Séminaire BOURBAKI Novembre 2006
59[e] année, 2006–2007, n[o] 968

COMPTER (RAPIDEMENT) LE NOMBRE DE SOLUTIONS D'ÉQUATIONS DANS LES CORPS FINIS

par **Antoine CHAMBERT-LOIR**

— Votre Sérénité, pouvez-vous me dire, c'est très important, concentrez-vous, pouvez-vous me dire quel est le numéro du compte en banque de monsieur ?
— Oui.
— Vous pouvez le dire ?
— Oui ! !
— Vous pouvez le dire ?
— Oui ! ! !
— Il peut le dire ! ! ! Bravo ! Il est extraordinaire, il est vraiment sensationnel.

Pierre Dac et Francis Blanche, *Sar Rabindranath Duval*

Table des matières

INTRODUCTION

Soit $\mathbf{F}$ un corps fini et soit $f_1, \dots, f_m$ des polynômes à coefficients dans $\mathbf{F}$ en n indéterminées $x_1, \dots, x_n$. Le but de cet exposé est de décrire des algorithmes permettant de calculer efficacement le nombre de solutions dans $\mathbf{F}^n$ du système d'équations $f_1 = \dots = f_m = 0$.

Pour tout entier $k \geqslant 1$, notons N_k le nombre de solutions de ce système dont les coordonnées appartiennent au corps $\mathbf{F}^{(k)}$, unique extension de $\mathbf{F}$ de degré k contenue dans une clôture algébrique fixée de $\mathbf{F}$; si X est le sous-schéma de l'espace affine défini par l'annulation des f_i, on a donc $N_k = |X(\mathbf{F}^{(k)})|$. La fonction zêta $Z(X,t)$ du schéma X est alors donnée par la formule

$$Z(X,t) = \exp\Big(\sum_{k=1}^{\infty} N_k \frac{t^k}{k}\Big) \tag{0.1}$$

et, ainsi que l'a démontré DWORK [37], c'est une fraction rationnelle. Par conséquent, la suite (N_k) est déterminée par un nombre fini de ses termes. Nous verrons aussi que ces algorithmes permettent de calculer la fonction zêta $Z(X,t)$.

Tous les algorithmes décrits ci-dessous reposent sur un premier principe : il suffit, pour calculer $|X(\mathbf{F})|$, de calculer une congruence $|X(\mathbf{F})| \equiv c \pmod{N}$, où N est un entier strictement supérieur à $|X(\mathbf{F})|$, par exemple $N > |\mathbf{F}|^n$. Plus généralement, il suffit que l'on connaisse un encadrement de $|X(\mathbf{F})|$ de largeur inférieure à N ; c'est là qu'interviendra l'analogue de l'hypothèse de Riemann sur les corps finis, que DELIGNE [29] a démontrée, généralisant ainsi des résultats de HASSE (courbes elliptiques) et WEIL (courbes, variétés abéliennes,...). Fixons-nous un tel encadrement $C \leqslant |X(\mathbf{F})| < C + R$.

Là où ces algorithmes diffèrent, c'est sur la façon de choisir un tel entier N puis de calculer c.

Les premiers algorithmes, que nous qualifierons de ℓ-adiques, font l'objet du chapitre 2 de ce rapport. Ils ont pour archétype l'algorithme découvert en 1985 par R. SCHOOF [98] pour calculer le nombre de points d'une courbe elliptique sur un corps fini. Ces algorithmes choisissent un ensemble fini $\{\ell_1, \dots, \ell_s\}$ de « petits » nombres premiers dont le produit $L = \ell_1 \dots \ell_s$ vérifie $L > R$ et calculent, pour tout i un élément $c_i \in \{0, \dots, \ell_i - 1\}$ tel que $|X(\mathbf{F})| \equiv c_i \pmod{\ell_i}$. Le théorème chinois permet d'en déduire un entier $c \in \{0, \dots, L-1\}$ tel que $|X(\mathbf{F})| \equiv c \pmod{L}$. L'origine de la terminologie « ℓ-adique » vient de ce qu'on peut interpréter la congruence modulo ℓ_i par le calcul de la cohomologie étale modulo ℓ_i.

Hors du degré 1 ou de ce qui en provient, la cohomologie étale semble peu accessible au calcul formel ; même dans ce cas, son calcul effectif amène rapidement à la considération de polynômes de très grand degré. Le champ d'application des algorithmes ℓ-adiques est ainsi limité aux courbes de petit genre, aux variétés abéliennes de petite dimension.

Néanmoins, ces algorithmes sont polynomiaux en le logarithme du cardinal de $\mathbf{F}$: aussi bien le temps de calcul que l'espace requis par le calcul sont majorés par une puissance de $\log|\mathbf{F}|$.

Nous présenterons au chapitre 3 les algorithmes p-adiques, où l'entier p désigne la caractéristique du corps $\mathbf{F}$. Ils procèdent en effet en choisissant pour N une puissance de p et en calculant (plus ou moins) la cohomologie p-adique de X modulo N. Par cohomologie p-adique, j'entends ici la cohomologie de Monsky-Washnitzer et ses avatars (rigide, cristalline), qui sont des analogues de la cohomologie de De Rham. Définie comme cohomologie d'un complexe explicite, la cohomologie p-adique se prête naturellement bien au calcul effectif et l'on peut espérer appliquer ces méthodes dans des situations géométriques très générales. Malgré tout, il semble que seules les courbes et les surfaces aient fait l'objet d'implémentations poussées.

Toutefois, parce qu'ils demandent de manipuler des polynômes de degrés au moins p, la dépendance en $\log p$ de leur complexité n'est pas polynomiale. Ils n'en restent pas moins des algorithmes de choix lorsque p est petit, notamment dans les applications cryptographiques où l'on a souvent $p = 2$.

Au fur et à mesure du développement de ces algorithmes, ils ont été programmés et leurs performances éprouvées à l'aune des records qu'ils permirent d'obtenir, c'est-à-dire le calcul de $|X(\mathbf{F})|$ pour des corps $\mathbf{F}$ de cardinal le plus grand possible. Lorsque X est une courbe elliptique, on a pu atteindre un cardinal q de plus de 2 000 chiffres (en base 10) par l'algorithme de Schoof, et d'environ 40 000 chiffres (mais en caractéristique $p = 2$) par l'algorithme 2-adique de Mestre. Ces calculs ont pris plusieurs mois. La diminution de l'espace mémoire nécessité par ces algorithmes a aussi fait l'objet de travaux importants.

Parallèlement, ils ont trouvé un champ d'application dans la cryptographie à clef publique et se sont retrouvés au cœur de logiciels commerciaux. Comme nous le verrons plus bas, les corps $\mathbf{F}$ qu'il faut alors manipuler sont de taille bien plus modeste, disons une cinquantaine de chiffres décimaux.

Le premier chapitre de ce texte est consacré à quelques applications de ce problème algorithmique et de ses diverses solutions efficaces. J'exposerai ensuite les grandes lignes de la plupart des algorithmes ℓ-adiques, puis p-adiques, actuellement utilisés. Il s'avère en fait qu'une bonne partie de la théorie générale et abstraite développée au XX^e^ siècle dans l'étude des conjectures de Weil donne naturellement lieu à des algorithmes efficaces. Cependant, cette constatation n'est pas allée de soi et le crédit en revient bien aux mathématiciens tels que Schoof, Elkies, Atkin (pour la partie ℓ-adique), Satoh, Mestre, Kedlaya, Lauder (pour la partie p-adique) dont les noms émailleront ce texte. À moins d'achever cet exposé juste après le chapitre consacré aux applications, il m'a ainsi fallu dépasser le lapidaire et spontané « On peut le faire ! » sans pour autant plonger le lecteur dans la complexité phénoménale des idées supplémentaires qui ont été nécessaires à l'obtention des records évoqués plus haut. Le compromis que j'ai essayé d'adopter dans ce texte, un peu différent des nombreux survols du sujet disponibles dans la littérature, est celui d'un mathématicien pur subitement intéressé par ce problème de mathématiques appliquées.

Lorsque je décris la complexité d'algorithmes en temps ou en espace, j'emploie les notations $\mathrm{O}(\cdot)$ et $\widetilde{\mathrm{O}}(\cdot)$. La première signifie que le nombre d'opérations élémentaires, resp. l'espace disque, requis par l'algorithme est majoré par un multiple de son argument, lorsque celui-ci tend vers l'infini. La seconde est analogue, à une puissance du logarithme de l'argument près ; en pratique, il suffit de retenir que $\widetilde{\mathrm{O}}(x)$ est majoré par $\mathrm{O}(x^{1+\varepsilon})$ pour tout $\varepsilon > 0$. Toutefois, même si je n'en parlerai jamais, il ne faut pas perdre de vue que le contrôle de la constante que cachent ces notations est d'une importance pratique capitale ; il est bien différent de pouvoir obtenir un résultat en une minute plutôt qu'en mille.

Je tiens à remercier Jean-Benoît Bost, Bas Edixhoven, Reynald Lercier, Bernard Le Stum, David Lubicz et Jean-François Mestre de l'aide qu'ils m'ont apportée au cours de la préparation de cet exposé.

1. APPLICATIONS

1.1. Critères de primalité

Être en mesure de décider si un entier naturel est ou pas un nombre premier est une question arithmétique fondamentale dont les techniques modernes de cryptographie ont d'ailleurs accru l'importance.

En 1986, S. Goldwasser et J. Killian ont proposé le premier algorithme permettant de décider si un entier N est un nombre premier dont la complexité soit polynomiale en $\log N$. Cet algorithme requiert de calculer le cardinal de courbes elliptiques E sur l'anneau $\mathbf{Z}/N\mathbf{Z}$ « choisies au hasard ». Pour cela, on peut tenter d'appliquer l'algorithme de Schoof, en faisant comme si N était premier. Si l'algorithme échoue, cela prouve que N n'est pas premier. Supposons qu'il fournisse un cardinal putatif c. On peut tester si un point au hasard P sur la courbe E est annulé par c ; si ce n'est pas le cas, N n'est pas premier. Inversement, supposons que l'ordre d de P possède un facteur premier p tel que $p > (1+\sqrt{N})^2$ et tel que le point $[d/p]P$ ne rencontre pas l'origine O de la courbe E (au sens où ce point $[d/P]P$ ait des coordonnées homogènes $(x : y : z)$ dans $(\mathbf{Z}/N\mathbf{Z})$, z étant premier à N) ; alors N est premier. (Sinon, désignant par ℓ le plus petit facteur premier de N, l'image de P dans $E(\mathbf{Z}/\ell\mathbf{Z})$ serait d'ordre multiple de p, et cela contredirait la borne de Hasse pour le cardinal d'une courbe elliptique sur un corps fini). L'algorithme de Goldwasser et Killian tente alors d'exhiber de telles familles (E, P, d, p) où $|E(\mathbf{Z}/N\mathbf{Z})| = 2p$, la primalité de p étant établie récursivement par la même méthode.

Comme l'algorithme de Schoof est de complexité polynomiale en $\log N$, il en est de même de celle de l'algorithme de Goldwasser et Killian. Toutefois, le fait que cet algorithme parvienne à conclure pour tout N dépend d'une conjecture apparemment hors de portée sur la répartition des nombres premiers dans de petits intervalles.

Adleman et Huang [2] ont eu l'idée d'utiliser des courbes de genre 2. Cela fournit plus de latitude et leur permet d'affirmer l'existence d'un algorithme probabiliste de complexité polynomiale en $\log N$ permettant de décider si l'entier N est premier.

Cependant, l'algorithme de Schoof, même avec les améliorations d'Atkin et Elkies (qui font l'objet du paragraphe 2.2.5 ci-dessous) n'est pas suffisamment efficace pour permettre d'envisager de tester ainsi la primalité d'entiers ayant plus de quelques centaines de chiffres décimaux. Si l'algorithme fastECPP (*fast elliptic curve primality proving*) a permis de prouver la primalité de nombres ayant plus de vingt mille chiffres décimaux (Morain, mi-2006), c'est en utilisant l'idée d'Atkin d'employer, plutôt que des courbes aléatoires, des courbes elliptiques à multiplication complexe (de discriminants relativement petits, au plus 10^6) dont l'algorithme de Cornacchia [88] bien que probabiliste, permet de calculer rapidement le cardinal.

Pour plus de détails, je renvoie à l'exposé de F. Morain [84] à ce Séminaire, au chapitre 9 du livre [22] d'H. Cohen, ainsi qu'au chapitre 25 du manuel [23].

1.2. Calcul d'une racine carrée modulo p

Soit p un nombre premier impair et soit a un élément de $\mathbf{F}_p$. Le calcul du symbole de Legendre $\left(\dfrac{a}{p}\right) = a^{(p-1)/2}$ est un moyen simple pour décider si a est un carré, à condition bien sûr de calculer la puissance par des élévations au carré successives. Ce que ce critère ne dit pas, c'est comment trouver une racine carrée, c'est-à-dire un élément $b \in \mathbf{F}_p$ tel que $b^2 = a$.

Lorsque $p \equiv 3 \pmod 4$, on peut poser $b = a^{(p+1)/4}$. Le cas crucial est donc celui où $p \equiv 1 \pmod 4$,

Les algorithmes de factorisation de polynômes dans $\mathbf{F}_p$, tel celui de Berlekamp, fournissent une solution efficace. Rappelons-en le principe dans ce cas particulier : si x est un élément de $\mathbf{F}_p$, distinct de $\pm b$, les deux racines $x+b$ et $x-b$ du polynôme $(X-x)^2-a$ seront simultanément carrés ou non carrés si et seulement si $(x+b)/(x-b)$ est un carré dans $\mathbf{F}_p$. Si ce n'est pas le cas, c'est-à-dire une fois sur deux si x est choisi au hasard, le pgcd des polynômes $X^2 - a$ et $(X+x)^{(p-1)/2} - 1$ sera l'un des polynômes $X \pm b$. Le calcul d'un tel pgcd requiert un nombre d'opérations élémentaires au plus égal à une puissance de $\log p$: il suffit en effet de calculer $(X+x)^{(p-1)/2} - 1$ dans la $\mathbf{F}_p$-algèbre $\mathbf{F}_p[X]/(X^2 - a)$.

Comme les autres algorithmes de factorisation dans les corps finis de complexité équivalente, il s'agit toutefois d'un algorithme probabiliste c'est-à-dire que l'on a seulement une très forte probabilité que l'algorithme se termine en un temps donné. Précisément, la probabilité que l'algorithme se termine en N étapes est $1 - 2^{-N}$, mais rien n'interdit de n'avoir pas de chance.

Connaissant un générateur du sous-groupe 2-primaire de $\mathbf{F}_p^*$, l'algorithme de Shanks présenté dans [100] permet alors de calculer des racines carrées dans $\mathbf{F}_p$ en temps $\widetilde{\mathrm{O}}(\log p)$. D'après [4], si l'hypothèse de Riemann généralisée aux fonctions L de Dirichlet est vérifiée, le plus petit entier positif x qui n'est pas un carré modulo p vérifie $x < 2(\log p)^2$.

Écrivons $p-1$ sous la forme $2^k q$ avec $k \geqslant 0$ et q impair ; on voit que $\xi = x^{(p-1)/q} \bmod p$ est un générateur du sous-groupe 2-primaire de $\mathbf{F}_p^*$. Modulo GRH, on a ainsi un algorithme pour calculer des racines carrées dans $\mathbf{F}_p^*$ dont la complexité est polynomiale en $\log p$. Hélas, on ne sait pas en général construire un tel générateur ξ de manière déterministe en temps polynomial en $\log p$ sans faire appel à l'hypothèse de Riemann.

Comme l'a montré Schoof, une conséquence de son algorithme de calcul du cardinal d'une courbe elliptique sur $\mathbf{F}_p$ est un algorithme déterministe (dépendant de a) de complexité polynomiale en $\log p$ pour calculer une racine carrée de a modulo p.

Supposons en effet que $a \equiv -D \pmod p$, où $-D$ est le discriminant d'un ordre $\mathscr{O}$ d'un corps quadratique imaginaire K. Par la théorie de la multiplication complexe, Schoof construit une courbe elliptique E sur une extension finie $\mathbf{F}$ de $\mathbf{F}_p$ dont l'anneau des endomorphismes est $\mathscr{O}$. C'est la partie de l'algorithme la plus coûteuse car $[\mathbf{F} : \mathbf{F}_p]$ est de l'ordre de $\sqrt{-D}$; la complexité de son algorithme dépend donc de l'entier a. Soit q le cardinal de $\mathbf{F}$. Dans le corps K, l'endomorphisme de Frobenius est de la forme $x+y\sqrt{D}$, avec $x, y \in \frac{1}{2}\mathbf{Z}$; on a $2x = t_E = q+1-|E(\mathbf{F})|$ et $x^2+Dy^2 = q$. Une fois calculé $|E(\mathbf{F})|$ par la méthode de Schoof (et non par celle de Cornacchia, probabiliste), on connaît ainsi x et $|y|$. Comme D est un carré modulo p, la courbe elliptique E est ordinaire et t_E n'est pas multiple de p ; par suite x et y ne sont pas multiples de p et la réduction modulo p de $(2x)/(2y)$ est une racine carrée de a.

Comme le remarque Schoof à la fin de [98], on peut combiner ceci avec l'algorithme de Shanks lorsqu'on suppose, par exemple, $p \not\equiv 1 \pmod{16}$. En effet, si ξ est un générateur de la composante 2-primaire de $\mathbf{F}_p^*$, c'est une racine de l'unité dont l'ordre divise 8, donc ξ s'exprime en termes de racines carrées de -1 et 2 dans $\mathbf{F}_p$. On peut ainsi calculer ξ en temps polynomial en $\log p$ par l'algorithme de Schoof utilisant les courbes elliptiques.

1.3. Cryptographie

En 1975, Diffie et Hellman ont proposé [35] une solution élégante permettant à deux individus d'échanger une information secrète bien que le canal de communication puisse être espionné par une oreille indiscrète.

Son principe est le suivant. Les deux protagonistes, Antoine et Bernadette, conviennent d'un groupe G (noté multiplicativement) et d'un élément g de ce groupe. Antoine choisit un entier a, calcule g^a et le transmet à Bernadette ; celle-ci choisit un entier b, calcule g^b et le transmet à Antoine. Le secret commun est l'élément g^{ab} du groupe G, que nos deux héros sont en mesure de calculer puisque $g^{ab} = (g^a)^b = (g^b)^a$; ils peuvent par exemple l'utiliser comme paramètre d'un système de codage symétrique.

Il est nécessaire d'indiquer que ce protocole ne résiste pas à une attaque active : supposons que Charles s'immisce dans la conversation et parvienne à se faire passer pour Antoine à Bernadette et à Bernadette pour Antoine. Il peut alors choisir des entiers a', b', transmettre $g^{a'}$ à Bernadette et $g^{b'}$ à Antoine. Ce dernier utilise donc $g^{ab'}$ pour coder ou décoder un message, tandis que Bernadette utilise $g^{a'b}$. Puisqu'il connaît $g^{ab'} = (g^a)^{b'}$

et $g^{a'b} = (g^b)^{a'}$, Charles peut intercepter un message d'Antoine, le décoder et le recoder à l'intention de Bernadette, ou inversement, sans qu'aucun des deux n'ait pu se douter de quoi que ce soit.

Même s'il n'a pu intervenir physiquement dans la conversation, Charles a connaissance de G, g ainsi que des deux éléments g^a et g^b. Pour qu'il puisse en déduire g^{ab}, il suffirait qu'il soit en mesure de calculer a (ou b).

Le problème, étant donné deux éléments g et h d'un groupe G, de déterminer un entier a tel que $h = g^a$ est appelé *problème du logarithme discret.* Pour que le protocole de Diffie–Hellman résiste à une attaque passive, il est manifestement nécessaire que le problème du logarithme discret dans le groupe G soit difficile à résoudre en pratique ; voir [77, 86] pour l'étude de la réciproque, conjecturalement vraie — il suffirait de savoir construire, pour tout facteur premier p de $|G|$, une courbe elliptique sur $\mathbf{F}_p$, dont le nombre de points est « lisse », c'est-à-dire que ses facteurs premiers sont petits.

Les groupes cycliques $\mathbf{Z}/n\mathbf{Z}$ ne conviennent évidemment pas, car l'algorithme d'Euclide permet très facilement, g étant un générateur fixé de ce groupe, de calculer $a \pmod n$ connaissant $ga \pmod n$. Diffie et Hellman ont proposé d'utiliser les groupes multiplicatifs de corps finis.

En 1985, Koblitz et Miller ont montré que les groupes formés des points d'une courbe elliptique sur un corps fini sont de bons candidats ; plus généralement, on peut imaginer utiliser les groupes $\operatorname{Pic}^0 C$ des diviseurs de degré 0 sur une courbe C définie sur un corps fini $\mathbf{F}$. Il s'agit toutefois de trouver un bon compromis entre la commodité du calcul et la difficulté du problème du logarithme discret dans le groupe G.

Si G est d'ordre n, il y a de nombreux algorithmes en $\widetilde{\mathrm{O}}(\sqrt{n})$ pour résoudre ce problème du logarithme discret, citons celui des kangourous Pollard [93] qui repose sur le *paradoxe des anniversaires* : tirons au hasard, avec remise, des éléments d'un ensemble fini de cardinal n ; le nombre moyen de tirages avant qu'on obtienne un élément déjà tiré est $\sqrt{\pi n/2}$.

Lorsque l'on connaît une factorisation de n, on peut tenter de résoudre le logarithme discret dans chacun des quotients d'ordre premier de G, puis utiliser le théorème chinois, d'où un algorithme de complexité $\widetilde{\mathrm{O}}(\sqrt{t})$ si t est le plus grand facteur premier de n (algorithme de Pohlig-Hellman, [92]).

Dans un groupe « générique », c'est-à-dire dont on ne sait rien et dont un oracle calcule le produit de deux éléments, l'inverse d'un élément et teste l'égalité de deux éléments, V. Shoup [102] a montré qu'un algorithme requiert un nombre de recours à l'oracle au moins proportionnel à $\sqrt{n}$.

Compte tenu de ces attaques et de la puissance des moyens de calcul actuels, l'entier n doit donc être au moins égal à 2^{160}, de même que son plus grand facteur premier. D'où en particulier la nécessité de connaître l'ordre du groupe G, donc de savoir calculer le cardinal d'une courbe elliptique ou, plus généralement, de la jacobienne d'une courbe définie sur un corps fini.

Pour les groupes $G = \mathbf{F}_q^*$, $G = \mathrm{Pic}^0(C)$, mentionnés plus haut, il y a de nombreuses tentatives pour calculer le logarithme discret. Les techniques d'indice fournissent par exemple des algorithmes sous-exponentiels pour les groupes multiplicatifs de corps finis ; pour les groupes de classes de diviseurs de courbes hyperelliptiques, ils sont plus efficaces que les algorithmes génériques lorsque le genre est > 4. La non dégénerescence de l'accouplement de Tate–Lichtenbaum

$$\mathrm{Pic}^0(C)[n] \times \mathrm{Pic}^0(C_{\mathbf{F}_{q^k}})/n \to \mathbf{F}_{q^k}^*/(\mathbf{F}_{q^k}^*)^n$$

permet une réduction du problème au cas du groupe multiplicatif d'une extension finie de $\mathbf{F}_q$: si $q^k \equiv 1 \pmod n$, cet accouplement (composé avec l'élévation à la puissance $(q^k-1)/n$) fournit une injection de G dans $\mathbf{F}_{q^k}^*$. Comme cet accouplement se calcule aisément [46], il convient donc de choisir des courbes C telles que l'ordre multiplicatif de q modulo n ne soit pas trop petit, en pratique $\leqslant 20$. En particulier, cela proscrit les courbes elliptiques supersingulières. De même, il faut éviter que l'ordre n de $\mathrm{Pic}^0(C)$ ne soit multiple de la caractéristique du corps $\mathbf{F}$.

Je renvoie aux ouvrages [10, 11, 23] pour une description détaillée des diverses attaques possibles, des choix raisonnables d'un corps fini, d'une courbe C et d'un élément de $\mathrm{Pic}^0(C)$, et de la façon dont tout ceci peut être implanté dans une carte à puce. En outre, les articles [66, 47] m'ont été très utiles pour écrire ce paragraphe.

Signalons enfin que les protocoles cryptographiques reposant sur la difficulté de résoudre le logarithme discret dans une courbe elliptique ont fait l'objet d'une spécification par divers organismes de normalisation (ANSI, ISO, etc.) et sont au cœur de nombreux systèmes cryptographiques commercialisés.

2. L'APPROCHE ℓ-ADIQUE

Soit $\mathbf{F}$ un corps fini à q éléments et soit E une courbe elliptique sur $\mathbf{F}$, donnée par une équation plane (inhomogène) de la forme

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{2.1}$$

où les coefficients a_1, a_2, a_3, a_4, a_6 sont des éléments de $\mathbf{F}$. Lorsque $p > 3$, on peut se ramener à une équation de la forme de Weierstrass :

$$y^2 = x^3 + ax + b, \tag{2.2}$$

où a et b sont des éléments de $\mathbf{F}$. Pour tout corps k contenant $\mathbf{F}$, notons $E(k)$ les k-points de E, c'est-à-dire l'ensemble des solutions de l'équation (2.1) auquel l'on adjoint le point à l'infini O de $\mathbf{P}^2(k)$ de coordonnées homogènes $(0 : 1 : 0)$. On sait que E possède une unique structure de groupe algébrique, commutatif, dont l'élément neutre est le point O. Elle se déduit de la construction par sécantes et tangentes : pour tout corps k contenant $\mathbf{F}$, trois points P_1, P_2 et P_3 de $E(k)$ sont alignés si et seulement l'on a $P_1 + P_2 + P_3 = O$ dans le groupe $E(k)$.

Nous voulons calculer le cardinal du groupe abélien $E(\mathbf{F})$.

2.1. Premières approches

2.1.1. Symboles de Legendre. — Lorsque E est de la forme 2.2, on a

$$|E(\mathbf{F})| = 1 + \sum_{x\in\mathbf{F}} \begin{cases} 2 & \text{si } x^3+ax+b \in (\mathbf{F}^*)^2 \\ 1 & \text{si } x^3+ax+b = 0 \\ 0 & \text{sinon} \end{cases} = q + 1 + \sum_{x\in\mathbf{F}} \left(\frac{x^3+ax+b}{q}\right),$$

où $\left(\dfrac{t}{p}\right)$ est le symbole de Legendre dans $\mathbf{F}$, qui vaut 1 si t est un carré non nul dans $\mathbf{F}$, 0 si $t = 0$ et -1 sinon. La complexité de cette méthode est $\widetilde{\mathrm{O}}(q)$. Elle n'est ainsi utilisable que si q est petit : un programme élémentaire requiert déjà 10 s pour déterminer que lorsque $q = 1\,048\,609$, et E a pour équation $y^2 = x^3 - 1$, $|E(\mathbf{F})| = 1\,049\,412$.

2.1.2. Frobenius. — L'élévation des coordonnées à la puissance q définit un morphisme $\pi_E \colon E \to E$ de groupes algébriques, appelé endomorphisme de Frobenius. Dans l'anneau $\mathrm{End}(E)$ des endomorphismes de E, π_E vérifie une relation polynomiale :

$$\pi_E^2 - t_E\pi_E + q = 0, \tag{2.3}$$

où t_E est un entier relatif tel que $|t_E| \leqslant 2\sqrt{q}$. En outre (Hasse, [57, 58]), cet entier t_E est relié au cardinal de $E(\mathbf{F})$ par la formule

$$|E(\mathbf{F})| = q + 1 - t_E. \tag{2.4}$$

Rappelons enfin que t_E est la trace de π_E dans $\mathrm{End}(E)$; on a en effet l'égalité :

$$t_E \,\mathrm{id}_E = \pi_E + \pi_E^\vee, \tag{2.5}$$

où $\pi_E^\vee$ est l'isogénie duale $\pi_E^\vee$, définie par $\pi_E^\vee \circ \pi_E = q\,\mathrm{id}_E$, traduisant le fait que la norme de π_E dans $\mathrm{End}(E)$ est égale à q.

2.1.3. Pas de bébés, pas de géants. — Pour calculer l'ordre d d'un élément g d'un groupe abélien fini G, la méthode la plus évidente consiste à calculer g, $2g$, etc. jusqu'à dg, égal à l'élément neutre. Cela requiert d opérations dans le groupe G.

Voici comment D. Shanks [100] propose de procéder si l'on connaît un encadrement $D \leqslant d < D + C$ de d, où D et C sont des nombres entiers. Soit $t = \lceil\sqrt{C}\rceil$ le plus petit entier supérieur ou égal à $\sqrt{C}$. Il existe des entiers i et j vérifiant $0 \leqslant i, j < t$ tels que $d - D = it + j$, d'où l'égalité $(d - D - j)g = itg$ dans G.

Il suffit alors de calculer d'une part les t multiples $g_i = itg$, pour $0 \leqslant i < t$, de tg, d'autre part les t multiples $b_j = (d - D)g - jg$, et de déterminer un élément de la première liste qui appartient à la seconde : si $g_i = b_j$, on a $d = D + it + j$. Le nom de la méthode, *baby steps—giant steps*, vient de ce que les éléments b_j sont dans une progression de « pas de bébé » g, tandis que les éléments g_i sont dans une progression de « pas de géant » tg, t étant approximativement égal à la racine carrée de C, supposé grand. Il en résulte un algorithme pour déterminer l'ordre d'un élément d'un groupe G, requérant $\mathrm{O}(\sqrt{C})$ opérations dans G et le stockage d'autant d'éléments de G lorsque l'on sait que cet ordre appartient à un intervalle de longueur C.

Appliqué au groupe $E(\mathbf{F})$, on peut ainsi trouver l'ordre d'un élément donné en un temps proportionnel à un multiple de $\sqrt{q}$ (multiplié par un facteur logarithmique en q, correspondant à la complexité du calcul dans un corps de cardinal q). Cela ne fournit cependant pas le cardinal de $E(\mathbf{F})$. Toutefois, si P est un point de $E(\mathbf{F})$ d'ordre d, on a $t_E \equiv q+1 \pmod d$ d'après le théorème de Lagrange, d'où la valeur exacte de t_E si $d > 4\sqrt{q}$.

Un tel point n'existe pas toujours. Toutefois, un lemme de Mestre affirme que si E n'a pas de point d'ordre au moins $4\sqrt{q}$, alors sa « tordue quadratique » E', en possède un, tout au moins si q est assez grand ($q \geqslant 1373$ suffit certainement, *cf.* [99], th. 3.1). Si, par exemple, E est donnée par l'équation (2.2), cette courbe E' est donnée par l'équation

$$y^2 = x^3 + a\omega^2 x + b\omega^3,$$

où ω est un élément de $\mathbf{F}^*$ qui n'est pas un carré. (Le moyen le plus simple d'obtenir un tel élément ω consiste à choisir des éléments de $\mathbf{F}^*$ au hasard, jusqu'à ce que l'un convienne.) Les cardinaux de ces courbes sont reliés par la relation

$$|E(\mathbf{F})| + |E'(\mathbf{F})| = 2(q+1),$$

si bien qu'il suffit de déterminer le cardinal de l'une d'entre elles. En choisissant des points au hasard sur ces deux courbes, on obtient rapidement un point d'ordre assez grand, puis, par la méthode de Shanks, le cardinal de $E(\mathbf{F})$ et $E'(\mathbf{F})$.

Le nombre d'opérations que peut requérir l'algorithme de Shanks est $\mathrm{O}(q^{1/4})$ et le calcul effectif dans $E(\mathbf{F})$ nécessite au plus une puissance de $\log q$ opérations élémentaires.

On a ainsi décrit un algorithme probabiliste, de complexité $\widetilde{\mathrm{O}}(q^{1/4})$ pour calculer le nombre de points d'une courbe elliptique sur un corps fini à q éléments.

2.1.4. Courbes à multiplication complexe. — Supposons que l'on sache que la courbe E admette de la multiplication complexe par un ordre $\mathscr{O}$ de discriminant $-D$ d'un corps quadratique imaginaire K. Comme nous l'avons dit dans le paragraphe consacré à l'extraction de racines carrées, l'endomorphisme de Frobenius est de norme q dans $\mathrm{End}(E)$, donc s'écrit $\pi_E = \frac{1}{2}(x + y\sqrt{-D})$ dans K, où x, y sont des entiers relatifs de même parité qui vérifient la relation

$$x^2 + Dy^2 = 4q. \tag{2.6}$$

Alors, $t_E = x$. Comme π_E n'est pas un multiple dans $\mathscr{O}$, le pgcd de x et y est 1 ou 2. Supposons-les impairs pour simplifier, les adapations à faire dans la suite sont évidentes.

L'algorithme de Cornacchia (voir [88] pour une démonstration élémentaire) permet de calculer tous les couples (x, y) d'entiers premiers entre eux qui vérifient l'équation (2.6).

La première étape consiste à déterminer les entiers u tels que $u^2 \equiv -D \pmod{4q}$ et $2q < u < 4q$. Pour trouver un tel u, on commence généralement par résoudre la congruence modulo p par un algorithme probabiliste, puis on utilise la méthode de Newton p-adique.

Pour chacun de ces entiers u, appliquons alors l'algorithme d'Euclide au couple $(4q, u)$ et arrêtons-nous au premier reste x strictement inférieur à $2\sqrt{q}$; si $(4q - x^2)/D$ est le carré d'un nombre entier y, alors $(\pm x, \pm y)$ est solution de (2.6). Sauf si $D = -1$ où il faut aussi considérer $(\pm y, \pm x)$, on obtient ainsi toutes les solutions (primitives) de l'équation (2.6).

Par cette méthode, on peut donc calculer $|E(\mathbf{F})|$ au choix du signe de x (voire celui de y si $D = -1$) près. Inévitable puisqu'on ne distingue pas la courbe E de sa tordue quadratique, cette ambiguïté se résout toutefois sans peine, par exemple en regardant l'ordre d'un point de $E(\mathbf{F})$ pris au hasard.

2.2. Algorithme de Schoof

2.2.1. Représentations. — Fixons une clôture algébrique $\overline{\mathbf{F}}$ de $\mathbf{F}$. Soit n un entier naturel premier à la caractéristique de $\mathbf{F}$ et notons $E[n]$ le sous-groupe de $E(\overline{\mathbf{F}})$ formé des points P tels que $nP = 0$; il est isomorphe à $(\mathbf{Z}/n\mathbf{Z})^2$. Tout endomorphisme u de E laisse stable $E[n]$, d'où une action de $\operatorname{End}(E)$ sur $E[n]$ qui, si l'on choisit une $(\mathbf{Z}/n\mathbf{Z})$-base de $E[n]$, s'identifie à un homomorphisme d'anneaux

$$\rho_n \colon \operatorname{End}(E) \to \mathrm{M}_2(\mathbf{Z}/n\mathbf{Z}). \tag{2.7}$$

En particulier, il correspond à π_E une (classe de conjugaison de) matrice dont le polynôme caractéristique est précisément $X^2 - t_E X + q$, modulo n, cf. l'équation (2.3).

2.2.2. Principe de l'algorithme de Schoof. — En 1985, R. Schoof [98] propose de calculer $|E(\mathbf{F})|$ de la façon suivante :

a) calculer t_E modulo ℓ, pour des nombres premiers $\ell_1, \ell_2, \dots$ distincts de la caractéristique de $\mathbf{F}$;
b) en déduire, par le théorème chinois, t_E modulo le produit L des ℓ_i ;
c) en déduire t_E grâce à l'inégalité de Hasse si $L > 4\sqrt{q}$.

La seconde étape est relativement évidente, de même que la dernière puisqu'il n'y a qu'un seul entier congru à t_E dans l'intervalle $[q + 1 - \frac{1}{2}L, q + 1 + \frac{1}{2}L]$ si $L > 4\sqrt{q}$. Expliquons donc comment calculer t_E modulo ℓ si ℓ est un nombre premier. Récrivons la relation (2.3) en la spécialisant aux points de $E[\ell]$: pour tout $P \in E[\ell]$, on a

$$\pi_E^2(P) + qP = t_E \pi_E(P).$$

Si l'on trouve un entier t tel que l'on ait $\pi_E^2(P) + qP = t\pi_E(P)$ pour un point $P \in E[\ell]$, il vient alors $(t - t_E)\pi_E(P) = O$, d'où $t = t_E \pmod{\ell}$ si P est d'ordre ℓ (c'est-à-dire $P \neq O$).

2.2.3. Polynômes de division. — La multiplication par ℓ dans E est donnée par une transformation rationnelle de $\mathbf{P}^2$, de degré ℓ^2, de la forme $(x:y:z) \mapsto (P_\ell(x,y,z) : Q_\ell(x,y,z) : R_\ell(x,y,z))$ où P_ℓ, Q_ℓ, R_ℓ sont trois polynômes homogènes de degrés ℓ^2 à coefficients dans $\mathbf{F}$, premiers entre eux. L'origine O de E étant l'unique point à l'infini de E, un point $(x:y:z) \in E(\overline{\mathbf{F}})$ appartient à $E[\ell]$ si et seulement si $R_\ell(x,y,z) = 0$. Si l'on se restreint au complémentaire de l'origine, le schéma des points d'ordre ℓ, $E_\ell^* = E[\ell] \cap \mathbf{A}^2$, est donné par les équations $R_\ell(x,y,1) = 0$ et (2.1).

Pour effectuer la première étape, il faudrait donc être capable de calculer les coordonnées d'un point de E_ℓ^*, c'est-à-dire de trouver une solution explicite $(x,y) \in \overline{\mathbf{F}}^2$ de ce système d'équations. Malheureusement, même s'il existe des algorithmes de complexité polynomiale en $\log q$ pour cela, ces algorithmes sont tous probabilistes, c'est-à-dire qu'ils requièrent l'utilisation d'un générateur de nombres aléatoires et que l'on a seulement une très forte probabilité que l'algorithme se termine en un temps polynomial en $\log q$. Schoof contourne cette difficulté en s'intéressant directement à la totalité des points d'ordre ℓ, c'est-à-dire au schéma E_ℓ^* lui-même. Soit A_ℓ l'anneau des fonctions de ce schéma E_ℓ^*, c'est-à-dire

$$A_\ell = \mathbf{F}[x,y]/(y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6, R_\ell(x,y,1)). \tag{2.8}$$

L'image du couple d'indéterminées (x,y) dans A_ℓ^2 donne les coordonnées d'un point, tautologique, d'ordre ℓ de E à coefficients dans A_ℓ. Les endomorphismes $\pi_E^2 + q$ et $t\pi_E$, pour $t \in \mathbf{Z}$ non multiple de ℓ, induisent des endomorphismes de E_ℓ^*, donc des endomorphismes de A_ℓ. Vu la présentation donnée de l'algèbre A_ℓ, un endomorphisme u de A_ℓ détermine deux éléments X_u et Y_u de A_ℓ, correspondant aux coordonnées de $u(P)$, lorsque P est le point tautologique de $E_\ell^*(A_\ell)$.

Schoof calcule ces éléments (X_u, Y_u) lorsque u est l'un des endomorphismes $v = \pi_E^2 + q\,\mathrm{id}_E$ et $u_t = t\pi_E$, pour $t \in \{\pm 1, \dots, \pm\frac{\ell-1}{2}\}$. S'il y a une coïncidence $(X_v, Y_v) = (X_{u_t}, Y_{u_t})$, alors $t_E \equiv t \pmod{\ell}$, sinon, $t_E \equiv 0 \pmod{\ell}$.

2.2.4. Complexité. — Il correspond à l'endomorphisme π_E un couple (X_π, Y_π) de A_ℓ, image de (x^q, y^q). Son calcul revient à une élévation à la puissance q qu'on effectue, par élévations successives au carré, en $\mathrm{O}(\log q)$ multiplications dans A_ℓ. En utilisant les formules d'addition dans E, chacun des $\ell - 1$ couples (X_{u_t}, Y_{u_t}) à considérer demande $\mathrm{O}(1)$ multiplications supplémentaires. Il faut donc effectuer $\mathrm{O}(\ell + \log q)$ multiplications dans A_ℓ pour calculer $t_E \pmod{\ell}$ selon la méthode décrite.

L'algèbre A_ℓ est de dimension $\ell^2 - 1$ sur $\mathbf{F}$ et sa présentation est assez pratique. Par exemple, si $p > 3$ et que E est donnée sous la forme (2.2), elle est de la forme

$$\mathbf{F}[x,y]/(\psi_\ell(x), y^2 - x^3 - ax - b), \tag{2.9}$$

où ψ_ℓ est un polynôme de degré $(\ell^2 - 1)/2$, appelé *polynôme de division* et tel que, si P est un point de E d'abscisse x, $\psi_\ell(x)$ soit l'abscisse du point ℓP.

Notons $M_q(n)$ le nombre de multiplications dans $\mathbf{F}$ requises par une multiplication dans une telle algèbre de dimension n. Naïvement, $M_q(n) = \mathrm{O}(n^2)$ lorsque n tend vers l'infini, mais la découverte de méthodes de multiplication rapide (Karatsuba, utilisation de la transformée de Fourier rapide par SCHÖNHAGE et STRASSEN) a permis de voir que $M_q(n) = \mathrm{O}(n^{1+\varepsilon})$ pour tout $\varepsilon > 0$, ce qu'on notera ici $M_q(n) = \widetilde{\mathrm{O}}(n)$. De même, si le corps $\mathbf{F}$ est présenté sous la forme $\mathbf{F}_p[t]/(f)$, où f est un polynôme irréductible de degré d à coefficients dans $\mathbf{F}_p$, la multiplication dans $\mathbf{F}$ nécessite $\widetilde{\mathrm{O}}(d)$ multiplications dans $\mathbf{F}_p$. Finalement, une multiplication dans A_ℓ requiert $\widetilde{\mathrm{O}}(\ell^2 \log q)$ multiplications élémentaires.

Ce sont bien sûr des évaluations asymptotiques et les constantes implicites dans ces expressions O et $\widetilde{\mathrm{O}}$ sont grandes ; ainsi, pendant longtemps, les méthodes rapides n'ont été compétitives que pour de grandes valeurs de n. Apparemment, l'évolution récente des ordinateurs les rend praticables.

En définitive, le calcul de t_E modulo ℓ a une complexité majorée par $\widetilde{\mathrm{O}}(\ell^3(\log q)^2)$.

Par ailleurs, le théorème des nombres premiers entraîne l'existence d'un nombre réel $c > 0$ tel que l'on ait pour tout nombre réel $x > 0$ la minoration [(1)]

$$\prod_{\ell < x} \ell \geqslant c e^x. \tag{2.10}$$

Par suite, le produit $L_N = \ell_1 \dots \ell_N$ des N premiers nombres premiers est supérieur à $4\sqrt{q}$ si N est minoré par un multiple de $\log q$. Cela fournit finalement un algorithme déterministe de calcul de t_E, et donc de $|E(\mathbf{F})|$, dont la complexité est $\widetilde{\mathrm{O}}((\log q)^5)$.

2.2.5. Améliorations d'Atkin et Elkies. — Étudions plus en détail l'action de π_E sur le groupe $E[\ell]$ des points de ℓ-torsion. Celle-ci s'interprète comme un endomorphisme $\pi_\ell = \rho_\ell(\pi_E)$ de $E[\ell]$, vu comme $\mathbf{F}_\ell$-espace vectoriel de dimension 2. Les espaces propres de π_ℓ correspondent aux sous-groupes cycliques C de $E[\ell]$ qui sont définis sur le corps $\mathbf{F}$. À un tel sous-groupe cyclique C correspond une courbe elliptique $E' = E/C$, définie sur $\mathbf{F}$, et liée à E par une isogénie de degré ℓ. Les invariants j et j' des courbes E et E' fournissent alors un point $\mathbf{F}$-rationnel (j, j') de la courbe modulaire $X_0(\ell)$, identifiée abusivement à son image dans $\mathbf{P}^1 \times \mathbf{P}^1 = X_0(1) \times X_0(1)$.

Inversement, si E n'est pas supersingulière et si son invariant j n'est ni égal à 0 ni égal à 1728 (courbes qu'on qualifiera d'exceptionnelles), ATKIN démontre qu'il correspond à tout invariant $j' \in \mathbf{F}$ tel que $(j, j') \in X_0(\ell)$ une courbe elliptique E' sur $\mathbf{F}$ et une isogénie de degré ℓ, $\varphi\colon E \to E'$. Cela repose sur le fait que sur les $\overline{\mathbf{F}}$-endomorphismes de telles courbes elliptiques sont définies sur $\mathbf{F}$ et que seuls $\pm\,\mathrm{id}$ sont d'ordre fini, voir [99].

Les courbes exceptionnelles sont traitées indépendamment. Celles d'invariants 0 et 1728 admettent des multiplications complexes par $\mathbf{Z}[j]$ et $\mathbf{Z}[i]$ respectivement et leur cardinal se calcule facilement par l'algorithme de CORNACCHIA. Quant aux courbes supersingulières, leur nombre de points dans $\mathbf{F}$ est si particulier (*cf.* [110], th. 4.1) que l'on peut rapidement, en choisissant des points au hasard, vérifier si E est supersingulière et calculer $E(\mathbf{F})$. Nous supposons donc que E n'est pas exceptionnelle.

L'équation de la courbe $X_0(\ell)$ dans $\mathbf{P}^1 \times \mathbf{P}^1$ est un polynôme $\Phi_\ell \in \mathbf{Z}[X, Y]$, symétrique et de degré $\ell + 1$ en chacune des variables — le *polynôme modulaire* ; autrement dit,

[(1)] Il semble qu'on puisse prendre $c = \frac{1}{2}$.

$\Phi_\ell(j,X)$ est le polynôme minimal sur $\mathbf{Q}(j)$ de la fonction méromorphe $j(q^\ell)$ sur $X_0(\ell)$. Son calcul effectif est possible, au moins si ℓ n'est pas trop grand, soit à l'aide du développement en série de Fourier de la fonction modulaire $j(q)$ et des fonctions $j(q^\ell)$, $j(\zeta q)$, pour $\zeta^\ell = 1$ (*cf.* [83]), soit par interpolation en choisissant des valeurs particulières de q (*cf.* [42]). Toutefois, les polynômes modulaires sont de hauteur très grande : d'après P. Cohen [24], lorsque ℓ tend vers l'infini,

$$h(\Phi_\ell) \sim 6\ell \log \ell \ ; \tag{2.11}$$

pour donner un exemple, le terme constant de Φ_5 possède 43 chiffres décimaux ! Comme ℓ est de l'ordre de $\log q$, on utilise d'autres équations de la courbe modulaire $X_0(\ell)$, données par le polynôme minimal d'autre fonctions sur $X_0(\ell)$. Atkin a par exemple proposé d'employer la fonction

$$f_\ell(\tau) = \ell^s \left(\frac{\eta(\ell\tau)}{\eta(\tau)}\right)^{2s}, \qquad s = 12/\operatorname{pgcd}(12, \ell-1), \tag{2.12}$$

où η désigne la fonction η de Dedekind, donnée par

$$\eta(\tau) = q^{1/24}\prod_{n=1}^{\infty}(1-q^n), \qquad q = e^{2i\pi\tau}. \tag{2.13}$$

Si j est l'invariant de la courbe E, supposée non exceptionnelle, la factorisation de $\Phi_\ell(j,Y)$ dans $\mathbf{F}[Y]$ reflète donc l'action de π_E sur $E[\ell]$:

a) si π_ℓ est diagonalisable, $\Phi_\ell(j,Y)$ possède deux facteurs de degré 1, ses autres facteurs sont de même degré r, et $t_2^2 - 4q$ est un carré modulo ℓ ;
b) si π_ℓ n'est pas semi-simple, $t_E^2 - 4q \equiv 0 \pmod{\ell}$ et $\Phi_\ell(j,Y)$ possède exactement deux facteurs irréductibles, l'un de degré 1 et l'autre de degré $r = \ell$;
c) si π_ℓ est semi-simple, non diagonalisable, $t_E^2 - 4q$ n'est pas un carré modulo ℓ et les facteurs irréductibles de $\Phi_j(j,Y)$ sont tous de même degré r.

Avec ces notations, r est l'ordre de la matrice π_ℓ et il existe un élément $\xi \in \overline{\mathbf{F}_\ell}^*$ d'ordre r tel que $t_E \equiv q(\xi + \xi^{-1})^2 \pmod{\ell}$.

Dans les deux premiers cas, il existe un sous-groupe C de $E[\ell]$ défini sur $\mathbf{F}$, correspondant à un quotient A'_ℓ de l'algèbre A_ℓ utilisée par Schoof, c'est-à-dire à un facteur ψ_C de degré $\ell - 1$ du polynôme de division ψ_ℓ. Pour déterminer ce facteur sans expliciter ψ_ℓ, N. Elkies explique dans [40] comment construire une courbe elliptique E' sur $\mathbf{F}$ et une isogénie $\varphi\colon E \to E'$ de noyau C. Ses formules utilisent la théorie des fonctions elliptiques et font intervenir des dénominateurs ; elles ne conviennent que si la caractéristique du corps $\mathbf{F}$ est supérieure à ℓ, *cf.* [99] et le chapitre 17 de [23]. En « petite caractéristique », diverses méthodes existent : utilisation de la loi de groupe formel ou du sous-groupe de p-torsion (Couveignes, [71, 25]), [72] en caractéristique 2.

Dans le troisième cas, la factorisation de Φ_ℓ ne fournit qu'une information partielle sur $t_E \pmod{\ell}$, dont O. Atkin a montré comment la connaissance pouvait accélérer grandement le calcul de t_E.

2.2.6. Résultats. — L'algorithme obtenu en combinant la méthode de Schoof et les améliorations d'Atkin et Elkies est surnommé sea. Sa complexité, en temps et en espace, est polynomiale en $\log q$, respectivement $\widetilde{\mathrm{O}}((\log q)^4)$ et $\mathrm{O}((\log q)^2)$. Toutefois, comme il requiert la factorisation d'un polynôme à coefficients dans un corps fini, c'est un algorithme probabiliste. Il est décrit en grand détail dans [87] lorsque la caractéristique du corps est au moins 3.

Son implémentation concrète a été réalisée par de nombreuses personnes, dans de nombreux systèmes de calcul algébrique, dont Magma [76] et Pari/GP [89]. L'implémentation en caractéristique 2 de Vercauteren lui a permis de calculer le cardinal d'une courbe elliptique sur $\mathbf{F}_{2^{1999}}$ à l'aide de 10 Pentium II 400 Mhz en environ une semaine, *cf.* [105]. Le record actuel est détenu par Enge, Gaudry et Morain qui ont calculé le nombre de points d'une courbe elliptique sur un corps fini de cardinal le nombre premier $p = 10^{2099}+6243$, *cf.* [43]. Le temps de calcul sur une machine puissante (Processeur AMD 64 3400+, 2,4 GHz) est de l'ordre de 200 jours, non compris le calcul des polynômes modulaires !

2.3. Généralisations

2.3.1. Cohomologie étale. — Pour expliquer le titre de ce chapitre et le principe des généralisations de l'algorithme de Schoof, il nous faut faire quelques rappels sur la cohomologie ℓ-adique. Soit $\mathbf{F}$ un corps fini, notons q son cardinal. Fixons une clôture algébrique $\overline{\mathbf{F}}$ de $\mathbf{F}$ et notons $\mathbf{F}_{q^n}$ le sous-corps à q^n éléments de $\overline{\mathbf{F}}$, de sorte que $\mathbf{F}_q = \mathbf{F}$. Soit φ l'automorphisme de Frobenius géométrique de $\overline{\mathbf{F}}$, inverse de l'automorphisme de Frobenius arithmétique $x \mapsto x^q$.

Soit ℓ un nombre premier distinct de la caractéristique de $\mathbf{F}$; notons $\mathbf{F}_\ell$ le corps $\mathbf{Z}/\ell\mathbf{Z}$, $\mathbf{Z}_\ell$ l'anneau des entiers ℓ-adiques et $\mathbf{Q}_\ell$ son corps des fractions.

Soit X un schéma séparé de type fini sur $\mathbf{F}$, posons $\overline{X} = X \otimes \overline{\mathbf{F}}$. Les groupes de cohomologie ℓ-adique à support propre de $\overline{X}$ définis par Grothendieck,

$$H^i_c(\overline{X}, \mathbf{F}_\ell), \quad H^i_c(\overline{X}, \mathbf{Q}_\ell), \quad H^i_c(\overline{X}, \mathbf{Z}_\ell), \tag{2.14}$$

sont respectivement des espaces vectoriels de dimension finie sur $\mathbf{F}_\ell$, $\mathbf{Q}_\ell$, et des $\mathbf{Z}_\ell$-modules de type fini, nuls si $i < 0$ ou si $i > 2\dim X$. Ils sont munis d'une action de $\mathrm{Gal}(\overline{\mathbf{F}}/\mathbf{F})$ et permettent le calcul du cardinal de $X(\mathbf{F})$ via une formule de Lefschetz [54, 53] :

$$|X(\mathbf{F})| = \sum_{i=0}^{2\dim X} (-1)^i \operatorname{Tr}(\varphi | H^i_c(\overline{X}, \mathbf{Q}_\ell)). \tag{2.15}$$

Cette formule, appliquée aux extensions finies de $\mathbf{F}$, entraîne la formule suivante pour la fonction zêta de X :

$$Z(X,t) = \exp\big(\sum_{n=1}^{\infty} |X(\mathbf{F}_{q^n})| \frac{t^n}{n}\big) = \prod_{i=0}^{2\dim X} \det(1 - t\varphi | H^i_c(\overline{X}, \mathbf{Q}_\ell))^{(-1)^{i+1}}, \tag{2.16}$$

d'où, de nouveau, la rationalité de la fonction zêta de X.

On a $H^i_c(\overline{X},\mathbf{Q}_\ell) = H^i_c(\overline{X},\mathbf{Z}_\ell)\otimes_{\mathbf{Z}_\ell}\mathbf{Q}_\ell$, et s'il n'est pas vrai que $H^i_c(\overline{X},\mathbf{Z}_\ell)\otimes_{\mathbf{Z}_\ell}\mathbf{F}_\ell$ est égal à $H^i_c(\overline{X},\mathbf{F}_\ell)$, ces deux groupes peuvent être reliés, de sorte que l'on a une congruence modulo ℓ ([30], Fonctions L modulo ℓ^n, p. 116, th. 2.2) :

$$|X(\mathbf{F})| \equiv \sum_{i=0}^{2\dim X} \mathrm{Tr}(\varphi|H^i_c(\overline{X},\mathbf{F}_\ell)) \pmod{\ell}. \tag{2.17}$$

Supposons par exemple que $X=E$ soit une courbe elliptique E. Si A est l'un des anneaux $\mathbf{F}_\ell$, $\mathbf{Z}_\ell$, $\mathbf{Q}_\ell$, alors $H^0_c(\overline{E},A)=A$, $H^2_c(\overline{E},A)=A$, les endomorphismes φ étant respectivement l'identité et la multiplication par q, tandis que $H^1_c(\overline{E},A)$ est un A-module libre de rang 2. En outre, $H^1_c(\overline{E},\mathbf{F}_\ell)$, muni de l'action de φ, s'identifie canoniquement à $E[\ell]$, muni de l'action de l'endomorphisme π_E, et le polynôme X^2-t_EX+q est le polynôme caractéristique de φ agissant sur $H^1_c(E,\mathbf{F}_\ell)$. En particulier, $t_E\equiv \mathrm{Tr}(\varphi|H^1_c(E,\mathbf{F}_\ell))$ $(\mathrm{mod}\ \ell)$. Dans ce cas, l'entier t_E est d'ailleurs la trace commune de φ sur tous les espaces $H^1_c(E,\mathbf{Z}_\ell)$, $H^1_c(E,\mathbf{Q}_\ell)$ et l'on a

$$Z(E,t) = \frac{1-t_Et+qt^2}{(1-t)(1-qt)}. \tag{2.18}$$

Ainsi, avec ces identifications, la congruence (2.17) n'est autre que celle qui est à la base de l'algorithme de Schoof, d'où le titre, *approche ℓ-adique*, de ce chapitre.

Revenons au cas général en supposant que X soit projective et lisse. P. Deligne [29] a démontré que pour tout i, le polynôme caractéristique de φ agissant sur l'espace $H^i_c(\overline{X},\mathbf{Q}_\ell)$ est un polynôme à coefficients entiers qui ne dépend pas de ℓ (distinct de la caractéristique de $\mathbf{F}$) et dont les racines complexes sont toutes de module $q^{i/2}$. Omettant par abus l'anneau $\mathbf{Q}_\ell$ des notations, on a en particulier la majoration

$$|\mathrm{Tr}(\varphi|H^i_c(\overline{X}))| \leqslant q^{i/2}\dim H^i_c(\overline{X}). \tag{2.19}$$

Cette inégalité généralise la majoration de Hasse ; conjecturée par Weil, c'est l'analogue pour la variété X de l'hypothèse de Riemann.

Pour calculer $|X(\mathbf{F})|$, il suffit de calculer $\mathrm{Tr}(\varphi|H^i_c(\overline{X}))$. Faisons l'hypothèse que X est projective, lisse et géométriquement intègre (sans pour autant supprimer l'indice c de la cohomologie), et supposons que l'on a $H^i_c(\overline{X},\mathbf{Z}_\ell))\otimes\mathbf{F}_\ell\simeq H^i_c(\overline{X},\mathbf{F}_\ell)$. On a alors la congruence

$$\mathrm{Tr}(\varphi|H^i_c(\overline{X}))\equiv \mathrm{Tr}(\varphi|H^i_c(\overline{X},\mathbf{F}_\ell)) \pmod{\ell}.$$

Adapté à ce cadre, l'algorithme de Schoof procéderait de la façon suivante :

a) calculer $\mathrm{Tr}(\varphi|H^i_c(\overline{X},\mathbf{F}_\ell))$ pour $\ell=\ell_1,\ell_2,\dots,\ell_n$ et $0\leqslant i\leqslant 2\dim X$;
b) en déduire, par le théorème chinois, l'entier $\mathrm{Tr}(\varphi|H^i_c(\overline{X}))$ modulo $L=\ell_1\dots\ell_n$;
c) en déduire l'entier $\mathrm{Tr}(\varphi|H^i_c(\overline{X}))$ si L est au moins égal à deux fois la borne donnée par l'équation (2.19).

Le problème est d'avoir une prise raisonnable sur le groupe de cohomologie $H^i_c(\overline{X},\mathbf{F}_\ell)$. Sous les hypothèses données, la dualité de Poincaré identifie H^i_c muni de φ et $H^{2\dim X-i}_c$ muni de $q^{\dim X}\varphi^{-1}$. Supposons donc $0\leqslant i\leqslant \dim X$. Pour $i=0$, on a $H^0_c(\overline{X},\mathbf{F}_\ell)=\mathbf{F}_\ell$

et $\varphi = \mathrm{id}$; la trace cherchée vaut 1. Pour $i = 1$, $H^1_c(\overline{X}, \mathbf{F}_\ell)$ s'identifie au groupe correspondant $H^1_c(A, \mathbf{F}_\ell)$, où A est la variété d'Albanese de X. C'est une variété abélienne que l'on peut espérer décrire explicitement de sorte à appliquer la méthode de Schoof. Toutefois, pour $2 \leqslant i \leqslant \dim X$, il ne semble pas y avoir, en général, de description raisonnablement effective de $H^i_c(\overline{X}, \mathbf{F}_\ell)$. Cette approche restera donc limitée aux courbes et aux variétés abéliennes, dont la cohomologie est contrôlée par le H^1, voire aux variétés pour lesquelles l'on peut décrire effectivement et efficacement la cohomologie à l'aide de variétés abéliennes.

2.3.2. Courbes et variétés abéliennes. — Généralisant des résultats de J. Pila [90], L. Adleman et M.-D. Huang ont ainsi donné dans [3] un algorithme qui calcule le nombre de points d'une variété abélienne A de dimension g définie sur un corps fini $\mathbf{F}_q$ à q éléments, plongée dans l'espace projectif $\mathbf{P}^N$. Il convient de remarquer que ces algorithmes ne calculent pas les traces $\mathrm{Tr}(\varphi | H^i_c(\overline{A}, \mathbf{F}_\ell))$ individuellement, mais leur somme alternée, c'est-à-dire une congruence $|A(\mathbf{F}_q)| \pmod{\ell}$. Supposant que l'on dispose de polynômes homogènes $F_1, \ldots, F_S$ de degrés au plus T définissant l'idéal de A dans $\mathbf{F}_q[x_0, \ldots, x_N]$, de formules pour l'addition de A données par des polynômes de degré D dans R cartes affines, la complexité de cet algorithme, $(\log q)^{\mathrm{O}(N^2(g + \log R + \log D))}$. L'exposant de $\log q$ est énorme : si, pour simplifier, le plongement est donné par le cube d'une polarisation principale, on a $N + 1 = 3^g g!$.

Par ces techniques, il est aussi possible de calculer le polynôme caractéristique de l'endomorphisme de Frobenius π_A agissant sur le module de Tate $T_\ell(A)$ de A (pour ℓ distinct de la caractéristique de $\mathbf{F}_q$). Pila procède par exemple en calculant, pour tout polynôme irréductible $r \in (\mathbf{Z}/\ell\mathbf{Z})[t]$, de degré au plus $2 \dim A$, et leurs puissances, le cardinal du noyau de l'endomorphisme $r(\varphi)$ du groupe fini $A[\ell]$. Il en déduit le polynôme caractéristique de φ sur le F_ℓ-espace vectoriel $A[\ell]$, puis le polynôme caractéristique de φ via le théorème chinois, ayant choisi des valeurs de $\ell \leqslant \mathrm{O}(\log q)$.

Supposons donc que A soit la jacobienne d'une courbe C sur $\mathbf{F}_q$, supposée projective, lisse et géométriquement intègre. D'après Weil [111], on a l'égalité

$$|C(\mathbf{F}_q)| = q + 1 - \mathrm{Tr}(\pi_A). \tag{2.20}$$

Comme on peut décrire effectivement une jacobienne, il existe donc un algorithme de complexité polynomiale en $\log q$ pour calculer le nombre de points d'une telle courbe sur un corps fini. D'après Pila, la complexité d'un tel algorithme est uniforme lorsque la courbe parcourt une famille algébrique, voir [91]. Si elle reste trop grande pour que cette méthode puisse être utilisée en pratique, le cas des courbes hyperelliptiques a fait l'objet d'améliorations importantes.

Supposons que A soit la jacobienne d'une courbe hyperelliptique C qui est donnée par une équation sous la forme (affine)

$$y^2 = f(x), \qquad f \in \mathbf{F}_q[x], \quad \deg f = 2g + 1. \tag{2.21}$$

Toute classe de diviseur de degré 0 sur C est alors représentée de manière unique par deux polynômes u et v vérifiant les conditions suivantes :

(i) u est unitaire ;
(ii) $\deg v < \deg u \leqslant g$;
(iii) u divise $v^2 - f$.

L'idéal du diviseur dans la carte affine ci-dessus n'est autre que $(u(x), y - v(x))$. Cette représentation, rappelée dans [85], est souvent appelée *description de Mumford* dans la littérature. Elle permet à Adleman et Huang de montrer l'existence d'un algorithme pour calculer le cardinal de $C(\mathbf{F}_q)$ et de $A(\mathbf{F}_q)$ dont la complexité est $(\log q)^{\mathrm{O}(g^2 \log g)}$.

Bien que considérablement inférieure à celle des variétés abéliennes générales, cette complexité reste exponentielle en le genre, et ces méthodes sont impropres aux applications cryptographiques. Voir toutefois l'article [50] par Gaudry et Harley concernant les courbes de genre 2 : l'usage de l'analogue des polynômes de division introduits par D. Cantor (voir [17]) leur permit de calculer le nombre de points d'une telle courbe sur un corps fini dont le cardinal est de l'ordre de 10^{20}.

2.4. Formes modulaires

Revenons pour l'instant au cas des courbes elliptiques et supposons que E soit une courbe elliptique définie sur $\mathbf{Q}$, donnée par une équation de Weierstrass (2.2), où a et b sont des entiers relatifs. Pour tout nombre premier p, on peut réduire l'équation modulo p et en déduire, tout au moins si p ne divise pas le discriminant $\Delta_E = -4a^3 - 27b^2$, une courbe elliptique sur $\mathbf{F}_p$; écrivons son cardinal sous la forme $p + 1 - a_p$. Pour les quelques nombres premiers qui restent, on peut définir un entier a_p analogue et définir la fonction L de Hasse-Weil de E par le produit eulérien et la série de Dirichlet

$$L(E,s) = \prod_{\substack{p \text{ premier} \\ p \nmid \Delta_E}} (1 - a_p p^{-s} + p^{1-2s})^{-1} \prod_{p \nmid \Delta_E} (1 - a_p p^{-s})^{-1} = \sum_{n=1}^{\infty} a_n n^{-s}. \tag{2.22}$$

Ce produit et cette série convergent pour $\Re(s) > 3/2$; d'après le théorème de Wiles et Taylor–Wiles, complété par [16], ils possèdent un prolongement holomorphe à $\mathbf{C}$ et une équation fonctionnelle reliant $L(E,s)$ à $L(E, 2-s)$. Plus précisément, si N_E désigne le conducteur de E, la fonction holomorphe sur le demi-plan de Poincaré donnée par le développement de Fourier

$$f_E(\tau) = \sum_{n=1}^{\infty} a_n q^n, \qquad q = e^{2i\pi\tau}, \tag{2.23}$$

est une forme modulaire de poids 2 pour le sous-groupe de congruence $\Gamma_0(N_E)$ de $\mathrm{SL}_2(\mathbf{Z})$. L'algorithme de Schoof apparaît ainsi comme un algorithme de calcul des coefficients des formes modulaires de poids 2.

Dans un article récent [39], Edixhoven, en collaboration avec Couveignes, de Jong, Merkl et Bosman, explique comment calculer les coefficients de Fourier d'une forme modulaire de poids $k \geqslant 2$, niveau N, parabolique et propre pour les opérateurs de Hecke. Leur approche n'est cependant entièrement menée au bout que pour la fonction Δ de Ramanujan, donnée par

$$\Delta(\tau) = \eta(\tau)^{24} = q\prod_{n=1}^{\infty}(1-q^n)^{24} = \sum_{n=1}^{\infty} a_n q^n, \qquad q = e^{2i\pi\tau}. \tag{2.24}$$

(L'entier a_n est classiquement noté $\tau(n)$.) Je me limite ici à une description rapide de quelques-unes des idées essentielles de ce long article. Soit donc f une forme modulaire sur $\Gamma_1(N)$, propre pour les opérateurs de Hecke, normalisée, de développement de Fourier $\sum a_n q^n$.

a) Si f était une série d'Eisenstein, son coefficient a_n serait une somme explicite de puissances de diviseurs de n ; on ne sait pas évaluer une telle somme sans factoriser n, et l'on ne sait pas factoriser n en temps polynomial en $\log n$. On se contentera donc des coefficients a_p, pour p un nombre premier.

b) D'après Deligne, voir [27], il existe pour tout ℓ une représentation de degré 2 de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, à coefficients dans $\mathbf{Z}_\ell$,

$$\rho_{f,\ell}\colon\ \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\mathbf{Z}_\ell) \tag{2.25}$$

telle que pour tout $p \neq \ell N$, a_p soit la trace de $\rho_f(\varphi_p)$, où φ_p est un élément de Frobenius (géométrique) en la place p. La construction géométrique de cette représentation et la démonstration par Deligne des conjectures de Weil entraînent en outre la majoration

$$|a_p| \leqslant 2p^{(k-1)/2} \tag{2.26}$$

qu'avait conjecturée Ramanujan.

La méthode de Schoof suggère donc de calculer la réduction modulo ℓ, disons $\overline{\rho}_{f,\ell}$, de cette représentation pour des valeurs de ℓ au plus égale à $\mathrm{O}(\log p)$.

c) Lorsque $k = 2$, cette représentation $\overline{\rho}_{f,\ell}$ se réalise dans celle associée aux points de ℓ-torsion de la jacobienne $J_1(N)$ de la courbe modulaire $X_1(N)$. Dans le cas général, la construction de Deligne fait intervenir un groupe de cohomologie de degré $k-1$ d'un produit fibré (désingularisé) $k-2$-fois de la « courbe elliptique universelle » sur $X_1(N)$. Comme on l'a évoqué plus haut, il ne semble pas possible de décrire cette cohomologie explicitement.

En revanche, des phénomènes de *congruence* entre formes modulaires entraînent que $\overline{\rho}_{f,\ell}$ se réalise dans la représentation galoisienne associée aux points de ℓ-torsion de la jacobienne $J_1(N\ell)$.

Comme le genre de $J_1(N\ell)$ est de l'ordre de $N^2\ell^2$, il s'agit de détecter une sous-représentation de dimension 2 dans une représentation de très grande dimension. Autrement dit, de détecter les ℓ^2-1 points d'ordre ℓ de $J_1(N\ell)$ correspondant à $\overline{\rho}_{f,\ell}$, le polynôme minimal d'un générateur de l'extension de $\mathbf{Q}$ engendrée par leurs coordonnées et l'action du groupe de Galois $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$.

d) Pour ce faire, Couveignes a suggéré de travailler dans $\mathbf{C}$ et de calculer une approximation de ce polynôme, en même temps qu'une borne pour sa hauteur. (Deux nombres rationnels distincts $x = a/b$ et $x' = a'/b'$ de hauteurs $\log \max(|a|, |b|)$ et $\log \max(|a'|, |b'|)$ au plus h diffèrent d'au moins e^{-2h}.)

Les bornes requises sur la hauteur sont obtenues en majorant certaines quantités concernant la théorie d'Arakelov des courbes modulaires $X_1(\ell)$: la hauteur de Faltings, certaines fonctions θ et les fonctions de Green ; ces bornes sont polynomiales en ℓ.

e) Plutôt que calculer dans la jacobienne $J_1(N\ell)$, les auteurs préfèrent utiliser le produit symétrique $X_1(N\ell)^{(g)}$ de la courbe modulaire, qui est muni d'une application naturelle birationnelle vers $J_1(N\ell)$. Pour garantir que les points d'ordre ℓ intervenant dans $\overline{\rho}_{f,\ell}$ ont un unique antécédent, la construction géométrique d'un diviseur ayant des propriétés spécifiques est nécessaire, si bien qu'à ce stade, les auteurs de [39] se cantonnent à la forme modulaire Δ de Ramanujan. Pour réaliser cette construction, ils réduisent modulo p, et l'utilisation d'un algorithme probabiliste leur est pour l'instant nécessaire.

Tout ceci combiné, Edixhoven et al. démontrent qu'il existe un algorithme probabiliste de complexité polynomiale en ℓ calculant $\overline{\rho}_{f,\ell}$, c'est-à-dire :

a) un corps de nombres K_ℓ donné par sa table de multiplication, galoisien sur $\mathbf{Q}$ correspondant au noyau de la représentation $\overline{\rho}_{f,\ell}$,
b) des matrices correspondant aux éléments σ du groupe $\mathrm{Gal}(K_\ell/\mathbf{Q})$ agissant $\mathbf{Q}$-linéairement sur K_ℓ, et
c) les matrices $\overline{\rho}_{f,\ell}(\sigma) \in \mathrm{GL}_2(\mathbf{F}_\ell)$ correspondantes.

Ils en déduisent qu'il existe un algorithme probabiliste calculant le coefficient $\tau(p)$ de la fonction de Ramanujan, algorithme dont la complexité est polynomiale en $\log p$.

3. MÉTHODES p-ADIQUES

3.1. Application de la théorie de Dwork

Comme je l'ai dit plus haut, la première démonstration de la rationalité de la fonction zêta d'une variété algébrique définie sur un corps fini est due à Dwork [37]. A. Lauder et D. Wan ont observé [69, 109] que la démonstration de Dwork permet un moyen de calcul effectif de la fonction zêta. Même si cette méthode s'avère moins efficace que celles qui ont été développées peu après, elle fournit un algorithme indépendant de la géométrie du système d'équations considéré.

3.1.1. Calculabilité de la fonction zêta. — Soit $\mathbf{F}$ un corps fini, notons q son cardinal et p sa caractéristique. Considérons une variété algébrique affine X, lieu des zéros dans $\mathbf{A}^n$ de m polynômes $f_1, \dots, f_m \in \mathbf{F}[x_1, \dots, x_n]$; soit a le maximum des degrés des f_i. L'espace nécessaire pour écrire ces polynômes est de l'ordre de $m(a+1)^n \log q$. On cherche un algorithme efficace, pour calculer la fonction zêta de X.

D'après Dwork, cette fonction zêta s'écrit comme le quotient P_1/P_2 de deux polynômes à coefficients entiers, premiers entre eux, de termes constants 1. Un théorème de Bombieri majore par $A = (4a+9)^{n+m}$ la somme des degrés de P_1 et de P_2 (prop. 4.2 et th. 1 de [12], appliqué à $f = 1$). Autrement dit, il existe des nombres entiers a_1 et a_2 tels que $a_1 + a_2 \leqslant A$, des entiers algébriques $\alpha_1, \dots, \alpha_{a_1}$, $\beta_1, \dots, \beta_{a_2}$ tels que pour tout entier $k \geqslant 1$,

$$|X(\mathbf{F}_{q^k})| = -\sum_{j=1}^{a_1} \alpha_j^k + \sum_{j=1}^{a_2} \beta_j^k, \tag{3.1}$$

la fonction zêta elle-même étant donnée par

$$Z(X,t) = \frac{\prod_{j=1}^{a_1}(1-\alpha_j t)}{\prod_{j=1}^{a_2}(1-\beta_j t)}. \tag{3.2}$$

Par conséquent, pour calculer la fonction zêta de X, il suffit de calculer les cardinaux $|X(\mathbf{F}_{q^k})|$ pour $1 \leqslant k \leqslant A+1$, d'en déduire les $A+1$ premiers termes du développement en série entière de $Z(X,t)$ puis de calculer une approximante de Padé de cette série. En particulier, *la fonction zêta est effectivement calculable.*

D'autre part, d'après Deligne [31], les valeurs absolues des α_j et β_j sont de la forme $q^{s/2}$, où s est un entier compris entre 0 et $2 \dim X$ (dépendant de j). En particulier, les coefficients de P_1 et de P_2 sont majorés par $2^A q^{nA}$. L'espace nécessaire pour écrire la fonction zêta est donc $\mathrm{O}(nA \log q) = \mathrm{O}(n(4a+9)^{n+m} \log q)$, sensiblement du même ordre de grandeur que celui nécessaire au stockage des données.

La question algorithmique qui se pose naturellement alors est la suivante : *Est-il possible de calculer la fonction zêta en temps* polynomial *en cette taille ?* Compte-tenu des bornes de Bombieri rappelées ci-dessus, cela revient à la question : *Est-il possible de calculer le cardinal de $X(\mathbf{F}_{q^k})$ en temps polynomial en $k(a+1)^{n+m} \log q$?*

Pour les variétés de dimension zéro de la droite affine, définies par un polynôme $f \in \mathbf{F}[x]$, de degré a, l'algorithme de Berlekamp a la complexité voulue. Si f est sans racines multiples, le pgcd de f et $x^q - x$ a pour degré le nombres de racines de f dans $\mathbf{F}_q$. On calcule bien sûr ce pgcd par l'algorithme d'Euclide, en commençant par évaluer x^q dans l'algèbre $\mathbf{F}[x]/(f)$ ce qui requiert en gros $\log q$ opérations dans cette algèbre ; la suite de l'algorithme nécessite au plus a divisions euclidiennes de polynômes de degrés au plus a à coefficients dans $\mathbf{F}$.

Pour les courbes planes toutefois, les résultats du chapitre précédent faisaient apparaître une dépendance exponentielle en le genre...

Si $q = p^d$, Lauder et Wan montrent que la réponse est oui si l'on se limite aux corps de caractéristique majorée. Ils déduisent de l'étude par Dwork de la fonction zêta d'une hypersurface une *congruence* modulo une puissance de p pour le nombre de points d'une hypersurface sur $\mathbf{F}_q$, d'où sa valeur si l'exposant de la puissance dépasse dn.

3.1.2. Une formule de congruence. — Nous allons nous borner au cas d'une hypersurface de l'espace affine d'équation $f = 0$, où $f \in \mathbf{F}_q[x_1, \dots, x_n]$. La méthode de Dwork est « torique » et commence en fait par étudier la fonction zêta de l'intersection X de cette hypersurface avec le tore ${\mathrm{G}_\mathrm{m}}^n$. Le reste s'étudie classiquement par récurrence, au moyen de la formule d'inclusion-exclusion, mais cela induit inexorablement des facteurs 2^n dans la complexité des algorithmes à venir.

La théorie des sommes de caractères fournit la formule

$$q|X(\mathbf{F}_q)| - (q-1)^n = \sum_{(x_0,\dots,x_n)\in \mathrm{G_m}^{n+1}(\mathbf{F}_q)} \chi_q(x_0 f(x_1,\dots,x_n)), \tag{3.3}$$

où $\chi_q\colon \mathbf{F}_q \to \Omega^*$ est un caractère additif non trivial de $\mathbf{F}_q$, Ω étant un corps de caractéristique zéro.

Soit W l'anneau des vecteurs de Witt de $\mathbf{F}$. C'est un anneau de valuation discrète, complet, de corps résiduel $\mathbf{F}$ et dont l'idéal maximal est engendré par p. Si $\mathbf{F} = \mathbf{F}_p$, W n'est autre que l'anneau $\mathbf{Z}_p$ des entiers p-adiques ; si $\mathbf{F}$ est décrit sous la forme $\mathbf{F}_p[x]/(f)$, où f est un polynôme de degré d, W est isomorphe à l'anneau quotient $\mathbf{Z}_p[x]/(\widetilde{f})$, où $\widetilde{f} \in \mathbf{Z}_p[x]$ est un polynôme de degré d arbitraire dont la réduction modulo p est égale à f.

Soit R l'anneau obtenu en adjoignant à W un élément π tel que $\pi^{p-1} = -p$. Notons Ω le corps des fractions de R. Sa valeur absolue $|\cdot|$ et sa valuation ord sont normalisées par $|p| = 1/p$ et $\operatorname{ord} p = 1$. Soit d l'entier tel que $q = p^d$. Notons $\omega\colon \mathbf{F} \to \Omega$ le caractère de Teichmüller, prolongé par $\omega(0) = 0$. Pour tout $x \in \mathbf{F}^*$, $\omega(x)$ est l'unique racine de l'unité d'ordre premier à p de W qui est congrue à x modulo p ; c'est aussi la limite de la suite ξ^{q^n}, où ξ est un élément arbitraire de W qui est congru à x modulo p.

Soit σ l'unique automorphisme de K tel que $\sigma(\pi) = \pi$ et est congru à l'automorphisme de Frobenius modulo p ; notons τ l'inverse de σ.

Si les coefficients de la série exponentielle sont p-adiquement trop grands, ceux de la série $\theta \in \Omega[[z]]$ définie par

$$\theta(z) = \exp(\pi z - \pi z^p) \tag{3.4}$$

sont de valeurs absolues inférieures ou égales à 1 et tendent vers 0. Précisément, on a

$$\operatorname{ord} \theta_n \geqslant \max\Big(\frac{n(p-1)}{p^2}, \frac{2}{p-1}\Big). \tag{3.5}$$

Dwork montre alors que l'on peut choisir pour caractère χ_q dans la formule (3.3) la fonction

$$\chi_q(z) = \theta(1)^{\operatorname{Tr}_{\mathbf{F}_q/\mathbf{F}_p}(z)} = \prod_{i=0}^{d-1} \theta(\omega(z)^{p^i}). \tag{3.6}$$

Soit F la série formelle en les indéterminées $x_0, \dots, x_n$ définie par

$$F(x) = \prod_J \theta(\omega(f_J)x^J), \qquad \text{où} \quad x_0 f(x_1,\dots,x_n) = \sum_J f_J x^J. \tag{3.7}$$

Les majorations (3.5) des coefficients de la série θ et l'hypothèse que f est de degré a entraînent que les coefficients de $F = \sum F_J x^J$ vérifient

$$\begin{cases} \operatorname{ord} F_J \geqslant j_0 \frac{p-1}{p^2} & \text{si } j_0 a \geqslant j_1 + \dots + j_n, \\ F_J = 0 & \text{sinon.} \end{cases} \tag{3.8}$$

Notons L l'ensemble des séries formelles qui vérifient ces inégalités et Δ l'ensemble des monômes x^J tels que $j_0 a \geqslant j_1 + \cdots + j_n$.

Soit ψ l'« opérateur de Dwork » sur $\Omega[[x_0, \ldots, x_n]]$ donné par

$$\psi(\sum_J u_J x^J) = \sum_J \tau(u_{pJ}) x^J. \tag{3.9}$$

L'opérateur composé α de ψ et de la multiplication par F applique L dans lui-même. Soit A sa matrice (infinie) dans la « base » Δ.

Le point crucial de la démonstration de Dwork est la nucléarité de l'opérateur linéaire α^d qui se déduit de majorations explicites pour les coefficients de la matrice A, elles-mêmes déduites de (3.8). En particulier, pour tout entier $k \geqslant 1$, α^{dk} possède une trace, d'ailleurs égale à la somme des coefficients diagonaux de sa matrice dans la base Δ, et l'on a

$$\operatorname{Tr}(\alpha^k)(q^k - 1)^{n+1} = q^k |X(\mathbf{F}_{q^k})| - (q^k - 1)^n. \tag{3.10}$$

Comme l'ont remarqué Lauder et Wan (voir [69], th. 28), ces majorations entraînent aussi que si l'on « tronque » l'opérateur α en considérant sa restriction α_ν au sous-espace (stable) engendré par les monômes x^J de Δ tels que $j_0 \leqslant \nu(p/(p-1))^2$, on obtient une congruence (pour simplifier, on ne regarde désormais que le cas $k = 1$) :

$$\operatorname{Tr}(\alpha_\nu)(q - 1)^{n+1} \equiv q|X(\mathbf{F}_q)| - (q - 1)^n \pmod{p^\nu} \tag{3.11}$$

Soit A_ν la matrice de l'application σ-linéaire α_ν ; elle est de taille $N = \mathrm{O}((\nu a + 1)^n)$. Pour calculer $\operatorname{Tr}(\alpha_\nu)$ modulo p^ν, il suffit de réduire A_ν modulo p^ν, d'effectuer le produit $A_\nu \tau(A_\nu) \ldots \tau^{a-1}(A_\nu)$ puis de calculer la trace de cette matrice modulo p^ν. Le produit de ces k matrices peut être effectué efficacement en adaptant l'algorithme d'exponentiation binaire ; on n'a alors que $\mathrm{O}(\log k)$ produits à faire.

Cela fournit un algorithme pour calculer $|X(\mathbf{F}_q)|$ modulo p^ν. Comme $0 \leqslant |X(\mathbf{F}_q)| < p^{dn}$, il suffit, pour en déduire la valeur de $|X(\mathbf{F}_q)|$, de choisir $\nu = nd$. La complexité de l'algorithme ainsi esquissé est $\widetilde{\mathrm{O}}(p^{2n+4} a^{3n} n^{3n+5} d^{3n+7})$ en temps, et $\widetilde{\mathrm{O}}(p a^{2n} n^{2n+3} d^{2n+4})$ en espace.

3.2. Relèvement canonique et moyenne arithmético-géométrique

Revenons au cas des courbes elliptiques. Soit E une courbe elliptique définie sur un corps fini $\mathbf{F}$; notons q le cardinal de $\mathbf{F}$, p sa caractéristique ; soit d l'entier tel que $q = p^d$. Notons enfin W l'anneau des vecteurs de Witt de $\mathbf{F}$ et K son corps des fractions.

L'algorithme que nous décrivons ici permet, une fois encore, de calculer $|E(\mathbf{F})|$. Il est dû à K. Satoh [96], au moins lorsque $p > 3$. La présentation que nous suivons ici tient compte d'articles parus ultérieurement dans lequel $p = 2$ et 3 sont pris en compte ([44], [103], [97] et [107]), ainsi que de sa variante, due à Mestre, fondée sur la moyenne arithmético-géométrique.

3.2.1. Relèvements. — Soit $\mathscr{E}$ un *relèvement de* E, c'est-à-dire une courbe elliptique sur W dont la réduction modulo p est égale à E. Une telle courbe peut être obtenue en considérant une équation de Weierstrass (2.1) ou (2.2) à coefficients dans W dont la réduction modulo p est une équation de Weierstrass de E. Un endomorphisme $\widetilde{u}$ de $\mathscr{E}$ définit, par réduction modulo p, un endomorphisme de E, d'où un homomorphisme d'anneaux, injectif, de $\operatorname{End}(\mathscr{E})$ dans $\operatorname{End}(E)$.

Si $\mathscr{E}$ est mal choisi, $\operatorname{End}(\mathscr{E}) = \mathbf{Z}$. Toutefois, si E est *ordinaire*, c'est-à-dire que E possède un point d'ordre p, un théorème de Deuring [34] affirme qu'il existe un unique relèvement $\mathscr{E}$ appelé le *relèvement canonique* de E pour lequel l'homomorphisme $\operatorname{End}(\mathscr{E}) \to \operatorname{End}(E)$ soit un isomorphisme ou, cela revient au même, le seul relèvement sur lequel l'endomorphisme de Frobenius π_E de E se relève en un endomorphisme $\pi_{\mathscr{E}}$ de $\mathscr{E}$.

Comme les traces de $\pi_{\mathscr{E}}$ dans $\operatorname{End}(\mathscr{E})$ et de π_E dans $\operatorname{End}(E)$ sont égales, il suffit de calculer la première. Celle-ci se voit au niveau des formes différentielles : si ω est une forme différentielle invariante (non nulle) sur $\mathscr{E}$, $\pi_{\mathscr{E}}^*\omega$ est une forme différentielle invariante, donc est proportionnelle à ω. Soit $c_{\mathscr{E}} \in W$ tel que $\pi_{\mathscr{E}}^*\omega = c_{\mathscr{E}}\omega$. Puisque l'isogénie duale $\pi_{\mathscr{E}}^\vee$ de $\pi_{\mathscr{E}}$ vérifie la relation

$$\pi_{\mathscr{E}}^\vee \circ \pi_{\mathscr{E}} = q\,\mathrm{id}_{\mathscr{E}}, \tag{3.12}$$

$c_{\mathscr{E}} \neq 0$ et $(\pi_{\mathscr{E}}^\vee)^*\omega = qc_{\mathscr{E}}^{-1}\omega$. La somme des endomorphismes $\pi_{\mathscr{E}}$ et $\pi_{\mathscr{E}}^\vee$ est la multiplication par la trace de $\pi_{\mathscr{E}}$, c'est aussi puisque l'homomorphisme $\operatorname{End}(\mathscr{E}) \to \operatorname{End}(E)$ est un isomorphisme, la multiplication par la trace de π_E. Autrement dit, on a l'égalité

$$|E(\mathbf{F})| = q + 1 - t_E = q + 1 - \left(c_{\mathscr{E}} + \frac{q}{c_{\mathscr{E}}}\right). \tag{3.13}$$

Cette méthode n'est pas praticable telle quelle car π_E est un endomorphisme de degré q, supposé très grand. L'idée de Satoh consiste, considérant la factorisation naturelle de π_E en d isogénies de degré p, à relever ces isogénies et à calculer des constantes analogues c_i dont $c_{\mathscr{E}}$ sera le produit. En fait, une telle factorisation est un point essentiel de la construction même de la courbe $\mathscr{E}$, suivant la méthode décrite par Lubin, Serre et Tate dans [75].

Soit σ l'automorphisme de $\mathbf{F}$ donné par $x \mapsto x^p$; comme $q = p^d$, on a $\sigma^d = \mathrm{id}$. Si E est une courbe elliptique sur $\mathbf{F}$, on notera $E^{(\sigma)}$ la courbe obtenue en appliquant l'automorphisme σ à ses coefficients ; elle est liée à E par une isogénie $\varphi\colon E \to E^\sigma$ de degré p qui correspond à l'élévation des coordonnées des points à la puissance p. On a ainsi une suite d'isogénies (de degré p)

$$E \xrightarrow{\varphi} E^{(\sigma)} \xrightarrow{\varphi} E^{(\sigma^2)} \xrightarrow{\varphi} \dots \xrightarrow{\varphi} E^{(\sigma^d)} = E. \tag{3.14}$$

Notons encore σ l'unique automorphisme de W dont la réduction modulo p est l'automorphisme σ de $\mathbf{F}$; on a aussi $\sigma^d = \mathrm{id}$. À la suite de [75], Satoh propose de chercher $\mathscr{E}$ de sorte que l'on ait encore une suite d'isogénies de degré p :

$$\mathscr{E} \xrightarrow{\varphi} \mathscr{E}^{(\sigma)} \xrightarrow{\varphi^{(\sigma)}} \mathscr{E}^{(\sigma^2)} \xrightarrow{\varphi^{(\sigma^2)}} \dots \xrightarrow{\varphi^{(\sigma^{d-1})}} \mathscr{E}^{(\sigma^d)} = \mathscr{E}. \tag{3.15}$$

En effet, étant donnée une telle courbe $\mathscr{E}$, l'endomorphisme composé $\varphi^{(\sigma^{d-1})}\circ\cdots\circ\varphi^{(\sigma)}\circ\varphi$ relève l'endomorphisme π_E de E, si bien que $\mathscr{E}$ est le relèvement canonique de E. Autrement dit, on va chercher un relèvement $\mathscr{E}$ de E tel que le couple $(\mathscr{E}, \mathscr{E}^{(\sigma)})$ soit un point de la courbe modulaire $X_0(p)$.

3.2.2. Résolution de l'équation modulaire. — Le polynôme modulaire Φ_p, équation de la courbe $X_0(p)$ dans $\mathbf{P}^1 \times \mathbf{P}^1$, vérifie une congruence modulo p, due à Kronecker :

$$\Phi_p(X, Y) \equiv (X^p - Y)(Y^p - X) \pmod{p}. \tag{3.16}$$

Lorsque l'invariant j_E de la courbe E n'appartient pas au corps $\mathbf{F}_{p^2}$, l'équation « sesqui-polynomiale » $\Phi_p(j, \sigma(j))$, où l'inconnue j appartient à l'ensemble des éléments de W dont la réduction est l'invariant j_E, est alors justiciable d'une variante de la méthode de Newton, d'où une construction du relèvement canonique de la courbe E dans ce cas. À chaque itération, l'équation linéarisée est de la forme, dite *équation d'Artin-Schreier* :

$$a\sigma(x) + bx = c. \tag{3.17}$$

Toutefois, le calcul effectif de σ est délicat. Les algorithmes efficaces de Lercier, Lubicz puis Harley pour les résoudre leur ont permis d'implémenter effectivement cette approche (voir [73, 55] et le chapitre 12 de [23]). Quant à Satoh, il procéda un peu différemment en prenant pour inconnue, non pas seulement la courbe $\mathscr{E}$, mais toutes les courbes $\mathscr{E}_i = \mathscr{E}^{(\sigma^i)}$ simultanément. Les d invariants $j_i = j(\mathscr{E}_i)$, pour $0 \leqslant i \leqslant d-1$, sont liés par le système d'équations polynomiales

$$\Phi_p(j_0, j_1) = \Phi_p(j_1, j_2) = \cdots = \Phi_p(j_{d-2}, j_{d-1}) = \Phi_p(j_{d-1}, j_0) \tag{3.18}$$

dont une résolution par la méthode de Newton classique est possible.

3.2.3. Itération de quotients. — Avec les notations précédentes, les courbes $\mathscr{E}_0$ et $\mathscr{E}_1$ sont liées par une isogénie $\varphi\colon \mathscr{E}_0 \to \mathscr{E}_1$ dont la réduction modulo p, le frobenius relatif, est une isogénie inséparable. Soit $\varphi\colon \mathscr{E}_0 \to \mathscr{E}_1$ un relèvement arbitraire de $\varphi\colon E \to E^{(\sigma)}$. Le sous-schéma de p-torsion, $\mathscr{E}_0[p]$, possède un sous-groupe de rang p connexe canonique, G_0, le quotient $\mathscr{E}_0[p]/G_0$ étant un W-schéma en groupes étale. (Localement pour la topologie étale, G_0 est isomorphe au schéma en groupes μ_p.) De plus, $\mathscr{E}_1$ est isomorphe à $\mathscr{E}_0/G_0$ et φ s'identifie à l'isogénie $\mathscr{E}_0 \to \mathscr{E}_0/G_0$. Ainsi, $\mathscr{E}_1$ est déterminée par $\mathscr{E}_0$.

Cette analyse faite, choisissons une courbe elliptique arbitraire $\mathscr{E}_0$ relevant E, soit G_0 le plus grand sous-schéma en groupes connexe de $\mathscr{E}_0[p]$, soit $\mathscr{E}_1$ le quotient de $\mathscr{E}_0$ par G_0 et soit $\varphi_0\colon \mathscr{E}_0 \to \mathscr{E}_1$ l'isogénie canonique. La courbe elliptique $\mathscr{E}_1$ relève la courbe ordinaire $E^{(\varphi)}$. Itérons le procédé. On en déduit une suite $(\mathscr{E}_n)$ de courbes elliptiques liées par des isogénies de degré p, $\varphi_i\colon \mathscr{E}_n \to \mathscr{E}_{n+1}$, dont le noyau, G_n, est le plus grand sous-schéma en groupes connexe de $\mathscr{E}_n[p]$.

Comme l'application $x \mapsto x^p$ est p-adiquement contractante, les sous-suites $(\mathscr{E}_{dn+j})$ sont convergentes dans la courbe modulaire. En particulier, les courbes $\mathscr{E}_{dn}$ convergent vers le relèvement canonique de E lorsque $n \to \infty$.

Une façon de le démontrer consisterait à utiliser le schéma formel des relèvements de la courbe E ([75, 79]), lequel s'identifie au schéma formel des relèvements de son groupe p-divisible. La théorie des coordonnées canoniques (qui s'appellent q d'ordinaire, mais que je noterai z ici) montre en effet qu'il est isomorphe au groupe multiplicatif formel sur W ; l'élément neutre correspond au relèvement canonique de la courbe E. Par ailleurs, les isogénies que nous considérons (ou plutôt les composées de d isogénies successives) ont pour effet d'élever à la puissance q la coordonnée canonique z essentiellement parce que l'élévation à la puissance q dans le groupe multiplicatif formel a pour noyau le schéma en groupes μ_q. Comme $|z-1|<1$, l'itération de l'application $z \mapsto z^q$ fournit une suite qui converge vers 1. On observe que la convergence n'est que linéaire.

Cette construction se généralise ainsi *mutatis mutandis* au cas des variétés abéliennes ordinaires — c'est le résultat principal du chapitre 2 de la thèse [18] de R. Carls.

Dans le cas des courbes elliptiques, son intérêt fut mis en évidence dans l'article [107] de Vercauteren, Preenel et Vandewalle, parce que sa considération améliore la complexité en espace de l'algorithme de Satoh. Toutefois, dans cet article, l'invariant j_{n+1} est calculé en appliquant une itération de l'algorithme de Newton à l'équation modulaire $\Phi_p(j, j_n) = 0$, l'inconnue étant j, le tout étant écrit à l'envers, car ces auteurs raisonnent, ainsi que Satoh, sur l'isogénie de Verschiebung.

3.2.4. Fin de l'algorithme. — Pour calculer explicitement sous forme d'une équation de Weierstrass (2.1) ces courbes $\mathscr{E}_n$ et les isogénies φ_n, on peut utiliser les formules de Vélu [108], voir aussi [18], th. 3.3.1.

Supposons donc la courbe $\mathscr{E}$ et l'isogénie φ explicitées et montrons comment terminer le calcul du cardinal de $E(\mathbf{F})$. Soit ω une base du W-module des formes différentielles invariantes sur $\mathscr{E}$. Il existe un unique élément $c \in W$ tel que $\varphi^*\omega^{(\sigma)} = c\omega$, et les formules de Vélu permettent d'ailleurs de le calculer aisément. Pour $i \in \{0, \dots, d-1\}$, on a donc $(\varphi^{(\sigma^i)})^*\omega^{(\sigma^{i+1})} = \sigma^i(c)\omega^{(\sigma^i)}$, si bien que

$$c_{\mathscr{E}} = c\sigma(c)\dots\sigma^{d-1}(c) = N_{K/\mathbf{Q}_p}(c) \tag{3.19}$$

est la norme de c dans l'extension $\mathbf{Q}_p \subset K$.

Si l'on ne connaît qu'une valeur approchée de c, disons modulo p^N, on en déduit une valeur de $c_{\mathscr{E}}$ modulo p^N, donc, via la formule (3.13), la valeur de t_E modulo p^{N-d}, la perte de précision étant due au fait que $c \equiv 0 \pmod{p}$. C'est pour pallier cet inconvénient que Satoh utilise l'isogénie duale ψ, dite *Verschiebung* ; comme E est ordinaire, ψ est séparable et la constante analogue c qui intervient dans le calcul de la trace est une unité de W.

Une fois calculé t_E modulo p^N, l'inégalité de Hasse $|t_E| \leqslant 2\sqrt{q}$ permet d'en déduire t_E si $p^N > 4\sqrt{q}$, c'est-à-dire si $N > \frac{d}{2}$, voire $\frac{d}{2}+2$ si $p=2$.

Décrivons rapidement la complexité de l'algorithme obtenu. Comme il faut calculer c modulo p^N, où $N = \mathrm{O}(d)$, et que la précision augmente de 1 à chaque itération, le nombre d'itérations à effectuer est $\mathrm{O}(d)$. Par ailleurs, la taille des objets à manipuler, des éléments de $(\mathbf{Z}/p^N\mathbf{Z})[x]/(f(x))$ dont la multiplication nécessite $\widetilde{\mathrm{O}}(Nd\log p)$

opérations, d'où une complexité de $\widetilde{\mathrm{O}}(d^2 \log p)$ opérations pour calculer c. Comme l'a remarqué HARLEY [55], les techniques efficaces pour calculer les résultants permettent de calculer la norme de c modulo p^N en $\widetilde{\mathrm{O}}(Nd \log p)$ opérations. Par suite, la complexité de l'algorithme de calcul de $|E(\mathbf{F})|$ suivant la méthode de SATOH est $\widetilde{\mathrm{O}}(d^2 \log p)$. Suite à [107], la complexité en espace est du même ordre.

Il convient de remarquer qu'elle n'est polynomiale en $\log q$ que si la caractéristique p du corps est fixe. Toutefois, pour les applications cryptographiques, on choisit souvent $p = 2$ et l'algorithme ainsi obtenu est très efficace. En 2002, FOUQUET, GAUDRY et HARLEY ont ainsi pu calculer le nombre de points d'une courbe elliptique sur un corps fini de cardinal $2^{8\,009}$ en environ 300 h de calcul ; le stockage des données a nécessité plus de 15 Go (voir [44]) !

3.2.5. Moyenne arithmético-géométrique. — La moyenne arithmético-géométrique $\mathrm{M}(a, b)$ de deux nombres réels, disons strictement positifs, a et b, est la limite commune des deux suites (a_n) et (b_n) définies par les relations de récurrence

$$a_{n+1} = \frac{a_n + b_n}{2}, \quad b_{n+1} = \sqrt{a_n b_n}, \tag{3.20}$$

et l'initialisation $a_0 = a$, $b_0 = b$. Ainsi que l'a découvert C.-F. GAUSS en 1799, elle est reliée aux intégrales elliptiques par les formules

$$\frac{\pi}{\mathrm{M}(a, b)} = 2 \int_0^{\pi/2} \frac{dt}{\sqrt{a^2 \cos^2 t + b^2 \sin^2 t}} = \int_0^\infty \frac{dx}{\sqrt{x(x + a^2)(x + b^2)}} \tag{3.21}$$

(changement de variables $x = b^2 \tan^2 t$) et permettent donc de calculer très rapidement les périodes de la courbe elliptique d'équation

$$y^2 = x(x + a^2)(x + b^2). \tag{3.22}$$

(L'autre période est obtenue en considérant la courbe tordue, d'équation $y^2 = x(x - a^2)(x - b^2)$, et fait intervenir $\mathrm{M}(a + b, a - b)$.) La raison d'être de la formule (3.21) est l'existence d'une isogénie de degré 2 entre la courbe elliptique précédente et celle d'équation

$$y^2 = x\big(x + (\frac{a + b}{2})^2\big)\big(x + ab\big). \tag{3.23}$$

Cette isogénie fournit un changement de variables dans l'intégrale elliptique qui ramène à une intégrale similaire où a et b sont remplacés par a_1 et b_1. Les suites (a_n) et (b_n) apparaissent ainsi comme un procédé simple pour calculer une suite d'isogénies de degré 2 particulières, en l'occurrence la seule fournissant une suite de courbes elliptiques dont les points d'ordre 2 sont tous définis sur $\mathbf{R}$.

En 2000, J.-F. MESTRE, voir [80], avait montré comment une variante 2-adique de la moyenne arithmético-géométrique permet de calculer efficacement relèvement canonique et nombre de points lorsque $p = 2$. L'algorithme AGM qui en résulte est essentiellement équivalent (mais antérieur !) à celui de SATOH modifié par VERCAUTEREN [107] ; son implémentation est cependant très aisée et son exécution plus rapide. GAUDRY, Harley, Lercier, Lubicz le mirent en œuvre fin 2002 dans des corps de très grand degré, le record semblant être détenu par Harley qui a pu calculer un tel cardinal $|E(\mathbf{F}_q)|$, pour $q = 2^{130\,020}$. (Un tel corps possède une base normale engendrée par une somme de Gauss, ce qui permet d'accélérer très notablement certains algorithmes.)

Profitons-en pour donner des formules.

Dans la suite, nous raisonnerons en fait sur la quantité $\xi = a/b$, dont le carré est l'invariant de Legendre de la courbe elliptique en question.

Dans ce paragraphe, supposons que $p = 2$ et que $q = p^d$, pour $d \geqslant 1$. Soit E une courbe elliptique ordinaire sur $\mathbf{F}_q$, donnée par une équation

$$y^2 + xy = x^3 + c \tag{3.24}$$

où $c \in \mathbf{F}^*$ est l'inverse de l'invariant j. (Ces courbes sont celles dont la 4-torsion est définie sur $\mathbf{F}_q$; on s'y ramène par une torsion quadratique.) Comme dans le cas complexe, le calcul de la moyenne arithmético-géométrique nécessite un choix de racines carrées ; pour tout $t \in W$ tel que $t \equiv 1 \pmod 8$, on note $\sqrt{t}$ l'unique élément de W congru à 1 modulo 4.

Soit ξ_4 un élément de W tel que $\xi_4 \equiv 1 + 8c \pmod{16}$. On définit alors une suite (ξ_n) par récurrence en posant, pour $n \geqslant 4$,

$$\xi_{n+1} = \frac{1 + \xi_n}{2\sqrt{\xi_n}}. \tag{3.25}$$

Pour $0 \leqslant i < d$, la suite (ξ_{dn+i}) converge vers un élément ξ_i^* dont le carré est l'invariant de Legendre de la courbe $\mathscr{E}_i = \mathscr{E}^{(\sigma^i)}$, $\mathscr{E}$ désignant le relèvement canonique de E. En outre, si l'on pose

$$\mu_n = \frac{2\xi_n}{1 + \xi_n} \quad \text{et} \quad t_n = \mu_n \sigma(\mu_n) \dots \sigma^{d-1}(\mu_n) = N_{K/\mathbf{Q}_2}(\mu_n), \tag{3.26}$$

on a pour tout entier $n \geqslant 0$ la congruence

$$q + 1 - |E(\mathbf{F})| = \operatorname{Tr}(\pi_E) \equiv t_n + \frac{q}{t_n} \pmod{2^n}, \tag{3.27}$$

d'où le calcul de $|E(\mathbf{F})|$ dès que $2^n > 4\sqrt{q}$, c'est-à-dire $n > \frac{1}{2}d + 2$.

3.2.6. Généralisation aux courbes de genre supérieur. — En 1836, Richelot a démontré l'existence d'un algorithme permettant de calculer les « intégrales hyperelliptiques de genre 2 », généralisant ainsi la formule (3.21). Comme dans le cas elliptique, ce théorème s'interprète en termes d'isogénies de surfaces abéliennes, voir [14]. Dans sa lettre [80], Mestre proposait d'utiliser ces relations de récurrence dans le cas 2-adique pour calculer le nombre de points d'une courbe de genre 2 définie sur un corps fini de caractéristique 2.

Dans [81], il reprend ce sujet en genre supérieur à l'aide des formules de duplication des fonctions θ. Elles permettent de calculer par un procédé itératif (convergeant ver la *moyenne de Borchardt*) un déterminant 2×2 formé à l'aide des périodes réelles d'une courbe hyperelliptique de genre 2 définie sur $\mathbf{R}$ dont les points de Weierstrass sont réels ;

l'initialisation de l'algorithme utilise les formules de Thomae (voir par exemple [85], chap. 3A, §8).

Mestre montre que cet algorithme est d'une grande utilité pour calculer le nombre de points d'une courbe hyperelliptique *ordinaire* sur un corps fini. Précisément, étant donnée une courbe C de genre 2 sur un corps fini $\mathbf{F}_q$, de caractéristique 2, cet algorithme, convenablement interprété dans l'anneau W des vecteurs de Witt, permet de calculer le relèvement $\mathscr{C}$ de C sur W dont la jacobienne $J_{\mathscr{C}}$ est le relèvement canonique de celle, J_C, de C. En outre, il fournit le déterminant de l'endomorphisme relevant celui de Verschiebung ψ_q agissant sur le W-module des formes différentielles globales de $\mathscr{C}$. Autrement dit, des quatre valeurs propres du frobenius $\pi_1, \dots, \pi_4$ on peut déterminer le produit $\pi_1\pi_2$ des deux qui sont inversibles modulo 2.

Cette dernière partie de l'algorithme, à savoir l'obtention du produit $\alpha = \pi_1 \dots \pi_g$ des valeurs propres $\pi_1, \dots, \pi_{2g}$ qui sont des unités 2-adiques, se généralise aux courbes hyperelliptiques ordinaires de tout genre g. Elle a en outre été étendue aux courbes de genre 3 non hyperelliptiques par Ritzenthaler [95] ; au lieu des points de Weierstrass qui apparaissent dans les formules de Thomae, il fait usage des bitangentes. Par contre, l'algorithme ne calcule pas le relèvement canonique de la jacobienne, pour la bonne raison que ce n'est pas forcément une jacobienne si $g \geqslant 4$.(2)

Une fois obtenu α, il n'est pas toujours possible d'en déduire les π_i, au moins lorsque $g \geqslant 4$. Mestre donne par exemple un exemple de variétés abéliennes de dimension 4 sur $\mathbf{F}_2$, ordinaires, non géométriquement isogènes et dont les invariants α sont égaux. Posons toutefois $\beta = \alpha + q^g\alpha^{-1}$ et considérons, à la suite de Mestre, le polynôme minimal P de β sur $\mathbf{Z}$ (calculé par exemple à l'aide d'une version 2-adique de l'algorithme LLL). Si P est de degré 2^{g-1}, ce qui arrive si par exemple la jacobienne J_C de C est simple, les racines de P sont les éléments

$$q^{|\complement I|}\frac{\prod_{i\in I}\pi_i}{\prod_{i\notin I}\pi_i} + q^{|I|}\frac{\prod_{i\notin I}\pi_i}{\prod_{i\in I}\pi_i}.$$

Cela permet de déterminer les π_i au signe près, d'où le cardinal de $J_C(\mathbf{F}_q)$ à une ambiguïté finie près. À l'opposé, si P est degré 1, c'est-à-dire si $\beta \in \mathbf{Z}$, alors J_C est géométriquement isogène à une puissance d'une courbe elliptique. Ces deux remarques permettent de démêler la situation lorsque $g = 2$ ou 3.

En genre 2, l'algorithme a été étudié et implémenté par Lercier et Lubicz [74] ; sa complexité est $\widetilde{\mathrm{O}}(n^2)$, tant en espace qu'en temps. Il leur a permis de calculer en quelques jours le cardinal de courbes de genre 2 sur un corps à $2^{32\,770}$ éléments, et de genre 3 sur un corps à $2^{4\,098}$ éléments. En genre 3, cette méthode a permis à Ritzenthaler (voir [95]) de calculer en deux semaines le nombre de points rationnels d'une courbe quartique plane (une courbe non hyperelliptique de genre 3) sur un corps de cardinal $2^{5\,002}$.

(2)Pour être précis, ce résultat n'est prouvé dans [36] que sous l'hypothèse que la caractéristique du corps est différente de 2...

3.3. Cohomologie de Monsky–Washnitzer

En 2001, K. Kedlaya [64] a proposé un algorithme calculant le nombre de points de courbes hyperelliptiques. Le rôle principal n'est plus tenu par la jacobienne de la courbe, comme dans les algorithmes précédents, mais par sa cohomologie de Monsky–Washnitzer dont Kedlaya montre qu'elle peut être calculée efficacement, au moins si la caractéristique du corps est petite.

Soit $\mathbf{F}$ un corps fini, de caractéristique p, de cardinal q. Soit W l'anneau des vecteurs de Witt de $\mathbf{F}$ et soit K son corps des fractions. Notons σ l'automorphisme de Frobenius sur $\mathbf{F}$, son relèvement à W et son extension à K ; si $q = p^d$, on a $\sigma^d = \mathrm{id}$.

3.3.1. Définition de la cohomologie de Monsky–Washnitzer. — Rappelons ce dont il s'agit, en renvoyant à [82, 7, 6, 94, 45, 70] pour plus de détails. Considérons une variété algébrique affine et lisse X définie sur $\mathbf{F}$. Le but est de définir une sorte de cohomologie de De Rham de X munie d'un endomorphisme de Frobenius induit par celui de X, de sorte à ce que la fonction zêta de X se calcule par une formule de Lefschetz. Le premier pas consiste à relever X en caractéristique 0.

D'après un théorème d'Elkik [41], il existe un W-schéma affine et lisse $\mathscr{X}$ dont la réduction modulo p est égale à X. Soit $\mathscr{X} \hookrightarrow \mathbf{A}^n_W$ une immersion fermée de $\mathscr{X}$ dans l'espace affine sur W, et soit $f_1, \dots, f_m \in W[x_1, \dots, x_n]$ des générateurs de l'idéal de $\mathscr{X}$. Si A désigne l'algèbre $W[x_1, \dots, x_n]/(f_1, \dots, f_m)$ de $\mathscr{X}$, on a donc un isomorphisme entre A/pA et l'anneau $\overline{A}$ des fonctions de X.

Notons $\Omega^*_{A/W}$ le complexe de De Rham de A ; le A-module $\Omega^1_{A/W}$ est engendré par des éléments $\mathrm{d}x_1, \dots, \mathrm{d}x_n$, liés par les relations $\mathrm{d}f_j = \sum_{i=1}^n \frac{\partial f_j}{\partial x_i} \mathrm{d}x_i = 0$; enfin, $\Omega^k_{A/W} = \bigwedge^k \Omega^1_{A/W}$. La cohomologie de ce complexe est assez pathologique, même si $\mathscr{X}$ est la droite affine ; en revanche, après tensorisation par K, on obtient d'après un théorème de Grothendieck [52] la cohomologie de De Rham de $\mathscr{X}_K$.

Toutefois, l'endomorphisme (semi-linéaire) de Frobenius de $\overline{A}$, $\varphi \mapsto x \mapsto x^p$, n'a en général pas de relèvement à A ; dans le cas des courbes elliptiques ordinaires, il aurait fallu avoir choisi précisément le relèvement canonique.

Introduisons alors la W-algèbre $W[x_1, \dots, x_n]^\dagger$ des séries formelles $f = \sum a_m x^m \in W[[x_1, \dots, x_n]]$ qui convergent dans un polydisque de rayon > 1, autrement dit, dont les coefficients a_m vérifient une inégalité de la forme $|a_m| \leqslant C\rho^{|m|}$, avec $\rho < 1$. Par définition, l'espace-dague $A^\dagger$, dit encore *complété faible*, de l'algèbre A est le quotient de l'algèbre $W[x_1, \dots, x_n]^\dagger$ par l'idéal engendré par les polynômes f_i. C'est un relèvement de l'anneau de X, au sens où $A^\dagger/pA^\dagger \simeq \overline{A}$. À isomorphisme près, il ne dépend que de la réduction modulo p de l'algèbre A, c'est-à-dire que de X. L'introduction de $A^\dagger$ permet en outre l'existence d'un relèvement semi-linéaire, noté φ, de l'endomorphisme de Frobenius de $\overline{A}$ à $A^\dagger$.

Le complexe de De Rham de l'algèbre $A^\dagger$ est le complexe $\Omega^*_{A^\dagger/W}$ des formes différentielles *surconvergentes*, donné par

$$\Omega^1_{A^\dagger/W} = \Omega^1_{A/W} \otimes_A A^\dagger, \qquad \Omega^k_{A^\dagger/W} = \bigwedge^k \Omega^1_{A^\dagger/W},$$

avec la différentielle évidente ; c'est un relèvement du complexe de De Rham de X. La cohomologie de Monsky–Washnitzer de X est alors définie par

$$H^i_{\mathrm{MW}}(X/K) = H^i(\Omega^*_{A^\dagger/W}) \otimes_W K. \tag{3.28}$$

L'action de l'endomorphisme φ de $A^\dagger$ induit un endomorphisme semi-linéaire bijectif de $H^i_{\mathrm{MW}}(X/K)$, c'est-à-dire que l'on a

$$\varphi(a\omega) = \sigma(a)\varphi(\omega), \qquad \text{pour } a \in K,\, \omega \in H^i_{\mathrm{MW}}(X/K), \tag{3.29}$$

Même si ce n'est pas évident sur leur définition, ces K-espaces vectoriels, de même que l'action de φ, ne dépendent que de X, et sont fonctoriels en X (la tensorisation par K est nécessaire à ce point).

Ils sont nuls pour $i < 0$ ou $i > \dim X$, de dimension finie (résultat dû indépendamment à Berthelot [9], Kedlaya [65] et Mebkhout [78]) et donnent lieu à une formule des traces de Lefschetz :

$$|X(\mathbf{F})| = \sum_{i=0}^{\dim X} (-1)^i q^{\dim X} \operatorname{Tr}(q^{\dim X} F_X^{-1} | H^i_{\mathrm{MW}}(X/K)), \tag{3.30}$$

où $F_X = \varphi^d$ est aussi induit par l'endomorphisme de Frobenius de X, donné par l'élévation à la puissance q sur le faisceau $\mathscr{O}_X$.

La définition a été étendue par P. Berthelot au cas des variétés algébriques générales sur $\mathbf{F}$, mais nous ne considérerons ici que celui de variétés lisses. Les espaces de cohomologie rigide $H^i_{\mathrm{rig}}(X/K)$ qu'il définit fonctoriellement sont des K-espaces vectoriels, munis d'un endomorphisme semi-linéaire bijectif « de Frobenius » φ (un σ-isocristal). Ils sont nuls pour $i < 0$ ou $i > 2\dim X$, de dimension finie, et donnent lieu à une formule des traces analogue à la précédente, si ce n'est que la somme va de $i = 0$ à $i = 2\dim X$.

L'apparition de $q^{\dim X} F_X^{-1}$ dans la formule (3.30) rappelle qu'il s'agit de cohomologie sans support ; Berthelot a aussi défini une cohomologie rigide à supports compacts, reliée dans le cas lisse à la cohomologie rigide par une dualité de Poincaré [8].

Lorsque X est affine et lisse, ses espaces de cohomologie rigide coïncident avec ceux définis par Monsky et Washnitzer. Par ailleurs, lorsque X est propre et lisse, sa cohomologie cristalline $H^i_{\mathrm{cris}}(X/W)$ définit un W-réseau de $H^i_{\mathrm{rig}}(X/K)$, stable par φ. Lorsque, de plus, X est la réduction modulo p d'un W-schéma propre et lisse $\mathscr{X}$, $H^i_{\mathrm{cris}}(X/W)$ s'identifie à la cohomologie de De Rham de $\mathscr{X}$, définie comme l'hypercohomologie du complexe de De Rham $\Omega^*_{\mathscr{X}}$.

Plus généralement, soit $\mathscr{X}^*$ un W-schéma propre et lisse, soit $\mathscr{Y}$ un diviseur de Cartier relatif de $\mathscr{X}^*$ lisse sur W (voire à croisements normaux stricts) et supposons que $\mathscr{X} = \mathscr{X}^* \setminus \mathscr{Y}$. Notons X^*, Y, X les réductions de $\mathscr{X}^*$, $\mathscr{Y}$ et $\mathscr{X}$. Par un théorème de Baldassarri et Chiarellotto [5], la cohomologie de De Rham algébrique

$H^i_{\mathrm{dR}}(\mathscr{X}_K/K)$ et la cohomologie rigide $H^i_{\mathrm{rig}}(X/K)$ sont des K-espaces vectoriels isomorphes (voir aussi [21] où il est montré que l'isomorphisme construit précédemment est compatible aux poids). Si, de plus, $\mathscr{X}$ est affine, d'anneau A, sa cohomologie rigide $H^i_{\mathrm{rig}}(X/K) = H^i_{\mathrm{MW}}(X/K)$, définie comme la cohomologie du complexe $\Omega^*_{A^\dagger/W} \otimes K$, est donc égale à la cohomologie du complexe $\Omega^*_{A/W} \otimes K$. En outre, d'après un théorème de Atiyah et Hodge ([59], voir aussi [26, 28]), on a alors un isomorphisme entre la cohomologie de De Rham de $\mathscr{X}^*_K$ à pôles logarithmiques le long de $\mathscr{Y}_K$ et la cohomologie de De Rham de $\mathscr{X}_K$:

$$H^i_{\mathrm{dR}}((\mathscr{X}^*, \mathscr{Y})) \otimes_W K \simeq H^i_{\mathrm{dR}}(\mathscr{X} \otimes_W K), \tag{3.31}$$

d'où un moyen concret, ne faisant intervenir qu'un complexe de K-espaces vectoriels de dimensions finies, pour calculer la cohomologie rigide de X.

Sous ces hypothèses, la cohomologie log-cristalline du couple (X^*, Y) et la cohomologie de De Rham à pôles logarithmiques $H^i_{\mathrm{dR}}((\mathscr{X}^*, \mathscr{Y}))$ sont des W-modules canoniquement isomorphes. Ils définissent un W-réseau de la cohomologie rigide $H^i_{\mathrm{rig}}(X/K)$, [101], munissant ainsi la cohomologie rigide d'une structure entière naturelle, stable par le frobenius ; cela peut être utile pour les calculs effectifs. Dans la suite, nous qualifierons cette situation géométrique de « bien relevée ».

La cohomologie cristalline des variétés propres et lisses sur $\mathbf{F}$ est une cohomologie de Weil. D'après [63], les espaces de cohomologie cristalline d'une telle variété X ont même dimension que les espaces correspondants en cohomologie ℓ-adique (pour $\ell \neq p$) et le polynôme caractéristique de F_X agissant sur $H^i_{\mathrm{cris}}(X/W) \otimes K$ est le même (avec les notations du paragraphe 2.3.1) que celui de φ agissant sur $H^i_c(\overline{X}, \mathbf{Q}_\ell)$. En particulier, $\mathrm{Tr}(F_X | H^i_{\mathrm{rig}}(X/K))$ est un entier et il vérifie la majoration

$$|\mathrm{Tr}(F_X | H^i_{\mathrm{rig}}(X/K))| \leqslant q^{i/2} \dim_K H^i_{\mathrm{rig}}(X/K). \tag{3.32}$$

D'après [20], cette majoration vaut encore (de même bien sûr que sa grande cousine ℓ-adique, établie par Deligne [31]) lorsque X est seulement supposé lisse sur $\mathbf{F}$.

3.3.2. Principe de l'algorithme de Kedlaya. — Soit X une variété algébrique définie sur $\mathbf{F}$. Pour calculer le cardinal de $X(\mathbf{F})$, Kedlaya suggère de calculer les polynômes caractéristiques du frobenius agissant sur la cohomologie rigide de X et d'en déduire $|X(\mathbf{F})|$ par la formule des traces de Lefschetz.

Supposons que l'on soit dans une situation géométrique bien relevée et que $\mathscr{X}$ soit un sous-schéma fermé de l'espace affine de dimension n, donné par des générateurs $(f_1, \ldots, f_m)$ de son idéal dans $W[x_1, \ldots, x_n]$. Notons A l'anneau de $\mathscr{X}$ et $A^\dagger$ son complété faible. L'algorithme de Kedlaya est le suivant.

a) Calculer le relèvement φ du frobenius sur $A^\dagger$, c'est-à-dire donner un algorithme pour calculer l'image d'un élément donné à une précision p-adique arbitraire. Compte tenu de la condition de surconvergence imposée aux séries, un tel algorithme ne manipule que des polynômes ;

b) Calculer des formes différentielles sur $\mathscr{X}$ dont les classes forment une base de la cohomologie de De Rham de $\mathscr{X}_K$ (il est judicieux, mais pas nécessaire, de choisir des formes différentielles entières, au sens où leur classe de cohomologie appartient à la cohomologie log-cristalline) ;
c) La cohomologie de Monsky–Washnitzer de X est celle du complexe $\Omega^*_{A^\dagger/W} \otimes K$ des formes différentielles surconvergentes, mais les classes des formes différentielles algébriques précédemment calculées en forment une base ; Donner un algorithme « de réduction » calculant à une précision p-adique arbitraire la classe de cohomologie d'une forme fermée surconvergente (connue à une précision suffisante) ;
d) En déduire une approximation p-adique de la matrice M de l'endomorphisme semilinéaire φ de $H^k_{\mathrm{MW}}(X/K)$, pour $0 \leqslant k \leqslant \dim X$. Le point délicat est que la primitive d'une forme exacte à coefficients entière peut faire apparaître des dénominateurs (exemple : $x^{p-1}\,\mathrm{d}x$), si bien que la structure entière de $\Omega^1_{A^\dagger}$ n'induit pas sur $H^k_{\mathrm{MW}}(X/K)$ sa structure entière donnée par la cohomologie cristalline (lemme 2 de [64], voir aussi le th. 2.2.5 de [1] pour un énoncé général) ;
e) En déduire une approximation p-adique de la matrice $M\sigma(M)\dots\sigma^{d-1}(M)$, de l'endomorphisme K-linéaire $F_X = \varphi^q$ de $H^k_{\mathrm{MW}}(X/K)$, puis de sa trace ;
f) Compte tenu de l'inégalité (3.32), on peut en déduire la trace elle-même, puis éventuellement $|X(\mathbf{F})|$, si la précision atteinte à l'étape précédente est suffisante.

3.3.3. Le cas des courbes hyperelliptiques. — La méthode que nous venons d'esquisser est susceptible de s'appliquer dans des situations très générales, mais une présentation détaillée ne semble disponible dans la littérature que pour les courbes et le complémentaire d'une hypersurface de $\mathbf{P}^3$. Nous considérons ci-dessous le cas des courbes hyperelliptiques qui faisait l'objet de l'article initial de Kedlaya [64] lorsque $p > 2$ et que Denef et Vercauteren [33] ont étendu au cas $p = 2$; voir aussi [106, 38].

Soit X^* une courbe hyperelliptique définie sur $\mathbf{F}$. C'est un revêtement double de la droite projective ; les points de ramification de ce revêtement sont appelés *points de Weierstrass* ; notons w leur nombre. Si $p \neq 2$, on a $w = 2g + 2$, mais si $p = 2$, toute valeur de w telle que $1 \leqslant w \leqslant g + 1$ est possible.

Soit Y l'ensemble des points de Weierstrass et posons $X = X^* \setminus Y$. De la cohomologie rigide de X, X^*, Y, on sait un certain nombre de choses

– on a $H^0_{\mathrm{rig}}(X/K) = H^0_{\mathrm{rig}}(X^*/K) = K$, les endomorphismes de Frobenius étant donnés par σ ;
– l'espace $H^0_{\mathrm{rig}}(Y/K)$ est la somme des espaces $H^0_{\mathrm{rig}}(P/K)$, où P parcourt les points de Y ; en outre, si P est de degré d sur $\mathbf{F}$, $H^0_{\mathrm{rig}}(P/K)$ s'identifie à l'extension non ramifiée de degré d de K munie de son endomorphisme de Frobenius ;
– on a $H^2_{\mathrm{rig}}(X^*/K) = K$ et le frobenius est donné par $p\sigma$.

De la suite exacte de localisation pour la cohomologie rigide à supports compacts et de la dualité de Poincaré, on déduit alors une suite exacte

$$0 \to H^1_{\mathrm{rig}}(X^*/K) \to H^1_{\mathrm{rig}}(X/K) \to H^0_{\mathrm{rig}}(Y/K)(-1) \to H^2_{\mathrm{rig}}(X^*/K) \to 0. \tag{3.33}$$

En outre, les morphismes de cette suite exacte commutent aux frobenius, le (-1) au milieu de cette formule signifiant que le frobenius de $H^0_{\mathrm{rig}}(Y/K)$ est multiplié par p. Par ailleurs, l'involution hyperelliptique ε agit sur ces espaces de cohomologie et les découpe en une partie paire et une partie impaire, notées respectivement d'un symbole $+$ et $-$, donnant lieu à une suite exacte

$$0 \to H^1_{\mathrm{rig}}(X/K)^+ \to H^0_{\mathrm{rig}}(Y/K)(-1) \to H^2_{\mathrm{rig}}(X^*/K) \to 0 \tag{3.34}$$

(car $H^1_{\mathrm{rig}}(X^*/K)^+ \simeq H^1_{\mathrm{rig}}(\mathbf{P}^1/K) = 0$) et un isomorphisme

$$H^1_{\mathrm{rig}}(X^*/K)^- \simeq H^1_{\mathrm{rig}}(X/K). \tag{3.35}$$

Il s'agit donc de calculer $H^1_{\mathrm{rig}}(X/K)^-$.

Les références ci-dessus ne traitent en fait que le cas où l'un des points de Weierstrass est rationnel. Dans ce cas, la courbe X^* possède une équation plane de la forme (affine)

$$y^2 = f(x), \qquad f \in \mathbf{F}[x], \quad \deg(f) = 2g+1 \tag{3.36a}$$

si $p \neq 2$; lorsque $p = 2$, elle a une équation du type

$$y^2 + f(x)y = g(x), \qquad \deg(f) \leqslant g, \quad \deg(g) = 2g+1. \tag{3.36b}$$

Avec ces équations, l'involution hyperelliptique est donnée par $(x,y) \mapsto (x,-y)$, resp. $(x,y) \mapsto (x, -f(x) - y)$; la projection vers $\mathbf{P}^1$ est donnée par l'application $(x,y) \mapsto x$; elle applique le point de Weierstrass choisi sur le point à l'infini de $\mathbf{P}^1$. Les autres points de Weierstrass sont ceux de coordonnées (x,y) tels que $f(x) = 0$. Lorsque $p \neq 2$, ce sont ceux d'ordonnée nulle ; lorsque $p = 2$, l'application d'une transformation convenable de la forme $(x,y) \mapsto (x, y + \alpha(x))$ permet de supposer que g s'annule en chacun de ces points ; leur ordonnée est encore nulle. Soit h le produit des facteurs irréductibles de f ; le diviseur de h est étale sur $\mathbf{F}$ et, au point à l'infini près, a pour support les points de Weierstrass de X^*.

Soit $\overline{B}$ l'anneau $\mathbf{F}[x, h(x)^{-1}]$; l'anneau $\overline{A}$ de la courbe affine X est un $\overline{B}$-module libre de rang 2, de base $(1, y)$, y vérifiant l'équation (3.36a) si $p \neq 2$, resp. (3.36b) si $p = 2$. En particulier, $\overline{A}$ est étale sur $\overline{B}$.

Lorsque $p \neq 2$, choisissons un relèvement $\widetilde{f}$ de f dans l'anneau $W[x]$ de même degré que f et posons $\widetilde{h} = \widetilde{f}$. L'équation analogue à (3.36a) définit une courbe hyperelliptique $\mathscr{X}^*$ de genre g qui relève la courbe X^* ; le schéma $\mathscr{Y}$ des points de Weierstrass de $\mathscr{X}^*$ est étale sur W et la W-courbe affine $\mathscr{X} = \mathscr{X}^* \setminus \mathscr{Y}$ relève X. Notons B l'anneau $W[x, \widetilde{f}(x)^{-1}]$; l'anneau A de $\mathscr{X}$ est égal à $B[y]/(y^2 - \widetilde{f})$ et est étale sur B.

Lorsque $p = 2$, le diviseur des points de Weierstrass d'une courbe $\mathscr{X}^*$ qui relève X^* n'est jamais étale sur W ; il convient alors de choisir un point de Weierstrass par classe résiduelle. De manière précise, Denef et Vercauteren commencent par relever h en un polynôme $\widetilde{h}$ de même degré puis exigent que chaque facteur irréductible de $\widetilde{h}$ divise $\widetilde{f}$ et $\widetilde{g}$ avec la même multiplicité que celle dont le facteur irréductible correspondant de h divise respectivement f et g. En particulier $\widetilde{g}$ s'annule en toute racine de $\widetilde{f}$. L'équation analogue à (3.36b) définit alors une courbe hyperelliptique $\mathscr{X}^*$ de genre g qui relève la courbe X^* ; notons $\mathscr{Y}$ la réunion du point à l'infini et du lieu défini par le polynôme $\widetilde{h}$.

C'est un sous-schéma étale de $\mathscr{X}^*$ dont la réduction modulo p a pour support l'ensemble des points de Weierstrass de $\mathscr{X}^*$. Posons $\mathscr{X} = \mathscr{X}^* \setminus \mathscr{Y}$. Posons $B = W[x, \widetilde{h}(x)^{-1}]$; l'anneau A de $\mathscr{X}$ est $B[y]/(y^2 + \widetilde{f}y - \widetilde{g})$.

Dans les deux cas, l'anneau $B^\dagger$ peut être décrit explicitement, comme un anneau de séries en x et $\widetilde{h}(x)^{-1}$ dont les coefficients tendent assez vite vers 0. L'anneau $A^\dagger$ est alors une $B^\dagger$-algèbre étale, libre de rang 2, de base $(1, y)$. Pour $p = 2$, ce sont les mêmes anneaux que ceux qu'on aurait obtenu en remplaçant $\mathscr{Y}$ par le sous-schéma des points de Weierstrass.

Pour relever le frobenius, nous commençons par choisir sur l'anneau $W[x]$ l'unique relèvement σ-linéaire tel que $x \mapsto x^p$, autrement dit $\sum a_n x^n \mapsto \sum \sigma(a_n) x^{pn}$. Comme A est étale sur $W[x]$, cet homomorphisme s'étend de manière unique en un homomorphisme σ-linéaire, noté φ, de $A^\dagger$ dans lui-même. Même si cela résulte d'une variante due à Bosch [13], du théorème d'approximation d'Artin pour les anneaux de séries surconvergentes, nous devons calculer φ explicitement, et en particulier déterminer l'élément $\varphi(y)$ de $A^\dagger$ qui relève y^p et tel que $\varphi(y)^2 = \widetilde{f}^\sigma(x^p)$ lorsque $p \neq 2$ et $\varphi(y)^2 + \widetilde{f}^\sigma(x^p)\varphi(y) - \widetilde{g}^\sigma(x^p)$ si $p = 2$. Supposons d'abord $p \neq 2$; il existe un élément $h \in W[x]$ tel que $\widetilde{f}^\sigma(x^p) = (\widetilde{f}(x))^p + ph(x)$, car σ relève l'automorphisme de Frobenius de $\mathbf{F}$. On pose alors

$$\varphi(y) = y^p \left(1 + p\frac{h(x)}{\widetilde{f}(x)^p}\right)^{1/2} = y^p \sum_{k=0}^{\infty} \binom{1/2}{k} p^k \frac{h(x)^k}{\widetilde{f}(x)^{pk}}. \tag{3.37}$$

La présence des coefficients p^k permet d'analyser très facilement la convergence de cette série. En particulier, l'élément $\varphi(y)$ écrit appartient à $A^\dagger$ et vérifie l'équation considérée. Dans le cas $p = 2$, le principe est similaire : comme on a pris soin de placer les points de Weierstrass sur l'axe $y = 0$, y est inversible dans $A^\dagger$ et on peut chercher $\varphi(y)$ sous la forme $y^p u$, avec $u \equiv 1 \pmod{p}$; je renvoie à [33], lemma 1, pour les détails. Signalons aussi qu'en pratique, $\varphi(y)$ n'est pas calculé en développant des séries entières mais en appliquant la méthode de Newton.

Comme $\widetilde{Y}$ est étale sur W, le théorème de comparaison entre cohomologies de De Rham algébrique et cohomologie rigide évoqué plus haut entraîne que $H^1_{\mathrm{MW}}(X/K)$ s'identifie au premier groupe de cohomologie de De Rham de $X \otimes K$.[(3)] Il en est de même de la partie $-$, ce qui montre que $H^1_{\mathrm{MW}}(X/K)^-$ admet pour base les classes $[x^i y^{-1} \mathrm{d}x]$, pour $0 \leqslant i \leqslant 2g-1$. Comme l'algorithme final n'utilisera qu'une précision finie, il est de toutes façons nécessaire de contrôler la valeur absolue des coefficients des différentielles exactes mises en jeu par une telle identification. L'« algorithme de réduction » permet d'écrire une forme différentielle fermée surconvergente à coefficients entiers ω comme somme de deux termes : d'une part une combinaison linéaire explicite des formes différentielles qui constituent la base de $H^1_{\mathrm{MW}}(X/K)$, d'autre part une forme

(3) C'est là qu'intervient le choix de $\mathscr{Y}$ en caractéristique 2 : il ne fallait pas enlever tous les points de Weierstrass de la courbe hyperelliptique $\mathscr{X}$, mais seulement un par point de Weierstrass de la fibre spéciale.

reste dont un multiple explicite est la différentielle d'une forme différentielle surconvergente à coefficients entiers.

Supposons ces deux points acquis et soit $i \in \{0, \ldots, 2g-1\}$. Pour calculer l'image par φ de la classe de la forme différentielle $\omega_i = x^i y^{-1}\mathrm{d}x$, il reste à effectuer les calculs suivants :

– développer en série la forme différentielle

$$\begin{aligned}\varphi(\omega_i) &= \varphi(x)^i \varphi(y)^{-1}\mathrm{d}\varphi(x) = px^{pi+p-1}\varphi(y)^{-1}\mathrm{d}x \\ &= px^{pi+p-1}\widetilde{f}(x)^{-(p-1)/2)}\left(1+p\frac{h(x)}{\widetilde{f}(x)^p}\right)^{1/2} y^{-1}\mathrm{d}x,\end{aligned} \tag{3.38}$$

à une précision p-adique suffisante ;

– écrire le terme principal comme une somme de deux termes : le premier est une combinaison linéaire des formes différentielles ω_k, pour $0 \leqslant k \leqslant 2g-1$, le second (qu'en fait on n'écrit pas) est une forme différentielle dont un multiple explicite est une forme exacte ;

– de même, l'image du terme reste dans la cohomologie sera alors combinaison linéaire des classes ω_i avec des coefficients p-adiquement petits.

Si la précision a été choisie assez grande, on en déduit une approximation de l'image de $[\omega_i]$ par φ, donc une approximation de la matrice M de φ. La matrice de $F_X = \varphi^d$ est, quant à elle, donnée par $M\sigma(M)\ldots\sigma^{d-1}(M)$. Pour finir, si la précision est suffisante, on peut calculer la trace de F_X (donc le cardinal de $X(\mathbf{F})$) et le déterminant de $1-tF_X$ (donc la fonction zêta de X).

3.3.4. Complexité et généralisations. — La complexité de l'algorithme que nous avons grossièrement décrit dépend de la précision requise pour effectuer les calculs ; je renvoie aux articles cités ainsi qu'à [49] pour l'analyse de cette complexité. Lorsque $p \neq 2$, il en ressort qu'elle est $\widetilde{\mathrm{O}}(pg^4d^3)$ en temps et $\widetilde{\mathrm{O}}(pg^3d^3)$ en espace. (Rappelons que $q = p^d$.) Lorsque $p = 2$, la complexité est un peu moins bonne en temps, à savoir $\widetilde{\mathrm{O}}(g^5d^3)$. Tout récemment, des idées remontant aux Chudnovsky ont permis de faire baisser la dépendance en p de linéaire à $\sqrt{p}$ (voir [56], ainsi que [15]).

En pratique, l'algorithme de Kedlaya a permis de calculer le cardinal de courbes hyperelliptiques de genres $\leqslant 4$ en quelques minutes ; le produit $gd\log_2 p$ (approximativement égal au logarithme en base 2 du cardinal de la jacobienne) étant de l'ordre de 200 ($p = 2$, [33] ; $p = 251$, [49]).

Par ailleurs, il a donné lieu à un certain nombre de généralisations : courbes superelliptiques ($y^m = f(x)$, [48]), courbes $C_{a,b}$ (revêtements de $\mathbf{P}^1$ totalement ramifiés à l'infini) dans [32], etc. Pour les courbes, l'algorithme le plus général semble celui de Castryck, Denef et Vercauteren dans [19] qui concerne les courbes planes qui sont non dégénérées par rapport à leur polytope de Newton ; si p est fixé, la complexité en temps de cet algorithme est $\widetilde{\mathrm{O}}(d^3g^{6,5})$, celle en espace est $\widetilde{\mathrm{O}}(d^3g^4)$.

Enfin, l'article [1] utilise cette méthode de calcul de la cohomologie p-adique pour évaluer le rang du nombre de Picard de surfaces projectives lisses, ces deux quantités étant reliées par une conjecture de Tate qui relie le rang du groupe de Néron-Severi d'une surface projective lisse S définie sur $\mathbf{F}$ à la multiplicité de la valeur propre q de l'endomorphisme F_S sur $H^2_{\mathrm{rig}}(X/K)$. (Pour démontrer une majoration du nombre de Picard, la conjecture de Tate n'est bien sûr pas nécessaire.)

3.4. Variation de la cohomologie p-adique

La complexité en temps des méthodes p-adiques décrites jusqu'ici est toujours exponentielle en la dimension de l'espace ambiant. Le dernier algorithme de ce texte, introduit par Lauder [67] en 2002, vise à supprimer ce défaut en tirant parti de la variation de la cohomologie p-adique dans une famille, longuement étudiée par Dwork dans les années 60.

Plusieurs incarnations de cet algorithme sont actuellement disponibles : l'article original de Lauder [67], rédigé dans le cadre de la théorie de Dwork, concerne les familles d'hypersurfaces dont un membre est une hypersurface diagonale. Indépendamment, N. Tsuzuki [104] a proposé un algorithme qui calcule des sommes de Kloosterman et le nombre de points des revêtements d'Artin-Scheier de $\mathrm{G_m}$. R. Gerkmann [51] dans le cas des courbes elliptiques, puis H. Hubrechts (voir [61, 62, 60] ainsi que l'esquisse [68]) pour les courbes hyperelliptiques, ont utilisé cette méthode et proposé un algorithme calculant le cardinal d'une telle courbe, de genre g, définie sur un corps fini de cardinal p^d, dont la complexité en espace est $\widetilde{\mathrm{O}}(pd^2g^4)$; cela améliore l'algorithme de Kedlaya par rapport au paramètre d. Ces derniers algorithmes sont rédigés en termes de cohomologie rigide ou Monsky–Washnitzer.

Même si la portée de cet algorithme est bien plus générale, je me contente ici d'en esquisser le principe dans le cas d'une famille de courbes. On reprend les notations $\mathbf{F}$, q, p, W et K.

3.4.1. La déformation. — Le but de l'algorithme est de calculer la fonction zêta d'une courbe X_1, ou plus simplement le cardinal de $X_t(\mathbf{F})$, lorsque X_t est la fibre en un point t d'une famille de courbes paramétrée par un ouvert U de $\mathbf{A}^1$. On peut imaginer par exemple une famille de courbes hyperelliptiques donnée par une équation hyperelliptique

$$X_t \colon y^2 = f_t(x),$$

où $f_t \in \mathbf{F}[x,t]$ est de degré $2g+1$ en x, $\mathbf{F}$ étant un corps fini de cardinal q. Dans ce cas, on notera U le plus grand ouvert de $\mathbf{A}^1$ au-dessus duquel f_t est séparable et de degré $2g+1$; son complémentaire est le lieu défini par le discriminant $D(t)$ de f_t. Si l'on s'intéresse à des courbes affines, il est prudent de considérer une famille propre et lisse $u\colon X^* \to U$, un diviseur Y étale sur U, puis de poser $X = X^* \setminus Y$. Pour $t \in U$, X^*_t, Y_t, X_t désignent les fibres de X^*, Y, X au-dessus de t.

L'algorithme de déformation repose sur le fait que lorsque t varie (en un certain sens), les matrices de Frobenius de $H^1_{\mathrm{rig}}(X_t/K)$ vérifient une équation différentielle. L'idée de Lauder est de partir de la matrice en un point $t = 0$, supposée déjà calculée par une autre méthode, et de résoudre cette équation différentielle pour arriver au point t.

Il y a en cohomologie rigide une notion d'image directe et les K-espaces vectoriels de cohomologie rigide $H^1_{\mathrm{rig}}(X_t, K)$, pour $t \in U$, sont (en un certain sens que nous préciserons plus bas) les fibres d'un objet $R^1(u_{\mathrm{rig}})_*(X/\mathbf{P}^1)$ (cohomologie rigide relative) qui est, au moins conjecturalement[(4)], un F-isocristal surconvergent sur U. Pour en donner une description concrète, on suppose toute la situation bien relevée en caractéristique 0 en se donnant un ouvert $\mathscr{U}$ de $\mathbf{P}^1_W$, complémentaire d'un W schéma étale d'équation $\widetilde{D}(t) = 0$, une famille propre et lisse $u\colon \mathscr{X}^* \to \mathscr{U}$ et un diviseur $\mathscr{Y}$ de $\mathscr{X}^*$, étale sur $\mathscr{U}$.

Notons S l'anneau $W[t, \widetilde{D}(t)^{-1}]$ et $S^\dagger$ son complété faible ; soit σ l'endomorphisme semi-linéaire de S qui applique t sur t^p. Identifions les éléments de $S^\dagger_K$ à des séries formelles en t ; alors, si $f \in S^\dagger_K$, $\sigma(f(t)) = f^\sigma(t^p)$, où f^σ est la série formelle obtenue en appliquant σ aux coefficients de f.

Alors, $R^1(u_{\mathrm{rig}})_*(X/\mathbf{P}^1)$ est un $S^\dagger_K$-module E, libre de rang $m = 2g - 1 + r$ (où g est le genre de X^*_t et r le nombre de points géométriques de Y_t, c'est la version en famille de (3.34)), muni d'une connexion

$$\nabla\colon E \to E \otimes_{S^\dagger} \Omega^1_{S^\dagger_K} \tag{3.39}$$

et d'un isomorphisme horizontal $\varphi\colon \sigma^* E \simeq E$. En outre, pour tout $t \in \mathbf{F}$, de relèvement de Teichmüller $\widetilde{t} \in W$ considéré comme un homomorphisme d'anneaux $S^\dagger_K \to K$, $E \otimes_{\widetilde{t}} K$ s'identifie à $H^1_{\mathrm{rig}}(X_t/K)$ et $\varphi \otimes_{\widetilde{t}} 1$ s'identifie à l'endomorphisme de Frobenius de la cohomologie rigide (noter que $\sigma(\widetilde{t}) = \widetilde{t}^p$). La connexion ∇ est bien sûr un avatar de la connexion de Gauss-Manin en cohomologie de De Rham (et devrait être la même lorsqu'on dispose d'un théorème de comparaison d'images directes entre cohomologie de De Rham et cohomologie rigide).

Fixons une base $(e_1, \dots, e_m)$ de E et soit $G(t)\mathrm{d}t$ la matrice de ∇ dans cette base ; on a donc, pour tout vecteur colonne $X(t)$ à coefficients dans $S^\dagger_K$,

$$\nabla\big((e_1, \dots, e_m)X(t)\big) = (e_1, \dots, e_m)(G(t)X(t) + \frac{\mathrm{d}X(t)}{\mathrm{d}t})\,\mathrm{d}t. \tag{3.40}$$

Soit aussi $F(t)$ la matrice de φ dans les bases $(e_i \otimes 1)$ et (e_i) ; on a ainsi

$$\varphi\big((e_1, \dots, e_m)X(t) \otimes 1\big) = (e_1, \dots, e_m)(F(t)X^\sigma(t^p)) \tag{3.41}$$

et l'horizontalité de φ se traduit par l'équation différentielle

$$F'(t) + G(t)F(t) = F(t)G^\sigma(t^p)pt^{p-1}. \tag{3.42}$$

3.4.2. Résolution et surconvergence. — Soit $X(t)$ une matrice fondamentale de l'équation différentielle homogène

$$X'(t) + G(t)X(t) = 0, \qquad X(0) = \mathrm{I}_m. \tag{3.43}$$

(4) Avec les hypothèses imprécises ci-dessus, c'est vraisemblable, mais je ne l'ai pas vérifié en détail ; dans le cas, présenté plus bas, des courbes hyperelliptiques, cela résulte de l'étude explicite faite par Hubrechts.

Ses coefficients sont des séries formelles à coefficients dans K. La démonstration du théorème de Cauchy fait apparaître des dénominateurs ; par exemple, le rayon de convergence p-adique de la série exponentielle, solution de $y' = y$ n'est que $p^{-1/(p-1)}$. Toutefois, une astuce due à DWORK reposant sur la formule (3.44) ci-dessous montre que le rayon de convergence de $X(t)$ est égal à 1, de sorte que $X(t)$ converge dans le disque unité *ouvert*.

Par horizontalité de φ, l'image de $(e_1, \dots, e_m)X(t) \otimes 1$ par φ est annulée par ∇ ; il existe donc une matrice *constante* C telle que l'on ait $F(t)X^\sigma(t^p) = X(t)C$, d'où $F(0) = C$ et

$$F(t) = X(t)F(0)X^\sigma(t^p)^{-1}. \tag{3.44}$$

Ayant calculé $X(t)$, on peut tout autant calculer $F(t)$, pourvu que la matrice $F(0)$ ait été calculée auparavant, c'est-à-dire que l'on connaisse l'action du frobenius sur la cohomologie du membre X_0 de notre famille. Ce n'est a priori qu'une série formelle à coefficients dans K, de même rayon de convergence que $X(t)$.

Mais $F(t)$ est bien plus : c'est une matrice à coefficients dans $S_K^\dagger$. Ce fait général, qui traduit la « surconvergence » de l'isocristal $R^1(u_{\mathrm{rig}})_*(X/\mathbf{P}^1)$ était déjà apparu dans cet exposé : la série θ de l'équation (3.4) dont on avait mentionné la décroissance vers 0 des coefficients est celle qui correspond à l'isocristal de Dwork sur la droite affine (voir par exemple [6], p. 28-29).

Puisque le développement en série formelle en l'origine définit un homomorphisme *injectif* de $S_K^\dagger$ dans $K[[t]]$, on peut exprimer de manière unique chaque entrée de la matrice $F(t)$ comme une série de la forme

$$f(t) = \sum_{n=-\infty}^{\infty} f_n \widetilde{D}(t)^n, \tag{3.45}$$

où les f_n sont des polynômes de degrés $< \deg \widetilde{D}$ dont les coefficients tendent rapidement vers 0 lorsque $|n| \to \infty$.

Supposons pour l'instant que l'on ait réussi à écrire les entrées de la matrice $F(t)$ sous cette forme. Si $t \in \mathbf{F}$ est un point de U, on peut alors évaluer F en le relèvement de Teichmüller $\widetilde{t}$ de t, car $|t| = |\widetilde{D}(t)| = 1$, d'où une matrice $F(\widetilde{t})$ qui est celle du frobenius agissant sur la cohomologie rigide de la fibre X_t.

Il reste à expliquer comment l'on peut calculer les f_n. Dans le cas spécifique d'une famille de courbes hyperelliptiques, HUBRECHTS fait dans [62] toute l'analyse précédente en grand détail, et de manière explicite ; il prouve de fait la surconvergence de l'isocristal $R^1(u_{\mathrm{rig}})_*(X/\mathbf{P}^1)$ en établissant une minoration explicite des valuations p-adiques des coefficients des polynômes f_n. Il peut alors considérer l'équation (3.45) comme un système d'équations linéaires à coefficients dans K. En chassant les dénominateurs et en se limitant à une précision p-adique donnée, on obtient un système linéaire en dimension finie dont on peut calculer une solution ; la précision obtenue est inférieure à la précédente car le système n'est pas inversible modulo p.

Ainsi, Hubrechts est en mesure de prévoir quelle précision initiale est nécessaire dans tout ce calcul pour, *in fine*, obtenir les entrées de la matrice $F(t)$ à une précision suffisante pour que la congruence qui en résultera sur la fonction zêta permette de la déterminer.

En pratique, plutôt que de calculer une solution fondamentale $X(t)$ de (3.43), puis $G(t)$ par la formule (3.44), Hubrechts donne des algorithmes itératifs efficaces pour résoudre directement des équations différentielles du type (3.42).

Pour les courbes elliptiques, l'algorithme ainsi décrit est moins rapide que l'agm, ce dernier étant cependant restreint en pratique au cas $p = 2$. Selon les données présentées à la fin de [62], l'algorithme est plus rapide que l'algorithme sea lorsque le degré est au moins 100 si $p = 3$, et 40 si $p = 7$. Le dénombrement d'une courbe elliptique sur un corps de cardinal 3^{500} nécessite un peu plus d'une heure de calcul et 50 Mo d'espace disque. En genre 2, il permit de calculer le nombre de points d'une courbe sur un corps de cardinal 3^{400} en une vingtaine d'heures et 120 Mo d'espace disque ; un tel calcul requerrait plusieurs Go avec l'algorithme de Kedlaya.

RÉFÉRENCES

[1] T. G. Abbott, K. S. Kedlaya, & D. Roe – « Bounding Picard numbers of surfaces using p-adic cohomology », 2006, `arXiv:math.NT/0601508`.

[2] L. M. Adleman & M.-D. Huang – *Primality testing and abelian varieties over finite fields*, Lecture Notes in Mathematics, vol. 1512, Springer-Verlag, Berlin, 1992.

[3] ______, « Counting points on curves and abelian varieties over finite fields », *J. Symbolic Comput.* **32** (2001), no. 3, p. 171–189.

[4] E. Bach – « Explicit bounds for primality testing and related problems », *Math. Comp.* **55** (1990), no. 191, p. 355–380.

[5] F. Baldassarri & B. Chiarellotto – « Algebraic versus rigid cohomology with logarithmic coefficients », in *Barsotti Symposium in Algebraic Geometry (Abano Terme, 1991)*, Perspect. Math., vol. 15, Academic Press, San Diego, CA, 1994, p. 11–50.

[6] P. Berthelot – « Géométrie rigide et cohomologie des variétés algébriques de caractéristique p », *Mém. Soc. Math. France* (1986), no. 23, p. 7–32, Introductions aux cohomologies p-adiques (Luminy, 1984).

[7] ______, « Cohomologie rigide et cohomologie rigide à supports propres. Première partie », Prépublication, IRMAR, Université Rennes 1, 1996.

[8] ______, « Dualité de Poincaré et formule de Künneth en cohomologie rigide », *C. R. Acad. Sci. Paris Sér. I Math.* **325** (1997), no. 5, p. 493–498.

[9] ______, « Finitude et pureté cohomologique en cohomologie rigide », *Invent. Math.* **128** (1997), no. 2, p. 329–377, avec un appendice en anglais par A. J. de Jong.

[10] I. F. Blake, G. Seroussi & N. P. Smart – *Elliptic curves in cryptography*, London Mathematical Society Lecture Note Series, vol. 265, Cambridge University Press, Cambridge, 2000, Reprint of the 1999 original.

[11] ______ (éds.) – *Advances in elliptic curve cryptography*, London Mathematical Society Lecture Note Series, vol. 317, Cambridge University Press, Cambridge, 2005.

[12] E. Bombieri – « On exponential sums in finite fields. II », *Invent. Math.* **47** (1978), no. 1, p. 29–39.

[13] S. Bosch – « A rigid analytic version of M. Artin's theorem on analytic equations », *Math. Ann.* **255** (1981), no. 3, p. 395–404.

[14] J.-B. Bost & J.-F. Mestre – « Moyenne arithmético-géométrique et périodes des courbes de genre 1 et 2 », *Gaz. Math.* (1988), no. 38, p. 36–64.

[15] A. Bostan, P. Gaudry & É. Schost – « Linear recurrences with polynomial coefficients and computation of the Cartier-Manin operator on hyperelliptic curves », in *Seventh International Conference on Finite Fields and Applications (Toulouse, 2003)*, Lecture Notes in Computer Science, vol. 2948, Springer-Verlag, 2004, p. 40–58.

[16] C. Breuil, B. Conrad, F. Diamond & R. Taylor – « On the modularity of elliptic curves over $\mathbf{Q}$: wild 3-adic exercises », *Amer. J. Math.* **14** (2001), no. 4, p. 843–939.

[17] D. G. Cantor – « On the analogue of the division polynomials for hyperelliptic curves », *J. reine angew. Math.* **447** (1994), p. 91–145.

[18] R. Carls – « A generalized arithmetico-geometric mean », Thèse, Rijksuniversiteit Groningen, 2004.

[19] W. Castryck, J. Denef & F. Vercauteren – « Computing Zeta Functions of Nondegenerate Curves », 2006, `arXiv:math.NT/0607308`.

[20] B. Chiarellotto – « Weights in rigid cohomology applications to unipotent F-isocrystals », *Ann. Sci. École Norm. Sup.* **31** (1998), no. 5, p. 683–715.

[21] B. Chiarellotto & B. Le Stum – « A comparison theorem for weights », *J. reine angew. Math.* **546** (2002), p. 159–176.

[22] H. Cohen – *A course in computational algebraic number theory*, Graduate Texts in Mathematics, vol. 138, Springer-Verlag, Berlin, 1993.

[23] H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen & F. Vercauteren (éds.) – *Handbook of elliptic and hyperelliptic curve cryptography*, Discrete Mathematics and its Applications (Boca Raton), Chapman & Hall/CRC, Boca Raton, FL, 2006.

[24] P. Cohen – « On the coefficients of the transformation polynomials for the elliptic modular function », *Math. Proc. Cambridge Philos. Soc.* **95** (1984), p. 389–402.

[25] J.-M. Couveignes – « Computing ℓ-isogenies using the p-torsion », in *Algorithmic number theory (Talence, 1996)*, Lecture Notes in Comput. Sci., vol. 1122, Springer, Berlin, 1996, p. 59–65.

[26] P. Deligne – *Équations différentielles à points singuliers réguliers*, Springer-Verlag, Berlin, 1970, Lecture Notes in Mathematics, Vol. 163.

[27] ———, « Formes modulaires et représentations ℓ-adiques », in *Séminaire Bourbaki 1968/69*, Lecture Notes in Math., no. 179, 1971, Exp. 355, p. 139–172.

[28] ———, « Théorie de Hodge II », *Publ. Math. Inst. Hautes Études Sci.* **40** (1972), p. 5–57.

[29] ———, « La conjecture de Weil, I », *Publ. Math. Inst. Hautes Études Sci.* **43** (1974), p. 273–307.

[30] ———, *Cohomologie étale (Séminaire de géométrie algébrique du Bois-Marie — SGA $4\frac{1}{2}$)*, Lecture Notes in Mathematics, vol. 569, Springer-Verlag, Berlin, 1977, Avec la collaboration de J.-F. Boutot, A. Grothendieck, L. Illusie et J.-L. Verdier.

[31] ———, « La conjecture de Weil, II », *Publ. Math. Inst. Hautes Études Sci.* **52** (1980), p. 137–252.

[32] J. Denef & F. Vercauteren – « Counting points on C_{ab} curves using Monsky-Washnitzer cohomology », *Finite Fields Appl.* **12** (2006), no. 1, p. 78–102.

[33] ———, « An extension of Kedlaya's algorithm to hyperelliptic curves in characteristic 2 », *J. Cryptology* **19** (2006), no. 1, p. 1–25.

[34] M. Deuring – « Die Typen der Multiplikatorringe elliptischer Funktionenkörper », *Abh. Math. Sem. Hannsischen Univ.* **14** (1941), p. 197–272.

[35] W. Diffie & M. Hellman – « New directions in cryptography », *IEEE Trans. Inform. Theory* **22** (1976), p. 644–654.

[36] B. Dwork & A. Ogus – « Canonical liftings of Jacobians », *Compositio Math.* **58** (1986), no. 1, p. 111–131.

[37] B. Dwork – « On the rationality of the zeta function of an algebraic variety », *Amer. J. Math.* **82** (1960), p. 631–648.

[38] B. Edixhoven – « Point counting after Kedlaya », EIDMA-Stieltjes Graduate course, Leiden, September 22–26, 2003, `http://www.math.leidenuniv.nl/~edix/oww/mathofcrypt/carls_edixhoven/kedlaya.pdf`, 2003.

[39] B. Edixhoven, J.-M. Couveignes, R. de Jong, F. Merkl & J. Bosman – « On the computation of coefficients of a modular form », Tech. report, 2006, `arXiv:math.NT/0605244`.

[40] N. Elkies – « Explicit isogenies », 1991.

[41] R. Elkik – « Solutions d'équations à coefficients dans un anneau hensélien », *Ann. Sci. École Norm. Sup.* **6** (1973), p. 553–603 (1974).

[42] A. Enge – « Computing modular polynomials in quasi-linear time », Prépublication, `http://www.lix.polytechnique.fr/Labo/Andreas.Enge/vorabdrucke/modcomp.pdf`, 2006.

[43] A. Enge, P. Gaudry & F. Morain – « A new record for SEA », `http://www.lix.polytechnique.fr/~morain/SEA/d2100x.annonce`, 2006.

[44] M. Fouquet, P. Gaudry & R. Harley – « An extension of Satoh's algorithm and its implementation », *J. Ramanujan Math. Soc.* **15** (2000), no. 4, p. 281–318.

[45] J. Fresnel & M. van der Put – *Rigid analytic geometry and its applications*, Progress in Mathematics, vol. 218, Birkhäuser Boston Inc., Boston, MA, 2004.

[46] G. Frey & H.-G. Rück – « A remark concerning m-divisibility and the discrete logarithm problem in the divisor class group of curves », *Math. Comp.* **62** (1994), no. 206, p. 865–874.

[47] S. Galbraith & A. Menezes – « Algebraic curves and cryptography », *Finite Fields Appl.* **11** (2005), p. 544–577.

[48] P. Gaudry & N. Gürel – « An extension of Kedlaya's point-counting algorithm to superelliptic curves », in *Advances in cryptology—ASIACRYPT 2001 (Gold Coast)*, Lecture Notes in Comput. Sci., vol. 2248, Springer, Berlin, 2001, p. 480–494.

[49] ———, « Counting points in medium characteristic using Kedlaya's algorithm », *Experiment. Math.* **12** (2003), no. 4, p. 395–402.

[50] P. Gaudry & R. Harley – « Counting points on hyperelliptic curves over finite fields », in *Algorithmic number theory (Leiden, 2000)*, Lecture Notes in Comput. Sci., vol. 1838, Springer, Berlin, 2000, p. 313–332.

[51] R. Gerkmann – « Relative rigid cohomology and point counting in families of elliptic curves », 2005, `http://joguinf.informatik.uni-mainz.de/~gerkmann/legendre.pdf`.

[52] A. Grothendieck – « On the de Rham cohomology of algebraic varieties », *Inst. Hautes Études Sci. Publ. Math.* (1966), no. 29, p. 95–103.

[53] ———, *Cohomologie ℓ-adique et fonctions L*, Lecture Notes in Math., no. 589, Springer-Verlag, 1972-73, SGA 5.

[54] ———, « Formule de Lefschetz et rationalité des fonctions L », in *Séminaire Bourbaki, Vol. 9*, Soc. Math. France, Paris, 1995, Exp. No. 279, Année 1964–1965, p. 41–55.

[55] R. Harley – « Asymptotically optimal p-adic point-counting », e-mail à la liste NMBRTHRY, décembre 2002.

[56] D. Harvey – « Kedlaya's Algorithm in Larger Characteristic », 2006, `arXiv:math.NT/0610973`.

[57] H. Hasse – « Beweis des Analogons der Riemannschen Vermutung für die Artinschen und F. K. Schmidtschen Kongruenzzetafunktionen in gewissen elliptischen Fällen. Vorläufie Mitteilung », *Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse* **42** (1933), no. 3, p. 253–262, `http://gdzdoc.sub.uni-goettingen.de/sub/digbib/loader?did=D64289`.

[58] ———, « Zur Theorie der abstrakten elliptischen Funktionenkörper III. Die Struktur des Meromorphismenrings. Die Riemannsche Vermutung. », *J. reine angew. Math.* **175** (1936), no. 4, p. 193–208, `http://gdzdoc.sub.uni-goettingen.de/sub/digbib/loader?did=D255900`.

[59] W. V. D. Hodge & M. F. Atiyah – « Integrals of the second kind on an algebraic variety », *Ann. of Math.* **62** (1955), p. 56–91.

[60] H. Hubrechts – « Memory efficient hyperelliptic curve point counting », 2006, `arXiv:math.NT/0609032`.

[61] ———, « Point counting in families of hyperelliptic curves », 2006, `arXiv:math.NT/0601438`.

[62] ———, « Point counting in families of hyperelliptic curves in characteristic 2 », 2006, `arXiv:math.NT/0607346`.

[63] N. M. Katz & W. Messing – « Some consequences of the Riemann hypothesis for varieties over finite fields », *Invent. Math.* **23** (1974), p. 73–77.

[64] K. S. Kedlaya – « Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology », *J. Ramanujan Math. Soc.* **16** (2001), no. 4, p. 323–338, Erratum : J. Ramanujan Math. Soc. **18** (2003), no. 4, 417–418.

[65] ———, « Finiteness of rigid cohomology with coefficients », *Duke Math. J.* **134** (2006), no. 1, p. 15–97.

[66] N. Koblitz & A. J. Menezes – « A survey of public-key cryptosystems », *SIAM Rev.* **46** (2004), no. 4, p. 599–634 (electronic).

[67] A. G. B. Lauder – « Deformation theory and the computation of zeta functions », *Proc. London Math. Soc.* **88** (2004), no. 3, p. 565–602.

[68] ———, « Rigid cohomology and p-adic point counting », *J. Théor. Nombres Bordeaux* **17** (2005), p. 169–180.

[69] A. G. B. Lauder & D. Wan – « Counting points on varieties over finite fields of small characteristic », in *Algorithmic Number Theory : Lattices, Number Fields, Curves and Cryptography* (J. Buhler & P. Stevenhagen, éds.), Mathematical Sciences Research Institute Publications, Cambridge University Press, 2007, À paraître, `http://www.maths.ox.ac.uk/`.

[70] B. Le Stum – *A course on rigid cohomology*, Cambridge Tracts in Mathematics, Cambridge Univ. Press, 2007, à paraître.

[71] R. Lercier & F. Morain – « Computing isogenies between elliptic curves over $\mathbf{F}_{p^n}$ using Couveignes's algorithm », *Math. Comp.* **69** (2000), no. 229, p. 351–370.

[72] R. Lercier – « Computing isogenies in $\mathbf{F}_{2^n}$ », in *Algorithmic number theory (Talence, 1996)*, Lecture Notes in Comput. Sci., vol. 1122, Springer, Berlin, 1996, p. 197–212.

[73] R. Lercier & D. Lubicz – « Counting points in elliptic curves over finite fields of small characteristic in quasi quadratic time », in *Advances in cryptology—EUROCRYPT 2003*, Lecture Notes in Comput. Sci., vol. 2656, Springer, Berlin, 2003, p. 360–373.

[74] ______, « A Quasi Quadratic Time Algorithm for Hyperelliptic Curve Point Counting », *The Ramanujan Journal* **12** (2006), `http://medicis.polytechnique.fr/~lercier/file/LL05.pdf`.

[75] J. Lubin, J.-P. Serre & J. Tate – « Elliptic curves and formal groups », 1964, Lecture notes prepared in connection with the seminars held at the Summer institute on Algebraic Geometry, Whitney State, Woods Hole, Massachusetts, `http://ma.utexas.edu/users/voloch/lst.html`.

[76] « The Magma computational algebra system for algebra, number theory and geometry » – `http://magma.maths.usyd.edu.au/magma/`.

[77] U. M. Maurer & S. Wolf – « The relationship between breaking the Diffie-Hellman protocol and computing discrete logarithms », *SIAM J. Comput.* **28** (1999), no. 5, p. 1689–1721 (electronic).

[78] Z. Mebkhout – « Sur le théorème de finitude de la cohomologie p-adique d'une variété affine non singulière », *Amer. J. Math.* **119** (1997), no. 5, p. 1027–1081.

[79] W. Messing – *The crystals associated to Barsotti-Tate groups : with applications to abelian schemes*, Lecture Notes in Math., no. 345, Springer-Verlag, 1976.

[80] J.-F. Mestre – « Utilisation de l'AGM pour le calcul de $E(\mathbf{F}_{2^n})$ », Lettre à Harley et Gaudry, décembre 2000, `http://www.math.jussieu.fr/~mestre`.

[81] ______, « Algorithmes pour compter des points de courbes en petite caractéristique et en petit genre », rédigé par David Lubicz, `http://www.math.jussieu.fr/~mestre/rennescrypto.ps`, 2002.

[82] P. Monsky & G. Washnitzer – « Formal cohomology I », *Ann. of Math.* **88** (1968), p. 181–217.

[83] F. Morain – « Calcul du nombre de points sur une courbe elliptique dans un corps fini : aspects algorithmiques », *J. Théor. Nombres Bordeaux* **7** (1995), no. 1, p. 255–282, Les Dix-huitièmes Journées Arithmétiques (Bordeaux, 1993).

[84] ______, « La primalité en temps polynomial (d'après Adleman, Huang ; Agrawal, Kayal, Saxena) », *Astérisque* (2004), no. 294, p. viii, 205–230.

[85] D. Mumford – *Tata lectures on Theta II*, Birkhäuser, 1984.

[86] A. Muzereau, N. P. Smart & F. Vercauteren – « The equivalence between the DHP and DLP for elliptic curves used in practical applications », *LMS J. Comput. Math.* **7** (2004), p. 50–72 (electronic).

[87] V. Müller – « Ein Algorithmus zur Bestimmung der Punktanzahl elliptischer Kurven über endlichen Körpern der Charakteristik größer drei », Thèse, University of Saarland, Saarbrücken, 1995.

[88] A. Nitaj – « L'algorithme de Cornacchia », *Exposition. Math.* **13** (1995), no. 4, p. 358–365.

[89] The PARI group – « PARI/GP », 2004, `http://pari.math.u-bordeaux.fr/`.

[90] J. Pila – « Frobenius maps of abelian varieties and finding roots of unity in finite fields », *Math. Comp.* **55** (1990), no. 192, p. 745–763.

[91] ———, « Counting points on curves over families in polynomial time », 1991.

[92] S. C. Pohlig & M. E. Hellman – « An improved algorithm for computing logarithms over GF(p) and its cryptographic significance », *IEEE Trans. Information Theory* **IT-24** (1978), no. 1, p. 106–110.

[93] J. M. Pollard – « Monte Carlo methods for index computation (mod p) », *Math. Comp.* **32** (1978), no. 143, p. 918–924.

[94] M. van der Put – « The cohomology of Monsky and Washnitzer », *Mém. Soc. Math. France (N.S.)* (1986), no. 23, p. 4, 33–59, Introductions aux cohomologies p-adiques (Luminy, 1984).

[95] C. Ritzenthaler – « Point counting on genus 3 non hyperelliptic curves », in *Algorithmic number theory*, Lecture Notes in Comput. Sci., vol. 3076, Springer, Berlin, 2004, p. 379–394.

[96] T. Satoh – « The canonical lift of an ordinary elliptic curve over a finite field and its point counting », *J. Ramanujan Math. Soc.* **15** (2000), no. 4, p. 247–270.

[97] T. Satoh, B. Skjernaa & Y. Taguchi – « Fast computation of canonical lifts of elliptic curves and its application to point counting », *Finite Fields Appl.* **9** (2003), no. 1, p. 89–101.

[98] R. Schoof – « Elliptic curves over finite fields and the computation of square roots mod p », *Math. Comp.* **44** (1985), no. 170, p. 483–494.

[99] ———, « Counting points on elliptic curves over finite fields », *J. Théor. Nombres Bordeaux* **7** (1995), no. 1, p. 219–254, Les Dix-huitièmes Journées Arithmétiques (Bordeaux, 1993).

[100] D. Shanks – « Class number, a theory of factorization, and genera », in *1969 Number Theory Institute (Proc. Sympos. Pure Math., Vol. XX, State Univ. New York, Stony Brook, N.Y., 1969)*, Amer. Math. Soc., Providence, R.I., 1971, p. 415–440.

[101] A. Shiho – « Crystalline fundamental groups. II. Log convergent cohomology and rigid cohomology », *J. Math. Sci. Univ. Tokyo* **9** (2002), no. 1, p. 1–163.

[102] V. Shoup – « Lower bounds for discrete logarithms and related problems », in *Advances in cryptology—EUROCRYPT '97*, Lecture Notes in Comput. Sci., vol. 1233, Springer, Berlin, 1997, p. 256–266.

[103] B. Skjernaa – « Satoh's algorithm in characteristic 2 », *Math. Comp.* **72** (2003), no. 241, p. 477–487 (electronic).

[104] N. Tsuzuki – « Bessel F-isocrystals and an algorithm for computing Kloosterman sums », 2003.

[105] F. Vercauteren – « The SEA algorithm in characteristic 2 », `http://homes.esat.kuleuven.be/~fvercaut/papers/SEA.pdf.gz`, 2000.

[106] ———, « Computing zeta functions of hyperelliptic curves over finite fields of characteristic 2 », in *Advances in cryptology—CRYPTO 2002*, Lecture Notes in Comput. Sci., vol. 2442, Springer, Berlin, 2002, p. 369–384.

[107] F. Vercauteren, B. Preneel & J. Vandewalle – « A memory efficient version of Satoh's algorithm », in *Advances in cryptology—EUROCRYPT 2001 (Innsbruck)*, Lecture Notes in Comput. Sci., vol. 2045, Springer, Berlin, 2001, p. 1–13.

[108] J. Vélu – « Isogénies entre courbes elliptiques », *C. R. Acad. Sci. Paris Sér. I Math.* **273** (1971), p. 238–241.

[109] D. Wan – « Algorithmic theory of zeta functions over finite fields », in *Algorithmic Number Theory : Lattices, Number Fields, Curves and Cryptography* (J. Buhler & P. Stevenhagen, éds.), Mathematical Sciences Research Institute Publications, Cambridge University Press, 2007, À paraître, `http://www.maths.ox.ac.uk/`.

[110] W. C. Waterhouse – « Abelian varieties over finite fields », *Ann. Sci. École Norm. Sup.* **2** (1969), p. 521–560, http://www.numdam.org/item?id=ASENS_1969_4_2_4_521_0.

[111] A. Weil – *Variétés abéliennes et courbes algébriques*, Actualités Sci. Ind., no. 1064, Hermann & Cie., Paris, 1948.

Antoine CHAMBERT-LOIR

Irmar
Université de Rennes 1
Campus de Beaulieu
35042 Rennes Cedex
E-mail : antoine.chambert-loir@univ-rennes1.fr