ste86]. Des implantations ont rapidement vu le jour et les résultats ne se sont pas fait attendre. Plus important encore que la factorisation d'entiers, cette découverte a provoqué un transfert de technologie massif de tous les algorithmes connus sur les groupes du type $(\mathbb{Z}/N\mathbb{Z})^*$ vers les courbes elliptiques, que ce soit en primalité, factorisation, cryptologie, etc. Elle a aussi stimulé l'étude des courbes de genre supérieur, avec un peu plus de difficulté.

Les papiers fondateurs de la méthode ECM sont [Len86, Len87]. Ma contribution à ce domaine est l'article [AM93b] qui propose de bonnes familles de courbes elliptiques (voir la section paramétrisation). Grâce à ces familles de courbes, Lercier [Ler93] et moi-même avons pu factoriser des nombres du projet Cunningham ou bien des nombres de partitions (voir la dernière section de ce chapitre).

On trouvera un survol sur la théorie dans [Bre90a, Bre90b]. L'article le plus récent est [Bre96].

§1. Présentation de l'algorithme

Pour ce qui va suivre, il est nécessaire de donner un sens à la notion de courbe elliptique modulo un nombre composé.

1.1 Courbes elliptiques sur $\mathbb{Z}/N\mathbb{Z}$: pseudo-addition

Il est possible de définir rigoureusement la notion de courbes elliptiques sur un anneau, en utilisant le "groupe formel" d'une courbe elliptique [Sil86, Ch. IV] et les systèmes d'équations polynomiales décrits dans [LR85]. C'est ce que décrit Lenstra dans [Len86]. Cette présentation est intéressante d'un point de vue théorique, mais est inutilement compliquée pour son application à la factorisation. On se contente généralement d'une définition agréable qui autorise des calculs faciles.

On définit une courbe elliptique modulo N (entier premier avec 6) par

$$E_N = \{\ (x, y, z),\ y^2 z \equiv x^3 + axz^2 + bz^3 \bmod N\ \}$$

dont le discriminant, $\Delta = -16(4a^3 + 27b^2)$, est premier avec N. Soit p un diviseur premier de N. Il est clair que E_p est une "vraie" courbe elliptique. De plus, il est facile de passer de E_N à E_p par réduction : si M est un point sur E_N, on désigne par $M(p)$ sa réduction modulo p.

[1]un lundi.

Nous définissons maintenant sur l'ensemble E_N une “loi”, appelée *pseudo-addition*, qui utilise les formules de calcul de la loi sous forme homogène. Cette loi permet d'additionner deux points P et Q sur E_N, obtenant un point $R = (x_R, y_R, z_R)$. Si $\mathrm{pgcd}(z_R, N) = 1$, alors le point R est tel que $R(p) = P(p) + Q(p)$. Dans le cas contraire, on a trouvé un facteur de N.

1.2 La méthode ECM

On peut résumer cette méthode en disant que c'est un analogue de l'algorithme de factorisation $p-1$ dû à Pollard [Pol74]. On commence par choisir deux entiers v et w. Grosso modo, on cherche à trouver tous les facteurs premiers p de N qui sont plus petits que v et pour lesquels une certaine courbe elliptique a un ordre w-friable, c'est-à-dire que tous les facteurs premiers de l'ordre sont plus petits que w. On choisit ensuite trois entiers a, x_0 et y_0 qui permettent de construire une courbe et un point sur cette courbe.

procedure ECM1(N, v, w, a, x_0, y_0)

1. construire la courbe E d'équation $y^2 = x^3 + ax + b$ avec $b = y_0^2 - x_0^3 - ax_0$;
2. calculer

$$Q = \left(\prod_{\substack{2 \leqslant r \leqslant w \\ r^i \leqslant v + 2\sqrt{v} + 1 < r^{i+1}}} r^i \right) P = (x_Q, y_Q, z_Q)$$

sur E

3. si $\gcd(z_Q, N) \neq 1$ alors on a un facteur de N.

La méthode la plus efficace utilise l'approche précédente avec au plus h courbes, c'est-à-dire avec h triplets (a, x_0, y_0) différents. C'est cette méthode qu'on appelera ECM dans la suite. On verra plus loin comment choisir la valeur de h.

§2. Analyses de la méthode

La méthode ECM trouve un facteur p de N si l'ordre de la courbe $E(\mathbb{F}_p)$ est w-friable et si $\#E(\mathbb{F}_q)$ n'est pas w-friable pour les autres diviseurs premiers q de N. L'analyse d'ECM nécessite donc d'étudier la probabilité que cet ordre soit divisible par un nombre donné M. La probabilité que N soit premier est étudiée dans [Kob88].

Lenstra [Len87, Proposition 1.4], puis Howe [How93] ont étudié la probabilité qu'une courbe ait un ordre divisible par un entier M donné. Les démonstrations utilisent les propriétés des courbes modulaires $X_1(M)$ introduites au chapitre 3. Il apparaît que cet ordre est divisible par M avec une probabilité plus grande que $1/M$ et plus proche de $1/\varphi(M)$. On peut traduire cela en disant que la cardinalité m d'une courbe elliptique a plus de chance d'être divisible par un entier M qu'un nombre au hasard de la même taille que m. Ce genre de raisonnement tend à confirmer que la méthode ECM factorise mieux qu'on ne pourrait s'y attendre.

2.1 Application à ECM

L'analyse se fait en deux temps. Dans un premier temps, on estime la probabilité de succès d'ECM utilisant h courbes. Dans un second temps, on évalue le temps de calcul nécessaire et on optimise celui-ci. On aboutit finalement au résultat suivant, modulo une hypothèse (plausible) de répartition des cardinalités friables dans des petits intervalles :

Proposition 7.1 *La méthode ECM trouve un facteur p de l'entier N en temps moyen $K(p)(\log N)^2$ où $K(x)$ est une fonction vérifiant $\log K(x) = \sqrt{(2+o(1))\log x \log\log x}$ quand x tend vers $+\infty$.*

L'une des raisons du succès tant théorique que pratique de la méthode ECM tient précisément à ce résultat. En effet, la vitesse de l'algorithme dépend essentiellement de la taille du plus petit facteur premier de N et non de N lui-même. En cela, la méthode est proche de la méthode ρ. D'autre part, le cas le pire se produit quand $p \sim \sqrt{N}$. Dans ce cas, le temps de calcul est proche de celui du crible quadratique, mais bien supérieur au crible algébrique [Pom89].

Pour finir, notons que l'algorithme ECM, comme présenté ici, peut servir d'algorithme théorique rigoureux de détection des nombres friables, ce qui permet par exemple d'analyser certains algorithmes de factorisation d'entiers [Pom87a, Len88, HM89, LP92] (voir également [LPP93] pour une généralisation aux courbes hyperelliptiques).

§3. Améliorations pratiques

3.1 Choix de la paramétrisation

La présentation originelle de l'algorithme de Lenstra utilise la paramétrisation de Weierstrass classique, sous forme projective. Dans [CC86], les auteurs ont testé des paramétrisations affines (nécessitant des inversions modulo N), homogènes (un point a pour coordonnées $(X/Z^2, Y/Z^3)$) et projectives. Ils se sont également intéressés aux paramétrisations de Jacobi ou sous la forme Hessienne cubique.

Dans le cas de courbes ayant au moins un point de 2-torsion, on peut trouver des formules homogènes plus simples et plus rapides à évaluer [Mon87].

En fonction des besoins, il est souhaitable de garder une paramétrisation homogène ou rationnelle. La première version permet de diminuer le nombre de pgcd calculés, la seconde est utilisée quand on veut travailler simultanément sur plusieurs courbes à la fois. Tout dépend (jusqu'à un certain point) du rapport de vitesse entre un pgcd et une multiplication modulaire. Nous renvoyons aux références déjà données pour d'autres appréciations.

3.2 Choix des courbes elliptiques

La méthode ECM présente un avantage par rapport à la méthode $p-1$. Il est en effet possible de construire des courbes qui ont une torsion prescrite. On peut construire des familles de courbes elliptiques avec une torsion prescrite, définies sur $\mathbb{Q}$ qui admettent au moins un point d'ordre infini. Des groupes de torsion de cardinal 12 ont été construits dans [Suy] (voir aussi [Mon87]) et nous avons construits des groupes de cardinal 16 dans [AM93b] (voir également [Mon92]), ce qui est le plus grand possible sur $\mathbb{Q}$ d'après [Maz77].

§4. Implantations

La méthode ECM étant du type $p-1$, les améliorations apportées à ce test s'appliquent *mutatis mutandis*. Les références principales dans ce domaine sont [Bre86, Mon87, Bre96] et également [Mon92] pour l'extension FFT, qui demande un peu plus de travail que pour la méthode $p-1$ comme présenté dans [MS90].

Il est rapidement apparu qu'ECM était d'autant plus efficace qu'un grand nombre de courbes était utilisé. Cela se comprend facilement car chaque courbe différente fournit un groupe différent et donc augmente la probabilité de trouver une cardinalité friable. Cela conduit naturellement à distribuer les calculs, ou bien à utiliser des machines parallèles [DL93]. Une analyse pratique des paramètres à utiliser dans les implantations se trouve dans [Mon92] et [SW93]. Des tentatives d'explication heuristique du succès de la méthode sont données dans [McK96].

4.1 Performances ; records

Les performances sont assez intéressantes, car on trouve de manière routinière des facteurs de l'ordre de 10^{15} à 10^{25}. Rien n'indiquait, quand ECM a été annoncée, quelles seraient ses performances en pratique. Les plus grands facteurs trouvés (au 01/09/98) sont donnés dans la table suivante :

taille	N	auteur	date
42	$10^{201}-1$	Rusin	[Mon92]
43	$p(19997)$	Berger	1993
44	$p(19069)$	Müller	21/06/95
47	$5^{256}+1$	Montgomery	27/11/95
48	$24^{121}+1$	Brent	08/10/97
49	$2^{1071}+1$	Zimmermann	24/06/98

Notons également qu'ECM a permis de terminer les factorisations de F_{10} et F_{11} [Bre96].

Deux baromètres permettent de mesurer le succès de la méthode ECM : ce sont les tables des factorisations du Projet Cunningham [BLS$^+$88] et celles du Challenge des Partitions de RSA, inc.

Les récentes mises à jour des tables du Projet Cunningham montrent clairement qu'ECM a permis de trouver de nombreux facteurs des nombres de la forme $b^n \pm 1$, $1 \leqslant b \leqslant 12$. Par exemple, la lettre de Wagstaff, prenant en compte les factorisations trouvées entre le 29/12/94 et le 14/05/95 fait état de 61 factorisations, dont 41 sont dues à ECM, 5 à ppmpqs et 15 à nfs.

Le challenge des partitions, lancé en 1991, consiste à factoriser des listes de nombres de partitions d'indice premier $\leqslant 30000$, considérés comme des nombres aléatoires. Rapporte des points une factorisation *complète* d'un des nombres. Au 18 avril 1996 (qui est pris comme date de référence), seuls ces nombres ayant entre 100 et 176 chiffres décimaux sont pris en considération pour l'attribution de points transformés en dollars chaque fin de trimestre. Parmi les nombres $p(n)$ pour $n \leqslant 24443$, de taille $\leqslant 169$ chiffres décimaux, ce qui fait 1634 nombres, 1295 sont factorisés. Pour 1200 d'entre eux, on dispose des méthodes utilisées (apparemment, les factorisations faciles ne nécessitent pas de commentaires !) : pour 959 d'entre elles, ECM a fourni au moins un facteur, et pour 743 ECM a permis la factorisation complète (modulo les tests de primalité des facteurs).

CHAPITRE 8

Pseudoprimalité et primalité

On peut dire qu'il y a deux types de marché pour les tests de primalité. Dans le premier monde, on cherche à classifier les nombres en donnant des preuves : la rigueur scientifique exige un certificat de primalité, mais on peut prendre son temps pour le trouver. On s'intéresse par exemple à des grands nombres ayant des propriétés données (Mersenne, nombres de partitions, etc.). Depuis l'avènement des systèmes de cryptographie à clefs publiques, il existe un marché pour les générateurs de nombres premiers ≪ aléatoires ≫. Dans ce second monde, on doit générer des nombres probablement premiers à haute cadence, et si possible avec le programme le plus petit possible. L'intérêt est le compromis vitesse/sécurité et on se montre un peu moins exigeant sur les preuves.

Au moment de l'apparition de RSA, on ne disposait que de tests probabilistes de primalité ainsi que de tests de primalité partielle. En 1978 est apparu le premier test tous usages, mais en temps sous-exponentiel, sans certificat, et avec une théorie très élaborée : c'est l'algorithme des sommes de Gauss [APR83], amélioré dans [CL84, CL87, BvdH90b]. Un deuxième algorithme est celui de Goldwasser-Kilian qui utilise les courbes elliptiques et permet de tester presque tous les nombres en temps polynomial [GK86]. Malheureusement, dans sa forme initiale, il est inutilisable, car il repose sur l'algorithme de Schoof[1]. Indépendamment, Atkin a mis au point un algorithme basé sur des idées similaires à celles de Goldwasser et Kilian, mais efficace en pratique, et dont l'étude et l'optimisation ont été la base de ma thèse. Notons que l'algorithme de Goldwasser et Kilian a été généralisé au cas des courbes de genre 2 dans [AH86, AH92], fournissant le premier algorithme de primalité exacte dont le temps de calcul est polynomial probabiliste.

Les tests décrits ci-dessus sont très élaborés, mais aussi très efficaces. Les temps de calcul de ces algorithmes sur des nombres de taille utile sont très raisonnables (moins d'une minute pour ECPP sur des nombres de 100 chiffres décimaux sur DecAlpha). Par contre, si l'on envisage de les implémenter sur une carte à puce, le nombre de lignes de programme est prohibitif. On peut remplacer ces tests sûrs par des tests probabilistes, qui sont plus rapides et plus simples à programmer. Pour mesurer leur taux d'échec, il est nécessaire d'étudier les nombres pseudopremiers, c'est-à-dire ceux déclarés premiers alors qu'ils sont composés.

Depuis 1991, on a assisté à un regain d'intérêt pour les nombres pseudopremiers, conduisant par exemple à l'article majeur [AGP94] (comparer [GM92]). Arnault a construit dans sa thèse [Arn93, Arn95] des nombres composés qui sont déclarés premiers par MAPLE et AXIOM. Ces deux systèmes utilisent tous deux des tests de primalité basés sur les propriétés de $\mathbb{Z}/N\mathbb{Z}$, et donc sur la factorisation de $N-1$. Une voie de recherche consiste à utiliser d'autres groupes – les courbes elliptiques par exemple – associés à d'autres tests. On va voir que là encore on utilise des courbes à multiplication complexe.

[1] Malgré les progrès récents dans l'implantation de cet algorithme, il n'est toujours pas possible de l'utiliser dans le but de prouver la primalité des entiers.

Ce chapitre commence par faire le point sur les nombres pseudopremiers elliptiques, puis on donnera quelques résultats sur l'algorithme ECPP. Ma contribution essentielle à ce domaine est bien sûr celle d'ECPP et en particulier les différents algorithmes auxiliaires qui l'ont rendu extrêmement rapide. Une des applications de mon travail avec Guillaume [GM96] permet également la construction de nombres pseudopremiers elliptiques ayant un grand nombre de facteurs premiers.

§1. Nombres pseudopremiers elliptiques

1.1 Définitions et premiers résultats

Les nombres pseudopremiers elliptiques ont été introduits pour la première fois par Gordon [Gor89b, Gor89a]. Commençons par quelques rappels. Soient p un nombre premier, E une courbe elliptique sur $\mathbb{Z}/p\mathbb{Z}$ et $m = \#E(\mathbb{Z}/p\mathbb{Z})$. On a bien sûr $mP = O_E$. Si E est à multiplication complexe par un ordre $\mathcal{O}_D$, et si p est inerte dans $\mathbb{Q}(\sqrt{-D})$ (c'est-à-dire $(-D/p) = -1$), alors $\#E(\mathbb{Z}/p\mathbb{Z}) = p+1$. Si $h(-D) = 1$, alors E peut être définie sur $\mathbb{Q}$, Un point $P_D = (x, y)$ étant donné sur E, on a donc $(p+1)P_D = O_E$. On suppose dans la suite que D, E_D et P_D sont fixés. Pour éviter des problèmes liés au choix d'une chaîne d'addition pour évaluer $(n+1)P$, on utilise les polynômes ψ_k introduits au chapitre 2. Rappelons que $P \in E(\mathbb{Z}/p\mathbb{Z})$ est d'ordre divisible par k si et seulement si $\psi_k(x, y) \equiv 0 \bmod p$. On a alors la définition suivante.

Définition 8.1 *Un nombre N impair et composé est dit* pseudopremier elliptique *pour* $(E_D, P_D = (x_D, y_D))$ *– en abrégé ppell(E_D, P_D) – si et seulement si $(-D/N) = -1$ et $\psi_{N+1}(x_D, y_D) \equiv 0 \bmod N$.*

Par analogie avec les tests de pseudoprimalité classique, on définit également les nombres *Carmichael elliptique* (cell), qui sont ppell(E_D, P) pour tout P sur E_D. Dans la même veine, on définit les nombres *pseudopremiers elliptiques d'Euler* et les nombres *pseudopremiers elliptiques forts* (ppellf(E_D, P_D)).

1.2 Construction de nombres ppell

Notons que l'on peut construire les nombres ppell de la façon suivante :

Proposition 8.1 *Si pour tout p premier divisant N, on a $p+1 \mid N+1$ et $(-D/p) = -1$, alors N est ppell(E_D, P_D).*

Par analogie avec les nombres pseudopremiers classiques [Rib96], on a

Théorème 8.1 (Gordon) *Si $P = (x_P, y_P)$ est d'ordre infini soit $N = \psi_{2p}(x_P, y_P)/\psi_2(x_P, y_P)$ pour p assez grand. Alors N impair est ppell si $(-D/p) = -1$ et $(-D/N) = -1$.*

Notons que dans le théorème précédent, on peut écrire

$$N = \frac{\psi_{2p}(x_P, y_P)}{\psi_2(x_P, y_P)} = f_p(x_P) f_{2p}(x_P).$$

Auger [Aug93] a remarqué que les N ainsi construits ont presque toujours des facteurs communs avec Δ, le discriminant de la courbe. Il a suggéré de remplacer $f_n(X)$ par

$$\tilde{f}_n(X) = \frac{f_n(X)}{\mathrm{pgcd}(f_n(X), (n\Delta)^{n^2})}$$

pour obtenir

Théorème 8.2 *Avec les notations habituelles, soit* $N = \tilde{f}_p(x_P)\tilde{f}_{2p}(x_P)$ *avec* p *premier tel que* $(-D/p) = -1$ *et* $\operatorname{pgcd}(p, \Delta) = 1$. *Alors* N *est ppell.*

Ce résultat lui a permis de construire quelques nombres ppell assez grands.

Arnault a construit dans sa thèse [Arn93] des nombres ppellf en utilisant des courbes E_D ayant de la 2-torsion rationnelle (en fait dans les cas $D = 4$ ou 8, le cas $D = 7$ n'étant pas abordé). Dans [GM96], nous abordons entre autres la construction de nombres ppell ayant un grand nombre de facteurs premiers.

1.3 Fonctions de comptage

Toujours par analogie, on désigne par $\mathcal{E}(x)$ le nombre de ppell plus petits que x. Gordon [Gor89a] a tabulé tous les nombres ppell plus petits que 10^8 pour les 9 corps quadratiques de nombre de classes 1. Il a également montré, par analogie avec le cas classique

Théorème 8.3 *Le couple* (E, P) *étant fixé, alors* $\mathcal{E}(x) = O(x \log\log x / \log^2 x)$ *sous l'hypothèse de Riemann généralisée.*

Il a de plus conjecturé

Conjecture 8.1 *Le nombre de cell plus petits que* x *est* $xL(x)^{-1+o(1)}$ *avec*

$$L(x) = \exp\{\log x \log_3 x / \log_2 x\}.$$

Le meilleur résultat à ce jour (améliorant les travaux [MM89] et [BM90]) est décrit dans [GP91] et fournit

$$\mathcal{E}(x) \ll xL(x)^{-1/3}.$$

§2. Primalité avec les courbes elliptiques

2.1 Les précurseurs

Dans la foulée des travaux de Lenstra sur la factorisation d'entiers, Bosma [Bos85] a donné des théorèmes de primalité basés sur les courbes elliptiques à multiplication complexe par $\mathbb{Z}[i]$ et $\mathbb{Z}[\rho]$. Dans [CC86], les auteurs anticipent les travaux d'Atkin en utilisant des anneaux d'entiers de nombre de classe 1.

Suite aux travaux de Schoof [Sch85] et de l'annonce de Lenstra [Len87] concernant ECM, Goldwasser et Kilian ont mis au point le premier test de primalité qui teste presque tous les nombres en temps polynomial. Malheureusement, cet algorithme a essentiellement un intérêt théorique, car il est basé sur l'algorithme de Schoof. Malgré les progrès récents dans l'implantation de ce dernier (voir chapitre 6), l'algorithme GK est beaucoup plus lent que l'algorithme ECPP.

Donnons rapidement le schéma de l'algorithme de Goldwasser et Kilian. Le théorème de primalité utilisé est le suivant. Nous en donnons une version faible.

Proposition 8.2 *Soit* E *une courbe elliptique modulo* N *et* $P = (x, y, z)$ *un point sur* E. *Soient* m *et* s *deux entiers tels que* $s \mid m$ *et* $s > (\sqrt[4]{N} + 1)^2$. *On suppose que* $sP = O_E$ *et pour tout* q *premier divisant* s, $(s/q)P = (x_q, y_q, z_q)$ *avec* $\operatorname{pgcd}(z_q, N) = 1$. *Alors* N *est premier.*

procédure GoKi(N) ;
  répéter
    choisir E au hasard et P sur E ;
    calculer $m = \#E$ en utilisant l'algorithme de Schoof ;

si $m = 2N'$ avec N' probablement premier, **alors**
utiliser la proposition 8.2 pour prouver la primalité de N et prouver récursivement la primalité de N' avec GoKi.

Notons que si l'on savait construire facilement des courbes elliptiques d'ordre donné modulo N (ce qui est possible théoriquement, mais difficile en toute généralité, voir chapitre 9), on pourrait alors montrer la primalité de N très facilement. Comme l'a montré Pomerance [Pom87b], il suffirait de savoir construire des courbes elliptiques d'ordre friable (par exemple divisible par une grande puissance de 2).

2.2 ECPP

ECPP a constitué l'essentiel de ma thèse [Mor91b], dont le cœur est l'article [AM93a]. Des références complémentaires sont [Mor90b, Mor92a]. On pourra consulter également [Cox89].

Théorie

L'algorithme est basé sur le théorème suivant, qui complète les théorèmes de multiplication complexe donnés au chapitre 4 ainsi que les résultats de la section 1.2 (en particulier le théorème 5.4).

Théorème 8.4 *Soit $-D$ un discriminant fondamental et p un nombre premier $> D$. Alors p se scinde dans le corps de classe K_H de $K = \mathbb{Q}(\sqrt{-D})$ si et seulement si p est une norme dans K, i.e. $4p = A^2 + DB^2$ avec A et B dans $\mathbb{Z}$. Cette propriété est équivalente au fait que $(-D/p) = +1$ et $H_D(X)$ a une racine j_0 modulo p. Dans ce cas, il existe une courbe elliptique $E/\mathbb{F}_p$ d'invariant j_0 et dont le nombre de points m vérifie $4m = (A-2)^2 + DB^2$.*

L'algorithme ECPP est alors :

procédure ECPP(N) ;
répéter
choisir D tel que $4N = A^2 + DB^2$;
calculer $m = ((A-2)^2 + DB^2)/4$;
si $m = 2N'$ avec N' probablement premier, **alors**
construire la courbe E à multiplication complexe par $\mathcal{O}_K$ à partir d'une racine de $H_D(X) \bmod N$;
utiliser la proposition 8.2 pour prouver la primalité de N et la primalité de N'.

Le calcul des polynômes $H_D(X)$ a déjà été décrit dans le chapitre 4. L'analyse précise d'ECPP n'est pas encore faite. La seule référence à ce sujet est [LL90].

Progrès théoriques récents

La recherche de discriminant convenable se fait en utilisant l'algorithme de Cornacchia [Cor08] que j'avais exhumé du livre de Dickson [Dic52, Tome II, ch. XXIII, p.673]. Depuis l'exposition qui en a été faite avec J.-L. Nicolas dans ma thèse, plusieurs auteurs ont donné des preuves de la validité de l'algorithme [HMW90a, Nit95, Sch95a]. Voir également [HMW90b, Mus92, Wil94, Wil95b] pour des extensions.

Si p se scinde dans K_H, il existe un idéal premier de K_H de degré 1 tel que $\mathfrak{P} \mid p$. Au cours de l'algorithme ECPP, il nous faut connaître l'équation de $E/\mathfrak{P}$ pour pouvoir appliquer le théorème de primalité. Connaissant l'invariant j_0 de $E/\mathfrak{P}$, l'équation de la courbe est déterminée à une tordue près. La solution générale au problème peut se limiter à essayer les deux courbes possibles.

Dans certains cas, on peut trouver une formule exacte pour l'équation de la courbe $E/\mathfrak{P}$ en fonction de l'écriture de p comme norme. J'ai ainsi pu reprendre les travaux de Rajwade *et alii*, qui utilisent une méthode utilisant les points de $\sqrt{-D}$ division. Après avoir prouvé des résultats conjecturés dans ces articles, j'ai pu remplacé des calculs fastidieux de recherche de solutions d'équations diophantiennes par l'utilisation de l'algorithme LLL. Cette approche est décrite dans [JM95] (comparer avec [PV96]). Elle permet de résoudre le cas $h = 1$ et le cas $D = 15$ (pour lequel $h = 2$). Signalons que récemment [Sta96], Stark a résolu le problème complètement pour le cas $(D, 6) = 1$.

Avec Leprévost [LM95a], nous avons pu traiter le cas $D = 20$ comme cas particulier d'application d'un théorème qui permet de construire le revêtement de courbes elliptiques à multiplication complexe par la jacobienne d'une courbe hyperelliptique de genre 2. Les courbes en question ont des paramètres s'exprimant naturellement en fonction des fonctions de Weber.

Les programmes

J'ai réalisé à ce jour trois implantations d'ECPP. La première en `LeLisp` pour ma thèse, les deux autres `C` après ma thèse, de façon à fournir un programme autonome et portable. Le premier programme avait permis de prouver la primalité de plusieurs centaines de nombres, dont une bonne partie du projet Cunningham [BLS$^+$88]. Le deuxième programme m'a permis de tester la primalité du nombre qui constitue toujours le record actuel[2]. Il s'agit du nombre de partitions $p(1840926)$ qui a 1505 chiffres décimaux [Mor92b]. Ce record a bien sûr été établi en utilisant une implantation distribuée. Le programme correspondant est toujours en ftp anonyme à l'INRIA.

Depuis 5 ans, j'ai collaboré à la certification de plusieurs grands nombres premiers. Parmi ceux-ci, citons [KM92]. Dans [Mor92a], j'ai décrit quelques nombres curieux révélés par ECPP. Récemment [Mor96], j'ai utilisé ECPP pour prouver la primalité de facteurs algébriques de $N_p = (2^p + 1)/3$ pour $p \in \{10501, 12391\}$, ce qui m'a permis de prouver la primalité des N_p en utilisant des théorèmes classiques [BLS75].

Il existe quelques traces de l'utilisation de mon programme par d'autres chercheurs : il a par exemple servi à certifier les facteurs de RSA-129 et les facteurs de F_{10} (voir [Bre96]). Voir également [Yan95] pour une autre utilisation.

La troisième version du programme correspond à une récriture du système de librairies que j'ai développé et appelé maintenant FERMAT. Il a bénéficié des retombées des optimisations des algorithmes de pgcd implantés par Lercier [Ler97a]. Des binaires pour cette version sont disponibles sur ma page web[3]. Cette nouvelle version de mon programme est plus rapide, grâce à de nombreuses nouvelles astuces d'implantation [Mor98].

Enfin, j'ai donné une version intermédiaire de mon programme au groupe MAGMA, pour qu'ils l'intègrent à la version 2.2.

Génération de nombres premiers certifiés

C'est là l'application qui avait motivé mes travaux en premier lieu et dont les résultats avaient été esquissés dans [Mor90a]. Grâce à l'augmentation de puissance des machines actuelles, il est possible de générer des nombres premiers certifiés très rapidement. Dans certains cas, c'est une alternative aux méthodes utilisant des nombres de factorisation donnée [Mau95, VZ95].

---

[2] Ce qui était vrai en octobre 1997 ne l'est plus, car le record, porté à 2196 chiffres avec E. Mayer a été battu par Mihailescu [Mih98].

[3] `http ://www.lix.polytechnique.fr/Labo/Francois.Morain.`

À titre d'exemple, on trouvera dans le tableau ci-dessous des temps de certification pour des nombres de taille utilisable en cryptographie. On donne le temps moyen pour 50 nombres premiers, temps en secondes sur une DecAlpha `3000 - M300LX`.

n	temps(s)
128	0.4
256	3.8
512	35.0

Temps de certification pour des nombres premiers de n bits.

CHAPITRE 9

Applications à la cryptologie

Tout cryptosystème construit sur $\mathbb{F}_q$ peut être transposé sur une courbe elliptique définie sur $\mathbb{F}_q$. La sécurité des algorithmes ainsi construits repose soit sur la difficulté de calculer le logarithme discret sur les courbes, soit sur la difficulté de factoriser un nombre composé dans le cas de systèmes construits sur $\mathbb{Z}/N\mathbb{Z}$.

L'avantage d'utiliser les courbes elliptiques est que le logarithme discret y est bien plus difficile en général. La conséquence est qu'à sécurité égale, les paramètres recommandés sont plus petits que dans le cas des corps finis, ce qui résulte en une moins grande quantité de données à stocker et parfois en un gain de temps (voir par exemple [HMV93]).

Nous vivons actuellement une phase de transition pendant laquelle les cryptosystèmes elliptiques tentent de détrôner les algorithmes déjà en place, alors même que le commerce électronique frémit et s'apprête à faire une percée fulgurante sur les réseaux. La bataille fait rage actuellement entre CERTICOM et RSA par exemple, pour savoir lequel des deux systèmes (courbes elliptiques ou bien RSA) sera utilisé dans les protocoles SET de Visa et Mastercard. D'un autre côté, l'IEEE (voir [MQV]) propose de normaliser l'utilisation des courbes elliptiques en cryptographie publique (projet P1363).

En tout état de cause, il serait présomptueux d'affirmer que les cryptosystèmes elliptiques sont plus robustes dans l'absolu que leurs précurseurs. Ceux-ci peuvent se prévaloir d'une résistance de 20 ans alors que ceux-là n'ont pas encore subi l'épreuve du feu d'une utilisation massive par le grand public.

Dans ce chapitre, nous allons donner des indications sur le problème du logarithme discret et faire un bref survol des cryptosystèmes proposés, ainsi que des résultats de complexité théorique obtenus par Maurer. Une section est consacrée à la fabrication de "bonnes" courbes elliptiques. C'est dans ce domaine que se trouve ma participation à la cryptologie, en plus de mes travaux sur la génération de nombres premiers certifiés. Dans [Mor91a], j'ai expliqué comment utiliser la multiplication complexe et dans [LM95c] (voir également [Ler97b]), nous avons décrit l'optimisation de l'algorithme de Schoof pour la construction de courbes.

Une bonne référence pour ce chapitre est [Men93].

§1. La difficulté du calcul du logarithme discret

Nechaev [Nec94] et Shoup [Sho97] ont tous deux donné des bornes inférieures sur le temps de calcul du logarithme discret dans des cas restrictifs qui correspondent peu ou prou au cas des courbes elliptiques. Dans le cas où on ne s'autorise qu'une seule loi de groupe, alors la meilleure attaque est nécessairement celle des pas de bébé et des pas de géant.

Menezes, Okamoto et Vanstone ont décrit la première attaque non triviale du problème. Ils ont établi une réduction entre le logarithme discret sur une courbe et le logarithme discret sur un corps fini. Les références sont [MOV90, MOV91, MOV93] (voir aussi [Men93]). On peut résumer cette approche en disant que le problème du logarithme discret sur une courbe elliptique se réduit au calcul du logarithme discret sur une extension du corps de base, au moyen du couplage de Weil. Dans le cas des courbes elliptiques supersingulières, le degré de cette extension est très petit, ce qui fournit un algorithme de calcul du logarithme discret en temps sous-exponentiel. Ces courbes sont donc à proscrire.

1.1 Le problème

Soit $E/\mathbb{F}_q$ une courbe elliptique de type (n_1, n_2) avec $n_2 \mid n_1$. Ces deux nombres peuvent être déterminés en temps polynomial probabiliste si la factorisation de $\mathrm{pgcd}(m, q-1)$ est connue, en utilisant l'algorithme de Miller (voir chapitre 5). On suppose d'autre part que $m = \#E(\mathbb{K})$ est premier avec q, ce qui implique que $E[n_1] \simeq \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_1\mathbb{Z}$. Soit P un point d'ordre $n \mid n_1$ sur E et R un point du sous-groupe engendré par P, que nous noterons $< P >$. Le problème est de trouver ℓ, $1 \leqslant \ell < n$, tel que $R = \ell P$. Ce problème se pose par exemple quand R est intercepté lors d'un protocole de type Diffie-Hellman.

Les seuls algorithmes connus pour résoudre directement le problème, sont celui de Pohlig-Hellman si m est friable et celui de Pollard dans le cas général. Dans ce cas, le temps de calcul est $O(\sqrt{m})$. Une implantation de cet algorithme est décrite dans [HMV93][1].

1.2 La réduction MOV

La réduction proposée utilise de façon essentielle le couplage de Weil. Voici l'algorithme. On suppose que P est un point d'ordre n de E et que $R \in < P >$:

procédure MOV(E, P, n, R)

1. soit k le plus petit entier tel que $E[n] \subset E(\mathbb{F}_{q^k})$;
2. trouver Q dans $E[n]$ tel que $\alpha = e_n(P, Q)$ est d'ordre n ;
3. calculer $\beta = e_n(R, Q)$;
4. calculer ℓ comme le logarithme discret de β en base α dans $\mathbb{F}_{q^k}$.

On a donc réduit le problème du logarithme discret sur E à celui du logarithme discret dans $\mathbb{F}_{q^k}$. Si le degré k n'est pas trop grand, alors le temps de calcul est sous-exponentiel en $\log q$ par les méthodes connues [Pom90].

Une condition nécessaire sur k est $q^k \equiv 1 \bmod n$ (dans le cas où $(q, n) = 1$), ce qui montre qu'en général k est grand. La condition est également suffisante comme montré dans [BK98].

1.3 Le cas des courbes supersingulières

Remarquons que le cardinal d'une telle courbe étant $q + 1 - t$ avec $p \mid t$, on a $\mathrm{pgcd}(m, q) = 1$ et donc l'algorithme donné précédemment s'applique.

On sait d'après [Wat69], que le Frobenius ϕ d'une courbe supersingulière vit dans une extension de degré au plus 6 du corps de base. Autrement dit, $\phi^k = \mathrm{Id}$ pour un $k \leqslant 6$. Si n est un entier, on en déduit que $X^{q^k} = X \bmod f_n(X)$. Cela équivaut à $E[n] \subset E(\mathbb{F}_{q^k})$. Les valeurs de k sont connues précisément, voir [Wat69] et les tables données dans [MOV90, MOV91, MOV93, Men93].

[1] Voir aussi la dernière section de ce chapitre.

1.4 Les courbes anormales

Il existe des courbes pour lesquelles la réduction ne peut pas marcher. Ce sont les courbes “anormales” ayant q points en caractéristique p. Le couplage de Weil est toujours trivial sur ces courbes, puisque tous les points sont dépendants (parce que $E[q] \simeq \mathbb{Z}/q\mathbb{Z}$).

Il est facile de générer de telles courbes en utilisant la multiplication complexe. C'est ce qu'ont fait Koblitz [Kob92] dans le cas $q = 2^n$ et Miyaji [Miy93b] dans le cas $q = p$. Comme l'a montré Koblitz, l'un des avantages de telles courbes est que l'on peut accélérer les calculs d'exponentiation en utilisant les propriétés du Frobenius (voir également [MS93]).

Malheureusement, plusieurs auteurs, indépendamment ont trouvé un algorithme de calcul du logarithme discret sur ces courbes, qui fonctionne en temps polynomial [Sma97, SA97, Sem98].

§2. Cryptosystèmes

2.1 Cryptosystèmes sur un corps fini

Algorithmes basés sur le logarithme discret

Les premières traductions des cryptosystèmes classiques sont dues à Miller [Mil87] pour le protocole de Diffie et Hellman ; Koblitz [Kob87] pour le système de Massey-Omura et celui d'El Gamal. Miyaji [Miy93a] a généralisé l'algorithme de Schnorr [Sch91a] (voir [Miy96] pour des développements récents).

Autres algorithmes

Kaliski [Kal87] a construit un générateur aléatoire de bits basés sur les courbes elliptiques sur $\mathbb{F}_p$ et a étendu ses résultats à la fabrication de fonctions *one-way* [Kal91] utilisant des courbes elliptiques cycliques. Une construction de telles courbes a été donnée dans [Mor91a] en utilisant une variante de l'algorithme ECPP. L'article [MS93] contient la généralisation de la théorie des permutations au cas de $\mathbb{F}_{2^n}$.

Koblitz [Kob91] a décrit l'utilisation de courbes elliptiques d'ordre premier pour implanter des *blobs*, appliquant les idées de [BKK90].

2.2 Cryptosystèmes basés sur $\mathbb{Z}/N\mathbb{Z}$, N composé

Les schémas

Dans [KMOV91], les auteurs proposent un système (appelé KMOV), utilisant la loi de groupe sur $E(\mathbb{Z}/N\mathbb{Z})$ avec $N = pq$ composé, et qui permet de faire uniquement la signature. L'article [OFF93] généralise le schéma d'Okamoto [Oka90]. Demytko [Dem94] a proposé d'utiliser E et sa “tordue” pour chiffrer et déchiffrer. Koyama [Koy95] propose d'utiliser une courbe elliptique singulière. Smith et Boyd [SB95] ont généralisé l'algorithme de McCurley [McC88]. Meyer et Müller [MM96] ont récemment généralisé KMOV ; casser leur système est équivalent à factoriser N et le chiffrement est plus rapide que le déchiffrement.

Les attaques

On a longtemps cru que les attaques du type de celle de Hastad [Hås86] ne s'appliquaient pas aux algorithmes KMOV et Demytko. Il n'en est rien, comme l'ont montré les auteurs de [KOT95]. Remarquons que cette attaque marche également dans le cas de [Koy95].

De même, on peut employer contre KMOV le même genre d'attaque que pour RSA, quand par exemple la clef de déchiffrement est trop petite (attaque de Wiener [Wie90] généralisée par Pinch [Pin95]), ou bien qu'on connait une partie du message (attaques à la Coppersmith [Cop96, CFPR96] détaillée par Bleichenbacher [Ble97]).

Dans RSA, on peut construire de fausses signatures de la façon suivante : si un attaquant veut faire signer m, il fait signer $s' = (mr^e)^d$ et construit $s'r^{-1}$. Dans le cas de Demytko, cela ne semblait pas possible, puisqu'à partir de x_i et x_j, on ne peut pas construire facilement x_{i+j}. Récemment, Kaliski [Kal95] a remarqué qu'à partir de x_i, x_j et x_{i-j} il est possible de calculer x_{i+j} facilement (en utilisant la loi de groupe). C'est en fait une généralisation de la méthode de Bleichenbacher, Bosma et Lenstra [BBL95].

Conclusion

Les systèmes basés sur des courbes elliptiques définies sur $\mathbb{Z}/N\mathbb{Z}$, N composé, ne présentent pas beaucoup d'intérêt par rapport à RSA, sauf peut-être l'inexistence de l'attaque par homomorphisme dans le cas du schéma de Demytko[2].

§3. Implantations et performances

Les premières implantations logicielles datent des années 1990 : [BC90, MV90b, HMV93]. Des implantations *hardware* sont décrites dans [AMV93].

Signalons pour finir qu'étant donnée la technologie actuelle, un corps $\mathbb{F}_{2^n}$ avec $155 \leqslant n \leqslant 200$ est conseillé. Une implémentation *hardware* des opérations de bases sur des courbes elliptiques dans ce corps est décrite dans [AMV93]. Une implantation *software* est donnée dans [SOOS95] et la conclusion de cet article laisse apparaître qu'à sécurité égale, l'implantation du protocole de Diffie-Hellman est dix à vingt fois plus rapide sur une courbe elliptique définie sur ce corps que sur $\mathbb{Z}/p\mathbb{Z}$ avec p de 512 bits.

§4. Construction de bonnes courbes

Nous ne parlerons pas ici de la construction de courbes supersingulières, qui est assez facile et n'est pas intéressante à cause de la réduction MOV (voir toutefois [BC90, MV90b, Lay94, Mor97]).

Pour qu'une courbe résiste à MOV, une condition nécessaire est que le plus petit entier k tel que $q^k \equiv 1 \bmod m$ soit le plus grand possible. Une façon de réaliser cela est d'imposer que $\varphi(m)$ ne soit pas B-friable pour une certaine borne B, ce qui implique $k \geqslant B$. Une variante de ECPP permet alors de réaliser cette tâche [CTT94]. Une autre façon de résister à MOV est d'utiliser des courbes anormales comme indiqué plus haut.

Si l'on n'impose pas grand-chose sur l'ordre de la courbe, par exemple qu'il soit simplement friable ou premier, on peut bien sûr se contenter d'utiliser l'algorithme de Schoof, à cause des améliorations indiquées plus haut et grâce auxquelles les temps de calcul sont maintenant raisonnables (comparer [MV93] et [LM95c, Ler97b] – noter que [MV93] contient des tables de courbes).

Une autre méthode de construction de courbes est envisageable pour des corps $\mathbb{F}_{p^n}$ si n est composé. Supposons que $n = kl$ avec k petit. On construit d'abord une courbe sur $E/\mathbb{F}_{p^k}$ et on

[2]Et bien non, cf. [Joy97] que l'on consultera de façon plus générale pour les attaques récentes contre certains protocoles.

calcule son ordre facilement puisque le corps est petit. On calcule alors le cardinal de $E/\mathbb{F}_{(p^k)^l}$ à l'aide du théorème de Weil. Cette méthode est décrite dans [BS92].

Dans bien des cas pourtant, on souhaiterait trouver une courbe de cardinal donné pour un corps donné. Cela n'est pas possible dans l'état actuel de la technologie. On présente plusieurs solutions alternatives, qui suffisent dans la pratique et utilisent généralement la multiplication complexe.

4.1 Construire une courbe d'ordre donné pour un corps donné

On a vu dans le chapitre 5 que pour presque tout t permis par le théorème de Hasse, il existe une courbe elliptique définie sur $\mathbb{K}$ et ayant $q+1-t$ points. Ce résultat est malheureusement non effectif. En dehors des cas où E est supersingulière (cas pour lesquels on peut calculer facilement des courbes elliptiques d'ordre donné [Mor97]), la théorie de la multiplication complexe nous dit que E est à multiplication complexe par l'anneau des entiers de $\mathbb{Q}(\sqrt{-D})$ avec $-D = t^2 - 4q$. La courbe E est définie sur une extension de degré $h(-D)$. Si $h(-D)$ est petit, il est possible de construire E en utilisant la machinerie développée pour le test de primalité ECPP dans le cas $q = p$ [Mor91a] et généralisée au cas des corps finis dans [LZ94, CHTT95]. Dans le cas général, cet algorithme est exponentiel, en $O(\sqrt[4]{q})$.

Remarquons que la résolution de ce problème en temps polynomial fournirait un algorithme de primalité polynomial grâce à l'idée de Pomerance déjà relatée au chapitre 8.

4.2 Courbe d'ordre donné

Considérons le problème

Étant donné m, trouver q et une courbe E sur $\mathbb{F}_q$ ayant m points.

Pour résoudre ce problème, on peut utiliser la théorie de la multiplication complexe en étendant l'approche de [Mor91a]. Dans le cas $q = p$, on cherche à construire un corps quadratique imaginaire de petit nombre de classes dans lequel m est la norme d'un entier $\pi - 1$. Reste à espérer que π est un nombre premier. Le cas $q = 2^b$ est abordé dans [LZ94] et requiert la connaissance de corps quadratiques de nombre de classes 2^b. Notons que pour représenter m par une norme, il est nécessaire de connaître la factorisation de m.

4.3 Courbe cyclique sur $\mathbb{K}$

On peut utiliser les résultats de Deuring [Deu41], Waterhouse [Wat69] et Schoof [Sch87] si l'on souhaite trouver des courbes elliptiques cycliques supersingulières. Dans le cas des courbes ordinaires, on peut utiliser une variante de l'algorithme ECPP qui interdit les nombres de points pour lesquels $\mathrm{pgcd}(m, p-1) > 1$. C'est ce qui est fait dans [Mor91a].

4.4 Courbe d'ordre friable

Ce problème est évoqué dans [LZ94] pour le cas $q = 2^n$ pour certaines valeurs de n. Plus précisément, n est choisi comme étant le nombre de classes d'un corps quadratique imaginaire K dans lequel 2^n est la norme de π. On teste alors si $\mathrm{Norme}(\pi - 1)$ est de la forme souhaitée.

§5. Les travaux de Maurer

Généralisant l'approche de den Boer [dB90], Maurer (voir [Mau94] ainsi que [MW96] pour des extensions à d'autres groupes et [BL96] pour des résultats voisins) a montré que le cassage de l'algorithme de Diffie-Hellman pour un groupe cyclique G de générateur g est équivalent à la résolution du problème du logarithme discret si l'on dispose d'un oracle qui, étant données les deux quantités g^x et g^y, retourne g^{xy}.

Remarquons dès à présent que cet oracle permet en fait de calculer $g^{f(x)}$ pour toute fraction rationnelle f à coefficients entiers.

Considérons pour simplifier le cas où $\#G = p$ est un nombre premier et soit $E/\mathbb{F}_p$ une courbe elliptique cyclique dont l'ordre soit friable et de générateur $P = (u, v)$. Supposons que l'on veuille trouver le logarithme de $a = g^x$ dans G. On fait l'hypothèse que x est l'abscisse d'un point sur la courbe. On peut calculer l'ordonnée y de ce point par application de l'oracle, en résolvant

$$g^{x^3+ax+b} = g^{y^2}.$$

Comme E est cyclique, il existe k tel que $(x, y) = kP$. Si l'on trouve k, on peut alors en déduire x. Pour ce faire, on remarque que étant donnés (g^{u_1}, g^{v_1}) et (g^{u_2}, g^{v_2}) sur E, on peut calculer le couple (g^{u_3}, g^{v_3}) où $(u_3, v_3) = (u_1, v_1) + (u_2, v_2)$ sur E. On utilise alors l'algorithme de Shanks pour trouver k.

§6. Addenda

Cette section contient des mises à jour et recense quelques articles parus depuis la soutenance.

6.1 Compléments sur le logarithme discret

Le 6 novembre 1997, Certicom a lancé un concours de cassage de logarithmes discrets, en proposant sur sa page WEB[3] des « exercices ». À ce jour, seuls les premiers exercices ont été résolus. Le plus grand corps utilisé a une taille de 97 bits et il a fallu 2×10^{14} opérations sur la courbe elliptique.

Théorie

D'un point de vue théorique, Zuccherato [Zuc98] a montré l'équivalence entre le calcul du logarithme discret sur les courbes elliptiques et la recherche de l'infrastructure d'un corps de fonction quadratique, en caractéristique 2. Malheureusement, calculer l'infrastructure semble à peu près aussi difficile que le problème de départ.

Pratique

La seule méthode d'attaque réaliste utilisable pour casser un logarithme discret dans le cas général (courbe ordinaire) est la méthode ρ de Pollard, de préférence utilisée en parallèle à la van Oorschot et Wiener [vOW94], donc avec une complexité $O(\sqrt{q}/m)$ où m est le nombre de processeurs utilisés. Les avancées récentes portent surtout sur la diminution de la constante du grand O.

Teske [Tes98] a proposé quelques améliorations concernant la méthode ρ de Pollard pour le calcul du logarithme discret. Il s'agit ici de remplacer la fonction proposée par Pollard par une fonction plus élaborée. Le résultat principal est une amélioration de la constante dans $O(\sqrt{q})$.

Dans le cas des courbes binaires anomales à la Koblitz [Kob92, Sol97], c'est-à-dire des courbes définies sur $\mathbb{F}_2$ et remontées dans $\mathbb{F}_{2^m}$, il est également possible d'améliorer la constante [GLV98, WZ98].

[3] Voir `http ://www.certicom.com/`

6.2 Contributions diverses

Vanstone et Zuccherato [VZ97] ont proposé un système de chiffrement qui utilise une courbe elliptique dans $\mathbb{Z}/N\mathbb{Z}$ avec $N = pq$ et $\#E(\mathbb{Z}/p\mathbb{Z})$ et $\#E(\mathbb{Z}/q\mathbb{Z})$ friables simultanément. Les auteurs proposent de fabriquer E comme composée de deux courbes modulo p ou q avec multiplication complexe « facile » (par exemple $y^2 = x^3 + ax$ ou $y^2 = x^3 + b$). La fabrication donnée en exemple conduit malheureusement à des N faciles à factoriser [Cop98].

Dans [KK98], il est montré que compter le nombre de points sur une courbe définie sur un anneau $\mathbb{Z}/N\mathbb{Z}$ est équivalent à factoriser N.

CHAPITRE 10

Courbes elliptiques et codes

Mes activités de recherche m'ont amené à fréquenter la théorie des codes, sans pour le moment aller plus loin. Dans ce chapitre, j'expose quelques idées de théorie des codes liées aux courbes algébriques. La théorie des codes est présentée dans l'incontournable [MS77], le classique [vL82] ou encore le très pédagogique [PW95].

De même, la théorie des codes géométriques est abondamment décrite dans de nombreux livres, à commencer par celui de Goppa [Gop91], et aussi [Mor91c, Sti93, TV91, JvdG88]. Plus récemment, le numéro spécial des IEEE Transactions on Information Theory (volume 41, numéro 6, 1995), fait le point sur tous les aspects du domaine. Pour les quelques pages qui suivent, je me suis fortement inspiré de présentations un peu plus anciennes, à savoir [Wol86] et [Per89]. Pour des survols de la théorie, voir également [Mic89] qui contient une bibliographie importante sur le sujet, ainsi que [vL90].

En dehors de l'utilisation des courbes elliptiques comme exemple non trivial dans la réalisation de codes de Goppa géométriques, les courbes elliptiques ont été utilisées pour énumérer les poids de mots de codes dans certains cas particuliers. Je conclus ce chapitre en indiquant brièvement comment les courbes elliptiques sont utilisées dans la recherche de codes MDS.

§1. Quelques rappels de la théorie des codes

1.1 Définitions et premières propriétés

Soit $\mathbb{K} = \mathbb{F}_q = \mathbb{F}_{p^n}$ un corps fini. Un *code C de longueur n* sur $\mathbb{K}$ est un sous-ensemble de $\mathbb{K}^n$. La *distance de Hamming* de deux mots $x = (x_1, x_2, \dots, x_n)$ et $y = (y_1, y_2, \dots, y_n)$ de C est définie par

$$d(x,y) = \#\{i, x_i \neq y_i\}.$$

La *distance minimale* de C est la plus petite des distances $d(x,y)$ de deux éléments x et y distincts de C. Un code de distance minimale d permet de corriger $\lfloor (d-1)/2 \rfloor$ erreurs.

Le *poids* de $x \in C$ est défini par $w(x) = d(x,0)$; c'est le nombre de composantes non nulles de x.

Un *code linéaire* (n,k,d) est un sous-espace vectoriel C de $\mathbb{K}^n$ de dimension k et de distance minimale d. Il est clair que $d = \min_{x \in C, x \neq 0} w(x)$ pour un tel code. Un code linéaire C est généralement décrit par sa matrice génératrice G, c'est-à-dire par une matrice $n \times k$ dont les lignes forment une base de C. Le codage d'un mot $a = (a_1, a_2, \dots, a_k)$ se fait en calculant

$$x = (x_1, x_2, \dots, x_n) = (a_1, a_2, \dots, a_k)G.$$

1.2 Bornes

Deux paramètres permettent de caractériser les performances d'un code : il s'agit du *rendement* k/n et du *taux de correction* d/n. Ces deux quantités vérifient la *borne de Singleton* :

$$\frac{k}{n} + \frac{d}{n} \leqslant 1 + \frac{1}{n}. \tag{10.1}$$

Cette inégalité montre que les deux quantités ne peuvent être grandes en même temps. Les codes réalisant l'égalité dans cette relation sont appelés MDS (*maximum distance separable*). Un des axes de recherche dans la théorie des codes est la maximisation de k/n et/ou d/n.

On peut chercher aussi à caractériser l'ensemble $\mathbb{U}_q$ des paires de réels (a, b) pour lesquels il existe une famille de codes linéaires $(C_i)_{i\in\mathbb{N}}$ de paramètres (n_i, k_i, d_i) pour lesquels n_i tend vers l'infini et d_i/n_i tend vers a et k_i/n_i tend vers b. Une caractérisation importante de $\mathbb{U}_q$ est donnée par Manin [Man81].

Théorème 10.1 *Il existe une fonction continue décroissante* $\alpha_q : [0,1] \to [0,1]$ *telle que* $\alpha_q(0) = 1$, $\alpha_q(\delta) = 0$ *pour* $\delta \in [(q-1)/q, 1]$ *et*

$$\mathbb{U}_q = \{(a,b), 0 \leqslant a \leqslant 1, b \leqslant \alpha_q(a)\}.$$

La fonction α_q n'est pas connue explicitement, mais on connait une borne supérieure, appelée borne de Plotkin. Si $0 \leqslant \delta \leqslant q-1$

$$\alpha_q(\delta) \leqslant 1 - \frac{q}{q-1}\,\delta. \tag{10.2}$$

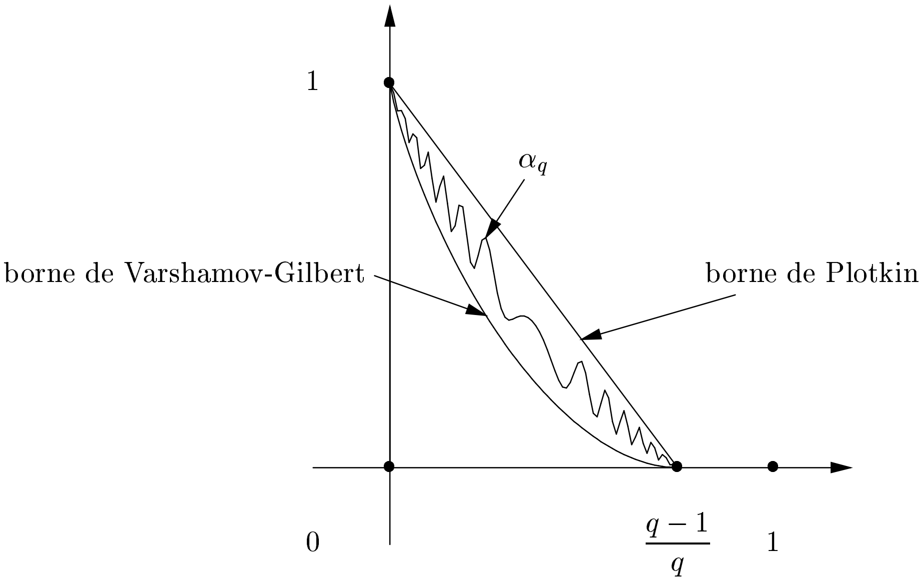
Un minorant de α_q est donné par la borne de Varshamov-Gilbert : si $0 \leqslant \delta \leqslant (q-1)/q$, on a

$$\alpha_q(\delta) \geqslant 1 - H_q(\delta) \tag{10.3}$$

où H_q est la fonction d'entropie :

$$H_q(\delta) = \delta \log_q(q-1) - \delta \log_q \delta - (1-\delta)\log_q(1-\delta).$$

Il est classique de représenter toutes ces fonctions sur un graphique.



Il existe d'autres bornes que nous ne présentons pas ici. On peut les trouver dans [MS77, vL82].

§2. Codes géométriques

Goppa donne un moyen de construire des codes linéaires basés sur une courbe $\mathcal{C}$ de genre g définie sur $\mathbb{K}$ et ayant au moins n points. Les outils utilisés sont les espaces de formes différentielles et le théorème de Riemann-Roch. Pour chaque entier a, $0 < a < n$, il est possible de construire un code linéaire de paramètres (n, k, d) vérifiant

$$k \geqslant a - g + 1, d \geqslant n - a.$$

On en déduit ainsi que

$$\frac{k}{n} + \frac{d}{n} \geqslant 1 + \frac{1}{n} - \frac{g}{n}. \tag{10.4}$$

Notons que ces bornes ont été améliorées dans [DM85].

2.1 Des courbes avec beaucoup de points

La relation (10.4) montre immédiatement l'intérêt de trouver des courbes $\mathcal{C}$ qui ont beaucoup de points par rapport à leur genre. On appelle classiquement $N_q(g)$ le nombre maximum de points d'une courbe de genre g dans $\mathbb{F}_q$ (nous reviendrons plus loin sur les valeurs connues de $N_q(g)$). On pose

$$A(q) = \limsup_{g \to +\infty} \frac{N_q(g)}{g}.$$

En utilisant la borne de Weil, on a

$$N_q(g) \leqslant q + 1 + \lfloor 2g\sqrt{q} \rfloor$$

et Serre [Ser83] a donné

$$N_q(g) \leqslant q + 1 + g\lfloor 2\sqrt{q} \rfloor.$$

On a

Théorème 10.2 (Tsfasman) *L'intersection de la droite d'équation $x + y = 1 - 1/A(q)$ et du carré $[0, 1] \times [0, 1]$ est contenue dans $\mathbb{U}_q$.*

On remarque alors que si

$$A(q) > \frac{1}{\log_q((2q - 1)/q)}, \tag{10.5}$$

alors il existe une famille de codes dépassant la borne VG.

La valeur de $A(q)$ est mal connue. Après les travaux de Ihara, Tsfasman, Vlăduţ et Zink [TVZ82], on sait que (voir paragraphe suivant pour quelques explications) :

Théorème 10.3 *Si q est un carré, alors $A(q) = \sqrt{q} - 1$.*

On en déduit alors que si $q \geqslant 49$, la relation (10.5) est satisfaite. Quand q n'est pas un carré, les résultats sont loins d'être complets. Le lecteur curieux est renvoyé à l'excellent survol [GS95a].

Construction de codes

La construction conduisant au théorème 10.3 peut être présentée comme suit. Si N est un entier et p un nombre premier ne divisant pas N, la courbe $X_0(N)$ (introduite au chapitre 3) a bonne réduction modulo p et même genre $g(N)$. On peut montrer que le nombre de points de $X_0(N)$ sur $\mathbb{F}_{p^2}$ vaut asymptotiquement, quand N augmente, $g(N)(p-1) \sim g(N)\sqrt{p^2}$ et donc $A(p^2) \geqslant p-1$. Il est alors possible d'étendre ce résultat au cas p^{2m}.

Des constructions explicites de ces codes ont été entreprises. Par exemple, un algorithme permettant de construire des codes basés sur les courbes modulaires est donné dans [MV85] (voir aussi [TV91]). Le livre [Mor91c] consacre un chapitre entier à cette construction.

Récemment [GS95b], des codes ont été construits en utilisant des courbes définies sur des extensions d'Artin-Schreier ; il y a quelques mois, Elkies a montré que ces courbes sont en fait des courbes modulaires $X_0(2^r)$ et $X_0(3^r)$. De plus amples références sont données dans le volume exceptionnel des IEEE (volume 41, numéro 6, 1995).

Pour finir, notons que pendant longtemps, le problème du décodage de ces codes était considéré comme très difficile, voire impossible. Toutefois, dès 1988, des techniques de décodage ont commencé à voir le jour et les premiers algorithmes effectifs commencent à être optimiser. Le lecteur, là encore, est renvoyé au survol [HP95].

Retour à $N_q(g)$

D'après Waterhouse [Wat69], on sait que

$$N_q(1) = q + \epsilon(q) + \lfloor 2\sqrt{q} \rfloor$$

avec $\epsilon(q) = 0$ si $q = p^m$ avec m impair $\geqslant 3$ et $p \mid \lfloor 2\sqrt{q} \rfloor$ et $\epsilon(q) = 1$ sinon. Il est facile de fabriquer des courbes elliptiques sur $\mathbb{F}_q$, q carré, atteignant la borne $N_q(1)$. En effet, dans ce cas, les courbes elliptiques sont supersingulières et on peut les expliciter aisément [Sho92b].

La valeur de $N_q(2)$ est connue, mais le cas $g > 2$ reste en grande partie obscur. Pour certaines valeurs particulières de g, on connait des courbes atteignant la valeur maximale donnée par la borne de Weil [Lac87, Wol87, Wol89b]. Pour plus d'information, nous renvoyons à [Ser83, GS95a].

2.2 Codes basés sur les courbes elliptiques

La combinaison de (10.1) et (10.4) montre immédiatement que si $g = 0$, le code associé est MDS. Dans le cas $g = 1$, il est possible de caractériser les codes MDS issus de courbes elliptiques [DM86, DM87, Sho92c, Mun93]. La construction explicite de codes géométriques elliptiques sur $\mathbb{F}_{2^m}$ est décrite dans [Dri86, DM86, DM87]. Un algorithme de décodage de ces codes est donné dans [Dri86], mais il ne corrige que $d/4$ erreurs. Cet algorithme est supplanté par les travaux récents (voir par exemple [HP95]).

§3. Distribution de poids de codes classiques

L'énumération des poids des mots de certains codes cycliques se fait souvent en évaluant des sommes de caractères dans des corps finis (voir par exemple [BM72]). Ces sommes de caractères peuvent à leur tour être interprétées comme des nombres de points sur des courbes algébriques. Les résultats esquissés ci-dessous dans le cas particulier des courbes elliptiques se trouvent dans [LW87, Wol89d, Wol89c, KL89, LW90, SvdV91]. Notons que ces résultats ont été redécouverts indépendamment dans [vdG91].

Une exploitation plus approfondie des liens entre courbes algébriques et codes cycliques est donnée dans [Wol87, Wol89a] où sont considérées des courbes de la forme $y^q - y = f(x)$ (voir aussi [vdGvdV92c]). Des liens entre courbes supersingulières et codes sont donnés dans [vdGvdV92b, vdGvdV92a] (voir également [Sch95b]).

Liens avec les sommes de Kloosterman

Plaçons-nous dans $\mathbb{K} = \mathbb{F}_{2^m}$ et notons la trace de x par

$$\mathrm{Tr}(x) = x + x^2 + x^{2^2} + \cdots + x^{2^{m-1}}.$$

La somme de Kloosterman est définie pour $a \in \mathbb{K}^*$ par

$$K(a) = \sum_{x \in \mathbb{K}^*} (-1)^{\mathrm{Tr}(x^{-1} + ax)}.$$

L'évaluation des sommes $K(a)$ permet d'énumérer les poids des mots contenus dans les orthogonaux de certains codes cycliques (Melas, Goppa étendus).

Le nombre $K(a)$ est relié au nombre de points sur la courbe $\mathcal{K}_a \ : y^2 + y = x^{-1} + ax$ par la formule :

$$\sum_{x \in \mathbb{K}^*} (1 + (-1)^{\mathrm{Tr}(x^{-1} + ax)}) = q + 1 + K(a).$$

Comme la courbe $\mathcal{K}_a$ est isomorphe à la courbe elliptique

$$y^2 + xy = x^3 + a,$$

les travaux de Deuring permettent de déduire de la formule précédente le

Théorème 10.4 *L'ensemble des $K(a)$ pour a parcourant $\mathbb{K}^*$, est l'ensemble de tous les entiers $s \equiv -1 \bmod 4$ dans l'intervalle $[-2^{(t/2)+1}, 2^{(t/2)+1}]$.*

Notons que des sommes de Kloosterman plus générales sont étudiées dans [vdGvdV91].

3.1 Géométrie finie

Soit $PG(2, q)$ le plan projectif de $\mathbb{F}_q$. On appelle $(n\ ; m)$-arc un ensemble de n points dont au plus m se trouvent sur une même droite et m au moins sur une droite. L'une des questions qui se posent est de déterminer quand un $(n\ ; m)$-arc est une courbe algébrique irréductible de degré m. Le cas des courbes elliptiques est le cas de $m = 3$ et il est traité dans [HV98].

Notons qu'on peut étendre la notion d'arc aux espaces projectifs $PG(k-1, q)$. On appelle alors n-arc un ensemble de n points dont au plus $k-1$ se trouvent dans un même hyperplan. Il est possible de montrer (voir par exemple [Hir95] et les références données) l'équivalence entre l'existence d'un n-arc et d'un code linéaire C de paramètres $[n, k, n-k+1]$ (un code MDS donc).

D'autres utilisations des courbes elliptiques en géométrie finie se trouvent dans [Ugh88, Kee88].

Chapitre 11

Applications diverses

Ce chapitre contient des utilisations diverses des courbes elliptiques dans les corps finis, ce qui permet de boucler le tour d'horizon de l'utilisation des courbes elliptiques dans les corps finis.

§1. Formules de multiplication optimales

Soit K un corps and L/K une extension de degré fini n de K. On considère L comme espace vectoriel sur K. Soit L^* le dual de L. On définit le rang $R(L/K)$ par

$$R(L/K) = \min\{r \in \mathbb{N}, \exists u_i, v_i \in L^*, \exists w_i \in L, \forall a, b \in L, ab = \sum_{i=1}^{r} u_i(a)v_i(b)w_i\}.$$

C'est ce qu'on appelle la complexité bilinéaire de la multiplication dans L/K.

On sait d'après [de 83] que $R(L/K) \geqslant 2n-1$ avec égalité si et seulement si $\#K \geqslant 2n-2$. Les algorithmes optimaux réalisant cette borne sont des algorithmes d'interpolation [Win79] opérant sur la droite projective de $\mathbb{F}_q$.

Les Chudnovsky [CC88a] ont généralisé cette construction en remplaçant la droite projective par des courbes algébriques bien choisies. Spécialisant au cas des courbes elliptiques, Shokrollahi [Sho92d] a montré que l'algorithme des Chudnovsky fournit le rang exact $2n$ pour des extensions $\mathbb{F}_{q^n}/\mathbb{F}_q$ si $\frac{1}{2}q+1 < n < (q+1+\varepsilon(q))/2$ où

$$\varepsilon(q) = \begin{cases} \text{le plus grand entier} \leqslant 2\sqrt{q} \text{ premier avec } q & \text{si } q \text{ n'est pas un carré} \\ 2\sqrt{q} & \text{si } q \text{ est un carré.} \end{cases}$$

Un exemple détaillé de calcul dans le cas $\mathbb{F}_{256}/\mathbb{F}_8$ est donné dans [BS91]. Une méthode générale de production d'un algorithme optimal est donné dans [Sho92a] pour $\mathrm{pgcd}(q,6) = 1$ et le cas $2 \mid q$ ou $3 \mid q$ est traité dans [SW92].

§2. Calcul d'intégrales algébriques

Le problème de l'intégration des fonctions algébriques est un des sujets de recherche importants du calcul formel. Étant donnée une courbe $\mathcal{C}/\mathbb{Q}$ et une fonction h de $\mathbb{Q}(\mathcal{C})$, on cherche à savoir si l'intégrale $\int h(x)\mathrm{d}x$ est élémentaire ou non. Les premiers pas dans la résolution de ce problème ont été faits par Risch [Ris70]. Il existe deux types d'algorithmes basés sur ces idées [Dav81] et [Tra84]. Le premier utilise des séries de Puiseux et l'algorithme de Coates [Coa70]. Le second utilise des calculs sur les diviseurs de la jacobienne $Jac(\mathcal{C})$, représentés par des polynômes. Les opérations de base sont essentiellement des calculs sur des matrices de polynômes.

Dans le cas général, l'algorithme de Risch-Trager, comme implanté par exemple dans MAPLE ou AXIOM, est très lent. Dans le cas où C est hyperelliptique, c'est-à-dire $C\ : y^2 = f(x)$ avec par exemple f de degré impair, il est possible d'accélérer les calculs considérablement, comme indiqué dans [Ber95]. Bertrand y explique comment on peut utiliser une représentation plus simple des diviseurs due à Cantor [Can87]. Un des problèmes à résoudre est celui de la recherche de l'ordre d'un diviseur sur la courbe. Cela se fait par réduction modulo un nombre premier bien choisi.

Le cas particulier des courbes elliptiques est traité et simplifié dans [vH94].

§3. Factorisation de polynômes

La méthode de factorisation $p-1$ a un analogue dans le cas de la factorisation de polynômes. Il en est de même pour ECM. Nous présentons ici brièvement ces deux analogies.

3.1 Corps finis de cardinal friable

Soit $K = \mathbb{F}_q = \mathbb{F}_{p^\ell}$ le corps fini à q éléments. On suppose q impair et $q-1 = \prod_{i=1}^r p_i^{a_i}$. Soit $f(X)$ un polynôme à coefficients dans $\mathbb{K}$. La décomposition de $f(X)$ s'écrit $f(X) = f_1(X)^{e_1} \cdots f_r(X)^{e_r}$.

Le premier, Moenck [Moe77] a montré comment factoriser rapidement et de façon déterministe un polynôme $f(X)$ modulo p si $p-1 = L \times 2^l$ avec $L \approx \log p$ et si on possède une racine primitive modulo p. Cette approche a été généralisée par von zur Gathen [Gat87]. On désigne par $S(m)$ le plus grand facteur premier de l'entier m.

Théorème 11.1 *Soit $f(X)$ un polynôme de degré d sur $\mathbb{F}_{p^\ell}$ et $n = \max(d, \ell, \log p, S(p-1))$. Si on dispose d'une racine primitive modulo p, alors on peut trouver un facteur de $f(X)$ avec $O(n^8)$ bit-opérations, de façon déterministe.*

Un théorème analogue est prouvé dans [MS88]. L'idée de la méthode est la suivante. Supposons pour simplifier que pour tout i, $e_i = 1$. On pose $\mathbb{K}_i^* = \{b \in \mathbb{K}, b^{p_i} = 1\}$ pour tout i. On tire alors parti de l'isomorphisme

$$\mathbb{K}^* \simeq \mathbb{K}_1^* \times \cdots \times \mathbb{K}_r^*$$

en écrivant :

$$f(X) = \prod_{(a_1,\ldots,a_r)\in\mathbb{K}_1^*\times\cdots\times\mathbb{K}_r^*} \mathrm{pgcd}(f, X^{(q-1)/p_1} - a_1, \ldots, X^{(q-1)/p_r} - a_r).$$

On factorise f en factorisant récursivement tous les $\mathrm{pgcd}(f, X^{(q-1)/p_i} - a_i)$ pour tout i et tout a_i dans $\mathbb{K}_i^*$. Ceci ne peut se faire rapidement que si les p_i sont petits.

Rónyai a amélioré le théorème 11.1 en montrant qu'une racine d'ordre $p_1 p_2 \cdots p_r$ suffit (voir [Rón89a]). Notons que Shoup a donné un meilleur temps de calcul dans [Sho91].

3.2 Utilisation de courbes elliptiques d'ordre friable

Rónyai [Rón89b, Rón92] a donné un algorithme de factorisation de $f(X)$ dans le cas $q = p$ en utilisant des courbes elliptiques friables. Plus précisément, soit E la courbe d'équation $y^2 = x^3 + ax + b$ définie sur $\mathbb{F}_p$ et $C = \#E(\mathbb{F}_{p^2})$. On suppose que $C = p_1^{e_1} \cdots p_r^{e_r}$ et $t = \max(p_i)$. Rónyai utilise la propriété suivante :

Propriété : $\mathbf{P}_{\leqslant D}$: pour tout nombre premier $r \leqslant D$, on dispose de deux polynômes F_r et G_r tels que F_r soit un facteur du r-ième polynôme cyclotomique dans $\mathbb{K}$ et $\deg(G_r) < \deg(F_r)$ est tel que $b_r = G_r \bmod F_r$ est un non-résidu d'ordre r dans $\mathbb{K}[X]/(F_r)$.

Notons qu'à l'heure actuelle, cette condition ne peut être satisfaite en temps polynomial que si GRH est vraie (cf. [Hua85]).

Théorème 11.2 *On suppose que* $\mathbf{P}_{\leqslant 2t^6}$ *est satisfaite. Alors on peut trouver les facteurs de* f *en temps* $O(t+d+\log p)^{O(1)}$ *à l'aide de la courbe* E.

§4. Calcul d'isomorphismes entre corps finis

On considère le corps fini $\mathbb{K} = \mathbb{F}_q = \mathbb{F}_{p^n}$ représenté de deux façons différentes par deux polynômes irréductibles de degré n, notés $f(X)$ et $g(Y)$. Pour simplifier, notons $\mathbb{K}_1 = \mathbb{F}_p[X]/(f(X))$ et $\mathbb{K}_2 = \mathbb{F}_p[Y]/(g(Y))$. Il s'agit de trouver un isomorphisme ϕ entre ces deux corps.

L'idée de Pinch [Pin92] est la suivante : pour trouver ϕ, il suffit d'être capable d'identifier deux éléments de même ordre dans les deux représentations du corps.

Le premier cas explicité est celui où $q-1$ a un petit diviseur premier r. On appelle α un élément de $\mathbb{K}_1$ et β élément de $\mathbb{K}_2$, tous les deux d'ordre r. Il est clair que α est envoyé par ϕ sur un élément d'ordre r de $\mathbb{K}_2$ et donc sur une puissance de β, soit $\phi(\alpha) = \beta^s$ pour $1 \leqslant s \leqslant r-1$. Si A et B_s sont les deux matrices de α et β^s dans leurs bases canoniques respectives

$$\begin{pmatrix} 1 \\ \alpha \\ \alpha^2 \\ \cdots \\ \alpha^{n-1} \end{pmatrix} = A \begin{pmatrix} 1 \\ X \\ X^2 \\ \cdots \\ X^{n-1} \end{pmatrix}$$

et

$$\begin{pmatrix} 1 \\ \beta^s \\ \beta^{2s} \\ \cdots \\ \beta^{(n-1)s} \end{pmatrix} = B_s \begin{pmatrix} 1 \\ Y \\ Y^2 \\ \cdots \\ Y^{n-1} \end{pmatrix}$$

alors la matrice de ϕ est simplement $A^{-1}B_s$. On en déduit alors $\phi(X)$ comme un polynôme en Y. Il ne reste plus qu'à tester que $g(\phi(Y)) = 0$ dans $\mathbb{K}_2$. Un exemple numérique est traité dans l'article en référence.

Dans le second cas, on remplace le groupe $\mathbb{K}^*$ par une courbe elliptique $E(\mathbb{F}_p)$ définie sur le corps premier et qui a un point d'ordre r petit. On identifie alors les abscisses des points d'ordre r dans les deux corps. Les détails sont donnés dans l'article.

Chapitre 12

Conclusion

J'ai décrit dans ce mémoire les applications de la théorie des courbes elliptiques sur les corps finis à la résolution de problèmes algorithmiques variés, incluant la factorisation et la primalité d'entiers, la construction de cryptosystèmes résistants, la fabrication de bons codes. J'ai participé de près ou de loin à la majeure partie des avancées faites dans ce domaine. Les courbes elliptiques ont apporté des améliorations aussi bien qualitatives (meilleures complexités connues pour certains problèmes) que quantitatives (programmes performants de primalité ou de calcul de la cardinalité par exemple). Ces travaux s'intègrent naturellement à la grande œuvre de recherche de méthodes effectives de calcul sur les courbes algébriques, aussi bien dans les corps de nombres que dans les corps finis.

Ces avancées théoriques débouchent aujourd'hui sur des réalisations pratiques insoupçonnées à l'origine. En effet, l'utilisation des courbes elliptiques comme substitut aux groupes classiques est très à la mode, comme le montrent les efforts de normalisation et de promotion de Certicom. Nul doute qu'une partie au moins de mes travaux pourra être valorisée dans le monde industriel.

Tous les résultats obtenus dans le cas des courbes elliptiques se transposent en grande partie au cas des courbes de genre supérieur, à commencer par le cas du genre 2 ou celui un peu plus général des courbes hyperelliptiques. Dans le cas de $\mathbb{Q}$, les premiers algorithmes de calcul du rang, torsion, etc. commencent à apparaître (voir par exemple le survol [Poo96] et l'indispensable [CF96]). Dans le cas des corps finis, les algorithmes existent en grande partie sur le papier, mais leur implantation efficace est encore en devenir.

Dans le cas de la primalité, Adleman et Huang ont obtenu le premier test de primalité probabiliste polynomial [AH86, AH92] ; Lenstra, Pila et Pomerance ont analysé la généralisation de la méthode ECM aux courbes de genre 2 [LPP93] (méthode HECM). La cryptologie n'est pas en reste, avec les articles [Kob89] et [OS92]. Le calcul du nombre de points est abordé dans [AH86, AH92, Pil90]. Spallek a utilisé la multiplication complexe pour construire des cryptosystèmes [Spa94]. Ses travaux ont été étendus récemment par van Wamelen [vW97].

À part le cas de Spallek, aucune implantation efficace de ces algorithmes n'est connue. Tous ces thèmes fournissent autant de sujets de recherche théorique et algorithmique pour lesquels l'investissement théorique que j'ai fait dans le cas du genre 1 commence à être récompensé.

Bibliographie

[Adl80] L. M. Adleman. A subexponential algorithm for the discrete logarithm problem with applications to cryptography. In *Foundations of computer science*, 1980.

[AGP94] W. R. Alford, A. Granville, and C. Pomerance. There are infinitely many Carmichael numbers. *Ann. of Math. (2)*, 139(3):703–722, May 1994.

[AH86] L. M. Adleman and M.-D. A. Huang. Recognizing primes in random polynomial time. In *Proceedings 19th STOC*, pages 462–469. ACM Press, 1986. New-York City, May 25–27, 1987.

[AH92] L. M. Adleman and M.-D. A. Huang. *Primality testing and Abelian varieties over finite fields*, volume 1512 of *Lecture Notes in Math.* Springer–Verlag, 1992.

[AH94] L. Adleman and M.-D. Huang, editors. *ANTS-I*, volume 877 of *Lecture Notes in Comput. Sci.* Springer-Verlag, 1994. 1st Algorithmic Number Theory Symposium - Cornell University, May 6-9, 1994.

[AM93a] A. O. L. Atkin and F. Morain. Elliptic curves and primality proving. *Math. Comp.*, 61(203):29–68, July 1993.

[AM93b] A. O. L. Atkin and F. Morain. Finding suitable curves for the elliptic curve method of factorization. *Math. Comp.*, 60(201):399–405, January 1993.

[AMV93] G. B. Agnew, R. C. Mullin, and S. A. Vanstone. On the development of a fast elliptic curve cryptosystem. In R. A. Rueppel, editor, *Advances in Cryptology – EUROCRYPT '92*, volume 658 of *Lecture Notes in Comput. Sci.*, pages 482–487. Springer-Verlag, May 1993.

[APR83] L. M. Adleman, C. Pomerance, and R. S. Rumely. On distinguishing prime numbers from composite numbers. *Ann. of Math. (2)*, 117:173–206, 1983.

[Arn93] F. Arnault. *Sur quelques tests probabilistes de primalité.* Thèse, Université de Poitiers, December 1993.

[Arn95] F. Arnault. Rabin-Miller primality test: composite numbers which pass it. *Math. Comp.*, 64(209):355–361, January 1995.

[ARS78] L. M. Adleman, R. L. Rivest, and A. Shamir. A method for obtaining digital signatures and public-key cryptosystems. *Comm. ACM*, 21(2):120–126, 1978.

[Art24] E. Artin. Quadratische Körpern im Gebiet der höheren Kongruenzen, I, II. *Math. Z.*, 19:153–246, 1924. See also *The collected papers of Emil Artin*, edited by S. Lang and J. T. Tate, Addison-Wesley, 1965, pp. 1–94.

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

[Atk92] A. O. L. Atkin. The number of points on an elliptic curve modulo a prime (II). Draft. Available on `http://listserv.nodak.edu/archives/nmbrthry.html`, 1992.

[Aug93] V. Auger. *Primalité et courbes elliptiques.* Thèse, Paris VII, June 1993.

[BB87] J. M. Borwein and P. B. Borwein. *Pi and the AGM.* John Wiley, 1987.

[BB88] J. M. Borwein and P. B. Borwein. More Ramanujan-type series for $1/\pi$. In G.E. Andrews, R.A. Askey, B.C. Berndt, K.G. Ramanathan, and R.A. Rankin, editors, *Ramanujan revisited*, pages 359–374. Academic Press, 1988.

[BB93] J. M. Borwein and P. B. Borwein. Class number three Ramanujan type series for $1/\pi$. *Journal of Computationl and Applied Mathematics*, 46:281–290, 1993.

[BBL95] D. Bleichenbacher, W. Bosma, and A. K. Lenstra. Some remarks on Lucas-based cryptosystems. In D. Coppersmith, editor, *Advances in Cryptology – CRYPTO '95*, volume 963 of *Lecture Notes in Comput. Sci.*, pages 386–396. Springer-Verlag, 1995. 15th annual International Cryptology Conference, Santa Barbara, California, USA, August 27–31.

[BC90] A. Bender and G. Castagnoli. On the implementation of elliptic curve cryptosystems. In G. Brassard, editor, *Advances in Cryptology – CRYPTO '89*, volume 435 of *Lecture Notes in Comput. Sci.*, pages 186–192. Springer-Verlag, 1990. Proceedings of a conference on the theory and application of cryptology, Santa Barbara, August 20–24.

[BCH+66] A. Borel, S. Chowla, C. S. Herz, K. Iwasawa, and J.-P. Serre. *Seminar on complex multiplication*. Number 21 in Lecture Notes in Math. Springer, 1966.

[Ber95] L. Bertrand. Computing a hyperelliptic integral using arithmetic in the Jacobian of the curve. *Appl. Algebra Engrg. Comm. Comput.*, 6:275–298, 1995.

[Bir68] B. J. Birch. How the number of points of an elliptic curve over a fixed prime field varies. *J. London Math. Soc.*, 43:57–60, 1968.

[BK75] B. J. Birch and W. Kuyk, editors. *Modular functions of one variable IV*, volume 476 of *Lecture Notes in Math.* Springer, 1975. Proceedings International Summer School University of Antwerp, RUCA, July 17-Agust 3, 1972.

[BK98] R. Balasubramanian and N. Koblitz. The improbability that an elliptic curve has subexponential discrete log problem under the Menezes-Okamoto-Vanstone algorithm. *J. of Cryptology*, 11:141–145, 1998.

[BKK90] J.-F. Boyar, S. A. Kurtz, and M. W. Krentel. A discrete logarithm implementation of perfect zero-knowledge blobs. *J. of Cryptology*, 2:63–76, 1990.

[BL96] D. Boneh and R. J. Lipton. Algorithms for black-box fields anf their application to cryptography. In N. Koblitz, editor, *Advances in Cryptology – CRYPTO '96*, volume 1109 of *Lecture Notes in Comput. Sci.*, pages 283–297. Springer-Verlag, 1996. 16th Annual International Cryptology Conference, Santa Barbara, California, USA, August 1996, Proceedings.

[Ble97] D. Bleichenbacher. On the security of the KMOV public key cryptosystem. In B. Kaliski, editor, *Advances in Cryptology – CRYPTO '97*, volume 1294 of *Lecture Notes in Comput. Sci.*, pages 235–248. Springer-Verlag, 1997. Proceedings of a conference on the theory and application of cryptography held at the University of California, Santa Barbara, August 18-21, 1997.

[BLS75] J. Brillhart, D. H. Lehmer, and J. L. Selfridge. New primality criteria and factorizations of $2^m \pm 1$. *Math. Comp.*, 29(130):620–647, 1975.

[BLS+88] J. Brillhart, D. H. Lehmer, J. L. Selfridge, B. Tuckerman, and S. S. Wagstaff, Jr. *Factorizations of* $b^n \pm 1$, $b = 2, 3, 5, 6, 7, 10, 11, 12$ *up to high powers*. Number 22 in Contemporary Mathematics. AMS, 2 edition, 1988.

[Blu98a] A. Bluher. Formal groups, elliptic curves, and some theorems of Couveignes. In J. P. Buhler, editor, *Algorithmic Number Theory*, volume 1423 of *Lecture Notes in Comput. Sci.*, pages 482–501. Springer-Verlag, 1998. Third International Symposium, ANTS-III, Portland, Oregon, june 1998, Proceedings.

[Blu98b] A. W. Bluher. Relations between certain power sums of elliptic modular forms in characteristic two. *J. Number Theory*, 70:127–145, 1998.

[BM72] L. D. BAUMERT AND R. J. MCELIECE. Weights of irreducible cyclic codes. *Information and Control*, 20:158–175, 1972.

[BM90] R. BALASUBRAMANIAN AND M. RAM MURTY. Elliptic pseudoprimes, II. In C. GOLDSTEIN, editor, *Séminaire de Théorie des Nombres, Paris 1988–1989*, volume 91 of *Progr. Math.*, pages 13–25, Boston, 1990. Birkhäuser.

[Bos85] W. BOSMA. Primality testing using elliptic curves. Technical Report 85-12, Math. Instituut, Universiteit van Amsterdam, 1985.

[Bre86] R. P. BRENT. Some integer factorization algorithms using elliptic curves. *Australian Computer Science Communications*, 8:149–163, 1986.

[Bre90a] R. P. BRENT. Parallel algorithms for integer factorization. In J. H. LOXTON, editor, *Number theory and cryptography*, volume 154 of *London Math. Soc. Lecture Note Ser.*, pages 26–37. Cambridge University Press, 1990.

[Bre90b] R. P. BRENT. Vector and parallel algorithms for integer factorization. In *Proc. Third Australian Supercomputer Conference*, 1990.

[Bre96] R. P. BRENT. Factorization of the tenth and eleventh Fermat numbers. Preprint, January 1996.

[BS91] U. BAUM AND M. A. SHOKROLLAHI. An optimal algorithm for multiplication in F_{256}/F_4. *Appl. Algebra Engrg. Comm. Comput.*, 2:15–20, 1991.

[BS92] T. BETH AND F. SCHAEFER. Non supersingular elliptic curves for public key cryptosystems. In D. DAVIES, editor, *Advances in Cryptology – EUROCRYPT '91*, volume 547 of *Lecture Notes in Comput. Sci.*, pages 316–327. Springer–Verlag, 1992. Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques, Brighton, United Kingdom, April 8–11, 1991.

[BSD63] B. BIRCH AND H. P. F. SWINNERTON-DYER. Notes on elliptic curves I. *J. Reine Angew. Math.*, 212:7–25, 1963.

[BSD65] B. BIRCH AND H. P. F. SWINNERTON-DYER. Notes on elliptic curves II. *J. Reine Angew. Math.*, 218:79–108, 1965.

[Buh98] J. P. BUHLER, editor. *Algorithmic Number Theory*, volume 1423 of *Lecture Notes in Comput. Sci.* Springer-Verlag, 1998. Third Algorithmic Number Theory Symposium, ANTS-III, Portland, Oregon, USA, June 1998.

[BvdH90a] W. BOSMA AND M.-P. VAN DER HULST. Faster primality testing. In J.-J. QUISQUATER, editor, *Advances in Cryptology*, volume 434 of *Lecture Notes in Comput. Sci.*, pages 652–656. Springer-Verlag, 1990. Proc. Eurocrypt '89, Houthalen, April 10–13.

[BvdH90b] W. BOSMA AND M.-P. VAN DER HULST. *Primality proving with cyclotomy.* PhD thesis, Universiteit van Amsterdam, December 1990.

[Can87] D. G. CANTOR. Computing in the Jacobian of an hyperelliptic curve. *Math. Comp.*, 48(177):95–101, 1987.

[CC86] D. V. CHUDNOVSKY AND G. V. CHUDNOVSKY. Sequences of numbers generated by addition in formal groups and new primality and factorization tests. *Adv. in Appl. Math.*, 7:385–434, 1986.

[CC88a] D. V. CHUDNOVSKY AND G. V. CHUDNOVSKY. Algebraic complexities and algebraic curves over finite fields. *J. Complexity*, 4:285–316, 1988.

[CC88b] D. V. CHUDNOVSKY AND G. V. CHUDNOVSKY. Approximations and complex multiplication according to Ramanujan. In G.E. ANDREWS, R.A. ASKEY, B.C. BERNDT, K.G. RAMANATHAN, AND R.A. RANKIN, editors, *Ramanujan revisited*, pages 375–472. Academic Press, 1988.

[CC89] D. V. Chudnovsky and G. V. Chudnovsky. The computation of classical constants. *Proc. Natl. Sci. USA*, 86:8178–8182, November 1989.

[CCR91] L. S. Charlap, R. Coley, and D. P. Robbins. Enumeration of rational points on elliptic curves over finite fields. Draft, 1991.

[CDM96] J.-M. Couveignes, L. Dewaghe, and F. Morain. Isogeny cycles and the Schoof-Elkies-Atkin algorithm. Research Report LIX/RR/96/03, LIX, April 1996.

[CF96] J. W. S. Cassels and E. V. FLynn. *Prolegomena to a middlebrow arithmetic of curves of genus 2*, volume 230 of *London Math. Soc. Lecture Note Ser.* Cambridge University Press, 1996.

[CFPR96] D. Coppersmith, M. Franklin, J. Patarin, and M. Reiter. Low exponent RSA with related messages. In U. Maurer, editor, *Advances in Cryptology – EUROCRYPT '96*, volume 1070 of *Lecture Notes in Comput. Sci.*, pages 1–9. Springer-Verlag, 1996. International Conference on the Theory and Application of Cryptographic Techniques, Saragossa, Spain, May 1996.

[CHTT95] J. Chao, K. Harada, K. Tanada, and S. Tsujii. Design of cryptographically secure elliptic curves over extension fields with CM field method. Preprint, 1995.

[CL84] H. Cohen and H. W. Lenstra, Jr. Primality testing and Jacobi sums. *Math. Comp.*, 42(165):297–330, 1984.

[CL87] H. Cohen and A. K. Lenstra. Implementation of a new primality test. *Math. Comp.*, 48(177):103–121, 1987.

[CM94] J.-M. Couveignes and F. Morain. Schoof's algorithm and isogeny cycles. In L. Adleman and M.-D. Huang, editors, *ANTS-I*, volume 877 of *Lecture Notes in Comput. Sci.*, pages 43–58. Springer-Verlag, 1994. 1st Algorithmic Number Theory Symposium - Cornell University, May 6-9, 1994.

[Coa70] J. Coates. Construction of rational functions on a curve. *Proc. Camb. Phil. Soc.*, 68:105–123, 1970.

[Coh84] P. Cohen. On the coefficients of the transformation polynomials for the elliptic modular function. *Math. Proc. Cambridge Philos. Soc.*, 95:389–402, 1984.

[Coh93] H. Cohen. *A course in algorithmic algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer–Verlag, 1993.

[Coh96] H. Cohen, editor. *Algorithmic Number Theory*, volume 1122 of *Lecture Notes in Comput. Sci.* Springer-Verlag, 1996. 2nd Algorithmic Number Theory Symposium - Université de Bordeaux, May 18-23, 1996.

[Cop96] D. Coppersmith. Finding a small root of a univariate modular equation. In U. Maurer, editor, *Advances in Cryptology – EUROCRYPT '96*, volume 1070 of *Lecture Notes in Comput. Sci.*, pages 155–165. Springer-Verlag, 1996. International Conference on the Theory and Application of Cryptographic Techniques, Saragossa, Spain, May 1996.

[Cop98] D. Coppersmith. Specialized integer factorization. In K. Nyberg, editor, *Advances in Cryptology – EUROCRYPT '98*, volume 1403 of *Lecture Notes in Comput. Sci.*, pages 542–545. Springer-Verlag, 1998. International Conference on the Theory and Application of Cryptographic Techniques, Espoo, Finland, May/June 1998, Proceedings.

[Cor08] G. Cornacchia. Su di un metodo per la risoluzione in numeri interi dell' equazione $\sum_{h=0}^{n} C_h x^{n-h} y^h = P$. *Giornale di Matematiche di Battaglini*, 46:33–90, 1908.

[Cou94] J.-M. Couveignes. *Quelques calculs en théorie des nombres.* Thèse, Université de Bordeaux I, July 1994.

[Cou96] J.-M. Couveignes. Computing l-isogenies using the p-torsion. In H. Cohen, editor, *Algorithmic Number Theory*, volume 1122 of *Lecture Notes in Comput. Sci.*, pages 59–65. Springer Verlag, 1996. Second International Symposium, ANTS-II, Talence, France, May 1996, Proceedings.

[Cou97] J.-M. Couveignes. Isomorphisms between Artin-Schreier towers. Draft, available on `http://www.math.u-bordeaux.fr/~couveign`, January 1997.

[Cox89] D. A. Cox. *Primes of the form* $x^2 + ny^2$. John Wiley & Sons, 1989.

[Cre92] J. Cremona. *Algorithms for modular elliptic curves.* Cambridge University Press, 1992.

[CTT94] J. Chao, K. Tanada, and S. Tsujii. Design of elliptic curves with controllable lower boundary of extension degree for reduction attacks. In Y. Desmedt, editor, *Advances in Cryptology – CRYPTO '94*, volume 839 of *Lecture Notes in Comput. Sci.*, pages 50–55. Springer-Verlag, 1994. Proc. 14th Annual International Cryptology Conference, Santa Barbara, Ca, USA, August 21–25.

[Dav31] H. Davenport. On the distribution of quadratic residues (mod p). *J. London Math. Soc.*, 6:49–54, 1931.

[Dav81] J. Davenport. *On the integration of algebraic functions*, volume 102 of *Lecture Notes in Comput. Sci.* Springer-Verlag, 1981.

[dB90] B. den Boer. Diffie-Hellman is as strong as discrete log for certain primes. In S. Goldwasser, editor, *Advances in Cryptology – CRYPTO '88*, volume 403 of *Lecture Notes in Comput. Sci.*, pages 530–539. Springer–Verlag, 1990. Proceedings of a conference on the theory and application of cryptography held at the University of California, Santa Barbara, August 21-25, 1988.

[de 83] H. F. de Groote. Characterization of division algebras of minimal rank and the structure of their algorithm varieties. *SIAM J. Comput.*, 12:101–117, 1983.

[Del74] P. Deligne. La conjecture de Weil. *Publ. Math. IHES*, 43:273–307, 1974.

[Dem94] N. Demytko. A new elliptic curve based analogue of RSA. In Tor Helleseth, editor, *Advances in Cryptology – EUROCRYPT '93*, volume 765 of *Lecture Notes in Comput. Sci.*, pages 40–49. Springer-Verlag, 1994. Workshop on the Theory and Application of Cryptographic Techniques, Lofthus, Norway, May 23–27, 1993.

[Deu41] M. Deuring. Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. *Abh. Math. Sem. Hamburg*, 14:197–272, 1941.

[Dew95] L. Dewaghe. Un corollaire aux formules de Vélu. Preprint, December 1995.

[Dew98] L. Dewaghe. Remarks on the Schoof-Elkies-Atkin algorithm. *Math. Comp.*, 67(223):1247–1252, July 1998.

[DH76] W. Diffie and M. E. Hellman. New directions in cryptography. *IEEE Trans. Inform. Theory*, IT-22-6, November 1976.

[Dic52] L. E. Dickson. *History of the Theory of Numbers*, volume I, II, III. Chelsea, New York, 1952.

[DL93] B. Dixon and A. K. Lenstra. Massively parallel elliptic curve facoring. In R. A. Rueppel, editor, *Advances in Cryptology – EUROCRYPT '92*, volume 658 of *Lecture Notes in Comput. Sci.*, pages 183–193. Springer-Verlag, 1993. Workshop on the Theory and Application of Cryptographic Techniques, Balatonfüred, Hungary, May 24–28, 1992, Proceedings.

[DM85] Y. Driencourt and J.-F. Michon. Remarques sur les codes géométriques. *C. R. Acad. Sci. Paris Sér. I Math.*, 301:15–17, 1985.

[DM86] Y. Driencourt and J.-F. Michon. Rapports sur les codes géométriques. Technical report, Univ. Aix-Marseille II et CIRM, Univ. Paris 7, October 1986.

[DM87] Y. Driencourt and J.-F. Michon. Elliptic codes over fields of characteristic 2. *J. Pure Appl. Algebra*, 45:15–39, 1987.

[DM96] D. S. Dummit and W. L. Miller. The Steinitz class of the Mordell-Weil group of some CM elliptic curves. *J. Number Theory*, 56:52–78, 1996.

[Dri86] Y. Driencourt. Some properties of elliptic codes over a field of characteristic 2. In J. Calmet, editor, *Algebraic algorithms and error-correcting codes*, volume 229 of *Lecture Notes in Comput. Sci.*, pages 185–193. Springer, 1986. Proc. 3rd International Conference, AAECC-3, Grenoble, France, July 1985.

[Elk87] N. D. Elkies. The existence of infinitely many supersingular primes for every elliptic curve over $\mathbb{Q}$. *Invent. Math.*, 89:561–567, 1987.

[Elk91] N. D. Elkies. Explicit isogenies. Draft, 1991.

[Elk92] N. D. Elkies. Distribution of supersingular primes. In *Journées Arithmétiques 1989*, volume 198–199-200 of *Astérisque*, pages 127–132, 1992.

[Elk98] N. D. Elkies. Elliptic and modular curves over finite fields and related computational issues. In D. A. Buell and J. T. Teitelbaum, editors, *Computational Perspectives on Number Theory: Proceedings of a Conference in Honor of A. O. L. Atkin*, volume 7 of *AMS/IP Studies in Advanced Mathematics*, pages 21–76. American Mathematical Society, International Press, 1998.

[FM95] E. Fouvry and M. R. Murty. Supersingular primes common to two elliptic curves. In S. David, editor, *Number theory*, volume 215 of *London Math. Soc. Lecture Note Ser.*, pages 91–102, Cambridge, 1995. Cambridge Univ. Press.

[FM96] E. Fouvry and R. Murty. On the distribution of supersingular primes. *Canad. J. Math.*, 48(1):81–104, 1996.

[Gat87] J. Von Zur Gathen. Factoring polynomials and primitive elements for special primes. *Theoret. Comput. Sci.*, 52:77–89, 1987.

[GK86] S. Goldwasser and J. Kilian. Almost all primes can be quickly certified. In *Proc. 18th STOC*, pages 316–329. ACM, 1986. May 28–30, Berkeley.

[GLV98] R. Gallant, R. Lambert, and S. Vanstone. Improving the parallelized Pollard lambda search on binary anomalous curves. `http://www.certicom.com/chal/download/paper.ps`, 1998.

[GM86] R. Gupta and M. Ram Murty. Primitive points on elliptic curves. *Compositio Math.*, 58:13–44, 1986.

[GM90] R. Gupta and M. Ram Murty. Cyclicity and generation of points mod p on elliptic curves. *Invent. Math.*, 101:225–235, 1990.

[GM92] D. Guillaume and F. Morain. Building Carmichael numbers with a large number of prime factors. Research Report LIX/RR/92/01, Ecole Polytechnique–LIX, February 1992.

[GM96] D. Guillaume and F. Morain. Building pseudoprimes with a large number of prime factors. *Appl. Algebra Engrg. Comm. Comput.*, 7(4):263–277, 1996.

[Gop91] V. D. Goppa. *Geometry and codes*, volume 24 of *Mathematics and its applications*. Kluwer, 1991.

[Gor89a] D. M. Gordon. On the number of elliptic pseudoprimes. *Math. Comp.*, 52(185):231–245, January 1989.

[Gor89b] D. M. Gordon. Pseudoprimes on elliptic curves. In J.-M. De Koninck and Claude Levesque, editors, *Théorie des nombres*, pages 290–305. Walter de Gruyter, 1989. Proceedings of the International Number Theory Conference held at Université de Laval, July 5–18, 1987.

[GP91] D. M. Gordon and C. Pomerance. The distribution of Lucas and elliptic pseudoprimes. *Math. Comp.*, 57(196):825–838, October 1991. Corrigendum, ibid., 60, 202, 1993, p. 877.

[GPZ94] J. Gebel, A. Pethö, and H. G. Zimmer. Computing integral points on elliptic curves. *Acta Arith.*, LXVIII:171–192, 1994.

[GS95a] A. Garcia and H. Stichtenoth. Algebraic function fields over finite fields with many rational places. *IEEE Trans. Inform. Theory*, 41(6):1548–1563, November 1995.

[GS95b] A. Garcia and H. Stichtenoth. A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vladut bound. To appear in Invent. Math., 1995.

[GZ85] B. H. Gross and D. B. Zagier. On singular moduli. *J. Reine Angew. Math.*, 355:191–220, 1985.

[Haj93a] F. Hajir. Elliptic units of cyclic unramified extensions of complex quadratic fields. *Acta Arith.*, LXIV:69–85, 1993.

[Haj93b] F. Hajir. *Unramified elliptic units.* Phd in mathematics, Princeton Univesity, June 1993.

[Has33] H. Hasse. Beweis des Analogons der Riemannschen Vermutung für die Artinschen und F. K. Smidtschen Kongruenzzetafunktionen in gewissen elliptischen Fällen. *Ges. d. Wiss. Narichten. Math.-Phys. Klasse*, pages 253–262, 1933.

[Has34a] H. Hasse. Abstrakte Begründung der komplexen Multiplikation und Riemannsche Vermutung in Funktionenkörpern. *Abh. Math. Sem. Univ. Hamburg*, 10:325–348, 1934.

[Has34b] H. Hasse. Existenz separabler zyklisher unverzweigter Erweiterungskörper von Primzahlgrad p über elliptischen Funktionenkörpern der Charakteristik p. *J. Reine Angew. Math.*, 172:77–85, 1934.

[Hås86] J. Håstad. On using RSA with low exponent in a public key network. In H. C. Williams, editor, *Advances in Cryptology*, volume 218 of *Lecture Notes in Comput. Sci.*, pages 403–408. Springer-Verlag, 1986. Proceedings Crypto '85, Santa Barbara (USA), August 18–22, 1985.

[HBJ92] F. Hirzebruch, T. Berger, and R. Jung. *Manifolds and modular forms*, volume E20 of *Aspects of Mathematics*. Vieweg, 1992. A publication of the Max-Planck-Institut für Mathematik, Bonn.

[Hir95] J. W. P. Hirschfeld. The main conjecture for MDS codes. In C. Boyd, editor, *Cryptography and coding*, volume 1025 of *Lecture Notes in Comput. Sci.*, pages 44–52. Springer-Verlag, 1995. 5th IMA Conference, Cirencester, UK, December 1995.

[HM89] J. L. Hafner and K. S. McCurley. On the distribution of running times of certain integer factoring algorithms. *J. Algorithms*, 10:531–556, 1989.

[HMV93] G. Harper, A. Menezes, and S. Vanstone. Public-key cryptosystems with very small key length. In R. A. Rueppel, editor, *Advances in Cryptoloy – EUROCRYPT '92*, volume 658 of *Lecture Notes in Comput. Sci.*, pages 163–173. Springer-Verlag, 1993. Workshop on the Theory and Application of Cryptographic Techniques, Balatonfüred, Hungary, May 24–28, 1992, Proceedings.

[HMW90a] K. Hardy, J. B. Muskat, and K. S. Williams. A deterministic algorithm for solving $n = fu^2 + gv^2$ in coprime integers u and v. *Math. Comp.*, 55(191):327–343, July 1990.

[HMW90b] K. Hardy, J. B. Muskat, and K. S. Williams. Solving $n = au^2 + buv + cv^2$ using the Euclidean algorithm. *Utilitas Math.*, 38:225–236, 1990.

[Hou78] C. Houzel. *Abrégé d'histoire des mathématiques 1700–1900*, volume II, chapter Fonctions elliptiques et intégrales abéliennes, pages 1–113. Hermann, 1978. J. Dieudonné, Ed..

[How93] E. W. Howe. On the group orders of elliptic curves over finite fields. *Compositio Math.*, 85:229–247, 1993.

[HP95] T. Høholdt and R. Pellikaan. On the decoding of algebraic-geometric codes. *IEEE Trans. Inform. Theory*, 41(6):1589–1614, November 1995.

[Hua85] M-D. A. Huang. Riemann hypothesis and finding roots over finite fields. In *Proc. 17th ACM STOC*, pages 121–130. ACM, 1985. Providence, Rhode Island, May 6–8.

[Hus87] D. Husemöller. *Elliptic curves*, volume 111 of *Graduate Texts in Mathematics*. Springer, 1987.

[HV96] F. Hajir and F. R. Villegas. Explicit elliptic units. Preprint, 1996.

[HV98] J. W. P. Hirschfeld and J. F. Voloch. The characterization of elliptic curves over finite fields. *J. Austral. Math. Soc. Ser. A*, 45:275–286, 1998.

[Igu58] J.-I. Igusa. Class number of a definite quaternion with prime discriminant. *Proc. Nat. Acad. Sci. U.S.A*, 44:312–314, 1958.

[Igu59] J.-I. Igusa. Kroneckerian model of fields of elliptic modular functions. *Amer. J. Math.*, 81:561–577, 1959.

[Igu68] J.-I. Igusa. On the algebraic theory of elliptic modular functions. *J. Math. Soc. Japan*, 20(1–2):96–106, 1968.

[JL98] A. Joux and R. Lercier. Counting points of elliptic curves defined over $GF(2^n)$. Email to the `NMBRTHRY` mailing list; available on `http://listserv.nodak.edu/archives/nmbrthry.html`, June 1998.

[JM95] A. Joux and F. Morain. Sur les sommes de caractères liées aux courbes elliptiques à multiplication complexe. *J. Number Theory*, 55(1):108–128, November 1995.

[Joy97] M. Joye. *Security analysis of RSA-type cryptosystems*. Phd thesis, Université catholique de Louvain, October 1997.

[JvdG88] van Lint J, H and G. van der Geer. *Introduction to coding theory and algebraic geometry*, volume Band 12 of *DMV Seminar*. Birkhäuser, 1988.

[Kal87] B. S. Kaliski, Jr. A pseudo-random bit generator based on elliptic logarithms. In A. M. Odlyzko, editor, *Advances in Cryptology – CRYPTO '86*, volume 263 of *Lecture Notes in Comput. Sci.*, pages 13–21. Springer Verlag, 1987. Proceedings, Santa Barbara (USA), August 11–15, 1986.

[Kal88] B. S. Kaliski, Jr. *Elliptic curves and cryptography: a pseudorandom bit generator and other tools*. PhD thesis, MIT, Cambridge, January 1988. MIT/LCS/TR-411.

[Kal91] B. S. Kaliski, Jr. One-way permutations on elliptic curves. *J. of Cryptology*, 3(3):187–199, 1991.

[Kal95] B. S. Kaliski, Jr. A chosen message attack on Demtyko's elliptic curve cryptosystem. To appear in *J. of Cryptology*, November 1995.

[Kan89] M. Kaneko. Supersingular j-invariants as singular moduli mod p. *Osaka J. Math*, 26:849–855, 1989.

[Kat76] N. M. Katz. An overview of deligne's proof of the riemann hypothesis for varieties over finite fields. In *Proc. Symposium in Pure Mathematics*, pages 275–305, 1976. volume 28.

[Kee88] A. D. Keedwell. Simple constructions for elliptic cubic curves with specified small number of points. *European J. Combin.*, 9:463–481, 1988.

[KK98] N. Kunihiro and K. Koyama. Equivalence of counting the number of points on elliptic curve over the ring $\mathfrak{Z}_n$ and factoring n. In K. Nyberg, editor, *Advances in Cryptology – EUROCRYPT '98*, volume 1403 of *Lecture Notes in Comput. Sci.*, pages 47–58. Springer-Verlag, 1998. International Conference on the Theory and Application of Cryptographic Techniques, Espoo, Finland, May/June 1998, Proceedings.

[KL89] N. Katz and R. Livné. Sommes de Kloosterman et courbes elliptiques universelles en caractéristique 2 et 3. *C. R. Acad. Sci. Paris Sér. I Math.*, 309:723–726, 1989.

[KM92] W. Keller and F. Morain. The complete factorization of some large Mersenne composites. *Abstracts of the AMS*, 13(5):506, October 1992. 92T-11-163.

[KMOV91] K. Koyama, U. M. Maurer, T. Okamoto, and S. A. Vanstone. New public-key schemes based on elliptic curves over the ring Z_n. In *Advances in Cryptology*, volume 576 of *Lecture Notes in Comput. Sci.*, pages 252–266. Springer-Verlag, 1991. Proc. Crypto '91, Santa Barbara, August 12–15.

[Kna92] A. W. Knapp. *Elliptic curves*. Princeton University Press, 1992.

[Knu81] D. E. Knuth. *The Art of Computer Programming: Seminumerical Algorithms*. Addison-Wesley, 2nd edition, 1981.

[Kob87] N. Koblitz. Elliptic curve cryptosystems. *Math. Comp.*, 48(177):203–209, January 1987.

[Kob88] N. Koblitz. Primality of the number of points on an elliptic curve over a finite field. *Pacific J. Math.*, 131(1):157–165, 1988.

[Kob89] N. Koblitz. Hyperelliptic cryptosystems. *J. of Cryptology*, 1:139–150, 1989.

[Kob90] N. Koblitz. Constructing elliptic curve cryptosystems in characteristic 2. In A. J. Menezes and S. A. Vanstone, editors, *Advances in Cryptology – CRYPTO '90*, volume 537 of *Lecture Notes in Comput. Sci.*, pages 156–167. Springer-Verlag, 1990. Proc., Santa Barbara, August 11–15, 1990.

[Kob91] N. Koblitz. Elliptic curve implementation of zero-knowledge blobs. *J. of Cryptology*, 4(3):207–213, 1991.

[Kob92] N. Koblitz. CM-curves with good cryptographic properties. In Joan Feigenbaum, editor, *Advances in Cryptology – CRYPTO '91*, volume 576 of *Lecture Notes in Comput. Sci.*, pages 279–287. Springer-Verlag, 1992. Santa Barbara, August 12–15.

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

[KOT95] K. Kurosawa, K. Okada, and S. Tsujii. Low exponent attack against elliptic curve RSA. In J. Pieprzyk and R. Safavi-Naini, editors, *Advances in Cryptology – ASIACRYPT '94*, volume 917 of *Lecture Notes in Comput. Sci.*, pages 376–383. Springer-Verlag, 1995. 4th International Conference on the Theory and Applications of Cryptology, Wollongong, Australia, November/December 1994, Proceedings.

[Koy95] K. Koyama. Fast RSA-type schemes based on singular cubic curves $y^2 + axy \equiv x^3 \pmod{n}$. In L. C. Guillou and J.-J. Quisquater, editors, *Advances in Cryptology – EUROCRYPT '95*, volume 921 of *Lecture Notes in Comput. Sci.*, pages 329–340. Springer-Verlag, 1995. International Conference on the Theory and Application of Cryptographic Techniques, Saint-Malo, France, May 1995, Proceedings.

[KT92] K. Koyama and Y. Tsuroka. Speeding up elliptic cryptosystems by using a signed binary window method. In Ernest F. Brickell, editor, *Advances in Cryptology – CRYPTO '92*, volume 740 of *Lecture Notes in Comput. Sci.*, pages 345–357. Springer-Verlag, 1992. 12th Annual International Cryptology Conference, Santa Barbara, California, USA, August 16–20, 1992, Proceedings.

[Kub76] D. S. Kubert. Universal bounds on the torsion of elliptic curves. *Proc. London Math. Soc.*, 3(33):193–237, 1976.

[KZ98] M. Kaneko and D. Zagier. Supersingular j-invariants, hypergeometric series, and Atkin's orthogonal polynomials. In D. A. Buell and J. T. Teitelbaum, editors, *Computational Perspectives on Number Theory: Proceedings of a Conference in Honor of A. O. L. Atkin*, volume 7 of *AMS/IP Studies in Advanced Mathematics*, pages 97–126. American Mathematical Society, International Press, 1998.

[Lac87] G. Lachaud. Sommes d'Eisenstein et nombre de points de certaines courbes algébriques sur les corps finis. *C. R. Acad. Sci. Paris Sér. I Math.*, 305:729–732, 1987.

[Lan73] S. Lang. *Elliptic functions.* Addison-Wesley, 1973.

[Lay94] G.-J. Lay. Konstruktion elliptischer Kurven mit vorgegebener Gruppenordnung über endlichen Primkörpern. Diplomarbeit, 1994. Saabrücken.

[Len81] H. W. Lenstra, Jr. Primality testing algorithms (after Adleman, Rumely, Williams). *Séminaire Bourbaki*, 576, 1980-1981.

[Len86] H. W. Lenstra, Jr. Elliptic curves and number theoretic algorithms. Technical Report Report 86-19, Math. Inst., Univ. Amsterdam, 1986.

[Len87] H. W. Lenstra, Jr. Factoring integers with elliptic curves. *Ann. of Math. (2)*, 126:649–673, 1987.

[Len88] A. K. Lenstra. Fast and rigorous factorization under the generalized Riemann hypothesis. *Indag. Math.*, 50(4):443–454, 1988.

[Len96] H. W. Lenstra, Jr. Complex multiplication structure of elliptic curves. *J. Number Theory*, 56:227–241, 1996.

[Ler93] R. Lercier. Factoriser des entiers par la méthode des courbes elliptiques. Mémoire de DEA, École Polytechnique, 91128 Palaiseau CEDEX, France, July 1993.

[Ler96] R. Lercier. Computing isogenies in F_{2^n}. In H. Cohen, editor, *Algorithmic Number Theory*, volume 1122 of *Lecture Notes in Comput. Sci.*, pages 197–212. Springer Verlag, 1996. Second International Symposium, ANTS-II, Talence, France, May 1996, Proceedings.

[Ler97a] R. Lercier. *Algorithmique des courbes elliptiques dans les corps finis.* Thèse, École polytechnique, June 1997.

[Ler97b] R. Lercier. Finding good random elliptic curves for cryptosystems defined over F_{2^n}. In W. Fumy, editor, *Advances in Cryptology – EUROCRYPT '97*, volume 1233 of *Lecture Notes in Comput. Sci.*, pages 379–392. Springer-Verlag, 1997. International Conference on the Theory and Application of Cryptographic Techniques, Konstanz, Germany, May 1997, Proceedings.

[LL90] A. K. Lenstra and H. W. Lenstra, Jr. Algorithms in number theory. In J. van Leeuwen, editor, *Handbook of Theoretical Computer Science*, volume A: Algorithms and Complexity, chapter 12, pages 674–715. North Holland, 1990.

[LM95a] F. Leprévost and F. Morain. Revêtements de courbes elliptiques à multiplication complexe par des courbes hyperelliptiques et sommes de caractères. Technical Report MPI/95–124, Max-Planck-Institut für Mathematik Bonn, 1995.

[LM95b] R. Lercier and F. Morain. Counting points on elliptic curves over F_{p^n} using Couveignes's algorithm. Research Report LIX/RR/95/09, École Polytechnique–LIX, September 1995. A shortened version is to appear in *Math. Comp.*

[LM95c] R. Lercier and F. Morain. Counting the number of points on elliptic curves over finite fields: strategies and performances. In L. C. Guillou and J.-J. Quisquater, editors, *Advances in Cryptology – EUROCRYPT '95*, volume 921 of *Lecture Notes in Comput. Sci.*, pages 79–94, 1995. International Conference on the Theory and Application of Cryptographic Techniques, Saint-Malo, France, May 1995, Proceedings.

[LM98] R. Lercier and F. Morain. Algorithms for computing isogenies between elliptic curves. In D. A. Buell and J. T. Teitelbaum, editors, *Computational Perspectives on Number Theory: Proceedings of a Conference in Honor of A. O. L. Atkin*, volume 7 of *AMS/IP Studies in Advanced Mathematics*, pages 77–96. American Mathematical Society, International Press, 1998.

[LMMS94] F. Lehmann, M. Maurer, V. Müller, and V. Shoup. Counting the number of points on elliptic curves over finite fields of characteristic greater than three. In L. Adleman and M.-D. Huang, editors, *ANTS-I*, volume 877 of *Lecture Notes in Comput. Sci.*, pages 60–70. Springer-Verlag, 1994. 1st Algorithmic Number Theory Symposium - Cornell University, May 6-9, 1994.

[LP92] H. W. Lenstra, Jr. and C. Pomerance. A rigorous time bound for factoring integers. *J. Amer. Math. Soc.*, 5(3):483–516, July 1992.

[LPP93] H. W. Lenstra, Jr., J. Pila, and C. Pomerance. A hyperelliptic smoothness test, I. *Philos. Trans. Roy. Soc. London Ser. A*, 345:397–408, 1993.

[LR85] H. Lange and W. Ruppert. Complete systems of addition laws on abelian variety. *Invent. Math.*, 79:603–610, 1985.

[LT76] S. Lang and H. Trotter. *Frobenius distributions in GL_2 extensions*, volume 540 of *Lecture Notes in Mathematics*. Springer, 1976.

[LW87] G. Lachaud and J. Wolfmann. Sommes de Kloosterman, courbes elliptiques et codes cycliques en caractéristique 2. *C. R. Acad. Sci. Paris Sér. I Math.*, 305:881–883, 1987.

[LW90] G. Lachaud and J. Wolfmann. The weights of the orthogonals of the extended quadratic binary Goppa codes. *IEEE Trans. Inform. Theory*, 36(3):686–692, May 1990.

[LZ94] G.-J. Lay and H. G. Zimmer. Constructing elliptic curves with given group order over large finite fields. In L. Adleman and M.-D. Huang, editors, *ANTS-I*, volume 877 of *Lecture Notes in Comput. Sci.*, pages 250–263. Springer-Verlag, 1994. 1st Algorithmic Number Theory Symposium - Cornell University, May 6-9, 1994.

[Man81] Y. Manin. What is the maximum number of points on a curve over F_2? *J. Fac. Sci. Univ. Tokyo Sect. IA Math.*, 28:715–720, 1981.

[Mau94] U. M. Maurer. Towards the equivalence of breaking the Diffie-Hellman protocol and computing discrete logarithms. In Y. G. Desmedt, editor, *Advances in Cryptology – CRYPTO '94*, volume 839 of *Lecture Notes in Comput. Sci.*, pages 271–281. Springer-Verlag, 1994. Proc. 14th Annual International Cryptology Conference, Santa Barbara, Ca, USA, August 21–25.

[Mau95] U. M. Maurer. Fast generation of prime numbers and secure public-key cryptographic parameters. *J. of Cryptology*, 8(3):123–155, 1995.

[Maz77] B. Mazur. Rational points on modular curves. In *Modular forms of one variable V*, volume 601 of *Lecture Notes in Math.*, pages 107–148. Springer Verlag, 1977. Proceedings International Conference, University of Bonn, Sonderforschungsbereich Theoretische Mathematik, July 2-14, 1976.

[McC88] K. S. McCurley. A key distribution scheme equivalent to factoring. *J. of Cryptology*, 1(2):95–105, 1988.

[McK94] J. McKee. Computing division polynomials. *Math. Comp.*, 63(208):767–771, October 1994.

[McK96] J. McKee. Subtleties in the distribution of the numbers of points on elliptic curves over a finite prime field. Preprint, 1996.

[Men93] A. J. Menezes. *Elliptic curve public key cryptosystems.* Kluwer Academic Publishers, 1993.

[Mer96] L. Merel. Bornes pour la torsion des courbes elliptiques sur les corps de nombres. *Invent. Math.*, 124:437–449, 1996.

[Mes83] J.-F. Mestre. Courbes elliptiques et formules explicites. In M.-J. Bertin, editor, *Séminaire de Théorie des Nombres, Paris 1982*, volume 38 of *Progress in Mathematics*, pages 179–187, Boston, Ma, 1983. Birkhäuser. Séminaire Delange-Pisot-Poitou.

[Mes86] J.-F. Mestre. La méthode des graphes. Exemples et applications. In *Proc. of the International Conference on class numbers and fundamental units of algebraic number fields*, pages 217–242, Nagoya, 1986. Nagoya Univ. Katata (Japan).

[Mic89] J.-F. Michon. Codes and curves. In T. Mora, editor, *Applied algebra, algebraic algorithms and error-correcting codes*, volume 357 of *Lecture Notes in Comput. Sci.*, pages 22–30. Springer, 1989. Proc. of the 6th international conference, AAECC-6, Rome, July 4-8, 1988.

[Mih98] P. Mihăilescu. Cyclotomy primality proving – recent deelopments. In J. P. Buhler, editor, *Algorithmic Number Theory*, volume 1423 of *Lecture Notes in Comput. Sci.*, pages 95–110. Springer-Verlag, 1998. Third International Symposium, ANTS-III, Portland, Oregon, june 1998, Proceedings.

[Mil86] V. Miller. Short programs for functions on curves. Draft, 1986.

[Mil87] V. Miller. Use of elliptic curves in cryptography. In A. M. Odlyzko, editor, *Advances in Cryptology – CRYPTO '86*, volume 263 of *Lecture Notes in Comput. Sci.*, pages 417–426. Springer-Verlag, 1987. Proceedings, Santa Barbara (USA), August11–15, 1986.

[Miy93a] A. Miyaji. Elliptic curves over F_p suitable for cryptosystems. In J. Seberry and Y. Zheng, editors, *Advances in cryptology - AUSCRYPT '92*, volume 718 of *Lecture Notes in Comput. Sci.*, pages 479–491. Springer-Verlag, 1993. Workshop on the theory and application of cryptographic techniques, Gold Coast, Queensland, Australia, December 13-16, 1992.

[Miy93b] A. Miyaji. On ordinary elliptic curve cryptosystems. In *Advances in Cryptology – ASIACRYPT '91*, volume 739 of *Lecture Notes in Comput. Sci.*, pages 50–55. Springer-Verlag, 1993. International Conference on the theory and application of cryptology, Fujiyoshida, Japan, November 11–14, 1991, Proceedings.

[Miy96] A. Miyaji. A message recovery signature scheme equivalent to DSA over elliptic curves. In Kwangjo Kwangjo and Tsutomu Matsumoto, editors, *Advances in Cryptology – ASIACRYPT '96*, volume 1163 of *Lecture Notes in Comput. Sci.*, pages 1–14. Springer-Verlag, 1996. International Conference on the Theory and Applications of Cryptology and Information Security, Kyongju, Korea, November 1996, Proceedings.

[MM89] I. Miyamoto and M. R. Murty. Elliptic pseudoprimes. *Math. Comp.*, 53(187):415–430, July 1989.

[MM96] B. Meyer and V. Müller. A public key cryptosystem based on elliptic curves over $\mathbb{Z}/n\mathbb{Z}$ equivalent to factoring. In U. Maurer, editor, *Advances in Cryptology – EUROCRYPT '96*, volume 1070 of *Lecture Notes in Comput. Sci.*, pages 49–59. Springer-Verlag, 1996. International Conference on the Theory and Application of Cryptographic Techniques, Saragossa, Spain, May 1996.

[MO19] J.-F. Mestre and J. Oesterlé. La méthode des graphes. Preprint, 19??

[MO90] F. Morain and J. Olivos. Speeding up the computations on an elliptic curve using addition-subtraction chains. *RAIRO Inform. Théor. Appl.*, 24(6):531–543, 1990.

[Moe77] R. T. Moenck. On the efficiency of algorithms for polynomial factoring. *Math. Comp.*, 31:235–250, 1977.

[Mon87] P. L. Montgomery. Speeding the Pollard and elliptic curve methods of factorization. *Math. Comp.*, 48(177):243–264, January 1987.

[Mon92] P. L. Montgomery. *An FFT extension of the Elliptic Curve Method of factorization*. PhD thesis, University of California – Los Angeles, 1992.

[Mor22] L. J. Mordell. On the rational solutions of the indeterminate equations of the third and fourth degree. *Proc. of the Cambridge Philos. Soc.*, 21:179–192, 1922.

[Mor90a] F. Morain. Atkin's test: news from the front. In J.-J. Quisquater, editor, *Advances in Cryptology – EUROCRYPT '89*, volume 434 of *Lecture Notes in Comput. Sci.*, pages 626–635. Springer-Verlag, 1990. Proc. Eurocrypt '89, Houthalen, April 10–13.

[Mor90b] F. Morain. *Courbes elliptiques et tests de primalité*. Thèse, Université Claude Bernard–Lyon I, September 1990.

[Mor91a] F. Morain. Building cyclic elliptic curves modulo large primes. In D. Davies, editor, *Advances in Cryptology – EUROCRYPT '91*, volume 547 of *Lecture Notes in Comput. Sci.*, pages 328–336. Springer–Verlag, 1991. Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques, Brighton, United Kingdom, April 8–11, 1991.

[Mor91b] F. Morain. Distributed primality proving and the primality of $(2^{3539}+1)/3$. In I. B. Damgård, editor, *Advances in Cryptology – EUROCRYPT '90*, volume 473 of *Lecture Notes in Comput. Sci.*, pages 110–123. Springer–Verlag, 1991. Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques, Aarhus, Denmark, May 21–24, 1990.

[Mor91c] C. J. Moreno. *Algebraic curves over finite fields*, volume 97 of *Cambridge Tracts in Mathematics*. Cambridge University Press, 1991.

[Mor92a] F. Morain. Easy numbers for the Elliptic Curve Primality Proving algorithm. In Paul S. Wang, editor, *ISSAC '92*, pages 263–268, New York, 1992. ACM Press. Proceedings, July 27–29, Berkeley.

[Mor92b] F. Morain. Prime values of partition numbers and the primality of $p(1840926)$. Rapport de Recherche LIX/92/RR/11, Laboratoire d'Informatique de l'Ecole Polytechnique (LIX), 1992.

[Mor93] L. J. Mordell. The number of solutions of some congruences in two variables. *Math. Z.*, 37:193–209, 1993. à vérifier.

[Mor95] F. Morain. Calcul du nombre de points sur une courbe elliptique dans un corps fini : aspects algorithmiques. *J. Théor. Nombres Bordeaux*, 7:255–282, 1995.

[Mor96] F. Morain. More primes of the form $(2^p+1)/3$. Draft, May 1996.

[Mor97] F. Morain. Classes d'isomorphismes des courbes elliptiques supersingulières en caractéristique $\geqslant 3$. *Utilitas Math.*, 52:241–253, December 1997.

[Mor98] F. Morain. Primality proving using elliptic curves: an update. In J. P. Buhler, editor, *Algorithmic Number Theory*, volume 1423 of *Lecture Notes in Comput. Sci.*, pages 111–127. Springer-Verlag, 1998. Third International Symposium, ANTS-III, Portland, Oregon, june 1998, Proceedings.

[MOV90] A. Menezes, T. Okamoto, and S. A. Vanstone. Reducing elliptic curves logarithms to logarithms in a finite field. Technical report, University of Waterloo, 1990. Preliminary version.

[MOV91] A. Menezes, T. Okamoto, and S. A. Vanstone. Reducing elliptic curves logarithms to logarithms in a finite field. In *Proceedings 23rd Annual ACM Symposium on Theory of Computing (STOC)*, pages 80–89. ACM Press, 1991. May 6–8, New Orleans, Louisiana.

[MOV93] A. MENEZES, T. OKAMOTO, AND S. A. VANSTONE. Reducing elliptic curves logarithms to logarithms in a finite field. *IEEE Trans. Inform. Theory*, 39(5):1639–1646, September 1993.

[MQV] A. MENEZES, M. QU, AND S. VANSTONE. Working draft, IEEE P1363 standard, part 4, (draft 6), november 6, 1995. Available on `http://stdsbbs.ieee.org/`.

[MS77] F. J. MACWILLIAMS AND N. J. A. SLOANE. *The theory of error-correcting codes*. North-Holland, 1977.

[MS88] M. MIGNOTTE AND C. SCHNORR. Calcul déterministe des racines d'un polynôme dans un corps fini. *C. R. Acad. Sci. Paris Sér. I Math.*, 306:467–472, 1988.

[MS90] P. L. MONTGOMERY AND B. SILVERMAN. An FFT extension to the $P-1$ factoring algorithm. *Math. Comp.*, 54(190):839–854, April 1990.

[MS93] W. MEIER AND O. STAFFELBACH. Efficient multiplication on certain nonsupersingular elliptic curves. In ERNEST F. BRICKELL, editor, *Advances in Cryptology – CRYPTO '92*, volume 740 of *Lecture Notes in Comput. Sci.*, pages 333–344. Springer-Verlag, 1993. Proc., Santa Barbara, August 16–20, 1992.

[Mül94] V. MÜLLER. Looking for the eigenvalue in Schoof's algorithm. In preparation, October 1994.

[Mül95] V. MÜLLER. *Ein Algorithmus zur Bestimmung der Punktanzahl elliptischer Kurven über endlichen Körpern der Charakteristik größer drei.* PhD thesis, Technischen Fakultät der Universität des Saarlandes, 1995.

[Mun93] C. MUNUERA. On MDS elliptic codes. *Discrete Math.*, 117:279–286, 1993.

[Mur83] M. RAM MURTY. On Artin's conjecture. *J. Number Theory*, 16:147–168, 1983.

[Mus92] J. B. MUSKAT. A refinement of the Hardy-Muskat-Williams algorithm for solving $n = fu^2 + gv^2$. *Utilitas Math.*, 41:109–117, 1992.

[MV85] Y. I. MANIN AND S. G. VLĂDUŢ. Linear codes and modular curves. *J. Soviet Math.*, 30:2611–2643, 1985.

[MV90a] A. MENEZES AND S. VANSTONE. Isomorphism classes of elliptic curves over finite fields of characteristic 2. *Utilitas Math.*, 38:135–153, 1990.

[MV90b] A. MENEZES AND S. A. VANSTONE. The implementation of elliptic curve cryptosystems. In J. SEBERRY AND J. PIEPRZYK, editors, *Advances in Cryptology – AUSCRYPT '90*, number 453 in Lecture Notes in Comput. Sci., pages 2–13. Springer–Verlag, 1990. Proceedings, Sysdney (Australia), January 1990.

[MV93] A. J. MENEZES AND S. A. VANSTONE. Elliptic curve cryptosystems and their implementation. *J. of Cryptology*, 6:209–224, 1993.

[MW96] U. M. MAURER AND S. WOLF. Diffie-Hellman oracles. In N. KOBLITZ, editor, *Advances in Cryptology – CRYPTO '96*, volume 1109 of *Lecture Notes in Comput. Sci.*, pages 268–282. Springer-Verlag, 1996. 16th Annual International Cryptology Conference, Santa Barbara, California, USA, August 1996, Proceedings.

[Nec94] V. I. NECHAEV. Complexity of a determinate algorithm for the discrete logarithm. *Mathematical Notes*, 55(2):165–172, 1994.

[Nit95] A. NITAJ. L'algorithme de Cornacchia. *Exposition. Math.*, 13:358–365, 1995.

[OFF93] T. OKAMOTO, A. FUJIKODA, AND E. FUJISAKI. An efficient digital signature scheme based on an elliptic curve over the ring Z_n. In *Advances in Cryptology – CRYPTO '92*, volume 740 of *Lecture Notes in Comput. Sci.*, pages 54–65. Springer-Verlag, 1993. Proc., Santa Barbara, August 16–20, 1992.

[Oka90] T. OKAMOTO. A fast signature scheme based on congruential polynomial operations. *IEEE Trans. Inform. Theory*, 36(1):47–53, January 1990.

[OS92] T. Okamoto and K. Sakurai. Efficient algorithms for the construction of hyperelliptic cryptosystems. In J. Feigenbaum, editor, *Advances in Cryptology – CRYPTO '91*, volume 576 of *Lecture Notes in Comput. Sci.*, pages 267–278. Springer-Verlag, 1992. Proc., Santa Barbara, August 11–15, 1991.

[Per89] M. Perret. Families of codes exceeding the Varshamov-Gilbert bound. In G. Cohen and J. Wolfmann, editors, *Coding theory and applications*, volume 388 of *Lecture Notes in Comput. Sci.*, pages 28–36. Springer-Verlag, 1989. 3rd International Colloquium, Toulon, France, 1988.

[Pil90] J. Pila. Frobenius maps of abelian varieties and finding roots of unity in finite fields. *Math. Comp.*, 55(192):745–763, October 1990.

[Pin92] R. Pinch. Recognizing elements of finite fields. In C. Mitchell, editor, *Cryptography and coding II*, volume 33 of *Institute of mathematics and its applications conference series*, pages 193–197, Oxford, 1992. Clarendon Press. Based on the proceedings of the 2nd conference on Cryptography and coding, held at the Royal agricultural college, Cirencester, December 1989, organized by the Institute of mathematics and its applications.

[Pin95] R. Pinch. Extending the Wiener attack to RSA-type cryptosystems. *Electronics Letters*, 31(20):1736–1738, September 1995.

[Poi01] H. Poincaré. Sur les propriétés arithmétiques des courbes algébriques. *J. de Liouville (V)*, 7:161–xxx, 1901.

[Pol74] J. M. Pollard. Theorems on factorization and primality testing. *Proc. Cambr. Philos. Soc.*, 76:521–528, 1974.

[Pom87a] C. Pomerance. Fast, rigorous factorization and discrete logarithm algorithms. In D. S. Johnson, T. Nishizeki, A. Nozaki, and H. S. Wilf, editors, *Proc. of the Japan-US Joint Seminar, Discrete Algorithms and Complexity*, pages 119–143, Orlando, 1987. Academic Press.

[Pom87b] C. Pomerance. Very short primality proofs. *Math. Comp.*, 48(177):315–322, 1987.

[Pom89] C. Pomerance. *Cryptology and computational number theory*, chapter Factoring. AMS, 1989. Lecture Notes, August 6–7, 1989, Boulder, Colorado.

[Pom90] C. Pomerance, editor. *Cryptology and computational number theory*, number 42 in Proc. Symp. Appl. Math. Amer. Math. Soc., 1990. Lecture Notes, August 6–7, 1989, Boulder, Colorado.

[Poo96] B. Poonen. Computational aspects of curves of genus at least 2. In H. Cohen, editor, *Algorithmic Number Theory*, volume 1122 of *Lecture Notes in Comput. Sci.*, pages 283–306. Springer Verlag, 1996. Second International Symposium, ANTS-II, Talence, France, May 1996, Proceedings.

[PV96] R. Padma and S. Venkataraman. Elliptic curves with complex multiplication and a character sum. *J. Number Theory*, 61:274–282, 1996.

[PW95] O. Papini and J. Wolfmann. *Algèbre discrète et codes correcteurs*, volume 20 of *Mathématiques et Applications*. Springer-Verlag, 1995.

[PZ89] M. Pohst and H. Zassenhaus. *Algorithmic algebraic number theory*. Cambridge Univ. Press, 1989.

[Ram14] S. Ramanujan. Modular equations and approximations to π. *Quarterly J. Math.*, XLV:350–372, 1914.

[Rei86] M. A. Reichert. Explicit determination of nontrivial torsion structures of elliptic curves over quadratic number fields. *Math. Comp.*, 46(174):637–658, April 1986.

[Rib96] P. Ribenboim. *The new book of prime number records*. Springer-Verlag, 1996.

[Ris70] R. H. RISCH. The solution of the problem of integration in finite terms. *Bull. Amer. Math. Soc.*, 76:605–608, 1970.

[Rón89a] L. RÓNYAI. Factoring polynomials modulo special primes. *Combinatorica*, 9(2):199–206, 1989.

[Rón89b] L. RÓNYAI. Galois groups and factoring polynomials over finite fields. In *Proc. 30th FOCS*, pages 99–104, 1989.

[Rón92] L. RÓNYAI. Galois groups and factoring polynomials over finite fields. *SIAM J. Discrete Math.*, 5(3):345–365, August 1992.

[Rüc87] H.-G. RÜCK. A note on elliptic curves over finite fields. *Math. Comp.*, 49(179):301–304, July 1987.

[SA97] T. SATOH AND K. ARAKI. Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves. Preprint, 1997.

[SB95] A. SMITH AND C. BOYD. An elliptic analogue of McCurley's key agreement scheme. In C. BOYD, editor, *Cryptography and coding*, volume 1025 of *Lecture Notes in Comput. Sci.*, pages 150–157. Springer-Verlag, 1995. 5th IMA Conference, Cirencester, UK, December 1995.

[Sch74] B. SCHOENEBERG. *Elliptic modular functions*, volume 203 of *Die Grundlehren der mathematischen Wissenschaften in Einzeldarstellungen*. Springer–Verlag, 1974.

[Sch85] R. SCHOOF. Elliptic curves over finite fields and the computation of square roots mod p. *Math. Comp.*, 44:483–494, 1985.

[Sch87] R. SCHOOF. Nonsingular plane cubic curves over finite fields. *J. Combin. Theory Ser. A*, 46:183–211, 1987.

[Sch90] N. SCHAPPACHER. *Séminaire de Théorie des Nombres, Paris 1988–1989*, volume 91 of *Progr. Math.*, chapter Développement de la loi de groupe sur une cubique, pages 159–184. Birkhauser, 1990.

[Sch91a] C. P. SCHNORR. Efficient signature generation by smart cards. *J. of Cryptology*, 4(3):161–174, 1991.

[Sch91b] R. SCHOOF. The exponents of the groups of points on the reductions of an elliptic curve. In G. VAN DER GEER, F. OORT, AND J. STEENBRINK, editors, *Arithmetic Algebraic Geometry*, volume 89 of *Progress in Mathematics*, pages 325–335. Birkhäuser, 1991.

[Sch95a] R. SCHOOF. Counting points on elliptic curves over finite fields. *J. Théor. Nombres Bordeaux*, 7:219–254, 1995.

[Sch95b] R. SCHOOF. Families of curves and weight distributions of codes. *Bull. Amer. Math. Soc.*, 32(2):171–183, April 1995.

[Sem98] I. A. SEMAEV. Evaluation of discrete logarithms on some elliptic curves. Preprint, 1998.

[Ser70] J.-P. SERRE. *Cours d'arithmétique*. PUF, 1970.

[Ser83] J.-P. SERRE. Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini. *C. R. Acad. Sci. Paris Sér. I Math.*, 296:397–402, 1983.

[Shi71] G. SHIMURA. *Introduction to the arithmetic theory of automorphic functions*, volume 11 of *Publications of the Mathematical Society of Japan*. Iwanami Shoten and Princeton University Press, 1971.

[Sho91] V. SHOUP. Smoothness and factoring polynomials over finite fields. *Inform. Process. Lett.*, 38:39–42, 1991.

[Sho92a] M. A. SHOKROLLAHI. Efficient randomized generation of optimal algorithms for multiplication in certain finite fields. *Comput. Complexity*, 2:67–96, 1992.

[Sho92b] M. A. Shokrollahi. Generation of optimal bilinear multiplication algorithms: theory and implementation. Technical Report 8575-CS, Universität Bonn, December 1992.

[Sho92c] M. A. Shokrollahi. Minimum distance elliptic codes. *Adv. Math.*, 93:251–281, 1992.

[Sho92d] M. A. Shokrollahi. Optimal algorithms for multiplication in certain finite fields using elliptic curves. *SIAM J. Comput.*, 21(6):1193–1198, December 1992.

[Sho95] V. Shoup. A new polynomial factorization algorithm and its implementation. *J. Symbolic Comput.*, 20:363–397, 1995.

[Sho97] V. Shoup. Lower bounds for discrete logarithms and related problems. In W. Fumy, editor, *Advances in Cryptology – EUROCRYPT '97*, volume 1233 of *Lecture Notes in Comput. Sci.*, pages 256–266. Springer-Verlag, 1997. International Conference on the Theory and Application of Cryptographic Techniques, Konstanz, Germany, May 1997, Proceedings.

[Sil86] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics.* Springer, 1986.

[Sma97] N. Smart. The discrete logarithm problem on elliptic curves of trace one. Preprint HP-LABS Technical Report (Number HPL-97-128), 1997.

[Sol97] J. A. Solinas. An improved algorithm for arithmetic on a family of elliptic curves. In B. Kaliski, editor, *Advances in Cryptology – CRYPTO '97*, volume 1294 of *Lecture Notes in Comput. Sci.*, pages 357–371. Springer-Verlag, 1997. Proceedings of a conference on the theory and application of cryptography held at the University of California, Santa Barbara, August 18-21, 1997.

[SOOS95] R. Schroeppel, H. Orman, S. O'Malley, and O. Spatscheck. Fast key exchange with elliptic curve systems. In D. Coppersmith, editor, *Advances in Cryptology – CRYPTO '95*, volume 963 of *Lecture Notes in Comput. Sci.*, pages 43–56. Springer-Verlag, 1995. 15th annual International Cryptology Conference, Santa Barbara, California, USA, August 27–31.

[Spa94] A.-M. Spallek. *Kurven vom Geschlecht 2 und ihre Anwendung in Public-Key-Kryptosystemen.* PhD thesis, Universität Gesamthochschule Essen, July 1994.

[ST94] R. J. Stroeker and N. Tzanakis. Solving elliptic diophantine equations by estimating linear forms in elliptic logarithms. *Acta Arith.*, LXVII:177–196, 1994.

[Sta73] H. M. Stark. Class-numbers of complex quadratic fields. In W. Kuyk, editor, *Modular functions of one variable I*, volume 320 of *Lecture Notes in Math.*, pages 155–174. Springer Verlag, 1973. Proceedings International Summer School University of Antwerp, RUCA, July 17-Agust 3, 1972.

[Sta96] H. M. Stark. Counting points on CM elliptic curves. *Rocky Mountain J. Math.*, 26(3):1115–1138, 1996.

[Ste86] N. M. Stephens. Lenstra's factorisation method based on elliptic curves. In H. C. Williams, editor, *Advances in cryptology – CRYPTO '85*, volume 218 of *Lecture Notes in Comput. Sci.* Springer, 1986.

[Sti93] H. Stichtenoth. *Algebraic function fields and codes.* Springer-Verlag, 1993.

[Suy] H. Suyama. Informal preliminary report (8). 25 Oct 1985.

[SvdV91] R. Schoof and M. van der Vlugt. Hecke operators and the weight distributions of certain codes. *J. Combin. Theory Ser. A*, 57:163–186, 1991.

[SW92] M. A. Shokrollahi and K. Werther. Generation of optimal bilinear multiplication algorithms: theory and implementation. Research report 8575-cs, Universität Bonn, December 1992.

[SW93] R. D. Silverman and S. S. Wagstaff, Jr. A practical analysis of the elliptic curve factoring method. *Math. Comp.*, 61:445–462, 1993.

[Tat65] J. Tate. Algebraic cycles and poles of zeta functions. In O. F. G. Schilling, editor, *Arithmetical Algebraic Geometry*, pages 93–110, New-York, 1965.

[Tat66] J. Tate. Endomorphisms of Abelian varieties over finite fields. *Invent. Math.*, 2:134–144, 1966.

[Tes98] E. Teske. Speeding up Pollard's rho method for computing discrete logarithms. In J. P. Buhler, editor, *Algorithmic Number Theory*, volume 1423 of *Lecture Notes in Comput. Sci.*, pages 541–554. Springer-Verlag, 1998. Third International Symposium, ANTS-III, Portland, Oregon, june 1998, Proceedings.

[Tra84] B. M. Trager. *Integration of algebraic functions.* Ph.d., dpt of eecs, MIT, 1984.

[TV91] M. A. Tsfasman and S. G. Vlăduţ. *Algebraic-geometric codes.* Kluwer Acad. Publ., 1991.

[TVZ82] M. A. Tsfasman, S. G. Vlăduţ, and Th. Zink. Modular curves, Shimura curves and Goppa codes that are better than the Varshamov-gilbert bound. *Math. Nachr.*, 109:163–166, 1982.

[TW95] R. Taylor and A. Wiles. Ring theoretic properties of certain Hecke algebras. *Ann. of Math.*, 141:553–572, 1995.

[Ugh88] E. Ughi. On the number of points of elliptic curves over a finite field and a problem of B. Segre. *European J. Combin.*, 4:263–270, 1988.

[vdG91] G. van der Geer. Codes and elliptic curves. In G. van der Geer, F. Oort, and J. Steenbrink, editors, *Arithmetic Algebraic Geometry*, volume 89 of *Progress in Mathematics*, pages 159–168. Birkhäuser, 1991.

[vdGvdV91] G. van der Geer and M. van der Vlugt. Kloosterman sums and the p-torsion of certain Jacobians. *Math. Ann.*, 290:549–563, 1991.

[vdGvdV92a] G. van der Geer and M. van der Vlugt. Reed-Muller codes and supersingular curves. I. *Compositio Math.*, 84:333–367, 1992.

[vdGvdV92b] G. van der Geer and M. van der Vlugt. Supersingular curves of genus 2 over finite fields of characteristic 2. *Math. Nachr.*, 159:73–81, 1992.

[vdGvdV92c] G. van der Geer and M. van der Vlugt. Trace codes and families of algebraic curves. *Math. Z.*, 209:307–315, 1992.

[Vél71] Jacques Vélu. Isogénies entre courbes elliptiques. *C. R. Acad. Sci. Paris Sér. I Math.*, 273:238–241, July 1971. Série A.

[vH94] M. van Hoeij. An algorithm for computing an integral basis in an algebraic function field. *J. Symbolic Comput.*, 18(4):353–364, October 1994.

[vL82] J. H. van Lint. *Introduction to coding theory.* Springer-Verlag, 1982.

[vL90] J. H. van Lint. *Coding theory and desing theory part I: coding theory*, volume 20 of *The IMA volumes in mathematics and its applications*, chapter Algebraic geometric codes, pages 137–162. Springer, 1990. D. Ray-Chaudhuri, Ed..

[Vlă91] S. G. Vlăduţ. *Kronecker's Jugendtraum and modular functions*, volume 2 of *Studies in the development of modern mathematics.* Gordon and Breach science publishers, 1991. Translated from the Russian by M. Tsfasman.

[Vol88] J. F. Voloch. A note on elliptic curves over finite fields. *Bull. Soc. Math. France*, 116:455–458, 1988.

[vOW94] P. C. van Oorschot and M. J. Wiener. Parallel collision search with application to hash functions and discrete logarithms. In *2nd ACM Conference on Computer and Communications Security*, pages 210–218, 1994. Nov. 2-4, Fairfax, Virginia.

[vW97] P. van Wamelen. Examples of genus two CM curves defined over the rationals. To appear in *Math. Comp.*, March 1997.

[VZ95] S. A. Vanstone and R. J. Zuccherato. Short RSA keys and their generation. *J. of Cryptology*, 8(2):101–114, 1995.

[VZ97] S. A. Vanstone and R. J. Zuccherato. Elliptic curve cryptosystems using curves of smooth order over the ring Z_n. *IEEE Trans. Inform. Theory*, IT-43:1231–1237, 1997.

[Wat69] E. Waterhouse. Abelian varieties over finite fields. *Ann. Sci. École Norm. Sup.*, 2:521–560, 1969.

[Web02] H. Weber. *Lehrbuch der Algebra*, volume I, II, III. Chelsea Publishing Company, New York, 1902.

[Wei28] A. Weil. L'arithmétique sur les courbes algébriques. *Acta Math.*, 52:281–315, 1928.

[Wei48] A. Weil. *Sur les courbes algébriques et les variétés qui s'en déduisent*. Hermann, Paris, 1948.

[Wei49] A. Weil. Number of solutions of equations in finite fields. *Bull. AMS*, 55:497–508, 1949.

[Wie90] M. J. Wiener. Cryptanalysis of short RSA secret exponents. *IEEE Trans. Inform. Theory*, 36(3):553–558, May 1990.

[Wil94] K. S. Williams. On finding the solutions of $n = au^2 + buv + cv^2$ in integers u and v. *Utilitas Math.*, 46:3–19, 1994.

[Wil95a] A. Wiles. Modular elliptic curves and Fermat's last theorem. *Ann. of Math.*, 141:443–551, 1995.

[Wil95b] K. S. Williams. Some refinements of an algorithm of Brillhart. In K. Dilcher, editor, *Number Theory*, volume 15 of *CMS Conf. Proc.*, pages 409–416, Providence, RI, 1995. AMS. Fourth Conference of the Canadian Number Theory Association, July 2–8, 1994, Halifax, Nova Scotia, Canada.

[Win79] S. Winograd. On multiplication in algebraic extension fields. *Theoret. Comput. Sci.*, 8:359–377, 1979.

[Wol86] J. Wolfmann. Recent results on coding and algebraic geometry. In J. Calmet, editor, *Algebraic algorithms and error-correcting codes*, volume 229 of *Lecture Notes in Comput. Sci.*, pages 167–184. Springer, 1986. Proc. 3rd International Conference, AAECC-3, Grenoble, France, July 1985.

[Wol87] J. Wolfmann. Nombre de points rationnels de courbes algébriques sur des corps finis associées à des codes cycliques. *C. R. Acad. Sci. Paris Sér. I Math.*, 305:345–348, 1987.

[Wol89a] J. Wolfmann. New bounds on cyclic codes from algebraic curves. In G. Cohen and J. Wolfmann, editors, *Coding theory and applications*, volume 388 of *Lecture Notes in Comput. Sci.*, pages 47–62. Springer-Verlag, 1989. 3rd International Colloquium, Toulon, France, 1988.

[Wol89b] J. Wolfmann. The number of points on certain algebraic curves over finite fields. *Comm. Algebra*, 17(8):2055–2060, 1989.

[Wol89c] J. Wolfmann. The weights of the dual code of the Melas code over GF(3). *Discrete Math.*, 74:327–329, 1989.

[Wol89d] J. Wolfmann. The weights of the orthogonals of certain codes or extended Goppa codes. In T. Mora, editor, *Applied algebra, algebraic algorithms and error-correcting codes*, volume 357 of *Lecture Notes in Comput. Sci.*, pages 476–480. Springer, 1989. Proc. of the 6th international conference, AAECC-6, Rome, July 4-8, 1988.

[WZ98] M. J. Wiener and R. J. Zuccherato. Faster attacks on elliptic curve cryptosystems. In xxx, editor, *SAC '98*, volume xxx of *Lecture Notes in Comput. Sci.*, page yyy. Springer-Verlag, 1998. Available on `http://grouper.ieee.org/groups/1363/contrib.html`.

[Yan95] S. Y. Yan. Primality testing of large numbers in Maple. *Comput. Math. Appl.*, 29(12):1–8, 1995.

[Yat84] S. Yates. Titanic primes. *J. Recr. Math.*, 16:250–260, 1983/84.

[Yat85] S. Yates. Sinkers of the Titanics. *J. Recr. Math.*, 17(4):268–274, 1984/85.

[YZ97] N. Yui and D. Zagier. On the singular values of Weber modular functions. *Math. Comp.*, 66(220):1645–1662, October 1997.

[Zuc98] R. J. Zuccherato. The equivalence between elliptic curve and quadratic function field discrete logarithms in characteristic 2. In J. P. Buhler, editor, *Algorithmic Number Theory*, volume 1423 of *Lecture Notes in Comput. Sci.*, pages 620–638. Springer-Verlag, 1998. Third International Symposium, ANTS-III, Portland, Oregon, june 1998, Proceedings.