Autour de la cryptographie à base de tores algébriques

Clément Dunand

N° d'ordre : 4270 ANNÉE 2010

THÈSE / UNIVERSITÉ DE RENNES 1

sous le sceau de l'Université Européenne de Bretagne

pour le grade de

DOCTEUR DE L'UNIVERSITÉ DE RENNES 1

Mention : mathématiques et applications

École doctorale Matisse

présentée par

Clément Dunand

préparée à l'unité de recherche 6625 du CNRS : IRMAR
Institut de Recherche Mathématique de Rennes
UFR de mathématiques

Autour de la cryptographie à base de tores algébriques

Thèse soutenue à Rennes
le 3 décembre 2010

devant le jury composé de :

Delphine Boucher
Université de Rennes 1 / examinatrice

Claude Carlet
Université de Paris 8 / rapporteur

Jean-Marc Couveignes
Université de Bordeaux / examinateur

Reynald Lercier
DGA & Université de Rennes 1 / directeur de thèse

Christian Maire
Université de Franche-Comté / rapporteur

Felix Ulmer
Université de Rennes 1 / examinateur

À Maman qui, je le sais, aurait adoré feuilleter ce manuscrit...

REMERCIEMENTS

MERCI. Le mot paraît un peu faible quand je pense à la foule de gens que je voudrais mentionner ici. Je dois beaucoup à beaucoup de monde et je suis un peu contrit de n'avoir que ces cinq petites lettres à leur offrir. Je vais tenter d'être le plus méthodique possible afin d'éviter les oublis, longueurs et redondances.

« C'est le rôle essentiel du professeur d'éveiller la joie de travailler et de connaître. » (Albert Einstein)

À l'heure où j'écris ces lignes je n'y suis pas encore, mais je m'imagine le 3 décembre, debout devant le tableau noir. J'ai alors face à moi beaucoup des gens que je souhaite remercier. Au plus près de moi, il y a en premier lieu les membres de mon jury, un exemplaire de ce manuscrit entre les mains. Merci à mes deux rapporteurs, Claude Carlet et Christian Maire, d'avoir accepté la lourde tâche de relire mon travail, et d'avoir fait le déplacement, long et/ou fastidieux j'imagine, jusqu'à Rennes ce jour-là.

Merci à Jean-Marc Couveignes qui vient de loin également, et notamment de contrées à la météo plus hospitalière. Merci aussi de m'avoir invité dans une de ces contrées pour le séminaire de théorie des nombres de Toulouse. Cet exposé très formateur, de par son format justement, m'a permis de prendre pas mal de recul sur mon travail. Merci enfin d'avoir sans compter partagé avec moi votre temps, parfois même en plein mois d'août, et vos lumières. J'ai beaucoup appris de vos savants conseils.

Au premier rang, je croise aussi le regard de Felix Ulmer, sans qui cette thèse n'aurait pas été possible. Merci pour tout car je n'ai pas seulement profité de ton aide administrative mais aussi d'un magnifique cours de théorie des groupes il y a bien longtemps déjà. C'est donc avec émotion et fierté que j'ai partagé avec toi, quelques années plus tard, une partie de ma mission d'enseignement.

J'en viens naturellement à celui qui n'est pas qu'un membre de mon jury, mais qui m'accompagne et me guide depuis bientôt quatre ans maintenant dans cette aventure. Merci à mon directeur de thèse, Reynald Lercier, qui a rempli bien plus que cette fonction officielle. Que ce soit au CÉLAR, les quelques fois où j'ai montré patte blanche, ou dans le bureau 612, j'ai toujours trouvé tout ce dont j'avais besoin. Tout ton savoir lorsque le mien et les livres étaient trop flous, de judicieux conseils lorsque je m'égarais, de précieux encouragements lorsque je stagnais, une patience exemplaire si je stagnais encore, un indéfectible soutien dans toutes nos recherches, mais aussi et surtout toute ton amitié, dans les moments fastes comme dans les moments plus difficiles. Merci de m'avoir attiré vers cet exaltant domaine de recherche, de m'y avoir initié puis accompagné avec tant de bienveillance.

Dans ce bureau 612, nous avons toujours été chaleureusement accueillis par Delphine Boucher. Merci d'avoir accepté de faire partie de mon jury, mais merci aussi pour ton aide et tout le temps que tu nous as accordé lors de nos régulières entrevues ou pour la relecture de mon mémoire, qui s'accompagnait toujours de clairvoyantes remarques. Merci enfin de nous avoir gratifiés de quelques superbes gestes techniques sur le terrain.

Rien de tel que le foot du vendredi pour évacuer toute la pression d'une semaine de travail ou toutes les calories du pot de thèse du jour. J'ai toujours essayé d'être au rendez-vous, malgré quelques entorses à cette règle, et je remercie tous les footeux de toujours avoir bien accueilli le novice que je suis. Je ne prendrai pas le risque de citer tout le monde mais je voudrais quand même rendre hommage aux plus anciens dont Richard, Gweltaz, Arnaud, Jon, Nirmal, Bachir, Yao, Ronan, Serge...

Sur un terrain de foot ou ailleurs, on ne soupçonne pas l'importance que prennent les moments de détente, les parties de rigolade avec les amis. Je voudrais saluer ici tous les gens, jeunes ou vieux, qui ont partagé notre repas au RU, quelques blagues fines ou non, quelques séminaires du midi, comme Yann, Fanny, Jacques, les Matthieu, Fabien, Noura, Sabine, Arnaud, Sandrine, Alina, Pierre, Maher, Gaël, Adrien, Anjara, Jean-Louis, Basile, Yoann, Nicolas, Anna...

Mais il y a un endroit au labo que j'ai occupé plus que tout autre durant ces années, c'est le bureau 620. Ses occupants ainsi que les voisins du 621 ont largement contribué à rendre ces moments agréables. Merci à Viviana, Colas, Noël, Fabrice, Alberto, Mouton pour votre bonne compagnie. Merci Jérémy pour tes multiples talents, qu'il s'agisse de résoudre mes questions mathématiques (je ferai pareil pour toi quand je comprendrai les tiennes), de nous divertir toujours de maintes manières ou d'épeler un mot de sept lettres, l'air grave et le front plissé (alors, M _ _ _ Z _ _ ?).

Lorsque je n'occupais pas mon bureau, j'étais certainement en train de régler telle ou telle question administrative. Je veux remercier tous les membres bienveillants des différents secrétariats auprès de qui j'ai toujours trouvé une aide précieuse. Un grand merci tout spécialement à Véronique Le Goff pour ta disponibilité et tout le

travail que tu accomplis tant du côté des professeurs que du côté des étudiants. J'ai rarement vu autant de dévouement dans un si petit espace (je fais naturellement mention de l'exiguïté de ton bureau).

Merci enfin aux cryptographes d'avoir si bien accueilli le matheux que je suis, notamment au séminaire. Une pensée toute particulière pour mes deux frangins, Thomas le grand et Jean-Gabriel le petit (*sic*).

Il serait réducteur de résumer mon travail à l'écriture de ma thèse ; j'ai aussi dispensé ces dernières années quelques enseignements. Transmettre des connaissances de la manière la plus agréable possible, voilà bien une mission on ne peut plus captivante. Je tiens à remercier tous les enseignants qui, en amont, ont fait naître ma passion pour ce métier, Martine Husson, Michel Pierre, Grégory Vial et Dominique Cerveau pour n'en citer que quatre parmi tant d'autres ou encore Jacques Grandjean à qui je rends hommage ici. Mais je voudrais aussi chaleureusement saluer et remercier en aval tous les élèves et étudiants qui sont passés entre mes griffes. Quel bonheur de vous avoir, incroyable bouffée d'oxygène quand quelque question épineuse m'aura plongé dans une trop longue apnée.

Et puis il y a une vie hors des locaux de la fac aussi. Je voudrais en premier lieu remercier Aurélien qui depuis 4 ans de colocation me supporte avec placidité. Il y a toujours à l'appart un bon petit plat qui mijote, une joyeuse bonne ambiance, quelques douces notes de guitare, la prévision d'un film pourri à la télé, le doux parfum d'un jeu de mots délicat qui plane encore, tout étonné de ce qui lui arrive. Parfois il y a même toutes ces choses à la fois ; merci donc pour ton amitié qui tapisse les sols et les murs de la meilleure colocation qui soit.

« La modération est une chose fatale. « Assez » est mauvais comme un repas. « Trop » est bon comme un festin. » (Oscar Wilde)

Il me tient aussi beaucoup à cœur de remercier tous les amis qui ont participé à nos occasionnelles agapes ; Mikaël, alors ces huîtres c'est pour quand ; Sten, Émilie, j'envie votre situation géographique...je pense aux vignobles bien sûr ; Mathilde tu es la bienvenue chaque fois que tu n'as que des petits pois pour dîner, Damian, *mir hei guet gässe, gäll ?*, Sébastien, flûte, je ne sais que te dire. Merci à tous pour votre amitié et votre bonne humeur. Je profite du couplet gastronomique pour saluer ma deuxième maison, l'*Atelier des Gourmets*, modèle de bon accueil et de cuisine raffinée.

Bien sûr les amis qui n'ont pas ou pas souvent festoyé avec nous méritent aussi un grand coucou, même s'ils ne rentrent pas dans la catégorie précédente. Une amicale pensée donc pour Coko (merci pour le gâteau), Rook et Fifi (putain de caddie), et puis ceux que j'oublie. Ma tête est distraite mais mon cœur ne l'est pas.

« Le plus grand malheur de l'homme, c'est un mariage heureux. Aucun espoir de divorce. » (Milan Kundera)

Si vous n'avez pas encore trouvé un mot vous concernant, c'est certainement que je vous réservais ce paragraphe. J'ai eu la chance de partager avec vous ces moments privilégiés et je vous en suis reconnaissants. Merci Marie et Lionel pour votre cœur en or et votre amitié. Festins, soirée jeux et festivals de bonne blagues ont toujours bien marché grâce à vous. Jean-Romain, Viktoria, obwohl Ihr jetzt leider ein bisschen weit weg von uns seid, ist mir Eure Freundschaft immer sehr wertvoll.

Dans la lignée des jeunes mariés, je pense ici à Ludovic. Mon amitié pour toi est, du moins en l'état actuel des choses, inversement proportionnelle à la fréquence de nos rencontres, mais j'ai le sentiment qu'elle ne s'en trouverait pas diminuée si cette dernière augmentait. Merci enfin à Alexis que je ne classe pas ici pour des raisons de noces (ou alors tu m'aurais caché cela) mais plutôt en tant qu'ami non rennais. Merci pour le bol d'air que tu verses toujours généreusement au milieu de mon monde scientifique.

« La musique c'est du bruit qui pense. » (Victor Hugo)

Il m'aurait été impossible de ne pas mentionner la musique dans ces quelques pages car elle me suit partout et m'offre toujours de délicieux instants. Je pense en premier lieu à mon ami François. Merci pour ton accueil à Toulouse et pour nos moments musicaux. Voilà peut-être ce qui me manque le plus depuis que le sud t'a arraché à nous. Par chance j'ai encore de fréquentes occasions d'étancher ma soif musicale. Merci donc à tous les membres de l'harmonie, de l'ensemble de clarinettes et des écoles de musiques de Betton et Saint-Grégoire ; merci Marie-Claire pour ta confiance et ton amitié.

« Seuls l'art et la science élèvent l'homme jusqu'à la divinité. » (Ludwig van Beethoven)

Merci à tous les gens qui, sans le savoir, ont partagé un peu de mon temps au cours de ces années et dont la compagnie a été des plus agréables. Citons, dans une liste non exhaustive, Frédéric Chopin, Abdel Rahman El Bacha, Johann Sebastian Bach, Glenn Gould, Hilary Hahn, Sharon Kam, Franz Schubert, Claudio Abbado, Dmitri Chostakovitch, Yuja Wang, Ludwig van Beethoven, Sviatoslav Richter, Maurice André, Nathalie Dessay, Antonio Vivaldi, Cecilia Bartoli, Philippe Jaroussky, Maxim Vengerov, Victor Hugo, Boris Vian, Patrick Süskind, Ken Follett, Katie Melua, Tim Burton, Danny Elfman, Matt Groening, Marcel Gotlib...

« Où peut-on être mieux - Qu'au sein de sa famille ? » (François Marmontel)

J'en viens enfin au délicat paragraphe de ma famille. J'ai repoussé l'échéance car je ne sais comment leur témoigner tout mon amour. Et d'ailleurs il existe des odes de plusieurs milliers de vers qui l'expriment bien mieux que tout ce que je pourrais écrire. Je voudrais simplement les remercier tous, qu'ils soient présents ou

absents (tu nous manques quand même, hein...), mes parents en priorité bien sûr, pour leur amour et leur indéfectible soutien dans tout ce que j'aurai entrepris. Mes trop rares retours vers la côte vendéenne constituent toujours une pause privilégiée et indispensable, grâce au bon air marin certes mais surtout pour passer un peu de temps avec les gens qu'on aime.

Les mathématiques sont la poésie des sciences.

Léopold Sédar Senghor

INTRODUCTION

Utile depuis des millénaires, la cryptographie constitue une réponse au besoin ancestral des hommes de communiquer de manière confidentielle. Il peut s'agir de communications individuelles, comme dans les rubriques d'annonces personnelles (*agony columns*) du *Times* au XIX^{e} siècle ; mais beaucoup plus couramment c'est à des fins diplomatiques, militaires ou commerciales que l'on cherche à dissimuler des messages aux yeux de l'adversaire. Le terme cryptographie vient du grec κρύπτω, cacher et γράφω, écrire. Si les premiers balbutiements de cette science datent de plusieurs millénaires, c'est au XX^{e} siècle avec l'avènement de l'informatique et le développement des enjeux commerciaux que les techniques se sont automatisées. Cependant un grand nombre de questions de la cryptographie moderne ont été soulevées indépendamment des nouvelles technologies et de leur utilisation.

Plusieurs critères définissent un bon cryptosystème. À la fin du XIX^{e} siècle, le cryptologue Auguste Kerckhoffs a énoncé sept règles pour assurer une communication confidentielle. Parmi elles on dégage les quelques grands principes suivants. Le premier point est la sécurité : une information codée ne doit pas être accessible sans connaissance de la clef. D'un point de vue de l'utilisation pratique en outre, les cryptogrammes doivent être télégraphiables. En particulier la masse d'information à échanger entre les deux protagonistes ne doit pas être disproportionnée par rapport à la taille du message. Enfin le système doit être simple d'utilisation. C'est dans l'optique de gagner sur l'un ou l'autre de ces points que de nombreux cryptosystèmes et variations de ces derniers ont été élaborés.

On appelle usuellement Alice et Bob les deux protagonistes cherchant à communiquer de manière confidentielle. Le nom de l'adversaire, du pirate, de l'espion de cette conversation est un peu moins consensuel ; je l'appellerai Oscar.

Des guerres médiques aux guerres mondiales

Les premiers Alice et Bob de l'histoire se sont surtout adonnés à la stéganographie, du grec στεγανός qui signifie couvert. Si étymologiquement la différence est ténue, elle est flagrante dans la pratique. La stéganographie consiste simplement à dissimuler physiquement le message que l'on transmet à son interlocuteur. Les plus anciens exemples de tels procédés sont relatés par Hérodote et remontent aux guerres médiques. Vers 499 avant J.-C., Histiée organise la révolte ionienne contre le roi de Perse. Il communique avec Aristagoras de Milet en utilisant la stéganographie, comme en atteste l'extrait suivant. « Il fit raser la tête au plus fidèle de ses esclaves, y imprima des caractères, et attendit que ses cheveux fussent revenus. Lorsqu'ils le furent, il l'envoya aussitôt à Milet, avec ordre seulement de dire, à son arrivée, à Aristagoras de lui raser la tête, et de l'examiner ensuite. » (Hérodote, *Histoires*, livre V : Terpsichore)

Depuis Pline l'Ancien, qui décrit au premier siècle la fabrication de l'encre sympathique, jusqu'à Giovanni Porta qui explique comment cacher un message dans la coquille d'un œuf dur, la stéganographie a profité de la créativité humaine. Cependant elle présente l'inconvénient qu'une fouille minutieuse permet en théorie d'intercepter n'importe quel message. On a donc dû réfléchir à des techniques plus robustes ou des précautions supplémentaires pour garantir une meilleure sécurité.

À cette fin, la cryptographie ne se concentre plus sur la dissimulation du message, mais sur son brouillage. On y distingue deux stratégies bien différentes, la transposition et la substitution. La transposition tout d'abord consiste simplement à réorganiser le message transmis, comme on le fait avec une anagramme. À titre d'exemple, on peut citer la scytale. Il s'agit d'un bâton, aussi appelé bâton de Plutarque, autour duquel on enroule une fine lanière de cuir. Alice l'enroule en spirale jusqu'à recouvrir toute une partie du bâton. Maintenant elle écrit son message le long du bâton, et donc de manière transversale sur la bande de cuir. Elle envoie cette lanière à Bob qui, pour déchiffrer le texte, doit disposer d'un bâton de même diamètre autour duquel l'enrouler pour reconstituer le message. Sans ce dispositif il n'apparaît sur le cuir qu'une succession de caractères sans aucun sens. Le message est bien là, visible de tous, mais dans le désordre.

La sécurité offerte par un ordonnancement aléatoire des lettres du message est très forte du fait de la croissance exponentielle du nombre d'anagrammes d'un texte en fonction de sa longueur. Mais le problème est que le décodage du message d'Alice sera aussi difficile pour Bob que pour Oscar. Pour pallier cette difficulté, la réorganisation des caractères doit répondre à des règles logiques et rigoureuses. Mais en contrepartie la tâche est également facilitée pour l'éventuel espion.

C'est pourquoi, du moins avant l'arrivée des techniques modernes, les procédés de substitution se sont plus largement imposés à grande échelle. Il s'agit cette fois de remplacer le message clair par un autre qui est indéchiffrable si l'on ne dispose

pas de la clef utilisée. On distingue usuellement les *chiffres* et les *codes*. En pratique, un chiffre fait de la substitution lettre par lettre, alors qu'un code a recours à la substitution à l'échelle des mots, phrases ou groupes de lettres. Plusieurs avantages et inconvénients de ces deux techniques apparaissent. D'une part les chiffres offrent une sécurité plus faible car on peut procéder à une analyse des fréquences d'apparition de chaque lettre pour déchiffrer les messages. Cependant ils sont aussi plus facilement utilisables. Un code requiert en effet un dictionnaire beaucoup plus riche. De plus l'éventuelle perte de ce code au profit de l'adversaire est beaucoup plus dramatique car c'est tout un nouveau langage qu'il faut alors mettre au point. C'est pour cette raison que, du XVI^{e} siècle à la seconde guerre mondiale, on a plutôt cherché à chiffrer intelligemment.

L'arme principale d'un cryptanalyste face à un message chiffré est l'analyse des fréquences, qu'il s'agisse des fréquences d'apparition des lettres, groupes de lettres ou motifs. Pour brouiller ces pistes, on peut imaginer tout d'abord écrire sans aucun souci de l'orthographe, ou encore via plusieurs alphabets distincts (chiffre *polyalphabétique*). L'outil le plus célèbre et un des plus aboutis avant l'automatisation du codage est la machine Enigma. Conçue en 1918 par l'inventeur allemand Arthur Scherbius, elle vise à remplacer les systèmes de cryptage vieillots encore utilisés lors de la première guerre mondiale. Elle repose sur des procédés purement mécaniques et électriques, mais mis en œuvre de telle sorte qu'il en résulte un redoutable chiffre polyalphabétique.

Qui dit mécanisation du cryptage dit aussi mécanisation de la cryptanalyse. Dans les années 30, face à l'utilisation de plus en plus judicieuse d'Enigma, le cryptanalyste polonais Marian Rejewski mit au point des machines, appelées *bombes*, capables d'effectuer un grand nombre de tests. Cette technologie, combinée à la fine analyse et l'intelligence de Rejewski, permettait d'intercepter les communications allemandes. Durant la guerre, c'est Alan Turing qui prit la relève en Grande-Bretagne. Malgré les formidables avancées d'Enigma qui tinrent en échec Rejewski à la fin des années 30, Turing parvint à développer de nouvelles bombes encore plus performantes. L'exploitation de ces machines ainsi que l'analyse de certaines failles dans l'utilisation d'Enigma rendirent possible le décryptage de nombreuses communications ennemies.

En 1943 on assista à une nouvelle surenchère des deux côtés. Les communications entre Hitler et ses généraux sont cryptées à l'aide du chiffre de Lorenz, beaucoup plus robuste encore qu'Enigma. Pour en venir à bout, Max Newman à la conception et Tommy Flowers à la réalisation mirent au point la machine *Colossus*, véritable ancêtre de l'ordinateur programmable moderne.

L'avènement de la cryptographie moderne

Jusque dans les années 1970, on a toujours imaginé des cryptosystèmes symétriques. C'est-à-dire qu'Alice et Bob peuvent envoyer un message codé ou déchiffrer

des messages grâce à une clef commune. Il s'agit d'un dictionnaire qu'ils partagent et qui leur permet aussi bien de chiffrer un message que de le décoder. C'est le procédé le plus naturel, le plus intuitif, et celui qui a été utilisé pendant des siècles voire des millénaires. La partie délicate de ce genre de méthodes concerne l'initialisation du système. Il faut se mettre d'accord sur le dictionnaire en question. À cette fin, Alice et Bob doivent se rencontrer une première fois.

C'est alors que l'année 1976 changea beaucoup de choses dans le monde de la cryptographie. Whitfield Diffie et Martin Hellman firent deux bonds en avant grâce à des idées novatrices. Si la première naquit dans l'esprit d'Hellman et la seconde fut dans un premier temps imaginée par Diffie, on associe usuellement leurs noms car c'est finalement leur étroite collaboration qui permit ces découvertes. Simon Singh rapporte, au sujet du processus de négociation de clef mis au point par Hellman, que ce dernier dit : « C'est à moi que la muse a parlé, mais nous avions posé les fondations ensemble. » En 1976 apparaît donc un processus permettant un échange sécurisé de clef entre Alice et Bob. Il porte naturellement le nom de négociation de clef de Diffie-Hellman et permet qu'Alice et Bob se mettent d'accord à distance sur une clef pour leur communication future. La grande innovation est qu'ils n'ont plus besoin de se rencontrer ; ils peuvent grâce à ce système le faire tout en communiquant sur un canal non sécurisé, à condition bien sûr que leurs messages soient transmis de manière fidèle.

Par ailleurs est publié la même année un texte fondateur de Diffie et Hellman, véritable acte de naissance de la cryptographie *à clef publique*. Dans les cryptosystèmes symétriques, Alice et Bob échangent secrètement une clef, dite clef privée, et l'utilisent ensuite pour coder leur communication. En 1975, Diffie eut une idée révolutionnaire, fruit d'une approche très différente de la question et de quelques difficiles années de doute. Il s'agit d'un nouveau type de chiffre qui met en jeu une clef dite publique. Si Alice doit recevoir un message de Bob, elle publie une clef qui permet à Bob de chiffrer son message. Puis ce dernier l'envoie à Alice et l'heureuse destinataire déchiffre son message grâce à une clef secrète dont elle est la seule détentrice. Ce système est dit *asymétrique* car il permet exclusivement l'envoi de messages à destination d'Alice. En revanche, la clef de chiffrement étant publiée par Alice, d'autres personnes peuvent l'utiliser pour lui envoyer un message.

Une fois cette idée publiée, il a ensuite fallu attendre 1978 pour la mise au jour d'une méthode effective fondée sur ce principe. Ron Rivest, Adi Shamir et Leonard Adleman inventent le système RSA, baptisé ainsi d'après leurs trois initiales, et qui reste encore largement utilisé aujourd'hui pour la transmission sécurisée d'informations, notamment dans le monde bancaire. Ils introduisent la notion de fonction *trappe*. Une fonction trappe est une fonction facilement calculable dont l'inverse se calcule également en temps raisonnable, à condition de disposer d'une certaine (petite) quantité d'information supplémentaire. En résumé, les messages sont cryptés à l'aide d'une clef publique et le destinataire les décrypte via ce petit surplus d'in-

formation, la clef privée dont il est seul détenteur. Cette technique va également permettre quelques autres applications, comme signer des messages par exemple.

Le fonctionnement basique de RSA est le suivant. Alice publie une clef comme étant un entier N produit de deux nombres premiers. Bob ou tout autre interlocuteur crypte son message pour Alice via une fonction trappe : une fonction puissance modulo N. Le décryptage peut être effectué par Alice seule grâce à la connaissance des deux facteurs de N. Le secret est garanti par la grande difficulté du problème de factorisation si N est choisi assez grand. C'est également une exponentiation qui est à la base du système ElGamal, publié en 1985.

D'un point de vue théorique, la sécurité de ces systèmes cryptographiques est basée sur des fonctions dites *à sens unique* c'est-à-dire des fonctions dont la réciproque est difficile à calculer. Métaphoriquement, elles consistent à verrouiller un cadenas, opération facile qu'il est ensuite difficile d'inverser. La sécurité du système RSA repose sur un problème reconnu comme difficile, le problème de factorisation. Il est aisé de calculer le produit de deux grands nombres premiers ; en revanche, étant donné le résultat, retrouver les deux termes qui le composent est beaucoup plus difficile, y compris pour un ordinateur si l'on choisit des nombres assez grands. La fonction intervenant dans le système de négociation de clef de Diffie-Hellman est l'élévation à une certaine puissance. L'opération réciproque est le calcul d'un logarithme. Dans un groupe fini, qui est la structure choisie pour ce protocole cryptographique, cela porte le nom de *logarithme discret*. La difficulté de cette opération garantit la sécurité du système.

Les variantes de ces cryptosystèmes ou les modifications qui leur sont apportées visent ensuite à améliorer leur sécurité, leur coût de fonctionnement ou le coût de communication. Nous allons maintenant nous pencher sur le rôle des tores algébriques dans cette évolution. Un premier pas dans cette voie est effectué par Smith et Lennon. En 1993, ils utilisent une fonction à sens unique différente, basée sur des fonctions dites *de Lucas*, pour proposer le cryptosystème LUC qu'ils annoncent comme étant plus robuste que RSA.

Plus tard, en 2000, Lenstra et Verheul proposent une évolution du schéma de Diffie-Hellman sous le nom de XTR. Leur contribution vise à en améliorer l'efficacité. De plus, leur protocole permet aussi une meilleure compression des données. On a vu que le protocole de Diffie-Hellman était développé dans un groupe fini. De manière élémentaire on utilise le groupe multiplicatif $\mathbb{F}_q^\times$ d'un corps fini avec q un nombre premier. Les systèmes basés sur les fonctions de Lucas, déjà, proposent de travailler dans un corps plus grand afin d'augmenter la sécurité du protocole. Avec XTR, Lenstra et Verheul travaillent dans un sous-groupe du groupe multiplicatif de ce corps fini. Ainsi, même si leur motivation première était la recherche d'efficacité, ils profitent en plus de la sécurité maximale de ce corps tout en réduisant le coût de communication : on paramètre plus facilement et plus économiquement un sous-ensemble de l'espace tout entier.

Dès lors le développement de la cryptographie à base de tores algébriques était lancé. Certains des sous-groupes en question, en effet, sont doublés d'une structure de variété algébrique. Plus précisément ils sont les points rationnels sur le corps de base de tores algébriques. Cette structure sera développée dans le chapitre 4.

Toujours est-il que l'on fonde de grands espoirs dans cette nouvelle idée. En guise de groupe, on dispose d'un ensemble de points de taille raisonnable mais qui jouit d'une sécurité beaucoup plus forte, à savoir celle du corps, plus grand, dans lequel il est naturellement plongé. Mais pour profiter de cet avantage, il faut savoir paramétrer ce sous-groupe aussi efficacement que sa taille le permet. La question d'un paramétrage rationnel des tores algébriques est pour l'instant sans réponse et l'on ne dispose que de méthodes *ad hoc* dans des cas particuliers. Ainsi, XTR propose un paramétrage avec deux coordonnées d'un sous groupe de $\mathbb{F}_{q^6}^\times$, soit le gain d'un facteur 3 par rapport à l'écriture directe des six coordonnées sur $\mathbb{F}_q$.

Dans cette voie et à la recherche d'une compression des données, Rubin et Silverberg ont formalisé en 2003 le concept de cryptographie à base de tores et ont proposé un nouveau cryptosystème appelé CEILIDH comme *Compact, Efficient, Improves on LUC, Improves on Diffie-Hellman*. Ce nouveau protocole atteint le même gain que XTR en termes de coût de communication puisqu'il utilise un sous-groupe de $\mathbb{F}_{q^6}^\times$ représenté par deux coordonnées sur $\mathbb{F}_q$. Cependant là encore, la méthode est très particulière et se limite aux petites dimensions.

Organisation du document

Le travail présenté ici a été motivé par les travaux, en 2004 de van Dijk et Woodruff, rejoints par plusieurs autres auteurs en 2005. Ce protocole, décrit plus en détail par la suite, permet de paramétrer des éléments d'un sous-groupe de $\mathbb{F}_{q^n}^\times$ à l'aide de $\varphi(n)$ coordonnées, à condition de l'utiliser sur un grand nombre de points à la fois. Cela s'avèrera donc utile pour des cryptosystèmes nécessitant d'échanger plus d'une information, comme les négociations de clefs multiples. C'est-à-dire que l'on a besoin de $\varphi(n)$ coordonnées par élément paramétré, ainsi qu'un coût complémentaire fixe, quel que soit le nombre des points échangés. D'où un gain asymptotique de $n/\varphi(n)$. Si le gain moyen est à peu près équivalent à celui de XTR ou CEILIDH, ce principe ne souffre pas des mêmes limitations quant à la dimension des objets considérés et au degré de l'extension de corps.

On propose ici par ailleurs une amélioration du coût de fonctionnement de ce protocole, basée sur deux outils majeurs. D'une part les opérations apparaissant dans la mise en œuvre de ce paramétrage sont sensibles à la représentation choisie pour les extensions de corps fini étudiées. Aussi on montre que le choix de bases particulières pour ces extensions permet d'améliorer le coût asymptotique du paramétrage à effectuer. Par ailleurs les tailles des objets considérés font intervenir des polynômes cyclotomiques et leurs inverses modulaires. Des propriétés concernant l'amplitude

de leurs coefficients garantissent également l'efficacité des opérations arithmétiques mises en jeu.

La suite de ce document s'organise autour de deux parties. La première concerne les polynômes cyclotomiques et leur arithmétique. Le résultat principal de cette partie fait l'objet d'un article [19], soumis au *Journal of Computational Mathematics*. La seconde partie aborde la cryptographie et les tores algébriques à proprement parler. Le théorème principal a été publié en 2009 [20].

Le chapitre 1 rappelle les définitions et propriétés arithmétiques élémentaires utiles autour des polynômes cyclotomiques. Puis il présente quelques résultats sur les résultants et la coprimalité de deux polynômes cyclotomiques. En particulier, on démontre le corollaire 1.1 utile dans le chapitre et qui ne semble pas apparaître dans la littérature, bien qu'il soit certainement déjà connu. Enfin le paragraphe 1.3 expose les différents résultats connus quant à la taille des coefficients de polynômes cyclotomiques, qui a été pour les mathématiciens un sujet de fascination depuis plus d'un siècle.

Dans le chapitre 2, on s'intéresse maintenant à certains inverses modulaires de polynômes cyclotomiques, c'est-à-dire l'inverse d'un de ces polynômes, noté Φ_m, modulo un autre Φ_n. Dans le cas où leurs indices m et n sont des diviseurs d'un produit de deux nombres premiers distincts, on parvient à des expressions explicites de ces coefficients, ou du moins à une borne sur leur amplitude. Les différents cas possibles font intervenir diverses techniques algébriques et arithmétiques. On démontre le théorème suivant, résultat principal de cette partie.

Theorème 1.
Pour tous nombres premiers distincts p et r,

(i) $\Phi_p^{-1} \bmod \Phi_1 = 1/p$ *et* $\Phi_1^{-1} \bmod \Phi_p = (-1/p)(X^{p-2} + 2X^{p-3} + \ldots + p - 1)$.

(ii) $\Phi_{pr}^{-1} \bmod \Phi_1 = 1$ *et* $\Phi_1^{-1} \bmod \Phi_{pr} = \sum_{i=0}^{\varphi(pr)-1} v_i X^i$ *avec* $v_i \in \{-1, 0, +1\}$.

(iii) $\Phi_{pr}^{-1} \bmod \Phi_p = \frac{1}{r} \sum_{i=0}^{d-1} X^i$ *avec* $d = r \bmod p$ *et*

$\Phi_p^{-1} \bmod \Phi_{pr} = \frac{1}{r} \sum_{i=0}^{\varphi(pr)-1} v_i X^i$ *avec* $|v_i| < r$.

(iv) $\Phi_p^{-1} \bmod \Phi_r = \sum_{i=0}^{\varphi(r)-1} v_i X^i$ *avec* $v_i \in \{-1, 0, +1\}$.

Le chapitre 3 aborde le problème de la cryptographie à base de tores algébriques, sa genèse, et le travail de van Dijk et Woodruff sur lequel nous nous appuyons. Dans le chapitre 4, on propose une présentation du contexte mathématique de cette étude, à savoir la structure de tore algébrique à proprement parler. On met en évidence

le lien entre les sous-groupes utiles en cryptographie et la structure de variété algébrique sous-jacente. En ce qui concerne les variétés algébriques, on rappelle le calcul de leur dimension. Les groupes que leurs points rationnels décrivent admettent deux définitions plus directes à base d'équations aux normes dont on démontre l'équivalence.

Dans le chapitre 5, on rappelle la construction de bases normales elliptiques pour représenter les extensions de corps finis. On démontre enfin comment leur utilisation, combinée aux résultats de la partie 2, permet d'accélérer les paramétrages de tores proposés par van Dijk et Woodruff. On aboutit au théorème suivant qui annonce, par rapport aux constructions existantes, une amélioration de la complexité asymptotique de ces paramétrages.

Theorème 2.
Soient $p \neq r$ deux nombres premiers impairs et $q \equiv -1 \bmod (pr)$. Alors il existe un algorithme de complexité $n^{2+o(1)} \log^{1+o(1)} q + n^{1+o(1)} \log^{2+o(1)} q$, donné par l'algorithme 2 (paragraphe 5.2.2), qui prend en entrée des éléments de $T_n \times \mathbb{F}_{q^p}^\times \times \mathbb{F}_{q^r}^\times$ et qui renvoie leur image par θ (voir figure 5.2) dans $\mathbb{F}_q^\times \times \mathbb{F}_{q^{pr}}^\times$.

Première partie

Polynômes cyclotomiques

« Учиться, учиться, учиться » как завещал великий Ленин...

Sergueï Prokofiev

CHAPITRE 1

POLYNÔMES CYCLOTOMIQUES ET ARITHMÉTIQUE

Suivant « l'ordre traditionnel du raisonnement » plutôt que la « logique des passions » chère à Camus, nous placerons les prémisses avant la conclusion. Nous présentons dans ce chapitre la notion de polynômes cyclotomiques ainsi que tous les prérequis arithmétiques à l'étude qui en est faite plus loin, et notamment aux résultats qui sont démontrés au chapitre suivant. Le but de ces deux chapitres est l'étude de l'amplitude des coefficients des inverses modulaires de polynômes cyclotomiques. À cette fin plusieurs étapes sont nécessaires.

Qui dit inverse modulaire, c'est-à-dire inverse d'un polynôme modulo un autre, dit coprimalité. Alors on aura besoin de quelques résultats sur les résultants de deux polynômes cyclotomiques. De tels calculs ont été publiés par Apostol et nous les rappelons ici. Ce qui nous intéresse particulièrement dans ces résultants est de savoir à quelle condition ils valent 1 car dans ce cas on sait écrire une relation de Bézout entre les polynômes qui s'avèrera utile par la suite.

Enfin on en arrive à la question de la taille des coefficients. Avant d'examiner les polynômes inverses, on rappelle les études menées depuis la fin du XIX^{e} siècle autour des polynômes cyclotomiques eux-mêmes. La taille (je parlerai en général en valeur absolue) des coefficients des polynômes cyclotomiques intrigue les mathématiciens depuis le XIX^{e} siècle. En effet on peut trouver des coefficients arbitrairement grands pour ces polynômes. Cependant quand on les calcule de manière récursive, on observe des coefficients très petits. Par exemple les 104 premiers polynômes cyclotomiques n'ont pas de coefficients autres que -1, 0 ou $+1$. Dans le cas d'indices composés de quelques facteurs premiers, on a obtenu des bornes sur ces coefficients.

1.1 Définitions et propriétés élémentaires

On commence par un rapide inventaire de quelques propriétés très classiques mais qui nous seront utiles concernant les fonctions indicatrice d'Euler et μ de Möbius. On renvoie le lecteur vers les références indiquées ou tout autre livre de théorie des nombres pour plus de détails sur ces résultats.

La *fonction indicatrice d'Euler* (voir par exemple Itard [29]) est notée φ et pour tout entier $n > 0$, $\varphi(n)$ désigne le nombre d'entiers positifs inférieurs à n qui sont premiers avec n. En particulier $\varphi(n)$ désigne le cardinal de $(\mathbb{Z}/n\mathbb{Z})^\times$, groupe des inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$. L'indicatrice d'Euler a une propriété de multiplicativité, à savoir que si deux entiers m et n sont premiers entre eux, alors $\varphi(mn) = \varphi(m)\varphi(n)$.

En outre il en existe une expression explicite, si l'on note $n = \prod_{i=1}^{r} p_i^{a_i}$ la décomposition de n en produit de facteurs premiers, alors

$$\varphi(n) = \prod_{i=1}^{r} (p_i^{a_i} - p_i^{a_i - 1}).$$

Une autre propriété classique et qui nous sera utile est la formule d'inversion de Möbius. La *fonction de Möbius* (voir par exemple Tenenbaum *et al.* [48]) est notée μ et est définie pour tout entier positif n par :

$$\mu(n) = \begin{cases} 1 & \text{si } n = 1, \\ (-1)^k & \text{si } n \text{ est produit de } k \text{ nombres premiers distincts}, \\ 0 & \text{sinon.} \end{cases}$$

Une première propriété calculatoire de la fonction de Möbius concerne la somme de ses valeurs en tous les diviseurs positifs d'un entier. Pour tout $n \in \mathbb{N}^*$,

$$\sum_{d|n} \mu(d) = \begin{cases} 0 \text{ si } n > 1, \\ 1 \text{ sinon.} \end{cases} \tag{1.1}$$

La formule d'inversion de Möbius est valable pour toute fonction arithmétique (c'est-à-dire dont le domaine est $\mathbb{N}^*$), mais on l'écrit ici pour φ car c'est la version qui nous servira. Si on note $\psi(n) = \sum_{d|n} \varphi(d)$, alors $\varphi(n) = \sum_{d|n} \mu\left(n/d\right) \psi(d)$. On en a aussi une version multiplicative :

$$\text{si } \psi(n) = \prod_{d|n} \varphi(d), \text{ alors } \varphi(n) = \prod_{d|n} \psi(d)^{\mu\left(\frac{n}{d}\right)}. \tag{1.2}$$

Définition 1.1.
Pour $n \in \mathbb{N}^*$, on appelle n^{e} polynôme cyclotomique *et l'on note Φ_n le polynôme unitaire dont les racines sont exactement les racines primitives n^{es} de l'unité.*

Pour ce qui concerne les polynômes cyclotomiques, on peut se référer par exemple à [15]. On peut démontrer les propriétés suivantes.

Proposition 1.1.

(i) $X^n - 1 = \prod_{d|n} \Phi_d(X)$.

(ii) $\Phi_n(X) = \prod_{d|n} (X^d - 1)^{\mu(n/d)}$.

(iii) *Le polynôme Φ_n est à coefficients entiers et de degré $\varphi(n)$.*

(iv) *Si p est premier et ne divise pas n, alors*

$$\Phi_{pn}(X) = \frac{\Phi_n(X^p)}{\Phi_n(X)};$$

en revanche si p divise n, alors $\Phi_{pn}(X) = \Phi_n(X^p)$.

(v) *Si n est impair, $\Phi_{2n}(X) = \Phi_n(-X)$.*

On peut noter que l'assertion *(i)* de la proposition ci-dessus permet de calculer les polynômes cyclotomiques de manière récursive. En outre, la même assertion fournit, via l'égalité des degrés des polynômes mis en jeu, la propriété suivante de la fonction indicatrice d'Euler :

$$n = \sum_{d|n} \varphi(d).$$

L'assertion *(ii)* donne, dans le cas particulier d'un nombre premier p :

$$\Phi_p(X) = \frac{X^p - 1}{X - 1} = 1 + X + \ldots + X^{p-1}.$$

Enfin l'assertion *(iv)* donne, dans le cas particulier d'une puissance d'un nombre premier p,

$$\Phi_{p^\alpha}(X) = \Phi_p\left(X^{p^{\alpha-1}}\right). \tag{1.3}$$

Une autre propriété moins immédiate et qui nous sera utile concerne l'évaluation en 1 d'un polynôme cyclotomique. On peut montrer que pour tout entier $n \geqslant 1$,

$$\Phi_n(1) = \begin{cases} p & \text{si } n = p^a,\ p \text{ premier},\ a \in \mathbb{N}^*, \\ 1 & \text{sinon.} \end{cases} \tag{1.4}$$

La démonstration de ce résultat se fait de manière récursive sur le nombre de facteurs premiers de n.

Pour $n = p$ premier, on a $\Phi_p(1) = 1^0 + 1^1 + 1^2 + \cdots + 1^{p-1} = p$; tout aussi facilement, lorsque $m = p^a$, il suffit d'évaluer en 1 l'équation (1.3).

Plus généralement pour $m = p_1^{a_1} \dots p_r^{a_r}$ on utilise l'assertion *(i)* de la proposition 1.1. En factorisant par $X - 1$ et en évaluant à nouveau en 1, on trouve

$$n = \prod_{\substack{d|n \\ d>1}} \Phi_d(1).$$

Les termes où d est une puissance d'un nombre premier font, d'après l'étude du cas précédent, apparaître $p_1^{a_1} \dots p_r^{a_r}$. Les autres termes sont donc nécessairement tous égaux à 1.

1.2 Coprimalité

Deux polynômes cyclotomiques distincts sont toujours premiers entre eux car ils n'ont aucune racine en commun. En effet les racines primitives n^{es} et m^{es} de l'unité ne coïncident jamais si $m \neq n$.

Ce qui nous intéresse plus à terme, ce sont les évaluations des polynômes cyclotomiques en une puissance d'un nombre premier. Pour cela la première étape est l'étude des résultants de deux polynômes cyclotomiques. Il s'agit d'un résultat dû à Apostol en 1970 dont on rappelle la démonstration ici en guise d'introduction au type des calculs menés par la suite.

Notations. Dans toute la suite, $\mathcal{P}$ désigne l'ensemble des nombres premiers. Par ailleurs pour ne pas alourdir les écritures, on emploiera pour désigner le pgcd de deux nombres A et B la notation (A, B).

Theorème 1.1 (Apostol, [2])**.**
On a les formules suivantes pour les résultants de polynômes cyclotomiques.

(i) *Soit $m > 1$, alors*

$$\operatorname{Res}(\Phi_1, \Phi_m) = \begin{cases} p & \text{si } m = p^a, \text{ } p \text{ premier, } a \geqslant 1, \\ 1 & \text{sinon.} \end{cases}$$

(ii) *Soient $m > n > 1$. Pour tout diviseur d de n, si $\frac{m}{(m,d)}$ est une puissance d'un nombre premier p, on note $\frac{m}{(m,d)} = p^a$. Alors*

$$\operatorname{Res}(\Phi_m, \Phi_n) = \prod_{\substack{d|n \\ p\in\mathcal{P} \text{ tel que } \frac{m}{(m,d)}=p^a}} p^{\mu(n/d)\frac{\varphi(m)}{\varphi(p^a)}}. \tag{1.5}$$

En d'autres termes, le produit est réalisé sur les diviseurs d de n et pour chacun de ces diviseurs, un terme apparaît lorsque $\frac{m}{(m,d)}$ est une puissance p^a d'un nombre premier.

Démonstration.

On utilisera les formules suivantes pour le calcul de résultant. Étant donnés deux polynômes notés $A(X) = a_n \prod_{k=1}^{n}(X - x_k)$ et $B(X) = b_m \prod_{j=1}^{m}(X - y_j)$, on a

$$\mathrm{Res}(A, B) = a_n^m b_m^n \prod_{k=1}^{n}\prod_{j=1}^{m}(x_k - y_j) = a_n^m \prod_{k=1}^{n} B(x_k). \tag{1.6}$$

Tout d'abord pour $\mathrm{Res}(\Phi_1, \Phi_m)$, il suffit de savoir que $\Phi_1(X) = X - 1$. Alors la formule (1.6) du résultant donne $\mathrm{Res}(\Phi_1, \Phi_m) = \Phi_m(1)$, ce qui démontre le premier point d'après l'équation (1.4).

Venons-en au calcul moins immédiat de $\mathrm{Res}(\Phi_m, \Phi_n)$. On utilise la formule d'inversion de Möbius, et plus précisément sa version exponentielle, donnée par l'équation (1.2). Le résultant possède une propriété de multiplicativité qui entraîne

$$\begin{aligned} \mathrm{Res}(\Phi_m, X^n - 1) &= \prod_{d|n} \mathrm{Res}(\Phi_m, \Phi_d), \text{ puis par inversion de Möbius :} \\ \mathrm{Res}(\Phi_m, \Phi_n) &= \prod_{d|n} \mathrm{Res}(\Phi_m, X^d - 1)^{\mu\left(\frac{n}{d}\right)}. \end{aligned} \tag{1.7}$$

Or on a

$$\begin{aligned} \mathrm{Res}(\Phi_m, x^d - 1) &= \prod_{\substack{1\leqslant k\leqslant m \\ (k,m)=1}} \left(e^{2ik\pi d/m} - 1\right) \quad \text{(formule (1.6))}, \\ &= \prod_{\substack{1\leqslant k\leqslant m \\ (k,m)=1}} \left(1 - e^{2i\pi\left(\frac{kd}{m}\right)}\right) \end{aligned}$$

car il y a $\varphi(m)$ facteurs et que $\varphi(m)$ est pair pour $m > 2$. On va maintenant réindexer le produit. Comme les entiers d et m ne sont *a priori* pas premiers entre eux, on va introduire $\delta = \mathrm{pgcd}(d, m)$ et écrire $\frac{kd}{m} = \frac{k(d/\delta)}{m/\delta}$ dans l'exponentielle.

Maintenant on va partitionner l'ensemble des indices k considérés suivant leur congruence modulo m/δ,

$$\{1 \leqslant k \leqslant m, (k, m) = 1\} = \bigsqcup_{\substack{1\leqslant r\leqslant m/\delta \\ (r,m/\delta)=1}} \{1 \leqslant k \leqslant m, (k, m) = 1, k \equiv r \bmod (m/\delta)\}.$$

Cette partition découpe l'ensemble $\{1 \leqslant k \leqslant m, (k, m) = 1\}$ en parties de même cardinal $\varphi(m)/\varphi(m/\delta)$. Pour cela on peut la voir comme l'union disjointe des fibres $r(\mathrm{Ker}\ f)$ du morphisme de groupes

$$\begin{aligned} f : \ (\mathbb{Z}/m\mathbb{Z})^\times &\to (\mathbb{Z}/(m/\delta)\mathbb{Z})^\times, \\ k &\mapsto r = k \bmod (m/\delta). \end{aligned}$$

Pour démontrer sa surjectivité, on construit pour r premier avec m/δ un antécédent k premier avec m défini par le système de congruences

$$\begin{cases} k \equiv r \bmod (m/\delta), \\ k \equiv 1 \bmod m', \end{cases}$$

où m' est le produit des facteurs premiers de m qui sont premiers avec m/δ. Ainsi le théorème chinois garantit l'obtention du k recherché. On peut trouver ce raisonnement plus en détail dans [1, lemme 6].

Pour tout $k \equiv r \bmod (m/\delta)$, on a

$$e^{2i\pi\left(\frac{kd}{m}\right)} = \left(e^{2i\pi\left(\frac{r}{m/\delta}\right)}\right)^{d/\delta}.$$

De plus d/δ et m/δ sont premiers entre eux. Donc lorsque r parcourt $\{1 \leqslant r \leqslant m/\delta, (r, m/\delta) = 1\}$, il en est de même pour rd/δ. on peut finalement réindexer et regrouper les termes du produit, si bien que

$$\begin{aligned} \operatorname{Res}(\Phi_m, X^d - 1) &= \prod_{\substack{1 \leqslant r \leqslant m/\delta \\ \left(r, \frac{m}{\delta}\right)=1}} \left(1 - e^{2i\pi r/(m/\delta)}\right)^{\varphi(m)/\varphi\left(\frac{m}{\delta}\right)}, \\ &= \Phi_{m/\delta}(1)^{\varphi(m)/\varphi\left(\frac{m}{\delta}\right)}, \end{aligned}$$

soit $p^{\varphi(m)/\varphi\left(\frac{m}{\delta}\right)}$ si m/δ est une puissance de p premier, et 1 sinon. Il reste à réinjecter ce résultat dans la formule (1.7) pour obtenir le second point de la proposition.

□

Cela entraîne une intéressante propriété des polynômes cyclotomiques dont on n'a pas trouvé de démonstration dans la littérature, bien que ce résultat semble assez classique.

Corollaire 1.1.
Soient $m > n \geqslant 1$ des entiers. Alors

$$\operatorname{Res}(\Phi_m, \Phi_n) \neq 1 \Leftrightarrow m = np^a \quad \textit{avec } p \textit{ un nombre premier et } a \geqslant 1.$$

Démonstration.

Ce résultat repose sur la proposition précédente. C'est évident lorsque $n = 1$. En effet :

$$\operatorname{Res}(\Phi_m, \Phi_1) = (-1)^{\varphi(m)} \operatorname{Res}(\Phi_1, \Phi_m)$$

et $\varphi(m)$ est pair dès que $m > 2$. Alors le résultant vaut 1 si et seulement si m n'est pas une puissance d'un nombre premier.

Démontrons-le maintenant pour $m > n > 1$. On va retravailler l'équation (1.5) du théorème 1.1. Il s'agit d'évaluer les contributions de chaque diviseur d de n au résultant $\mathrm{Res}(\Phi_m, \Phi_n)$. Un facteur $p^{\mu(n/d)\frac{\varphi(m)}{\varphi(p^a)}}$ apparaît dans le produit lorsque le d correspondant est tel que $\frac{m}{(m,d)} = p^a$.

On va tout d'abord isoler l'éventuel facteur commun à m et n, c'est-à-dire que l'on écrit $m = wM$ et $n = wN$ avec $(M, N) = 1$. Comme tout diviseur d de n est désormais premier avec M, on a

$$\frac{m}{(m,d)} = \frac{wM}{(wM,d)} = \frac{w}{(w,d)}M.$$

Dans le cas d'une contribution non triviale au produit, on a $\frac{w}{(w,d)}M = p^a$, ce qui entraîne que M est aussi une puissance de p. Notons $M = p^\alpha$ et alors $\frac{w}{(w,d)} = p^{a-\alpha}$. Si p apparaît à une puissance strictement supérieure à 1 dans $\frac{w}{(w,d)}$, alors c'est aussi le cas dans n/d et c'est alors $\mu(n/d)$ qui s'annule et neutralise la contribution au produit. Seuls deux cas se présentent donc : $a = \alpha$ ou $a = \alpha + 1$.

1er cas : $a = \alpha$. Dans ce cas $\frac{w}{(w,d)} = 1$, donc w divise d. Notons $d = wd'$. Alors on a pour contribution au produit les termes

$$\prod_{d'|N} p^{\mu(N/d')\frac{\varphi(m)}{\varphi(p^\alpha)}} = \left(p^{\frac{\varphi(m)}{\varphi(p^\alpha)}}\right)^{\sum_{d'|N}\mu\left(\frac{N}{d'}\right)}.$$

2e cas : $a = \alpha + 1$. Dans ce cas $d = wd'/p$ et l'on trouve dans le produit les termes

$$\prod_{d'|N} p^{\mu\left(\frac{pN}{d'}\right)\frac{\varphi(m)}{\varphi(p^{\alpha+1})}} = \left(p^{\mu(p)\frac{\varphi(m)}{\varphi(p^{\alpha+1})}}\right)^{\sum_{d'|N}\mu\left(\frac{N}{d'}\right)}$$

d'après la multiplicativité de la fonction μ.

On peut réindexer $\sum_{d'|N}\mu\left(\frac{N}{d'}\right) = \sum_{d'|N}\mu(d')$ et l'on distingue finalement les deux formes suivantes pour le résultant, suivant que seul le cas $a = \alpha$ se présente ou que les diviseurs d font apparaître les deux éventualités $a = \alpha$ et $a = \alpha + 1$. On rappelle également dans cette formule synthétique que le résultant vaut 1 si M n'est pas une puissance d'un nombre premier.

$$\mathrm{Res}(\Phi_m, \Phi_n) = \begin{cases} 1 \text{ si } M \neq p^\alpha, \\ \left(p^{\frac{\varphi(m)}{\varphi(p^\alpha)}}\right)^{\sum_{d'|N}\mu(d')} & \text{si } a = \alpha, \\ \left(p^{\frac{\varphi(m)}{\varphi(p^\alpha)}} p^{\mu(p)\frac{\varphi(m)}{\varphi(p^{\alpha+1})}}\right)^{\sum_{d'|N}\mu(d')} & \text{si } a = \alpha \text{ et } a = \alpha + 1. \end{cases} \tag{1.8}$$

Dans tous les cas, les puissances de p sont différentes de 1, donc

$$\mathrm{Res}(\Phi_m, \Phi_n) \neq 1 \Leftrightarrow \sum_{d_2|N} \mu(d_2) \neq 0 \Leftrightarrow N = 1 \Leftrightarrow m = np^a,$$

avec p un nombre premier et $a \geqslant 1$.

□

Corollaire 1.2.
Pour tous entiers q et $m > n \geqslant 1$, si m ne divise pas n, alors $\Phi_m(q)$ et $\Phi_n(q)$ sont premiers entre eux.

Démonstration.
Si m ne divise pas n, on sait d'après le corollaire 1.1 que $\mathrm{Res}(\Phi_m, \Phi_n) = 1$, ce qui est valable dans $\mathbb{Z}$ mais aussi dans $\mathbb{Z}/\ell\mathbb{Z}$ pour tout $\ell \in \mathbb{Z}$. Si $\Phi_m(q)$ et $\Phi_n(q)$ avaient un facteur commun, disons ℓ, alors Φ_m et Φ_n auraient pour racine commune q dans $\mathbb{Z}/\ell\mathbb{Z}$ et leur résultant serait alors nul, ce qui est faux.

□

1.3 Taille des coefficients

En ce qui concerne la taille des coefficients de polynômes cyclotomiques, deux approches majeures ont été développées. D'une part une approche asymptotique montre que l'on peut trouver des coefficients arbitrairement grands dans des polynômes cyclotomiques bien choisis. D'autre part, des polynômes cyclotomiques Φ_n avec n assez simple, produit de peu de facteurs premiers, font apparaître des coefficients étonnamment petits. En particulier, l'assertion *(v)* de la proposition 1.1 nous montre que l'amplitude des coefficients ne se trouve pas modifiée par la multiplication de n par 2.

Dans toute la suite, on écrit

$$\Phi_n(X) = \sum_{k=0}^{\varphi(n)} a_k(n) X^k.$$

Lorsqu'il n'y a pas d'ambiguïté, on note simplement a_k les coefficients.

1.3.1 Polynômes cyclotomiques binaires

On appelle polynômes cyclotomiques *binaires* les polynômes Φ_{pq} avec p et q deux nombres premiers impairs distincts. Dès la fin du XIX$^{\text{e}}$ siècle, Migotti et Bang montrent que leurs coefficients sont tous égaux à 0 ou ± 1.

Theorème 1.2 (Migotti, [38],Bang, [4])**.**
Pour tout $0 \leqslant k \leqslant \varphi(pq)$,

$$a_k(pq) \in \{-1, 0, +1\}.$$

En 1964, Marion Beiter [7] donne un critère pour que leur valeur soit 0, 1 ou -1.

Theorème 1.3 ([7]).
Pour tout $0 \leqslant k \leqslant \varphi(pq)$,

$$a_k(pq) = \begin{cases} (-1)^\delta \text{ si l'on a } k = \alpha p + \beta q + \delta \text{ de manière unique,} \\ 0 \text{ sinon.} \end{cases}$$

avec $\alpha, \beta \in \mathbb{N}$ *et* $\delta \in \{0, +1\}$.

À titre d'illustration, pour $\Phi_{15}(X) = X^8 - X^7 + X^5 - X^4 + X^3 - X + 1$, on a $p = 3$ et $q = 5$. Le coefficient a_2 est nul car 2 ne s'écrit pas $3\alpha + 5\beta + \delta$ avec α, β, δ comme ci-dessus. Le nombre 6, quant à lui admet deux décompositions distinctes $2p + 0q + 0$ et $0p + 1q + 1$, c'est pourquoi a_6 est nul également. En revanche tous les autres entiers compris entre 0 et $\varphi(15) = 8$ admettent une unique écriture de ce type.

Le calcul effectué par Marion Beiter pour établir ce résultat repose sur l'expression *(ii)* de la proposition 1.1 où l'on développe en série le terme $1/(1 - X^p)$.

$$\begin{aligned} \Phi_{pq}(X) &= \frac{(X^{pq} - 1)(X - 1)}{(X^p - 1)(X^q - 1)}, \\ &= (1 - X)(1 + X^q + \ldots + X^{(p-1)q}) \sum_{\beta=0}^{+\infty} X^{\beta p}, \\ &= \sum_{\alpha=0}^{p-1} X^{\alpha q} \sum_{\beta=0}^{+\infty} X^{\beta p} - \sum_{\alpha=0}^{p-1} X^{\alpha q+1} \sum_{\beta=0}^{+\infty} X^{\beta p}, \\ &= \sum_{\alpha,\beta,\delta} (-1)^\delta X^{\alpha q+\beta p+\delta}, \end{aligned}$$

où α va de 0 à $p-1$, β parcourt l'ensemble des entiers naturels et δ prend simplement les valeurs 0 et 1.

L'examen du terme général de cette somme lui a permis de conclure : on étudie les éventuelles décompositions des entiers $k \in [0, \varphi(pq)]$ sous la forme $\alpha q + \beta p + \delta$. Lorsqu'il n'existe pas de telle partition de k, le coefficient a_k correspondant est nul. Lorsqu'il en existe une unique, le coefficient a_k vaut $(-1)^\delta$. Enfin si deux décompositions distinctes existent,

$$k = \alpha_1 q + \beta_1 p + \delta_1 = \alpha_2 q + \beta_2 p + \delta_2,$$

alors $\delta_1 \neq \delta_2$. En effet, sinon on a $q(\alpha_1 - \alpha_2) = p(\beta_1 - \beta_2)$. Mais alors p divise $\alpha_1 - \alpha_2$ et comme $\alpha < p$, nécessairement $\alpha_1 - \alpha_2 = \beta_1 - \beta_2 = 0$. On a donc deux décompositions

distinctes avec des δ distincts et dans ce cas le coefficient correspondant est $a_k = (-1)^0 + (-1)^1 = 0$.

Dans le même article [7], Marion Beiter ajoute, en s'appuyant sur la même écriture sommatoire, le calcul du coefficient central de Φ_{pq}.

Theorème 1.4 (Beiter, [7])**.**
Le coefficient central de Φ_{pq} a pour valeur

$$a_{\varphi(pq)/2}(pq) = (-1)^{k-1},$$

où k est le plus petit entier positif tel que $pk \equiv 1 \bmod q$.

Deux ans plus tard, en 1966, Carlitz [12] calcule le nombre de coefficients non nuls dans Φ_{pq}.

Theorème 1.5 (Carlitz, [12])**.**
Si l'on suppose $p < q$ premiers et que l'on définit $0 < u < p$ tel que $qu \equiv -1 \bmod p$, alors le nombre de coefficients strictement positifs dans Φ_{pq} est

$$N_+ = \frac{(p-u)(uq+1)}{p}.$$

Et les termes non nuls sont au nombre de $2N_+ - 1$.

Enfin en 1996 Lam et Leung [31] donnent une expression totalement explicite de Φ_{pq} (théorème 1.6), avec une démonstration élégante. Une fois n'est pas coutume, l'énoncé du théorème se trouve après sa démonstration pour des raisons de notations.

On considère $n = pq$ produit de deux nombres premiers distincts. Alors Φ_{pq} est de degré $\varphi(pq) = (p-1)(q-1)$ d'après la propriété de multiplicativité de l'indicatrice d'Euler. Comme p et q sont deux nombres premiers distincts, il existe r et s deux entiers positifs tels que $(p-1)(q-1) = pr + qs$. En effet il s'agit simplement des entiers vérifiant $r + 1 = 1/p \bmod q$ et $s + 1 = 1/q \bmod p$.

En outre, si l'on appelle ζ une racine primitive pq-ième de l'unité, alors ζ^p et ζ^q sont des racines primitives respectivement q^{e} et p^{e} de l'unité. Cela se traduit par les deux égalités suivantes.

$$\Phi_q(\zeta^p) = \sum_{i=0}^{q-1} (\zeta^p)^i = 0 \quad \text{et} \quad \Phi_p(\zeta^q) = \sum_{j=0}^{p-1} (\zeta^q)^j = 0.$$

En coupant ces sommes respectivement à r et s, on obtient

$$\sum_{i=0}^{r} (\zeta^p)^i = -\sum_{i=r+1}^{q-1} (\zeta^p)^i \quad \text{et} \quad \sum_{i=0}^{s} (\zeta^q)^j = -\sum_{j=s+1}^{p-1} (\zeta^q)^j.$$

Ceci nous donne, en multipliant ces deux égalités terme à terme,

$$\left(\sum_{i=0}^{r}\zeta^{ip}\right)\left(\sum_{j=0}^{s}\zeta^{jq}\right)-\left(\sum_{i=r+1}^{q-1}\zeta^{ip}\right)\left(\sum_{i=s+1}^{p-1}\zeta^{jq}\right)=0.$$

Ainsi, on a un polynôme dont ζ est racine. Comme de plus $\zeta^{pq}=1$, ζ est racine du polynôme

$$f(X)=\underbrace{\left(\sum_{i=0}^{r}X^{ip}\right)\left(\sum_{j=0}^{s}X^{jq}\right)}_{f_1(X)}-\underbrace{\left(\sum_{i=r+1}^{q-1}X^{ip}\right)\left(\sum_{i=s+1}^{p-1}X^{jq}\right)X^{-pq}}_{f_2(X)}.$$

si l'on note $f(X)=f_1(X)-f_2(X)$ comme ci-dessus, alors le degré de f_1 est $rp+sq$, c'est-à-dire $(p-1)(q-1)$ d'après la définition de r et s. Quant au degré de f_2, il est borné par $(r+1)p+(s+1)q-pq$ et $(q-1)p+(p-1)q-pq$, c'est-à-dire par 1 et $\varphi(pq)-1$.

Le degré de f_2 est donc $(p-1)(q-1)-1$, et c'était là tout l'intérêt d'y faire intervenir le monôme X^{-pq}. Finalement $f(X)$ est un polynôme de degré $(p-1)(q-1)=\varphi(pq)$ dont toutes les racines primitives pq-ièmes de l'unité sont racines. Donc $f(X)=\Phi_{pq}(X)$, ce qui fournit une expression explicite de Φ_{pq}.

Ceci démontre le théorème suivant.

Theorème 1.6 (Lam & Leung, [31])**.**
Soient p et q deux nombres premiers distincts. Alors pour tout $0\leqslant k\leqslant\varphi(pq)$,

$$a_k(pq)=\begin{cases}+1 \text{ si } k=ip+jq \text{ avec } i\leqslant r \text{ et } j\leqslant s,\\ -1 \text{ si } k+pq=ip+jq \text{ avec } i>r \text{ et } j>s,\\ 0 \text{ sinon.}\end{cases}$$

On peut remarquer que ce calcul démontre aussi que les $+1$ et les -1 alternent parmi les coefficients de Φ_{pq} (au milieu d'autres coefficients nuls bien sûr). Par ailleurs, le nombre de termes non nuls calculé par le théorème 1.5 de Carlitz peut s'exprimer plus simplement avec les r et s ainsi construits : le nombre de $+1$ est $(r+1)(s+1)$ et le nombre de -1 est $(p-s-1)(q-r-1)$ et ces deux quantités diffèrent de 1 ; d'où un nombre total de coefficients non nuls égal à $2(r+1)(s+1)-1$. Enfin, le coefficient central de Φ_{pq} s'écrit aussi très simplement avec ces notations : il est simplement égal à $(-1)^r$.

1.3.2 Polynômes cyclotomiques ternaires

On appelle polynômes cyclotomiques *ternaires* les polynômes Φ_{pqr} avec $p<q<r$ trois nombres premiers impairs. Des estimations ont également été obtenues sur

l'amplitude de leurs coefficients. Dès 1895, Bang [4] montre qu'ils admettent pour borne supérieure (en valeur absolue) $p-1$.

En 1968, Marion Beiter conjecture une borne plus fine.

Conjecture 1.1 (Beiter, [8])**.**
Pour tout $0 \leqslant k \leqslant \varphi(pqr)$,

$$|a_k(pqr)| \leqslant \frac{p+1}{2}.$$

Deux ans plus tard, Möller montre que si elle était établie, cette borne serait la meilleure possible, ce qui lui confère un caractère d'optimalité et accentue l'intérêt que l'on lui porte depuis lors. Il exhibe en effet une famille de paramètres permettant d'atteindre cette borne.

Theorème 1.7 (Möller, [39])**.**
Soient $3 < p < q < r$ *trois nombres premiers tels que* $q \equiv 2 \bmod p$ *et* $r = (mpq-1)/2$ *avec* m *entier. Alors*

$$a_{(p-1)(qr+1)/2}(pqr) = \frac{p+1}{2}.$$

Deux bornes plus faibles ont été, quant à elles, établies dans deux articles indépendants par Beiter [8] et Bloom [10], parus dans le même numéro de *The American Mathematical Monthly*.

Theorème 1.8 (Beiter, [8])**.**
Soient $3 < p < q < r$ *trois nombres premiers tels que* q *ou* r *soit congru à* $1 \bmod p$. *Alors pour tout* $0 \leqslant k \leqslant \varphi(pqr)$,

$$|a_k(pqr)| \leqslant \frac{p+1}{2}.$$

Les techniques mises en œuvre pour démontrer ces résultats sont similaires à la démonstration du théorème 1.3. Pour commencer, Bang écrit Φ_{pqr} en faisant apparaître une série,

$$\Phi_{pqr}(X) = (1 + X + \ldots X^{p-1})(1 - X^q)(1 - X^r) \sum_{\alpha,\beta,\gamma} X^\eta, \tag{1.9}$$

où la sommation s'effectue sur les $\alpha, \beta, \gamma \in \mathbb{N}$ tels que $\eta = \alpha pq + \beta pr + \gamma qr$. Un examen des différentes contributions aux coefficients du polynôme montre que l'on n'excédera pas $p-1$.

Puis Marion Beiter pousse l'équation (1.9) jusqu'à obtenir dès 1960 dans [6]

$$\Phi_{pqr}(X) = \sum_{k=0}^{\varphi(pqr)} (-1)^{\delta_1+\delta_2} X^k, \tag{1.10}$$

où $k = a + \alpha pq + \beta pr + \gamma qr + \delta_1 q + \delta_2 r$ avec $0 \leqslant a < p$, $0 \leqslant \alpha < r$, $0 \leqslant \beta < q$, $0 \leqslant \gamma < p-1$ et $\delta_1, \delta_2 \in \{0, 1\}$. Plus précisément cela signifie que pour tout k, on cherche des partitions de la forme ci-dessus. Pour chacune d'entre elles, on ajoute $(-1)^{\delta_1+\delta_2}$ au coefficient de X^k.

Sans entrer dans les détails, la fin de la démonstration, disponible dans [9], requiert l'étude des différentes formes de la décomposition de n en fonction des valeurs δ_1 et δ_2. Essentiellement, la valeur du coefficient est maximale (*i.e.* égale à $p-1$) lorsque n admet $p-1$ partitions de la forme ci-dessus avec des δ_1 et δ_2 toujours égaux ou toujours distincts. Ceci n'arrive pas dans les cas où q ou r est congru à 1 modulo p, comme annoncé par le théorème.

Des considérations plus fines encore sur les combinaisons linéaires à coefficients positifs de pq, pr et qr ont conduit Gennady Bachman à démontrer en 2003 le résultat technique suivant.

Theorème 1.9 (Bachman, [3])**.**
Soient $3 \leqslant p < q < r$ trois nombres premiers et soient q^* et r^* les inverses respectifs de q et r modulo p, pris entre 0 et p. On pose $a = \min(q^*, r^*, p-q^*, p-r^*)$ et b tel que $abqr \equiv 1 \bmod p$. Alors pour tout $0 \leqslant k \leqslant \varphi(pqr)$, on a

$$a_k(pqr) \leqslant \min\left(\frac{p-1}{2} + a, p-b\right) \quad \text{et} \quad -a_k(pqr) \leqslant \min\left(\frac{p-1}{2} + a, b\right).$$

Si ce théorème n'est certes pas très lisible, Bachman en tire quelques corollaires plus explicites. Le premier étend le théorème 1.8 de Beiter à des cas de congruences supplémentaires. Quant au second, il donne une borne simple pour les coefficients dans le pire cas des majorations ci-dessus.

Corollaire 1.3 (Bachman, [3])**.**
Si q ou r est congru à ± 1 ou ± 2 modulo p, alors pour tout $0 \leqslant k \leqslant \varphi(pqr)$, on a

$$|a_k(pqr)| \leqslant \frac{p+1}{2}.$$

Corollaire 1.4 (Bachman, [3])**.**
Pour tout $0 \leqslant k \leqslant \varphi(pqr)$, on a

$$|a_k(pqr)| \leqslant p - \left\lceil \frac{p}{4} \right\rceil.$$

Cette dernière inégalité améliore légèrement la borne de $p - \lfloor p/4 \rfloor$ obtenue par Beiter dans [9] en 1971.

Il est à noter que Bloom a même proposé en 1968 une borne supérieure pour l'amplitude des coefficients d'un polynôme cyclotomique quaternaire, dont la démonstration est proche de celle de Bang pour les polynômes ternaires.

Theorème 1.10 (Bloom, [10]).
Soient $p < q < r < s$ quatre nombres premiers impairs. Alors pour tout $0 \leqslant k \leqslant \varphi(pqrs)$, on a

$$|a_k(pqrs)| \leqslant p(p-1)(pq-1).$$

1.3.3 Bornes inférieures et propriétés asymptotiques

Les premières traces de recherche dans cette direction semblent remonter à Schur en 1931 qui démontre le théorème suivant.

Theorème 1.11 (Schur).
Il existe des polynômes cyclotomiques avec des coefficients arbitrairement grands (en valeur absolue).

La démonstration de ce résultat n'a pas été publiée mais a été essentiellement retrouvée dans une lettre de Schur adressée à Landau. Emma Lehmer l'a retranscrite pour nous dans [32].

On examine Φ_n avec n choisi comme produit de t nombres premiers impairs $p_1 < p_2 < \ldots < p_t$ avec t impair. Ainsi $n = p_1 p_2 \ldots p_t$ et l'on suppose de plus que $p_1 + p_2 > p_t$. De telles familles de nombres premiers existent pour tout t (voir la remarque ci-dessous). On va montrer que dans ce cas le coefficient de X^{p_t} dans Φ_n vaut $1 - t$. Pour cela on va travailler modulo X^{p_t+1}. Comme on a choisi t impair, modulo X^{p_t+1}, on a

$$\begin{aligned}
\Phi_n(X) &\equiv \prod_{i=1}^{t}(1 - X^{p_i})/(1 - X), \\
&\equiv (1 + X + \ldots + X^{p_t-1})(1 - X^{p_1})(1 - X^{p_2}) \ldots (1 - X^{p_{t-1}}), \\
&\equiv (1 + X + \ldots + X^{p_t-1})(1 - X^{p_1} - X^{p_2} - \ldots - X^{p_{t-1}}), \qquad (1.11)
\end{aligned}$$

car on a supposé $p_1 + p_2 > p_t$ et donc *a fortiori* la somme de deux ou plus de ces t nombres premiers excède toujours le dernier d'entre eux. si l'on développe cette expression, on constate alors que le coefficient de X^{p_t} vaut $-(t-1)$.

Remarque. Ce résultat ainsi que le suivant utilisent l'existence pour tout $t > 2$ de familles de nombres premiers $p_1 < p_2 < \ldots < p_t$ tels que $p_1 + p_2 > p_t$. En effet si ce n'était pas le cas, alors pour un certain t, toute famille de t nombres premiers ordonnés comme ci-dessus vérifierait $p_1 + p_2 \leqslant p_t$, et donc $2p_1 < p_t$. En particulier entre deux bornes, l'une étant double de l'autre, il y aurait moins de t nombres premiers. Notamment dans chaque intervalle $[2^{k-1}, 2^k]$ on aurait au plus $t - 1$ nombres premiers. Donc au total le nombre de nombres premiers inférieurs à 2^k serait $\pi(2^k) < kt$, ce qui contredrait le théorème des nombres premiers. En effet $\pi(x) > x/\log x$ pour tout $x > 17$.

Si les coefficients d'un polynôme cyclotomique peuvent avoir une amplitude arbitraire, Jiro Suzuki a également montré en 1987 que tous les entiers naturels apparaissent comme coefficients de polynômes cyclotomiques.

Theorème 1.12 (Suzuki, [47])**.**
On a

$$\{a_k(n) | k \in \mathbb{N}, n \in \mathbb{N}^*\} = \mathbb{Z}.$$

La démonstration passe par le résultat précédent. L'équation (1.11), nous montre que $a_{p_t}(n) = -t + 1$ quand on choisit n comme ci-dessus, produit de t nombres premiers distincts avec t impair. Pour obtenir les coefficients impairs, on peut démontrer de manière similaire que $a_{p_t-2}(n) = -t+2$. Il reste à atteindre les entiers positifs. On considère pour cela Φ_{2n}. On a vu (proposition 1.1) que $\Phi_{2n}(X) = \Phi_n(-X)$. Ainsi, $a_{p_t}(2n) = t - 1$ et $a_{p_t-2}(2n) = t - 2$, ce qui donne des coefficients égaux à tous les entiers positifs.

On obtient ainsi des coefficients arbitrairement grands en valeur absolue, quitte à considérer Φ_n avec n composé d'un grand nombre de nombres premiers. La question qui s'est naturellement posée à la suite de ce théorème dû à Schur a été de savoir s'il était nécessaire de choisir de tels n composés. En effet, si l'apparition du premier coefficient différent de 0 ou ± 1 lui donne raison ($a_7(3.5.7) = -2$), on observe un autre phénomène pour le premier 3. La technique de la démonstration précédente indique que -3 apparaîtra comme 23^{e} coefficient du polynôme $\Phi_{11.13.17.19.23} = \Phi_{1062347}$. Cependant on en trouve plus tôt dans la liste des polynômes cyclotomiques. Notamment pour $5 \times 7 \times 11 = 385$, on observe que $a_{119}(5.7.11) = -3$. Plus précisément, Bunger démontre le théorème suivant en 1934 lors d'un exposé à Göttingen. Il fait apparaître des coefficients de taille $(p + 1)/2$ dans Φ_{pqr} en supposant entre autres que deux nombres premiers parmi p, q et r sont jumeaux, c'est-à-dire distants de 2.

Theorème 1.13 (Bunger)**.**
S'il existe une infinité de nombres premiers jumeaux, on peut trouver des coefficients arbitrairement grands dans des polynômes cyclotomiques de la forme Φ_n où n parcourt les produits de trois nombres premiers distincts.

En 1936, Emma Lehmer parvient à adapter cette démonstration pour remplacer l'hypothèse sur les nombres premiers jumeaux (qui résiste encore aujourd'hui) par l'utilisation du théorème de progression arithmétique de Dirichlet.

Theorème 1.14 (E. Lehmer, [32])**.**
On peut trouver des coefficients arbitrairement grands dans les polynômes cyclotomiques Φ_n où n parcourt les produits de trois nombres premiers.

La démonstration (technique) consiste à exhiber un coefficient égal à $(p - 1)/2$ dans le polynôme Φ_{pqr} avec $q = \ell p + 2$ et $r = (mpq - 1)/2$ (pour $\ell, m \in \mathbb{N}$). De tels nombres premiers existent grâce au théorème de progression arithmétique de

Dirichlet. Alors on peut montrer que $a_k(pqr) = (p-1)/2$ avec $k = (p-3)(qr+1)/2$. Le premier 3 qui apparaît avec cette formule est $a_{11088}(7.23.241) = 3$. C'est un peu plus compliqué que le $a_{119}(5.7.11) = -3$ car $7 \times 23 \times 241 = 38801$, mais cela reste plus accessible que le classique $a_{23}(11.13.17.19.23) = -3$.

On qualifie souvent d'impossible
ce qu'on a pas tenté

Lord Chesterfield

CHAPITRE 2

INVERSES MODULAIRES DE POLYNÔMES CYCLOTOMIQUES

Il apparaît dans le chapitre 1 que la question de la taille des coefficients d'un polynôme cyclotomique a donné lieu à de nombreux travaux déjà. Plus récemment Moree [25] a étendu cette étude aux polynômes cyclotomiques inverses, c'est-à-dire de la forme $(X^n-1)/\Phi_n(X)$. Leurs coefficients s'avèrent petits également, et cela peut s'étendre aux développements de Taylor de $1/\Phi_n(X)$ par exemple.

Ici il est question d'une famille encore différente de polynômes, à savoir des inverses modulaires de polynômes cyclotomiques. Si m et n sont distincts, Φ_m et Φ_n sont premiers entre eux ; il est alors légitime de s'interroger sur l'allure de $\Phi_m^{-1} \bmod \Phi_n$. Dans cette partie on étudie exhaustivement les cas où m et n sont des diviseurs d'un produit de deux nombres premiers distincts. L'application et l'utilisation de ces résultats sont développées au chapitre 5. On y voit naturellement apparaître ces polynômes lorsque l'on construit un morphisme entre le groupe multiplicatif $\mathbb{F}_{q^n}^\times$ et le produit de certains de ses sous-groupes. Ces structures sont utiles dans les cryptosystèmes à base de tores qui seront décrits au chapitre 3.

Pour m et n distincts, donc tels que Φ_m et Φ_n soient premiers entre eux, on s'intéresse aux valeurs ou du moins à la taille des coefficients de Φ_m^{-1} modulo Φ_n. Les polynômes Φ_m et Φ_n étant premiers entre eux, on écrit une relation de Bézout les liant,

$$\Phi_m U + \Phi_n V = 1,$$

et l'on cherche à étudier $U = \Phi_m^{-1} \bmod \Phi_n$.

Le résultat dont on va démontrer tour à tour les assertions est le suivant.

Theorème 2.1.
Pour tous nombres premiers distincts p et r,

(i) $\Phi_p^{-1} \bmod \Phi_1 = 1/p$ *et* $\Phi_1^{-1} \bmod \Phi_p = (-1/p)(X^{p-2} + 2X^{p-3} + \ldots + p - 1)$.

(ii) $\Phi_{pr}^{-1} \bmod \Phi_1 = 1$ *et* $\Phi_1^{-1} \bmod \Phi_{pr} = \sum_{i=0}^{\varphi(pr)-1} v_i X^i$ *avec* $v_i \in \{-1, 0, +1\}$.

(iii) $\Phi_{pr}^{-1} \bmod \Phi_p = \frac{1}{r} \sum_{i=0}^{d-1} X^i$ *avec* $d = r \bmod p$ *et*
$\Phi_p^{-1} \bmod \Phi_{pr} = \frac{1}{r} \sum_{i=0}^{\varphi(pr)-1} v_i X^i$ *avec* $|v_i| < r$.

(iv) $\Phi_p^{-1} \bmod \Phi_r = \sum_{i=0}^{\varphi(r)-1} v_i X^i$ *avec* $v_i \in \{-1, 0, +1\}$.

2.1 Cas $m = p$ et $n = 1$ et cas inverse

Les polynômes cyclotomiques Φ_p et Φ_1 sont les plus simples. Les expressions de leurs inverses sont faciles à écrire explicitement.

Proposition 2.1.
Pour tout nombre premier p,

(i) $\Phi_p^{-1} \bmod \Phi_1 = 1/p$,

(ii) $\Phi_1^{-1} \bmod \Phi_p = -(1/p)(X^{p-2} + 2X^{p-3} + \ldots + p - 1)$.

Démonstration.
Il suffit de vérifier la relation de Bézout correspondante entre Φ_p et Φ_1,

$$\begin{aligned} -\Phi_1(X)(X^{p-2} + 2X^{p-3} + \ldots + p - 1) + \Phi_p(X) & \\ = (X-1)\sum_{k=0}^{p-2}(k+1-p)X^k + \Phi_p(X), & \\ = \sum_{k=1}^{p-1}(k-p)X^k - \sum_{k=0}^{p-2}(k+1-p)X^k + \sum_{k=0}^{p-1} X^k = p. & \end{aligned}$$

□

2.2 Cas $m = pr$ et $n = 1$ et cas inverse

L'expression explicite de Φ_{pr} est moins pratique que celle de Φ_p, mais on l'a cependant grâce au résultat de Lam et Leung [31], rappelé par le théorème 1.6.

Proposition 2.2.
Pour tous nombres premiers distincts p et r,

(i) $\Phi_{pr}^{-1} \bmod \Phi_1 = 1$.

(ii) $\Phi_1^{-1} \bmod \Phi_{pr} = \sum_{i=0}^{(p-1)(r-1)-1} v_i X^i$ *avec* $v_i \in \{-1, 0, +1\}$.

Démonstration.

Tout d'abord on cherche U dans la relation de Bézout

$$\Phi_{pr} U + \Phi_1 V = 1,$$

dont on sait qu'il est de degré 0. Il suffit alors d'évaluer cette relation en 1 et l'on obtient $U(1) = 1$ car $\Phi_{pr}(1) = 1$. Donc ${\Phi_{pr}}^{-1} \bmod \Phi_1 = 1$.

On s'intéresse maintenant à V qui est caractérisé par

$$(X-1)V(X) = 1 - \Phi_{pr}(X). \tag{2.1}$$

Posons $V(X) = \sum_{i=0}^{d-1} v_i X^i$ et $\Phi_{pr}(X) = \sum_{i=0}^{d} a_i X^i$ avec $d = (p-1)(r-1)$. Alors on peut écrire l'équation (2.1) comme un système linéaire,

$$\begin{bmatrix} -1 & 0 & \dots & 0 \\ 1 & -1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 1 & -1 \end{bmatrix} \begin{bmatrix} v_0 \\ v_1 \\ \vdots \\ v_{d-1} \end{bmatrix} = \begin{bmatrix} 1 - a_0 \\ -a_1 \\ \vdots \\ -a_{d-1} \end{bmatrix} \Leftrightarrow \begin{bmatrix} v_0 \\ v_1 \\ \vdots \\ v_{d-1} \end{bmatrix} = \begin{bmatrix} 1 & 0 & \ddots & 0 \\ 1 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 1 & \dots & 1 & 1 \end{bmatrix} \begin{bmatrix} a_0 - 1 \\ a_1 \\ \vdots \\ a_{d-1} \end{bmatrix}.$$

D'après le théorème 1.6, $a_0 = 1$ et pour tout i, $a_i \in \{-1, 0, +1\}$. De plus les signes ($+1$ ou -1) des coefficients alternent. Donc chaque v_i vaut nécessairement 0 ou ± 1. □

Remarque. Comme on l'a fait pour Φ_{pr}, on peut aussi trouver Φ_n^{-1} modulo Φ_1 pour tout $n \neq 1$ puisqu'il s'agit simplement de $1/\Phi_n(1)$ que l'on connaît explicitement.

2.3 Cas $m = pr$ et $n = p$

Cette fois l'expression explicite de Φ_{pr} sera nécessaire.

Proposition 2.3.
Pour tous nombres premiers distincts p et r,

$$\Phi_{pr}^{-1} \bmod \Phi_p = \frac{1}{r} \sum_{i=0}^{d-1} X^i \text{ avec } d = r \bmod p.$$

Démonstration.

On va montrer directement que $\left(\sum_{i=0}^{d-1} X^i\right) \Phi_{pr} \equiv r \bmod \Phi_p$. Pour cela, on rappelle l'expression de Φ_{pr} établie lors de la démonstration du théorème 1.6. Soient s et t deux entiers positifs tels que $(p-1)(r-1) = \varphi(pr) = sp + tr$. Alors

$$\Phi_{pr}(X) = \left(\sum_{i=0}^{s} X^{ip}\right)\left(\sum_{j=0}^{t} X^{jr}\right) - \left(\sum_{i=s+1}^{r-1} X^{ip}\right)\left(\sum_{j=t+1}^{p-1} X^{jr}\right) X^{-pr}.$$

Comme $X^p \equiv 1 \bmod \Phi_p(X)$ on a,

$$\begin{aligned}\Phi_{pr}(X) \sum_{i=0}^{d-1} X^i \bmod \Phi_p(X) &= \left((s+1)\sum_{j=0}^{t} X^{jr} - (r-1-s)\sum_{j=t+1}^{p-1} X^{jr}\right)\sum_{i=0}^{d-1} X^i, \\ &= \left((s+1)\sum_{j=0}^{p-1} X^{jr} - r\sum_{j=t+1}^{p-1} X^{jr}\right)\sum_{i=0}^{d-1} X^i.\end{aligned}$$

Mais on a $\sum_{j=0}^{p-1} X^{jr} = \Phi_p(X^r)$, et $\Phi_p(X^r) \equiv 0 \bmod \Phi_p(X)$, donc

$$\Phi_{pr}(X) \sum_{i=0}^{d-1} X^i \bmod \Phi_p(X) = -r \sum_{j=t+1}^{p-1} X^{jr} \sum_{i=0}^{d-1} X^i = r\frac{X^{(t+1)r}-1}{X^r-1}\,\frac{X^d-1}{X-1}.$$

On peut enfin vérifier que $(t+1)r = 1+pr-p(s+1)$. Donc $X^{(t+1)r} \equiv X \bmod \Phi_p(X)$. Comme $d \equiv r \bmod p$, alors $X^d \equiv X^r \bmod \Phi_p(X)$ et l'on obtient le résultat : le produit calculé se résume à r.

□

2.4 Cas $m = p$ et $n = pr$

Proposition 2.4.

Pour tous nombres premiers distincts p et r,

$$\Phi_p^{-1} \bmod \Phi_{pr} = \frac{1}{r}\sum_i v_i X^i \text{ avec } |v_i| < r.$$

Démonstration.

On cherche V dans la relation de Bézout $\Phi_{pr}U + \Phi_p V = 1$ et pour cela on calcule $rV(X)$. On a

$$rV(X) = \frac{r - rU(X)\Phi_{pr}}{\Phi_p(X)} = (-rU(X)\Phi_{pr}(X)) \div \Phi_p(X).$$

Ici l'opérateur $\div$ renvoie le quotient dans la division euclidienne du terme de gauche par le terme de droite et en effet le terme constant r ne modifie que le reste de cette division.

D'après la proposition 1.1, on a $\Phi_{pr}(X) = \Phi_r(X^p)/\Phi_r(X)$ et l'on va écrire $\Phi_r(X^p)$ différemment d'après l'égalité suivante :

$$(X^p-1)\sum_{j=0}^{r-2}(r-1-j)X^{pj} = \sum_{j=0}^{r-2}(r-1-j)X^{p(j+1)} - \sum_{j=0}^{r-2}(r-1-j)X^{pj} = \Phi_r(X^p) - r.$$

D'après la proposition 2.3 précédente, on sait que $rU(X) = \sum_{i=0}^{d-1} X^i = (X^d - 1)/(X-1)$ avec d le représentant dans $[0, p[$ de r modulo p. Comme de plus $X^r - 1 = (X-1)\Phi_r(X)$, on a finalement

$$rV(X) = \left(-(X-1)(X^d-1)\sum_{j=0}^{r-2}(r-1-j)X^{pj}\right) \div (X^r-1).$$

Dans le cas où $r < p$, on a $d = r$ et donc après simplification des termes (X^r-1), le quotient de cette division est directement $rV(X) = -(X-1)\sum_{j=0}^{r-2}(r-1-j)X^{pj}$. Les termes non nuls de la somme étant espacés de p, il n'y a aucune collision lorsque l'on distribue le facteur $(X-1)$. Donc les coefficients de rV sont tous inférieurs à r en valeur absolue.

Examinons maintenant le cas $r > p$. On va commencer par effectuer la division euclidienne de $\sum_{j=0}^{r-2}(r-1-j)X^{pj}$ par X^r-1. Notons Q son quotient et R son reste. Pour tout $0 \leqslant j < r-2$, on vérifie que

$$X^{pj} = X^{pj \bmod r} + (X^r-1)\sum_{\substack{0\leqslant k<pj \\ k=pj \bmod r}} X^k,$$

en voyant par exemple la somme du membre de droite comme une somme géométrique. D'où

$$Q(X) = \sum_{j=0}^{r-2}(r-1-j)\sum_{\substack{0\leqslant k<pj \\ k=pj \bmod r}} X^k \text{ et } R(X) = \sum_{j=0}^{r-1}((-1-j/p) \bmod r)X^j. \quad (2.2)$$

Il est à noter que pour l'expression du reste, on s'est autorisé l'ajout d'un terme nul, à savoir celui qui correspond à $j = r-1$ avant le changement d'indice. On a finalement

$$rV(X) = -(X-1)(X^d-1)Q(X) - ((X-1)(X^d-1)R(X)) \div (X^r-1).$$

Or comme $(X-1)(X^d-1)R(X)$ est de degré strictement inférieur à $2r$, son quotient par (X^r-1) est de degré strictement inférieur à r, donc égal au quotient par X^r. Il proviendra alors simplement des termes de plus hauts degrés de $(X-1)(X^d-1)R(X)$. Plus précisément, si l'on note Q' ce quotient, il proviendra des

termes de degré au moins égal à r dans $(X^{d+1} - X^d + X)R(X)$. Si l'on appelle a le représentant de $1/p$ modulo r, alors on a immédiatement les premier et dernier termes de Q' :

$$Q'(X) = (a-1)X^d + \ldots - (r-1).$$

En effet le coefficient dominant de R est $R_{r-1} = a-1$. Le coefficient constant de Q', quant à lui, est une combinaison de coefficients de R, à savoir

$$R_{r-d-1} - R_{r-d} - R_{r-1} = (da + a - 1) \bmod r - (da - 1) \bmod r - (a-1).$$

Il faut maintenant déterminer la valeur de $(da + a - 1) \bmod r$ pour savoir comment elle se simplifie avec $(da - 1) \bmod r$. Si l'on note $d = r - ep$ avec $e = \lfloor r/p \rfloor$, alors $(da-1) \bmod r = -(e+1) \bmod r = r - e - 1$. Il reste à comparer cette quantité avec $a \bmod r$. On sait que $p(a \bmod r) = 1 + kr$ avec $k \geqslant 1$ entier.

– Si $k = 1$, alors $a \bmod r = (r+1)/p = e + 1$ par définition de la partie entière.

– Par ailleurs si $k \geqslant 2$, alors $p(a \bmod r) \geqslant r+p$ *a fortiori*, et donc $a \bmod r \geqslant e+1$.

Dans tous les cas $(da - 1) \bmod r + a \bmod r \geqslant r$ et donc

$$R_{r-d-1} - R_{r-d} - R_{r-1} = 1 - a + a \bmod r - r = 1 - r.$$

En outre, pour $1 \leqslant k < d$, le coefficient du monôme X^k est exactement

$$((-1 - (r - d - 1 + k)/p) \bmod r) - (-1 - (r - d + k)/p) \bmod r) \in \{a, a - r\}.$$

Par un raisonnement similaire, on trouve que les $d + 1$ coefficients de plus bas degrés de $(X - 1)(X^d - 1)Q(X)$ (mis à part le premier qui est nul) sont égaux à la différence de deux coefficients consécutifs de $Q(X)$, soit $-a$ ou $r - a$. Plus précisément, on obtient

$$((X-1)(X^d-1)Q(X) \bmod X^{d+1}) + \\ ((X-1)(X^d-1)R(X)) \div (X^r - 1) = -X^d + (r-1)X - (r-1).$$

Il reste à borner les coefficients des monômes de $(X^d - 1)(X - 1)Q(X)$ de degrés supérieurs à d.

On remarque déjà que chacun des coefficients de $(X - 1)Q(X)$ s'obtient par la différence de deux coefficients de monômes consécutifs de Q, et est donc un entier compris dans l'intervalle d'extrémités $[a - r, a]$.

De même, tout coefficient de $(X^d - 1)(X - 1)Q(X)$ est égal à la différence de coefficients de monômes de $(X - 1)Q(X)$ distants de d. Il est donc borné en valeur absolue par r. On va maintenant vérifier que deux coefficients distants de d dans

$(X-1)Q(X)$ ne sont jamais exactement égaux à $a-r$ et a respectivement. Ainsi les valeurs r et $-r$ ne peuvent pas être atteintes.

Dans la suite de ce calcul et pour alléger les notations on notera entre crochets les quantités prises modulo r. Une réindexation dans l'écriture (2.2) nous donne

$$Q(X) = \sum_{\substack{k=0 \\ [ka]p \geqslant k+1}}^{p(r-2)} (r-1-[ka])X^k = \sum_{\substack{k=0 \\ [ka]p \geqslant k+1}}^{p(r-2)} q_k X^k.$$

Dans ce qui suit, la notation δ désigne, à l'instar du symbole de Kronecker, l'évaluation booléenne de la condition en indice et prend donc pour valeur $+1$ si cette dernière est vraie et 0 sinon. Alors le coefficient de X^k dans $(X-1)Q(X)$ est

$$\Delta_k = q_{k-1} - q_k = (r-1-[(k-1)a])\delta_{[(k-1)a]p \geqslant k} - (r-1-[ka])\delta_{[ka]p \geqslant k+1}.$$

Or $[(k-1)a] = [ka] - a$ si $[ak] \geqslant a$, et $[ka] - a + r$ sinon.

1er cas : $0 \leqslant [ak] < a$.

$\Delta_k = (-1-[ka]+a)\delta_{(r-a)p+[ka]p \geqslant k} - (r-1-[ka])\delta_{[ka]p-1 \geqslant k}$.

- si $k > [ka]p + (r-a)p$ alors $\Delta_k = 0$,
- si $[ka]p + (r-a)p \geqslant k > [ka]p - 1$, alors $0 \leqslant \Delta_k = a - 1 - [ka] < a$,
- si $[ka]p - 1 \geqslant k$, alors $\Delta_k = (-1-[ka]+a) - (r-1-[ka]) = a - r$.

2e cas : $a \leqslant [ak] < r$.

$\Delta_k = (r-1-[ka]+a)\delta_{[ka]p \geqslant k+ap} - (r-1-[ka])\delta_{[ka]p \geqslant k+1}$.

- si $[ka]p < k+1$ alors $\Delta_k = 0$,
- si $k+1 \leqslant [ka]p < k+ap$, alors $0 \geqslant \Delta_k = -r+1+[ka] > -r+a$,
- si $k+ap \leqslant [ka]p$, alors $\Delta_k = (r-1-[ka]+a) - (r-1-[ka]) = a$.

Maintenant le coefficient de X^k dans $(X^d-1)(X-1)Q(X)$ est la différence $\Delta_{k-d} - \Delta_k$. D'après les encadrements ci-dessus, elle est toujours strictement inférieure à r en valeur absolue, sauf si l'un des termes vaut $a-r$ et l'autre a.

1er cas : $\Delta_k = a - r$ et $\Delta_{k-d} = a$.

Alors $0 \leqslant [ak] < a$ et $[ka]p - 1 \geqslant k$ et $a \leqslant [a(k-d)] < r$ et $k - d + ap \leqslant [(k-d)a]p$.

- si $[ak] > [ad]$, alors $[a(k-d)] = [ak] - [ad]$, d'où $a > [ak] \geqslant a + [ad]$, ce qui est impossible.
- si $[ak] < [ad]$, alors $[a(k-d)] = [ak] - [ad] + r$ et donc $[ak] - [ad] + r \geqslant a$. On pose $\eta = [ad]$. Finalement, on a

$$a + \eta - r \leqslant [ak] < a.$$

On remarque que si $k' = k + p$ alors $[ak'] = [ak] + 1$. Cela revient donc à $k \in \{k_1, k_1 + p, \ldots, k_2\}$ avec les bornes telles que $[ak_1] = a - (r - \eta)$ et $[ak_2] = a - 1$. Or $[a(d+1)] = [a + \eta] = [a + \eta - r]$. Donc $[k_1] = d + 1$ et donc $k_2 = d + 1 + (r - \eta - 1)p$. Finalement les k possibles sont $k = d + 1 + xp$ avec $x \in \{0, 1, \ldots, r - \eta - 1\}$, $0 \leqslant d + 1 < r$ étant bien le premier.

L'inégalité $k-d+ap \leqslant [(k-d)a]p$ s'écrit alors $1+(a+x)p \leqslant [a+x]p$. D'une part ceci n'est possible que si $(a+x)$ dépasse r. Mais d'autre part, cela implique aussi $1+(a+x)p < rp$ et donc $a+x < r$, d'où une contradiction.

2e cas : $\Delta_k = a$ et $\Delta_{k-d} = a-r$.

Alors $0 \leqslant [a(k-d)] < a$ et $[(k-d)a]p-1 \geqslant k-d$ et $a \leqslant [ak] < r$ et $k+ap \leqslant [ka]p$.

- si $[ak] < [ad]$, alors $[ak]-[ad]+r < a \leqslant [ak]$, ce qui est impossible.
- si $[ak] > [ad]$, alors $[a(k-d)] = [ak]-[ad]$. Comme ci-dessus, les différentes inégalités nous fournissent un encadrement de $[ak]$:

$$a \leqslant [ak] < a+\eta.$$

Cela correspond à η valeurs de k en progression arithmétique de raison p et dont la première est $k_1 = 1$, telle que $[ak_1] = a$. On peut donc écrire $k = 1+xp$ avec $x \in \{0, \ldots, \eta-1\}$. Alors l'inégalité $k+ap \leqslant [ka]p$ devient $1+(x+a)p \leqslant [a+x]p$, ce qui fournit exactement la même contradiction que dans le cas précédent.

En conclusion, on a montré qu'aucun coefficient de $(X^d-1)(X-1)Q(X)$ n'est exactement égal à r en valeur absolue, ce qui garantit l'inégalité stricte recherchée. □

2.5 Cas $m = p$ et $n = r$

Il s'agit de la dernière assertion du théorème 2.1. Nous allons évaluer la relation de Bézout $\Phi_p U + \Phi_r V = 1$ en les racines de Φ_r et utiliser ces évaluations comme points d'interpolation pour U. Avant cela nous allons légèrement modifier l'équation pour des raisons de commodité du système linéaire. Si l'on multiplie les deux membres de cette égalité par $X-1$, on obtient

$$\Phi_p \widetilde{U} + (X^r-1)V = X-1,$$

où l'on note $\widetilde{U} = (X-1)U$.

L'évaluation de notre relation de Bézout en les racines r^{es} de l'unité ξ^j donne

$$\forall 0 \leqslant j \leqslant r-1, \quad \Phi_p(\xi^j)\widetilde{U}(\xi^j) = \xi^j - 1.$$

En notant $\widetilde{U} = \sum_{i=1}^{r} \widetilde{u}_i X^{i-1}$, cette équation peut s'écrire

$$\forall 0 \leqslant j \leqslant r-1, \quad \sum_{i=1}^{r} \widetilde{u}_i (\xi^j)^{i-1} = (\xi^j - 1)(\Phi_p(\xi^j))^{-1}.$$

En premier lieu, nous allons estimer les coefficients de $\widetilde{U}$.

Lemme 2.1.
Pour tout $1 \leqslant i \leqslant r$,

$$\widetilde{u}_i \in \{-1, 0, +1\}.$$

Démonstration.

Les coefficients $(\widetilde{u}_i)_{1\leqslant i\leqslant r}$ sont solutions d'un système d'équations linéaires dont la version matricielle s'écrit $A\widetilde{U} = W$, avec $W = \left[(\xi^j - 1)\Phi_p(\xi^j)^{-1}\right]_{0\leqslant j\leqslant r-1}$ et

$$A = \begin{bmatrix} 1 & 1 & \dots & 1 \\ 1 & \xi & \dots & \xi^{r-1} \\ \vdots & \vdots & \vdots & \vdots \\ 1 & \xi^{r-1} & \dots & (\xi^{r-1})^{r-1} \end{bmatrix} = \mathrm{VdM}(1, \xi, \dots, \xi^{r-1}).$$

Ici VdM() désigne la matrice de Vandermonde dont les paramètres sont indiqués entre parenthèses. Comme tous les $\{\xi^j\}_{j\in\{0,\dots,r-1\}}$ sont distincts, A est inversible. On peut ainsi résoudre explicitement en $\widetilde{U}$ ce système linéaire : $\widetilde{U} = A^{-1}W$. On trouve par exemple dans [26] que l'inverse d'une matrice de Vandermonde fait intervenir une nouvelle matrice de Vandermonde dont les paramètres sont inverses des premiers. En d'autres termes, ici $A^{-1} = (1/r)\mathrm{VdM}(1, \xi^{-1}, \dots, \xi^{-r+1})$.

Les solutions du système linéaire sont donc données par

$$\forall 1 \leqslant i \leqslant r, \quad \widetilde{u}_i = \frac{1}{r}\sum_{j=0}^{r-1}(\xi^{-(i-1)})^j(\xi^j - 1)\Phi_p(\xi^j)^{-1}.$$

Maintenant en utilisant $\Phi_p(X) = (1 - X^p)/(1 - X)$, on trouve

$$\forall 1 \leqslant i \leqslant r, \quad \widetilde{u}_i = \frac{1}{r}\sum_{j=0}^{r-1}(\xi^{1-i})^j(\xi^j - 1)\frac{1 - \xi^j}{1 - \xi^{jp}}. \tag{2.3}$$

Cette expression peut être améliorée en utilisant l'identité suivante :

$$\frac{1}{1 - \xi^{jp}} = \frac{1}{r}\left(\xi^{jp(r-2)} + 2\xi^{jp(r-3)} + \ldots + (r-1)\right).$$

En effet,

$$\begin{aligned}
(1 - \xi^{jp})&\sum_{k=0}^{r-2}(r - 1 - k)\xi^{jpk} \\
&= \sum_{k=0}^{r-2}(r - 1 - k)\xi^{jpk} - \sum_{k=0}^{r-2}(r - 1 - k)\xi^{jp(k+1)}, \\
&= \sum_{k=0}^{r-2}(r - 1 - k)\xi^{jpk} - \sum_{k=1}^{r-1}(r - k)\xi^{jpk}, \\
&= (r-1) - \underbrace{\sum_{k=1}^{r-2}(\xi^{jp})^k}_{=-1-\xi^{jp(r-1)} \text{ si } jp\not\equiv 0 \bmod r} - \xi^{jp(r-1)}, \\
&= r \quad \text{car } jp \not\equiv 0 \bmod r \ (p \text{ premier et } 1 \leqslant j \leqslant r-1).
\end{aligned}$$

Après avoir développé et ordonné les termes de l'équation (2.3), on obtient la forme suivante pour $\widetilde{u}_i$.

$$\widetilde{u}_i = -\frac{1}{r^2}\sum_{k=0}^{r-2}(r-k-1)\sum_{j=0}^{r-1}(\xi^{j(pk+1-i)} - 2\xi^{j(pk+2-i)} + \xi^{j(pk+3-i)}),$$

ou en appelant $S_l(k) = \sum_{j=0}^{r-1}\xi^{j(pk+l-i)}$,

$$\widetilde{u}_i = -\frac{1}{r^2}\sum_{k=0}^{r-2}(r-k-1)\underbrace{(S_1(k) - 2S_2(k) + S_3(k))}_{S(k)}.$$

Le calcul des coefficients $\widetilde{u}_i$ passe maintenant par une bonne compréhension des sommes $S_l = \sum_{j=0}^{r-1}(\xi^A)^j$. Elles somment en fait toutes les puissances d'une racine r^{e} de l'unité donnée. Donc si ξ^A est une racine primitive de l'unité, la somme s'annule simplement. Et si ce n'est pas une racine primitive, la seule possibilité est que $\xi^A = 1$ (*i.e.* $A \equiv 0 \bmod r$) et dans ce cas la somme vaut r. Donc $\widetilde{u}_i$ dépend des valeurs modulo r des puissances $pk + l - i$.

La plupart du temps les trois sommes mises en jeu vaudront 0 et alors $S_1 - 2S_2 + S_3$ sera nul. Mais il peut y avoir jusqu'à trois valeurs de k pour lesquelles une de ces sommes ne vaudra pas 0 mais r. Pour $l \in \{1,2,3\}$, s'il existe $0 \leqslant k_l \leqslant r-2$ tel que $pk_l + l - i \equiv 0 \bmod r$, alors $S_l(k_l) = r$.

Maintenant, l'argument clef est le suivant : dans chaque somme S_l, toutes les puissances de ξ apparaissent, sauf celle qui fait intervenir $k = r-1$. Par ailleurs, les puissances $\{pk + l - 1 \bmod r, 0 \leqslant k \leqslant r-1\}$ prennent toutes les valeurs de $\{0, \ldots, r-1\}$ car p et r sont premiers entre eux. Donc de deux choses l'une : soit il existe $0 \leqslant k_l \leqslant r-2$ tel que $pk_l + l - i \equiv 0 \bmod r$, soit nécessairement $p(r-1) + l - i \equiv 0 \bmod r$.

Démontrons tout d'abord qu'il existe au moins deux k_l sur les trois k_1, k_2 et k_3. Si l'un d'entre eux n'existe pas, alors $p(r-1) + l - i \equiv 0 \bmod r$. Donc si deux différents n'existent pas, disons k_l et $k_{l'}$, on aura cette même relation pour les deux indices l et l' de $\{1,2,3\}$. Et alors $l \equiv l' \bmod r$, ce qui est impossible si $l \neq l'$. Ceci montre qu'au moins deux des trois k_l existent et donne conséquemment quatre différents cas.

– S'il existe $k_1, k_2, k_3 \in \{0, \ldots, r-2\}$, alors on a le système de trois équations suivant.

$$\begin{cases} pk_1 + 1 - i & \equiv & 0 \bmod r & (a) \\ pk_2 + 2 - i & \equiv & 0 \bmod r & (b) \\ pk_3 + 3 - i & \equiv & 0 \bmod r & (c) \end{cases}.$$

Donc $p(k_1 + k_3 - 2k_2) \equiv 0 \bmod r$. Comme p et r sont premiers entre eux, $r | (k_1 + k_3 - 2k_2)$. Et comme $|k_l|$ n'excède pas $r-1$, $k_1 + k_3 - 2k_2 = 0$ ou $\pm r$. Donc $-r^2\widetilde{u}_i = (r - k_1 - 1)r + (r - k_2 - 1)(-2r) + (r - k_3 - 1)r = 0$ ou $\pm r^2$, si bien que $\widetilde{u}_i = 0$ ou ± 1.

– Si c'est k_1 qui n'existe pas, alors l'équation (a) devient

$$p(r-1) + i - 1 \equiv 0 \bmod r.$$

Donc $p \equiv 1 - i \bmod r$. Puis en injectant ce p dans les équations (b) et (c), on a $(1-i)(k_2+1) \equiv -1 \bmod r$ et $(1-i)(k_3+1) \equiv -2 \bmod r$. D'où la relation $2k_2 - k_3 + 1 = 0$. Donc $-r^2(1-i)\widetilde{u}_i = (1-i)(r-k_2-1)(-2r) + (1-i)(r-k_3-1)r = -(1-i)r^2$. Mais $1 - i \neq 0$ (car $p \not\equiv 0 \bmod r$), si bien que $\widetilde{u}_i = 1$.

– Si c'est k_2 qui n'existe pas, alors l'équation (b) devient

$$p(r-1) + 2 - i \equiv 0 \bmod r.$$

Donc $p \equiv 2 - i \bmod r$; en particulier $i \neq 2$. Puis avec cette valeur de p, les équations (a) et (c) donnent, comme précédemment, $(2-i)(k_1+1) \equiv 1 \bmod r$ et $(2-i)(k_3+1) \equiv -1 \bmod r$. D'où la relation $k_1 + k_3 + 2 = r$. Donc $-r^2(2-i)\widetilde{u}_i = (2-i)(r-k_1-1)r + (2-i)(r-k_3-1)r = (2-i)r^2$, si bien que $\widetilde{u}_i = -1$.

– Si c'est k_3 qui n'existe pas alors l'équation (c) devient

$$p(r-1) + 3 - i \equiv 0 \bmod r.$$

Donc $p \equiv 3 - i \bmod r$ et $i \neq 3$. Puis avec cette valeur de p, la résolution des équations (a) et (c) donne, comme précédemment, la relation $2k_2 - k_1 + 1 = r$. Donc $-r^2(3-i)\widetilde{u}_i = 0$, si bien que $\widetilde{u}_i = 0$.

□

Proposition 2.5.
Pour tous nombres premiers distincts p et r,

$$\Phi_p^{-1} \bmod \Phi_r = \sum_{i=1}^{r-1} u_i X^{i-1} \text{ avec } u_i \in \{-1, 0, +1\}.$$

Démonstration.

On peut maintenant évaluer les coefficients de U tel que $\widetilde{U} = (X-1)U$. On a déjà effectué un calcul similaire dans la démonstration de la proposition 2.2, ce qui donne

$$\begin{bmatrix} u_1 \\ u_2 \\ \vdots \\ u_{r-1} \end{bmatrix} = \begin{bmatrix} 1 & 0 & \dots & 0 \\ 1 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 1 & \dots & 1 & 1 \end{bmatrix} \begin{bmatrix} \widetilde{u}_1 \\ \widetilde{u}_2 \\ \vdots \\ \widetilde{u}_{r-1} \end{bmatrix}.$$

Comme u_i est une somme de $\widetilde{u}_j$ consécutifs, il suffit de montrer que les +1 et les -1 alternent dans $(\widetilde{u}_j)_{1 \leqslant j \leqslant r}$ (entre autres éventuels zéros).

Avec les notations de la démonstration précédente, pour tout $1 \leqslant i \leqslant r$, on pose $K(i) = (k_1(i), k_2(i), k_3(i))$ où $k_l(i) \in \{0, \dots, r-1\}$ est le coefficient tel que $pk_l(i) + l - i \equiv 0 \bmod r$. Alors $r\widetilde{u}_i = k_1(i) - 2k_2(i) + k_3(i)$.

En outre, $k_3(i) = k_2(i) - 1/p = k_1(i) - 2/p$ et la connaissance de $K(i)$ nous permet aussi de trouver $K(i+1)$. En effet $i+1 \equiv 1 + l + pk_l(i+1) \bmod r$. Ainsi

$$k_2(i+1) = k_1(i), k_3(i+1) = k_2(i) \text{ et } k_1(i+1) \equiv k_3(i) + 3/p \bmod r.$$

Finalement, étant donné $k = k_1(i)$, alors $K(i) = (k, k-1/p, k-2/p)$ et le triplet suivant est $K(i+1) = (k+1/p, k, k-1/p)$, toutes les valeurs étant prises modulo r.

Maintenant on est en mesure de dire si $r\widetilde{u}_i = k_1(i) - 2k_2(i) + k_3(i)$ vaut $-r, 0$ ou $+r$. L'enchaînement des valeurs de $r\widetilde{u}_i$ dépend de celui des valeurs de k_l modulo r. Si l'on calcule successivement les $r\widetilde{u}_i$, les k_l croissent de $1/p$ à chaque étape. Lorsque k_1 ou k_3 en vient à dépasser r, le fait de prendre ces valeurs modulo r entraîne une chute de r pour $r\widetilde{u}_i$. De même si k_2 doit excéder r, le fait de prendre sa valeur modulo r se traduit par une hausse de $2r$ dans $r\widetilde{u}_i$ (car k_2 apparaît avec le coefficient -2). Comme les k_l vont dépasser r successivement (toujours dans l'ordre k_1 puis k_3 puis k_2 puis k_1...), on ajoutera alternativement $-r$, $-r$ et $+2r$ à $r\widetilde{u}_i$ pour obtenir $r\widetilde{u}_{i+1}$. Le nombre de telles opérations à chaque étape dépend de p et i mais n'excédera en aucun cas 2 (les trois k_l ne peuvent pas tous dépasser r en même temps car on leur ajoute $1/p \bmod r$ et ils couvrent un intervalle d'amplitude le double de cette valeur). Donc il suffit de vérifier que leurs premières valeurs sont prises dans $[-r, r]$ pour montrer qu'il en sera de même lors de l'itération du procédé.

Le premier coefficient (pour $i = 1$) correspond à

$$K(1) = (0, -1/p \bmod r, -2/p \bmod r).$$

Deux triplets sont donc possibles.

- si $1/p < r/2$, alors $K(1) = (0, r - 1/p, r - 2/p)$ et donc $r\widetilde{u}_1 = -r$. Comme $k_2(1) > k_1(1)$, on commence par ajouter $2r$. En effet, $k_2(2) \equiv 0 \bmod r$, ce qui correspond à augmenter $r\widetilde{u}_1$ de $2r$, soit $r\widetilde{u}_2 = r$.
- si $1/p > r/2$, alors $K(1) = (0, r - 1/p, 2r - 2/p)$, et donc $r\widetilde{u}_1 = 0$. Comme précédemment, le triplet suivant sera $K(2) = (1/p, 0, r - 1/p)$, ce qui ajoute à la fois $-r$ et $2r$ à $r\widetilde{u}_1$, si bien que $r\widetilde{u}_2 = r$.

Dans les deux cas, l'initialisation du processus est correcte et l'on a finalement montré l'alternance des +1 et des -1 dans $(\widetilde{u}_i)_{1 \leqslant i \leqslant r}$. Ceci suffit pour conclure que les coefficients u_i décrivent $\{-1, 0, +1\}$ pour tout $1 \leqslant i \leqslant r$.

□

Deuxième partie

Tores algébriques et cryptographie

L'essence des mathématiques,
c'est la liberté

Georg Cantor

CHAPITRE 3

LA CRYPTOGRAPHIE, DE DIFFIE-HELLMAN AUX TORES

Que de chemin parcouru depuis l'introduction ! Rappelons-nous cependant ce que nous y avons évoqué : un cryptosystème comme celui de Diffie-Hellman met en jeu une structure de groupe. Un des enjeux de la cryptographie dans ce domaine est de bien choisir les groupes utilisés. On cherche des groupes permettant une arithmétique efficace afin que la mise en œuvre des protocoles ne soit pas trop coûteuse, mais qui rendent aussi assez difficiles les opérations sur la complexité desquelles leur sécurité repose, comme le problème du logarithme discret dans notre cas. L'exemple le plus simple en est le groupe multiplicatif $\mathbb{F}_q^\times$ d'un corps fini ; on peut également penser aux groupes sur des courbes elliptiques, qui sont la source de nombreux travaux. Certaines recherches se penchent depuis maintenant quelques années sur des sous-groupes particuliers du groupe multiplicatif d'un corps fini.

Nous verrons dans la partie 3.2 comment cette idée s'est développée et l'utilisation qui en a été faite. Auparavant le paragraphe 3.1 présente quelques rappels sur le système de Diffie-Hellman et son contexte cryptographique.

3.1 Le protocole de Diffie-Hellman

Ce n'est qu'avec l'avènement des technologies modernes que la cryptographie est devenue une discipline principalement mathématique et informatique. Jusqu'à la seconde guerre mondiale, on recrutait des cryptanalystes également parmi les linguistes voire les bons cruciverbistes. C'est dans ce contexte que naissent Whitfield Diffie et Martin Hellman, en 1944 et 1945 respectivement. Une trentaine d'années plus tard, ils participent aux fondations de la cryptographie moderne. En particulier

ils mettent au point un procédé permettant à Alice et Bob de convenir d'une clef pour leurs communications.

Le fonctionnement en est le suivant. Les deux protagonistes se mettent d'accord sur un groupe cyclique et un générateur de ce groupe : $\langle g \rangle = G$. Alice et Bob choisissent chacun secrètement un entier, respectivement a et b puis échangent l'élément de G obtenu en élevant le générateur à cet ordre : Alice envoie g^a à Bob et Bob répond g^b. Chacun peut ainsi, en élevant le résultat reçu à la puissance son propre exposant, calculer le même nombre $K = g^{ab}$ qui constitue alors leur clef secrète. La figure 3.1 illustre cette démarche. La clef secrète peut ensuite être utilisée pour envoyer des informations de manière sécurisée.

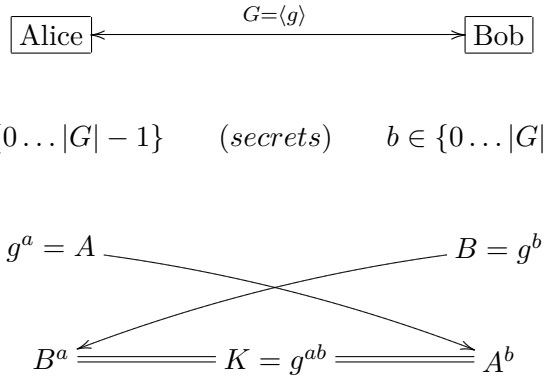

FIGURE 3.1 – Protocole de négociation de clef de Diffie-Hellman.

La sécurité de ce protocole repose sur la difficulté du problème du logarithme discret. En effet, le moyen le plus simple pour l'adversaire Oscar d'intercepter des informations est la connaissance de la clé K. C'est-à-dire que le pirate cherche g^{ab}. S'il a épié le dialogue, il a vu $A = g^a$ et $B = g^b$ mais pour obtenir K à partir de ces données, le seul moyen connu est de disposer de a ou b. Résoudre par exemple en a l'équation $g^a = A$ dans G, est précisément le problème du logarithme discret. Sa difficulté assure la confidentialité de l'échange. Plus précisément, Shoup a montré dans [45] que pour un algorithme calculant le logarithme discret dans un groupe fini générique, il n'y a pas de meilleure complexité en temps que l'ordre de la racine carrée du cardinal dudit groupe. Le résultat est en fait qu'un algorithme effectuant moins de m opérations a, si q premier divise l'ordre du groupe, une probabilité de succès majorée par $O(m^2/q)$.

Notons que la résolution du problème du logarithme discret permet de casser le modèle de Diffie-Hellman mais on n'a pas encore totalement répondu à la question de la réciproque. C'est-à-dire que même si l'on trouve quelques travaux dans ce domaine, notamment [37], on ne sait pas encore si le problème de Diffie-Hellman est aussi difficile que celui du logarithme discret.

3.2 Cryptographie à base de tores

Ici on va s'intéresser au groupe multiplicatif $\mathbb{F}_{q^n}^\times$ d'un corps fini avec q premier et $n > 0$. Plus précisément on considère les sous-groupes de cet objet. L'idée est d'avoir une structure aussi complexe que $\mathbb{F}_{q^n}$ lui-même, qui est une extension de degré n sur $\mathbb{F}_q$. De ce fait le paramétrage d'un élément générique de $\mathbb{F}_{q^n}$ requiert n coordonnées sur $\mathbb{F}_q$. Cependant, on espère en n'en considérant qu'un sous-ensemble, pouvoir représenter les éléments qui nous intéressent de manière moins coûteuse. Ainsi les algorithmes efficaces pour les calculs de logarithme discret doivent travailler dans le corps complet, alors que ceux qui pourraient profiter de la plus petite taille du sous-groupe sont de complexité exponentielle. C'est un équilibre qu'il faut trouver pour cette structure à la fois complexe, autant que $\mathbb{F}_{q^n}$ tout entier si possible, mais assez creuse pour optimiser son paramétrage.

À cette fin, divers travaux ont été effectués avec ce que l'on peut appeler un sous-groupe maximal de $\mathbb{F}_{q^n}^\times$. Il s'agit du sous-groupe de $\mathbb{F}_{q^n}^\times$ d'ordre $\Phi_n(q)$, que je noterai par la suite T_n. Cette notation, bien qu'un peu abusive va considérablement alléger le texte de ce chapitre. Pour se convaincre malgré tout de son bien-fondé, il s'agit de voir que le groupe en question est composé des $\mathbb{F}_q$-points du tore algébrique T_n, c'est-à-dire $\mathrm{T}_n(\mathbb{F}_q)$ dont les définitions équivalentes seront données au chapitre 4.

Les deux plus célèbres exemples d'avancée dans cette voie sont les systèmes appelés LUC et XTR, même si ce dernier protocole a été conçu en recherchant avant tout une efficacité de calcul. Dans les deux cas, l'idée est de représenter un élément de $\mathbb{F}_{q^n}$ par son polynôme minimal sur un sous-corps $\mathbb{F}_{q^d}$. Cela peut paraître revenir au même car on a toujours un polynôme de degré $n/d-1$, soit n/d éléments de $\mathbb{F}_{q^d}$, mais dans ces cas particuliers justement, certaines relations entre les coefficients peuvent rendre la représentation plus compacte.

3.2.1 Genèse de la cryptographie à base de tores

En 1993, Peter Smith et Michael Lennon [33] proposent un nouveau cryptosystème à clef publique, appelé LUC, basé sur des fonctions de Lucas. Introduites au XIX$^{\text{e}}$ siècle par Édouard Lucas, les fonctions de Lucas sont des fonctions définies par des récurrences linéaires d'ordre 2. Les similitudes entre leurs propriétés et celles de l'exponentiation permettent d'élaborer le système LUC de manière analogue au RSA, même si leurs premières applications ont été la factorisation et les tests de primalité.

On considère la suite $(U_k)_k$ définie par la relation de récurrence linéaire d'ordre 2, $U_k = PU_{k-1} - QU_{k-2}$. Dans ce cas, on sait que le terme général s'écrit $U_k = c_1\alpha^k + c_2\beta^k$ où α et β sont les racines du polynôme $X^2 - PX + Q$. Les constantes c_1 et c_2 peuvent être déterminées pour peu que l'on connaisse les valeurs de deux

termes de la suite. Une solution nous intéresse en particulier, à savoir

$$V_k = \alpha^k + \beta^k \quad \text{avec } c_1 = c_2 = 1.$$

Comme elle ne dépend que de P et Q, on la note souvent $V_k(P, Q)$. Alors le cryptosystème LUC repose essentiellement sur le fait que

$$V_{rk}(P, Q) = V_r(V_k(P, Q), Q^k),$$

et en particulier

$$V_{rk}(P, 1) = V_r(V_k(P, 1), 1).$$

Notons que si l'on travaille sur le corps fini $\mathbb{F}_{q^2}$ et que $X^2 - PX + Q$ est supposé irréductible, alors β n'est autre que α^q et V_k représente la trace de α^k. Pour plus de détails, on peut consulter [33] et [46].

Arjen Lenstra et Eric Verheul proposent en 2000 un nouveau système du nom de XTR, comme sigle de *Efficient and Compact Subgroup Trace Representation*. Quelques propositions ont déjà été faites pour améliorer l'efficacité de systèmes du type Diffie-Hellman, comme dans [44]. En 1999 dans [11], Brouwer, Pellikaan et Verheul proposent une méthode avec un faible coût de communication. Comme son nom l'indique, XTR [35] concilie ces deux objectifs et améliore l'efficacité des systèmes connus jusqu'à présent tout en conservant le gain en communication proposé un an plus tôt.

Voici une description succincte du fonctionnement des deux systèmes LUC et XTR d'un point de vue des extensions mises en jeu. On utilise une extension de corps fini de degré respectivement 2 ou 6, et l'on représente avec un minimum de coordonnées les éléments d'un sous-groupe particulier de son groupe multiplicatif.

Le cas de LUC met en jeu le sous-groupe G_2 de $\mathbb{F}_{q^2}$ d'ordre $\Phi_2(q) = q + 1$. Le polynôme minimal d'un élément $h \in G_2$ sur $\mathbb{F}_q$ est :

$$\begin{aligned} P_h &= (X - h)(X - h^q) \\ &= X^2 - (h + h^q)X + 1 \\ &= X^2 - \mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(h)X + 1. \end{aligned}$$

Ainsi $Tr_{\mathbb{F}_{q^2}/\mathbb{F}_q}(h) \in \mathbb{F}_q$ suffit à déterminer P_h. C'est un simple élément de $\mathbb{F}_q$, ce qui est plus économique que les deux coordonnées prévues par la représentation classique.

Le cas de XTR utilise le sous-groupe G_6 de $\mathbb{F}_{q^6}$ d'ordre $\Phi_6(q) = q^2 - q + 1$. Le polynôme minimal de l'élément $h \in G_6$ sur $\mathbb{F}_{q^2}$ est :

$$\begin{aligned} P_h &= (X - h)(X - h^{q^2})(X - h^{q^4}) \\ &= X^3 - (h + h^{q^2} + h^{q^4})X^2 + (h^{q^2+1} + h^{q^4+1} + h^{q^4+q^2})X - h^{q^4+q^2+1}. \end{aligned}$$

On remarque bien sûr que $h + h^{q^2} + h^{q^4} = Tr_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}}(h)$. Mais par un jeu de congruences des exposants modulo $q^2 - q + 1$, on a aussi $h^{q^4+q^2+1} = 1$ et

$$h^{q^2+1} + h^{q^4+1} + h^{q^4+q^2} = h^q + h^{q^5} + h^{q^3} = Tr_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}}(h)^q.$$

Finalement $Tr_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}}(h) \in \mathbb{F}_{q^2}$ suffit à déterminer P_h. C'est un simple élément de $\mathbb{F}_{q^2}$, ce qui est plus économique que les trois coordonnées requises pour la représentation classique du corps $\mathbb{F}_{q^6}$ vu comme extension de $\mathbb{F}_{q^2}$.

Suite à cela, les acteurs de la cryptographie à base de tores se sont posé la question du paramétrage de ces sous-groupes de $\mathbb{F}_{q^n}$, non plus par n coordonnées sur $\mathbb{F}_q$ mais, si possible, seulement $\varphi(n)$, comme c'est le cas pour LUC et XTR. Pour une synthèse plus exhaustive des développements de ces idées, on peut consulter [23].

3.2.2 L'idée de van Dijk et Woodruff

Pouvoir paramétrer ces tores avec des $\varphi(n)$-uplets au lieu de n-uplets permettrait de réduire le coût de la communication tout en espérant conserver la même sécurité que dans $\mathbb{F}_{q^n}^\times$. Et bien que l'on trouve quelques constructions pour des valeurs particulières de n, (par exemple, 2, 3 ou 6 avec LUC [33], XTR [35] ou CEILIDH [42]), la rationalité de ces structures pour tout n n'est que conjecturale [49] et le reste depuis de nombreuses années.

Un paramétrage proposé par van Dijk et Woodruff [18] permet d'éluder astucieusement ce problème. Il s'agit d'identifier T_n avec une partie de $\mathbb{F}_{q^n}^\times$, ce qui ne constitue qu'une injection, puis de mettre en jeu des termes complémentaires afin de la rendre bijective. On obtient une application bijective θ donnée par

$$\theta : T_n \times \prod_{\substack{d \,|\, n \\ \mu(n/d)=-1}} \mathbb{F}_{q^d}^\times \to \prod_{\substack{d \,|\, n \\ \mu(n/d)=+1}} \mathbb{F}_{q^d}^\times, \tag{3.1}$$

où μ désigne la fonction de Möbius.

Pour justifier un tel paramétrage, on écrit dans un premier temps la bijection $\prod_{d \,|\, n} T_d \simeq \mathbb{F}_{q^n}^\times$ qui, moyennant quelques termes toriques complémentaires dans le membre de gauche, fournit une représentation de T_n. Puis van Dijk et Woodruff identifient ces tores avec des groupes du type $\mathbb{F}_{q^d}^\times$, $d \,|\, n$. Par exemple, si p est un nombre premier, on peut identifier $T_1 \times T_p$ et $\mathbb{F}_p^\times$. À ce stade, on peut avoir besoin de quelques nouveaux tores de plus petite dimension. Si l'on a plusieurs termes de la forme T_p différents, on aura besoin de plusieurs éléments complémentaires de la forme T_1 pour tous les apparier. Aussi, on les ajoutera dans le membre de droite également afin de conserver le caractère bijectif. Mais on peut itérer le processus et identifier à nouveau ces termes résiduels dans des groupes de la forme $\mathbb{F}_{q^d}^\times$. Après un nombre fini de telles étapes (la dimension des termes complémentaires décroît strictement à chaque itération), on aboutit à la bijection θ ci-dessus.

Le domaine de cette bijection est plus grand que T_n seul, mais dans le cas où l'on cherche à encoder un grand nombre d'éléments du tore, on peut obtenir un taux de compression quasi-optimal. Comme nous allons le voir au paragraphe 5.3.1, cette bijection permet de représenter m éléments de T_n avec environ $m\varphi(n)$ éléments de $\mathbb{F}_q$ lorsque m est suffisamment grand. On remarque que les $\Phi_d(q)$ n'étant pas nécessairement premiers entre eux, cette bijection n'est pas *a priori* un isomorphisme de groupe.

Exemple. Dans le cas particulier $n = 15$ la bijection θ prend la forme suivante. On sait que

$$T_1 \times T_3 \times T_5 \times T_{15} \simeq \mathbb{F}_{q^{15}}^{\times}\,.$$

Donc $(T_1 \times T_3) \times (T_1 \times T_5) \times T_{15} \simeq \mathbb{F}_{q^{15}}^{\times} \times T_1$, d'où la bijection

$$\theta : \mathbb{F}_{q^3}^{\times} \times \mathbb{F}_{q^5}^{\times} \times T_{15} \xrightarrow{\sim} \mathbb{F}_{q^{15}}^{\times} \times \mathbb{F}_{q}^{\times}\,,$$

car

$$T_1 \simeq \mathbb{F}_q^{\times},\ T_3 \times T_1 \simeq \mathbb{F}_{q^3}^{\times} \ \text{ et } \ T_5 \times T_1 \simeq \mathbb{F}_{q^5}^{\times}.$$

3.2.3 L'algorithme

Van Dijk et Woodruff ont proposé un moyen algorithmique de paramétrer le tore T_n, moyennant quelques contraintes sur q et n [18].

Nous allons maintenant présenter la construction explicite de l'application θ. Notons que son inverse s'obtiendrait de manière similaire ; cependant seul son sens direct sera détaillé ici afin de ne pas alourdir la présentation.

Pour tout $d \,|\, n$, on appelle U_d le plus petit entier positif tel que

$$\forall e \,|\, d,\ \forall f \,|\, d \text{ avec } e \neq f,\ \gcd\left(\Phi_e(q), \Phi_f(q), \frac{q^d-1}{U_d}\right) = 1. \tag{3.2}$$

De plus pour $e \,|\, d \,|\, n$, on pose $y_{d,e} = \gcd\left(\Phi_e(q), (q^d-1)/U_d\right)$ et $z_{d,e} = \gcd(\Phi_e(q), U_d)$. Soient enfin w_d, $w_{d,e}$ et $u_{d,e}$, $v_{d,e}$ les coefficients dans les relations de Bézout

$$\frac{q^d-1}{U_d} w_d + \sum_{e \,|\, d} \frac{q^d-1}{y_{d,e}} w_{d,e} = 1 \ \text{ et } \ \frac{\Phi_e(q)}{y_{d,e}} u_{d,e} + \frac{\Phi_e(q)}{z_{d,e}} v_{d,e} = 1\,. \tag{3.3}$$

Avec ces notations, on a les bijections suivantes, pour tout $d \,|\, n$.

$$\mathbb{F}_{q^d}^{\times} \xrightarrow{\sim} \mathbb{Z}/U_d\mathbb{Z} \times \prod_{e \,|\, d} \mathbb{Z}/y_{d,e}\mathbb{Z} \ \text{ et } \ \mathbb{Z}/U_d\mathbb{Z} \xrightarrow{\sim} \prod_{e \,|\, d} \mathbb{Z}/z_{d,e}\mathbb{Z}\,.$$

Ces deux bijections successives donnent pour chaque $\mathbb{F}_{q^d}$ la décomposition suivante en briques élémentaires :

$$\left(\prod_{e\,|\,d}\mathbb{Z}/y_{d,e}\mathbb{Z}\right)\times\left(\prod_{e\,|\,d}\mathbb{Z}/z_{d,e}\mathbb{Z}\right).$$

La première bijection est canonique et est simplement donnée par le théorème chinois, alors que la seconde n'est pas canonique est doit être réalisée point par point, ce que l'on appelle en anglais *table lookup*. Van Dijk et Woodruff ont démontré que les tailles des objets mis en jeu sont raisonnables lorsque quelques conditions techniques sont réalisées pour n et q, à savoir que n soit un produit de nombres premiers distincts et que q soit d'ordre maximal modulo ces nombres premiers.

Il s'agit maintenant de donner une décomposition des deux membres de l'application θ en ces petites briques élémentaires et d'identifier celles qui apparaissent de chaque côté de la bijection. On y retrouve les mêmes groupes dans un ordre différent, à l'exception de T_n qui s'envoie sur $\mathbb{Z}/y_{n,n}\mathbb{Z}\times\mathbb{Z}/z_{n,n}\mathbb{Z}$. Pour tout $d\,|\,n$, $d\neq n$, on identifie $\prod_{e\,|\,d}\mathbb{Z}/z_{d,e}\mathbb{Z}\longrightarrow\prod_{e\,|\,d}\mathbb{Z}/z_{\rho_e(d),e}\mathbb{Z}$ où ρ_e est la bijection

$$\rho_e : \{d : e\,|\,d\,|\,n, \mu(n/d)=1\}\xrightarrow{\sim}\{d : e\,|\,d\,|\,n, \mu(n/d)=-1\}.$$

Finalement on obtient l'algorithme 1.

Algorithme 1 : Calcul de θ.

Entrées : $x\in T_n$ et $x_d\in\mathbb{F}_{q^d}^\times$ pour tout $d\,|\,n$ tel que $\mu(n/d)=-1$.

Sorties : $x_d\in\mathbb{F}_{q^d}^\times$ pour tout $d\,|\,n$ tel que $\mu(n/d)=1$.

pour chaque $d\,|\,n$ tel que $\mu(n/d)=-1$ **faire**
  Calculer $x_d\mapsto x_d^{(q^d-1)/U_d}$, l'application canonique $\mathbb{F}_{q^d}^\times\to\mathbb{Z}/U_d\mathbb{Z}$.
  Calculer $x_d^{(q^d-1)/U_d}\mapsto(Z_{d,e})_{e\,|\,d}$, le *table lookup* $\mathbb{Z}/U_d\mathbb{Z}\to\prod_{e\,|\,d}\mathbb{Z}/z_{d,e}\mathbb{Z}$.
  Associer $(Z_{d,e})_{e\,|\,d}\mapsto(Z_{\rho_e(d),e})_{e\,|\,d}$ avec $Z_{\rho_e(d),e}=(Z_{d,e}^{v_{d,e}}x_d^{(q^d-1)u_{d,e}/y_{d,e}})^{\Phi_e(q)/z_{\rho_e(d),e}}$, *i.e.* associer $\prod_{e\,|\,d}\mathbb{Z}/z_{d,e}\mathbb{Z}\to\prod_{e\,|\,d}\mathbb{Z}/z_{\rho_e(d),e}\mathbb{Z}$.
fin
Calculer $Z_{n,n}=x^{\Phi_n(q)/z_{n,n}}\in\mathbb{Z}/z_{\rho(n),n}\mathbb{Z}$.
pour chaque $d\,|\,n$ tel que $\mu(n/d)=1$ **faire**
  Calculer $(Z_{d,e})_{e\,|\,d}\mapsto Z_d$, le *table lookup* $\prod_{\substack{\rho_e(d')=d,\\ e\neq d}}e\,|\,d\,\mathbb{Z}/z_{d',e}\mathbb{Z}\to\mathbb{Z}/U_d\mathbb{Z}$.
  Calculer $x_d=Z_d^{w^d}\prod_{\substack{\rho_e(d')=d,\\ e\neq d}}e\,|\,d(Z_{d',e}^{v_{d',e}}x_{d'}^{(q^{d'}-1)u_{d',e}/y_{d',e}})^{\Phi_e(q)w_{d,e}/y_{d,e}}\in\mathbb{F}_{q^d}^\times$.
fin
Multiplier x_n par $x^{\Phi_n(q)w_{n,n}/y_{n,n}}$.

Exemple. On revient au cas $n = 15$ avec $U_d = 1$ pour tout $d \mid n$, qui permet de bien comprendre ce qui se passe. La figure 3.2 donne un aperçu de la construction de θ dans ce cas.

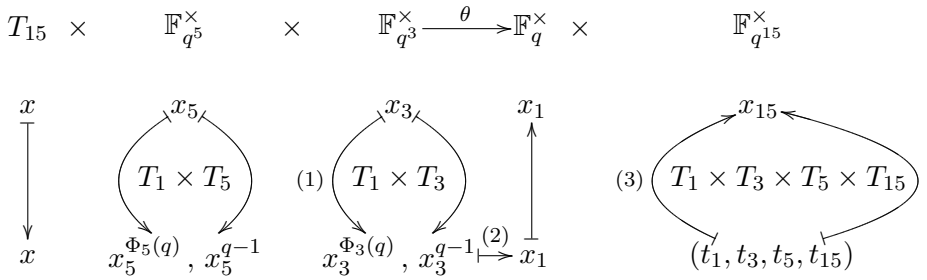

FIGURE 3.2 – La bijection θ pour $n = 15$ et $U_1 = U_3 = U_5 = U_{15} = 1$.

Il y a plusieurs simplifications par rapport au cas général. Pour tout $e \mid d$, $y_{d,e} = \Phi_e(q)$ et $z_{d,e} = 1$. Donc les groupes $\mathbb{Z}/y_{d,e}\mathbb{Z}$ ne sont autres que les tores T_e. En outre, $u_{d,e} = 1$ et $v_{d,e} = 0$. L'équation 3.3 devient alors $\sum_{e \mid d} \frac{q^d-1}{\Phi_e(q)} w_{d,e} = 1$, et x_{15} est donné par $x_{15} = t_1^{w_{15,1}} t_3^{w_{15,3}} t_5^{w_{15,5}} t_{15}^{w_{15,15}}$.

Via un calcul explicite, on peut montrer que les $w_{15,e}$ ont pour dénominateur commun 15. D'où $x_{15} = (t_1^{r_1} t_3^{r_3} t_5^{r_5} t_{15}^{r_{15}})^{1/15}$, où les r_e sont des polynômes agréables en q,

$$\begin{cases} r_1 = 1, \\ r_3 = -q - 2, \\ r_5 = -q^3 - 2\,q^2 - 3\,q - 4, \\ r_{15} = q^7 - 3\,q^5 + 4\,q^4 - 5\,q^3 + 7\,q - 8. \end{cases}$$

3.2.4 Complexité

Le coût du paramétrage présenté dans la figure 3.2 est le suivant.

Phase (1). Les élévations aux puissances $q - 1$, $\Phi_3(q) = q^2 + q + 1$ et $\Phi_5(q) = q^4 + q^3 + q^2 + q + 1$ coûtent en moyenne respectivement $\frac{1}{2}\log q$, $\frac{1}{2}(2\log q)$ et $\frac{1}{2}(4\log q)$ multiplications car les exposants sont de tailles respectives q, q^2 et q^4.

Phase (2). Négligeable.

Phase (3). Si l'on se rappelle les expressions des coefficients r_e, les élévations à ces puissances requièrent en moyenne $\deg r_e \times (\frac{1}{2}\log q)$, soit en tout $(0 + 1 + 3 + 7) \times (\frac{1}{2}\log q)$ multiplications.

Cette évaluation montre que le coût moyen est d'environ $9 \log q$ multiplications dans $\mathbb{F}_{q^{15}}$, c'est-à-dire $\log^{2+o(1)} q$ opérations élémentaires. Van Dijk et Woodruff proposent

quelques pistes pour améliorer ce résultat en pratique (étude de redondances, multi-exponentiations, *etc.*), mais la complexité asymptotique reste quasi-quadratique en $\log q$.

On peut maintenant évaluer plus précisément la complexité de l'algorithme 1. On commence par construire un polynôme irréductible $P \in \mathbb{F}_q[X]$ de degré n, ce qui peut se faire en $n^{2+o(1)} \log^{2+o(1)} q$ opérations [41]. Soit $\alpha = X \bmod P$. Alors $(1, \alpha, \ldots, \alpha^{n-1})$ est une $\mathbb{F}_q$-base de $\mathbb{F}_{q^n}$. Les additions, les soustractions et les comparaisons se font en $O(n \log q)$ opérations élémentaires. Les multiplications et les divisions en nécessitent $n^{1+o(1)} \log^{1+o(1)} q$.

Il faut aussi gérer les changements de base entre $\mathbb{F}_{q^n}$ et ses sous-corps $\mathbb{F}_{q^d}$. De tels sous-corps peuvent constituer un réseau assez important : il y en a $d(n)$, autant que des diviseurs de n (voir l'exemple d'un produit de trois nombres premiers distincts figure 3.3). Pour des raisons de simplicité, on considère que les éléments de $\mathbb{F}_{q^d}$, avec $d \mid n$, sont donnés dans la base $(1, \alpha, \ldots, \alpha^{n-1})$ également, ce qui ne change pas la complexité. On peut donc aisément multiplier deux éléments de deux sous-corps distincts. Simplement, afin d'obtenir les bonnes tailles en entrée et en sortie de l'algorithme, on applique à un élément de $\mathbb{F}_{q^d}$ donné dans $\mathbb{F}_{q^n}$ une compression $\mathbb{F}_q$-linéaire, dérivée d'équations du type $x^{q^d} = x$. On a ainsi des matrices $A_{n,d} \in \mathcal{M}_{n,d}(\mathbb{F}_q)$ représentant l'injection $\mathbb{F}_{q^d} \hookrightarrow \mathbb{F}_{q^n}$. La multiplication par ces matrices ainsi que leur construction préalable requièrent n^3 multiplications dans $\mathbb{F}_q$. Comme elles sont au nombre de $d(n) \simeq n^{o(1)}$, on obtient un coût total de $n^{3+o(1)} \log^{1+o(1)} q$ opérations élémentaires.

Si cela explique le principe de construction, on considérera cependant que l'ensemble de cette structure est donné. Ainsi le réseau de sous-corps et les projections ou injections qui les relient sont calculées au préalable.

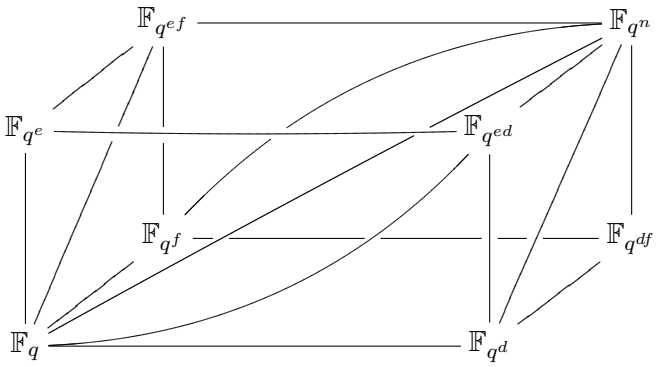

FIGURE 3.3 – Réseau de corps finis dans le cas $n = def$, produit de trois nombres premiers distincts.

Van Dijk et Woodruff soulignent que pour des entiers n et q raisonnables, à savoir n un produit de nombres premiers distincts et q d'ordre maximal modulo ces nombres premiers, le *table lookup* a une complexité négligeable et les opérations les plus coûteuses de l'algorithme sont les étapes 4 et 9. Les exposants mis en jeu proviennent de polynômes cyclotomiques. Le calcul de Φ_n peut se faire essentiellement en temps égal à sa taille (on reconstruit Φ_n à partir d'approximations de ses racines complexes). Comme il est de degré $\varphi(n)$ et que ses coefficients sont bornés en valeur absolue par $n^{d(n)/2}$ [22, 5], il est de taille au plus $n^{1+o(1)}$ bits. Les évaluations de tous les Φ_d en q donnent des exposants de $d \log q$ bits et peuvent se faire en $n^{2+o(1)} \log^{1+o(1)} q$ opérations élémentaires. En remarquant finalement que $\sum_{d \mid n} d \simeq n^{1+o(1)}$, les étapes 4 et 9 coûtent au total $n^{3+o(1)} \log^{2+o(1)} q$.

3.2.5 La variante de van Dijk *et al.*

En 2005, van Dijk *et al.* [17] ont apporté une amélioration aux travaux de l'année précédente et il faut naturellement la prendre en compte dans notre étude. Ils montrent dans cet article que si n est sans facteur carré et si m est un diviseur de n, alors l'équation (3.1) peut être remplacée par la bijection

$$\mathrm{T}_n(\mathbb{F}_q) \times \prod_{d \mid \frac{n}{m},\ \mu(\frac{n}{md})=-1} \mathrm{T}_m(\mathbb{F}_{q^d}) \to \prod_{d \mid \frac{n}{m},\ \mu(\frac{n}{md})=1} \mathrm{T}_m(\mathbb{F}_{q^d})\,. \tag{3.4}$$

Ceci prend tout son sens lorsque les T_m sont eux-mêmes rationnels, c'est-à-dire lorsque m est composé d'au plus deux facteurs premiers, du moins dans l'état actuel des connaissances sur la rationalité des tores algébriques [49]. Par exemple pour $n = 30$ et $m = 6$, cela donne un excellent taux de compression pour le paramétrage de $\mathrm{T}_{30}(\mathbb{F}_q)$.

Cette bijection consiste à nouveau en une phase de décomposition en petits tores élémentaires suivie d'une phase de reconstruction, comme on peut le voir sur la figure 3.4. Tous les éléments des tores présents dans l'équation (3.4) peuvent être vus comme éléments de $\mathrm{T}_m(\mathbb{F}_{q^{n/m}})$. Ainsi, sous certaines conditions techniques sur q et n, ces deux phases se résument à des exponentiations dans $\mathrm{T}_m(\mathbb{F}_{q^{n/m}})$. Les puissances mises en jeu sont des produits d'évaluations de polynômes cyclotomiques $\Phi_d(q)$ ou de leurs inverses.

Pour $n = 30$, van Dijk *et al.* obtiennent une implémentation rapide en représentant le corps $\mathbb{F}_{q^5}$ par une base normale gaussienne de type 2 pour y effectuer des opérations arithmétiques. Cependant on ne peut espérer étendre cette stratégie à un n quelconque car les bases normales gaussiennes de type petit sont connues pour de rares degrés d'extensions.

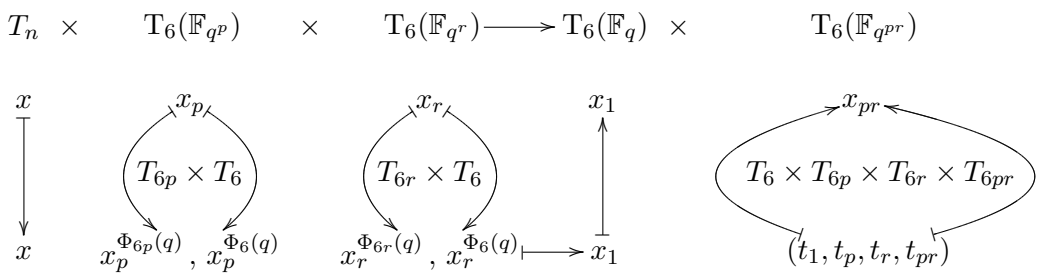

FIGURE 3.4 – Variante de van Dijk *et al.* pour $n = 6pr$.

3.2.6 Vers une nouvelle approche

On observe que la plupart des travaux effectués dans le domaine de la cryptographie se concentre sur des tores spécifiques, à savoir T_2, T_6 ou T_{30} qui sont en accord avec les tailles cryptographiques standard. On peut notamment consulter [34, 27, 17] pour des résultats détaillés sur l'optimisation de certaines des implémentations connues. Comme on a pu l'entr'apercevoir dans les exemples du paragraphe 3.2.1, il est clair que l'ingrédient clef de ces travaux est l'automorphisme de Frobenius sur $\mathbb{F}_{q^2}$ ou $\mathbb{F}_{q^6}$. Le choix de $n = 2$, 6 ou 30 n'est pas anodin. En effet le rapport de compression $\varphi(n)/n$ est optimal lorsque n est composé des plus petits facteurs premiers distincts possibles.

Il est maintenant légitime de se demander si ces techniques se généralisent à une plus grande variété de degrés d'extensions. Un premier pas dans cette direction consiste naturellement à examiner le problème de manière asymptotique, dans l'espoir d'y trouver l'inspiration pour implémenter des fonctions plus efficaces. La majeure partie de la complexité vient des exponentiations dans $\mathbb{F}_{q^n}$. Comme quelques études l'ont déjà relevé, certains de ces exposants sont des polynômes cyclotomiques évalués en des puissances de q et tendent à avoir une décomposition agréable en base q. D'autres font intervenir des inverses modulaires de polynômes cyclotomiques. Cependant leur arithmétique particulière semble avoir été assez peu exploitée pour l'accélération de cette phase. Dans le chapitre 5, nous allons utiliser les résultats arithmétiques du chapitre 2 afin de rendre plus efficace le calcul de ces exponentiations.

Gewisse Bücher scheinen geschrieben zu sein, nicht damit man daraus lerne, sondern damit man wisse, dass der Verfasser etwas gewusst hat.

Johann Wolfgang von Goethe

CHAPITRE 4

TORES ALGÉBRIQUES

Un grand pas en avant vient d'être effectué. L'on vient de voir l'utilisation en cryptographie de nouvelles structures que nous avons naturellement appelées tores. Cette appellation n'est pas anodine ; en effet les groupes appelés T_n dans le chapitre précédent peuvent être vus comme les $\mathbb{F}_q$-points de variétés algébriques bien particulières : les tores algébriques. Ce chapitre présente leur structure et le lien avec les constructions du chapitre 3, ainsi que la structure de leur anneau d'endomorphismes.

On pose aussi les définitions directes que l'on peut donner d'un tore en tant que groupe et l'on montre leur équivalence, qui repose sur l'arithmétique des polynômes cyclotomiques. Par ailleurs, le calcul de la dimension d'un tore en tant que variété algébrique nous éclairera sur les espoirs de compression de données lorsque l'on cherche à paramétrer ses éléments.

4.1 Structure des tores algébriques

Soient K un corps et $\bar{K}$ une clôture algébrique de K. On note $\mathbb{G}_m$ le groupe multiplicatif. C'est un groupe algébrique absolument connexe de dimension 1. Soit enfin $\mathbb{A}^s$ l'espace affine de dimension s.

Définition 4.1.
Un tore algébrique *sur K est un groupe algébrique connexe* T *qui est isomorphe sur $\bar{K}$ à $\mathbb{G}_m^s$ avec $s \in \mathbb{N}$. On appelle* corps de décomposition *de* T *tout sous-corps L de $\bar{K}$ sur lequel* T *est isomorphe à $\mathbb{G}_m^s$.*

On considère dorénavant des extensions finies de corps finis. Soient $L = \mathbb{F}_{q^n}$ une extension finie galoisienne de $K = \mathbb{F}_q$ avec q premier et $n \in \mathbb{N}^*$. On note G le groupe

de Galois $\mathrm{Gal}(L/K)$ et $\mathrm{Res}_{L/K}$ le foncteur de la restriction des scalaires de Weil de L à K. Pour un exposé plus complet des propriétés de la restriction de Weil, on peut consulter [49] ou [50] par exemple. Ce qui nous sera utile ici découle de sa propriété universelle.

Notation. Étant donnés V une variété et F un ensemble fini, on note

$$V^F = \bigoplus_{f\in F} V \simeq V^{|F|}.$$

Proposition 4.1 ([43])**.**

(i) *Soit V une variété définie sur K. Alors on a un L-isomorphisme*

$$\iota : \mathrm{Res}_{L/K} V \xrightarrow{\sim} V^G. \tag{4.1}$$

dont les applications coordonnées sont données par des morphismes de projection $\mathrm{Res}_{L/K} V \to V$.

(ii) *De plus pour toute extension intermédiaire $K \subseteq F \subseteq L$, on a une bijection*

$$(\mathrm{Res}_{L/K} V)(F) \simeq V(F \otimes_K L). \tag{4.2}$$

Notations. L'équation (4.2) implique que $(\mathrm{Res}_{F/K} \mathbb{G}_m)(K) \simeq \mathbb{G}_m(F) = F^\times$ et de même $(\mathrm{Res}_{F/K} \mathbb{A}^1)(K) \simeq \mathbb{A}^1(F) \simeq F$. On notera par la suite $\mathbb{A}_F = \mathrm{Res}_{F/K} \mathbb{A}^1$ et $\mathbb{G}_F = \mathrm{Res}_{F/K} \mathbb{G}_m$.

Dans le cas particulier où $V = \mathbb{G}_m$, l'isomorphisme (4.1) permet de représenter un L-point de $(\mathrm{Res}_{L/K} \mathbb{G}_m)$ avec $|G|$ coordonnées à valeurs dans $\mathbb{G}_m \subset \mathbb{A}^1$. On peut définir des applications norme et trace en effectuant respectivement le produit et la somme de ces coordonnées. On définit ainsi une norme

$$\begin{array}{rccccc} \mathrm{N}_{L/K} : & \mathbb{G}_L & \xrightarrow{\iota} & \mathbb{G}_m^G & \to & \mathbb{G}_m \\ & \alpha & \mapsto & (\alpha_g)_{g\in G} & \mapsto & \prod_{g\in G} \alpha_g, \end{array}$$

qui se trouve être définie sur K.

Plus généralement, pour toute extension intermédiaire $K \subseteq F \subseteq L$, on peut construire des normes partielles $\mathrm{N}_{L/F,K} : \mathrm{Res}_{L/K} \mathbb{G}_m \to \mathrm{Res}_{F/K} \mathbb{G}_m$. À cette fin, on note $H := \mathrm{Gal}(L/F) \subseteq G$. Si $n = |G|$ et $d = |H|$ désignent les degrés de ces extensions, alors on peut définir des morphismes de projection particuliers pour $1 \leqslant i \leqslant d$:

$$\sigma_{i,F} : \mathbb{A}_F \xrightarrow{\sim} \mathbb{A}^H \to \mathbb{A}^1,$$

où la première application est la bijection (4.1) de la propriété précédente et la seconde est le i^{e} polynôme symétrique élémentaire en les d projections canoniques (coordonnées) $\mathbb{A}^H \to \mathbb{A}^1$.

On définit la norme $\mathrm{N}_{L/F}$ et la trace $\mathrm{Tr}_{L/F}$ comme étant respectivement $\sigma_{d,F}$ et $\sigma_{1,F}$. On comprend via le diagramme commutatif suivant écrit pour tout $1 \leqslant i \leqslant d$ que ces applications correspondent aux norme et trace usuelles sur L.

$$\begin{array}{ccc} \mathbb{A}_L(K) & \xrightarrow{\sigma_{i,K}} & \mathbb{A}^1(K) \\ \sim\downarrow & & \downarrow\sim \\ L & \xrightarrow{\sigma_{i,K}} & K \end{array}$$

Notons maintenant que $\mathrm{Res}_{F/K}\,\mathrm{Res}_{L/F}\,\mathbb{A}^1 = \mathrm{Res}_{L/K}\,\mathbb{A}^1$. Via la restriction de Weil de F à K, les applications $\sigma_{i,F}$ induisent donc des $\hat{\sigma}_{i,F} : \mathbb{A}_L \to \mathbb{A}_F$. Comme ci-dessus, le choix particulier de deux de ces applications permet de définir la norme $\mathrm{N}_{L/F,K} = \hat{\sigma}_{d,F}$ et la trace $\mathrm{Tr}_{L/F,K} = \hat{\sigma}_{1,F}$. L'inclusion naturelle de $\mathbb{G}_m$ dans $\mathbb{A}^1$ en induit une de $\mathbb{G}_F$ dans $\mathbb{A}_F$ via $\mathrm{Res}_{F/K}$. La restriction des $\mathrm{N}_{L/F,K}$ à ces groupes fournit donc des applications normes sur $\mathbb{G}_F$ pour toute extension $K \subseteq F \subseteq L$.

Définition 4.2.
On définit le tore algébrique T_L *comme l'intersection des noyaux des normes* $\mathrm{N}_{L/F,K}$ *pour tous les sous-corps stricts* $K \subset F \subsetneq L$.

$$\mathrm{T}_L = \bigcap_{K \subseteq F \subsetneq L} \mathrm{Ker}\,[\mathbb{G}_L \xrightarrow{\mathrm{N}_{L/F,K}} \mathbb{G}_F].$$

Pour comprendre la structure et notamment la dimension de ces tores, il convient de passer par une formulation différente de cette construction. Avec les notations ci-dessus, on considère les normes définies pour tout H sous-groupe de $G = \mathrm{Gal}(L/K)$ par

$$\begin{array}{rccc} \mathrm{N}_H & : & \mathbb{G}_m^G & \to & \mathbb{G}_m^{G/H} \\ & & (\alpha_g)_{g\in G} & \mapsto & \left(\displaystyle\prod_{\gamma\in gH} \alpha_\gamma\right)_{gH\in G/H} \end{array}. \tag{4.3}$$

On définit alors le tore algébrique $\mathbb{T}_G$ comme l'intersection des noyaux de ces normes pour tous les sous-groupes non triviaux de G.

$$\mathbb{T}_G = \bigcap_{\{1\}\subsetneq H \subseteq G} \mathrm{Ker}\,[\mathbb{G}_m^G \xrightarrow{\mathrm{N}_H} \mathbb{G}_m^{G/H}].$$

L'isomorphisme de la proposition 4.1 entre $\mathrm{Res}_{K/k}\,\mathbb{G}_m$ et $\mathbb{G}_m^G$ donne une correspondance entre T_L et $\mathbb{T}_G$.

4.2 Point de vue des groupes

Toujours dans le cas où $K = \mathbb{F}_q$ et $L = \mathbb{F}_{q^n}$ avec q premier et $n \in \mathbb{N}^*$, pour tout x de $\mathbb{F}_{q^n}$ et toute extension $\mathbb{F}_q \subseteq \mathbb{F}_{q^d} \subseteq \mathbb{F}_{q^n}$ avec $d|n$, on a l'expression de la norme

$$\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^d},\mathbb{F}_q}(x) = x^{\frac{q^n-1}{q^d-1}}.$$

On définit alors le tore $\mathrm{T}_n(\mathbb{F}_q)$ comme l'intersection des noyaux de ces normes, pour tous les diviseurs stricts d de n.

$$\mathrm{T}_n(\mathbb{F}_q) = \left\{ x \in \mathbb{F}_{q^n}^\times, \forall d | n, 1 \leqslant d < n, x^{\frac{q^n-1}{q^d-1}} = 1 \right\}. \tag{4.4}$$

On peut également donner comme définition

$$\mathrm{T}_n(\mathbb{F}_q) = \left\{ x \in \mathbb{F}_{q^n}^\times, x^{\Phi_n(q)} = 1 \right\}, \tag{4.5}$$

qui lui est équivalente comme l'indique la proposition suivante, énoncée notamment dans [42]. Cela repose sur quelques résultats techniques comme ceux présentés dans le chapitre 1.

Proposition 4.2.
Les définitions données par les équations (4.4) *et* (4.5) *du tore T_n sont équivalentes.*

Démonstration.
Commençons par écrire différemment la relation (4.4). En effet dans l'expression des normes $\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^d}}$, chaque terme $q^d - 1$ s'écrit $\prod_{k|d} \Phi_k(q)$; et l'on a bien sûr aussi $q^n - 1 = \prod_{d|n} \Phi_d(q)$. Ainsi,

$$\mathrm{T}_n(\mathbb{F}_q) = \left\{ x \in \mathbb{F}_{q^n}^\times, \forall d | n, 1 \leqslant d < n, x^{\prod_{\substack{k|n \\ k\nmid d}} \Phi_k(q)} = 1 \right\}.$$

Dans la définition (4.5), on a l'équation $x^{\Phi_n(q)} = 1$. Il est bien évident que cette seule équation entraîne toutes celles présentes dans la famille ci-dessus. Donc la définition (4.5) entraîne la définition (4.4).

Montrons maintenant la réciproque. Pour parvenir à cette seule dernière équation à partir de toutes celles qui précèdent, il faut réussir à éliminer la plupart des $\Phi_k(q)$ de manière à ne garder plus que $\Phi_n(q)$. Pour cela, on va écrire $q^n - 1$ d'une manière bien particulière. Notons $\varpi(d)$ le nombre de diviseurs premiers, distincts ou non, de d. Alors

$$q^n - 1 = \prod_{j \geqslant 0} \prod_{\substack{k|n \\ \varpi(k)=j}} \Phi_k(q) = \Phi_1(q) \prod_{\substack{k|n \\ k \in \mathcal{P}}} \Phi_k(q) \prod_{\substack{k=p_1p_2|n \\ p_1,p_2 \in \mathcal{P}}} \Phi_k(q) \dots \Phi_n(q).$$

On va raisonner par récurrence, en examinant d'abord $\prod_{\substack{k|n \\ k \in \mathcal{P}}} \Phi_k(q)$ puis les suivants, dans l'ordre. Voici le fonctionnement de ce procédé. On a la famille d'équations suivante :

$$\left(x^{\prod_{\substack{k|n \\ k\nmid d}} \Phi_k(q)} = 1 \right)_{\substack{d|n \\ 1 \leqslant d < n}}.$$

L'idée est d'éliminer les $\Phi_k(q)$ un à un de la manière suivante. Quand on arrive à isoler dans les puissances de x deux polynômes cyclotomiques d'indices non multiples l'un de l'autre, alors on peut utiliser leur coprimalité pour les éliminer. En clair, si l'on a deux équations $(x^P)^{\Phi_r(q)}$ et $(x^P)^{\Phi_s(q)}$ (où P est une puissance quelconque, en l'occurrence une partie du produit) avec r et s non multiples l'un de l'autre, alors on sait d'après le corollaire 1.2 que $\Phi_r(q)$ et $\Phi_s(q)$ sont premiers entre eux. Il existe en particulier une relation de Bézout : $\Phi_r(q)U + \Phi_s(q)V = 1$ et alors $\left(x^{P\Phi_r(q)}\right)^U \left(x^{P\Phi_s(q)}\right)^V = x^P$ nous donne l'équation $x^P = 1$, où $\Phi_r(q)$ et $\Phi_s(q)$ ont été éliminés. On va simplement utiliser cette technique de nombreuses fois successivement et de manière suffisamment astucieuse pour se ramener à $x^{\Phi_n(q)} = 1$.

Avec $d \in \mathcal{P}$ un nombre premier et si l'on note $d_1, \ldots, d_r$ les diviseurs premiers de n, alors les différentes puissances intervenant dans les équations sont

$$\left(\prod_{\substack{k|n, k\in\mathcal{P} \\ k\neq d_i}} \Phi_k(q) \overbrace{\prod_{\substack{k=p_1p_2|n \\ p_1,p_2\in\mathcal{P}}} \Phi_k(q)\ldots\Phi_n(q)}^{P_2} \right)_{1\leqslant i\leqslant r}.$$

Le facteur x^{P_2} est invariablement présent. Seules changent les contributions du premier produit. Pour éliminer d_1 et d_2, on utilise les équations de x^{P_2} aux puissances

$$\begin{array}{llll} \Phi_{d_2}(q)\Phi_{d_3}(q) & \ldots & \Phi_{d_r}(q) \text{ et} \\ \Phi_{d_1}(q)\Phi_{d_3}(q) & \ldots & \Phi_{d_r}(q), \end{array}$$

avec d_1 et d_2 non multiples l'un de l'autre. Une relation de Bézout entre $\Phi_{d_1}(q)$ et $\Phi_{d_2}(q)$ permet, comme expliqué plus haut, de les éliminer.

De même on élimine $\Phi_{d_i}(q)$ et $\Phi_{d_{i+1}}(q)$ pour tout $1 \leqslant i \leqslant r-1$. On a alors une famille d'équations dont les puissances de x, mis à part le facteur P_2 toujours présent, font apparaître $\left(\Phi_{d_1}(q), \ldots, \Phi_{d_i}(q), \Phi_{d_{i+3}}(q), \ldots, \Phi_{d_r}(q)\right)_{1\leqslant i\leqslant r-2}$. Ainsi à partir de termes faisant intervenir tous les d_i sauf 1, à tour de rôle, on s'est ramené à des termes évitant à tour de rôle les paires de d_i, d_{i+1} successifs. On peut généraliser ce procédé :

À partir des produits

$$\Phi_{d_1}(q)\ldots\Phi_{d_i}(q)\Phi_{d_{i+j}}(q)\ldots\Phi_{d_r}(q) \text{ et } \Phi_{d_1}(q)\ldots\Phi_{d_{i+1}}(q)\Phi_{d_{i+j+1}}(q)\ldots\Phi_{d_r}(q),$$

on peut, en appliquant une identité de Bézout à $\Phi_{d_{i+1}}(q)$ et $\Phi_{d_{i+j}}(q)$, se ramener à $\Phi_{d_1}(q)\ldots\Phi_{d_i}(q)\Phi_{d_{i+j+1}}(q)\ldots\Phi_{d_r}(q)$, qui présente une lacune d'un indice de plus que les deux équations de départ.

Ainsi l'itération de cette technique permet d'éliminer tout le premier produit. On s'est ainsi ramené à une équation où l'on a éliminé tout le premier produit en puissance. Il s'agit maintenant de répéter le processus, toujours en utilisant la

coprimalité de $\Phi_r(q)$ et $\Phi_s(q)$ lorsque r et s ne sont pas multiples l'un de l'autre. Amorçons le procédé pour se convaincre de son bon fonctionnement.

Soit $d = p_1 p_2$ un diviseur de n avec deux facteurs premiers. L'équation associée à cette extension, dans la caractérisation (4.4), est $x^{\frac{q^n-1}{q^d-1}} = 1$, avec

$$\frac{q^n-1}{q^d-1} = \prod_{\substack{k|n, k\in\mathcal{P} \\ k\neq p_1,p_2}} \Phi_k(q) \prod_{\substack{k|n, k\neq d \\ \varpi(k)=2}} \Phi_k(q)\dots\Phi_n(q).$$

On va recouper cette équation avec l'équation faisant apparaître

$$\prod_{\substack{k=p_1p_2|n \\ p_1,p_2\in\mathcal{P}}} \Phi_k(q)\dots\Phi_n(q)$$

et éliminer $\Phi_d(q)$. En effet, $\Phi_d(q)$ est premier avec tous les $\Phi_k(q)$, $k \in \mathcal{P}, k \neq p_1, p_2$ (car d est non multiple de ces indices). On peut ainsi écrire une relation de Bézout entre $\Phi_d(q)$ et $\prod_{\substack{k|n, k\in\mathcal{P} \\ k\neq p_1,p_2}} \Phi_k(q) = 1$, ce qui permet par combinaison des deux équations, de se ramener à :

$$x^{\prod_{\substack{k=p_1p_2|n \\ k\neq d}} \Phi_k(q) \prod_{\substack{k|n \\ \varpi(k)\geqslant 3}} \Phi_k(q)} = 1.$$

On peut naturellement procéder de même avec chaque diviseur d tel que $\varpi(d) = 2$, et ainsi obtenir une famille d'équations avec chacune une lacune dans le produit. Il reste à combiner toutes les équations de cette famille pour éliminer jusqu'au dernier les facteurs du produit portant sur les diviseurs d tels que $\varpi(d) = 2$. L'élimination se fait de manière récursive, exactement comme dans le cas des diviseurs premiers : si l'on note I l'ensemble des indices k sur lesquels porte ce produit, la combinaison de $I \setminus \{d_i \dots d_{j-1}\}$ et de $I \setminus \{d_{i+1} \dots d_j\}$ permet d'obtenir l'équation où le produit porte sur $I \setminus \{d_i \dots d_j\}$. Le diagramme de la figure 4.1 synthétise le processus. La colonne de gauche représente les différents ensembles d'indices intervenant dans les équations à notre disposition au départ. Le parcours du graphe vers la droite se fait par éliminations successives des facteurs du produit, par l'utilisation du théorème de Bézout, comme exposé précédemment.

On arrive ainsi à éliminer de l'équation tout le facteur $x^{\prod_{\substack{k|n \\ \varpi(k)=2}} \Phi_k(q)}$.

La suite consiste simplement en la répétition de ce procédé pour les produits portant sur les diviseurs k tels que $\varpi(k) = 3$ puis 4, etc. On peut assez facilement se convaincre du bon fonctionnement de cette méthode. En effet les étapes suivantes sont très similaires à la deuxième, qui vient d'être traitée.

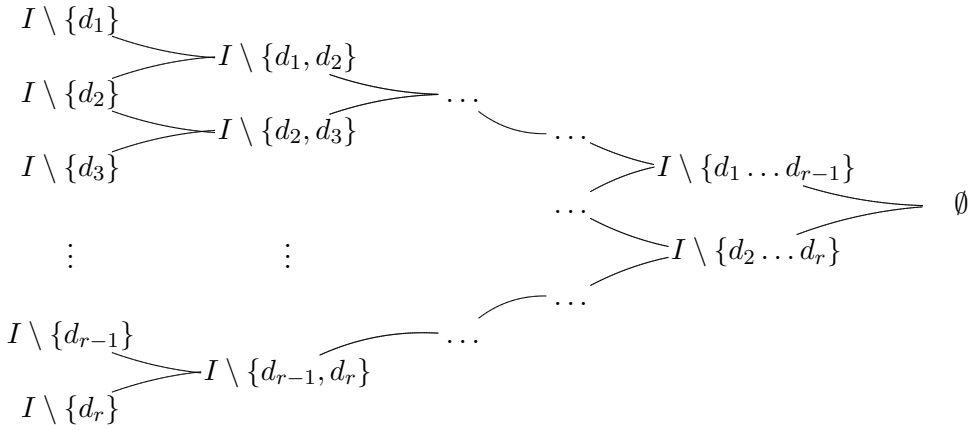

FIGURE 4.1 – Procédé d'élimination successive des indices, de la gauche vers la droite.

Pour l'étape au rang $r > 1$ par exemple, supposons que l'on ait éliminé tous les produits portant sur les k tel que $\varpi(k) < r$. Alors pour d diviseur de n avec un nombre r de facteurs premiers, diviser $q^n - 1$ par $q^d - 1$ revient à ôter du produit tous les termes correspondant à un indice $k \nmid d$. Ainsi d est non multiple de tous les indices restants et l'on élimine $\Phi_d(q)$ comme précédemment car il est premier avec $\prod_{\substack{k \nmid d \\ \varpi(k) < \varpi(d)}} \Phi_k(q)$. On peut faire cette opération pour chaque diviseur d produit de r facteurs premiers. On obtient une famille d'équations qui permettent, comme pour le cas des diviseurs premiers ou comme explicité dans le diagramme ci-dessus, d'éliminer successivement tous les facteurs provenant des indices k avec $\varpi(k) = r$. Ceci justifie l'hérédité du procédé.

Ce processus s'achève quand on arrive à la seule équation $x^{\Phi_n(q)} = 1$, qui est précisément celle que l'on recherchait.

□

4.3 Dimension

Une question naturelle enfin est celle de la dimension d'un tore algébrique. La proposition un peu technique suivante montre que le tore $\mathbb{T}_G$ est de dimension $\varphi(n)$, où φ désigne la fonction indicatrice d'Euler et n, rappelons-le, le cardinal de G. On suppose en premier lieu que G est cyclique. Si l'on écrit la décomposition de son cardinal en produit de facteurs premiers, on note

$$n = \prod_{i=1}^{r} p_i^{a_i} \quad \text{et} \quad G = \prod_{i=1}^{r} G_i^{a_i} \quad \text{avec } G_i \text{ cyclique et } |G_i| = p_i^{a_i}.$$

Pour tout $1 \leqslant i \leqslant r$, on note H_i sous-groupe de G_i d'ordre $|H_i| = p_i$. Soient C_i un ensemble de représentants des classes de G_i/H_i et $\Gamma_i = G_i \setminus C_i$. Soit enfin $\Gamma = \prod_i \Gamma_i$ un sous-ensemble de G.

Proposition 4.3 (Rubin & Silverberg, [43])**.**
Avec les notations ci-dessus, on a un isomorphisme entre $\mathbb{T}_G$ et $\mathbb{G}_m^\Gamma$ donné par la composition

$$\mathbb{T}_G \hookrightarrow \mathbb{G}_m^G \twoheadrightarrow \mathbb{G}_m^\Gamma.$$

Démonstration.

On commence par donner une caractérisation des éléments de $\mathbb{T}_G$ parmi tous ceux de $\mathbb{G}_m^G$.

Pour tout $\beta = (\beta_\gamma)_{\gamma \in G} \in \mathbb{G}_m^G$, on a

$$\begin{aligned} \beta \in \mathbb{T}_G &\Leftrightarrow \forall 1 \leqslant i \leqslant r, \mathrm{N}_{H_i}(\beta) = 1, \\ &\Leftrightarrow \forall 1 \leqslant i \leqslant r, \forall gH_i \in G/H_i, \prod_{\gamma \in gH_i} \beta_\gamma = 1 \quad \text{(d'après (4.3))}, \\ &\Leftrightarrow \forall 1 \leqslant i \leqslant r, \forall g \in G, \prod_{h \in H_i} \beta_{\gamma h} = 1. \end{aligned} \tag{4.6}$$

On montre l'injectivité de l'application en construisant une section de $\mathbb{G}_m^\Gamma$ dans $\mathbb{G}_m^G$. Soit $\alpha = (\alpha_\gamma)_{\gamma \in \Gamma} \in \mathbb{G}_m^\Gamma$. On va construire une image β de α de la manière suivante. Pour $\gamma \in G$, on note $\gamma = \gamma_1 \dots \gamma_r$ avec $\gamma_i \in G_i$ pour tout i. On isole maintenant les γ_i qui sont des représentants de classes de G_i/H_i. Autrement dit on pose $I_\gamma = \{1 \leqslant i \leqslant r, \gamma_i \in C_i\}$ l'ensemble des indices concernés. On ne retient de même que les H_i concernés et l'on note $D_\gamma = \prod_{i \in I_\gamma} (H_i \setminus \{1\})$. Soit alors enfin

$$\beta_\gamma = \left(\prod_{\tau \in D_\gamma} \alpha_{\gamma\tau} \right)^{(-1)^{|I_\gamma|}}. \tag{4.7}$$

Il est à noter que $\gamma\tau$ est bien dans Γ car pour tout $i \in I_\gamma$, on a $\gamma_i \in C_i$ et $\tau_i \neq 1$ (avec la notation évidente $\tau = \prod_{i \in I_\gamma} \tau_i$), donc $\gamma_i \tau_i \in \Gamma_i$.

Montrons maintenant que $(\beta_\gamma)_{\gamma \in G} \in \mathbb{T}_G$. Pour cela on va vérifier la caractérisation donnée par (4.6).

Toujours en écrivant $\gamma = \gamma_1 \dots \gamma_r$, pour tout $1 \leqslant i \leqslant r$, il y a dans C_i un unique représentant de la classe $\gamma_i H_i$. Cet élément $\gamma_i h_i \in C_i$ est tel que $i \in I_{\gamma h_i}$. Ce h_i est

même le seul élément de H_i qui permette cela ; autrement dit, si $h \in H_i \setminus \{h_i\}$, alors $I_{\gamma h_i} = I_{\gamma h} \sqcup \{i\}$. Et donc $D_{\gamma h_i} = D_{\gamma h} \times (H_i \setminus \{1\})$. L'ensemble $D_{\gamma h}$ est indépendant du choix de $h \neq h_i$ et on l'appelle $\widehat{D}$.

La stratégie est désormais d'exprimer $\beta_{\gamma h_i}$ en fonction des autres $\beta_{\gamma h}$ afin d'obtenir la relation souhaitée qui les lie. D'après l'équation (4.7), on a par définition

$$\beta_{\gamma h_i} = \left(\prod_{\tau \in D_{\gamma h_i}} \alpha_{\gamma h_i \tau} \right)^{(-1)^{|I_{\gamma h_i}|}}.$$

Mais on vient de voir que $D_{\gamma h_i} = \widehat{D} \times (H_i \setminus \{1\})$ et que $|I_{\gamma h_i}| = |I_{\gamma h}| + 1$. Donc

$$\beta_{\gamma h_i} = \left(\prod_{\tau \in \widehat{D}} \prod_{h \in (H_i \setminus \{1\})} \alpha_{\gamma h_i h \tau} \right)^{(-1)^{|I_{\gamma h}|+1}} = \left(\prod_{\tau \in \widehat{D}} \prod_{h \in (H_i \setminus \{h_i\})} \alpha_{\gamma h \tau} \right)^{(-1)^{|I_{\gamma h}|+1}}.$$

On intervertit les deux produits et l'on reconnaît l'expression de $\beta_{\gamma h}$, à une puissance de (-1) près :

$$\left(\prod_{\tau \in \widehat{D}} \alpha_{\gamma h \tau} \right)^{(-1)^{|I_{\gamma h}|+1}} = \beta_{\gamma h}^{-1}.$$

On a ainsi montré

$$\beta_{\gamma h_i} = \prod_{h \in H_i \setminus \{h_i\}} \beta_{\gamma h}^{-1},$$

c'est à dire $\prod_{h \in H_i} \beta_{\gamma h} = 1$, et ce pour tout $1 \leqslant i \leqslant r$.

Conclusion : $(\beta_\gamma)_{\gamma \in G} \in \mathbb{T}_G$, ce qui montre la surjectivité de notre morphisme.

Montrons maintenant son injectivité, ce qui se fait (avec les notations précédentes) par récurrence sur l'ordre de I_γ. Soit $(\beta_\gamma)_{\gamma \in G}$ tel que $\beta_\gamma = 1$ pour tout $\gamma \in \Gamma$, c'est-à-dire dont l'image dans $\mathbb{G}_m^G$ est l'élément unité. Soit maintenant $\gamma \in G$, on va montrer que $\beta_\gamma = 1$.

Tout d'abord si $|I_\gamma| = 0$, alors pour tout i, $\gamma_i \in \Gamma_i$ et donc $\gamma \in \Gamma$. La simple définition de β permet alors de conclure.

Procédons par récurrence et supposons le résultat établi pour γ tel que $0 \leqslant |I_\gamma| < k$. Si maintenant $|I_\gamma| = k \geqslant 1$, alors on a $\gamma = \gamma_1 \dots \gamma_r$ avec $\gamma_i \notin \Gamma_i$ pour un certain i. Comme $\beta_\gamma \in \mathbb{T}_G$, d'après la caractérisation (4.6), on a $\prod_{h \in H_i} \beta_{\gamma h} = 1$, soit encore

$$\beta_\gamma \prod_{h \in H_i \setminus \{1\}} \beta_{\gamma h} = 1.$$

Mais si $h \neq 1$, alors $\gamma_i h \in \Gamma_i$ (car $\gamma_i \notin \Gamma_i$). Donc $i \notin I_{\gamma h}$ et $|I_{\gamma h}| \leqslant |I_\gamma| - 1$. D'après l'hypothèse de récurrence, on a alors $\beta_{\gamma h} = 1$ pour tout $h \in H_i$, et donc $\beta_\gamma = 1$, ce qui montre l'injectivité de notre morphisme.

Nous avons maintenant un isomorphisme entre $\mathbb{T}_G$ et $\mathbb{G}_m^\Gamma$. La dimension de $\mathbb{T}_G$ découle du fait que $|\Gamma| = \varphi(n)$. En effet $|C_i| = p_i^{a_i-1}$, le nombre de classes dans G_i/H_i ; donc $|\Gamma_i| = |G_i| - p_i^{a_i-1}$. On retrouve alors l'expression de l'indicatrice d'Euler,

$$|\Gamma| = \prod_{i=1}^{r}(p_i^{a_i} - p_i^{a_i-1}) = \varphi(n).$$

□

4.4 Endomorphismes de tores

Un tore algébrique T de dimension s est par définition isomorphe à $\mathbb{G}_m^s$ sur une clôture algébrique. Autrement dit, c'est un tordu de $\mathbb{G}_m^s$ sur $\mathbb{F}_q$. Donc il existe un $\bar{K}$-isomorphisme $I : \mathrm{T} \to \mathbb{G}_m^s$.

On appelle $\sigma : \bar{K} \to \bar{K}$ l'automorphisme de Frobenius. Soit ${}^\sigma I : \mathrm{T} \to \mathbb{G}_m^s$ le conjugué de I sous l'action de σ. Alors la composée ${}^\sigma I I^{-1}$ constitue un endomorphisme de $\mathbb{G}_m^s$. Des arguments de cohomologie galoisienne [13] montrent qu'il existe une correspondance bijective entre les tordus de $\mathbb{G}_m^s$ et les classes de conjugaison de ${}^\sigma I I^{-1}$ dans l'anneau des endomorphismes de $\mathbb{G}_m^s$.

Un endomorphisme de $\mathbb{G}_m^s$ est donné par

$$\mathfrak{a} : (g_1, \ldots, g_s) \mapsto \left(\prod_{1 \leqslant j \leqslant s} g_j^{a_{i,j}} \right)_{1 \leqslant i \leqslant s}.$$

On peut caractériser cette application par la matrice des exposants $(a_{i,j})_{1 \leqslant i,j \leqslant s}$. C'est une matrice carrée de taille s à coefficients entiers et elle correspond à un endomorphisme du $\mathbb{Z}$-module des caractères de $\mathbb{G}_m^s$. Le morphisme $\mathfrak{a}$ est inversible si et seulement si la matrice $(a_{i,j})_{1 \leqslant i,j \leqslant s}$ l'est. Donc le groupe des automorphismes de $\mathbb{G}_m^s$ est $\mathrm{GL}_s(\mathbb{Z})$.

Dans le cas particulier de la restriction de Weil $\mathrm{Res}_{\mathbb{F}_{q^n}/\mathbb{F}_q} \mathbb{G}_m$, on obtient ${}^\sigma I I^{-1} = \omega$ où ω désigne la permutation circulaire des coordonnées,

$$\omega(g_1, g_2, \ldots, g_n) = (g_n, g_1, \ldots, g_{n-1}).$$

Cherchons l'anneau des $\mathbb{F}_q$-endomorphismes de ce tore. À chaque endomorphisme ε de $\mathbb{G}_m^n$, on associe un endomorphisme de $\mathrm{Res}_{\mathbb{F}_{q^n}/\mathbb{F}_q} \mathbb{G}_m$ tel que le diagramme suivant commute.

$$\begin{array}{ccc} \mathrm{Res}_{\mathbb{F}_{q^n}/\mathbb{F}_q} \mathbb{G}_m & \xrightarrow{I^{-1}\varepsilon I} & \mathrm{Res}_{\mathbb{F}_{q^n}/\mathbb{F}_q} \mathbb{G}_m \\ I \downarrow \sim & & I \downarrow \sim \\ \mathbb{G}_m^n & \xrightarrow{\varepsilon} & \mathbb{G}_m^n \end{array}$$

L'endomorphisme $I^{-1}\varepsilon I$ est défini sur $\mathbb{F}_q$ si et seulement s'il est invariant sous l'action de σ, c'est-à-dire ${}^{\sigma}I^{-1}\varepsilon^{\sigma}I = I^{-1}\varepsilon I$. Donc ε induit un $\mathbb{F}_q$-endomorphisme de $\mathrm{Res}_{\mathbb{F}_{q^n}/\mathbb{F}_q}\mathbb{G}_m$ si et seulement si $\omega\varepsilon = \varepsilon\omega$.

Ce que l'on a mis en évidence est en fait une correspondance fonctorielle entre la catégorie des tores algébriques sur les corps finis et la catégorie des $\mathbb{Z}$-modules avec un automorphisme. Ainsi par exemple le tore $\mathrm{Res}_{\mathbb{F}_{q^d}/\mathbb{F}_q}\mathbb{G}_m$ correspond à $\mathbb{Z}[X]/(X^q-1)$ avec l'automorphisme ω qui n'est autre que la multiplication par X.

L'identité $X^n - 1 = \prod_{d|n}\Phi_d(X)$ induit l'isomorphisme

$$\mathbb{Q}[X]/(X^n-1) \simeq \prod_{d|n}\mathbb{Q}[X]/\Phi_d(X).$$

On n'a pas pour autant nécessairement un isomorphisme entre $\mathbb{Z}[X]/(X^n-1)$ et $\prod_{d|n}\mathbb{Z}[X]/\Phi_d(X)$. Cependant on peut écrire

$$(\mathbb{Z}[1/n])[X]/(X^n-1) \simeq \prod_{d|n}(\mathbb{Z}[1/n])[X]/\Phi_d(X).$$

Il y a donc deux isogénies entre les groupes algébriques $\mathrm{Res}_{\mathbb{F}_{q^n}/\mathbb{F}_q}\mathbb{G}_m$ et $\prod_{d|n}\mathrm{T}_{\mathbb{F}_{q^d}}$ telles que leur composition est la multiplication par une puissance de n. Ceci explique notamment la présence du dénominateur égal à n dans les coefficients $w_{d,e}$ qui apparaissent dans l'algorithme de calcul de l'application θ (voir paragraphe 3.2.3).

Les mathématiques ne sont pas une moindre immensité que la mer.

Victor Hugo

CHAPITRE 5

COMPRESSION EFFICACE DANS LES TORES ALGÉBRIQUES

ENFIN DANS ce chapitre on présente comment les résultats arithmétiques du chapitre 2 vont permettre d'améliorer le temps de calcul de l'algorithme 1. Ceci est fondé sur une nouvelle représentation des extensions de corps, due à Couveignes et Lercier, et dont la construction est présentée dans le paragraphe 5.1. Puis la partie 5.2 montre comment on adapte le paramétrage de van Dijk et Woodruff présenté dans le paragraphe 3.2.2 pour rendre son exécution asymptotiquement plus efficace.

5.1 Bases elliptiques

L'amélioration de la complexité de l'algorithme passe par une nouvelle représentation des extensions de corps. Couveignes et Lercier ont récemment construit un nouveau type de bases normales, appelées bases normales elliptiques [14]. Contrairement aux précédentes constructions, parmi lesquelles on trouve les bases normales gaussiennes de type 1 ou 2, les bases normales elliptiques sont disponibles pour toutes les extensions de $\mathbb{F}_q$. De plus elles permettent une arithmétique peu coûteuse sur $\mathbb{F}_{q^n}$ et dans le cadre des tores algébriques, cela va se traduire par le gain d'un facteur $\log q$ dans la complexité de l'encodage.

Soit $E/\mathbb{F}_q$ une courbe elliptique donnée dans sa forme de Weierstrass par

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

On pose $x = X/Z$ et $y = Y/Z$. Si A est un point de $E(\mathbb{F}_q)$, on note $\tau_A : E \to E$ la translation par A. On pose $x_A = x \circ \tau_{-A}$ et $y_A = y \circ \tau_{-A}$ les compositions respectives

de x et y par la translation par $-A$. Maintenant si A et B sont deux points distincts de $E(\mathbb{F}_q)$, on définit la fonction $u_{A,B} \in \mathbb{F}_q(E)$ par

$$u_{A,B} = \frac{y_A - y(A-B)}{x_A - x(A-B)}.$$

Elle est de degré 2 et a deux pôles simples en A et B. Avec C un troisième point de $E(\mathbb{F}_q)$ distinct de A et B, on pose

$$\Gamma(A,B,C) = u_{A,B}(C) = \frac{y(C-A) - y(A-B)}{x(C-A) - x(A-B)}\,.$$

On peut démontrer les identités suivantes avec des développements de Taylor aux pôles :

$$\left\{\begin{array}{rcl} \Gamma(A,B,C) & = & \Gamma(B,C,A) = -\Gamma(B,A,C) - a_1, \\ & = & -\Gamma(-A,-B,-C) - a_1\,, \\ u_{A,B} + u_{B,C} + u_{C,A} & = & \Gamma(A,B,C) - a_1\,, \\ u_{A,B}u_{A,C} & = & x_A + \Gamma(A,B,C)u_{A,C} + \Gamma(A,C,B)u_{A,B} \\ & & +a_2 + x_A(B) + x_A(C)\,, \\ u_{A,B}^2 & = & x_A + x_B - a_1 u_{A,B} + x_A(B) + a_2\,. \end{array}\right. \tag{5.1}$$

Supposons que $E(\mathbb{F}_q)$ contienne un sous-groupe cyclique $\mathcal{T}$ d'ordre n et soit $I : E \to E'$ l'isogénie de degré n dont le noyau est $\mathcal{T}$. Alors le quotient $E'(\mathbb{F}_q)/I(E(\mathbb{F}_q))$ est isomorphe à $\mathcal{T}$.

Soit A un point de $E'(\mathbb{F}_q)$ tel que $A \bmod I(E(\mathbb{F}_q))$ engendre ce quotient. La fibre $\mathcal{P} = I^{-1}(A) = \sum_{T\in\mathcal{T}}[B+T]$ est un diviseur irréductible. Les n points géométriques au-dessus de A sont définis sur une extension de $\mathbb{F}_q$ de degré n (et permutés par l'action de Galois), c'est-à-dire que $\mathbb{F}_{q^n}$ est l'extension résiduelle de $\mathbb{F}_q(E)$ en $\mathcal{P}$.

Pour tout $k \in \mathbb{Z}/n\mathbb{Z}$, on pose $u_k = \mathfrak{a}u_{kT,(k+1)T} + \mathfrak{b}$. ($\mathfrak{a}$ et $\mathfrak{b}$ étant des constantes choisies telles que $\sum u_k = 1$). Alors le système $\Theta = (u_k(B))_{k\in\mathbb{Z}/n\mathbb{Z}}$ est une base normale de $\mathbb{F}_{q^n}$ sur $\mathbb{F}_q$.

De plus, on peut multiplier deux éléments donnés dans une base normale elliptique en complexité quasi-linéaire. Cet algorithme est principalement basé sur la série d'équations (5.1). Il repose sur un principe d'évaluation puis d'interpolation en d points $R + kT$, avec $R \in E(\mathbb{F}_q) - E[n]$.

Finalement on a le théorème suivant.

Theorème 5.1 (Couveignes & Lercier, [14])**.**
À chaque couple (q,n) avec q une puissance d'un nombre premier et $n \geqslant 2$ entier tel que $n_q \leqslant \sqrt{q}$, on peut associer une base normale $\Theta(q,n)$ de l'extension de $\mathbb{F}_q$ de degré n telle que :

- *il existe un algorithme qui multiplie deux éléments de $\Theta(q,n)$ au coût de $n^{1+o(1)}\log^{1+o(1)} q$ opérations élémentaires.*

Ici n_q est tel que

- $v_\ell(n_q) = v_\ell(n)$ si ℓ est premier avec $q-1$, $v_\ell(n_q) = 0$ si $v_\ell(n) = 0$,
- $v_\ell(n_q) = \max(2v_\ell(q-1)+1, 2v_\ell(n))$ si ℓ divise à la fois $q-1$ et n.

On peut aisément étendre ce résultat à tous q et n (voir [14]).

Dans les applications cryptographiques, les corps finis sont en général de taille trop petite pour tirer parti d'algorithmes de multiplication du type de la transformée de Fourier rapide. Cependant on peut lire dans [14] que les multiplications se font dans une base normale elliptique au prix de cinq convolutions de taille n sur $\mathbb{F}_q$. On peut même économiser certaines d'entre elles du fait de redondances dans les élévations au carré ou les multiplications par une constante. Finalement la complexité moyenne totale d'une exponentiation de λ bits est de $3/2 \times 4\ \lambda n^2$ multiplications sur $\mathbb{F}_q$ pour des exposants de λ bits. En comparaison, elle est de $3/2 \times k^2\ \lambda n^2$ pour les corps finis avec une base normale gaussienne de type k petit.

Couveignes et Lercier exhibent également des bases normales non-elliptiques, dans lesquelles le calcul de l'endomorphisme de Frobenius requiert $n-1$ multiplications sur $\mathbb{F}_q$ et la multiplication de deux éléments environ $2,6\,n^2$ multiplications sur $\mathbb{F}_q$, pour un coût de stockage de $n^2/12$ (*cf.* [14, lemmes 2 et 3]). On atteint donc une complexité moyenne totale de $3/2 \times 2.6\ \lambda n^2$ multiplications sur $\mathbb{F}_q$ pour des exposants de λ bits.

En résumé on a le tableau comparatif suivant (figure 5.1) qui recense les complexités théorique et pratique de deux opérations de base en fonction des bases choisies pour représenter l'extension $\mathbb{F}_{q^n}$ de $\mathbb{F}_q$: gaussienne de type k, elliptique ou normale elliptique

Complexité \ Base		gaussienne de type k	elliptique	normale elliptique
Frobenius	théo.	$kn \log q$	$(n-1)\log q$	$n \log q$
	asym.	$kn^{1+o(1)}$	$n^{1+o(1)} \log^{1+o(1)} q$	$n^{1+o(1)}$
multiplication	théo.	$k^2 n^2 \log^2 q$	$2{,}6 n^2 \log^2 q$	$4n^2 \log^2 q$
	asym.	$(kn)^{1+o(1)} \log^{1+o(1)} q$	$2{,}6 n^2 \log^{1+o(1)} \log^{1+o(1)}$	$n^{1+o(1)} \log^{1+o(1)} q$

FIGURE 5.1 – Comparaison des complexités d'opérations de base en fonction du type de base choisi.

5.2 Paramétrage effectif

Avec les notations du paragraphe 3.2.2, on s'attache maintenant au cas $U_d = 1$ pour tout $d \,|\, n$. Ce n'est pas une trop grande restriction, du moins à des fins cryptographiques. En effet le lemme 5.1 du paragraphe 5.2.1 suivant montre que

pour une infinité de valeurs de n, on peut trouver une infinité de valeurs de q qui le permettent.

Tout l'enjeu de ce travail est que la plupart des exponentiations à effectuer dans l'algorithme 1 mettent en jeu des puissances dont la décomposition en base q est creuse. C'est pourquoi on s'intéresse pour l'écriture de $\mathbb{F}_{q^n}$ sur $\mathbb{F}_q$ à une base normale, donc de la forme $(\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}})$ plutôt qu'à une base polynomiale $(1, \alpha, \ldots, \alpha^{n-1})$. En effet, avec le choix d'une base normale, les puissances q sont gratuites car elles consistent en une simple permutation circulaire des coordonnées dans cette base. Comme on cherche également à multiplier les éléments de $\mathbb{F}_{q^n}$ en temps quasi-linéaire, on se tourne tout naturellement vers les bases normales elliptiques présentées dans la partie 5.1.

5.2.1 Restrictions sur n et q

On démontre le résultat suivant pour des entiers n sans facteur carré.

Lemme 5.1.
Pour une infinité d'entiers n sans facteur carré, il existe une infinité de valeurs de q telles que $U_d = 1$ pour tout $d \mid n$.

Démonstration.
On déduit de l'équation (3.2) que

$$U_d = 1 \Leftrightarrow \forall e \mid d,\ \forall f \mid d\ e \neq f,\ \operatorname{pgcd}(\Phi_e(q), \Phi_f(q)) = 1\,. \tag{5.2}$$

Cette condition est toujours satisfaite si $\operatorname{Res}(\Phi_e, \Phi_f) = 1$ et ceci est équivalent à la condition $f \neq e\,p^i$ avec p premier et $i \geqslant 1$, comme on l'a vu au théorème 1.1.

Il reste à vérifier que lorsque $f = e\,p^i$, il existe des entiers q tels que l'équation (5.2) soit vérifiée. Comme on a supposé n sans facteur carré, les seuls cas sont les f de la forme $f = ep$, avec p premier.

Cas $e = 1$. Le diviseur f vaut alors p premier, et $\operatorname{Res}(\Phi_1, \Phi_f) = f$. Pour avoir $\operatorname{pgcd}(\Phi_e(q), \Phi_f(q)) = 1$, q ne doit pas être une racine commune de Φ_e et Φ_f modulo f. Autrement dit, il faut que $q \not\equiv 1 \bmod f$.

Cas $e > 1$. Alors le diviseur f vaut pe où p est premier. Comme e est sans facteur carré, on sait d'après l'équation (1.5) de la proposition 1.1 que $\operatorname{Res}(\Phi_e, \Phi_{pe}) = p^{\varphi(e)}$. Donc q ne doit pas être une racine commune de Φ_e et Φ_{pe} modulo p. Modulo p, Φ_e se décompose en produit de polynômes irréductibles de même degré, et ce degré est égal à $p \bmod e$ (*cf.* [36]). En d'autres termes, Φ_e et Φ_{pe} ne peuvent avoir de racine commune que lorsque $p \equiv 1 \bmod e$. Dans ce cas, q ne doit pas être une des $\varphi(e)$ racines de Φ_e modulo p.

Les restrictions ci-dessus laissent pour q une infinité de possibilités, du moins pour une infinité de valeurs de n. Par exemple, posons p un nombre premier impair

et $r \equiv 2 \bmod p$. Soit $n = pr$ et q tel que $q \not\equiv 1 \bmod p$ et $q \not\equiv 1 \bmod r$. En outre, comme $r \not\equiv 1 \bmod p$, toutes les conditions ci-dessus sont satisfaites. On a ainsi une famille infinie de nombres q qui conviennent pour chaque n, et une infinité de valeurs possibles pour n lui-même.

□

Ce lemme démontre l'existence d'une infinité de paramètres acceptables pour la construction visée. Cependant on peut encore se demander si ces paramètres sont adaptés aux applications cryptographiques. La génération pratique de bons paramètres en termes de sécurité cryptographique nécessite un compromis entre la taille du sous-groupe utilisé et la complexité sous-exponentielle des algorithmes de crible connus pour le calcul du logarithme discret dans les corps finis (*number field sieve* ou *function field sieve*). Pour plus de détails sur ces études on peut se référer à [30] ou [28]. Ce problème est lié à la construction de paramètres adaptés aux couplages (dits aussi *pairing-friendly*) dont il est notamment question dans [24].

5.2.2 L'adaptation du paramétrage de van Dijk et Woodruff

On vient de voir que l'on peut, sans trop de perte de généralité, se placer dans la situation confortable où $U_d = 1$ pour tout $d \,|\, n$. Dans ce cas le procédé d'encodage décrit par van Dijk et Woodruff peut être légèrement simplifié.

Avec les notations de la partie 3.2.2, on a déjà vu que pour tout $e \,|\, d$, $y_{d,e} = \Phi_e(q)$ et $z_{d,e} = 1$. Dans ce cas, les groupes $\mathbb{Z}/y_{d,e}\mathbb{Z}$ sont les tores $\mathrm{T}_e(\mathbb{F}_q)$ et de plus $u_{d,e} = 1$ et $v_{d,e} = 0$. Donc l'essentiel de l'algorithme 1 est réduit aux deux phases principales : la décomposition $\mathbb{F}_{q^d}^\times \to \prod_{e \,|\, d} \mathrm{T}_e(\mathbb{F}_q)$ pour tout diviseur d de n tel que $\mu(n/d) = -1$ du côté gauche de l'application, et la reconstruction $\prod_{e \,|\, d} \mathrm{T}_e(\mathbb{F}_q) \to \mathbb{F}_{q^d}^\times$ pour tout diviseur d de n tel que $\mu(n/d) = 1$ du côté droit.

Maintenant il faut évaluer l'économie réalisée par l'utilisation d'une base normale elliptique. Essentiellement, chaque exponentiation faisant intervenir une puissance de q se traduit par une permutation circulaire de la base, tandis que l'on peut toujours effectuer des multiplications en temps quasi-linéaire. On gagne ainsi un facteur $\log q$ pour chaque exponentiation de ce type. Il est aisé de constater que les exposants apparaissant dans la première phase de décomposition ont une décomposition en base q agréable. En effet ce sont des produits d'évaluations en q de polynômes cyclotomiques. Mais la phase de reconstruction est plus délicate car on y trouve les coefficients de Bézout $w_{d,e}$ qui n'ont pas *a priori* les mêmes propriétés. En fait on préfère calculer directement les polynômes $W_{d,e}$ tels que

$$\sum_{e \,|\, d} \frac{X^d - 1}{\Phi_e(X)} W_{d,e}(X) = 1.$$

Ils vérifient $w_{d,e} = W_{d,e}(q) \bmod \Phi_e(q)$.

Contrairement aux polynômes cyclotomiques, ces polynômes ne sont pas à coefficients entiers. En revanche, pour n sans facteur carré, et donc pour ses diviseurs d

sans facteur carré également, tous les coefficients de ces polynômes sont rationnels et admettent d pour dénominateur commun. Plus précisément, on a

$$W_{d,e}(X) = \prod_{f \,|\, d, f \neq e} \Phi_f(X)^{-1} \bmod \Phi_e(X)\,. \tag{5.3}$$

Conséquemment, on peut observer en premier lieu que $\Phi_f(X)^{-1} \bmod \Phi_e(X)$ a des coefficients entiers si et seulement si $f \neq e\,p^i$ avec p premier et $i \geqslant 1$, car $\mathrm{Res}(\Phi_e, \Phi_f) = 1$ dans ce cas (voir la démonstration du lemme 5.1). D'autre part, lorsque $f = e\,p^i$, les coefficients de $\Phi_f(X)^{-1} \bmod \Phi_e(X)$ ont un dénominateur commun égal à f. L'équation (5.3) et le fait que d soit sans facteur carré nous permettent de dire que les coefficients de $W_{d,e}(X)$ admettent exactement d pour dénominateur commun.

On a observé en outre que les dénominateurs des polynômes $W_{d,e}$ ont également des petits coefficients en valeur absolue (voir 5.2.3 pour une étude un peu plus détaillée dans le cas où $n = pr$). Par conséquent, on se limite aux valeurs de q qui sont des puissances d'un nombre premier et telles que n soit inversible modulo $q^n - 1$. L'algorithme 2 présente une variante de θ dans le cas où $U_d = 1$ pour tout $d|n$.

Algorithme 2 : Calcul de θ dans le cas $U_d = 1$.

Entrées : $x \in \mathrm{T}_n(\mathbb{F}_q)$ et $x_d \in \mathbb{F}_{q^d}^\times$ pour tout $d \,|\, n$ tel que $\mu(n/d) = -1$.

Sorties : $x_d \in \mathbb{F}_{q^d}^\times$ pour tout $d \,|\, n$ tel que $\mu(n/d) = 1$.

pour chaque $d \,|\, n$ tel que $\mu(n/d) = -1$ **faire**
    Calculer $x_d \mapsto (Z_{\rho_e(d),e})_{e \,|\, d}$ avec $Z_{\rho_e(d),e} = x_d^{(q^d-1)/\Phi_e(q)}$.
fin
Poser $Z_{n,n} = x$.
pour chaque $d \,|\, n$ tel que $\mu(n/d) = +1$ **faire**
    Calculer $x_d = \prod_{\substack{\rho_e(d')=d, e \,|\, d \\ e \neq d}} Z_{d',e}^{W_{d,e}(q)} \in \mathbb{F}_{q^d}^\times$.
fin

Notons que les identifications nécessaires pour voir $\mathbb{F}_{q^d}$ comme sous-corps de $\mathbb{F}_{q^n}$ sont aisées. En fait, un élément de $\mathbb{F}_{q^d}$ admet un ensemble périodique de coordonnées dans toute base normale de $\mathbb{F}_{q^n}$. Ainsi pour la compression il s'agit simplement de tronquer les d premières composantes. L'expansion, quant à elle, consiste en la concaténation de n/d copies d'un d-uplet d'éléments de $\mathbb{F}_q$. Les coûts de ces opérations sont négligeables.

Avant d'examiner en détail dans le paragraphe 5.2.3 le cas où $n = pr$ est un produit de deux nombres premiers distincts, et de dire quelques mots du cas général

au paragraphe 5.2.6, on s'intéresse à nouveau au cas particulier $n = 15$ afin de comparer les résultats avec la partie 3.2.2.

Exemple. Avec les notations de la figure 3.2, les coûts sont les suivants.

Phase (1). Les élévations aux puissances $\Phi_3(q) = q^2 + q + 1$ et $\Phi_5(q) = q^4 + q^3 + q^2 + q + 1$ coûtent respectivement 2 et 4 multiplications car l'élévation à la puissance q est gratuite (c'est une simple permutation circulaire des éléments de la base). L'élévation à la puissance $q-1$ coûte une inversion, que l'on réalise en temps linéaire.

Phase (2). Négligeable.

Phase (3). Reprenons les expressions des coefficients r_e. Par exemple $r_{15} = q^7 - 3\,q^5 + 4\,q^4 - 5\,q^3 + 7\,q - 8$. Élever à cette puissance requiert 6×3 multiplications pour les coefficients (6 coefficients de taille au plus 2^3) et 6 multiplications pour additionner les sept monômes. Le même calcul pour chaque r_e donne le coût total de la phase (3) : $3 + ((0) + (1 \times 1 + 1) + (2 \times 2 + 2) + (6 \times 3 + 6)) = 35$ multiplications et 3 inversions.

Enfin le calcul de $1/n$ dans T_{15} devrait nécessiter $8 \times (3/2) \log q$. Cependant pour un q bien choisi, le lemme 5.2 ci-après nous permet le calcul de $1/n \bmod q^n - 1$ en $2 \times (3/2) \log q + 6$ multiplications.

Cela représente au total une économie substantielle si l'on compare avec les résultats mentionnés dans le chapitre 3.2.4 sans l'utilisation des bases elliptiques. On avait un coût moyen d'environ $9 \log q$ qui tombe ici à $3 \log q$ multiplications, en plus d'une quantité fixe d'une cinquantaine de multiplications. Le plus intéressant est que l'on économise sur le coefficient de $\log q$, donc sur la complexité asymptotique.

5.2.3 Cas $n = pr$: exécution

Dans le cas où $n = pr$ avec p et r deux nombres premiers distincts, la situation est très similaire à l'exemple $n = 15$ (voir la figure 3.2).

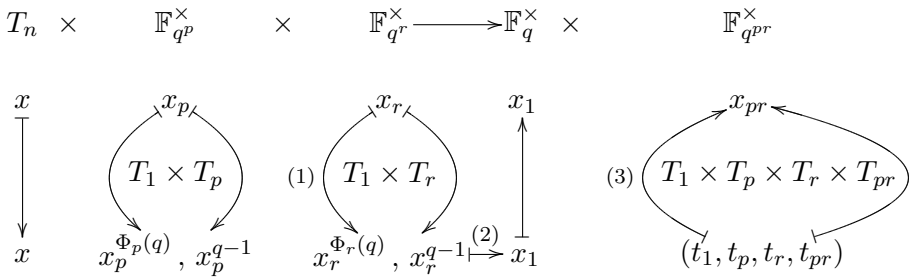

FIGURE 5.2 – La bijection θ pour $n = pr$ et $U_1 = U_p = U_r = U_{pr} = 1$.

Nous allons avant tout donner quelques précisions sur les constructions des différentes applications mises en jeu. Pour cela, on utilisera plusieurs fois le principe suivant. Étant donné le résultant de deux polynômes P et Q, on sait qu'il existe U et V tels que

$$U(X)P(X) + V(X)Q(X) = \mathrm{Res}(P, Q).$$

En évaluant cette égalité en un certain entier, on obtient une relation de type Bézout qui montre que $\mathrm{pgcd}(P(q), Q(q))$ divise $\mathrm{Res}(P, Q)$. En particulier, en utilisant le théorème 1.1, on a une relation liant les évaluations en q de deux polynômes cyclotomiques.

$$U(q)\Phi_n(q) + V(q)\Phi_m(q) = \mathrm{Res}(\Phi_n, \Phi_m).$$

Considérons d'abord l'exemple simple de $\mathbb{F}_{q^p}^\times$. Alors on a les deux applications normes suivantes.

$$\begin{array}{rcl} \mathbb{F}_{q^p}^\times & \to & T_1, \\ x_p & \mapsto & x_p^{\Phi_p(q)} \end{array} \quad \text{et} \quad \begin{array}{rcl} \mathbb{F}_{q^p}^\times & \to & T_p, \\ x_p & \mapsto & x_p^{q-1}. \end{array}$$

De plus, comme $\mathrm{Res}(\Phi_1, \Phi_p) = p$, on obtient une équation reliant $q-1$ et $\Phi_p(q)$, à savoir

$$\Phi_p(q)u_1 + (q-1)u_p = p,$$

où u_1 et u_p sont des nombres entiers. On peut également construire une application réciproque

$$\begin{array}{rcl} T_1 \times T_p & \to & \mathbb{F}_{q^p}^\times, \\ (t_1, t_p) & \mapsto & t_1^{u_1} t_p^{u_p}. \end{array}$$

Elle est telle que sa composition avec le produit des deux normes ci-dessus donne la multiplication par p.

On a une construction similaire pour $\mathbb{F}_{p^r}^\times$:

$$\begin{array}{rcl} \mathbb{F}_{q^r}^\times & \to & T_1 \times T_r, \\ x_r & \mapsto & (x_r^{\Phi_r(q)}, x_r^{q-1}), \\ t_1^{v_1} t_r^{v_r} & \leftarrow\!\shortmid & (t_1, t_r). \end{array}$$

avec la relation $\Phi_r(q)v_1 + (q-1)v_r = r$.

On examine maintenant le cas de $\mathbb{F}_{q^{pr}}^\times$ et ses quatre sous-groupes d'ordres $q-1$, $\Phi_p(q)$, $\Phi_r(q)$ et $\Phi_{pr}(q)$ que sont respectivement T_1, T_p, T_r et T_{pr}.

On peut construire l'application suivante dont les composantes sont les quatre normes usuelles.

$$\begin{array}{rcl} \mathbb{F}_{q^{pr}}^\times & \to & T_1 \times T_p \times T_r \times T_{pr}, \\ x_{pr} & \mapsto & (x_{pr}^{U_1(q)}, x_{pr}^{U_p(q)}, x_{pr}^{U_r(q)}, x_{pr}^{U_{pr}(q)}), \end{array}$$

avec $U_k(X) = \frac{X^{pr}-1}{\Phi_k(X)}$.

On cherche maintenant une réciproque à cette fonction. Suivant l'exemple précédent, dès que l'on a une relation de type Bézout,

$$U_1V_1 + U_pV_p + U_rV_r + U_{pr}V_{pr} = pr,$$

on peut construire une application

$$\begin{array}{rcl} T_1 \times T_p \times T_r \times T_{pr} & \to & \mathbb{F}_{q^{pr}}^{\times}, \\ (t_1, t_p, t_r, t_{pr}) & \mapsto & t_1^{V_1(q)} t_p^{V_p(q)} t_r^{V_r(q)} t_{pr}^{V_{pr}(q)}. \end{array}$$

De plus elle est telle que la composition des deux applications précédentes donne la multiplication par pr sur $\mathbb{F}_{q^{pr}}^{\times}$.

En pratique, on obtient une telle relation en deux étapes. On écrit tout d'abord deux relations de Bézout, entre Φ_{pr} et Φ_1 d'une part et entre Φ_p et Φ_r d'autre part. Donc la première étape consiste en deux applications,

$$\begin{array}{rcll} T_1 \times T_{pr} & \xrightarrow{\sim} & G_1 \subset \mathbb{F}_{q^{pr}}^{\times}, & \text{où } \Phi_{pr}(q)u_1 + \Phi_1(q)u_{pr} = 1, \\ (t_1, t_{pr}) & \mapsto & y_1 = t_1^{u_1} t_{pr}^{u_{pr}}, & \end{array}$$

et

$$\begin{array}{rcll} T_p \times T_r & \xrightarrow{\sim} & G_2 \subset \mathbb{F}_{q^{pr}}^{\times}, & \text{où } \Phi_r(q)u_p + \Phi_p(q)u_r = 1. \\ (t_p, t_r) & \mapsto & y_2 = t_p^{u_p} t_r^{u_r}, & \end{array}$$

Ensuite on écrit une relation de type Bézout qui lie $\Phi_p\Phi_r$ et $\Phi_1\Phi_{pr}$. Le théorème 2.1 indique que $(\Phi_p\Phi_r)^{-1}$ fait apparaître un facteur $1/pr$ modulo Φ_1 et Φ_{pr}. On peut recombiner cela en la relation suivante : il existe des polynômes V_1 et V_2 à coefficients entiers tels que

$$(\Phi_p\Phi_r)V_1 + (\Phi_1\Phi_{pr})V_2 = pr.$$

Cette égalité permet d'apparier $y_1 \in G_1$ et $y_2 \in G_2$ pour former un élément de $\mathbb{F}_{q^{pr}}$ de la manière suivante :

$$\begin{array}{rcl} G_1 \times G_2 & \to & \mathbb{F}_{q^{pr}}^{\times}, \\ (y_1, y_2) & \mapsto & y_1^{V_1(q)} y_2^{V_2(q)}. \end{array}$$

En appelant $v_1 = V_1(q)$ et $v_2 = V_2(q)$, on obtient le diagramme de la figure 5.3.

5.2.4 Cas $n = pr$: complexité

On peut maintenant examiner la complexité de l'application θ. Avec les notations de la figure 5.2, le coût de la phase (1) provient des exponentiations aux puissances $\Phi_p(q)$ et $\Phi_r(q)$, c'est à dire p et r multiplications puisque l'élévation à la puissance q est gratuite. Cela revient à $n^{2+o(1)} \log^{1+o(1)} q$ opérations élémentaires. L'élévation à

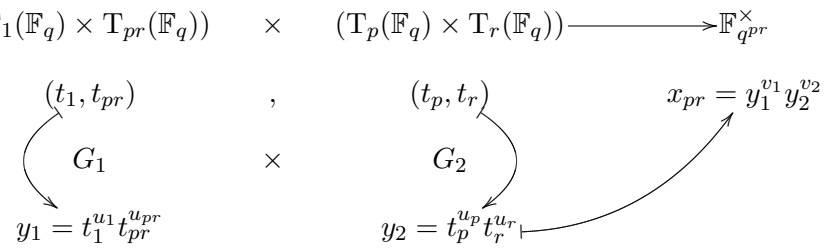

FIGURE 5.3 – Phase de reconstruction dans le cas $n = pr$.

la puissance $q-1$ coûte une inversion, qui peut également se faire asymptotiquement en temps quasi-linéaire.

Voici maintenant le calcul du coût de la phase (3) dont on vient de détailler l'exécution (figure 5.3). Les puissances qui apparaissent dans la première étape, appelées u_1, u_p, u_r, et u_{pr} sont les évaluations en q de $\Phi_{pr}^{-1} \bmod \Phi_1$, ${\Phi_r}^{-1} \bmod \Phi_p$, ${\Phi_p}^{-1} \bmod \Phi_r$ et ${\Phi_1}^{-1} \bmod \Phi_{pr}$, tous à coefficients égaux à 0 ou ± 1.

Les puissances v_1 et v_2 apparaissant dans la seconde étape sont les évaluations respectives en q de $\Phi_p^{-1}\Phi_r^{-1} \bmod \Phi_1\Phi_{pr}$ et $\Phi_1^{-1}\Phi_{pr}^{-1} \bmod \Phi_p\Phi_r$. Pour les calculer, il est nécessaire de connaître les huit inverses suivants Φ_p^{-1} modulo Φ_1 et Φ_{pr}, Φ_r^{-1} modulo Φ_1 et Φ_{pr}, Φ_1^{-1} modulo Φ_p et Φ_r, et enfin Φ_{pr}^{-1} modulo Φ_p et Φ_r. Ensuite pour calculer des inverses modulo un produit de deux polynômes cyclotomiques, on utilise le théorème chinois. Si $\Phi = A \bmod \Phi_{pr}$ et $\Phi = B \bmod \Phi_1$, alors

$$\Phi = \left(\frac{\Phi_1}{\Phi_1 \bmod \Phi_{pr}} A + \frac{\Phi_{pr}}{\Phi_{pr} \bmod \Phi_1} B \right) \bmod \Phi_1\Phi_{pr}\,.$$

On a bien évidemment une formule similaire pour l'autre inverse. Tout ceci donne les bornes suivantes sur les coefficients (en valeur absolue),

$$\begin{aligned}\Phi_p^{-1} \bmod \Phi_1\Phi_{pr} = [\ & \underbrace{\Phi_1}_{\text{au plus 1}} \underbrace{(\Phi_1^{-1} \bmod \Phi_{pr})}_{\text{au plus 1}} \underbrace{(\Phi_p^{-1} \bmod \Phi_{pr})}_{\text{au plus 1}} \\ & + \underbrace{\Phi_{pr}}_{\text{au plus 1}} \underbrace{(\Phi_{pr}^{-1} \bmod \Phi_1)}_{=1} \underbrace{(\Phi_p^{-1} \bmod \Phi_1)}_{=1/p}] \bmod \Phi_1\Phi_{pr}. \quad (5.4)\end{aligned}$$

On a aussi une borne similaire pour $\Phi_r^{-1} \bmod \Phi_1\Phi_{pr}$. Il suffit d'inverser les rôles de p et r dans l'équation (5.4).

Finalement, v_1 est le produit de Φ_p^{-1} et Φ_r^{-1} modulo $\Phi_1\Phi_{pr}$. Les puissances mises en jeu dans la dernière étape sont v_1 et v_2. Les coefficients de leurs décompositions en base q sont grossièrement majorées par n^5 en valeur absolue. Ceci ajoute à la complexité un facteur $n^{o(1)}$ qui est négligeable.

Il reste l'élévation à la puissance $1/n$, qui peut se faire de manière directe, mais en $n^{2+o(1)} \log^{2+o(1)} q$ opérations élémentaires. Cependant ce coût peut être réduit

au prix d'une hypothèse supplémentaire sur q. En effet on peut obtenir une forme agréable de l'inversion de n modulo $q^n - 1$.

Lemme 5.2.
Soient n un nombre impair et q une puissance d'un nombre premier telle que n divise $q+1$. On note $k = (n-1)/2$. Alors

$$1/n \bmod (q^n - 1) = \mu_0 + \mu_1\, q + \mu_0\, q^2 + \cdots + \mu_1\, q^{n-2} + \mu_0\, q^{n-1}\,, \qquad (5.5)$$

où

$$\mu_0 = \frac{k(q-1)+q}{n} \text{ et } \mu_1 = \frac{k(q-1)-1}{n}\,.$$

Démonstration.

On remarque que l'expression proposée pour l'inverse s'écrit

$$\begin{aligned} A := (\mu_0 + \mu_1 q)(1 + q^2 + \ldots + q^{n-1}) - \mu_1 q^n &= (\mu_0 + \mu_1 q)\frac{1-q^{n+1}}{1-q^2} - \mu_1 q^n, \\ &= \frac{q^n(\mu_0 q + \mu_1) - (\mu_0 + \mu_1 q)}{q^2 - 1}. \end{aligned}$$

Avec les μ_0 et μ_1 choisis comme dans l'énoncé du lemme, on a $n(\mu_0 q + \mu_1) = (k+1)(q^2-1)$ et $n(\mu_0 + \mu_1 q) = k(q^2-1)$. Ainsi, on simplifie l'expression

$$nA = (q^n - 1)(k+1) + 1 \equiv 1 \bmod (q^n - 1).$$

□

Élever des éléments $\mathbb{F}_{q^n}$ à la puissance $1/n$ avec $1/n$ donné par l'équation (5.5) requiert $n^{1+o(1)} \log^{2+o(1)} q$ opérations élémentaires si l'on utilise les bases normales. Finalement on a le théorème suivant.

Theorème 5.2.
Soient $p \neq r$ deux nombres premiers impairs et $q \equiv -1 \bmod (pr)$. Alors il existe un algorithme de complexité $n^{2+o(1)} \log^{1+o(1)} q + n^{1+o(1)} \log^{2+o(1)} q$, donné par l'algorithme 2, qui prend en entrée des éléments de $T_n \times \mathbb{F}_{q^p}^{\times} \times \mathbb{F}_{q^r}^{\times}$ et qui renvoie leur image par θ dans $\mathbb{F}_q^{\times} \times \mathbb{F}_{q^{pr}}^{\times}$.

Remarque. Le fait de calculer des racines n^{es} dans $\mathbb{F}_{q^n}$ nous interdit de travailler avec des entiers n pairs . Cependant on peut aisément contourner cette difficulté en travaillant dans le sous-groupe des résidus quadratiques de T_1 et T_2. Cela revient à remplacer $\Phi_1(q)$ and $\Phi_2(q)$ respectivement par $(q-1)/2$ et $(q+1)/2$ dans la construction de θ. On est amené à calculer des racines $n/2$-ièmes dans $\mathbb{F}_{q^n}$ et tout cela ne change pas la complexité globale du protocole.

5.2.5 Mise en œuvre pour $n = 15$

Si l'on considère à nouveau l'exemple $n = 15 = 3 \times 5$, alors un calcul explicite donne les valeurs suivantes, avec les notations de la figure 5.3 :

$$\begin{cases} u_1 = 1 \text{ et } u_{15} = -q^7 - q^4 - q^2 - q, \\ u_3 = -q \text{ et } u_5 = q^3 + 1, \\ v_1 = 2q^8 - 2q^7 - 3q^6 + 8q^5 - 10q^4 + 6q^3 + 7q^2 - 16q + 9, \\ v_2 = -2q^5 - 6q^4 - 9q^3 - 12q^2 - 10q - 6. \end{cases}$$

On observe que les coefficients sont petits en valeur absolue, beaucoup plus petits même que la borne grossière de n^5 annoncée au paragraphe 5.2.3.

5.2.6 Cas où n a plus de deux facteurs premiers

La phase de décomposition est la plus facile à étudier pour n quelconque. Les puissances auxquelles on fait les élévations sont des évaluations en q de polynômes cyclotomiques. Il sont au plus en quantité $d(n) = n^{o(1)}$ car ils sont de degré au plus n ; et chacun d'eux a des coefficients d'au plus $n^{1+o(1)}$ bits, ce qui entraîne une complexité de $n^{3+o(1)} \log^{1+o(1)} q$ opérations élémentaires.

La phase de reconstruction fait intervenir des inverses modulaires de ces polynômes cyclotomiques. Cependant dans l'état actuel de nos connaissances, il semble difficile d'obtenir des bornes similaires à celles du chapitre 2 dans ce cas plus général. Il semble que si n est produit d'un nombre fixé de facteurs premiers, alors les coefficients des polynômes cyclotomiques associés soient bornés par une puissance fixée de n (en valeur absolue toujours). Si c'était le cas, la complexité asymptotique de cette phase n'excéderait pas celle de la décomposition.

5.3 Application cryptographique à Diffie-Hellman

5.3.1 Négociation de clefs multiples

On commence par présenter le protocole de négociation de clefs multiples présenté par Rubin et Silverberg [42] comme application naturelle du paramétrage stablement rationnel des tores algébriques. On adopte pour cela la notation suivante : $\theta : \mathrm{T}_n(\mathbb{F}_q) \times \Pi^- \to \Pi^+$, pour la bijection θ définie par l'équation (3.1).

On suppose qu'Alice et Bob doivent convenir, non plus d'une clef, mais d'une famille de clefs $(K_i)_{1 \leqslant i \leqslant m}$, selon un protocole basé sur celui de Diffie-Hellman. Ainsi, après avoir choisi un générateur g de $\mathrm{T}_n(\mathbb{F}_q)$, chaque clef sera représentée par $K_i = g^{x_i y_i}$ où les x_i et y_i sont des exposants choisis aléatoirement par Alice et Bob.

Alice calcule les points $A_i = g^{x_i}$ du tore et après avoir choisi un élément aléatoire $S_0 \in \Pi^-$, elle calcule de manière récursive $\theta(A_i, S_{i-1}) = (a_i, S_i)$ pour i allant de 1

à m. Elle envoie ensuite à Bob les éléments $(a_i)_{1\leqslant i\leqslant m}$ ainsi que le dernier S_m. Ainsi il peut retrouver les A_i en appliquant $\theta^{-1}(a_i, S_i) = (A_i, S_{i-1})$ de manière récursive, en commençant par $i = m$ et décroissant jusqu'à 1. Il calcule finalement chaque clef $K_i = A_i^{y_i}$.

Par ce protocole, $A_1, \ldots, A_m$ sont représentés par S_m et $a_1, \ldots, a_m$. Le facteur de compression est optimal, à l'exception des quelques bits supplémentaires correspondant à l'élément S_m. Mais il est de longueur fixe et sa taille devient négligeable asymptotiquement, ou en tout cas pour un nombre m assez grand de clefs transmises.

De même avec $B_i = g^{y_i}$, si Bob choisit aléatoirement $T_0 \in \Pi^-$ et calcule tour à tour $(b_i, T_i) = \theta(B_i, T_{i-1})$, il peut envoyer $(b_i)_i$ et T_m à Alice. Cette dernière retrouve $(B_i)_i$ via les calculs successifs de $(B_i, T_{i-1}) = \theta^{-1}(b_i, T_i)$, pour i décroissant de m à 1. Alors $K_i = B_i^{x_i}$ fournit les clefs.

On note que le coût de m exponentiations de Diffie-Hellman est de l'ordre de m fois $n^{2+o(1)} \log^{2+o(1)} q$, ce qui est plus élevé que le coût asymptotique des encodages lors de la négociation de clefs, qui est d'après le théorème 5.2, m fois $n^{2+o(1)} \log^{1+o(1)} q + n^{1+o(1)} \log^{2+o(1)} q$.

5.3.2 Sélection de paramètres

On travaille avec un tore algébrique de dimension n sur $\mathbb{F}_q$. Ses $\mathbb{F}_q$-points forment un groupe de taille $\Phi_n(q)$ qui est plongé dans un corps fini de taille q^n. On cherche un sous groupe de ce tore, de taille r, avec r qui divise $\Phi_n(q)$.

On atteint un paramètre de sécurité de 128 bits avec un corps fini de taille environ 4096 bits.

Dans le cas présent d'une extension de degré 6, on cherche q de taille 682 bits. Donc on peut sélectionner de bons paramètres de la manière suivante :

1. Choisir x de taille 128 bits tel que $r = \Phi_n(x)$ est premier.
2. Énumérer des paramètres h de taille $682 - 256$ bits jusqu'à ce que $x + hr$ soit un nombre premier, et donc un paramètre acceptable pour q.

On présente ci-dessous quelques paramètres obtenus en pratique, à savoir les tailles q et r. On n'en donne qu'une paire pour des raisons d'encombrement, mais l'opération s'exécute en quelques secondes tout au plus.

q = 29455017889092500288723640235742845723465159712052258364501292009537853649697114961628
29333062475059185321978463057423167674233393859516049233603212477774172209138826092496858409159962543767937183058719024 1,

r = 13427555718841825383686713619336100085315042822010952337420943047124037686728 3.

Le même algorithme a également permis d'obtenir en quelques dizaines de minutes des paramètres pour une sécurité de 256 bits. Cette fois, du fait du terme cubique dans la complexité du logarithme discret, le corps fini doit être 8 fois plus grand, soit q de taille environ 5461 bits. Quant au sous-groupe, il doit être de taille 512 bits environ. Alors on obtient

$q = 14077150369591698382600660274897721886138915481779459865958649091212903638730398007780034549379437425113359428064837349909244765936352389626361530949933136179474175986742387175844541137607366529139219898250280197296258910767592558394922302095007862014700367370338681437524258632092380495476336306863446065216957873911944778589629328475109931311719633482191918771015456240564060341592937306772100350849142395490928150444232494569894276725797382759172787546316524930604751501200311797054312959736495125642178683023932320448358248810599344629919198379270286446441576053117340902076687207033807332067483543891559440910866390851914932898346593812164023626516951754788492855730801924582954251355338782633137903464591827049951251530650206357791575499566973111082773224677027659852735131390527769554527024006687886486418658634776294961625270379252524541195332554738174878109067238977797171380957230969415409043353169104115910822882924831819071590553879055734683264190431593818655525222700197200539282435456681131071615301117852269607519318665868233520827345337384975788516040701734003166394999949460371721355546598032369068372497634350500887929625593432542539004905334583294170276430239044411719260099244280091072656536405901503388205746281296731876798376626973514349020198339331127975415630742413275641926268765319773923986963699137512866465034814054173997258157566569343457091250087552761441514992218418269845415792024557260736778815077251697231017695535180780534943638751534814163386044626316481022256951566703346101607559844085444163239764571170099618431985213255269021128207721738633603754534379801525653629920686696984091158470568926913141051151 91,$

$r = 16817166055379728857904423795133212843553750428524279775861956946955673901677846340198795523783394289304807869201658084846018136318984455287453291354020757.$

BIBLIOGRAPHIE

[1] T. M. Apostol. Euler's φ-function and Separable Gauß Sums. *Proceedings of the American Mathematical Society*, vol. 24, n° 3 (1970), p. 482–485.

[2] T. M. Apostol. Resultants of Cyclotomic Polynomials. *Proceedings of the American Mathematical Society*, vol. 24, n° 3 (1970), p. 457–462.

[3] G. Bachman. On the Coefficients of Ternary Cyclotomic Polynomials. *Journal of Number Theory*, vol. 100 (2003), p. 104–116.

[4] A. S. Bang. Om Ligningen $\phi_n(x) = 0$. *Nyt Tidsskrift for Mathematik*, vol. 6 (1895), p. 6–12.

[5] P. T. Bateman. Note on the Coefficients of the Cyclotomic Polynomial. *Bulletin of the American Mathematical Society*, vol. 55, 1180–1181.

[6] M. Beiter. Coefficients in the Cyclotomic Polynomials for Numbers with at Most Three Distinct Odd Primes in their Factorization. *The Catholic University of America Press* (1960).

[7] M. Beiter. The Midterm Coefficient of the Cyclotomic Polynomial F_{pq}. *The American Mathematical Monthly*, vol. 71 (1964), p. 769–770.

[8] M. Beiter. Magnitude of the Coefficients of the Cyclotomic Polynomial F_{pqr}. *The American Mathematical Monthly*, vol. 75 (1968), p. 370–372.

[9] M. Beiter. Magnitude of the Coefficients of the Cyclotomic Polynomial F_{pqr}, II. *Duke math. J.*, vol. 38 (1971), p. 591–594.

[10] D. M. Bloom. On the Coefficients of the Cyclotomic Polynomials. *The American Mathematical Monthly*, vol. 75 (1968), p. 372–377.

[11] A. E. Brouwer, R. Pellikaan, E. R. Verheul. Doing More with Fewer Bits. *Advances in Cryptology* – Asiacrypt '99, Lecture Notes in Computer Science, vol. 1716, Springer Verlag (1999), p. 321–332.

[12] L. Carlitz. The Number of Terms in the Cyclotomic Polynomial F_{pqr}. *The American Mathematical Monthly*, vol. 73 (1966), p. 979–981.

[13] J.-M. Couveignes. Quelques mathématiques de la cryptologie à clés publiques (Journée annuelle de la SMF). *Nouvelles méthodes mathématiques pour la cryptographie*, Société mathématique de France (2007).

[14] J.-M. Couveignes & R. Lercier. Elliptic Periods for Finite Fields. *Finite Fields and their Applications*, vol. 15, n° 1, p. 1–22.

[15] B. Crstici & J. Sándor. *Handbook of Number Theory II*. Kluwer Academic Publisher (2004).

[16] W. Diffie & M. Hellman. New Directions in Cryptography. *IEEE Transactions on Information Theory*, vol. IT-22 (1976), p. 644–654.

[17] M. van Dijk, R. Granger, D. Page, K. Rubin, A. Silverberg, M. Stam, D. P. Woodruff. Practical Cryptography in High Dimensional Tori. *Advances in Cryptology* – EUROCRYPT 2005 (Ronald Cramer, ed.), Lecture Notes in Computer Science, vol. 3494, Springer (2005), p. 234–250.

[18] M. van Dijk & D. Woodruff. Asymptotically Optimal Communication for Torus-Based Cryptography. *Advances in Cryptology* – CRYPTO'04, Lecture Notes in Computer Science, vol. 3152, p. 157–178.

[19] C. Dunand. On Modular Inverses of Cyclotomic Polynomials and the Magnitude of their Coefficients. Soumis au *Journal of Computational Mathematics*, London Mathematical Society.

[20] C. Dunand & R. Lercier. Elliptic Bases and Torus-Based Cryptography. *Ninth International Conference on Finite Fields and Applications*, (G. McGuire *et al.*, eds.), American Mathematical Society (2009), p. 137–153.

[21] T. ElGamal. A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. *Advances in Cryptology* – CRYPTO 1984 (G. R. Blakley & D. Chaum, eds.), Lecture Notes in Computer Science, vol.196, Springer (1985), p. 10–18

[22] P. Erdös. On the Coefficients of the Cyclotomic Polynomial. *Bulletin of the American Mathematical Society*, vol. 52 (1946), p. 179–184.

[23] S. D. Galbraith. *Mathematics of Public-Key Cryptography*. En cours d'écriture, chapitres disponibles sur `http://www.isg.rhul.ac.uk/~sdg/crypto-book/crypto-book.html`.

[24] S. D. Galbraith & M. Scott. Exponentiation in Pairing-Friendly Groups Using Homomorphisms. *Pairing-Based Cryptography* – Pairing 2008, Lecture Notes in Computer Science, vol. 5209, Springer (2008), p. 211–224.

[25] Y. Gallot & P. Moree. Ternary Cyclotomic Polynomials Having a Large Coefficient. *Journal für die reine und angewandte Mathematik*, vol. 632 (2009), p. 105–125.

[26] J. von zur Gathen & J. Gerhard. *Modern Computer Algebra.* Cambridge University Press (1999).

[27] R. Granger, D. Page, M. Stam. A Comparison of CEILIDH and XTR. *6th International Algorithmic Number Theory Symposium*, ANTS (2004).

[28] R. Granger & F. Vercauteren. On the Discrete Logarithm Problem on Algebraic Tori, *Advances in Cryptology* – CRYPTO 2005, Lecture Notes in Computer Science, vol. 3621, Springer, 2005, p. 66–85.

[29] J. Itard. Les nombres premiers. vol. x des *Que sais-je ?*, PUF (1975).

[30] A. Joux & R. Lercier. The Function Field Sieve in the Medium Prime Case. *Advances in Cryptology* – EUROCRYPT 2006, Lecture Notes in Computer Science, vol. 4004, Springer (2006), p. 254–270.

[31] T. Y. Lam & K. H. Leung. On the Cyclotomic Polynomial $\Phi_{pq}(X)$. *The American Mathematical Monthly*, vol. 103 (1996), p. 562–564.

[32] E. Lehmer. On the Magnitude of Coefficients of the Cyclotomic Polynomials. *Bulletin of the America Mathematical Society*, vol. 42, 1936.

[33] M. J. Lennon & P. J. Smith. LUC : A New Public Key System. *IFIP TC11 Ninth International Conference on Information Security IFIP/Sec* (1994) p. 103–117.

[34] A. K. Lenstra & M. Stam. Efficient Subgroup Exponentiation in Quadratic and Sixth Degree Extensions. *Cryptographic, Hardware and Embedded Systems (CHES)*, Lecture Notes in Computer Science, vol. 2523, Springer (2002), p. 318–332.

[35] A. K. Lenstra & E. R. Verheul. The XTR Public Key System. *Advances in Cryptology* – CRYPTO'2000 (Mihir Bellare, ed.), Lecture Notes in Computer Science, vol. 1880 (2000), p. 1–19.

[36] R. Lidl & H. Niederreiter. *Finite Fields.* Encyclopedia of Mathematics and its Applications, vol. 20, Addison-Wesley (1983).

[37] U. M. Maurer & S. Wolf. The Relationship Between Breaking the Diffie-Hellman Protocol and Computing Discrete Logarithms. *SIAM J. Comput.*, vol. 28 (1999), p. 1698–1721.

[38] A. Migotti. Zur Theorie der Kreisteilungsgleichung. *Sitzungberichte der Mathematisch-Naturwissenschaftlichen Classe der Kaiserlichen Akademie der Wissenschaften in Wien*, vol. 87 (1883), p. 7–14.

[39] H. Möller. Über die i-ten Koeffizienten des n-ten Kreisteilungspolynome. *Math. Ann.*, vol. 188 (1970), p. 26–38.

[40] P. Moree. Inverse cyclotomic polynomials. *Journal of Number Theory*, vol. 129 (2009), p. 667–680.

[41] D. Panario & B. Richmond. Analysis of Ben-Or's polynomial Irreducibility Test. *Random Structures and Algorithms*, vol. 13 (1998), p. 439–456.

[42] K. Rubin & A. Silverberg. Torus-Based Cryptography. *Crypto'03*, Lecture Notes in Computer Science, vol. 2729, p. 349–365.

[43] K. Rubin & A. Silverberg. Algebraic Tori in Cryptography. *High Primes Misdemeanours : Lectures in Honour of the 60th Birthday of Hugh Cowie Williams*, Fields Inst. Commun., vol. 41, AMS (2004), p. 317–326.

[44] C. P. Schnorr. Efficient Signature Generation by Smart Cards. *Journal of Cryptology*, vol. 4, (1991), p. 161–174.

[45] V. Shoup. Lower Bounds for Discrete Logarithms and Related Problems. *Advances in Cryptology* – Eurocrypt'97 (1997), p. 256–266.

[46] C Skinner & P. J. Smith. A Public-Key Cryptosystem and a Digital Signature System Based on the Lucas Function Analogue to Discrete Logarithms. *Advances in Cryptology* – ASIACRYPT 1994 (J. Pieprzyk & R. Safavi-Naini, eds.), Lecture Notes in Computer Science, vol. 917 (1994), p. 357–364.

[47] J. Suzuki. On Coefficients of Cyclotomic Polynomials. *Proc. Japan Acad.*, vol. 63, Series A (1987), p. 279–280.

[48] G. Tenenbaum et M. Mendès France, Les nombres premiers. *Que sais-je ?*, vol. 571, Presses Universitaires de France.

[49] V. E. Voskresenskiĭ. *Algebraic Groups and Their Birational Invariants*. Translations of Mathematical Monographs, vol. 179, American Mathematical Society (1991).

[50] A. Weil. *Adeles and Algebraic Groups*. Progress in Math., vol. 23, Birkhäuser, Boston (1982).

TABLE DES MATIÈRES

Résumé

La cryptographie basée sur le logarithme discret a connu de nombreuses avancées dans les dix dernières années, notamment avec l'utilisation de tores algébriques introduite par Lenstra et Verheul. Ici, on axe notre travail sur la facette constructive de ces idées et l'on se penche sur le paramétrage de ces structures. Van Dijk et Woodruff ont récemment proposé une solution pour représenter de manière compacte une famille de points d'un tore algébrique. Afin d'améliorer la complexité asymptotique de cet algorithme, on a recours à plusieurs outils. D'une part on utilise un nouveau type de bases pour les extensions de corps finis, les bases normales elliptiques dues à Couveignes et Lercier. Par ailleurs, les tailles des objets manipulés font intervenir des polynômes cyclotomiques et leurs inverses modulaires. L'amplitude de leurs coefficients intervient directement dans l'étude de complexité. Dans le cas où leurs indices sont des diviseurs d'un produit de deux nombres premiers, on parvient à des bornes voire des expressions explicites pour ces coefficients, qui permettent de conclure quant à l'amélioration du coût de communication dans des protocoles cryptographiques comme une négociation de clefs multiples de Diffie-Hellman.

Abstract

Discrete logarithm-based cryptography has sustained many studies in the last decade. Lenstra and Verheul have especially proposed to make use of algebraic tori. We focus here on the computational aspect of these ideas and on the parametrization of such structures. Van Dijk and Woodruff have recently given an explicit way of compactly encoding a large set of points on an algebraic torus. The computational cost of this algorithm can be improved thanks to several tools. First we use a new class of bases for finite field extensions, namely elliptic normal bases due to Couveignes and Lercier. Besides we notice that the size of the groups involved is given in terms of cyclotomic polynomials and their modular inverses. The magnitude of their coefficients plays a dramatic role in the complexity study. In the case of indices dividing the product of two distinct primes, we manage to find bounds or explicit expressions of these coefficients, which allows us to compute the communication cost of protocoles such as a Diffie-Hellman multiple key exchange.