Ecole Normale Supérieure

Formation Interuniversitaire de Mathématiques Fondamentales et Appliquées

Mémoire de Magistère

Présentation du domaine de recherche

Ivan Boyer

Directeur de thèse
Jean-François Mestre

20 octobre 2009

Table des matières

Ivan Boyer

Le Freynet
38350 Nantes-en-Rattier

45 Rue d'Ulm
75005 Paris

Né le 28/01/1986
Nationalité Française

Tél. : 06 08 54 67 74
E-mail : ivan.boyer@ens.fr

Parcours universitaire

2008 – 2009	**M2 de Mathématiques** à l'université Paris–Diderot, *mention Très Bien.* • Théorie analytique des nombres I & II, R. de la Breteche, • Géométrie algébrique, N. Karpenko, • Courbes elliptiques, M. Hindry, • Variétés abéliennes, M. Hindry, • Codes correcteurs d'erreurs, calcul formel : applications à la cryptologie, J.-C. Faugère et J.-P. Tillich, • Mémoire sous la direction de Jean-François Mestre.
2007 – 2008	**Agrégation de Mathématiques,** reçu avec le rang 5.
2006 – 2007	**M1 de Mathématiques** *mention Très Bien.* Mémoire dirigé par François Loeser.
2006 – 2007	**Licence de Mathématiques et d'Informatique** *mention Très Bien.*
2006	**Entrée à l'Ecole Normale Supérieure de Paris.** **Concours :** Ens Ulm (Info, rang 1), Ecole Polytechnique (rang 12).
2004 – 2006	**Classes préparatoires** *MPSI – MP*,* Lycée Champollion, Grenoble.
2004	**Baccalauréat série S** *mention Très Bien,* Lycée de La Mure, Isère.

Textes et exposés

2009	Mémoire de Magistère : *Compter les points rationnels d'une courbe algébrique.*
2009	Mémoire de Master : *Diverses applications de la géométrie algébrique à la théorie de l'information.*
2008	Exposé d'informatique : *Algorithmes de cribles efficaces.*
2007	Mémoire de maîtrise : *Factorisation dans* $\mathbb{Z}[X]$.
2007	Exposé de langage formel : *Parties reconnaissables de* $\mathbb{N}$.
2007	Exposé d'algorithmique : *Multiplication de matrices.*

Expériences mathématiques

2007 –	Interrogateur de mathématiques et d'informatique en classe de MP* (Lycée Charlemagne, Paris).
2002 – 2004	Préparation Animath aux Olympiades Internationales de Mathématiques.
2003	Olympiades académiques de Mathématiques (premier, académie de Grenoble).
2001	Coupe Euromath par équipe (vainqueur).

Informations diverses

Langues	Anglais (lu, écrit, parlé) Espagnol (connaissances de base).
Programmation	C, Ocaml, Unix.
Logiciels	LaTeX, Maple, ...
Sports	Escalade, course à pied, vélo.

Géométrie algébrique en théorie de l'information : cryptographie et codes correcteurs.

Présentation du domaine de recherche.

Ivan Boyer
Sous la direction de Jean-François Mestre.

20 octobre 2009

Table des matières

Dans notre société de communication, deux problématiques majeures apparaissent au moment d'échanger des informations : la confidentialité d'une part et l'exactitude d'autre part. Il est intéressant de noter que la géométrie algébrique y trouve une place de plus en plus importante, notamment dans la possibilité de trouver des courbes ayant beaucoup de points rationnels.

On présente d'une part la cryptographie à clé publique basée sur des courbes elliptiques. La taille des clés et la rapidité sont supérieures à celle du système Rsa mais encore trop jeune pour bénéficier de la même confiance. On verra notamment l'algorithme de Schoof et des améliorations pratiques.

D'autre part, on expliquera l'intérêt de courbes algébriques ayant beaucoup de points rationnels dans l'utilisation de codes correcteurs. On présentera quelques bornes d'efficacité à notre disposition, notamment la borne Tvz . On verra enfin ce que l'on sait du nombre maximum de points rationnels sur une courbe lorsque l'on fixe son genre (par exemple les courbes elliptiques et la borne de Hasse-Weil en genre 1).

1 Compter les points rationnels d'une courbe elliptique.

1.1 Cryptographie à clé publique.

En 1985, N. Koblitz et V. Miller proposèrent indépendamment d'utiliser des courbes elliptiques dans des procédés cryptographiques à clé publique. Leurs techniques reposent sur la notion de fonction à sens unique :

Définition 1.1 (Fonction à sens unique)**.** *Soit $f : \Sigma \to \Sigma'$ une fonction. On dit qu'elle est à* sens unique *si*

(i) Pour $x \in \Sigma$, $f(x)$ peut être calculé en temps polynomial.

(ii) Il n'y a pas d'algorithme polynomial tel, qu'étant donné $y \in \Sigma'$, il décide si $y \notin \mathrm{im}(f)$ et donne dans le cas contraire un $x \in \Sigma$ tel que $f(x) = y$.

Le procédé d'échange de clés de Diffie et Hellman repose sur une fonction dont on espère qu'elle est à sens unique[†] : Alice et Bob commencent par décider d'un groupe $(G, \oplus)$ et d'un élément $P \in G$. Ensuite, ils choisissent chacun de leur côté des entiers e_A et e_B puis rendent publiques les quantités $[e_A]P$ et $[e_B]P$.

†. On ne sait pas le prouver ; on aurait alors **P≠NP** !

Ensuite, tous deux peuvent calculer la quantité $[e_A e_B]P$ qui sera leur clé commune permettant d'utiliser des techniques cryptographiques symétriques. Comme ce procédé ne dépend que du sous-groupe engendré par P, on peut choisir en fait $G = \langle P \rangle$ cyclique. La sécurité de ce système repose sur :

Définition 1.2 (Problème du Logarithme Discret, DLP [†]). *Soit $G = \langle b \rangle$ un groupe cyclique d'ordre [‡] n. On appelle* logarithme discret *la fonction*

$$\begin{aligned} \log_b : G &\longrightarrow \mathbb{Z}/n\mathbb{Z} \\ b^k &\longmapsto k \mod n \ . \end{aligned}$$

1.2 Courbes elliptiques : loi de groupe.

Afin de mettre en place ces idées, il nous faut trouver un groupe où l'on sache calculer facilement sans que le DLP soit facile. Pour cela, on considère une courbe elliptique E définie sur un corps $\mathbb{F}_q$ dont on notera p la caractéristique. Pour simplifier, on supposera $p \neq 2, 3$ de sorte que l'on puisse écrire une équation de E sous la forme $y^2 = x^3 + ax + b$, avec $\Delta = 4a^3 - 27b^2 \neq 0$ (la courbe est lisse).

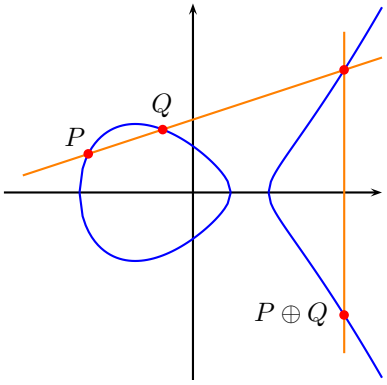


FIGURE 1: Loi de groupe sur une courbe elliptique.

Proposition 1.3 (Formules d'addition). *Soient (x_1, y_1) et (x_2, y_2) deux points de E distincts de $\mathcal{O}$ (le point à l'infini), non opposés l'un de l'autre. La loi d'addition par cordes et tangentes, illustrée ci-contre, est donnée algébriquement par les formules :*

$$\begin{cases} x_3 = \lambda^2 - x_1 - x_2 \\ y_3 = \lambda(x_1 - x_3) - y_1 \end{cases} \quad \text{où } \lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & \text{si } x_1 \neq x_2, \\ \dfrac{3x_1 + a}{2y_1} & \text{sinon.} \end{cases}$$

Grâce à ces formules on peut calculer rapidement dans ce groupe abélien : on peut notamment calculer la multiplication par $m \in \mathbb{N}$ (notée dans dans ce contexte $[m]$) par exponentiation rapide.

Afin de ne pas faciliter la résolution du DLP, il faut pouvoir trouver une courbe dont le groupe a un cardinal possédant un très grand facteur premier. Pour cela, il nous faut calculer ce cardinal efficacement. Il existe des méthodes élémentaires ; on peut par exemple citer la formule :

$$|E(\mathbb{F}_q)| = q + 1 + \sum_{x \in \mathbb{F}_q} \left(\frac{x^3 + ax + b}{q} \right).$$

Le problème est que la complexité de cette méthode est bien trop élevée [¶]. Le point de départ des algorithmes l–adiques vient de la propriété cruciale que le nombre de points d'une courbe elliptique peut être encadré :

Théorème 1.4 (Borne de Hasse). *On a l'encadrement :*

$$\big| |E(\mathbb{F}_q)| - (q+1) \big| \leqslant 2\sqrt{q}.$$

L'idée fondamentale est alors de déterminer ce cardinal modulo des petits nombres premiers puis de le retrouver avec le théorème des restes chinois. Une application élémentaire du théorème des nombres premiers nous dit qu'il suffit de savoir le faire pour $O(\log q)$ nombres premiers de taille $O(\log q)$. Ainsi, la recherche d'un algorithme polynomial pour trouver $|E(\mathbb{F}_q)|$ se réduit à en trouver un qui calcule $|E(\mathbb{F}_q)| \mod l$ pour un nombre premier l de taille de l'ordre de $\log q$.

1.3 Outils algébriques et algorithme de Schoof.

Avant d'exposer les principales idées de l'algorithme de Schoof, il faut rappeler quelques outils algébriques essentiels dont on trouvera des précisions dans l'incontournable [Sil86].

Définition 1.5 (Isogénies). *On dit qu'un morphisme algébrique φ entre deux courbes elliptiques E_1 et E_2 est une* isogénie *si $\varphi(\mathcal{O}_1) = \mathcal{O}_2$. Si de plus φ n'est pas constante, on dit que E_1 et E_2 sont* isogènes.

†. Discrete Logarithm Problem en anglais.
‡. Il est facile de voir que la difficulté se réduit aux ordres premiers.
¶. Elle est ici exponentielle en la taille de q.

La condition sur le point à l'infini semble faible. Il n'en est rien :

Proposition 1.6. *Une isogénie $\varphi : E_1 \to E_2$ est aussi un morphisme de groupe.*

Deux isogénies jouent un rôle fondamental dans l'algorithme de Schoof. La première, sur laquelle repose toute l'idée de l'algorithme, est le Frobénius. En effet, il permet de déterminer les points de la courbe qui sont à coordonnées dans $\mathbb{F}_q$: ce seront naturellement ceux qui sont dans le noyau de $\pi_E - \mathrm{Id}$ où l'on a défini :

Définition 1.7. *Soit E une courbe elliptique définie sur $\mathbb{F}_q$. On appelle* morphisme de Frobenius *le morphisme algébrique*

$$\begin{aligned} \pi_E : E(\overline{\mathbb{F}_q}) &\longrightarrow E(\overline{\mathbb{F}_q}) \\ (x, y) &\longmapsto (x^q, y^q). \end{aligned}$$

C'est bien une isogénie puisqu'elle envoie le point à l'infini sur lui-même [†]. A ce stade, il nous faut quelques propriétés usuelles vérifiées par les isogénies pour pouvoir déterminer le cardinal du noyau de $\pi_E - \mathrm{Id}$:

Proposition 1.8. *Une isogénie φ non nulle est surjective et possède un noyau fini. Lorsqu'elle est séparable, on a de plus $|\ker \varphi| = \deg \varphi$.*

Pour toute isogénie $\varphi : E_1 \to E_2$ il existe une unique isogénie $\hat{\varphi} : E_2 \to E_1$ vérifiant

$$\hat{\varphi} \circ \varphi = [m]_{E_1} \text{ et } \varphi \circ \hat{\varphi} = [m]_{E_2},$$

où $m = \deg \varphi$. On a de plus $\widehat{\lambda \circ \varphi} = \hat{\lambda} \circ \hat{\varphi}$ et $\widehat{\varphi + \psi} = \hat{\varphi} + \hat{\psi}$, pour des isogénies $\lambda : E_2 \to E_3$ et $\psi : E_1 \to E_2$.

On a en particulier $\hat{\hat{\varphi}} = \varphi$ ce qui justifie la qualification de dualité. On définit finalement :

Définition 1.9 (Norme et trace)**.** *Soit $\varphi : E \to E$ une isogénie. On définit sa* norme *et sa* trace *par*

$$\mathrm{N}\,\varphi = \varphi \circ \hat{\varphi} \in \mathbb{N} \quad et \quad \mathrm{tr}\,\varphi = \varphi + \hat{\varphi} \in \mathbb{Z}.$$

Maintenant on écrit d'une part

$$\begin{aligned} |E(\mathbb{F}_q)| = \deg(\pi_E - \mathrm{Id}) = \mathrm{N}(\pi_E - \mathrm{Id}) = (\pi_E - \mathrm{Id}) \circ \widehat{(\pi_E - \mathrm{Id})} &= (\pi_E - \mathrm{Id}) \circ (\hat{\pi}_E - \mathrm{Id}) \\ &= q + 1 - (\pi_E + \hat{\pi}_E) = q + 1 - \mathrm{tr}\,\pi_E. \end{aligned}$$

et, d'autre part, on compose par π_E l'égalité $\mathrm{tr}\,\pi_E = \pi_E + \hat{\pi}_E$: on obtient $(\mathrm{tr}\,\pi_E)\pi_E = \pi_E^2 + q$. Ce sont les propriétés fondatrices de l'algorithme de Schoof :

Proposition 1.10.

(i) Le cardinal de $E(\mathbb{F}_q)$ est donné par la trace de π : $|E(\mathbb{F}_q)| = q + 1 - \mathrm{tr}\,\pi_E$.

(ii) L'endomorphisme π_E vérifie, dans End E*, l'équation*

$$\pi_E^2 - (\mathrm{tr}\,\pi_E)\pi_E + q = 0.$$

Ainsi, suivant le principe que l'on a décrit dans le paragraphe précédent, on va chercher à déterminer $\mathrm{tr}\,\pi_E \mod l$ pour différents l. Pour cela, on réduit l'équation « modulo » l. On note q' l'entier $0 < q' < l$ congru à q modulo l et on a la proposition :

Proposition 1.11. *La relation*

$$\pi_E^2 - t'\pi_E + q' \qquad t' = 0, 1, 2, \ldots, l-1 \tag{$\star$}$$

est vérifiée sur le sous-groupe $E[l]$ des points de l–torsions si et seulement si $t' \equiv \mathrm{tr}\,\pi_E \mod l$.

Notons qu'il suffit en fait de vérifier la relation sur une partie de $E[l]$ non réduite à $\{\mathcal{O}\}$. Le problème est de trouver un point de $E[l]\backslash\{\mathcal{O}\}$ (et donc le sous-groupe d'ordre l qu'il engendre).

L'idée de Schoof (voir [Sch85]) est alors d'utiliser les polynômes de divisions. Ce sont des polynômes qui caractérisent, pour un entier m donné, les points de m–torsion. Concrètement, il n'est pas difficile de trouver ces polynômes : il suffit par exemple d'écrire le morphisme rationnel $[m]$ puis de n'en garder que les dénominateurs [‡] ; il s'agira en effet des polynômes annulateurs des points qui s'envoient sur le point infini, élément neutre du groupe. La forme particulière d'une équation de Weierstrass nous donne des polynômes ayant une forme relativement simple :

†. On devrait écrire l'expression du Frobénius en coordonnées projectives, $[X, Y, Z] \mapsto [X^q, Y^q, Z^q]$, ce qui montre clairement que l'image de $\mathcal{O} = [0, 1, 0]$ est bien lui-même.

‡. Encore une fois, on préfère garder une notation affine des morphismes ; sinon, il faut écrire le morphisme $[m]$ avec des polynômes homogènes et résoudre $[F_m, G_m, H_m] = [0, 1, 0]$.

Proposition 1.12. *Les polynômes de division peuvent se calculer grâce aux formules suivantes :*

$$\begin{aligned}
\Psi_1 &= 1, \qquad \Psi_2 = 2y,\\
\Psi_3 &= 3x^4 + 6ax^2 + 12bx - a^2,\\
\Psi_4 &= 4y(x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - 8b^2 - a^3),\\
\Psi_{2m+1} &= \Psi_{m+2}\Psi_m^3 - \Psi_{m-1}\Psi_{m+1}^3 \qquad (m \geqslant 2),\\
2y\Psi_{2m} &= \Psi_m(\Psi_{m+2}\Psi_{m-1}^2 - \Psi_{m-2}\Psi_{m+1}^2) \qquad (m \geqslant 3).
\end{aligned}$$

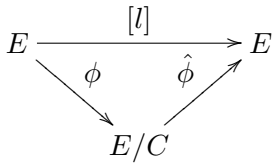
Une fois ces polynômes à notre disposition, il nous suffit de chercher quel t' vérifie la relation $(\star)$ dans l'anneau $\mathbb{F}_q[X,Y]/\langle \Psi_m(X,Y), Y^2 - X^3 - aX - b\rangle$, dans lequel on sait calculer efficacement.

1.4 L'algorithme Sea.

Néanmoins, de l'avis de Schoof lui-même, son algorithme tel quel n'est pas très performant notamment à cause du degré élevé des polynômes de division. Même si cela est maintenant à relativiser, Atkin et Elkies ont proposé quelques méthodes pour améliorer la complexité, en travaillant avec des polynômes de plus petite taille. L'idée principale est de trouver un facteur de Ψ_l de degré beaucoup plus petit, en l'occurrence $\frac{l-1}{2}$. Cela revient à factoriser l'isogénie $[l]$ de degré l^2 par une isogénie de degré l. Le noyau d'une telle isogénie serait alors $\mathbb{Z}/l\mathbb{Z}$ qui est cyclique. Soit C un des $l+1$ sous-groupes cycliques d'ordre l de $E[l] \simeq (\mathbb{Z}/l\mathbb{Z})^2$.

Proposition 1.13. *Il existe une unique courbe elliptique E' et une isogénie séparable $\phi : E \to E'$ telle que $\ker\phi = C$. On note E/C cette courbe elliptique et on dit qu'elle est l–isogène à E.*

On peut résumer l'idée principale de ces améliorations par le diagramme suivant : l'algorithme de Schoof utilise la flèche $[l]$ tandis que les améliorations d'Atkin et Elkies reposent sur ϕ :



Pour trouver ces courbes l–isogènes à E, on doit faire appel à un invariant très important dans la théorie des courbes elliptiques : l'invariant modulaire ou j–invariant. Sans entrer dans les détails, disons que cet invariant décrit les courbes elliptiques à isomorphisme près sur une clôture algébrique.

Théorème 1.14. *Soit E/K une courbe elliptique définie sur un corps K de caractéristique différente de l. Soit j son invariant : alors, les $l+1$ zéros de $\Phi_n(X,j)$ dans $\overline{K}$ sont précisément les j–invariants des courbes E' l–isogènes à E.*

Le reste est assez technique à présenter mais plutôt bien maîtrisé à l'heure actuelle. Même si l'on peut encore chercher à l'améliorer, l'algorithme Sea obtenu est finalement assez performant pour répondre à nos besoins : la complexité chute en $\tilde{O}((\log q)^4)$ et les améliorations d'Atkin agissent fortement sur la constante cachée dans le O.

Mentionnons pour finir que le nombre de points d'une courbe elliptique peut être relié étroitement à celui de son anneau d'endomorphismes. Si l'on connaît ce dernier à l'avance, alors, on peut trouver plus facilement le nombre de points rationnels : on utilise l'algorithme de Cornaccia. Cet algorithme est très efficace mais probabiliste puisqu'il repose sur l'extraction d'une racine carrée dans F_q. Notons que Schoof, dans son article original ([Sch85]) a eu l'idée de « renverser » cet algorithme pour en tirer le résultat surprenant :

Théorème 1.15 (Schoof (1985))**.** *Soit $D \in \mathbb{Z}$ un entier fixé. Soit $p \equiv 1 \mod 4$ [†] un nombre premier tel que $\left(\frac{D}{p}\right) = +1$. Alors, il existe un algorithme* déterministe *et polynomial en $\log p$ calculant la racine carrée de D modulo p, i.e. $y \in \mathbb{F}_p$, $y^2 \equiv D \mod p$. Cet algorithme dépend exponentiellement de la taille ($\log D$) de l'entier D.*

†. Le cas $p = 2$ n'a aucun intérêt et pour $p \equiv -1 \mod 4$, la racine carrée, si elle existe, s'obtient polynomialement en élevant à la puissance $\frac{p+1}{4}$.

2 Codes correcteurs géométriques.

2.1 Enjeux.

Une autre partie de la théorie de l'information fait appel à la géométrie algébrique : ce sont les codes correcteurs. Il s'agit de s'assurer que le message transmis est reçu sans erreur et dans le cas contraire, d'essayer de corriger ces erreurs. L'idée générale est de se placer sur un alphabet fini ($\mathbb{F}_q$ dans nos applications), de considérer une partie de $\mathbb{F}_q^n$, « le code » (généralement un sous-espace vectoriel) tels que deux mots de codes soient suffisamment éloignés, au sens de la distance de Hamming, qui compte le nombre de composantes différentes.

L'émetteur code le message à envoyer grâce à une fonction injective (généralement linéaire). Le récepteur vérifiera que le message est dans le code [†] et à défaut cherchera le mot de code le plus proche. Pour les détails et les définitions, on pourra par exemple se reporter à [vL82].

Deux quantités fondamentales interviennent pour juger de la qualité d'un code : son rendement R, c'est-à-dire le rapport du nombre de symboles du mot à coder par celui transmis, et sa distance minimale relative δ, *i.e.* le rapport de la distance minimale entre deux mots de codes distincts et la taille du code. Des bornes élémentaires relient ces deux quantités :

Les excellentes familles de codes sont définies comme des ensembles de codes dont les paramètres (δ_n, R_n) ont un point d'accumulation (quand la longueur du code tend vers l'infini) au-dessus de la borne de Gilbert–Varshamov. Les codes de Goppa sur $\mathbb{F}_q$ atteignent cette borne mais il a fallu attendre assez longtemps et l'utilisation centrale de géométrie algébrique pour la dépasser.

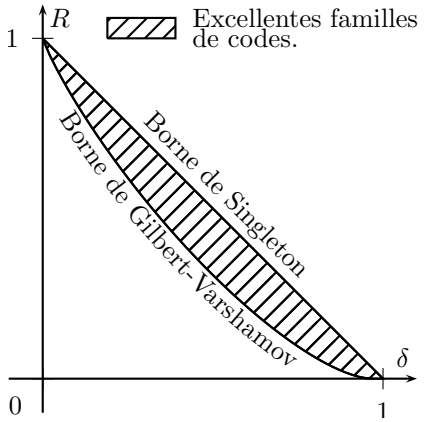


FIGURE 2: Bornes asymptotiques pour $q = 32$.

2.2 Codes géométriques.

On considère un objet géométrique $\mathcal{X}$ et un ensemble $\mathcal{P} = \{P_1, \ldots, P_n\}$ de points sur $\mathcal{X}$. On suppose ensuite que l'on dispose d'un $\mathbb{F}_q$–espace vectoriel L de fonctions de $\mathcal{X}$ à valeurs dans $\mathbb{F}_q$. On peut alors définir une fonction d'évaluation :

$$\begin{aligned} \mathrm{ev}_{\mathcal{P}} : L &\longrightarrow \mathbb{F}_q^n \\ f &\longmapsto (f(P_1), \ldots, f(P_n)) \ . \end{aligned}$$

L'image de $\mathrm{ev}_{\mathcal{P}}$ est un code linéaire que l'on qualifiera de géométrique. Quitte à remplacer L par $L/\ker \mathrm{ev}_{\mathcal{P}}$, on peut supposer que l'application est bien injective.

Un premier exemple simple mais important est celui où l'on choisit pour $\mathcal{X}$ la droite affine $\mathbb{F}_q$ et $\{P_1, \ldots, P_n\}$ un ensemble de n points distincts de $\mathbb{F}_q$. L'espace vectoriel L peut être choisi comme l'espace des polynômes à coefficients dans $\mathbb{F}_q$, de degré au plus $k-1$ avec $k \leqslant n$. On obtient ainsi le code classique dit de Reed–Solomon (RS) dont la distance minimale est $n-k+1$ et le rendement k/n pourraient atteindre la borne asymptotique de Gilbert–Varshamov si l'on n'était pas limité par le choix de n points distincts de $\mathbb{F}_q$.

Un autre exemple très important est celui des codes de Goppa classiques [‡] : en effet, ils sont à la base d'une famille de codes qui atteint la borne de Gilbert–Varshamov, sans toutefois la dépasser.

Ces deux exemples, que l'on qualifie de classiques, peuvent être réinterprétés dans le cadre plus général des codes géométriques des paragraphes suivants, où l'on choisit $\mathcal{X} = \mathrm{P}^1(\mathbb{F}_q)$. Cette variété a l'avantage de donner une construction « simple » de ces codes mais est limité par son nombre de points.

Plus formellement, on choisit désormais pour $\mathcal{X}$ une courbe projective lisse définie sur un corps fini K : un des enjeux cruciaux sera donc de trouver une telle courbe avec beaucoup de points rationnels. Cela permettra déjà de construire des codes de grande taille, mais seront-ils bons pour autant ?

Pour cela, il faut étudier la distance minimale : elle est d'autant plus grande que le nombre de points d'évaluation imposant l'égalité de deux fonctions est petit. L'idée est alors de se restreindre aux fonctions rationnelles sur $\mathcal{X}$ dont on impose des pôles ou des zéros.

On introduit dès lors la notion de diviseur sur la courbe $\mathcal{X}$: c'est un élément du groupe abélien libre engendré par les points de $\mathcal{X}$ (à coordonnées dans $\overline{K}$). On rappelle qu'un tel diviseur est dit défini sur K s'il

†. Cela ne certifie pas que la transmission est correcte mais on peut fixer une probabilité d'erreur.

‡. Il s'agit en fait des codes de Goppa géométriques, présentés un peu plus loin, où l'on se place sur $\mathrm{P}^1(\mathbb{F}_q)$.

est invariant par $\mathrm{Gal}_{\overline{K}/K}$. Par exemple le diviseur d'une fonction rationnelle à coefficients dans K est défini sur K ; un tel diviseur est appelé principal et son degré est nul (la somme de ses coefficients est nulle).

Maintenant, pour imposer le comportement d'une fonction, on choisit un diviseur D et on impose que $\mathrm{div}\, f + D \geqslant 0$: ainsi, les pôles de f sont dans l'ensemble $\{P, n_P > 0\}$ dont l'ordre n'excède pas n_P et chaque point de l'ensemble $\{P, n_P < 0\}$ est un zéro d'ordre au moins n_P de f.

Le théorème de Riemann–Roch. L'outil fondamental utilisé ici est le théorème de Riemann–Roch dont on rappelle brièvement l'énoncé. Pour cela, introduisons l'espace vectoriel

$$\mathscr{L}(D) = \{f \in \overline{K}(\mathcal{X})^*, \quad \mathrm{div}\, f + D \geqslant 0\} \cup \{0\}.$$

Théorème 2.1 (Riemann–Roch)**.** *Soit G un diviseur. L'espace vectoriel $\mathscr{L}(G)$ a une dimension finie que l'on note $\ell(G)$. Plus précisément, si $G < 0$, $\mathscr{L}(G) = \{0\}$. Sinon, soit $W_{\mathcal{X}} = \mathrm{div}\, \omega_{\mathcal{X}}$ où $\omega_{\mathcal{X}}$ est une différentielle non nulle sur $\mathcal{X}$: alors, il existe un entier g, le genre de $\mathcal{X}$, tel que*

$$\ell(G) - \ell(W_{\mathcal{X}} - G) = \deg G - g + 1.$$

En particulier, $\ell(W_{\mathcal{X}}) = g$, $\deg(W_{\mathcal{X}}) = 2g - 2$ et $\deg G > 2g - 2 \Rightarrow \ell(G) = \deg G - g + 1$.

Remarque 2.2. Le théorème de Riemman–Roch s'énonce pour un corps algébriquement clos. Néanmoins, si G est défini sur K alors, $\mathrm{Gal}_{\overline{K}/K}$ agit sur $\mathscr{L}(G)$ et on peut alors en trouver une base constituée de fonctions dans $K(\mathcal{X})$. C'est en fait ce résultat que l'on utilise dans notre cas puisque l'application aux codes correcteurs nécessite de se placer sur $\mathbb{F}_q$ et non sur sa clôture algébrique.

Le théorème de Riemann–Roch peut se réénoncer en terme de différentielles : si G est un diviseur, on introduit l'espace vectoriel

$$\Omega(G) = \{\omega \in \Omega(\mathcal{X}),\ \mathrm{div}\, \omega - G \geqslant 0\} \cup \{0\}$$

et on dote $\delta(G)$ la dimension de cet espace vectoriel.

Théorème 2.3. *Soit $W_{\mathcal{X}}$ le diviseur d'une différentielle non nulle sur $\mathcal{X}$. Alors,*

$$\delta(G) = \ell(W_{\mathcal{X}} - G).$$

Les codes géométriques. Les deux points de vue du théorème de Riemann–Roch conduisent à la construction de deux types de codes géométriques. D'une part, on construit les codes de Reed–Solomon géométriques en choisissant une courbe lisse $\mathcal{X}$ définie sur $\mathbb{F}_q$, un diviseur positif G défini sur $\mathbb{F}_q$ et n points rationnels $(P_1, \ldots, P_n)$ de $\mathcal{X}$ n'appartenant pas au support de G. Notons D le diviseur $\sum(P_i)$ et L l'espace vectoriel $\mathscr{L}_{\mathbb{F}_q}(G) = \{f \in \mathbb{F}_q(\mathcal{X}), \mathrm{div}(f) + G \geqslant 0\} \cup \{0\}$. On considère alors le code construit par l'évaluation $\mathrm{ev}_{\mathcal{P}}$ des fonctions de L aux points P_i. Remarquons que puisque D et G ont des supports disjoints, les fonctions de f n'ont pas de pôles en les P_i.

On note ces codes $\mathcal{C}(D, G)$. Si on choisit $\deg G < n$ alors l'évaluation $\mathrm{ev}_{\mathcal{P}}$ est bien injective puisque si jamais on a $\mathrm{ev}_{\mathcal{P}}(f) = 0$ pour $f \neq 0$ alors, $\mathrm{div}(f) \geqslant D - G > 0$, ce qui est impossible. Voyons maintenant les caractéristiques des codes $\mathcal{C}(D, G)$:

Théorème 2.4. *Supposons que $\deg G < n$. Alors, le code $\mathcal{C}(D, G)$ a pour dimension*

$$k \geqslant \deg G - g + 1,$$

avec égalité si $\deg G > 2g - 2$. De plus, sa distance minimale vérifie l'inégalité

$$d \geqslant n - \deg G.$$

On remarque que l'on a l'inégalité $k + d \geqslant n - g + 1$ ou encore $R + \delta \geqslant 1 - \frac{1-g}{n}$. La première inégalité est à rapprocher de $k + d = n + 1$ que l'on a pour les codes RS, qui peuvent être interprétés comme un cas particulier.

Mentionnons maintenant la deuxième classe de codes géométriques : les codes de Goppa géométriques $\mathcal{C}^*(D, G)$, où D et G sont des diviseurs choisis comme ci-dessus. Par contre, on choisit pour L l'espace $\Omega(G - D)$ et la fonction d'évaluation $\mathrm{ev}^*_{\mathcal{P}} : \omega \to (\mathrm{Res}_{P_1}(\omega), \ldots, \mathrm{Res}_{P_n}(\omega))$. D'une manière comparable aux codes de Reed–Solomon géométriques, on constate que cette fonction d'évaluation est injective dès que $\deg G > 2g - 2$.

Théorème 2.5. *Soit G un diviseur vérifiant $\deg G > 2g-2$. Le code $\mathcal{C}^*(D,G)$ a pour dimension*

$$k \geqslant n - \deg G + g - 1$$

avec égalité si $\deg G < n$. Sa distance minimale vérifie

$$d \geqslant \deg G - 2g + 2.$$

On justifie la notation $\mathcal{C}^*$ en montrant que les codes $\mathcal{C}(D,G)$ et $\mathcal{C}^*(D,G)$ sont duaux (la matrice génératrice de l'un et la matrice de parité de l'autre).

De plus, comme dans le cas des codes de Reed–Solomon, on note que l'on a $k+d \geqslant n-g+1$. Ceci n'est pas une coïncidence puisque les deux catégories de codes sont étroitement liées :

Proposition 2.6. *Soit $\{P_1,\dots,P_n\}$ un ensemble de n points rationnels sur $\mathcal{X}$. Alors, il existe une différentielle ω avec des pôles simples en les P_i tels que $\mathrm{Res}_{P_i}(\omega)=1$. De plus, pour G ayant un support disjoint de P,*

$$\mathcal{C}^*(D,G) = \mathcal{C}(D, \operatorname{div}\omega + D - G).$$

Plus généralement, on peut montrer qu'il n'existe « globalement » qu'une seule catégorie de codes géométriques.

Proposition 2.7. *Soit C un code q–aire. Alors, on peut trouver une courbe $\mathcal{X}$ définie sur $\mathbb{F}_q$ et deux diviseurs D et G vérifiant les propriétés habituelles, tels que C soit un sous-code de $\mathcal{C}(D,G)$.*

2.3 Des courbes avec beaucoup de points rationnels.

Comme on l'a vu dans la section précédente, il apparaît fondamental de pouvoir trouver des courbes ayant beaucoup de points rationnels : ce seront de bonnes candidates pour construire des codes géométriques. Commençons par les définitions et notations suivantes.

Définition 2.8. *On note $N_q(g)$ le nombre maximum de points rationnels d'une courbe projective absolument irréductible, lisse, de genre g, définie sur $\mathbb{F}_q$. On note aussi*

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

La dernière quantité peut être motivée par la borne de Hasse–Weil qui généralise le théorème 1.4 en genre supérieur :

Théorème 2.9 (Hasse–Weil)**.** *Soit $\mathcal{X}$ une courbe projective lisse, absolument irréductible, de genre g définie sur $\mathbb{F}_q$. Alors, le nombre de points rationnels $|\mathcal{X}(\mathbb{F}_q)|$ vérifie les inégalités*

$$\big||\mathcal{X}(\mathbb{F}_q)| - (q+1)\big| \leqslant 2g\sqrt{q}.$$

Maintenant, on peut s'intéresser d'une part aux résultats asymptotiques sur $A(q)$ et d'autre part aux quantités $N_q(g)$ à q et g fixées.

Résultats asymptotiques : la borne Tvz. Le théorème de Hasse–Weil nous donne une première idée de $A(q)$ puisque l'on a facilement l'inégalité $A(q) \leqslant 2\sqrt{q}$. Néanmoins, cette borne n'est pas optimale. En fait, on a le théorème :

Théorème 2.10 (Drinfeld–Vlăduţ)**.** *On a l'inégalité*

$$A(q) \leqslant \sqrt{q} - 1,$$

qui est en fait une égalité si q est un carré.

Corollaire 2.11 (Borne Tvz)**.** *On fixe $q = p^{2k}$ un carré. Pour chaque R, il existe une asymptotiquement bonne famille de codes dont le taux d'information tend vers R et la distance relative tend vers un δ vérifiant*

$$R + \delta \geqslant 1 - \frac{1}{\sqrt{q}-1}.$$

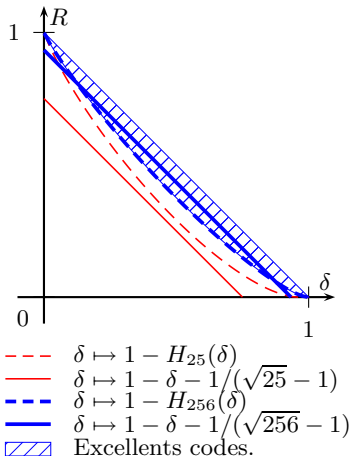


FIGURE 3: Borne TVZ.

Cette borne est meilleure que celle de Gilbert–Varshamov dès que $q \geqslant 49$, comme l'illustre la figure ci-contre où l'on a pris $q = 25$ et $q = 256$. La démonstration est intéressante puisqu'elle met vraiment en avant le lien entre excellents codes et nombres de points rationnels.

Comme q est un carré, on a égalité dans le théorème de Drinfeld–Vlăduţ : il existe une suite de courbes $\mathcal{X}_l$ définies sur $\mathbb{F}_q$ de genre g_l ayant n_l+1 points rationnels, $(P_0, \dots, P_{n_l})$, avec la propriété

$$\lim_{l\to\infty} \frac{n_l+1}{g_l} = \sqrt{q} - 1.$$

Pour chacune de ces courbes, on choisit $D = \sum_{i=1}^{n_l}(P_i)$ et $G = m_l(P_0)$ avec m_l vérifiant $m_l < n_l$ et† $\frac{m_l - g_l + 1}{n_l} \to R$. Ainsi, le code $\mathcal{C}(D,G)$ de longueur n_l vérifie, si l'on note d_l sa distance minimale et k_l sa dimension,

$$k_l + d_l \geqslant n_l + 1 - g_l \Longrightarrow R_l + \delta_l \geqslant 1 - \frac{g_l - 1}{n_l}.$$

En faisant tendre l vers l'infini et quitte à extraire une sous-suite pour que $(\delta_l)_l$ converge, on a montré le résultat.

On peut démontrer le théorème 2.10 de Drinfeld–Vlăduţ en utilisant les *conjectures de Weil* et une formule explicite due à Serre ([Ser84]). En fait, on peut exhiber une suite de courbes dans le cas $q = p^{2k}$, qui montre que $A(q) \geqslant \sqrt{q} - 1$: ce sont les courbes hermitiennes : on se place sur $\mathbb{F}_q$ avec $q = r^2 = p^{2k}$ et on considère le polynôme $F(X,Z) = X^{r+1} - Z^r - Z$. On construit une suite de courbes $\mathcal{X}_n$ définies par les idéaux‡

$$\mathcal{I}_n = \langle F(X_1,X_2), F(X_2,X_3), \dots, F(X_{n-1},X_n)\rangle \subset \mathbb{F}_q[X_1, X_2, \dots, X_n].$$

Ces idéaux sont premiers et définissent des variétés algébriques irréductibles ; comme elles sont de degré de transcendance 1, ce sont des courbes irréductibles.

Estimations de $N_q(g)$. Commençons par présenter les premiers résultats obtenus par Serre ([Ser84]). Tout d'abord, dans le cas où q n'est pas un carré, Serre améliore la borne de Weil :

Proposition 2.12 (Serre)**.** *Soit $\mathcal{X}$ une courbe projective lisse absolument irréductible. Soit g son genre. Alors, son nombre de points rationnels sur $\mathbb{F}_q$ vérifie*

$$\big||\mathcal{X}(\mathbb{F}_q)| - (q+1)\big| \leqslant g[2\sqrt{q}],$$

où $[x]$ dénote la partie entière de x.

La démonstration de ce théorème fait intervenir les célèbres *conjectures de Weil*¶ que l'on ne saurait passer sous silence dans la recherche du nombre de points rationnels sur les corps finis.

Théorème 2.13 (Conjectures de Weil)**.** *Soit $\mathcal{X}$ une courbe définie sur $\mathbb{F}_q$, lisse, complètement irréductible et de genre g. Alors, si l'on note $|\mathcal{X}(\mathbb{F}_{q^n})|$ le nombre de points rationnels de $\mathcal{X}$ sur $\mathbb{F}_{q^n}$, la fonction zêta de $\mathcal{X}$ définie par*

$$Z_{\mathcal{X}}(T) \stackrel{\text{def}}{=} \exp\left(\sum_{n=1}^{\infty} |\mathcal{X}(\mathbb{F}_{q^n})| \frac{T^n}{n}\right),$$

est une fraction rationnelle à coefficients entiers. Plus précisément, il existe un polynôme $P_{\mathcal{X}}(T)$ de degré $2g$ à coefficients entiers et de terme constant 1 tel que

$$Z_{\mathcal{X}}(T) = \frac{P_{\mathcal{X}}(T)}{(1-T)(1-qT)}.$$

Enfin, si l'on note $P_X(T) = \prod(1-\omega_j T)(1-\overline{\omega}_j T)$ alors, $|\omega_j| = \sqrt{q}$.

En particulier, $|\mathcal{X}(\mathbb{F}_q)|$ est donné par la valeur en 0 de la dérivée logarithmique de $Z_{\mathcal{X}}$: $|\mathcal{X}(\mathbb{F}_q)| = q + 1 - \sum(\omega_j + \overline{\omega}_j)$.

†. Ceci est possible puisque l'on peut supposer $R < 1 - \frac{1}{\sqrt{q}-1}$ sans quoi il n'y a rien à montrer.

‡. Il faudrait, pour être exact, homogénéiser les polynômes engendrant $\mathcal{I}_n$.

¶. On continue à les appeler *conjectures* bien qu'elles aient été démontrées en 1973 grâce aux travaux de Dwork, Grothendieck puis Deligne.

Les genres 1 et 2. On appellera l'inégalité de la proposition 2.12, la borne de Weil–Serre. Celle-ci est presque optimale en petit genre. En effet, on a un théorème de Hasse et Deuring :

Théorème 2.14. *Soit $q = p^n$ et $m = [2\sqrt{q}]$. Alors,*

$$N_q(1) = q + 1 + m$$

sauf si $m \equiv 0 \mod p$, $n \geqslant 3$ et n est impair. Sous ces conditions, $N_q(1) = q + m$.

Le cas $g = 2$ est un peu plus délicat. Avec Serre, on note $m = [2\sqrt{q}]$ et on dit que $q = p^n$ avec n impair est *spécial* s'il vérifie l'une des conditions suivantes :

(i) $m \equiv 0 \mod p$.

(ii) il existe $x \in \mathbb{Z}$ tel que $q = x^2 + 1$ ou $q = x^2 + x + 1$ ou $q = x^2 + x + 2$.

On justifiera un peu plus loin cette dernière condition un peu mystérieuse.

Théorème 2.15. *On a $N_4(2) = 10$, $N_9(2) = 20$. Sinon, si q n'est pas spécial alors,*

$$N_q(2) = q + 1 + 2m.$$

Si q est spécial alors,

$$N_q(2) = \begin{cases} q + 2m & \text{si } \{m\} > \frac{\sqrt{5}-1}{2}, \\ q + 2m - 1 & \text{sinon,} \end{cases}$$

où l'on a noté $\{x\} = x - [x]$ la partie fractionnaire de x.

Le genre 3. Le cas $g = 3$ est bien plus compliqué et est toujours l'objet de recherches à l'heure actuelle. Un problème très naturel qui apparaît dans les cas $g = 2, 3$, est de savoir s'il existe une constante dépendante de g telle que pour tout q,

$$q + 1 + 2m - N_q(g) \leqslant C(g).$$

Par exemple, les deux théorèmes 2.14 et 2.15 nous donnent $C(1) = 2$ et $C(2) = 1 + \sqrt{5}$, mais on ne sait pas montrer l'existence d'une telle constante en genre 3 et encore moins en genre quelconque ! Voyons, sans rentrer dans tous les détails, ce que l'on peut dire du genre 3. Le principal résultat général en genre 3 qui tente de répondre à la question précédente est le théorème suivant énoncé par Lauter. On peut consulter [LR07] et [Lau02].

Théorème 2.16. *Il existe une courbe (projective, lisse et absolument irréductible) de genre 3 sur $\mathbb{F}_q$ telle que*

$$\big||\mathcal{X}(\mathbb{F}_q)| - (q+1)\big| \geqslant 3m - 3,$$

où $m = [2\sqrt{q}]$.

Le problème est que l'on ne sait pas si la courbe donnée par ce théorème a le nombre maximal ou minimal de points ! A la différence des courbes elliptiques (ou hyperelliptiques), on ne peut pas résoudre simplement cette complication avec une tordue quadratique.

Pour arriver à ce théorème, on commence par prendre une courbe elliptique E qui possède le nombre maximal de points sur le corps $\mathbb{F}_q$. On considère ensuite naturellement la variété abélienne $E \times E \times E$ qui possède beaucoup de points rationnels.

Les jacobiennes de courbes permettent de passer des variétés abéliennes aux courbes. De plus, il est possible de relier le nombre de points rationnels d'une courbe C à celui de sa jacobienne $\mathrm{Jac}(C)$ (et donc à celui de toute variété abélienne A isogène *sur* $\mathbb{F}_q$ à $\mathrm{Jac}(C)$). Plus précisément, le nombre de points rationnels de C est $q + 1 + \operatorname{tr} \mathrm{Fr}_A$, ce qui explique le choix de $E \times E \times E$ pour A.

Néanmoins, toute variété abélienne n'est pas isogène sur $\mathbb{F}_q$ à la jacobienne d'une courbe. On sait déjà (en dimension $g = 3$) que lorsque l'on se place sur une clôture algébrique de $\mathbb{F}_q$, ceci n'est vrai que lorsque la variété abélienne est principalement polarisée et indécomposable.

Pour y remédier, on commence par fixer un entier a premier avec la caractéristique p du corps $\mathbb{F}_q$ et tel que $d = a^2 - 4q$ soit négatif : ce sera le discriminant de l'équation caractéristique du Frobenius d'une courbe elliptique E dont la trace est a. Avec le théorème 2.14 on peut prendre $a = -m$ où $-m + 1$. On pose $R = \mathbb{Z}[X]/(X^2 - aX + q)$ qui est un ordre (engendré par le Frobenius) dans le corps quadratique imaginaire $\mathbb{Q}(\sqrt{d})$. Pour simplifier, on suppose que c'est l'ordre maximal, c'est-à-dire l'anneau des entiers. On note $\mathrm{Ab}(a, q)$ la catégorie des variétés abéliennes isogènes sur $\mathbb{F}_q$ à un produit de copies de E et $\mathrm{Mod}(R)$ la catégorie des R–modules sans torsion de type fini. Par exemple, $\mathrm{Hom}(E, A)$ est un objet de cette catégorie.

Proposition 2.17. *Le foncteur $T : \mathrm{Ab}(a,q) \to \mathrm{Mod}(R)$, défini par $T(A) = \mathrm{Hom}(E, A)$, est une équivalence de catégorie. Le foncteur S inverse de T est donné par la variété abélienne $S(L) = L \otimes_R E$ que l'on abrègera en A_L.*

En fait, munir A_L d'une polarisation revient exactement à faire de L un R–module hermitien :

Théorème 2.18 (Serre)**.** *Une variété abélienne A_L principalement polarisée est indécomposable si et seulement si L est indécomposable comme module hermitien (de discriminant 1).*

Ainsi, pour obtenir une variété abélienne A indécomposable, isogène sur $\mathbb{F}_q$ à $E \times E \times E$, il faut et il suffit qu'il existe un R–module hermitien indécomposable. Un théorème, énoncé par Hoffmann, règle le cas des modules hermitiens indécomposables en dimension 2 et 3 :

Théorème 2.19. *On rappelle que d est le discriminant de l'anneau R. Alors, il n'existe aucun R–module hermitien indécomposable de discriminant 1 si et seulement si*

(i) on est en dimension 2 et $d = -3, -4$ ou -7,

(ii) on est en dimension 3 et $d = -3, -4, -8$ ou -11.

Par exemple, en dimension 2, on peut vérifier que les exceptions correspondent exactement, outre le cas $m \equiv 0 \mod p$, aux discriminants qui apparaissent dans le cas *spécial (ii)* du théorème 2.15. En dimension 3, c'est ce qui explique, dans le théorème 2.16, le défaut de 3 par rapport à la borne de Weil–Serre.

Il nous reste encore un écueil : l'isogénie entre $E \times E \times E$ n'est pas forcément définie sur $\mathbb{F}_q$. En fait on a le résultat :

Théorème 2.20. *Soit L un R–module hermitien indécomposable de rang 3. Alors, il existe une courbe C définie sur $\mathbb{F}_q$ telle que $\mathrm{Jac}(C)$ est isomorphe sur $\mathbb{F}_q$ à A_L **ou** à sa tordue quadratique. De plus, si C n'est pas hyperelliptique, les deux cas s'excluent.*

On trouve ainsi une courbe de genre 3 dont le nombre de points rationnels sur $\mathbb{F}_q$ est soit $q+1+3m$ soit $q+1-3m$, ce qui, avec une étude détaillée des cas du théorème 2.19 en genre 3, conduit à une preuve du théorème 2.16.

2.4 Conclusion – Questions ouvertes.

Que ce soit à travers la cryptographie ou les codes correcteurs d'erreurs, compter les points d'une variété algébrique définie sur un corps fini s'avère un sujet riche dont on connaît déjà de nombreuses applications pratiques. Paradoxalement, il reste encore beaucoup de questions naturelles en suspens. Même pour les résultats asymptotiques que le théorème de Drinfeld–Vlăduţ semble régler de façon satisfaisante, il reste une zone d'ombre. Ce théorème traite le cas d'une puissance paire d'un nombre premier, mais qu'en est-il du cas impair ? Serre a montré que l'on pouvait minorer $A(q)$ par $c \log q$ (pour une constante $c > 0$) mais l'encadrement $c \log q \leqslant A(q) \leqslant \sqrt{q} - 1$ est loin d'être précis !

Les estimations de $N_q(g)$, centrales dans la construction de codes géométriques, sont finalement encore assez mal maîtrisées : la section précédente présente la majeure partie de ce que l'on connaît à l'heure actuelle quand on fixe un genre. Une autre approche consiste à choisir des formes particulières pour q, ou encore de chercher des familles infinies pour lesquelles on a une propriété intéressante sur $N_q(g)$,... De plus, outre la recherche théorique de courbes optimales, il se pose aussi le problème de la construction effective (et efficace) de telles courbes.

Bibliographie

[Lau02] K. Lauter – « The maximum or minimum number of rational points on genus three curves over finite fields », *Compositio Mathematica* **134** (2002), p. 87–111, avec un appendice de J.-P. Serre.

[LR07] G. Lachaud et C. Ritzenthaler – « On a conjecture of Serre on abelian threefolds », `http://arxiv.org/abs/0710.3303v1`, 2007.

[Sch85] R. Schoof – « Elliptic curves over finite fields and the computation of square roots mod p », *Mathematics of Computation* **44** (1985), no. 170, p. 483–494.

[Ser84] J.-P. Serre – « Nombres de points des courbes algébriques sur $\mathbb{F}_q$ », Oeuvres – Collected papers, vol. 3, Springer, 1972–1984, p. 664–668.

[Sil86] J. H. Silverman – *The arithmetic of elliptic curves*, GTM 106, Springer, 1986.

[vL82] J. H. van Lint – *Introduction to coding theory*, GTM 86, Springer, 1982.

Université Paris Diderot – Paris 7

Master 2e année
Mathématiques Fondamentales

Diverses applications de la géométrie algébrique à la théorie de l'information

Ivan Boyer

sous la direction de

Jean-François Mestre

15 juin 2009

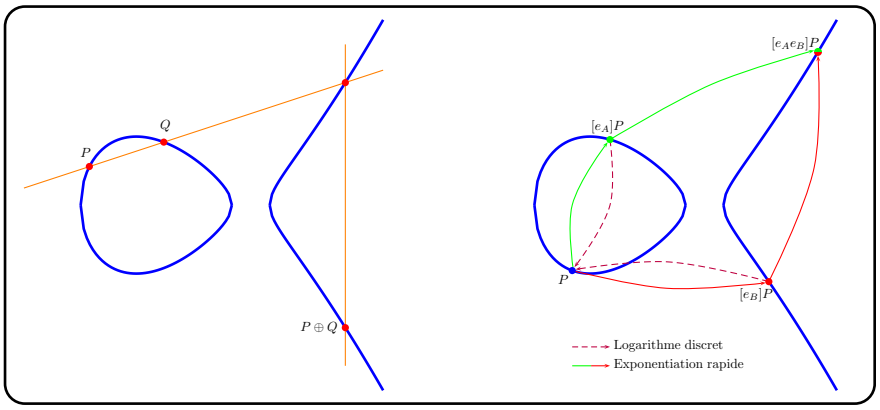


Table des matières

Liste des Algorithmes

Table des figures

1 Introduction.

Dans notre société de communication, l'échange de l'information prend une place quasi centrale. Plusieurs problématiques se posent au moment d'échanger ces informations. Nous nous concentrerons sur deux des plus importantes : d'une part, s'assurer que personne ne puisse intercepter et lire un message et d'autre part être sûr que le message envoyé est identique au message reçu. A première vue, les techniques utilisées dans ces deux domaines sont assez éloignées. Néanmoins, la géométrie algébrique prend une place assez importante, notamment dans la possibilité de trouver des courbes ayant beaucoup de points rationnels.

La première problématique a donné naissance à *la cryptographie* : celle-ci était présente dès l'antiquité comme peut en témoigner le code de Jules César. Néanmoins, jusqu'à la moitié du siècle dernier, les procédés utilisés étaient symétriques, nécessitant de se mettre d'accord sur une clé privée. Cela pose des problèmes tant sur le plan de la sécurité que sur le plan pratique : ce procédé utilisé seul ne permettrait pas les transactions sur internet telles que nous les connaissons.

Ce sont des procédés asymétriques, dits *à clés publiques*, qui ont permis cette explosion des transactions en ligne. Ce domaine est assez récent, tout du moins à l'échelle du développement de la cryptographie ! Le "monopole" est pour le moment assuré par le système Rsa, qui date pratiquement de l'invention de la cryptographie asymétrique. Néanmoins, ce système demande une puissance de calcul assez importante et un concurrent de plus en plus sérieux commence à retenir l'attention : la cryptographie sur courbes elliptiques.

Cette dernière nécessite de trouver des courbes elliptiques dont le groupe des points rationnels a un ordre grand et premier (ou tout du moins possédant un grand facteur premier). Ainsi, un prérequis à la construction de tels systèmes est de savoir compter ce nombre de points rationnels. C'est en fait un problème polynomial comme l'a montré Schoof dans les années 80. La première partie est consacrée à montrer cette assertion ainsi qu'à donner des améliorations et des applications de ce résultat. On verra notamment l'application surprenante au problème de l'extraction de racines carrés dans un corps fini, sans utiliser l'hypothèse de Riemann.

La seconde problématique est beaucoup plus récente puisque liée aux problèmes de fiabilité des moyens de communications modernes (transmissions radios, électriques, micro-gravures,...) Un des premiers codes correcteurs est le "*Alpha, Bravo, Charlie*" des communications radio. Néanmoins, ce code redondant ne saurait être utilisé de la même manière aux Cds, puisque l'on multiplie la longueur du message par un facteur au moins 5 !

De même que l'importance grandissante des transactions internet a contribué au développement de la cryptographie asymétrique, l'exploration spatiale lointaine est un véritable moteur dans la recherche de *codes correcteurs d'erreurs* efficaces, c'est-à-dire sans trop de redondance et pouvant corriger de nombreuses erreurs.

Pendant près de trente ans, personne n'a réussi à améliorer la borne "élémentaire" de Gilbert–Varshamov, à tel point qu'on l'a cru optimale. Il a fallu attendre l'utilisation de la géométrie algébrique (via notamment le théorème de Riemann–Roch) pour pouvoir améliorer cette borne. Après les définitions et l'étude de ces codes géométriques, la deuxième partie cherche à montrer l'importance de trouver des courbes algébriques ayant beaucoup de points rationnels dans la construction de ces codes linéaires, asymptotiquement meilleurs que la borne de Gilbert–Varshamov. La fin de cette partie est un aperçu de l'état actuel des recherches dans ce domaine.

Notons finalement, s'il fallait encore insister sur le parallèle *cryptographie–codes correcteurs d'erreurs*, que McEliece a proposé à la fin des année 70 un cryptosystème basé sur les codes géométriques (plus précisément le code de Goppa sur la droite projective) pour le cryptage, et la complexité du problème général de décodage pour la sécurité. Si ce n'est la longueur de la clé, ce système possède lui aussi de nombreux avantages sur Rsa, notamment la résistance aux algorithmes quantiques.

Je tiens à remercier J.-F. Mestre pour m'avoir fait découvrir ce domaine particulièrement riche à la croisée de la géométrie algébrique et de la théorie de l'information. Je le remercie aussi pour ses précieux conseils de lectures ainsi que ses explications particulièrement éclairantes.

2 Compter les points rationnels d'une courbe elliptique.

2.1 Enjeux cryptographiques.

2.1.1 Complexité algorithmique.

Avant de se lancer dans les algorithmes de calcul du nombre de points sur une courbe elliptique, voici quelques conventions utilisées dans la suite :

Définition 2.1 (Notation O)**.** *Soient f, g deux fonctions réelles de k variables.*

On dit que f est dominée *par g s'il existe des constantes C et n telles que pour $n_i \geqslant n$, on ait $|f(n_1, \ldots, n_k)| \leqslant Cg(n_1, \ldots, n_k)$.*

On dit que f est dominée par g à un facteur logarithmique près *s'il existe une constante $p > 0$ et telle que $f(n_1, \ldots, n_k) = O(g(n_1, \ldots, n_k) \log^p(g(n_1, \ldots, n_k)))$.*

On utilisera souvent des bornes utilisant la fonction logarithme : on la notera log sans préciser la base (qui est absorbée par le O). Néanmoins, on l'utilisera implicitement en base 2 (notamment en raison de la représentation des entiers en mémoire, de l'utilisation de techniques *diviser pour régner*, ...).

Définition 2.2 (Taille des données)**.** *On appellera taille des données la quantité d'espace mémoire qu'il faut pour stocker les données (initiales, intermédiaires, finales) au cours d'un algorithme.*

Remarque 2.3. Cette notion est très imprécise et dépend fortement du choix que l'on fait pour représenter les objets. Néanmoins, on l'utilisera ici dans les cas simples suivants :

(i) Un entier n nécessite $O(\log n)$ bits pour être stocké.

(ii) Un polynôme de degré d dont les coefficients sont des entiers bornés par M nécessite $O(d \log M)$ bits en mémoire.

(iii) Un élément de $\mathbb{F}_q$ nécessite $O(\log q)$ bits pour être représenté : en effet, si on note $q = p^r$, on représente cet élément par un polynôme de degré au plus $r - 1$ à coefficients dans $\mathbb{F}_p$: il faut donc $r \log p = \log q$ bits pour le stocker.

Définition 2.4 (Complexité d'un problème)**.** *On appelle* opération élémentaire*, toute opération qu'un ordinateur classique sait réaliser en temps constant : par exemple, un test booléen, une addition de deux bits avec retenue, un accès mémoire (dans un tableau par exemple), ...*

On dit qu'un problème s'exécute en temps $O(f)$ (sous-entendu en la taille des données) si le nombre d'opérations élémentaires effectuées lors de l'exécution du programme est dominée par f lorsque la taille des données tend vers l'infini.

On dit qu'un problème est polynomial *si on peut trouver une domination f qui est un polynôme. On dit qu'un problème est* exponentiel *si la fonction f s'écrit $f(x) = \exp P(x)$ pour un polynôme P.*

On dit enfin qu'un problème est dans la classe **P** *s'il existe un algorithme polynomial qui permet de le résoudre. On dit qu'il est* **NP** *s'il existe un algorithme polynomial qui permet de tester si une solution est valide.*

Par exemple, on verra plus tard que l'algorithme de Schoof a permis de montrer que le calcul du nombre de points rationnels d'une courbe elliptique était dans la classe **P**. Le problème du logarithme discret que l'on introduit dans la section 2.1.2 est quant à lui **NP**.

Afin d'estimer la vitesse d'exécution d'un algorithme, voici quelques résultats de complexité classiques. On pourra par exemple consulter [Coh00] ou [GG03]

Proposition 2.5 (Complexité des algorithmes "naïfs".)**.**

(i) L'addition et la soustraction de deux entiers de taille n se font en $O(n)$ opérations.

(ii) La multiplication est quadratique en utilisant l'algorithme naïf.

(iii) La division euclidienne de a par b (avec $0 < b < a$) se réalise en $O(\log a(\log a - \log b))$.

(iv) L'algorithme d'Euclide permet de calculer le pgcd de deux entiers $a > b > 0$ en $O(\log a \log b)$ opérations élémentaires

Proposition 2.6 (Algorithmes rapides)**.**

(i) La multiplication de deux entiers de taille n se réalise grâce à la transformée de Fourier rapide en $O(n \log n \log\log n) = \tilde{O}(n)$.

(ii) La multiplication de deux polynômes de degré n peut s'effectuer en $\tilde{O}(n)$

(iii) La division euclidienne d'un polynôme $F \in \mathbb{A}[X]$ par un polynôme unitaire G (vérifiant $\deg F \geqslant \deg G$) peut se calculer en $\tilde{O}(\deg F)$ opérations $(+, -, \times)$ dans l'anneau $\mathbb{A}$.

On note l'importance, dans ce dernier point, de toujours réaliser des divisions euclidiennes par des polynômes unitaires, la division étant souvent plus coûteuse que les autres opérations. En application, voyons ce que cela nous apporte pour calculer dans les corps finis :

Exemple 2.7 (Calculs dans les corps finis)**.**

(i) L'addition dans $\mathbb{F}_p$ se fait en temps $O(\log p)$, la multiplication en $\tilde{O}(\log p)$ par transformée de Fourier rapide et l'inverse en $O((\log p)^2)$ grâce à l'algorithme d'Euclide étendu sur les entiers.

(ii) L'addition dans un corps fini à q éléments se réalise en $O(\log q)$: il s'agit de l'addition de deux polynômes de degré au plus $q-1$ dont les coefficients sont de taille $\log p$.

(iii) La multiplication dans $\mathbb{F}_q$ nécessite de multiplier deux polynômes de degré au plus $r-1$ dont les coefficients sont de taille $\log p$: cela demande $\tilde{O}(r)$ opérations dans $\mathbb{F}_p$. Il reste à faire une division euclidienne, ce qui donne au final $\tilde{O}(\log q)$ opérations.

(iv) Pour la division, chaque itération de l'algorithme d'Euclide étendu s'exécute en $O(d(\log p)^2)$ opérations : on a une division euclidienne avec des polynômes dont le degré est borné par d mais qui ne sont pas forcément unitaires, suivie de $O(1)$ multiplications pour mettre à jour les coefficients de Bezout. Comme on a au plus d itérations, cela donne une complexité de $O((\log q)^2)$.

Voyons pour finir une technique assez centrale et très efficace dans le calcul de puissances.

Proposition 2.8 (Exponentiation Rapide)**.** *Soit G un ensemble muni d'une loi de composition interne associative. Soit $a \in G$. On peut calculer, pour un entier $e \geqslant 1$, a^e en appliquant au plus $2\lceil \log_2 e \rceil$ fois la loi de composition interne.*

Démonstration. On écrit $e = \sum_{i=0}^{k} e_i 2^i$ et on calcule dans une boucle à chaque itération $b_i = a^{2^i}$ puis $a_i = a^{\sum_{k \leqslant i} e_i 2^i}$. Le calcul de b_i se fait à partir de b_{i-1} avec une application de la loi de composition. Celui de a_i se réalise avec a_{i-1} et b_i et demande une opération seulement lorsque $e_i = 1$. On a bien au plus $2k$ appels à la loi de composition interne. □

2.1.2 Courbes elliptiques et cryptographie.

Comme on l'a évoqué dans l'introduction, du code de Jules César à la machine Enigma, la cryptographie a bien longtemps reposé sur des procédés dits symétriques : deux personnes souhaitant communiquer se mettent d'accord sur une clé secrète, qu'ils utilisent pour coder et décoder. Ces systèmes, toujours utilisés (comme l'AES), présentent l'avantage d'un codage et décodage très efficace. Néanmoins, l'inconvénient majeur est celui posé par la clé secrète : on ne peut se l'échanger à distance. C'est là qu'intervient la cryptographie asymétrique, dite à clé publique.

Cryptographie à clé publique. En 1985, N. Koblitz et V. Miller proposèrent (indépendemment) d'utiliser des courbes elliptiques dans des applications cryptographiques à clé publique. Exposons brièvement les idées sous-jacentes, afin de montrer l'importance d'être capable de compter efficacement le nombre de points rationnels d'une courbe elliptique. Pour une description bien plus avancée, on pourra consulter la "bible" [CF06].

Tout d'abord, ces techniques cryptographiques reposent sur la notion de fonction à sens unique :

Définition 2.9 (Fonction à sens unique)**.** *Soit $f : \Sigma \to \Sigma'$ une fonction. On dit qu'elle est à* sens unique *si*

(i) Pour $x \in \Sigma$, $f(x)$ peut être calculé en temps polynomial.

(ii) Il n'y a pas d'algorithme polynomial tel, qu'étant donné $y \in \Sigma'$, il décide si $y \notin \mathrm{im}(f)$ et donne dans le cas contraire un $x \in \Sigma$ tel que $f(x) = y$.

On dit de plus qu'une telle fonction possède une trappe *si connaissant une information supplémentaire, il soit alors possible d'inverser f en temps polynomial.*

Personne n'a encore exhibé une fonction à sens unique et pour cause ! En effet, il serait alors facile de montrer que **P**≠**NP**. L'une des fonctions, supposée à sens unique, la plus connue, est celle à base du protocole Rsa : c'est l'élévation à une certaine puissance e dans $(\mathbb{Z}/N\mathbb{Z})^*$ avec $N = pq$ produit de deux grands nombres premiers. Pour inverser cette fonction, il faut connaître l'inverse de e dans $(\mathbb{Z}/N\mathbb{Z})^*$. Ceci peut se réaliser par exemple à l'aide de $\varphi(n)$ qui est notre trappe. Celle-ci est réputée dure à obtenir puisque équivalente à factoriser N.

Echange de clés et courbes elliptiques. Introduisons maintenant le protocole d'échange de clés introduit par Diffie et Hellman dès 1976. Alice et Bob commencent par décider d'un groupe $(G, \oplus)$ et d'un élément $P \in G$. Ensuite, ils choisissent secrètement des clés e_A et e_B puis rendent publiques les quantités $[e_A]P$ et $[e_B]P$ (où $[m]$ désigne l'application de m fois la loi $\oplus$). Ensuite, chacun peut calculer la quantité $[e_A e_B]P$ puis en extraire une clé identique (par exemple les k derniers bits de la représentation binaire de cet élément). Une fois cette clé déterminée, Alice et Bob peuvent s'échanger des données grâce à des techniques cryptographiques symétriques. Comme ce procédé ne dépend que du sous-groupe engendré par P, on peut choisir en fait $G = \langle P \rangle$ cyclique.

La fonction à sens unique utilisée ici est la fonction $n \mapsto [n]P$. C'est donc sur la fonction inverse que la sécurité de ce protocole d'échange de clés est basée et ceci motive la définition suivante.

Définition 2.10 (Problème du Logarithme Discret, Dlp [†])**.** *Soit $G = \langle b \rangle$ un groupe cyclique d'ordre n. On appelle* logarithme discret *la fonction*

$$\begin{aligned} \log_b : G &\longrightarrow \mathbb{Z}/n\mathbb{Z} \\ b^k &\longmapsto k \mod n \ . \end{aligned}$$

Par exemple, pour$G = (\mathbb{Z}/n\mathbb{Z}, +)$ et $b \in (\mathbb{Z}/n\mathbb{Z})^*$ la fonction $\log_b$ est simplement la multiplication par b^{-1} : dans ce cas, le Dlp est polynomial.

Une autre idée consiste à utiliser le groupe cyclique $\mathbb{F}_q^*$ d'un corps fini. Dans ce cas, il existe des algorithmes sous-exponentiels pour résoudre le Dlp, par exemple en temps

$$O\left(\exp(O(1)(\log q)^{\frac{1}{3}}(\log\log q)^{\frac{2}{3}})\right).$$

Il existe des algorithmes généraux pour résoudre ce problème du logarithme discret, c'est-à-dire n'utilisant aucune propriété particulière du groupe G, la loi de groupe étant donnée par une "boîte noire". Tout d'abord, remarquons que si le cardinal de $G = \langle P \rangle$ peut se décomposer en $|G| = mn$ avec m et n premiers entre eux, le Dlp est plus facile. En effet, supposons que l'on cherche $\log_P(Q)$: on commence par chercher $r = \log_{mP}(mQ)$ et $s = \log_{nP}(nQ)$, ce qui constitue deux Dlp sur des groupes cycliques d'ordre n et m. On reconstruit la solution originale avec le théorème chinois : $um + vn = 1$ et ainsi $\log_P(Q) = umr + vsn$
Si maintenant $|G| = p^k$ pour un nombre premier p, alors, on commence par résoudre $r_1 = \log_{[p^{k-1}]P}([p^{k-1}]Q)$ puis on se place dans le groupe cyclique $\langle [p]P \rangle$ et on résout récursivement le Dlp pour $Q - [r_1]P$. Il suffit donc au final de résoudre k fois le Dlp sur des groupes d'ordre p.

Ainsi, résoudre le Dlp revient essentiellement au cas $n = |G|$ premier. Dans cette situation, que ce soit l'algorithme ρ–de Pollard, l'algorithme *pas de bébés, pas de géants* (que l'on rencontrera dans la section 2.3.1), ou d'autres, aucun algorithme "général" ne peut donner une meilleure complexité que $O(\sqrt{n})$, comme l'a montré Shoop dans [Sho97].

†. Discrete Logarithm Problem en anglais.

L'idéal serait donc de trouver un groupe sur lequel on n'ait aucune information autre que son caractère cyclique, afin d'être contraint à utiliser des algorithmes généraux pour résoudre le DLP. C'est ici qu'interviennent les courbes elliptiques. En effet, jusqu'à aujourd'hui, il semble que ce soit le cas pour le groupe des points rationnels (sur un corps fini) d'une courbe elliptique, choisie suffisamment générale †. Ainsi, si l'on travaille sur un corps fini de taille k, on peut espérer une sécurité de l'ordre de $\frac{k}{2}$. Dès lors, si l'on souhaite une sécurité de 128 bits, un codage à base de courbes elliptiques demande de travailler sur des données de taille 256 bits lorsque RSA a besoin d'une clé de l'ordre de 3072 bits ‡.

Tout ceci motive donc la recherche de tels groupes et il apparaît naturel et crucial de savoir déterminer efficacement le nombre de points rationnels d'une courbe elliptique définie sur un corps fini : c'est à ceci que le reste de cette partie est consacré.

2.2 Courbes elliptiques : généralités.

2.2.1 Notations et conventions.

Dans tout ce paragraphe, on notera E une courbe elliptique (lisse) définie sur un corps $\mathbb{F}_q$ à q éléments dont on notera p la caractéristique. On note aussi pour $\mathbb{F}$ une extension de $\mathbb{F}_q$, $E(\mathbb{F})$ l'ensemble des points à cordonnées dans $\mathbb{F}$ appartenant à E. On rappelle que c'est un groupe dont l'élément neutre est le point à l'infini, noté $\mathcal{O}$.

Dans un souci de simplification, on considérera que la courbe E est donnée par une équation de Weierstrass "simplifiée" de la forme $y^2 = x^3+ax+b$, avec $\Delta = 4a^3-27b^2 \neq 0$. Cela est toujours possible en caractéristique $p \geqslant 5$ mais par exemple, en caractéristique 2, une telle équation donne systématiquement une courbe singulière. Malgré tout, sauf mention contraire, on peut généraliser les idées exprimées ci-dessous en caractéristique 2 ou 3.

On confondra parfois un point P et ses coordonnées affines (x, y) en notant par exemple abusivement, pour un morphisme φ, $\varphi(P) = \varphi(x, y)$. On prendra garde qu'avec ces notations et une équation de Weierstrass simplifiée, on aura $-(x, y) = (x, -y)$, le premier signe "$-$" se référant à la loi de groupe sur E.

2.2.2 Calculer sur une courbe elliptique.

Avant d'exposer divers algorithmes permettant de calculer le nombre de points rationnels sur une courbe elliptique, il est important de rappeler comment et à quel coût on peut calculer dans le groupe $E(\mathbb{F}_q)$. Les formules ci-dessous, relativment simples, sont valables pour une équation $y^2 = x^3 + ax + b$ mais peuvent se généraliser.

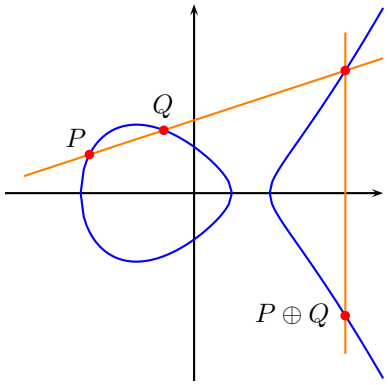


FIGURE 2: Loi de groupe sur une courbe elliptique.

Proposition 2.11 (Formule d'addition)**.** *Soient (x_1, y_1) et (x_2, y_2) deux points de E distincts de $\mathcal{O}$, non opposés l'un de l'autre. La loi d'addition par cordes et tangentes illustrée ci-contre est donnée algébriquement par les formules :*

$$\begin{cases} x_3 = \lambda^2 - x_1 - x_2 \\ y_3 = \lambda(x_1 - x_3) - y_1 \end{cases} \quad \text{où } \lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & \text{si } x_1 \neq x_2, \\ \dfrac{3x_1 + a}{2y_1} & \text{sinon.} \end{cases}$$

Ainsi, une addition dans $E(\mathbb{F}_q)$ se résume à un nombre constant d'opérations dans le corps fini $\mathbb{F}_q$, ce qui se réalise en $O((\log q)^2)$.

†. Il existe par exemple de bons algorithmes pour les courbes elliptiques supersingulières.

‡. Cela permet d'obtenir des protocoles plus rapides mais dont la sécurité peut être mise en question. On dispose en effet d'un recul insuffisant sur le problème du logarithme discret appliqué aux courbes elliptiques comparé à celui de la factorisation d'entiers.

Grâce à ces formules on peut calculer comme dans n'importe quel groupe abélien : on peut notamment calculer la multiplication par $m \in \mathbb{N}$ (notée dans dans ce contexte $[m]$) par exponentiation rapide en $\tilde{O}(\log m(\log q)^2)$. Néanmoins, comme on le verra dans la suite, il est intéressant de savoir calculer une expression du morphisme $[m]$ en lui-même. Pour cela, rappelons la notion centrale d'isogénie.

Définition 2.12 (Isogénies)**.** *On dit qu'un morphisme algébrique φ entre deux courbes elliptiques E_1 et E_2 est une* isogénie *si $\varphi(\mathcal{O}_1) = \mathcal{O}_2$. Si de plus φ n'est pas constante, on dit que E_1 et E_2 sont* isogènes*.*

Par exemple, la multiplication $[m]$ est une isogénie. La condition sur le point à l'infini semble faible. Il n'en est rien :

Proposition 2.13. *Une isogénie $\varphi : E_1 \to E_2$ est aussi un morphisme de groupe.*

Enfin, voici quelques propriétés de base vérifiées par les isogénies. La notion d'isogénie duale justifie la définition *symétrique* de courbes isogènes énoncée ci-dessus.

Proposition 2.14. *Une isogénie φ non nulle est surjective et possède un noyau fini. Lorsqu'elle est séparable, on a en plus $|\ker \varphi| = \deg \varphi$.*

Pour toute isogénie $\varphi : E_1 \to E_2$ il existe une unique isogénie $\hat{\varphi} : E_2 \to E_1$ vérifiant

$$\hat{\varphi} \circ \varphi = [m]_{E_1} \text{ et } \varphi \circ \hat{\varphi} = [m]_{E_2},$$

où $m = \deg \varphi$. On a de plus $\widehat{\lambda \circ \varphi} = \hat{\lambda} \circ \hat{\varphi}$ et $\widehat{\varphi + \psi} = \hat{\varphi} + \hat{\psi}$, pour des isogénies $\lambda : E_2 \to E_3$ et $\psi : E_1 \to E_2$.

On a en particulier $\hat{\hat{\varphi}} = \varphi$ ce qui justifie la qualification de dualité. On définit finalement :

Définition 2.15 (Norme et trace)**.** *Soit $\varphi : E \to E$ une isogénie. On définit sa* norme *et sa* trace *par*

$$\mathrm{N}\,\varphi = \varphi \circ \hat{\varphi} \in \mathbb{N} \quad et \quad \mathrm{tr}\,\varphi = \varphi + \hat{\varphi} \in \mathbb{Z}.$$

Pour des précisions sur ce sujet ainsi que sur de nombreux points de la suite de cette partie, on peut se référer à (l'incontournable) [Sil86].

On peut alors énoncer une proposition qui donne la forme particulière d'une isogénie entre courbes définies par des équations de Weierstrass (simplifiées) :

Proposition 2.16. *Soient E, E' deux courbes elliptiques données par une équation de Weierstrass simplifiée sur un corps K et $\varphi : E \to E'$ une isogénie définie sur K. Alors, si $P = (x, y) \in E$, on a l'existence d'une fraction rationnelle $I \in K(x)$ et d'une constante $c \in K$ telle que :*

$$\varphi(P) = (I(x), cyI'(x)).$$

De plus, $\deg I = 1$ *et lorsque φ est séparable, on peut écrire sous forme irréductible $I(x) = \frac{N(x)}{D(x)}$ avec*

$$D(x) = \prod_{Q \in (\ker \varphi)^*} (x - x_Q).$$

Démonstration. Tout d'abord, comme φ est un morphisme algébrique défini sur K, il s'écrit $\varphi(x, y) = (A(x, y), B(x, y))$ où $A, B \in K(E)$. Ensuite, φ est un morphisme de groupe et donc $\varphi(-(x, y)) = -\varphi(x, y)$: cela se traduit par $A(x, -y) = A(x, y)$ et $B(x, -y) = -B(x, y)$. Ainsi, les puissances de y intervenant dans A sont toutes paires et en utilisant l'équation de Weierstrass simplifiée, on peut choisir un représentant I de A ne faisant intervenir que la variable x. Pour B, on peut faire de même en remarquant que $\frac{B(x,y)}{y}$ vérifie les mêmes propriétés que pour A.

On a alors $\varphi(x, y) = (I(x), yJ(x))$. Mais alors, si on note ω_E et $\omega_{E'}$ les différentielles invariantes sur E et E', on a $\varphi^*\omega_{E'} = \lambda\omega_E$ avec $\lambda \in \overline{K}(E)$ puisque les différentielles sur la courbe E forment un $\overline{K}(E)$–espace vectoriel de dimension 1. En passant aux diviseurs dans l'égalité précédente et en se rappelant que $\mathrm{div}\,\omega_E = 0 = \mathrm{div}\,\omega_{E'}$, on a $\mathrm{div}\,\lambda = 0$ et donc $\lambda \in \overline{K}^*$. Maintenant, on peut aussi réécrire cette égalité :

$$\lambda \frac{\mathrm{d}x}{y} = \lambda\omega_E = \varphi^*\omega_{E'} = \frac{\mathrm{d}I(x)}{yJ(x)}$$

et donc $J(x) = I'(x)$. Enfin, comme φ est défini sur K, $I \in K(x)$ et ainsi $c = \frac{1}{\lambda} \in K$.

Enfin, les points du noyau de φ s'envoient sur $\mathcal{O}$ et doivent donc annuler le dénominateur. De même, un zéro du dénominateur correspond à un point du noyau. Soit maintenant $Q \in (\ker \varphi)^*$ d'ordre 2. On suppose pour simplifier que x_Q est racine simple de $x^3 + a'x + b'$ (équation de E') ; alors, $\mathrm{ord}_Q(x - x_Q) = 2$. Si Q n'est pas d'ordre 2, $y_Q \neq 0$ et $\mathrm{ord}_Q(x - x_Q) = 1$. Maintenant, comme φ est supposée séparable, elle est non ramifiée. Ainsi, $\mathrm{ord}_Q(\varphi^* x) = e_\varphi(Q)\,\mathrm{ord}_{\mathcal{O}'} x = -2$, c'est-à-dire $\mathrm{ord}_Q\left(\frac{N(x)}{D(x)}\right) = -2$ Comme $D(x_Q) = 0$ et que D et N sont premiers entre eux, on en déduit que lorsque Q n'est pas d'ordre 2, x_Q est racine double de D, simple autrement : on retrouve bien l'expression de D annoncée. □

Remarque 2.17. (Formules de Vélu). On note $y^2 = x^3 + ax + b$ une équation de E. Dans le cas † où $c = 1$, des formules dues à Vélu ([Vél71]) donnent une expression encore plus explicite de φ :

$$I(x) = x + \sum_{Q \in (\ker \varphi)^*} \left(x - x_Q - \frac{3x^2 + a}{x - x_Q} + 2\frac{x^3 + ax + b}{(x - x_Q)^2} \right).$$

De plus, si l'on note $D(x) = x^{l-1} - \sigma x^{l-2} + \sigma_2 x^{l-3} - \sigma_3 x^{l-4} + \dots$ où $l = \deg \varphi$ alors, une équation de E' est donnée par $y^2 = x^3 + a'x + b'$ où

$$a' = a - 5(a(l-1) + 3(\sigma^2 - 2\sigma_2)) \text{ et } b' = b - 7(3a\sigma + 2b(l-1) + 5(\sigma^3 - 3\sigma\sigma_2 + 3\sigma_3)).$$

Notons enfin que c'est le polynôme $D(x)$ qui est souvent le plus intéressant dans les applications et on peut mentionner l'équation différentielle :

$$\frac{N(x)}{D(x)} = lx - \sigma - (3x^2 + a)\frac{D'(x)}{D(x)} - 2(x^3 + ax + b)\left(\frac{D'(x)}{D(x)}\right)'.$$

Exemple 2.18. Soit m premier avec la caractéristique du corps de telle sorte que $[m]$ soit séparable. Avec la formule bien connue $[m]^* \omega_E = m\omega_E$, on en déduit que l'isogénie $[m] : E \to E$ s'écrit sous la forme

$$(x, y) \mapsto \left(\frac{N(x)}{D(x)}, \frac{y}{m}\left(\frac{N(x)}{D(x)}\right)' \right).$$

De plus, si m est impair, $D(x) = g(x)^2$ avec $\deg g = \frac{m^2-1}{2}$ et si m est pair, on peut aussi écrire $D(x) = yg(x)^2$ (où l'on rappelle que $y^2 = x^3 + ax + b$). Cette remarque conduit à la définition suivante :

Définition 2.19 (Polynômes de division)**.** *On appelle* polynômes de division *les polynômes $\Psi_m \in K[x] \oplus yK[x]$ tels qu'avec les notations ci-dessus, $\Psi_m(x, y) = mg(x)$ si m est impair et $\Psi_m(x, y) = myg(x)$ si m est pair.*

En fait, on peut être un peu plus précis en affirmant que $\Psi_m \in \mathbb{Z}[x, a, b] \oplus y\mathbb{Z}[x, a, b]$ (où la courbe est donnée par $y^2 = x^3 + ax + b$). Cela se déduit facilement de la proposition suivante (dont la démonstration est simplement fastidieuse, on pourra consulter [Sil86] pour les étapes) :

Proposition 2.20. *On peut calculer récursivement les polynômes de division grâce aux formules suivantes :*

$$\begin{aligned}
\Psi_1 &= 1, \qquad \Psi_2 = 2y, \\
\Psi_3 &= 3x^4 + 6ax^2 + 12bx - a^2, \\
\Psi_4 &= 4y(x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - 8b^2 - a^3), \\
\Psi_{2m+1} &= \Psi_{m+2}\Psi_m^3 - \Psi_{m-1}\Psi_{m+1}^3 \qquad (m \geqslant 2), \\
2y\Psi_{2m} &= \Psi_m(\Psi_{m+2}\Psi_{m-1}^2 - \Psi_{m-2}\Psi_{m+1}^2) \qquad (m \geqslant 3).
\end{aligned}$$

†. On dit alors que l'isogénie est normalisée ; elle est en particulier séparable.

Cette proposition donne un algorithme évident pour le calcul des polynômes Ψ_m : sa complexité est en $\tilde{O}(m \times m^2 \log q)$. Grâce à la proposition 2.16 dans le cas où m est impair, on sait que Ψ_m possède toutes ses racines simples, qui sont exactement les abscisses des points de m–torsion distincts de $\mathcal{O}$. La même proposition donne aussi l'existence de polynômes $\phi_m \in K[x]$ et $\omega_m \in K[x] \oplus yK[x]$ tels que

$$[m]P = \left(\frac{\phi_m(P)}{\Psi_m(P)^2}, \frac{\omega_m(P)}{\Psi_m(P)^3} \right).$$

Ainsi, il suffit de calculer une expression du morphisme $[m]$ pour calculer les polynômes Ψ_m. Cela peut bien sûr se faire naïvement en appliquant m fois la loi d'addition. On peut aussi utiliser l'exponentiation rapide (2.8) : cela demande donc l'application de $\log m$ fois la loi d'addition. Les polynômes en jeu n'excèdent pas le degré m^2 et leurs coefficients sont dans $\mathbb{F}_q$: on calcule ainsi $D(x)$ en $\tilde{O}(m^2(\log q)^2)$. Il ne reste plus qu'à prendre la racine carrée de $D(x)$ (ou bien celle $\frac{D(x)}{x^3+ax+b}$) pour trouver $\Psi_m(x)$ cela se fait aussi en $\tilde{O}(m^2(\log q)^2)$, par exemple avec une itération de Newton. On peut résumer ceci en :

Proposition 2.21. *Il existe un algorithme polynomial s'exécutant en temps $\tilde{O}((m \log q)^2)$ qui calcule le m^e polynôme de division Ψ_m sur le corps fini $\mathbb{F}_q$.*

2.2.3 Le j–invariant d'une courbe elliptique.

Point de vue algébrique. Il existe une quantité importante qui permet de caractériser les courbes elliptiques isomorphes : le j–invariant. Celui-ci joue un rôle important dans plusieurs algorithmes de comptage de points.

Définition 2.22 (j–invariant)**.** *Soit E une courbe elliptique (lisse) définie sur un corps K. Pour simplifier les formules, on suppose encore que E est donnée par une équation de Weierstrass simplifiée : $y^2 = x^3 + ax + b$. On définit alors :*

$$j = -1728 \frac{(4a)^3}{\Delta} = \frac{6912a^3}{4a^3 + 27b^2},$$

*nommé j–*invariant *de E.*

Proposition 2.23.

(i) Pour $j_0 \in \overline{K}$, il existe une courbe elliptique définie sur $K(j_0)$ dont le j–invariant est j_0.

(ii) Deux courbes elliptiques (définies sur un corps K) sont isomorphes sur $\overline{K}$ si et seulement si elles ont le même j–invariant. Plus précisément, si $j = 0$ alors, les deux courbes sont isomorphes sur une extension de degré 6 (ou divisant 6) de K ; si $j = 1728$, alors, c'est une extension de degré 4 et sinon de degré 2.

Démonstration. Pour $j_0 = 0$ ou 1728 on a les deux courbes

$$\begin{array}{lll} y^2 + y = x^3 & j = 0 & \Delta = -27 \\ y^2 = x^3 + x & j = 1728 & \Delta = -64 \end{array}$$

Un simple calcul montre que pour $j_0 \neq 0, 1728$, la courbe définie par

$$y^2 + xy = x^3 - \frac{36}{j_0 - 1728} x - \frac{1}{j_0 - 1728}$$

a pour j–invariant j_0. En caractéristique différente de 2 ou 3, on peut choisir

$$y^2 = x^3 - \frac{3j_0}{j_0 - 1728} x - \frac{2j_0}{j_0 - 1728}.$$

Deux courbes définies par des équations de Weierstrass simplifiées [†] ($y^2 = x^3 + ax + b$ et $y'^2 = x'^3 + a'x' + b'$) sont isomorphes sur $\overline{K}$ si et seulement s'il existe $u \in \overline{K}$ et $x' = u^2 x$ et $y' = u^3 y$. Le sens direct en découle directement. Pour le sens indirect, si $j = j'$ alors $a^3 b'^2 = a'^3 b^2$. En prenant $u = \left(\frac{a}{a'}\right)^{\frac{1}{4}}$ ou $\left(\frac{b}{b'}\right)^{\frac{1}{6}}$ suivant les cas, on arrive au résultat souhaité. □

†. Encore une fois le résultat subsiste en caractéristique 2 ou 3 mais les formules sont plus compliquées.

Ainsi, on peut très bien avoir deux courbes elliptiques définies sur K, isomorphes sur $\overline{K}$ mais pas sur K. Dans ce cas, on dit qu'elles sont *tordues* l'une par rapport à l'autre. Lorsqu'elles sont isomorphes sur une extension de degré 2 mais pas sur K, on parle de *tordue quadratique.*

Proposition 2.24 (Tordue quadratique sur un corps fini)**.**

(i) Pour chaque $j \in \mathbb{F}_q \backslash \{0, 1728\}$, il existe à isomorphisme défini sur $\mathbb{F}_q$ près, exactement deux courbes elliptiques possédant ce j–invariant.

(ii) Si E est une courbe elliptique définie sur $\mathbb{F}_q$ par une équation de Weierstrass $y^2 = x^3+ax+b$ et si $\omega \in \mathbb{F}_q$ n'est pas un carré, alors, la courbe E' définie par $y^2 = x^3 + a\omega^2 x + b\omega^3$ est la tordue quadratique de E.

(iii) On a l'égalité : $|E(\mathbb{F}_q)| + |E'(\mathbb{F}_q)| = 2(q + 1)$.

Démonstration. Soient E et E' d'équation respective $y^2 = x^3 + ax + b$ et $y'^2 = x'^3 + a'x' + b'$ ayant le même j–invariant différent de 0 et 1728 (ainsi $aa'bb' \neq 0$). Alors, il existe $u \in \overline{\mathbb{F}}_q^*$ tel que $x = u^2x'$ et $y = u^3y'$ et ainsi $u^4 = \frac{a}{a'}$ et $u^6 = \frac{b}{b'}$. On pose $\omega = u^2 \in \mathbb{F}_q$ et l'équation de E' devient $y^2 = x^3 + a\omega^2 x + b\omega^3$. E' n'est pas isomorphe à E sur $\mathbb{F}_q$ si et seulement si $u \notin \mathbb{F}_q$ ou encore si et seulement si ω n'est pas un carré.

Finalement, si on pose $\omega x'' = x'$ et $y'' = \omega y'$, l'équation de E' devient $y''^2 = \omega(x''^3 + ax'' + b)$. Ainsi, lorsque ω n'est pas un carré, on a $\omega(x^3 + ax + b)$ carré dans $\mathbb{F}_q$ si et seulement si $x^3 + ax + b$ n'en est pas un, ce qui montre la troisième affirmation. □

Ainsi, calculer le nombre de points d'une courbe équivaut à calculer celui de sa tordue quadratique. Néanmoins, il faut pour cela trouver une équation de E' : comme on l'a vu, il suffit de trouver $\omega \in \mathbb{F}_q$ qui n'est pas un carré. Le plus simple est encore de tirer un élément au hasard et de tester si c'est un carré (en l'élevant à la puissance $\frac{q-1}{2}$), fournissant ainsi un algorithme polynomial mais probabiliste.

Point de vue analytique. On a une relation importante entre j–invariant et courbes modulaires. Pour cela, revenons un instant aux courbes elliptiques définies sur $\mathbb{C}$. Via la fonction $\wp$ de Weierstrass, une courbe elliptique sur $\mathbb{C}$ n'est autre que le quotient de $\mathbb{C}$ par un réseau de $\mathbb{C}$. De plus, deux courbes sont isomorphes si et seulement si il existe un complexe α non nul qui envoie par multiplication un réseau sur l'autre. On voit alors facilement que l'on peut se ramener avec un réseau de la forme $\mathbb{Z} + \tau\mathbb{Z}$ avec τ (unique) dans le domaine fondamental du demi-plan $\mathscr{H}$ de Poincaré sous l'action du groupe modulaire. Ainsi, le j–invariant d'une courbe elliptique sur $\mathbb{C}$ est une fonction de τ invariante sous l'action de $\mathrm{SL}_2(\mathbb{Z})$: c'est une fonction modulaire de poids 0. (On pourra voir [Ser70] pour les définitions et propriétés des fonctions modulaires). En reprenant la définition de j et l'expression des coefficients dans l'équation différentielle sur la fonction $\wp$ de Weierstrass, on trouve le développement de j en série pour $q = \exp(2i\pi\tau)$, $|q| < 1$

$$j(q) = \frac{1}{q} + 744 + \sum c(n)q^n, \quad \text{où } c(n) \in \mathbb{Z}.$$

On peut de plus montrer le résultat suivant, important pour différents algorithmes présentés dans la suite ; la première partie est due à Petersson, mentionnée dans [Sil95]. On peut trouver la seconde dans [BP05].

Théorème 2.25. *Les coefficients $c(n)$ sont équivalents à l'infini à $\frac{e^{4\pi\sqrt{n}}}{\sqrt{2}n^{3/4}}$. On a de plus la majoration optimale :*

$$c(n) \leqslant \frac{e^{4\pi\sqrt{n}}}{\sqrt{2}n^{3/4}}, \quad \forall n \geqslant 1.$$

Venons-en maintenant aux courbes modulaires. On pourra trouver quelques détails supplémentaires dans [Mil90].

Définition 2.26 (Groupe modulaire — Courbe modulaire)**.**

(i) On appelle groupe modulaire *le groupe $\Gamma(1) = \mathrm{SL}_2(\mathbb{Z})/\{\pm 1\}$ image de $\mathrm{SL}_2(\mathbb{Z})$ dans $\mathrm{PSL}_2(\mathbb{R})$.*

(ii) On appelle n^e sous-groupe de congruence *le sous-groupe de $\Gamma(1)$ défini par :*

$$\Gamma_0(n) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad c \equiv 0 \mod n \right\}.$$

(iii) On appelle courbe modulaire *(compacte) le quotient du compactifié $\mathscr{H}^* = \mathscr{H} \cup \mathrm{P}^1(\mathbb{Q})$ de $\mathscr{H}$ par un sous-groupe de congruence :*

$$X_0(n) = \mathscr{H}^*/\Gamma_0(n).$$

Remarquons que $\Gamma_0(1) = \Gamma(1)$, ce qui justifie la notation $\Gamma(1)$. On utilisera indifféremment les deux notations.

Proposition 2.27. *Le sous-groupe $\Gamma_0(n)$ est d'indice fini dans $\Gamma(1)$: plus précisément, si on note $\overline{\Gamma}_0(n)$ et $\overline{\Gamma}(1)$ les images de ces groupes par la réduction modulo n, on a :*

$$[\Gamma(1) : \Gamma_0(n)] = [\overline{\Gamma}(1) : \overline{\Gamma}_0(n)] = n \prod_{p|n} \left(1 + \frac{1}{p}\right).$$

Démonstration. On montre tout d'abord que la réduction modulo n induit une surjection $\mathrm{SL}_2(\mathbb{Z}) \twoheadrightarrow \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$. Ensuite, on vérifie que les applications $A\Gamma_0(n) \mapsto \overline{A}\ \overline{\Gamma}_0(n)$ d'une part, et $\overline{A}\ \overline{\Gamma}_0(n) \mapsto A\Gamma_0(n)$ d'autre part, sont bien définies, inverses l'une de l'autre. Enfin, l'image de $\Gamma_0(n)$ sous la réduction modulo n donne le groupe $\left\{ \left(\begin{smallmatrix} a & b \\ 0 & a^{-1} \end{smallmatrix} \right), a \in (\mathbb{Z}/n\mathbb{Z})^* \right\}$ dont le cardinal est $\varphi(n)n$. Il ne reste plus qu'à trouver celui de $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ que l'on calcule en étudiant $\mathrm{SL}_2(\mathbb{Z}/p^r\mathbb{Z})$ et on trouve $\varphi(n)n^2 \prod_{p|n} \left(1 + \frac{1}{p}\right)$. □

Voyons maintenant le lien avec les courbes elliptiques :

Théorème 2.28 (Equation modulaire)**.** *Le corps $\mathbb{C}(X_0(n))$ des fonctions modulaires pour $\Gamma_0(n)$ est généré sur $\mathbb{C}$ par $j(z)$ et $j_n(z) \overset{def}{=} j(nz)$. Le polynôme minimal $F(j, Y) \in \mathbb{C}(j)[Y]$ de j_n sur $\mathbb{C}(j)$ à pour degré $\mu \overset{def}{=} n \prod_{p|n} \left(1 + \frac{1}{p}\right)$. De plus, $F(j, Y)$ est un polynôme en j à coefficients dans $\mathbb{Z}$ que l'on note $\Phi_n(X, Y)$. Enfin, pour $n > 1$, $\Phi_n(X, Y)$ est symétrique.*

Remarque 2.29. Comme Φ_n est à coefficients entiers, on peut en fait définir $X_0(n)$ sur n'importe quel corps, comme étant la variété de $\mathrm{P}^1 \times \mathrm{P}^1$ définie par l'équation $\Phi_n(X, Y) = 0$.

Démonstration. On a déjà mentionné que j était une fonction modulaire pour $\Gamma_0(1)$ (et à fortiori pour $\Gamma_0(n)$). Rappelons aussi que toute fonction modulaire pour $\Gamma(1)$ est une fraction rationnelle en j : $\mathbb{C}(X_0(1)) = \mathbb{C}(j)$. Montrons que $j_n \in \mathbb{C}(X_0(n))$. Soit $\gamma = \left(\begin{smallmatrix} a & b \\ nc & d \end{smallmatrix} \right) \in \Gamma_0(n)$. alors,

$$j_n(\gamma z) = j\left(\frac{a(nz) + nb}{c(nz) + d}\right) = j(\tilde{\gamma} nz) = j_n(z).$$

car $\tilde{\gamma} = \left(\begin{smallmatrix} a & nb \\ c & d \end{smallmatrix} \right) \in \Gamma(1)$ et j est invariante sous l'action de $\tilde{\gamma}$.

Montrons que l'extension $\mathbb{C}(j) \subset \mathbb{C}(j, j_n)$ est de degré au plus μ : soit $\{\gamma_1, \ldots, \gamma_\mu\}$ un système de représentants pour $\Gamma(1)/\Gamma_0(n)$ et $f \in \mathbb{C}(X_0(n))$. Les fonctions $f \circ \gamma_i$ ne dépendent que de la classe de γ_i et leur ensemble est donc invariant sous l'action de $\Gamma(1)$: le polynôme $\prod(Y - f \circ \gamma_i)$ est symétrique en les $f \circ \gamma_i$ et est donc invariant sous $\Gamma(1)$: c'est donc un polynôme à coefficients dans $\mathbb{C}(j)$ et il est de degré μ.

Montrons enfin que les $f \circ \gamma_i$ sont conjugués entre eux et que pour $f = j_n$ ils sont deux à deux distincts, ce qui démontrera la première partie. Soit $F(j, Y)$ le polynôme minimal de f sur $C(j)$. Alors, F est irréductible et comme j est invariant sous l'action de $\Gamma(1)$, on a $F(j(z), f \circ \gamma_i(z)) = F\left(j(\gamma_i z), f(\gamma_i z)\right) = 0$ et les $f \circ \gamma_i$ sont conjugués. Supposons que $j_n(\gamma_i z) = j_n(\gamma_{i'} z)$ pour tout z. Mais comme j est bijectif de $\mathscr{H}^*/\Gamma_1 \mapsto \mathbb{S}^2$, on en déduit qu'il existe $\gamma \in \Gamma(1)$ tel que $n\gamma_i z = \gamma n \gamma_{i'} z$ ce qui se réécrit matriciellement en :

$$\begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix} \gamma_i = \pm\gamma \begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix} \gamma_{i'}.$$

Mais alors, un rapide calcul montre que le coefficient $(2,1)$ de $\gamma_i\gamma_{i'}^{-1}$ est divisible par n et donc γ_i et $\gamma_{i'}$ sont dans la même classe modulo $\Gamma_0(n)$.

Ainsi, le polynôme minimal de j_n est $\prod(Y - j_n \circ \gamma_i) \in \mathbb{C}(j)[Y]$ et comme ces coefficients sont holomorphes sur $\mathscr{H}$, ce sont des polynômes en j et $F \in \mathbb{C}[j,Y]$. Regardons le développement en série de $j_n \circ \gamma_i(z)$: on le réécrit en $j(\tilde{\gamma}_i z)$ où $\tilde{\gamma}_i \in \mathrm{M}_2(\mathbb{Z})$ de déterminant n. Par opérations élémentaires sur les lignes, on arrive facilement à trouver $U \in \mathrm{SL}_2(\mathbb{Z})$ telle que $U\tilde{\gamma}_i = \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)$. On a en particulier :

$$ad = n \text{ et } j_n \circ \gamma_i(z) = j\left(\frac{az+b}{d}\right). \qquad (\clubsuit)$$

En remplaçant dans le développement de j, on obtient une série en $\exp(\frac{2i\pi b}{d})\exp(\frac{2i\pi az}{d})$, ce qui donne une série en $q^{\frac{1}{n}}$ avec des coefficients dans $\mathbb{Z}[\exp(\frac{2i\pi}{n})]$, entiers algébriques. Ainsi, les fonctions symétriques en $f \circ \gamma_i$ sont des polynômes en j dont les coefficients sont des entiers algébriques (Sinon, on écrit $P(j) = \sum a_n j^n$ et si on note m le plus grand entier tel que a_m n'est pas un entier algébrique, le terme en q^{-m} dans le développement en série de $P(j)$ serait $a_m + \xi$ avec ξ entier algébrique, ce qui obligerait a_m à l'être aussi).

Maintenant, on écrit $\Phi_n(X,Y) = \sum c_{k,l} X^k Y^l$ et le développement en série de l'équation $\Phi_n(j, j_n) = 0$ donne un système d'équations en $c_{k,l}$ qui possède une unique solution sur $\mathbb{C}$ si l'on ajoute la condition $c_{0,\mu} = 1$. Comme le système est à coefficients dans $\mathbb{Q}$ la solution aussi et comme ce sont des entiers algébriques, ce sont en fait des entiers.

Enfin, en regardant $z' = \frac{-1}{nz}$, on obtient $0 = \Phi_n(j(z), j_n(z)) = \Phi_n(j(nz'), j(z'))$, soit encore $\Phi_n(j_n, j) = 0$. Ainsi, $\Phi_n(Y,X)$ est un multiple de $\Phi_n(X,Y)$. Comme ils sont irréductibles, on a facilement $\Phi_n(Y,X) = c\Phi_n(X,Y)$ pour une constante c et en échangeant à nouveau $c^2 = 1$. Si $c = -1$, $X - Y$ serait un facteur de $\Phi_n(X,Y)$ ce qui est impossible. □

Remarque 2.30.

(i) Cette démonstration a l'avantage d'être effective pour calculer les polynômes modulaires $\Phi_n(X,Y)$ en utilisant le développement en série de j et j_n puis en résolvant un système linéaire. Par ailleurs, lorsque $n = l$ est premier, la formule $(\clubsuit)$ nous indique que

$$\Phi_n(j(z), Y) = (Y - j(pz)) \prod_{m=0}^{p-1} \left(Y - j(\frac{z+m}{p})\right).$$

En utilisant le fait que F est symétrique et à coefficients entiers, on peut approximer cette relation pour obtenir une expression, de $\Phi_n(X,Y)$.

(ii) Les racines de $\Phi_n(j(\tau), X)$ sont précisément les j–invariants des courbes que l'on peut définir par un quotient $\mathbb{C}/\Lambda$ avec Λ un sous-réseau de $\mathbb{Z} + \tau\mathbb{Z}$ tel que $(\mathbb{Z} + \tau\mathbb{Z})/\Lambda \simeq \mathbb{Z}/n\mathbb{Z}$. Cela découle directement de la démonstration ci-dessus et du lemme suivant :

Lemme 2.31. *Soit $\tau \in \mathcal{H}$ et Λ un sous-réseau de $\mathbb{Z} + \tau\mathbb{Z}$. Alors, $(\mathbb{Z} + \tau\mathbb{Z})/\Lambda \simeq \mathbb{Z}/n\mathbb{Z}$ si et seulement si il existe $\gamma = \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)$ telle que $ad = n$ et $\Lambda = d(\mathbb{Z} + \gamma\tau\mathbb{Z})$.*

2.3 Algorithmes l–adiques.

2.3.1 Méthodes élémentaires.

Avant de présenter l'algorithme élaboré de Schoof, présentons deux méthodes plus simples mais moins efficaces pour calculer le nombre de points rationnels d'une courbe elliptique définie sur le corps fini $\mathbb{F}_q$ à q éléments. Ces algorithmes sont exponentiels en la taille des données, c'est-à-dire exponentiel en $\log q$

En caractéristique différente de 2 ou 3, la forme particulière de l'équation de Weierstrass $y^2 = x^3 + ax + b$ nous donne une première proposition. En fait, cette proposition est plus générale puisqu'elle fonctionne pour toute courbe définie par une équation du type $y^2 = f(x)$, ce qui est en fait le cas pour les courbes elliptiques en caractéristique 3.

Proposition 2.32. *Le nombre de points rationnels de (E) dans $\mathbb{F}_q$ est donné par la formule :*

$$|E(\mathbb{F}_q)| = q + 1 + \sum_{x \in \mathbb{F}_q} \left(\frac{x^3 + ax + b}{q} \right)$$

où $\left(\frac{\cdot}{q}\right)$ est le symbole de Legendre i.e. l'élévation à la puissance $\frac{q-1}{2}$.

Démonstration. En effet, pour x fixé, on a $1 + \left(\frac{x^3+ax+b}{q}\right)$ solutions en y. A toutes celles-ci, il faut ajouter le point à l'infini. □

Le calcul d'un symbole de Legendre se fait en temps polynomial : l'exponentiation rapide permet de n'effectuer que $O(\log(q))$ multiplications dans $\mathbb{F}_q$. Ainsi, cette proposition donne un algorithme de calcul simple mais dont l'exécution est en $\tilde{O}(q)$.

En caractéristique 2, cette méthode ne peut fonctionner sans modifications (par exemple, les courbes données par une équation $y^2 = f(x)$ sont toutes singulières). On doit écrire une équation de la forme $y^2 + h(x)y = f(x)$ avec $\deg f = 3 \geqslant \deg h$.

Proposition 2.33. *Soit $q = 2^n$. Le nombre de points rationnels de la courbe elliptique définie par l'équation $y^2 + h(x)y = f(x)$ est donné par la formule*

$$|E(\mathbb{F}_{2^n})| = 1 + |V_h(\mathbb{F}_{2^n})| + 2 \sum_{\alpha \in \mathbb{F}_{2^n}/\mathbb{F}_2} \left(1 - \mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2} \left(\frac{f(\alpha)}{h(\alpha)^2} \right) \right),$$

où V_h est la variété affine définie par $h(x) = 0$.

Démonstration. On a le point à l'infini et si $h(x) = 0$ on a une seule solution, ce qui justifie les deux premiers termes. Si $h(x) \neq 0$, on peut faire le changement de variable $zh(x) = y$ et obtenir l'équation $z^2 + z = f(x)/h(x)^2$: celle-ci possède soit deux solutions distinctes si $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2} = 0$ soit aucune si cette trace est égale à 1. En effet, si $z \in \overline{\mathbb{F}}_q$ est une racine, alors, on calcule par somme télescopique (on est en caractéristique 2) :

$$z^q - z = z^{2^n} + z = \sum_{i=0}^{n-1} (z^{2^{i+1}} + z^{2^i}) = \sum_{i=0}^{n-1} \left(\frac{f(\alpha)}{h(\alpha)^2} \right)^{2^i} = \mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2} \left(\frac{f(\alpha)}{h(\alpha)^2} \right).$$

Ainsi, cette trace est nulle si et seulement si $z \in \mathbb{F}_q$. □

On en déduit un algorithme similaire au précédent, de même complexité. Un premier théorème fondamental permet de nettement améliorer le temps d'exécution de ces méthodes, en utilisant des techniques assez élémentaires.

Théorème 2.34 (Hasse)**.** *On a l'encadrement :*

$$\big| |E(\mathbb{F}_q)| - (q+1) \big| \leqslant 2\sqrt{q}.$$

L'idée est alors de trouver un élément $P \in E(\mathbb{F}_q)$ et un entier $m \in [q+1-2\sqrt{q}, q+1+2\sqrt{q}]$ tel que $mP = 0$. Si m est l'unique entier vérifiant cette relation alors, le théorème de Hasse permet de conclure. Explicitons brièvement les techniques mises en place dans cette approche.

Pour trouver m, on peut utiliser le procédé *pas de bébés, pas de géants* : le théorème de Hasse permet de choisir des pas de géants de l'ordre de $2q^{\frac{1}{4}}$. En effet, si on note $k = [q^{\frac{1}{4}}] + 1$ et que l'on calcule d'une part les points $Q_i = (q + 1 + ik)P$, et d'autre part les points $R_j = jP$ pour $i, j \in [\![-t, t]\!]$, le théorème de Hasse assure l'existence de i, j tels que $Q_i = R_j$ puis d'un entier $m = q + i - j$ vérifiant ce que l'on voulait.

Toutefois, ceci ne permet pas de conclure quant au cardinal de $E(\mathbb{F}_q)$: en effet il se peut tout à fait que l'on choisisse un P qui ait un ordre inférieur à $4\sqrt{q}$ et on ne pourrait pas trouver un unique m. Néanmoins, on sait que cet ordre divise le cardinal cherché et une stratégie consiste à essayer avec un autre P. Cette technique peut échouer si l'exposant du groupe est inférieur à $4\sqrt{q}$. Pour y remédier, on a le théorème suivant :

Théorème 2.35 (Mestre)**.** *Soit $q \geqslant 1373$. Alors, soit E, soit sa tordue quadratique E', possède un point $\mathbb{F}_q$ rationnel d'ordre supérieur à $4\sqrt{q}$.*

Comme la proposition 2.22 relie le cardinal de E et de sa tordue quadratique E', ce théorème permet de conclure quant à un algorithme probabiliste en $\tilde{O}(q^{\frac{1}{4}})$. Néanmoins, cette solution ne peut être satisfaisante pour des cardinaux très élevés. En effet, elle utilise l'algorithme général *pas de bébés, pas de géants* dont la complexité est la "meilleure" pour résoudre le problème du logarithme discret général (*i.e.* dans un groupe dont on ne sait rien à part la loi de groupe donnée par une "boîte noire"). C'est d'ailleurs sur ce constat de difficulté à résoudre ce problème qu'est basée la sécurité des cryptosystèmes à base de courbes elliptiques comme on l'a déjà évoqué dans la section 2.1.2.

2.3.2 Méthodes l–adiques.

Une des idées fondamentales dans les algorithmes de comptage de points réside sur le fait qu'il est plus facile de calculer ce cardinal modulo l pour différents nombres premiers l. Ensuite, le théorème des restes chinois combiné avec le théorème de Hasse permet de retrouver le cardinal du groupe des points rationnels.

En effet, si on connaît $|E(\mathbb{F}_q)| \mod p_i$ pour des nombres premiers p_i vérifiant $\prod p_i > 4\sqrt{q}$, alors, le théorème des restes chinois nous permet de retrouver (en temps polynomial) $|E(\mathbb{F}_q)|$ comme étant le seul entier de l'intervalle $[q+1-2\sqrt{q}, q+1+2\sqrt{q}]$ ayant le résidu modulo $\prod p_i$ calculé.

Rappelons brièvement que le théorème des nombres premiers donne : $\prod_{p \leqslant x} p \geqslant e^{x(1+o(1))}$. De plus, on sait aussi que si p_n est le n^{e} nombre premier, on a $p_n \sim n \log n$. Ainsi, en prenant n de l'ordre de $\frac{\log q}{\log\log q}$, le produit des n premiers nombres premiers va dépasser $4\sqrt{q}$. Un algorithme de crible simple permettra de lister ces n nombres premiers en temps $O(p_n) = O(\log q)$.

Ainsi, pour avoir un algorithme polynomial calculant $|E(\mathbb{F}_q)|$, il suffit de savoir calculer pour l premier, $|E(\mathbb{F}_q)| \mod l$ en temps polynomial en $\log q$ et en l. C'est ce que l'on présente dans la prochaine section. Notons que dans la plupart des cas, on évitera le cas $l = p = \operatorname{car} \mathbb{F}_q$ pour des raisons de séparabilité ; de toute façon, le plus "grand" l sera généralement inférieur à p, car de l'ordre de $\log p \ldots$

2.3.3 L'algorithme de Schoof.

L'algorithme repose principalement sur l'utilisation du morphisme de Frobenius :

Définition 2.36. *Soit E une courbe elliptique définie sur $\mathbb{F}_q$. On appelle* morphisme de Frobenius *le morphisme algébrique*

$$\begin{aligned} \pi_E : E(\overline{\mathbb{F}_q}) &\longrightarrow E(\overline{\mathbb{F}_q}) \\ (x,y) &\longmapsto (x^q, y^q). \end{aligned}$$

Il est clair que π_E est un morphisme algébrique défini sur $\mathbb{F}_q$. C'est en fait une isogénie puisqu'elle envoie le point à l'infini sur lui-même †. Elle est de degré q, non séparable (en fait purement inséparable). On a alors la proposition, dont l'utilisation est fondamentale dans l'algorithme de Schoof :

Proposition 2.37 (Propriétés du Frobenius)**.**

(i) Le cardinal de $E(\mathbb{F}_q)$ est donné par la trace de π : $|E(\mathbb{F}_q)| = q + 1 - \operatorname{tr} \pi_E$.

(ii) L'endomorphisme π_E vérifie, dans $\operatorname{End} E$*, l'équation*

$$\pi_E^2 - (\operatorname{tr} \pi_E)\pi_E + q = 0.$$

Démonstration. Parmi l'ensemble des points de E (sur une clôture algébrique de $\mathbb{F}_q$), ceux qui sont effectivement des points $\mathbb{F}_q$–rationnels sont précisément les points fixes du Frobenius

†. On devrait écrire l'expression du Frobenius en coordonnées projectives, $[X,Y,Z] \mapsto [X^q, Y^q, Z^q]$, ce qui montre clairement que l'image de $\mathcal{O} = [0,1,0]$ est bien lui-même.

ou encore les points du noyau de l'isogénie $\pi_E - \mathrm{Id}$. Ainsi, avec la proposition 2.14 et les définitions 2.15,

$$\begin{aligned}|E(\mathbb{F}_q)| = \deg(\pi_E - \mathrm{Id}) = \mathrm{N}(\pi_E - \mathrm{Id}) &= (\pi_E - \mathrm{Id}) \circ \widehat{(\pi_E - \mathrm{Id})} \\ &= (\pi_E - \mathrm{Id}) \circ (\hat{\pi}_E - \mathrm{Id}) \\ &= q + 1 - (\pi_E + \hat{\pi}_E) = q + 1 - \operatorname{tr} \pi_E.\end{aligned}$$

D'autre part, en composant par π_E l'égalité $\operatorname{tr} \pi_E = \pi_E + \hat{\pi}_E$, on obtient bien la relation souhaitée : $(\operatorname{tr} \pi_E)\pi_E = \pi_E^2 + q$. □

Ainsi, suivant le principe que l'on a décrit dans le paragraphe précédent, on va chercher à déterminer $\operatorname{tr} \pi_E \mod l$ pour différents l. Pour cela, on réduit l'équation "modulo" l. On note q' l'entier $0 < q' < l$ congru à q modulo l et on a la proposition :

Proposition 2.38. *La relation*

$$\pi_E^2 - t'\pi_E + q' \qquad t' = 0, 1, 2, \ldots, l-1 \tag{$\star$}$$

est vérifiée sur le sous-groupe $E[l]$ des points de l–torsions si et seulement si $t' \equiv \operatorname{tr} \pi_E \mod l$.

Démonstration. En effet les points de $E[l]$ sont annulés par les multiples (dans $\operatorname{End} E$) de $[l]$. D'autre part, comme $l \neq p$, $E[l] \simeq (\mathbb{Z}/l\mathbb{Z})^2$. Soit alors $P \in E[l]\backslash\{\mathcal{O}\}$: il est d'ordre l. Supposons qu'il vérifie $\pi_E^2(P) - t'\pi_E(P) + [q'](P)$; comme il vérifie l'équation de la proposition 2.37 et le fait qu'il soit de l–torsion donne $[t' - t''](E) = 0$ où on a noté $t'' \in [\![0, l-1]\!]$ l'entier vérifiant $t'' = \operatorname{tr} \pi_E$. Comme P est d'ordre l et que $-l < t' - t'' < l$, on a $t' = t''$ □

Notons que l'on a démontré en fait quelque chose de plus fort puisqu'il suffit de vérifier la relation sur une partie de $E[l]$ non réduite à $\{\mathcal{O}\}$. Le problème est de trouver un point de $E[l]\backslash\{\mathcal{O}\}$ (et donc le sous-groupe d'ordre l qu'il engendre) : on pourrait penser à chercher une racine du polynôme de division Ψ_l ce qui conduirait à un algorithme probabiliste. On décrira une autre solution en détail dans la section 2.3.4.

L'idée de Schoof est en fait de vérifier les relations $(\star)$ dans l'anneau $\mathbb{F}_q[X,Y]/(\Psi_l(X), Y^2 - X^3 - aX - b)$. En effet, avec la proposition 2.38, il suffit de trouver l'entier $0 \leqslant t' < l$ tel que

$$(X^{q^2}, Y^{q^2}) + [q'](X^q, Y^q) \equiv [t'](X^q, Y^q) \mod (\Psi_l(X), Y^2 - X^3 - aX - b),$$

en prenant bien soin que le "+" qui apparaît dans la formule est l'addition sur la courbe elliptique.

C'est d'ailleurs une petite source de complication au moment de véritablement écrire l'algorithme. En effet, il se peut que les polynômes définissant les abscisses de X^{q^2} et $[q'](X^q, Y^q)$ peuvent être égaux modulo $\Psi_l(X)$, ce qui empêche d'utiliser la formule d'addition. Dans ce cas, deux solutions se présentent à nous :

(i) Soit les polynômes définissant les ordonnées sont égaux $\mod (\Psi_l(X), Y^2 - X^3 - aX - b)$. Dès lors, aucun calcul supplémentaire n'est nécessaire puisque l'on a $t \equiv 0 \mod l$.

(ii) Soit les ordonnées sont opposées (et $l \neq 2$). On a alors dans $E[l]$, $[t']\pi_E(P) = [2q'](P)$ et donc en prenant le déterminant, $t^2 q \equiv 4q^2 \mod l$ soit encore $t^2 = 4q \mod l$. Il "suffit" alors de calculer une racine w de $q \mod l$ et de tester les deux possibilités $t = \pm 2w \mod l$.

C'est ce que l'on présente dans l'algorithme ci-dessous, aux lignes 10 à 21. Pour finir avec ce détail, il faut mentionner que le calcul d'une racine carrée dans un corps fini est délicat, comme on le verra dans la section 2.3.5. Néanmoins, ici, cela ne pose aucun problème puisqu'un algorithme trivial en $\tilde{O}(l)$ convient puisque l est au plus de l'ordre de $\log q$.

Pour alléger les notations, on notera $\mathcal{I}_l$ l'idéal de $\mathbb{F}_q[X,Y]$ engendré par les polynômes Ψ_l et $Y^2 - X^3 - aX - b$. Nous avons maintenant tous les outils pour écrire le "pseudo–code" de l'algorithme de Schoof, sachant qu'avec tout ce que l'on a dit, la correction et la terminaison ne posent aucun problème. Il ne nous restera qu'à étudier sa complexité.

Algorithme 1 : SCHOOF (1985)

Entrée : $(a,b) \in \mathbb{F}_q^2$, $4a^3 - 27b^2 \neq 0$.
Sortie : $|E(\mathbb{F}_q)|$ avec où E est définie par $y^2 = x^3 + ax + b$.

1 $l \leftarrow 2$; $P \leftarrow 2$; TestHasse$\leftarrow$**Vrai**. /*P est le produit des l.*/
2 $R \leftarrow E(\mathbb{F}_q) \mod 2$; /*A l'aide du pgcd$(X^q - X, X^3 + aX + b)$.*/
3 **Tant que** TestHasse **Faire** /*On calcule dans la boucle $|E(\mathbb{F}_q)| \mod l$.*/
4 $l \leftarrow$NEXTPRIME(l). /*Avec un algorithme de crible par exemple.*/
5 $q' \leftarrow q \mod l$, $0 < q' < l$.
6 **Calculer** $\frac{1}{l}\Psi_l \in \mathbb{F}_q[X]$. /*Choisi unitaire pour les divisions euclidiennes.*/
7 $(Fr_x, Fr_y) \leftarrow (X^q, Y^q) \mod \mathcal{I}_l$ par exponentiation rapide *dans l'anneau* $\mathbb{F}_q[X,Y]/\mathcal{I}_l$.
8 $(Fr_x^{(2)}, Fr_y^{(2)}) \leftarrow ((Fr_x)^q, (Fr_y)^q)$.
9 $(Q_x, Q_y) \leftarrow [q'](X,Y) \mod \mathcal{I}_l$, par exponentiation rapide *de la loi de groupe* sur E.
10 **Si** $Q_x = Fr_x^{(2)} \pmod{\Psi_l(X)}$ **Alors**
11 **Si** $Q_y = Fr_y^{(2)} \pmod{\mathcal{I}_l}$ **Alors**
12 $t \leftarrow 0$.
13 **Sinon**
14 **Calculer** w tel que $q \equiv w^2 \mod l$.
15 $(A,B) \leftarrow [w](X^q, Y^q) \mod \mathcal{I}_l$.
16 **Si** $Q_y = B \pmod{\mathcal{I}_l}$ **Alors**
17 $t \leftarrow 2w \mod l$.
18 **Sinon**
19 $t \leftarrow -2w \mod l$.
20 **Fin Si**
21 **Fin Si**
22 **Sinon**
23 $(K_x, K_y) \leftarrow (Fr_x^{(2)}, Fr_y^{(2)}) + (Q_x, Q_y)$ avec le "+" de la loi de groupe sur E.
24 $A \leftarrow Fr_x$; $B \leftarrow Fr_y$.
25 **Pour** $k = 1$ *à* $\frac{l-1}{2}$ **Faire**
26 **Si** $K_x = A \pmod{\Psi_l(X)}$ **Alors** /*On teste les abscisses.*/
27 **Si** $K_y = B \pmod{\mathcal{I}_l}$ **Alors** /*$\pi_E^2 + [q] = [k]\pi_E$.*/
28 $t \leftarrow k$.
29 **Sinon** /*$\pi_E^2 + [q] = [-k]\pi_E$.*/
30 $t \leftarrow -k$.
31 **Fin Si**
32 **Interrompre Pour**.
33 **Sinon** /*On calcule l'expression de $[k+1](X^q, Y^q)$.*/
34 $(A,B) \leftarrow (Fr_x, Fr_y) + (A(X), B(X,Y)) \mod \mathcal{I}_l$ avec la loi de groupe sur E.
35 **Fin Si**
36 **Fin Pour**
37 **Fin Si**
38 $R \leftarrow uPt + vlR$ où $uP + vl = 1$; $P \leftarrow P \times l$.
39 $N \leftarrow \min\{n, n \geqslant q + 1 - 2\sqrt{q}, n \equiv R \mod P\}$.
40 **Si** $N + P > q + 1 + 2\sqrt{q}$ **Alors**
41 TestHasse$\leftarrow$**Faux**.
42 **Fin Si**
43 **Fin Tant que**
44 **Retourner** N.

Notons tout d'abord que l'on peut accélérer un peu la boucle **Pour**, lignes 25–36, en précalculant les polynômes de division Ψ_t : on modifie cette boucle **Pour** en calculant seulement les abscisses ce qui permet de déterminer t à un signe près puis de décider entre t et $-t$ en déterminant véritablement (c'est-à-dire avec les ordonnées) l'isogénie $[t]$, par exponentiation rapide.

Si ces modifications accélèrent l'algorithme, c'est seulement dans la constante du O. Passons maintenant à la complexité asymptotique.

Théorème 2.39. *L'algorithme de Schoof s'exécute en un temps* $\tilde{O}((\log q)^5)$ *en utilisant les techniques de multiplication rapide (voir 2.7).*

Démonstration. Tout d'abord, il est facile de voir que la complexité des lignes 10 à 21 est absorbée par le reste de l'algorithme.

Notons provisoirement $M_{l,q}$ le coût d'une multiplication dans l'anneau $\mathcal{A}_{l,q} \stackrel{\text{def}}{=} \mathbb{F}_q[X,Y]/\mathcal{I}_l$ où l'on rappelle que $\mathcal{I}_l = \langle \Psi_l(X), Y^2 - X^3 - aX - b\rangle$. De plus, on impose au résultat de cette multiplication d'être sous une forme réduite, c'est-à-dire d'avoir un degré en Y au plus 1 et un degré en X au plus $\frac{l^2-1}{2} - 1$.

Estimons la complexité du corps de la boucle **Pour**, ligne 25 à 36. Il s'agit d'ajouter "formellement" des polynômes avec la loi de groupe sur E. Si l'on applique la loi de groupe dans $\mathcal{A}_{l,q}$, il faudrait effectuer une division, ce qui reviendrait à un algorithme d'Euclide étendu. On peut en fait s'en passer, en calculant simplement une expression de $[t+1](X^q, Y^q)$ (ligne 34) sous la forme d'un quotient de deux éléments de $\mathcal{A}_{l,q}$: cela se fait en $O(1)$ multiplications (et additions) dans cet anneau et donc une complexité en $O(M_{l,q})$. Les tests aux lignes 26–27 demanderont alors eux aussi un coût en $O(M_{l,q})$ (on teste $a = \frac{b}{c}$ en testant $ac - b = 0$). Ainsi, cette boucle **Pour** requiert un temps d'exécution en $O(lM_{l,q})$.

Les lignes 8–9 comportent 4 calculs de complexité identique qui demandent une exponentiation rapide dans l'anneau $\mathcal{A}_{l,q}$: l'exposant étant q ou q^2, cela demande $O((\log q)M_{l,q})$ opérations élémentaires.

La ligne 2 se calcule aussi par exponentiation rapide. Il s'agit donc de réaliser $\log q$ divisions euclidiennes par le même polynôme *unitaire* $X^3 + aX + b$: comme les polynômes en jeu n'excéderont pas le degré 6, on aura à chaque fois $O(1)$ opérations $(+,-,\times)$ dans $\mathbb{F}_q$ et on calcule donc $X^q \mod X^3 + ax + b$ en $\tilde{O}((\log q)^2)$.

La ligne 9 demande $\log q' = O(\log l)$ formules d'additions dans E qui absorbent celles de la ligne 23. Comme dans le corps de la boucle **Pour**, on peut faire le calcul sous forme fractionnaire dans $\mathcal{A}_{l,q}$ et se ramener ainsi à $O((\log l)M_{l,q}) = o(l\,\mathrm{M}_{l,q})$ opérations élémentaires.

On a déjà vu que la ligne 6 demandait de l'ordre $\tilde{O}(l^2 \log q^2)$ opérations.

La ligne 4 peut s'obtenir par un algorithme de crible que l'on réalise en fait avant la boucle **Tant que** : comme l varie jusqu'à un $O(\log q)$, cette étape ne demande pas plus † que $\tilde{O}(\log q)$ opérations élémentaires.

Les lignes 5 et 38–40 sont de l'arithmétique élémentaire sur des entiers de taille $O(\log q)$: on réalise facilement toutes ces opérations en temps $O((\log q)^2)$.

La proposition suivante montre que l'on peut prendre $M_{l,q} = \tilde{O}(l^2 \log q)$. Avec ceci, toute la complexité est concentrée dans les lignes 7–9 et 25–36 et la boucle **Tant que** s'exécutant $O(\log q)$, on a finalement une complexité de

$$O\left(\sum_{l=3}^{O(\log q)} (l + \log q)M_{l,q}\right) = \tilde{O}\left(\sum_{l=3}^{O(\log q)} (l + \log q)l^2 \log q\right) = \tilde{O}((\log q)^5).$$

□

Proposition 2.40. *On peut multiplier deux éléments de l'algèbre* $\mathcal{A}_{l,q}$ *et retourner le résultat sous forme d'un polynôme de degré au plus* $\frac{l^2-1}{2} - 1$ *en* X *et au plus* 1 *en* Y *en temps* $\tilde{O}(l^2 \log q)$.

Démonstration. Remarquons tout d'abord que réduire modulo $Y^2 - X^3 - aX - b$ consiste simplement à remplacer les puissances de Y^2 par celles de $X^3 + aX + b$: comme on le fait à chaque étape, on reste dans le sous-ensemble $\mathbb{F}_q[X] \oplus Y\mathbb{F}_q[X]$ ainsi, le degré en Y dans les calculs intermédiaires ne peut excéder 2, et ce pour un seul monôme : le tout revient donc à une seule multiplication par $X^3 + aX + b$ ce qui se fait, même avec des algorithmes naïfs, en $O(l^2 \log q)$.

On peut donc se restreindre au problème plus classique de la multiplication dans l'anneau $\mathbb{F}_q[X]/(\Psi_l(X))$. On commence par multiplier deux polynômes de degré $O(l^2)$ et à coefficients dans $\mathbb{F}_q$: cela demande, avec des algorithmes rapides de transformée de Fourier, $\tilde{O}(l^2)$ opérations $(+,-,\times)$ dans $\mathbb{F}_q$ et donc une complexité en $O(l^2 \log q)$. Il reste alors à effectuer une division euclidienne par Ψ_l qui peut s'effectuer en $\tilde{O}(l^2)$ opérations $(+,-,\times)$ dans $\mathbb{F}_q$. □

†. En fait, dans les applications réalisables à l'heure actuelle, l reste dans un ordre de grandeur de 1000 et on peut facilement précalculer les nombres premiers jusque là !

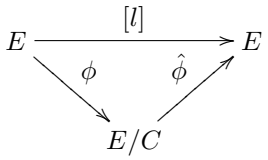
2.3.4 L'algorithme Sea : améliorations Atkin et Elkies.

Maintenant que l'on a montré que le problème de compter les points rationnels d'une courbe elliptique est dans la classe **P**, on va seulement chercher à accélérer l'algorithme. On va supposer que E n'est pas supersingulière et que $j \neq 0, 1728$. Justifions rapidement ces restrictions. En caractéristique p, il n'y a que $O(p)$ courbes supersingulières et dont la proportion est d'autant plus faible que $[\mathbb{F}_q : \mathbb{F}_p]$ est grand ; de plus, si E est définie sur $\mathbb{F}_p$ alors $|E(\mathbb{F}_p)| = p + 1$. Dans le cas où $j = 0, 1728$, on verra dans la section 2.3.5 que l'on a des algorithmes très performants, même s'ils ne sont pas déterministes.

Soit l un nombre premier *différent* de la caractéristique p. On a vu dans l'analyse de la complexité de l'algorithme de Schoof que celle-ci dépend fortement du degré du polynôme Ψ_l. L'idée est alors de trouver un facteur de Ψ_l de degré beaucoup plus petit, en l'occurrence $\frac{l-1}{2}$. Cela revient à factoriser l'isogénie $[l]$ de degré l^2 par une isogénie de degré l. Le noyau d'une telle isogénie serait alors $\mathbb{Z}/l\mathbb{Z}$ qui est cyclique. Soit C un des $l + 1$ sous-groupes cycliques d'ordre l de $E[l] \simeq (\mathbb{Z}/l\mathbb{Z})^2$.

Proposition 2.41. *Il existe une unique courbe elliptique E' et une isogénie séparable $\phi : E \to E'$ telle que $\ker \phi = C$. On note E/C cette courbe elliptique et on dit qu'elle est l–isogène à E.*

On peut résumer l'idée principale de ces améliorations par le diagramme suivant : l'algorithme de Schoof utilise la flèche $[l]$, les améliorations que l'on va présentées se reposent sur ϕ :



La remarque 2.30, la proposition précédente et un théorème de Deuring [Lan87], nous donnent le théorème suivant, en rappelant que l'on a noté Φ_n le n^{e} poynôme modulaire.

Théorème 2.42. *Soit E/K une courbe elliptique définie sur un corps K de caractéristique différente de l. Soit j son invariant : alors, les $l + 1$ zéros de $\Phi_n(X, j)$ dans $\overline{K}$ sont précisément les j–invariants des courbes E' l–isogènes à E.*

Comme dans l'algorithme de Schoof, on cherche à étudier l'endomorphisme de Frobenius. Plus précisément, pour $l \neq p$ premier, on étudie l'action de π_E sur $E[l]$ qui est en fait un $\mathbb{F}_l$ espace vectoriel de dimension 2. Si l'on arrive à trouver une valeur propre λ de π_E vu comme élément de $\mathrm{GL}_2(\mathbb{F}_l)$, on en déduit sa trace avec la formule

$$t \stackrel{\text{def}}{=} \operatorname{tr} \pi_E = \lambda + \frac{q}{\lambda} \in \mathbb{F}_l$$

puisque le polynôme caractéristique de $\pi_E \in \mathrm{GL}_2(\mathbb{F}_l)$ est $X^2 - tX + q$.

Proposition 2.43. *Soit E une courbe ordinaire (c'est-à-dire non supersingulière) sur $\mathbb{F}_q$ dont le j–invariant est différent de 0 et 1728. Alors,*

(i) Le polynôme $\Phi_l(X, j)$ a un zéro $\tilde{\jmath} \in \mathbb{F}_{q^r}$ si et seulement si le noyau de l'isogénie correspondante $E \to E/C$ est un espace propre de dimension 1 de π_E^r de $E[l]$.

(ii) Le polynôme $\Phi_l(X, j)$ est scindé sur $\mathbb{F}_{q^r}$ si et seulement si π_E^r agit comme une matrice scalaire sur $E[l]$.

Démonstration (Esquisse). *(i)* Si C est un espace propre, il est stable par π_E^r qui génère le groupe de Galois (d'une extension de F_{q^r} sur laquelle C est définie). Ainsi, avec les formules de Vélu (2.17), l'isogénie $E \to E/C$ est définie sur $\mathbb{F}_{q^r}$ tout comme la courbe E/C et donc $\tilde{\jmath} \in \mathbb{F}_{q^r}$.

Le sens indirect est plus délicat. Soit $\tilde{\jmath} \in \mathbb{F}_{q^r}$ tel que $\Phi_l(j, \tilde{\jmath}) = 0$ L'idée est de considérer une courbe E' définie sur $\mathbb{F}_{q^r}$ isomorphe sur $\overline{\mathbb{F}}_q$ à E/C. Alors, l'isogénie $\varphi : E \to E'$ a pour noyau C. Si cette isogénie est définie sur $\mathbb{F}_{q^r}$ alors, $\varphi \circ \pi_E^r = \pi_{E'}^r \circ \varphi$, ce qui montre que C est stable par π_E^r.

Le tout est donc de trouver $E'/\mathbb{F}_{q^r}$ $\mathbb{F}_{q^r}$–isogène à E. Notons ψ et ψ' les Frobenius de E et E' vues comme courbes définies sur $\mathbb{F}_{q^r}$ (en particulier, $\psi = \pi_E^r$). Remarquons que si $f, g : E \to E'$ sont deux isogénies telles que $\pi_E \circ f = g \circ \pi'_E$, alors $f = g$ est définie sur $\mathbb{F}_{q^r}$. Ainsi, E' est $\mathbb{F}_{q^r}$–isogène à E si et seulement si π_E et π'_E vérifient les mêmes équations caractéristiques.

Comme E et E' sont isogènes sur $\overline{\mathbb{F}}_q$ et qu'elles ne sont pas supersingulières, il existe † un corps quadratique imaginaire $\mathscr{K}$ tel que $\mathbb{Q} \otimes \mathrm{End}(E) \simeq \mathbb{Q} \otimes \mathrm{End}(E') \simeq \mathscr{K}$. Comme E et E' sont isogènes sur une extension finie de $\mathbb{F}_{q^r}$ (celle dans laquelle φ est définie), il existe un entier s tel que, à conjugaison près, $\psi^s = \psi'^s : \frac{\psi}{\psi'} \in \mathscr{K}$ est une racine de l'unité dans un corps quadratique et donc $s \in \{1, 2, 3, 4\}$. Si $s = 1$ il n'y a rien à montrer. Si $s = 2$ et que $\psi = -\psi'$, il suffit de remplacer E' par sa tordue quadratique, le Frobenius étant alors changé en son opposé. Les autres cas sont plus fastidieux que difficiles et on renvoie à [Sch95] pour le détail.

(ii) L'endomorphisme π_E^r agit comme une matrice scalaire si et seulement si les $l+1$ sous-espaces cycliques sont stables et donc si et seulement si $\Phi(j, X)$ est scindé dans $\mathbb{F}_{q^r}$. □

Cette proposition est très utile pour le théorème suivant, qui relie en quelque sorte l'ordre r de π_E à sa trace :

Théorème 2.44 (Atkin)**.** *Soit E comme dans la proposition précédente. Soit $f_1 f_2 \dots f_s$ la factorisation en polynômes irréductibles sur $\mathbb{F}_q[T]$ de $\Phi_l(j, T)$. Alors, on a les possibilités suivantes :*

(i) Il y a seulement deux facteurs, l'un de degré 1 l'autre de degré l. Dans ce cas, l divise le discriminant $t^2 - 4q$ du polynôme caractéristique de π_E. Notons $r = l$.

(ii) Il y a deux facteurs de degré 1 et tous les autres de degré r. Dans ce cas, $t^2 - 4q$ est un carré modulo l et π_E agit sur $E[l]$ comme une matrice diagonale à valeurs dans $\mathbb{F}_l^*$.

(iii) Tous les facteurs sont de degré $r > 1$. Dans ce cas, $t^2 - 4q$ n'est pas un carré modulo l.

Dans tous les cas, r est l'ordre de $\pi_E \in \mathrm{PGL}_2(\mathbb{F}_l)$ et sa trace vérifie

$$t^2 = (\zeta + 2 + \zeta^{-1})q \mod l, \qquad \text{pour } \zeta \in \mathbb{F}_{l^2} \text{ une racine } r^e \text{ primitive de l'unité.}$$

Démonstration. Comme on l'a déjà vu π_E agit sur $E[l]$ comme une matrice de $\mathrm{GL}_2(\mathbb{F}_l)$ de polynôme caractéristique $X^2 - tX + q$.

S'il y a une valeur propre double mais que la matrice n'est pas diagonalisable, on a un seul espace propre et de plus, le discriminant du polynôme caractéristique est nul. Par ailleurs, π_E^l agit comme une matrice scalaire et pour tout $k < l$, π_E^k n'a qu'un seul espace propre, celui de π_E : la proposition 2.43 permet de conclure qu'on est dans le cas *(i)*.

Si π_E est diagonalisable sur $E[l]$, alors, il y a deux espaces propres qui correspondent à deux facteurs de degré 1. De plus, le polynôme caractéristique est scindé et son discriminant est donc un carré modulo l. Notons ensuite $r = \min\{k \geqslant 1,\ \pi_E^k = \mathrm{Id} \in \mathrm{PGL}_2(\mathbb{F}_l)\}$. Une application directe de la proposition précédente montre que $\Phi_l(j, X)$ a tous ses autres 0 (autres que ceux correspondant aux deux premiers espaces propres mentionnés) dans $\mathbb{F}_{q^r}$ et donc que tous les autres facteurs irréductibles sont de degré r (éventuellement égal à 1). Ceci démontre le cas *(ii)*.

Dans le dernier cas, les valeurs propres sont dans $\mathbb{F}_{q^2}$ mais pas dans $\mathbb{F}_q$: le discriminant $t^2 - 4q$ n'est pas un carré modulo l. On n'a alors aucun espace propre et on définit r comme dans le cas précédent, ce qui montre *(iii)*.

Dans tous les cas, r est le plus petit entier positif tel que π_E agit comme une matrice scalaire c'est-à-dire qui soit l'identité dans $\mathrm{PGL}_2(\mathbb{F}_l)$. Enfin, si on note λ, μ inf $\mathbb{F}_{q^2}$ les deux valeurs propres on a $\lambda^r = \mu^r$ et comme $q = \lambda\mu$, $\lambda^{2r} = q^r$. Ainsi, il existe ζ racine r^{e} de l'unité telle que $\lambda^2 = \zeta q$. La minimalité de r assure que ζ est une racine primitive. Dès lors,

$$t^2 = \left(\lambda + \frac{q}{\lambda}\right)^2 = \lambda^2 + 2q + \frac{q^2}{\lambda^2} = q(\zeta + 2 + \zeta^{-1}).$$

Notons finalement que $\zeta = \lambda^2 q^{-1} \in \mathbb{F}_{l^2}$ et que réciproquement, si $\xi \in \mathbb{F}_{l^2}$ est d'ordre $r | (l \pm 1)$, alors, $(\xi + \xi^{-1})^l = \xi^l + \xi^{-l} = \xi + \xi^{-1}$ qui est donc dans $\mathbb{F}_l$. Si $r = l$, il est plus simple de choisir $\zeta = 1$. □

†. Voir la section suivante 2.3.5 pour les définitions et propriétés des anneaux d'endomorphismes d'une courbe elliptique.

Voyons tout d'abord comment on peut déterminer facilement dans quel cas on se trouve. Pour cela, il suffit de connaître le nombre de zéro de $\Phi_l(j,T)$ dans $\mathbb{F}_q$, ce qui peut se réaliser en calculant $\mathrm{pgcd}(T^q - T, \Phi_l(j,T))$ (en effet, un zéro $\tilde{j} \in \overline{\mathbb{F}}_q$ de $\Phi_l(j,T)$ est dans F_q si et seulement si $\tilde{j}^q = \tilde{j}$). Ce calcul s'effectue encore une fois par exponentiation rapide T dans $\mathbb{F}_q[T]/(\Phi_l(j,T))$.

Comme on l'a déjà vu, dans les deux premiers cas, on a la chance d'avoir une valeur propre, ce qui permet de calculer facilement la trace de π_E. Il convient donc de différentier les cas *(i)*, *(ii)* du cas *(iii)*.

Définition 2.45. *Dans les deux premiers cas, le nombre premier l est appelé un* nombre premier d'Elkies *et dans le dernier, un* nombre premier d'Atkin.

Nombres premiers d'Atkin. Regardons tout d'abord ce que propose Atkin pour accélérer l'algorithme de Schoof. Tout d'abord, on calcule l'ordre r du Frobenius dans $\mathrm{PGL}_2(\mathbb{F}_l)$: pour cela, on sait déjà que $r|(l+1)$. D'après la proposition 2.43 il suffit de trouver le plus petit i tel que $\mathrm{pgcd}(T^{p^i} - T, \Phi_l(j,T))$ ou encore le plus petit i tel que T^{q^i} est égal à T dans $\mathbb{F}_q[T]/(\Phi_l(j,T))$. On peut accélérer ce calcul grâce à la parité de $\frac{l+1}{r}$, qui est donnée par la proposition suivante :

Proposition 2.46. *Soit E une courbe elliptique ordinaire sur $\mathbb{F}_q$ dont le j–invariant n'est ni* 0 *ni* 1728*. Soit $l > 2$ un nombre premier et s le nombre de facteurs irréductibles de $\Phi_l(j,T)$ dans $\mathbb{F}_q[T]$. Alors,*

$$(-1)^s = \left(\frac{q}{l}\right).$$

Une fois que l'on a r, on peut chercher les racines primitives r^{e} de l'unité dans $\mathbb{F}_{l^2}$. Pour chacune de ces racines ζ, on calcule $q(\zeta + 2 + \zeta^{-1}) \in \mathbb{F}_l$, ce qui restreint les valeurs possibles pour la trace modulo l. Il y a $\varphi(r) \leqslant \frac{l+1}{2}$ racines r^{e} primitives de l'unité, ce qui donne par symétrie au plus $\frac{l+1}{4}$ valeurs pour t^2 et donc au plus $\frac{l+1}{2}$ valeurs pour t, ce qui divise le nombre de possibilités par 2 au moins.

Nombres premiers d'Elkies. Dans ce cas, la situation est beaucoup plus favorable pour calculer la trace de $\pi_E \mod l$. Tout d'abord, afin de savoir que l'on est dans ce cas, on a calculé $\mathrm{pgcd}(X^q - X, \Phi_l(j,T))$, ce qui nous donne une façon de trouver une racine de $\Phi_l(j,T)$.

(i) Soit ce pgcd est de degré 1 et on a beaucoup de chance ! En effet, on a $t^2 \equiv 4q \mod l$ et il suffit de calculer une racine carrée de $4q \mod l$. Nous discuterons dans la prochaine section de la complexité de cet algorithme, mais rappelons ici que l est très petit (inférieur $\log q$) et que même un algorithme naïf convient, les algorithmes probabilistes étant les plus adaptés ici.

(ii) Soit il est de degré 2 et on trouve une racine immédiatement.

(iii) Soit il est de degré $l+1$: on est dans le cas particulier où π_E agit comme une matrice scalaire et on a alors aussi $t^2 \equiv 4q \mod l$ comme dans le premier cas.

Une fois que l'on a déterminé un zéro $\tilde{j}$, on calcule le polynôme $F(X)$ dont les racines sont les abscisses des points du noyau correspondant à $\tilde{j}$. L'idée est ensuite similaire à celle de l'algorithme de Schoof : il suffit alors de tester

$$(X^q, Y^q) = [\lambda](X,Y), \qquad \lambda = 1, \dots l-1$$

ce qui nous donne une valeur propre puis la trace. Notons que l'on peut aussi accélérer ce processus en faisant le même travail que pour les nombres premiers d'Atkin. Il est clair que l'on a beaucoup simplifié la procédure de Schoof, tant sur les constantes cachées par la notation O que sur la complexité elle-même. En effet, puisque $\deg F = \frac{l-1}{2}$, on fait ainsi chuter la complexité d'un facteur $\log q$ (ou deux si on n'utilise pas les techniques de multiplication rapide).

Il ne reste donc "plus qu'à" trouver le polynôme $F(X)$. Pour cela, on commence par chercher une équation de la courbe l–isogène à E d'invariant $\tilde{j}$. Nous ne donnons que les formules, déjà suffisamment "lourdes" ; pour les démonstrations, on pourra voir [Sch95] par exemple.

Proposition 2.47 (Atkin). *Une équation de Weierstrass de E/C est donnée par $y^2 = x^3+\tilde{a}x+\tilde{b}$ où*

$$\tilde{a} = -\frac{\tilde{\jmath}'^2}{48\tilde{\jmath}(\tilde{\jmath}-1728)}, \quad \tilde{b} = -\frac{\tilde{\jmath}'^3}{864\tilde{\jmath}^2(\tilde{\jmath}-1728)},$$

avec $\tilde{\jmath}' \in \mathbb{F}_q$ défini par

$$\tilde{\jmath}' = -\frac{18b\frac{\partial\Phi_l}{\partial X}(j,\tilde{\jmath})}{lA\frac{\partial\Phi_l}{\partial Y}(j,\tilde{\jmath})}j.$$

Notons que ces formules sont valables seulement dans le cas où les deux dérivées partielles sont non nulles, ce qui n'est pas une très grande restriction (voir [Sch95] par exemple). On peut aussi montrer que la formule reste valable en calculant $H(Y) = \operatorname{pgcd}\left(\frac{\partial\Phi_l}{\partial X}(j,Y), \frac{\partial\Phi_l}{\partial Y}(j,Y)\right)$ et évaluant en $Y = \tilde{\jmath}$

$$\frac{\frac{\partial\Phi_l}{\partial X}(j,Y)/H(Y)}{\frac{\partial\Phi_l}{\partial Y}(j,Y)/H(Y)}.$$

Il reste ensuite à calculer l'isogénie entre E et E/C Pour cela, on commence par calculer la somme des racines des éléments non nuls de C :

Proposition 2.48. *La somme $\sigma = \sum_{Q\in C, Q\neq\mathcal{O}} x_Q$ est donnée par*

$$\sigma = \frac{l}{2}\overline{\jmath} + \frac{2l}{3}\left(\frac{a}{b} - l\frac{\tilde{a}}{\tilde{b}}\right) - 6l\left(\frac{b}{a} - l\frac{\tilde{b}}{\tilde{a}}\right),$$

où $\overline{\jmath} \in \mathbb{F}_q$ vaut

$$\overline{\jmath} = -\frac{j'^2\frac{\partial^2\Phi_l}{\partial X^2}(j,\tilde{\jmath}) + 2lj'\tilde{\jmath}'\frac{\partial^2\Phi_l}{\partial X\partial Y}(j,\tilde{\jmath}) + l^2\tilde{\jmath}'^2\frac{\partial^2\Phi_l}{\partial X^2}(j,\tilde{\jmath})}{j'\frac{\partial\Phi_l}{\partial X}(j,\tilde{\jmath})}, \quad \text{où} \quad j' = 18\frac{b}{a}j.$$

Maintenant, on sait que l'isogénie est donnée par une expression $\left(\frac{N(X)}{D(X)}, \left(\frac{N(X)}{D(X)}\right)'\right)$ où $D(X) = F(X)^2$. En réinjectant dans l'équation de E/C et en dérivant on obtient l'équation différentielle :

$$(3x^2+a)\left(\frac{N(x)}{D(x)}\right)' + 2(x^3+ax+b)\left(\frac{N(x)}{D(x)}\right)'' = 3\left(\frac{N(x)}{D(x)}\right)^2 + \tilde{b}.$$

En notant ensuite

$$\frac{N(x)}{D(x)} = x + \sum_{i\geqslant 1}\frac{h_i}{x^i},$$

on identifie † les coefficients dans l'équation différentielle : $h_1 = \frac{a-\tilde{a}}{5}$, $h_2 = \frac{b-\tilde{b}}{7}$ et

$$h_k = \frac{3}{(k-2)(2k+3)}\sum_{i=1}^{k-2} h_i h_{k-1-i} - \frac{2k-3}{2k+3}ah_{k-2} - \frac{2(k-3)}{2k+3}bh_{k-3}, \text{ pour } k \geqslant 3.$$

Il nous reste à calculer $D(x)$: on développe en série $\frac{D'(x)}{D(x)} = \sum p_i x^i$ et grâce à l'équation différentielle 2.17 (et à l'expression de σ ci-dessus), il suffit d'inverser le système suivant :

$$h_i = (2i+1)p_{i+1} + (2i-1)ap_{i-1} + (2i-2)bp_{i-2} \text{ pour } i \geqslant 1.$$

puis de retrouver $D(x)$ par des techniques classiques. Pour avoir un peu plus de détails sur ces calculs et/ou sur d'autres algorithmes rapides pour calculer cette isogénie, on peut se référer à [BSMS06].

L'algorithme Sea. Résumons les idées évoquées ci-dessus qui conduisent à l'algorithme Sea, du nom de son inventeur et de ceux qui l'ont amélioré.

†. On suppose ici $p \geqslant 11$; en petite caractéristique, on dispose d'algorithmes bien plus performants utilisant des techniques différentes.

Algorithme 2 : SEA (Schoof–Elkies–Atkin)

Entrée : Une courbe ordinaire sur $\mathbb{F}_q$ d'équation $y^2{=}x^3{+}ax{+}b$ et d'invariant $j{\neq}0{,}1728$.
Sortie : Le cardinal de $E(\mathbb{F}_q)$.

$N_{El} \leftarrow 2$, $El \leftarrow \{(t_2, 2)\}$ `/*`$t_2 \equiv E(\mathbb{F}_q) \mod 2$ `comme dans l'algorithme 1.*/`
$N_{At} \leftarrow 1$, $Al \leftarrow \{\}$ `/*El pour Elkies et At pour Atkin.*/`
$l \leftarrow 2$.
Tant que $N_{El}N_{At} < 4\sqrt{q}$ **Faire**
  $l \leftarrow$NEXTPRIME(l).
  Calculer $\Phi_l(X, Y) \mod p$.
  Calculer $G = X^q \mod \Phi_l(j, X)$ puis $H = \operatorname{pgcd}(G(X) - X, \Phi_l(j, X))$ et $d = \deg H$.
  Si $d \in \{1, l+1\}$ **Alors**
    $t_l \leftarrow \pm 2\sqrt{q} \mod l$.`/*On décide par exemple avec l'ordre d'un point aléatoire.*/`
    $N_{El} \leftarrow lN_{El}$ et $El \leftarrow El \cup \{(l, t_l)\}$.
    Revenir en 4.
  Fin Si
  Calculer $s \mod 2$ la parité du nombre de facteurs de $\Phi_l(j, X)$.
  Calculer $r = \min\{k > 0, X^{q^k} \equiv X \mod \Phi_l(j, X)\}$ en s'aidant de s.
  Calculer $S_l = \{t, \exists \zeta \in \mathbb{F}_l^2$ d'ordre $r, t^2 \equiv q(\zeta + 2 + \zeta) \mod l\}$.
  Si $d = 2$ **Alors**
    Calculer $\tilde{\jmath} \in \mathbb{F}_q$, $\Phi_l(j, \tilde{\jmath}) = 0$. `/*En cherchant une racine de` H`.*/`
    Calculer une équation de E/C (d'invariant $\tilde{\jmath}$) puis $F(x)$ le polynôme annulateur des abscisses de C.
    Pour $\lambda \in S_l$ **Faire**
      Si $(X^q, Y^q) = [\lambda](X, Y) \mod (F(X), Y^2 - X^3 - aX - b)$ **Alors**
        $N_{El} \leftarrow lN_{El}$ et $El \leftarrow El \cup \{(l, \lambda + \frac{q}{\lambda} \mod l)\}$.
        Revenir en 4.
      Fin Si
    Fin Pour
  Sinon `/*Dans ce cas` $d = 0$`.*/`
    $N_{At} \leftarrow lN_{At}$ et $At \leftarrow \{(S_l, l)\}$.
  Fin Si
Fin Tant que
Retourner $n \in [q + 1 - 2\sqrt{2}q, q + 1 + 2\sqrt{q}]$ vérifiant les congruences dans El et At grâce aux restes chinois (et éventuellement à un algorithme pas de bébés, pas de géants). Si la solution n'est pas unique recommencer la boucle **Tant que**.

Ceci étant, on ne peut finir cette présentation sans mentionner son point faible majeur : le polynôme modulaire Φ_l qui possède des coefficients entiers très grands. Pour pallier ce problème, Atkin propose de remplacer les fonctions modulaires j_l par les fonctions f_l définies par :

$$f_l(\tau) = l^s \left(\frac{\eta(l\tau)}{\eta(\tau} \right)^{2s},$$

où $12 = s \operatorname{pgcd}(12, l-1)$ et η est la fonction de Dedekind :

$$\eta(\tau) = q^{\frac{1}{24}} \prod_{n=1}^{\infty} (1 - q^n) \quad \text{où} \quad q = e^{2i\pi\tau}.$$

On peut montrer que les fonctions $f_l(\tau)$ sont des fonctions modulaires pour $\Gamma_0(l)$ et qu'elles ont un développement en série de la forme

$$f_l(\tau) = l^s q^v + \sum_{n \geqslant v+1} a_n q^n \quad \text{avec} \quad 12v = s(l-1).$$

De manière analogue qu'en 2.28 on montre que le polynôme minimal de f_l est donné par

$$\Phi_l^c(X, j(\tau)) = (X - f_l(\tau)) \prod_{k=0}^{l-1} \left(X - f_l\left(\frac{-1}{\tau + k} \right) \right).$$

Le polynôme $\Phi_l^c(X,Y) \in \mathbb{Z}[X,Y]$ est appelé *polynôme modulaire canonique*. Sa factorisation a le même comportement que dans la proposition 2.43 et le théorème 2.44. Pour trouver le j–invariant de la courbe l–isogène à E, on cherche tout d'abord un zéro f de $\Phi_l^c(X,j)$ puis on cherche un zéro $\tilde{j}$ de $\Phi_l^c(\frac{l^s}{f},Y)$. En effet, le théorème de Dedekind sur la fonction η (voir par exemple [Sil95]) nous dit que $\eta(\frac{-1}{\tau}) = \sqrt{i\tau}\eta(\tau)$ pour $\sqrt{\cdot}$ choisie positive sur $\mathbb{R}_+$. Ainsi, un calcul direct nous donne $f_l(\frac{-1}{l\tau}) = \frac{l^s}{f_l(\tau)}$ et donc si $\Phi_l^c(f_l,j)=0)$ alors $\Phi_l^c(\frac{l^s}{f_l},j_l)=0$.

On peut ensuite expliciter des formules analogues à celles présentées dans le paragraphe précédent mais cette fois avec Φ_l^c. On pourra les trouver par exemple dans [Mor95], avec un algorithme pour calculer Φ_l^c. Voici enfin un exemple pour $l=5$ qui fait apparaître l'intérêt d'utiliser Φ_l^c plutôt que Φ_l :

$$\begin{aligned}\Phi_5(X,Y) = {} & X^4+Y^4 - X^3Y^3 + 2232(X^3Y^2+X^2Y^3) - 1069956(X^3Y+XY^3) \\ & + 36864000(X^3+Y^3) + 2587918086X^2Y^2 + 8900222976000(X^2Y+XY^2) \\ & + 452984832000000(X^2+Y^2) - 770845966336000000XY \\ & + 1855425871872000000000(X+Y)\end{aligned}$$

tandis que

$$\Phi_5^c(X,Y) = X^6 + 30X^5 + 315X^4 + 1300X^3 + 1575X^2 - XY + 750X + 125.$$

Finissons par un mot sur la complexité de Sea. Les calculs de Φ_l^c, des isogénies et du polynôme F sont dominés par le reste de l'algorithme. On peut s'attendre à trouver une proportion de nombres premiers d'Elkies de l'ordre de $\frac{1}{2}$: ainsi, on travaillera sur des congruences modulo des nombres premiers de la même taille que ceux de l'algorithme de Schoof. Comme le polynôme F a pour degré $\frac{l-1}{2}$ quand celui de Ψ_l était de $\frac{(l-1)^2}{2}$, on gagne au final un facteur $\log q$ pour un temps d'exécution en $\tilde{O}((\log q)^4)$. Par ailleurs, comme on l'a déjà expliqué, les améliorations d'Atkin font chuter la constante dans le O, ce qui n'est pas négligeable.

2.3.5 Nombre de points et anneau des endomorphismes.

Finissons cette partie par exposer les liens entre le cardinal des points rationnels et l'anneau des endomorphismes : nous présenterons un algorithme se basant sur celui de Cornacchia polynomial mais non déterministe. De plus, on verra comment on pourra le "retourner" pour s'en servir afin d'extraire des racines modulo p, ce qui a été décrit par Schoof dans [Sch85].

Les outils mathématiques. Voyons dans un premier temps comment construire l'équation d'une courbe elliptique, étant donné un anneau convenable. Pour cela,il nous faut introduire quelques notions de théorie des nombres.

Définition 2.49 (Ordre)**.** *Soit $\mathscr{K}$ une algèbre de type fini sur $\mathbb{Q}$. Un* ordre *$\mathscr{R}$ est un sous-anneau de $\mathscr{K}$ qui est un $\mathbb{Z}$–module de type fini vérifiant $\mathscr{R}\otimes\mathbb{Q} = \mathscr{K}$.*

Exemple 2.50 (Corps quadratique)**.** On appelle *corps quadratique complexe* un corps de nombre $\mathscr{K} \simeq \mathbb{Q}(\sqrt{-d})$ pour un entier d sans facteur carré. L'anneau des entiers de $\mathscr{K}$ est un ordre. Plus précisément, les ordres d'un corps quadratique imaginaire $\mathscr{K}$ sont les $\mathbb{Z}+f\mathscr{O}_\mathscr{K}$ pour un certain entier f. Ce dernier vérifie $f = [\mathscr{O}_\mathscr{K} : \mathscr{R}]$ et est appelé le *conducteur* de $\mathscr{R}$.

Attardons-nous un peu sur les ordres d'un corps quadratique imaginaire :

Définition 2.51 (Discriminant †)**.** *Soient* (Id,σ) *les automorphismes d'un corps quadratique imaginaire $\mathscr{K}$ et soit (α,β) une $\mathbb{Z}$–base d'un ordre $\mathscr{R}$ de $\mathscr{K}$. On appelle* discriminant *de $\mathscr{R}$ l'entier :*

$$d_\mathscr{R} = \left(\det\begin{pmatrix}\alpha & \beta \\ \sigma(\alpha) & \sigma(\beta)\end{pmatrix}\right)^2.$$

†. Cette définition se généralise facilement à un corps de nombres quelconque.

Ainsi, soit $\mathscr{K} = \mathbb{Q}(\sqrt{-d})$ et notons † $d_{\mathscr{K}} = d$ si $d \equiv 1 \mod 4$, $d_{\mathscr{K}} = 4d$ si $d \equiv 2, 3 \mod 4$. On a classiquement que $(1, \frac{d_{\mathscr{K}}+\sqrt{d_{\mathscr{K}}}}{2})$ est une $\mathbb{Z}$–base de $\mathscr{O}_{\mathscr{K}}$. Ainsi, si $\mathscr{R} = \mathbb{Z} + f\mathscr{O}_{\mathscr{K}}$ est un ordre dans $\mathscr{K}$ une $\mathbb{Z}$–base de $\mathscr{R}$ peut être donnée par $(1, f\frac{d_{\mathscr{K}}+\sqrt{d_{\mathscr{K}}}}{2})$ et on a la formule

$$d_{\mathcal{R}} = \det \begin{pmatrix} 1 & f\frac{d_{\mathscr{K}}+\sqrt{d_{\mathscr{K}}}}{2} \\ 1 & f\frac{d_{\mathscr{K}}-\sqrt{d_{\mathscr{K}}}}{2} \end{pmatrix}^2 = f^2 d_{\mathscr{K}}.$$

Dès lors, si $x \in \mathbb{Z}_{<0}$, soit x, soit $4x$ est le discriminant d'un certain ordre. Réciproquement, si y est un discriminant, alors, il est facile de voir qu'il caractérise complètement un ordre dans un corps quadratique imaginaire.

Faisons maintenant le lien avec les courbes elliptiques :

Proposition 2.52 (Anneau des endomoprphismes)**.** *Soit E une courbe elliptique sur un corps K. Alors, l'anneau* End E *des endomorphismes est soit :*

(i) l'anneau $\mathbb{Z}$. (Les seules isogénies sont les multiplications par un entier).

(ii) un ordre dans un corps quadratique imaginaire. (L'automorphisme non trivial est donné par le passage à l'isogénie duale).

(iii) un ordre dans une algèbre de quaternions.

De plus, le dernier cas n'est envisageable que lorsque la caractéristique du corps est positive et E supersingulière.

Ainsi, dans le cas des courbes elliptiques sur $\mathbb{C}$, seuls les deux premiers cas surviennent. Dans le cas où l'anneau des endomorphismes est strictement plus grand que $\mathbb{Z}$, on dit que la courbe est *à multiplication complexe*. Voyons quelques-unes des propriétés de ces courbes.

Rappelons que si Λ est un réseau de $\mathbb{C}$ alors, $\mathrm{End}(\mathbb{C}/\Lambda) \simeq \{\alpha \in \mathbb{C},\ \alpha\Lambda \subset \Lambda\}$. Il nous faut donc étudier les idéaux des ordres qui vérifient ces propriétés. Remarquons que si $\mathfrak{a}$ est un idéal de $\mathscr{R}$ alors,

$$\mathscr{R} \subset \{\alpha \in \mathscr{K},\ \alpha\mathfrak{a} \subset \mathfrak{a}\},$$

mais on a pas forcément égalité. Cela conduit à la définition suivante. On pourra trouver les détails omis dans la suite de cette partie dans [Cox89].

Définition 2.53 (Idéaux d'un ordre quadratique imaginaire)**.** *On dit qu'un idéal $\mathfrak{a} \subset \mathscr{R}$ est* propre *si on a égalité dans l'inclusion ci-dessus.*

Par ailleurs, on appelle idéal fractionnaire *de $\mathscr{R}$, un $\mathscr{R}$–module de type fini. On dit enfin qu'un idéal fractionnaire $\mathfrak{a}$ est* inversible *s'il existe un idéal fractionnaire $\mathfrak{b}$ tel que $\mathfrak{ab} = \mathscr{R}$.*

On peut montrer qu'un idéal fractionnaire est de la forme $\alpha\mathfrak{a}$ où $\mathfrak{a}$ est un idéal de $\mathscr{R}$ et $\alpha \in \mathscr{K}$. De plus, un tel idéal est propre si est seulement si il est inversible. De cette observation, on peut introduire le groupe de classes des idéaux de $\mathscr{R}$:

Définition 2.54. *On note $I(\mathscr{R})$ l'ensemble des idéaux fractionnaires propres de $\mathscr{R}$ et $P(\mathscr{R})$ le sous-groupe des idéaux principaux. On appelle* groupe de classe d'idéaux *le quotient*

$$\mathscr{C}\ell(\mathscr{R}) = I(\mathscr{R})/P(\mathscr{R}).$$

On peut dès lors relier ce groupe avec les courbes elliptiques sur $\mathbb{C}$ ayant $\mathscr{R}$ comme anneau d'endomorphismes :

Théorème 2.55. *On garde les mêmes notations. Alors, il existe une bijection entre le groupe de classe d'idéaux $\mathscr{C}\ell(\mathscr{R})$ et les classes d'homothéties (sur $\mathbb{C}$) de réseaux Λ tels que $\mathscr{R} = \{\alpha \in \mathscr{K},\ \alpha\Lambda \subset \Lambda\}$, soit encore les courbes elliptiques sur $\mathbb{C}$ ayant $\mathscr{R}$ comme anneau d'endomorphismes. De plus, pour un tel réseau, le j–invariant correspondant est un entier algébrique dont le polynôme minimal sur $\mathbb{Q}$ n'est autre que*

$$H_D = \prod_{i=1}^{h}(X - j(\Lambda_h)),$$

où $(\Lambda_1, \ldots, \Lambda_h)$ est un ensemble de représentants correspondant aux éléments du groupe $\mathscr{C}\ell(\mathscr{R})$.

†. La quantité $d_{\mathscr{K}}$ est aussi appelée discriminant de $\mathscr{K}$, ce qui ne pose pas d'ambiguïté, comme on l'explique juste après.

On note ce polynôme H_D car il ne dépend que du discriminant de l'ordre $\mathscr{R}$ associé. On peut montrer que $H_D \in \mathbb{Z}[X]$. Décrivons un peu plus précisément ce polynôme en le caractérisant par ses racines. Pour cela, il nous faut un moyen de représenter les classes d'idéaux de $\mathscr{R}$.

Définition 2.56. *Soient a, b, c des entiers. Une forme quadratique $f(x, y) = ax^2 + bxy + cy^2$ est dite* définie positive *si $a > 0$. Elle est* primitive *si les entiers a, b, c sont premiers dans leur ensemble. On dit qu'elle est* réduite *si les entiers a, b, c vérifient de plus*

(i) $|b| \leqslant a \leqslant c$ *et*

(ii) $b \geqslant 0$ *si* $a = c$ *ou* $a = |b|$.

On appelle aussi classiquement discriminant *de f la quantité $b^2 - 4ac$.*

Le terminologie vient du fait que deux formes quadratiques f, g (à coefficients entiers) prennent les mêmes valeurs sur $\mathbb{Z}^2$ si et seulement si elles sont conjuguées sous l'action de $\mathrm{SL}_2(\mathbb{Z})$ c'est-à-dire $f(x, y) = g(\alpha x + \beta y, \gamma x + \delta y)$ avec $\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. La définition est motivée par la propriété que deux formes quadratiques primitives sont conjuguées si et seulement si elles le sont à une unique forme quadratique primitive et réduite. Notons $\mathscr{Cl}(D)$ l'ensemble des classes des formes quadratiques primitives réduites ; on a la proposition qui les relie aux classes d'idéaux d'un ordre et donc aux courbes elliptiques :

Proposition 2.57. *Soit $\mathscr{R}$ un ordre de discriminant D dans un corps quadratique imaginaire $\mathscr{K}$.*

(i) Soit $f(x, y) = ax^2 + bxy + cy^2$ une forme quadratique primitive de discriminant D. Alors, le $\mathbb{Z}$–module engendré par $(a, \frac{-b+\sqrt{D}}{2})$ est un idéal propre de $\mathscr{R}$.

(ii) Deux formes équivalentes induisent des idéaux équivalents.

(iii) L'application induite de $\mathscr{Cl}(D)$ dans $\mathscr{Cl}(\mathscr{R})$ est une bijection.

Démonstration. Notons pour simplifier $[\mathcal{F}]_{\mathbb{Z}}$ le $\mathbb{Z}$–module engendré par une famille $\mathcal{F}$.

(i) Le discriminant de $f(x, 1)$ est $D < 0$ et donc $f(x, 1)$ a une unique racine $\tau \in \mathscr{H}$, demi-plan de Poincaré, que l'on nommera la *racine* de f. En fait, comme $a > 0$, on a

$$\tau = \frac{-b + \sqrt{D}}{2a},$$

et si l'on note $D = f^2 d_{\mathscr{K}}$ avec f le conducteur de $\mathscr{R}$,

$$a\tau = \frac{-b + f\sqrt{d_{\mathscr{K}}}}{2} = -\frac{b + f d_{\mathscr{K}}}{2} + f\frac{d_{\mathscr{K}} + \sqrt{d_{\mathscr{K}}}}{2}.$$

Comme $D = b^2 - 4ac$, les entiers b et $f d_{\mathscr{K}}$ ont la même parité et donc $[1, a\tau]_{\mathbb{Z}} = \mathscr{R}$, ce qui montre que $[a, a\tau]_{\mathbb{Z}}$ est bien un idéal de $\mathscr{R}$.

Cet idéal est propre. Soit $\beta \in \mathscr{K}$ tel que $\beta[a, a\tau]_{\mathbb{Z}} \subset [a, a\tau]_{\mathbb{Z}}$, ce qui est équivalent à $\beta[1, \tau]_{\mathbb{Z}} \subset [1, \tau]_{\mathbb{Z}}$. Alors, il existe des entiers m, n tels que $\beta = m + n\tau$. Mais alors, en utilisant le fait que τ est une racine de f,

$$\beta\tau = -\frac{cn}{a} + \left(m - \frac{bn}{a}\right)\tau.$$

Comme a, b et c sont premiers dans leur ensemble, le fait que $\beta\tau \in [1, \tau]_{\mathbb{Z}}$ implique $a | n$ puis $\beta \in [1, a\tau]_{\mathbb{Z}} = \mathscr{R}$.

(ii) Si deux formes ont les mêmes "racines", au sens défini ci-dessus, elles sont proportionnelles et si elles ont le même discriminant, elles sont égales.. Soient f, g deux formes de discriminant D et de racines τ et τ'. On écrit simplement, pour $z \in \mathscr{H}$ et $M = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$

$$g(\alpha z + \beta, \gamma z + \delta) = (\gamma z + \delta)^2 g(M \cdot z, 1)$$

et comme on sait bien que $\mathscr{H}$ est stable sous l'action de $\mathrm{SL}_2(\mathbb{Z})$, on a l'équivalence

$$\begin{aligned} f(x, y) = g(\alpha x + \beta y, \gamma x + \delta y) &\iff \tau' = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \cdot \tau \\ &\iff [1, \tau]_{\mathbb{Z}} = (\gamma\tau + \delta)[1, \tau']_{\mathbb{Z}}. \end{aligned}$$

Ceci montre que deux formes sont équivalentes si et seulement si elles engendrent des idéaux équivalents (en effet, $\gamma\tau + \delta \in \mathscr{K} = \mathrm{frac}\,\mathscr{R}$).

(iii) Il ne reste plus que la surjectivité : Soit $\Lambda \in \mathscr{R}$ un idéal fractionnaire propre : c'est un réseau de $\mathbb{C}$ et s'écrit donc $[\alpha, \beta]_\mathbb{Z}$ avec $\alpha, \beta \in \mathscr{R}$. O pose alors $\tau = \frac{\alpha}{\beta}$ ou son inverse de telle sorte que $\tau \in \mathscr{H}$. Soit $a \in \mathbb{N}^*$ minimal tel que $a\tau \in \mathscr{R}$, alors $(1, a\tau) = \mathscr{R}$: en effet, si $x \in \mathscr{R}$, $\Lambda \ni x\beta = n\alpha + m\beta$ et ainsi $n\tau = x - m \in \mathscr{R}$. Comme a est minimal, $a|n$ et on a $[1, a\tau]_Z = \mathscr{R}$. Ainsi, on peut écrire pour un entier m, $a\tau = m + f\frac{d_\mathscr{K} + \sqrt{d_\mathscr{K}}}{2}$. Par ailleurs, comme $a\tau \in \mathscr{R}$, $a\tau\alpha \in \Lambda$ et il existe donc des entiers b, c tels que $a\tau\alpha = -b\alpha - c\beta$, ce qui donne en divisant par β : $a\tau^2 + b\tau + c = 0$. Mais alors,

$$a\tau = \frac{-b + \sqrt{b^2 - 4ac}}{2} = m + f\frac{d_\mathscr{K} + \sqrt{d_\mathscr{K}}}{2}$$

ce qui implique directement que le discriminant de $ax^2 + bx + c$ est bien $f^2 d_\mathscr{K}$. La minimalité de a assure que la forme $ax^2 + bxy + cy^2$ est primitive ; elle correspond à l'idéal $a[1, \tau]_\mathbb{Z}$, qui est équivalent à $\beta[1, \tau]_\mathbb{Z} = [\alpha, \beta]_\mathbb{Z}$, ce qui termine la preuve. □

Ainsi en notant $S_D = \{(a, b, c),\ ax^2 + bxy + cz^2 \textit{ est définie primitive et réduite.}\}$, chaque élément correspond à une classe d'idéaux de $\mathscr{R}$, mais donc aussi à une classe de réseaux modulo la multiplication par $\mathscr{K}$ (ou même $\mathbb{C}$), ce qui correspond finalement à une courbe elliptique, à isomorphisme près. Le j–invariant est donné par le réseau de cette classe écrit sous la forme $[1, \tau]_\mathbb{Z}$: avec la démonstration précédente, un triplet $(a, b, c) \in S_D$ donne $\tau = \frac{-b+\sqrt{D}}{2a}$. On en déduit ainsi une expression du polynôme H_D :

$$H_D(X) = \prod_{(a,b,c)\in S_D} \left(X - j\left(\frac{-b + \sqrt{D}}{2a}\right)\right) \in \mathbb{Z}[X]$$

Réduction sur les corps finis. Après avoir trouvé les courbes elliptiques sur $\mathbb{C}$ ayant comme anneau des endomorphismes un ordre fixé, faisons maintenant le lien avec les courbes elliptiques définies sur un corps fini. On veut écrire, pour un ordre donné $\mathscr{R}$ de discriminant D, une équation d'une courbe elliptique sur un corps fini dont l'anneau des endomorphismes soit $\mathscr{R}$.

Il y a tout d'abord le cas où $D = -3f^2$ ou $D = -4f^2$. Dans ce cas $\mathscr{R}$ est un ordre de $\mathbb{Z}[\exp(\frac{2i\pi}{3})]$ ou $\mathbb{Z}[i]$ et on prendra comme équations celles données en 2.23, valables sur n'importe quel corps. Le théorème 2.59 ci-dessous assure que ces courbes contiennent $\mathscr{R}$ dans leur anneau d'endomorphismes. On ne cherchera pas à être plus précis dans ce cas car ceci suffit pour le paragraphe suivant sur les algorithmes.

Soit pour l'instant, $\mathscr{L}$ un corps de nombres, $\mathfrak{p}$ un idéal premier et v la valuation qui lui est attachée. On note $\mathscr{L}_v$ la complétion de $\mathscr{L}$ suivant v : c'est un corps local de caractéristique p où p vérifie $N\mathfrak{p} = p^e$ pour un entier e. On dira que E a bonne réduction suivant $\mathfrak{p}$ (ou v) si elle a bonne réduction sur $\mathscr{L}_v$. Une utilisation du critère de Néron–Ogg–Shafarevich donne :

Théorème 2.58. *Soit E une courbe elliptique définie sur $\mathscr{L}$ et $\mathfrak{p}$ un idéal premier de $\mathscr{L}$. Alors, E a bonne réduction potentielle en $\mathfrak{p}$ c'est-à-dire il existe une extension finie de $\mathscr{L}$ et $\mathfrak{P}$ un idéal au-dessus de $\mathfrak{p}$ pour laquelle E a bonne réduction (suivant $\mathfrak{P}$).*

Soit D un discriminant et soit $\xi \in \overline{\mathbb{Q}}$ une racine de H_D. On va supposer que $\xi \neq 0, 1728$ car sinon $D = -3$ ou -4, cas que l'on a déjà réglé. Soit alors E une courbe elliptique définie sur $\mathbb{Q}(\xi)$ de j–invariant ξ (ce qui est possible grâce à 2.23). Alors, E a bonne réduction potentielle suivant tout idéal premier de $\mathbb{Q}(\xi)$. Les anneaux d'endomorphismes sont reliés par le théorème :

Théorème 2.59. *Soit L un corps de nombres, $\mathfrak{P}$ un idéal premier et E_1, E_2 deux courbes elliptiques ayant bonne réduction $\tilde{E}_1$ et $\tilde{E}_2$ en $\mathfrak{P}$. Alors, le morphisme "naturel"* $\mathrm{Hom}(E_1, E_2) \to \mathrm{Hom}(\tilde{E}_1, \tilde{E}_2)$ *est une injection.*

Démonstration. La théorie classique de réduction des courbes elliptiques donne que pour chaque entier m premier à $\mathrm{car}\,\mathfrak{P}$, $E_2[m] \hookrightarrow E_2$. Soit alors $\varphi \in \mathrm{Hom}(E_1, E_2)$ tel que $\tilde{\varphi} = 0$. Alors, pour tout point $P \in E_1[m]$, $\widetilde{\varphi(P)} = \tilde{\varphi}(\tilde{P}) = \tilde{\mathcal{O}}_2$. Mais comme $\varphi(P) \in E_2[m]$, on en déduit que $\varphi(P) = \mathcal{O}_E$. Ainsi, $E_1[m] \subset \ker\varphi$. Ceci étant vrai pour m arbitrairement grand, seule l'isogénie nulle peut avoir un noyau infini. □

Soit $\mathfrak{p}$ un idéal premier de $\mathscr{K} = \mathbb{Q}(\sqrt{-d})$ le corps quadratique imaginaire contenant $\mathscr{R}$. Notons aussi $p \in \mathbb{Z}$ le nombre premier correspondant. On a le résultat classique de Deuring :

Théorème 2.60 (Deuring)**.** *Soit E/L une courbe elliptique telle qu'elle ait bonne réduction en un idéal $\mathfrak{P}$ au-dessus de $\mathfrak{p}$. Alors, $E \mod \mathfrak{P}$ est supersingulière si et seulement si p est ramifié ou inerte dans $\mathscr{K}$, ce qui se note plus simplement $\left(\frac{-d}{p}\right) \neq +1$.*

Dans le cas inverse où p est décomposé dans K, et si $f = p^r c$ est le conducteur de $\mathscr{R}$ avec $\gcd(r,p) = 1$ alors, $\mathrm{End}(\tilde{E}) \simeq \mathbb{Z} + c\mathscr{O}_{\mathscr{K}}$. En particulier, si $r = 0$, $\mathscr{R} \simeq \mathrm{End}(E) \simeq \mathrm{End}(\tilde{E})$.

Choisissons alors un nombre premier tel que l'on ait $\left(\frac{-d}{p}\right) = 1$. Ainsi p est décomposé et $p\mathscr{O}_{\mathscr{K}} = \mathfrak{p}\mathfrak{p}'$ pour des idéaux premiers de norme p. On a la proposition :

Proposition 2.61. *Soit L une extension finie de $\mathbb{Q}(\xi)$ telle que E ait bonne réduction modulo un idéal premier $\mathfrak{P}$ au-dessus de $\mathfrak{p}$. Alors, $1728 - j \notin \mathfrak{P}$ (ou encore $v_{\mathfrak{P}}(1728 - j) = 0$).*

Démonstration. Notons $\tilde{\cdot}$ le morphisme de réduction "modulo" $\mathfrak{P}$. Supposons que $1728 - \xi \in \mathfrak{P}$. Alors, dans le corps résiduel, $\tilde{\xi} = 1728$ et le théorème 2.59 nous assure que $\mathrm{End}(\tilde{E})$ contient $\mathbb{Z}[i]$. L'injection est nécessairement stricte car sinon, l'anneau des endomorphismes de E serait un ordre de $\mathbb{Z}[i]$, ce que l'on a exclu au début de ce paragraphe. Ainsi, $\mathrm{End}(\tilde{E})$ est forcément de dimension 4 et donc $\tilde{E}$ est supersingulière, ce qui contredit le théorème de Deuring (2.60). □

On a maintenant tout ce qu'il faut pour "écrire" une équation d'une courbe elliptique sur un corps fini ayant un anneau des endomorphismes égal à $\mathscr{R}$ de discriminant D. Pour cela, choisissons un nombre premier p tel que $\left(\frac{D}{p}\right) = 1$ (c'est-à-dire p décomposé dans $\mathscr{K}$, ne divisant pas le conducteur). La proposition 2.61 nous assure que $\xi - 1728$ est inversible mod $\mathfrak{P}$ et que l'on peut réduire directement l'équation suivante "modulo" $\mathfrak{P}$:

$$y^2 + yx = x^3 - \frac{36}{\xi - 1728}x - \frac{1}{\xi - 1728}. \qquad (\star\star)$$

Mais alors, la réduction $\tilde{\xi}$ est une racine de H_D vu comme polynôme sur $\overline{\mathbb{F}}_p$ puisque la "réduction" modulo $\mathfrak{P}$ est un morphisme. Dès lors, il suffit de choisir une racine ξ_p de H_D dans $\overline{\mathbb{F}}_p$; elle est en fait dans une extension finie $\mathbb{F}_q$ de $\mathbb{F}_p$ (de degré inférieur à $\deg H_D$). Puisque chaque racine de H_D dans $\overline{\mathbb{F}}_p$ correspond à une racine de H_D dans $\mathbb{Q}(\xi)$ (qui contient toutes les racines de H_D), on a seulement besoin de réécrire l'équation $(\star\star)$ mais cette fois avec ξ_p, et donc à coefficients dans $\mathbb{F}_q$. Le théorème de Deuring (2.60) nous assure que l'on a trouvé l'équation d'une courbe sur un corps fini $\mathbb{F}_q$ dont l'anneau des endomorphismes est $\mathscr{R}$.

Les algorithmes. Cette théorie de la multiplication complexe à de nombreuses applications algorithmiques. En voici quelques-unes. Commençons par l'algorithme de Cornacchia : étant donné une courbe elliptique à multiplication complexe et son anneau des endomorphismes (*i.e.* le discriminant de son ordre), cet algorithme calcule efficacement son nombre de points rationnels.

On se place en caractéristique $p > 2$ et soit $E/\mathbb{F}_q$ une courbe elliptique dont l'anneau des endomorphismes est un ordre $\mathscr{R}$ de discriminant $D < 0$. On sait que le Frobenius n'appartient pas à $\mathbb{Z} \subset \mathscr{R}$ et a comme polynôme minimal $\pi_E^2 - t\pi_E + q$. On peut alors écrire $\pi_E = \frac{a+b\sqrt{D}}{2}$ et on a $q = \pi_E\hat{\pi}_E = \frac{a^2 - Db^2}{4}$. Il s'agit donc de résoudre l'équation

$$x^2 - Dy^2 = 4q, \text{ avec } x \equiv y \mod 2. \qquad (\spadesuit)$$

Pour cela, nous avons le théorème suivant, dont la démonstration, reposant sur l'utilisation de fractions continues, est détaillée dans [Nit95].

Théorème 2.62. *Soient α, β, m des entiers deux à deux premiers entre eux et $t \in [\![0, m]\!]$ une solution de $t^2 \equiv -\frac{\beta}{\alpha} \mod m$. On dira qu'une solution de*

$$\alpha x^2 + \beta y^2 = m$$

vérifiant $x \neq 0$ et $y > 0$ est primitive si $\gcd(x, y) = 1$.

Alors, si (x, y) est une solution primitive telle que $x \equiv ty \mod m$, elle est unique. De plus, $(-x, y)$ est une solution primitive associée à $t' = m - t$.

Enfin, si une solution vérifiant $x \equiv ty \mod m$ existe, elle est donnée par l'algorithme suivant :

Algorithme 3 : Cornacchia (1908)

Entrée : (α, β, m) premiers entre eux et $t \in [\![\frac{m}{2}, m]\!]$ tel que $t^2 \equiv -\frac{\beta}{\alpha} \mod m$.
Sortie : La solution positive primitive de $\alpha x^2 + \beta y^2 = m$, vérifiant $x = t \mod m$, si elle existe.

1 $r_0 \leftarrow m$; $r_1 \leftarrow t$.
2 **Tant que** $r_i > \sqrt{\frac{m}{\alpha}}$ **Faire**
3 | $r_{i+1} \leftarrow$ le reste de la division euclidienne de r_{i-1} par r_i.
4 **Fin Tant que**
5 $r \leftarrow$ le dernier reste calculé.
6 $s \leftarrow \sqrt{\frac{m - \alpha r^2}{b}}$.
7 **Si** s est un entier **Alors**
8 | **Retourner** (r, s).
9 **Sinon**
10 | **Retourner Echec**.
11 **Fin Si**

Nous savons dans notre application qu'une solution existe. Voyons comment utiliser le théorème 2.62 pour avoir des résultats d'unicité.

Notons que puisque $\mathrm{End}\, E = \mathscr{R}$, E ne saurait être supersingulière et ainsi, $\mathrm{tr}\, \pi_E \neq 0 \mod p$. Dès lors, D doit être premier † à p. Si $D \equiv 0[2]$, alors $x \equiv 0[2]$ tout comme y et il suffit de résoudre

$$x'^2 - Dy'^2 = q \qquad (\spadesuit\spadesuit)$$

Ainsi, suivant la parité de D, on résout ($\spadesuit$) ou ($\spadesuit\spadesuit$) qui satisfont les hypothèses du théorème 2.62. Pour finir cette analyse, on a un résultat d'unicité :

Lemme 2.63. *Supposons que $D \leqslant -4$. Alors, il y a au plus une solution (x, y) à l'équation ($\spadesuit$) vérifiant $x > 0$, $y > 0$, $x \equiv y \mod 2$.*

Démonstration. En effet, si (x, y) et (x', y') sont deux solutions alors, on a $\frac{x}{y} \equiv D \equiv \pm\frac{x'}{y'} \mod q$. Quitte à changer x' en $-x'$, on peut supposer qu'on a égalité. On a alors $x'y \equiv xy' \mod 2q$ puisque $x'y$ et xy' ont même parité. Mais, on a $|x| < \sqrt{q}$, $|y| < \sqrt{\frac{4q}{D}} \leqslant \sqrt{q}$ et de même pour x', y'. Ainsi, $xy', x'y \in [\![-q+1, q-1]\!]$ et comme ils sont égaux modulo $2q$, $x'y = xy'$. En notant $d = \mathrm{pgcd}(x, y)$ et de même avec x', y', on a alors $\frac{x}{d} = \frac{x'}{d'}$ et $\frac{y}{d} = \frac{y'}{d'}$. En réinjectant dans l'équation de départ, on obtient $d = d'$ puis le résultat. □

On résume toutes ces idées dans l'algorithme 4 ci-après, qui détermine le nombre de points rationnels connaissant l'anneau des endomorphismes.

Proposition 2.64. *Cet algorithme probabiliste s'exécute en temps $O(r(\log q)^3)$ avec probabilité d'échec de l'ordre de $\frac{1}{2^r}$.*

Démonstration. L'algorithme de Cornacchia s'exécute en temps $O(\log q^3)$ puisque l'on effectue au plus $\log q$ divisions euclidiennes. Les lignes 7 et 8 ont une complexité absorbée par le reste. C'est donc la première ligne qui capture toute la complexité de cette algorithme. Ceci montre la proposition, en utilisant par exemple l'algorithme probabiliste de Cippolla. □

†. C'est de toute façon compris dans la construction de l'équation de E puisqu'on a $\left(\frac{D}{p}\right) = 1$.

Algorithme 4 : Comptage de points avec CORNACCHIA.

Entrée : $a, b \in \mathbb{F}_q$ et $D < 0$ le discriminant de l'anneau des endomorphismes de E d'équation $y^2 = x^3 + ax + b$.
Sortie : Le cardinal de $E(\mathbb{F}_q)$.

1 **Calculer** $t \in [\![\frac{q}{2}, q]\!]$, $t^2 = D \mod q$.
2 **Essayer** et s'arrêter dès que CORNACCHIA ne retourne pas **Echec** :
3 **Commencer**
4 $(x, y) \leftarrow 2\times$CORNACCHIA$((1, -D, q), t)$. `/*Une solution ''paire'' de` $x^2 - Dy^2 = 4q$ `.*/`
5 $(x, y) \leftarrow$CORNACCHIA$((1, -D, 4q), t + 2q)$.`/*Les racines`[†] `de` $D \bmod 4q$ `sont` $\pm t \pm 2q$ `.*/`
6 **Fin**
7 $l \leftarrow \min\{r \text{ premier }, r \nmid 2x\}$.
8 **Si** $(X^{2q}, y^{2q}) + [q \mod l](X, Y) = [2x \mod l](X^q, Y^q) \mod (\Psi_l, Y^2 - X^3 - aX - b)$ **Alors**
9 **Retourner** $q + 1 - 2x$.
10 **Sinon**
11 **Retourner** $q + 1 + 2x$.
12 **Fin Si**

Application en cryptographie. Cet algorithme, séduisant par sa rapidité, peut paraître un peu anecdotique puisqu'il repose sur l'hypothèse que l'on connaît l'anneau des endomorphismes de E, ce qui n'est pas facile. Néanmoins, on peut le tourner à notre avantage. En effet, comme on l'a vu dans la section 2.1.2, il est intéressant, afin de limiter l'efficacité du logarithme discret, de trouver des courbes elliptiques sur un corps $\mathbb{F}_p$ dont le groupe $E(\mathbb{F}_p)$ a un grand facteur premier, de l'ordre de p. On a alors un algorithme efficace pour générer ce type de courbes :

Algorithme 5 : Génération de courbes elliptiques à multiplication complexe.

Entrée : $D < 0$ un discriminant, le polynôme H_D et une "taille" t.
Sortie : Une équation et un point rationnel dont l'ordre est de la taille de t.

1 **Répéter**
2 **Répéter**
3 Choisir p de la taille t.
4 **Jusqu' à** $\left(\frac{D}{p}\right) = 1$ et $\text{pgcd}(H_d(T), T^p - T) \neq 1$.
5 **Calculer** t racine carrée de D modulo p.
6 $(x, y) \leftarrow$CORNACCHIA$((1, -D, p), t)$.
7 $n_1 \leftarrow p + 1 - x$ et $n_2 \leftarrow p + 1 + x$.
8 **Jusqu' à** ce que n_1 ou n_2 ait un grand facteur premier de l'ordre de p.
9 Echanger si besoin n_1 et n_2 tel que n_1 ait la bonne propriété.
10 Soit r le grand facteur de n_1.
11 **Calculer** $j \in \mathbb{F}_p$ racine de H_D.
12 **Calculer** une équation de E_j et sa tordue E'_j.
13 $E \leftarrow E_j$ ou E'_j suivant que $|E_j(\mathbb{F}_p)| = n_1$ ou n_2.
14 Déterminer $P \in E(\mathbb{F}_p)$ d'ordre r.
15 **Retourner** (E, P).

Les lignes 13 et 14 se réalisent en tirant des points au hasard. On peut aussi modifier la boucle **Répéter** des lignes 1 à 8 pour avoir d'autres propriétés que l'on pourrait souhaiter sur le cardinal de $E(\mathbb{F}_q)$.

Extraction de racine carrée dans $\mathbb{F}_p$. Comme on l'a vu un peu plus haut, c'est le calcul d'un racine modulo p qui empêche (à l'heure actuelle) les algorithmes ci-dessus d'être déterministes. Néanmoins avec l'algorithme SEA, on a vu qu'il était possible de compter le nombre de points

†. Si la ligne précédente échoue, D est impair et comme c'est un discriminant, $D \equiv 1 \mod 4$: t est alors impair et $t^2 \equiv 1 \equiv D \mod 4$.

rationnels en temps polynomial. Utilisons le donc pour "retourner" l'algorithme 5 de comptage avec Cornacchia et ainsi trouver une racine carrée modulo p en temps "polynomial" :

Théorème 2.65 (Schoof (1985))**.** *Soit $D \in \mathbb{Z}$ un entier fixé. Soit $p \equiv 1 \mod 4$ [†] un nombre premier tel que $\left(\frac{D}{p}\right) = +1$. Alors, il existe un algorithme* déterministe *et polynomial en $\log p$ calculant la racine carrée de D modulo p, i.e. $y \in \mathbb{F}_p$, $y^2 \equiv D \mod p$. Cet algorithme dépend exponentiellement de la taille ($\log D$) de l'entier D.*

Remarque 2.66. En particulier , si $D = O((\log p)^k)$ pour un k fixé, cela donne un algorithme polynomial en $\log p$ pour trouver la racine de D modulo p. Par exemple, on pourra ainsi trouver une racine de -1 en temps polynomial avec un algorithme *déterministe*. Mentionnons qu'avec un théorème de Shanks (voir [Sha73]), cela permet d'extraire les racines carrées dans $\mathbb{F}_p$ avec $p \not\equiv 1 \mod 16$ en temps polynomial déterministe.

Démonstration. Tout d'abord, $p \geqslant 5$ et on ne sera jamais en caractéristique 2 ou 3. Notons ensuite que pour $p \equiv 1 \mod 4$, $(-1)^{\frac{p-1}{2}} = 1$ et -1 est un carré modulo p.

Soit donc $D \in \mathbb{Z}$ pour lequel on cherche une racine carrée modulo p. Comme on l'a déjà vu, l'un au moins parmi $\pm D$, $\pm 4D$ est le discriminant d'un ordre quadratique. Ainsi, au besoin, on devra au préalable exécuter l'algorithme sur -4 qui est bien le discriminant d'un ordre (en l'occurrence $\mathbb{Z}[i]$), et dès lors, on va supposer que D est le discriminant d'un ordre dans un corps quadratique imaginaire.

Comme $\left(\frac{D}{p}\right) = 1$, on a en particulier $p \nmid D$ est p ramifié dans $\mathbb{Q}(\sqrt{D})$: le paragraphe précédent donne une équation d'une courbe elliptique sur un corps fini ayant comme anneau des endomorphismes un ordre de discriminant D. Deux problèmes se posent pour effectivement écrire cette équation :

Calculer H_D. Pour cela, on commence par énumérer les éléments de S_D : on a nécessairement $|b| \leqslant a \leqslant \sqrt{|D|/3}$ et on peut donc calculer tous les triplets en temps $\tilde{O}(|D|)$. Ensuite, pour chaque triplet (a, b, c), on approxime la valeur de $j\left(\frac{-b+\sqrt{D}}{2a}\right)$, ce que l'on peut faire à la précision que l'on veut grâce au développement de j et la majoration de ces coefficients donnée en 2.25. On évalue ensuite les fonctions symétriques en ces racines pour trouver une approximation de H_D. Comme ce dernier est à coefficients dans $\mathbb{Z}$, il suffit d'avoir une précision au final inférieur à $\frac{1}{2}$. L'algorithme estime lui-même les précisions dans les calculs intermédiaires grâce au degré $\deg H_D = |S_D|$. Ce dernier peut être majoré trivialement par D ou plus précisément, un théorème de Siegel nous donne $\frac{\log \deg H_D}{\log |D|} \to \frac{1}{2}$. Tout ceci réuni, on peut calculer H_D en temps polynomial [‡] en $|D|$.

Ecrire une racine de $H_D \mod p$. Si le polynôme H_D vu dans $\mathbb{F}_p[X]$ était irréductible, cela ne poserait aucun problème puisqu'il suffirait de se placer dans le corps $\mathbb{F}_q \simeq \mathbb{F}_p[X]/(H_D(X))$. Néanmoins, cela n'est pas toujours le cas. On pourrait alors factoriser H_D via l'algorithme de Berlekamp par exemple, mais cela ruinerait nos espoirs d'avoir un algorithme polynomial déterministe en la taille de p. La solution consiste tout de même à calculer dans l'anneau $\mathbb{F}_p[X]/(H_D(X))$ qui contient des corps finis $\mathbb{F}_p[X]/(P(X))$ où P est un facteur irréductible de H_D. On peut additionner et multiplier sans que cela ne pose de problèmes. Pour la division, il faut avant tout tester si un élément, représenté par un polynôme $R \neq 0$, n'est pas nul dans le corps fini : pour cela, il suffit de calculer le pgcd de H_D et R :
- Si on trouve 1, alors l'élément n'est pas nul et on peut continuer sans soucis.
- Sinon, on a trouvé un facteur F de H_D. On calcule alors facilement un facteur G de H_D premier à F : on peut alors poursuivre les calculs dans $\mathbb{F}_p[X]/(G)$ dans lequel l'élément R n'est pas nul.

Au final, le tout ne revient pas plus cher que de calculer dans un corps de degré $\deg H_D = \tilde{O}(\sqrt{|D|})$ au-dessus de $\mathbb{F}_p$.

Ainsi, on peut "écrire" une équation d'une courbe elliptique E sur un corps fini $\mathbb{F}_q$ avec $q = p^d$, $d \leqslant \deg H_D$. Maintenant, on sait que l'anneau des endomorphismes de cette courbe est

†. Le cas $p = 2$ n'a aucun intérêt et pour $p \equiv -1 \mod 4$, la racine carrée, si elle existe, s'obtient polynomialement en élevant à la puissance $\frac{p+1}{4}$.

‡. En fait, il existe des algorithmes qui calculent H_D en temps quasi optimal en $\tilde{O}(|D|)$.

l'ordre de discriminant D. En particulier, il existe des entiers a, b tels que

$$\pi_E = \frac{a + b\sqrt{D}}{2},\ a \equiv b \mod 2$$

En particulier, $a = \operatorname{tr} \pi_E$ et $4q = 4N(\pi_E) = a^2 - b^2 D$. On peut alors calculer a grâce à l'algorithme de Schoof en temps $\tilde{O}(\log q)^5 = \tilde{O}(|D|^{\frac{5}{2}}(\log p)^5)$. On ne connaît pas q mais cela peut être contourné en calculant

$$\frac{a^2 - 4p^k}{D}$$

jusqu'à ce que l'on trouve un entier, carré parfait (il suffit de faire un calcul approché pour cela). Comme on sait que l'on va aboutir pour $k \leqslant \deg H_D = \tilde{O}(\sqrt{|D|})$, cette complexité est complètement absorbée par celle de l'algorithme de Schoof.

Finalement, le théorème de Deuring (2.60) nous assure que E n'est pas supersingulière et donc $p \nmid \operatorname{tr} \pi_E = a$. Mais alors, si jamais $p|b$, $p|4q + bD^2 = a^2 \Rightarrow p|a$ ce qui est impossible. Ainsi b est inversible dans $\mathbb{F}_p$ et on a finalement dans le corps fini $\mathbb{F}_p$ la relation $\dfrac{a^2}{b^2} = D$. □

3 Codes géométriques.

3.1 Codes correcteurs d'erreurs.

3.1.1 Généralités.

Rappelons brièvement la problématique des codes correcteurs d'erreurs : la fiabilité de la plupart des moyens de communication modernes ne peut être garantie, si ceux-ci sont utilisés tels quels. Néanmoins, on souhaite tout de même pouvoir transmettre des données en réduisant au maximum la probabilité d'erreur. On souhaite donc trouver une méthode pour s'assurer que le message transmis est le bon ou plus exactement un moyen d'être sûr dans certains cas que la transmission est fausse. Une idée simple est par exemple de rajouter un bit de parité, ce qui peut détecter au plus une erreur. Lorsque l'on peut communiquer facilement avec la source, il suffit de lui demander d'envoyer le message à nouveau.

Néanmoins, ce n'est pas toujours le cas, par exemple avec une transmission entre la Terre et un satellite lointain. On peut par exemple penser à envoyer deux fois le même message mais cela pose deux problèmes : le coût de la transmission est élevé et comment choisir lequel est le bon. La problématique est donc double : d'une part détecter si le message reçu est différent du message envoyé et d'autre part corriger ces erreurs.

Avant d'en venir aux codes géométriques, rappelons brièvement quelques notions de bases en théorie des codes correcteurs. On pourra trouver toutes les démonstrations et bien plus dans [vL82].

Définition 3.1 (Codes)**.** *Soit $\mathscr{A}$ un alphabet et $f : \mathscr{A}^k \to \mathscr{A}^n$ une fonction injective que l'on appelle* encodage*. L'entier n est appelé la* longueur *du code, l'image de f est appelée le* code *en lui-même et un élément de cette image un* mot de code*. On notera $q = |\mathscr{A}|$ et on parle de code q–aire.*

L'identité est un exemple de codage ! Néanmoins, tous les éléments de $\mathscr{A}^n$ sont des mots de codes, ce qui ne permet pas de détecter des erreurs. Il nous faut alors introduire un moyen de quantifier l'éloignement de deux mots de code :

Définition 3.2 (Distance de Hamming–Distance minimale)**.** *Soient $a, b \in \mathscr{A}^n$ deux mots. On appelle* distance de Hamming *entre a et b l'entier*

$$d(a,b) = \big|\{i \in [\![1,n]\!], a_i \neq b_i\}\big|.$$

On appelle distance minimale d'un code C l'entier

$$d(C) = \min_{(a,b)\in C^2,\ a\neq b} \{d(a,b)\}.$$

Notons qu'il s'agit en effet d'une distance au sens propre du terme sur l'ensemble $\mathscr{A}^n$. On note $V_q(n,r)$ le cardinal d'une boule fermée de rayon r pour la distance de Hamming. Un simple calcul donne

$$V_q(n,r) = \sum_{i=0}^{r} \binom{n}{i} (q-1)^i.$$

On pose classiquement $\theta = \frac{q-1}{q}$. Alors si l'on fixe une constante $\delta \in]0,\theta[$, le cardinal de cette boule se comporte de la façon suivante :

$$\frac{\log_q V_q(n,\delta n)}{n} \underset{n\to\infty}{\longrightarrow} H_q(\delta) \overset{\text{def}}{=} \delta \log_q(q-1) - \delta \log_q \delta - (1-\delta)\log_q(1-\delta).$$

Lorsque $\mathscr{A} = \mathbb{F}_q$, ce que l'on supposera dans la suite, on peut définir plus simplement le poids w de $a \in \mathbb{F}_q^n$ par le nombre de ses composantes non nulles. Dès lors, $d(a,b) = w(a-b)$.

Un code de distance d peut donc détecter $d-1$ erreurs au plus. De plus, si l'on a moins de $t = \left\lfloor \frac{d-1}{2} \right\rfloor$ erreurs, alors, il existe un unique mot de code à distance inférieure ou égale à t : on dit que le code est *t–correcteur.*

On voit dès lors que la distance minimale d'un code d, sa longueur n et le nombre de mots de codes M sont les quantités qui quantifient la qualité d'un code : on dit que l'on a des (n, M, d)-–codes. Plus précisément, ce sont les ratios par rapport à n qui mesurent cette qualité et l'on définit $\delta(C) = \frac{d}{n}$ la *distance relative* et $R(C) = \frac{\log_q M}{n}$ le *rendement du code* C. Ce dernier est donc le ratio des données utiles sur les données transmises, ce qui justifie aussi l'autre appellation de *taux d'information*. On note enfin $A_q(n, d) = \max\{M,$ il existe un (n, M, d)–code q–aire$\}$: il apparaît important de trouver des bornes (inférieures et supérieures) sur cette quantité :

Proposition 3.3 (Borne de Hamming)**.** *On a la majoration*

$$A_q(n, d) \leqslant \frac{q^n}{V_q(n, t)} \qquad \text{où } t = \left\lfloor \frac{d-1}{2} \right\rfloor.$$

Un code correcteur vérifiant cette borne est dit parfait : en effet, lorsque $d-1$ est pair, il n'y a alors aucun chevauchement puisque les boules de rayon t centrées en les mots de code forment une partition de $\mathscr{A}^n$. D'un autre côté, on a une minoration importante :

Proposition 3.4 (Borne de Gilbert–Varshamov (GV))**.** *On fixe un entier q et les codes considérés sont q–aires. On rappelle que l'on note $\theta = \frac{q-1}{q}$. On a la minoration*

$$A_q(n, d) \geqslant \frac{q^n}{V_q(n, d-1)}$$

dont la version asymptotique s'énonce pour $\delta = \frac{d}{n} \in]0, \theta[$,

$$a_q(\delta) \geqslant 1 - H_q(\delta),$$

où $a_q(\delta) \overset{def}{=} \sup\{R(C),$ tel que $\delta(C) = \delta\}$ vérifie $a_q(\delta) = \sup\{\frac{\log_q A_q(n, \delta n)}{n}\}$.

Mentionnons enfin le célèbre théorème de Shannon qui énonce un résultat d'optimalité :

Théorème 3.5 (Shannon)**.** *Il existe une famille de codes C_n de longueur n de rendement plus grand qu'un R fixé (inférieur à la capacité du canal) dont la probabilité d'erreur après décodage tend vers* 0*.*

Même si la borne GV est constructive (par un algorithme glouton), ni elle ni le théorème de Shannon ne permettent d'obtenir de bons codes utilisables (c'est-à-dire où le codage et le décodage sont faciles). Il nous faut rajouter un peu de structure, ce qui correspond à la section suivante.

3.1.2 Codes correcteurs linéaires.

Dorénavant, on considère comme fonction d'encodage une application linéaire injective d'un $\mathbb{F}_q$–espace vectoriel de dimension k vers $\mathbb{F}_q^n$. On dit alors que l'on a un $[n, k, d]$–code, qui correspond donc avec les notations précédentes à un (n, q^k, d)–code. En choisissant des bases des deux espaces, on peut représenter l'encodeur par une matrice G dit *génératrice* à k lignes et n colonnes de rang k. Un mot de code est donc un élément de la forme xG pour $x \in \mathbb{F}_q^k$. Notons que l'on peut mettre G sous la forme *standard* $(\mathrm{I}_k, \tilde{G})$, les premières colonnes se contentant d'envoyer le message, les dernières ajoutant de la redondance.

Définition 3.6 (Matrices de parité)**.** *Soit H une matrice de $n-k$ lignes et n colonnes de rang $n-k$. Si son noyau est précisément C, alors, on dit que la matrice H est une* matrice de parité *(ou de* contrôle*). Si $y \in \mathbb{F}_q^n$, on appelle* syndrome *de y le vecteur $H^t y$.*

Cette terminologie vient du fait que si $y = x + e$ où x est un mot de code et e une erreur de transmission alors le calcul $H^t y = H^t e$. permet de "repérer" l'erreur (on cherche ensuite un mot de $\mathbb{F}_q^n$ de poids minimal qui appliqué à H donne ce syndrome).

Proposition 3.7 (Codes duaux)**.** *On note C^* le sous-espace vectoriel de $\mathbb{F}_q^n$ de dimension $n-k$ orthogonal à C pour le produit scalaire usuel. C'est un code dont une matrice génératrice est donnée par une matrice de parité de C. On dit alors que les codes sont* duaux*.*

Voyons maintenant de quelles bornes on dispose pour les codes linéaires.

Proposition 3.8 (Borne de Singleton)**.** *Un code de dimension k dans $\mathbb{F}_q^n$ possède une distance minimale d vérifiant*

$$d \leqslant n - k + 1.$$

Un code vérifiant l'égalité sera dit Mds *(pour Minimal Distance Separable).*

Les codes Mds sont en quelque sorte les codes parfaits dans la catégorie des codes linéaires. Parmi ceux-ci, une classe importante est celle des codes de Reed–Solomon que l'on évoque dans la section suivante. Néanmoins, pour ces codes, il faut supposer que la taille q de l'alphabet est supérieur à n, ce qui peut s'avérer gênant : en effet, comme le laisse entrevoir le théorème de Shannon, si l'on veut des codes minimisant la probabilité d'erreur après décodage, il faut pouvoir disposer de codes de longueur arbitrairement grande.

Définition 3.9 (Domaine des codes–Bonne famille de codes)**.**

Considérons l'ensemble $\{\delta(C), R(C),\ C$ est un code q–aire.$\}$. On appelle domaine des codes *q–aires l'ensemble des points d'accumulation de cet ensemble.*

On dit que l'on a une asymptotiquement bonne famille de codes *si les couples de paramètres (δ_n, R_n) ont un point d'accumulation (δ, R) dans le domaine de code.*

On dit enfin que famille de code est excellente *si c'est une asymptotiquement bonne famille de codes dont les paramètres limites (R, δ) sont au dessus de la borne de Gilbert–Varshamov.*

On ne peut donc pas parler d'asymptotiquement bonne famille de codes pour les codes de Reed–Solomon puisque n est limité. De plus, la borne de Singleton affirme que $\delta + R \leqslant 1$ dans le domaine de code. On peut résumer ces notions sur le schéma ci-dessous :

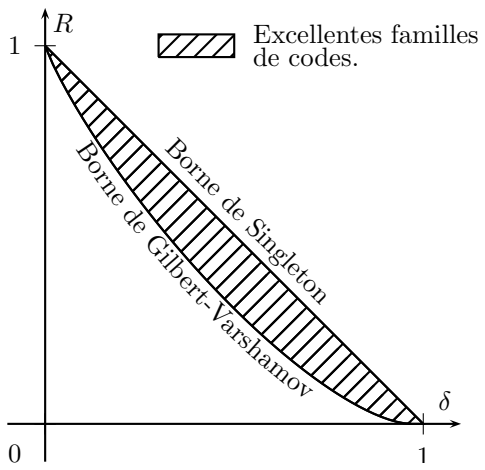


Figure 3: Bornes de Singleton et Gilbert–Varshamov pour $q = 32$.

La notion d'excellente famille de code est justifiée par la proposition suivante, qui affirme qu'une telle famille existe :

Proposition 3.10. *Soit $\delta \in]0, \theta[$, où $\theta = \frac{q-1}{q}$. Alors, il existe une asymptotiquement bonne famille de codes q–aires dont le point d'accumulation (δ, R) vérifie $R \geqslant 1 - H_q(\delta)$, ce que l'on appelle encore la borne de Gilbert–Varshamov.*

On peut estimer cette borne pour $q \to \infty$:

$$H_q(\delta) = \delta \log_q(q-1) + \frac{1}{\log q} H_2(\delta) = \delta + \frac{H_2(\delta)}{\log q} + O\left(\frac{1}{q \log q}\right),$$

et donc $R + \delta$ se "rapproche" de 1 à une vitesse proportionnelle à $\frac{1}{\log q}$.

On a longtemps pensé que cette borne était optimale, avant que l'on trouve une asymptotiquement bonne famille de codes qui vérifie pour $q = p^{2k}$,

$$R + \delta \geqslant 1 - \frac{1}{\sqrt{q} - 1}$$

ce qui est en fait bien meilleur et ce à partir de $q = 49$. Tout ceci repose sur les codes géométriques que l'on va maintenant étudier. Un premier aperçu de l'importance de cette famille de codes est donné dans [Lac85].

3.2 Codes géométriques.

3.2.1 Premiers exemples.

Commençons par donner une définition informelle des codes géométriques et étudier quelques exemples. On considère un objet géométrique $\mathcal{X}$ et un ensemble $\mathcal{P} = \{P_1, \ldots, P_n\}$ de points sur $\mathcal{X}$. On suppose ensuite que l'on dispose d'un $\mathbb{F}_q$–espace vectoriel L de fonctions de $\mathcal{X}$ à valeurs dans $\mathbb{F}_q$. On peut alors définir une fonction d'évaluation :

$$\begin{array}{rccc} \mathrm{ev}_{\mathcal{P}} : & L & \longrightarrow & \mathbb{F}_q^n \\ & f & \longmapsto & (f(P_1), \ldots, f(P_n)) \ . \end{array}$$

L'image de $\mathrm{ev}_{\mathcal{P}}$ est un code linéaire que l'on qualifiera de géométrique. Quitte à remplacer L par $L/\ker \mathrm{ev}_{\mathcal{P}}$, on peut supposer que l'application est bien un codage au sens que l'on a donné dans la section précédente : on ne se préoccupera plus de cette convention.

Evidemment, on n'a rien défini étant donné que l'on ne dit rien sur $\mathcal{X}$. Néanmoins, dans la suite, on ne considérera que des objets $\mathcal{X}$ définis comme des variétés affines ou projectives définies sur un corps fini $\mathbb{F}_q$, les points $P_1, \ldots, P_n$ étant des points $\mathbb{F}_q$–rationnels sur $\mathcal{X}$.

Un premier exemple simple mais important est celui où l'on choisit pour $\mathcal{X}$ la droite affine $\mathbb{F}_q$ et $\{P_1, \ldots, P_n\}$ un ensemble de n points distincts de $\mathbb{F}_q$. L'espace vectoriel L peut être choisi comme l'espace des polynômes à coefficients dans $\mathbb{F}_q$, de degré au plus $k-1$ avec $k \leqslant n$. On obtient ainsi le code classique dit de Reed–Solomon (RS) dont les paramètres sont $[n, k, n-k+1]$. Néanmoins, comme on l'a déjà mentionné, il faut pouvoir choisir n points distincts de $\mathbb{F}_q$ et donc avoir $n \leqslant q$.

Pour pallier ce problème, on peut choisir, dans la même veine, $\mathcal{X}$ l'espace affine de dimension m au-dessus de $\mathbb{F}_q$. Dans cette situation, on prend généralement pour $\mathcal{P}$ l'ensemble des q^m points et pour L les polynômes de m variables de degré total au plus r. On obtient ainsi les codes de Reed–Muller (RM) d'ordre r en m variables : on peut avoir alors une longueur de code plus grande que q mais le code n'est plus MDS.

3.2.2 Codes et géométrie algébrique.

Un premier exemple. Un théorème de géométrie algébrique nous conduit à une autre généralisation des codes de Reed–Solomon où l'on se place, à la différence de Reed–Muller, sur une courbe algébrique.

Théorème 3.11 (Bezout)**.** *Soit $\mathcal{X}_1$ et $\mathcal{X}_2$ deux courbes projectives planes sans composantes communes de degré d_1 et d_2. Alors, $\mathcal{X}_1$ et $\mathcal{X}_2$ s'intersectent en au plus $d_1 d_2$ points dans une clôture algébrique.*

En fait, on a une égalité si l'on introduit la notion de multiplicité d'intersection. Pour cela, il faut définir $\mathrm{mult}_P(\mathcal{X}_1, \mathcal{X}_2) = \dim \mathcal{O}_P/(F_1, F_2)_P$ où $\mathcal{O}_P$ désigne l'anneau local en P, et $F_i(x, y) = 0$ une équation de la courbe $\mathcal{X}_i$.

Soit donc $H \in \mathbb{F}_q[X, Y]$ un polynôme irréductible de degré m définissant † une variété projective $\mathcal{X}$. On choisit pour L l'ensemble des polynômes de $\mathbb{F}_q[X, Y]$ de degré total inférieur ou égal à l. Supposons que l'on dispose de n points rationnels sur $\mathcal{X}$, $(P_1, \ldots, P_n)$ tels que $n \geqslant lm$. Alors,

†. On sous-entend la variété définie par l'équation homogène $Z^m H(X/Z, Y/Z)$.

Proposition 3.12. *Le code obtenu par la méthode décrite dans la section précédente a pour dimension*

$$k = \begin{cases} \binom{l+2}{2} & \text{si } l < m, \\ lm + 1 - \binom{m-1}{2} & \text{sinon,} \end{cases}$$

et sa distance minimale vérifie

$$d \geqslant n - lm.$$

Remarque 3.13. Dans les deux cas, on vérifie aisément l'inégalité familière pour les codes géométriques

$$k + d \geqslant n + 1 - g$$

où $g = \frac{(m-1)(m-2)}{2}$ est précisément le genre de $\mathcal{X}$. On retrouve le fait que pour $g = 0$, on a un code MDS dont Reed–Solomon est un cas particulier.

Démonstration. Si un élément de $F \in L$ est envoyé sur le mot nul alors, F et H ont au moins n zéros en commun. Comme on a choisi $n \geqslant \deg H \deg F$, le théorème de Bezout implique que F et H ont un facteur commun et donc, puisque H est irréductible, $H|F$. Ainsi, la dimension du code est la dimension du quotient $L/(H)$, qui se calcule alors facilement et donne l'expression annoncée.

En fait, cet argument nous donne aussi la distance minimale. En effet, dès que l'image par $\mathrm{ev}_{\mathcal{P}}$ d'un mot a au moins $lm + 1$ composantes nulles, le théorème de Bezout assure qu'il est identiquement nul et donc un mot non nul a un poids au moins égal à $n - lm$. □

Si l'on note $(f_1, \ldots, f_k)$ une base du quotient $L/(H)$ alors, une matrice génératrice du code est donnée par $(f_i(P_j))_{i,j}$, ce qui fournit un moyen explicite de coder.

Le théorème de Riemann–Roch. Ce code fait déjà apparaître la problématique des codes géométriques, à savoir trouver beaucoup de points rationnels sur la variété $\mathcal{X}$, d'autant plus que ce nombre influe directement sur la distance minimale. Une idée pour améliorer la situation consiste à imposer des conditions sur les zéros et les pôles des fonctions de F afin qu'un plus petit nombre de valeurs communes en les P_i imposent l'égalité de deux fonctions. Cela fait fortement penser au théorème de Riemman–Roch qui décrit l'espace vectoriel des fonctions sur $\mathcal{X}$ dont le comportement en les zéros et les pôles est partiellement imposé. Avant de l'énoncer, rappelons quelques définitions pour fixer les notations : on considère dans toute la suite que $\mathcal{X}$ est une courbe algébrique lisse définie sur un corps K, que l'on supposera fini ensuite.

Avant d'introduire la notion de diviseur, rappelons rapidement la notion de différentielle sur $\mathcal{X}$. Notons $\Omega(\mathcal{X})$ le $\overline{K}(\mathcal{X})$–espace vectoriel engendré par les symboles df avec $f \in \overline{K}(\mathcal{X})$, où l'on a les relations classiques $d(f + g) = df + dg$, $d(fg) = fdg + gdf$ et $da = 0$ pour $a \in K$. On rappelle que $\Omega(\mathcal{X})$ est de dimension 1 sur $\overline{K}(\mathcal{X})$. Enfin, si $P \in \mathcal{X}$ et t est une uniformisante en P alors, pour une différentielle $\omega \in \Omega(\mathcal{X})$, il existe une fonction $g \in \overline{K}(\mathcal{X})$ telle que $\omega = gdt$. De plus, $\mathrm{ord}_P(g)$ ne dépend que de P et pas de t : on le note $\mathrm{ord}_P(\omega)$, qui est nul sauf pour un nombre fini de points P. On pourra voir [Ser59] pour plus de détails.

Définition 3.14 (Diviseurs)**.** *On note* $\mathrm{Div}(\mathcal{X})$ *le groupe abélien libre engendré par les points P de $\mathcal{X}$. Un diviseur D s'écrit donc*

$$D = \sum_{P \in \mathcal{X}} n_P(P),$$

où la somme est à support fini ; on définit son degré *par* $\deg D = \sum n_P$.

Si $f \in \overline{K}(\mathcal{X})^*$ est une fonction rationnelle non nulle sur $\mathcal{X}$, on définit le diviseur $\mathrm{div}\, f = \sum_{P \in \mathcal{X}} \mathrm{ord}_P(f)(P)$. *Ce diviseur est dit* principal. *On dit que deux diviseurs sont équivalents s'ils ne diffèrent que d'un diviseur principal et on définit le groupe de Picard* $\mathrm{Pic}(\mathcal{X})$ *comme le quotient du groupe des diviseurs par cette relation.*

Si $\omega \in \Omega(\mathcal{X})$ est une différentielle non nulle, on note de manière analogue aux fonctions rationnelles $\mathrm{div}\, \omega = \sum_{P \in \mathcal{X}} \mathrm{ord}_P(\omega)(P)$.

Enfin, on dit qu'un diviseur est positif *ou* effectif *(et on note $D \geqslant 0$) si tous les coefficients n_P de D sont positifs. On étend cette relation en posant $D_1 \geqslant D_2$ si $D_1 - D_2 \geqslant 0$.*

On rappelle que si f n'est pas constante alors $\operatorname{div} f \neq 0$ et $\deg \operatorname{div} f = 0$. Par ailleurs, on dit qu'un diviseur est défini sur K s'il est invariant sous l'action du groupe de Galois $\mathrm{Gal}_{\overline{K}/K}$. Par exemple, dans le cas où $f \in K(\mathcal{X})^*$, $\operatorname{div} f$ est défini sur K.

Cette notion permet notamment d'imposer le comportement d'une fonction définie sur $\mathcal{X}$. En effet, si $D = \sum n_P(P)$, une fonction f vérifiant $\operatorname{div} f + D \geqslant 0$ a ses pôles dans l'ensemble $\{P, n_P > 0\}$ dont l'ordre n'excède pas n_P et chaque point de l'ensemble $\{P, n_P < 0\}$ est un zéro d'ordre au moins n_P de f. On introduit alors l'espace vectoriel

$$\mathscr{L}(D) = \{f \in \overline{K}(\mathcal{X})^*, \quad \operatorname{div} f + D \geqslant 0\} \cup \{0\}.$$

Notons d'ores et déjà que si $D_1 = D_2 + \operatorname{div} g$ alors $f \mapsto gf$ définit un isomorphisme entre $\mathscr{L}(D_1)$ et $\mathscr{L}(D_2)$. Par exemple, les diviseurs des différentielles non nulles sur $\mathcal{X}$ définissent essentiellement un espace vectoriel.

On peut maintenant énoncer le théorème de Riemann–Roch, qui donne aussi une définition du genre d'une courbe :

Théorème 3.15 (Riemann–Roch)**.** *Soit G un diviseur. L'espace vectoriel $\mathscr{L}(G)$ est de dimension finie que l'on note $\ell(G)$. Plus précisément, si $G < 0$, $\mathscr{L}(G) = \{0\}$. Sinon, soit $W_{\mathcal{X}} = \operatorname{div} \omega_{\mathcal{X}}$ où $\omega_{\mathcal{X}}$ est une différentielle non nulle sur $\mathcal{X}$: alors, il existe un entier g, le genre de $\mathcal{X}$, tel que*

$$\ell(G) - \ell(W_{\mathcal{X}} - G) = \deg G - g + 1.$$

On en déduit classiquement que $\ell(W_{\mathcal{X}}) = g$, $\deg(W_{\mathcal{X}}) = 2g - 2$ et enfin,

$$\deg G > 2g - 2 \Rightarrow \ell(G) = \deg G - g + 1.$$

Remarque 3.16. Le théorème de Riemman–Roch s'énonce pour un corps algébriquement clos. Néanmoins, si G est défini sur K alors, $\mathrm{Gal}_{\overline{K}/K}$ agit sur $\mathscr{L}(G)$ et on peut alors en trouver une base constituée de fonctions dans $K(\mathcal{X})$. Ainsi, tout ce que l'on a énoncé ci-dessus peut très bien s'appliquer sur un corps non algébriquement clos, $\mathbb{F}_q$ dans notre cas.

Les codes géométriques. Nous pouvons maintenant en venir à la construction de codes géométriques : on considère une courbe lisse $\mathcal{X}$ définie sur $\mathbb{F}_q$, un diviseur positif G défini sur $\mathbb{F}_q$ et n points rationnels $(P_1, \ldots, P_n)$ de $\mathcal{X}$ n'appartenant pas au support de G. On note D le diviseur $\sum(P_i)$ et on choisit ensuite l'espace vectoriel $L = \mathscr{L}_{\mathbb{F}_q}(G) = \{f \in \mathbb{F}_q(\mathcal{X}), \operatorname{div}(f) + G \geqslant 0\} \cup \{0\}$. On considère alors le code construit par l'évaluation $\mathrm{ev}_{\mathcal{P}}$ des fonctions de L aux points P_i. Remarquons que puisque D et G ont des supports disjoints, les fonctions de f n'ont pas de pôles en les P_i.

On note ces codes $\mathcal{C}(D, G)$ que l'on appelle parfois des codes de Reed–Solomon géométriques, appellation que l'on peut justifier grâce à leurs matrices génératrices. Remarquons d'ores et déjà que si $\deg G < n$ alors l'évaluation $\mathrm{ev}_{\mathcal{P}}$ est injective puisque si jamais on a $\mathrm{ev}_{\mathcal{P}}(f) = 0$ pour $f \neq 0$ alors, $\operatorname{div}(f) \geqslant D - G > 0$, ce qui est impossible. Ainsi, si $(f_1, \ldots, f_k)$ est une base de $\mathscr{L}(G)$, alors, une matrice génératrice de $\mathcal{C}(D, G)$ est donnée par

$$\begin{pmatrix} f_1(P_1) & \ldots & f_1(P_n) \\ \vdots & \ddots & \vdots \\ f_k(P_1) & \ldots & f_k(P_n) \end{pmatrix}.$$

Ainsi, l'encodage est très facile, dès que l'on a trouvé une base de l'espace $\mathscr{L}(G)$. Nous verrons une méthode pour y arriver dans la section 3.2.4. Voyons maintenant les caractéristiques des codes $\mathcal{C}(D, G)$:

Théorème 3.17. *Supposons que $\deg G < n$. Alors, le code $\mathcal{C}(D, G)$ a pour dimension*

$$k \geqslant \deg G - g + 1,$$

avec égalité si $\deg G > 2g - 2$. De plus, sa distance minimale vérifie l'inégalité

$$d \geqslant n - \deg G.$$

Démonstration. Comme la fonction d'évaluation est injective, la dimension du code est directement donnée par le théorème de Riemman–Roch :

$$k = \dim \mathscr{L}(G) = \ell(G) = \deg G - g + 1 + \ell(W_{\mathcal{X}} - G) \geqslant \deg G - g + 1,$$

et si $\deg G > 2g - 2 = \deg W_{\mathcal{X}}$ on a bien l'égalité puisqu'alors $\ell(W_{\mathcal{X}} - G) = 0$.

Si maintenant une fonction $f \in \mathscr{L}(G)$ s'annule en l points de $\mathcal{P}$, disons $P_{i_1}, \ldots, P_{i_l}$, alors, on écrit $\operatorname{div} f \geqslant (P_{i_1}) + \cdots + (P_{i_l}) - G$ et ainsi,

$$0 = \deg \operatorname{div} f \geqslant l - \deg G.$$

Ainsi, si un mot de code a pour poids d, il s'annule en $n - d$ points et en faisant $l = n - d$ ci-dessus, on obtient l'inégalité annoncée. □

On remarque que l'on a une inégalité analogue à celle de la remarque 3.13 à savoir $k + d \geqslant n - g + 1$ ou encore $R + \delta \geqslant 1 - \frac{1-g}{n}$. En fait, cela n'est pas un hasard puisque l'on peut retrouver le résultat de la proposition 3.12 grâce à ce théorème. Pour cela, on interprète les polynômes de degré au plus l comme les fonctions sur la variété définie par le polynôme H dont les pôles sont contraints par l fois le diviseur G, que l'on définit par l'intersection de $Z^m H(X/Z, Y/Z) = 0$ et $Z = 0$. On obtient alors précisément le code $\mathcal{C}(\sum(P_i), lG)$.

Exemple 3.18. Explicitons un autre exemple important, qui est à la base des excellentes familles de codes que l'on détaillera en 3.3.2. Considérons $\mathcal{X}$ la courbe projective lisse de genre 1 (c'est-à-dire une courbe elliptique) définie sur $\mathbb{F}_4$ par l'équation $X^3 + Y^3 + Z^3 = 0$. Les points rationnels (sur $\mathbb{F}_4 = \{0, 1, \alpha, \overline{\alpha}\}$) sont résumés dans le tableau suivant :

	P_0	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8
x	0	0	0	1	1	1	1	1	1
y	1	α	$\overline{\alpha}$	0	0	0	1	α	$\overline{\alpha}$
z	1	1	1	1	α	$\overline{\alpha}$	0	0	0

On pose $G = 4(P_0)$ et $D = \sum_{i=1}^{8} (P_i)$. Une application directe du théorème de Riemann–Roch nous donne $\ell(G) = 4$ et on trouve assez facilement une base de $\mathscr{L}(G)$ dont les fonctions ont un pôle en P_0 de degré respectivement (0,2,3,4) : $(1, \frac{x}{y+z}, \frac{y}{y+z}, \frac{x^2}{(y+z)^2})$. La matrice génératrice du code $\mathcal{C}(D, G)$ est alors :

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & \overline{\alpha} & \alpha & 1 & \overline{\alpha} & \alpha \\ \overline{\alpha} & \alpha & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & \alpha & \overline{\alpha} & 1 & \alpha & \overline{\alpha} \end{pmatrix}$$

On sait que la distance minimale est au moins 4, ce qui s'avère être le cas sur la matrice génératrice, en ajoutant la deuxième et la quatrième ligne. Ainsi, on obtient un taux d'information de $\frac{1}{2}$ et une distance relative de $\frac{1}{2}$. On peut construire des codes similaires avec $G = l(P_0)$, $0 < l < 8$, vérifiant eux aussi $R + \delta = 1$.

Codes de Goppa géométriques. Passons maintenant à une deuxième classe de codes géométriques : l'idée est que théorème de Riemann–Roch peut se réécrire en terme de différentielles, la fonction d'évaluation en un point étant prise comme le résidu en ce point d'une différentielle. Explicitons ceci plus en détail.

Définition 3.19. *Soit G un diviseur sur le courbe $\mathcal{X}$. On définit l'espace vectoriel*

$$\Omega(G) = \{\omega \in \Omega(\mathcal{X}),\ \operatorname{div} \omega - G \geqslant 0\} \cup \{0\}$$

et on dote $\delta(G)$ la dimension de cet espace vectoriel.

Comme dans le théorème de Riemman–Roch, si G est défini sur un corps K quelconque, la dimension du K–espace vectoriel des différentielles sur $K(\mathcal{X})$ est la même si l'on remplace tout par $\overline{K}$. D'ailleurs, c'est une conséquence du théorème suivant :

Théorème 3.20. *Soit encore $W_{\mathcal{X}}$ le diviseur d'une différentielle non nulle. Alors,*

$$\delta(G) = \ell(W_{\mathcal{X}} - G).$$

Démonstration. En effet, si on note $W_{\mathcal{X}} = \operatorname{div}\omega$, l'application $f \mapsto f\omega$ définit un isomorphisme entre $\mathscr{L}(G)$ et $\Omega(W_{\mathcal{X}} - G)$. (De plus, si ω est une différentielle sur $K(\mathcal{X})$, cette flèche définit aussi un isomorphisme entre K–espaces vectoriels). □

Notons que si l'on prend $G = 0$ dans la formule ci-dessus, on voit qu'il existe g différentielles holomorphes † linéairement indépendantes sur $\mathcal{X}$, ce qui peut constituer une définition du genre de $\mathcal{X}$.

Introduisons finalement la notion de résidu d'une différentielle en un point $P \in \mathcal{X}$:

Définition 3.21. *Soit $\omega \in \Omega(\mathcal{X})$ une différentielle, t une uniformisante en P et $g \in \overline{K}(\mathcal{X})$ telle que $\omega = gdt$. Si l'on note $g = \sum_{n \gg -\infty} a_n t^n$ le développement en série de Laurent de g, on définit classiquement le* résidu *de ω en P par*

$$\operatorname{Res}_P(\omega) = a_{-1}.$$

Notons qu'il faut lever l'ambiguïté de cette définition en montrant que a_{-1} ne dépend pas du choix de l'uniformisante t : voir par exemple [Ser59]. Notons que si $\operatorname{ord}_P(\omega) \geqslant 0$ on a clairement $\operatorname{Res}_P(\omega) = 0$. Ainsi, la somme $\sum_{P\in\mathcal{X}} \operatorname{Res}_P(\omega)$ est bien définie et est à la base d'un théorème fondamental dont on pourra aussi trouver la démonstration dans [Ser59].

Théorème 3.22 (Formule des résidus)**.** *Soit ω une différentielle sur une courbe projective lisse $\mathcal{X}$. Alors,*

$$\sum_{P\in\mathcal{X}} \operatorname{Res}_P(\omega) = 0.$$

On peut dès lors définir le code de Goppa géométrique $\mathcal{C}^*(D, G)$, où D et G sont des diviseurs choisis comme dans le paragraphe précédent. Pour cela, on choisit pour L l'espace $\Omega(G - D)$ et la fonction d'évaluation $\operatorname{ev}^*_{\mathcal{P}} : \omega \to (\operatorname{Res}_{P_1}(\omega), \ldots, \operatorname{Res}_{P_n}(\omega))$. D'une manière comparable aux codes de Reed–Solomon géométriques, on constate que cette fonction d'évaluation est injective dès que $\deg G > 2g-2$. En effet, si $\omega \in \Omega(G-D)$, alors, $ord_{P_i}(\omega) \geqslant -1$ et donc si $\operatorname{Res}_{P_i}(\omega) = 0$, on a nécessairement $\operatorname{ord}_{P_i}(\omega) \geqslant 0$. Dès lors, si ω était une différentielle non nulle donnant une image nulle,

$$2g - 2 = \deg \operatorname{div} w \geqslant \deg G.$$

Voyons maintenant les paramètres du code $\mathcal{C}^*(D, G)$:

Théorème 3.23. *Soit G un diviseur vérifiant* $\deg G > 2g-2$. *Le code $\mathcal{C}^*(D, G)$ a pour dimension*

$$k \geqslant n - \deg G + g - 1$$

avec égalité si $\deg G < n$. *Sa distance minimale vérifie*

$$d \geqslant \deg G - 2g + 2.$$

Comme dans le cas des codes de Reed–Solomon, on note que l'on a $k + d \geqslant n - g + 1$. Ceci n'est pas une coïncidence, comme on le verra dans la section 3.2.3.

Démonstration. Avec la condition $\deg G > 2g - 2$, on a une injection et la dimension du code est celle de $\Omega(G - D)$. Une application du théorème de Riemann–Roch et de son corollaire 3.20 :

$$\begin{aligned}\delta(G - D) = \ell(W_{\mathcal{X}} + D - G) &= \ell(G - D) - \deg(G - D) + g - 1 \\ &\geqslant n - \deg G + g - 1,\end{aligned}$$

avec égalité si $\ell(G - D) = 0$, ce qui est le cas pour $\deg G < n$.

En reprenant la démonstration de l'injectivité de $\operatorname{ev}^*_{\mathcal{P}}$, si une différentielle à un poids d, alors il y a $n - d$ points où le résidu est nul et ainsi

$$2g - 2 = \deg \operatorname{div}\omega \geqslant \deg(G - P_{i_1} - \cdots - P_{i_d}) = \deg G - d,$$

ce qui entraîne l'assertion sur la distance minimale. □

†. On dit qu'une différentielle ω est holomorphe ou régulière si $\operatorname{div}\omega \geqslant 0$.

Le code de Goppa sur $\mathrm{P}^1(\mathbb{F}_q)$. Finissons cette section par un exemple important de codes géométriques, que l'on appelle souvent codes de Goppa (classiques). On les définit par un polynôme $g \in \mathbb{F}_q[X]$ et $\mathcal{P} = \{\gamma_1, \dots, \gamma_n\}$ un ensemble de n points distincts de $\mathbb{F}_q$ tels que $g(\gamma_i) \neq 0$:

$$\Gamma(\mathcal{P}, g) = \left\{ (c_1, \dots, c_n), \quad \sum_{i=1}^{n} \frac{c_i}{X - \gamma_i} = 0 \in \mathbb{F}_q[X]/(g(X)) \right\}$$

Notons que puisque $g(\gamma_i) \neq 0$, $X - \gamma_i$ est inversible modulo $g(X)$.

Proposition 3.24. *Notons $P_i = [\gamma_i : 1]$, $Q = [1 : 0]$, $D = \sum(P_i)$, $E = \operatorname{div}(g(X/Z))_+$ et $G = E - Q$ où D_+ est la partie positive du diviseur D. On a l'équivalence*

$$\underline{\boldsymbol{c}} = (c_1, \dots, c_n) \in \Gamma(\mathcal{P}, g) \iff \omega_{\underline{\boldsymbol{c}}} = \sum_{i=1}^{n} \frac{c_i}{X/Z - \gamma_i} d(X/Z) \in \Omega(G - D).$$

En particulier, $\Gamma(\mathcal{P}, g) = \mathcal{C}^*(D, G)$.

Démonstration. Supposons que $\underline{\boldsymbol{c}} \in \Gamma(\mathcal{P}, g)$. Si l'on écrit $u_i(X)(X - \gamma_i) + v_i(X)g(X) = 1$, la définition de $\Gamma(\mathcal{P}, g)$ donne l'existence d'un polynôme $h(X)$ vérifiant $g(X)h(X) = \sum c_i U_i(x)$ et on a ainsi :

$$\sum \frac{c_i}{X/Z - \gamma_i} = g(X/Z) \left(h(X/Z) + \sum \frac{c_i v_i(X/Z)}{X/Z - \gamma_i} \right).$$

Si R est un zéro de g (dans une clôture), alors, $R \notin \{Q, P_1, \dots, P_n\}$. On en déduit que X/Z est une uniformisante en R et que $\operatorname{div} \omega_{\underline{\boldsymbol{c}}} \geqslant E$. Comme X/Z est aussi uniformisante en P_i, on a $\operatorname{div} \omega_{\underline{\boldsymbol{c}}} \geqslant -(P_i)$. Enfin en réécrivant $\omega_{\underline{\boldsymbol{c}}} = -\big(\sum \frac{c_i Z/X}{1 - \gamma_i Z/X}\big)(X/Z)^2 d(Z/X)$, on a $\operatorname{div} \omega_{\underline{\boldsymbol{c}}} \geqslant -(Q)$, ce qui montre l'implication puisque D, E et (Q) ont des supports disjoints.

Réciproquement, on a $\operatorname{div}(g(X/Z)d(X/Z)) \geqslant E - (\deg G + 2)Q$ et ainsi on a l'inégalité $\operatorname{div}\left(\frac{1}{g(X/Z)}\omega_{\underline{\boldsymbol{c}}}\right) \geqslant (\deg(G) + 1)Q - D$. Ceci implique que $\frac{\sum \frac{c_i}{X - \gamma_i}}{g(X)}$ n'a aucun pôle en les zéros de G et donc que $\underline{\boldsymbol{c}} \in \Gamma(\mathcal{P}, g)$.

Pour la dernière assertion, on voit que si $\underline{\boldsymbol{c}} \in \Gamma(\mathcal{P}, g)$, alors, puisque $\operatorname{Res}_{P_i}(\omega_{\underline{\boldsymbol{c}}}) = c_i$, $\underline{\boldsymbol{c}} \in \mathcal{C}^*(D, G)$. Réciproquement considérons $\omega \in \Omega(G - D)$ une différentielle ayant pour résidu c_i en P_i et $\omega_{\underline{\boldsymbol{c}}}$ définie comme dans la proposition. On a alors $\operatorname{div}(\omega - \omega_{\underline{\boldsymbol{c}}}) \geqslant -(Q)$ mais une différentielle non nulle sur une courbe projective de genre 0 a pour degré -2. Ainsi, $\omega = \omega_{\underline{\boldsymbol{c}}}$ et donc $\omega_{\underline{\boldsymbol{c}}} \in \Omega(G - D)$, ce qui implique que $\underline{\boldsymbol{c}} \in \Gamma(\mathcal{P}, g)$, ce qui termine la démonstration. □

Si l'on note $t = \deg g$, voici une matrice de parité de ce code :

$$H = \begin{pmatrix} \frac{1}{g(\gamma_1)} & \cdots & \frac{1}{g(\gamma_n)} \\ \frac{\gamma_1}{g(\gamma_1)} & \cdots & \frac{\gamma_n}{g(\gamma_n)} \\ \vdots & \ddots & \vdots \\ \frac{\gamma_1^{t-1}}{g(\gamma_1)} & \cdots & \frac{\gamma_n^{t-1}}{g(\gamma_n)} \end{pmatrix}$$

On remarque que la famille $\{\frac{1}{g(X/Z)}, \frac{X/Z}{g(X/Z)}, \dots, \frac{(X/Z)^{t-1}}{g(X/Z)}\}$ est une base de l'espace $\mathscr{L}(G)$ qui est bien de dimension $\deg G - 0 + 1 = t$. On en déduit que ce code n'est autre que le dual du code de Reed–Solomon $\mathcal{C}(D, G)$. On étudiera ce phénomène dans la section suivante, ce qui justifiera le lien entre les notations $\mathcal{C}$ et $\mathcal{C}^*$.

Mais avant d'expliquer ceci, voyons une application des codes de Goppa à la démonstration de la proposition 3.10 sur la borne de Gilbert–Varshamov.

Pour cela, on étend la définition du code de Goppa classique en prenant pour g un polynôme de degré t mais à coefficients dans $\mathbb{F}_{q^m}$. Par contre, on continue à considérer les mots de codes à coefficients dans le sous-corps $\mathbb{F}_q$: on note Γ_{sub} ce code, qui vérifie donc $\Gamma_{sub} = \Gamma \cap \mathbb{F}_q^n$.

Proposition 3.25. *Le code Γ_{sub} a une dimension (sur $\mathbb{F}_q$) supérieure ou égale à $n - tm$.*

Démonstration. En effet, on a vu que le code Γ sur $\mathbb{F}_{q^m}$ avait une dimension plus grande que $n - t$. Le code Γ_{sub} a la même matrice de parité, disons H, que Γ. Par le théorème du rang, $\operatorname{rg}_{\mathbb{F}_{q^m}}(H) \leqslant t$. Ainsi, $\operatorname{rg}_{\mathbb{F}_q}(H) \leqslant mt$ et donc $\dim \Gamma_{sub} \geqslant n - mt$. □

Théorème 3.26. *A q fixé, il existe une asymptotiquement bonne suite de codes de Goppa (sur $\mathbb{F}_q$) qui atteignent la borne de Gilbert–Varshamov.*

Démonstration. Soit $\delta \in]0, \theta[$. Montrons que $(\delta, 1 - H_q(\delta))$ est dans le domaine de code.

Donnons-nous m et t deux paramètres (on fera tendre m vers l'infini et on choisira t qui nous arrange). On pose $n = q^m$ et on choisit pour $=(\gamma_1, \ldots, \gamma_n)$ tous les points de $\mathbb{F}_{q^m}$. On se limite aux polynômes $g \in \mathbb{F}_{q^m}[X]$ irréductibles de degré t.

Fixons un entier d et cherchons une condition (sur g) pour qu'il existe un code $\Gamma_{sub}(\mathbb{F}_{q^m}, g)$ de distance au moins d. Pour cela, considérons un mot $\underline{\boldsymbol{c}}$ de poids j. Sous forme irréductible, le numérateur de $\sum \frac{c_i}{x-\gamma_i}$ a un degré au plus égal à $j-1$ et g est un de ses facteurs irréductibles de degré t : il y en a au plus $\left[\frac{j-1}{t}\right]$. Comme on a $(q-1)^j \binom{n}{j}$ mots de poids j dans $\mathbb{F}_q^n$, et que l'on veut un code de distance au moins d, il nous faut exclure au plus

$$\sum_{j=1}^{d-1} \left[\frac{j-1}{t}\right] (q-1)^j \binom{n}{j} \leqslant \frac{d}{t} V_q(n, d-1)$$

polynômes irréductibles. Or, sur $\mathbb{F}_{q^m}$, on a au moins $\frac{1}{t} q^{mt}(1 - q^{m(-t/2+1)})$ polynômes irréductibles et une condition suffisante pour l'existence d'un code $\Gamma_{sub}(\mathbb{F}_{q^m}, g)$ de distance au moins d est

$$dV_q(n, d-1) < q^{mt}(1 - q^{-mt/2+m}), \qquad (\heartsuit)$$

En choisissant des distances d telles que $\frac{d}{n} \to \delta$, en prenant le logarithme en base q et en divisant par n dans l'expression $(\heartsuit)$, on obtient pour $n \to \infty$ (c'est-à-dire $m \to \infty$) :

$$H_q(\delta) + o(1) \leqslant \frac{mt}{n} + o(1).$$

Ainsi, comme on a toute liberté en t, on voit sur cette inégalité qu'on peut le choisir (en fonction de m) tel que d'une part $(\heartsuit)$ soit vérifiée et d'autre part $\frac{mt}{n} \to H_q(\delta)$.

Mais alors, en utilisant la proposition précédente, on obtient un code dont le taux d'information vérifie $R \geqslant 1 - \frac{mt}{n}$ En faisant tendre m (et donc n) vers l'infini, on trouve que $(\delta, 1 - H_q(\delta))$ est dans le domaine de code. □

3.2.3 Un ou plusieurs types de codes géométriques ?

Comme on l'a vu sur l'exemple du code de Goppa classique, il y a un lien étroit entre codes de Reed–Solomon géométriques et codes de Goppa géométriques :

Proposition 3.27. *Soient $D = \sum P_i$ et G deux diviseurs comme dans la section précédente et supposons que $2g - 2 < \deg G < n$. Alors, les codes géométriques $\mathcal{C}(D, G)$ et $\mathcal{C}^*(D, G)$ sont duaux.*

Démonstration. Tout d'abord, on a vu que la somme des dimensions de ces deux codes vaut bien n. Montrons donc que les deux codes sont orthogonaux.

Soit donc $f \in \mathscr{L}(G)$ et $\omega \in \Omega(G - D)$. On a $\operatorname{div} f\omega = \operatorname{div} f + \operatorname{div} \omega \geqslant -D$. Ainsi, $f\omega$ ne peut avoir que des pôles en D. Comme f n'a pas de pôle en P_i et que ω en a un d'ordre au plus 1 alors, $\operatorname{Res}_{P_i}(f\omega) = f(P_i) \operatorname{Res}_{P_i}(\omega)$. On peut alors appliquer la formule des résidus (3.22) :

$$0 = \sum_{P \in \mathcal{X}} \operatorname{Res}_P(f\omega) = \sum_{i=1}^{n} \operatorname{Res}_{P_i}(f\omega) = \sum_{i=1}^{n} f(P_i) \operatorname{Res}_{P_i}(\omega),$$

ce qui montre que les deux mots de codes associés à f et ω sont orthogonaux. □

En fait, non seulement ces deux types de codes sont duaux mais en fait ils ne forment qu'une seule catégorie de codes. En effet,

Proposition 3.28. *Soit $\{P_1, \ldots, P_n\}$ un ensemble de n points rationnels sur $\mathcal{X}$. Alors, il existe une différentielle ω avec des pôles simples en les P_i tels que $\operatorname{Res}_{P_i}(\omega) = 1$. Alors pour G ayant un support disjoint de P,*

$$\mathcal{C}^*(D, G) = \mathcal{C}(D, \operatorname{div} \omega + D - G).$$

Démonstration. En effet, il suffit de considérer $\omega = \sum \frac{dt_i}{t_i}$ où t_i est une uniformisante en P_i. Ensuite, comme on l'a déjà vu en (3.20), le morphisme

$$\begin{array}{ccc} \mathscr{L}(\operatorname{div}\omega + D - G) & \longrightarrow & \Omega(G-D) \\ f & \longmapsto & f\omega \end{array}$$

est un isomorphisme. Les deux codes ont ainsi même dimension. Par ailleurs, si $f \in \mathscr{L}(\operatorname{div}\omega + D - G)$, f n'a pas de pôles en P_i et donc $\operatorname{Res}_{P_i}(f\omega) = f(P_i)$. Ainsi, $\operatorname{ev}_{\mathcal{P}}(f) = \operatorname{ev}^*_{\mathcal{P}}(f\omega)$, ce qui montre l'égalité des codes. □

Dès lors, tous les exemples de codes géométriques sur $\mathbb{F}_q$ que l'on a donnés sont des codes ou sous-codes de Reed–Solomon géométriques. En fait, on ne pouvait pas en donner d'autres :

Proposition 3.29. *Soit C un code q–aire. Alors, on peut trouver une courbe $\mathcal{X}$ définie sur $\mathbb{F}_q$ et deux diviseurs D et G vérifiant les propriétés habituelles tels que C soit un sous-code de $\mathcal{C}(D,G)$.*

Démonstration. Soit $(M_{i,j}) \in \mathrm{M}_{k,n}(\mathbb{F}_q)$ une matrice génératrice de C. Soit $\mathcal{X}$ une courbe algébrique lisse possédant au moins n points rationnels $P_1, \dots, P_n$ et $D = \sum(P_i)$. Alors, par interpolation, on peut trouver k fonctions sur $\mathcal{X}$, $f_1, \dots, f_k$, telles que $f_i(P_j) = M_{i,j}$. Soit maintenant $G = \sum_{P\in\mathcal{X}} \max(0, \max_i\{-\operatorname{ord}_P(f_i)(P)\})$ de telle manière que $f_i \in \mathscr{L}(G)$ et que D et G ont des supports disjoints (puisque les f_i n'ont pas des pôles en les P_j). Ainsi, C est le sous-code de $\mathcal{C}(D,G)$ engendré par la famille libre $(f_1, \dots, f_k)$. □

3.2.4 Calculer une base de $\mathscr{L}(D)$.

Nous avons vu ci-dessus que dans la construction des codes géométriques, il est intéressant de savoir construire une base de l'espace $\mathscr{L}(D)$: par exemple, cela permet de construire facilement une matrice génératrice des codes de Reed–Solomon géométriques.

On présente les différentes étapes de l'algorithme de Brill–Noether permettant de construire cette base. Cet algorithme est un peu plus général que le cas lisse que l'on a rencontré dans les sections précédentes. C'est pourquoi, nous considérerons une courbe $\mathcal{X}$, irréductible sur un corps K, définie par $F \in K[X]$ irréductible. On autorise à $\mathcal{X}$ d'être singulière mais on impose néanmoins aux singularités d'être ordinaires. Pour les démonstrations et les affirmations non prouvées, on pourra se reporter par exemple à [Ful89].

Rappelons que toute courbe irréductible $\mathcal{X}$ est birationnelle à une courbe lisse irréductible, unique à isomorphisme près : on la nomme le *modèle lisse* de $\mathcal{X}$. Pour voir l'existence, on peut utiliser en chaque point singulier le procédé d'éclatement illustré ci-contre : ce schéma montre la désingularisation (en l'origine) de la courbe "elliptique" $y^2 = x^3 + x^2$. Ce procédé consiste à remplacer un point singulier par une droite projective. Chaque point régulier correspond à un unique point (régulier) et le point singulier se relève en deux points, correspondant aux deux tangentes. Le tout se réalise de façon algorithmique mais cela nous éloignerait trop du sujet. On pourra par exemple voir [LBR88].

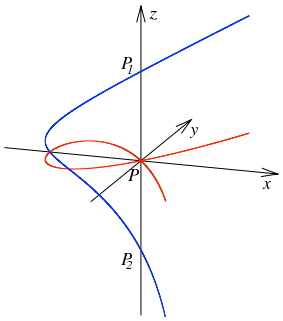


FIGURE 4: Désingularisation du point P de multiplicité 2.

Rappelons aussi que si Q est un point singulier, sa multiplicité peut être directement lue sur le polynôme F définissant $\mathcal{X}$. Par exemple, si $Q = (x, y, 1)$ est un point singulier, la multiplicité de Q est le plus grand entier r tel que toutes les parties homogènes de $F(X - x, Y - y, 1)$ de degré inférieur ou égal à r soient identiquement nulles. On note enfin $Q_1, \dots, Q_{r_Q}$ les points du modèle lisse au-dessus d'un point singulier Q de multiplicité r_Q. On définit alors le diviseur sur $\mathcal{X}$ "mesurant" les singularités :

Définition 3.30 (Diviseur d'adjonction)**.** *On appelle* diviseur d'adjonction *de $\mathcal{X}$ le diviseur*

$$\mathcal{A} = \sum_Q \sum_{i=1}^{r_Q} (r_Q - 1)(Q_i)$$

où la somme porte sur les points singuliers de $\mathcal{X}$.

On peut montrer que le genre de $\mathcal{X}$ est donné par la formule :

$$g(\mathcal{X}) = \frac{(m-1)(m-2)}{2} - \frac{\deg \mathcal{A}}{2} = \frac{(m-1)(m-2)}{2} - \sum_Q \frac{r_Q(r_Q-1)}{2},$$

où $m = \deg F$, F étant le polynôme définissant $\mathcal{X}$.

Définition 3.31. *Si G est un polynôme homogène, non divisible par F, on définit son diviseur, encore noté* $\operatorname{div}(G)$*, comme*

$$\sum_{P \in \mathcal{X}^*} \operatorname{ord}_P(G)(P),$$

où la somme porte sur le modèle lisse $\mathcal{X}^*$ de $\mathcal{X}$.

Notons qu'évaluer G en un point de la courbe n'a pas de sens, puisque l'on travaille en coordonnées projectives. Néanmoins, on peut décider si un point est un zéro. Enfin, si la courbe est lisse, le diviseur d'adjonction est nul et le diviseur (positif) de G est défini naturellement, comme dans le cas des fonctions rationnelles.

Considérons maintenant un diviseur D positif, défini sur K, et expliquons comment construire une base de $\mathscr{L}(D)$. Pour cela énonçons une conséquence du *théorème fondamental de* M. Noether :

Théorème 3.32 (Théorème des résidus)**.** *Soit G_0 un polynôme vérifiant* $\operatorname{div}(G_0) = \mathcal{A} + D + R$ *pour un certain diviseur R positif. Soit D' un diviseur lui aussi positif linéairement équivalent à D. Alors, il existe un polynôme homogène G' de même degré que G_0 tel que* $\operatorname{div}(G') = \mathcal{A} + D' + R$.

On peut en déduire assez facilement la proposition suivante, qui donne une idée de la construction de $\mathscr{L}(D)$

Proposition 3.33. *Soit G_0 un polynôme homogène de degré l, non divisible par F tel que* $\operatorname{div}(G_0) \geqslant \mathcal{A} + D$*. Alors, l'espace $\mathscr{L}(D)$ est engendré par les fonctions rationnelles $\frac{G}{G_0}$, pour un polynôme homogène G de degré l, non divisible par F et vérifiant* $\operatorname{div}(G) \geqslant \operatorname{div}(G_0) - D$.

Démonstration. Soit G comme dans la proposition. Alors, $\operatorname{div}(G/G_0) = \operatorname{div}(G) - \operatorname{div}(G_0) \geqslant -D$ et on a bien $\frac{G}{G_0} \in \mathscr{L}(D)$.

Réciproquement, si $\psi \in \mathscr{L}(D)$, $\psi \neq 0$ on pose $D' = \operatorname{div}\psi + D \geqslant 0$. Comme $\deg D' = \deg D$, on peut appliquer le théorème précédent : il existe G' homogène de degré l tel que $\operatorname{div}(G') = \operatorname{div}(G) - D + D'$. Dès lors, $\operatorname{div}(\psi \frac{G_0}{G'}) = 0$ et ψ et $\frac{G'}{G_0}$ ne différent que d'une constante. □

On résume ces idées dans l'algorithme 6. On note $\mathcal{H}_l$ les polynômes homogènes de degré l.

Algorithme 6 : Calculer une base de $\mathscr{L}(D)$ pour D positif.

Entrée : D un diviseur positif sur une courbe $\mathcal{X}$.
Sortie : Une base de $\mathscr{L}(D)$.

1 Choisir l "suffisamment" grand.
2 **Calculer** un polynôme G_0 vérifiant $\operatorname{div}(G_0) \geqslant \mathcal{A} + D$. Pour cela, résoudre dans $\mathcal{H}_l$ les conditions linéaires :
  – Pour chaque point P de $\operatorname{supp} D$, on calcule une uniformisante t_P en ce point et on écrit les conditions sur les coefficients de G_0 pour que $t_P^{n_P}$ divise G.
  – Pour chaque point Q de $\operatorname{supp}\mathcal{A}$, on s'assure que $\operatorname{ord}_P(Q) \geqslant r_Q$, en annulant les parties homogènes de G_0 de degré plus petit que r_Q.
3 Si l'on obtient aucune solution non divisible par F, retourner en 1 et augmenter l.
4 **Calculer** $E \leftarrow \operatorname{div} G_0 - D$.
5 **Calculer** $\tilde{\mathcal{B}} \leftarrow (\tilde{G}_1, \ldots, \tilde{G}_k)$ une base de $\{G \in \mathcal{H}_l, \operatorname{div}(G) \geqslant E\}$.
6 **Calculer** une base de $\{H \in \mathcal{H}_l, F | H\}$.
7 La compléter par une famille libre $\mathcal{B} = (G_1, \ldots, G_s)$ en une base de $\operatorname{vect}\tilde{\mathcal{B}}$.
8 **Retourner** $\{\frac{G_1}{G_0}, \ldots, \frac{G_s}{G_0}\}$.

La ligne 5 de l'algorithme peut s'effectuer d'une manière similaire à la deuxième à la seule différence que l'on doit remplacer le rôle de D par celui du diviseur positif $E - \mathcal{A}$

Notons que cet algorithme retourne une base de $\mathscr{L}(D)$ de fonctions à coefficients dans un corps sur lequel les diviseurs sont définis, c'est-à-dire une extension finie de K. En effet, non seulement les points du support de D ne sont pas forcément dans K, mais la ligne 4 nécessite de se placer sur le corps où les points d'intersection de $G = 0$ et $\mathcal{X}^*$ sont définis. Néanmoins, comme on l'a déjà vu, il existe une base définie sur K, que l'on peut alors trouver avec de l'algèbre linéaire élémentaire : on peut en effet montrer que pour $f = F_1/F_2 \in \mathscr{L}(D)$, il existe une fonction $g = G_1/G_2$ à coefficients dans K telle que $f = g \in K(\mathcal{X})$. Ainsi, il existe un polynôme F' tel que $F_1G_2 = F_2G_1 + F'F$ et $\deg(F_1G_2) = \deg(G_1F_2) = \deg(F'F)$. On écrit l'équation dans une extension de corps de la forme $K[X]/(Q(X))$ à inconnues dans K, puis on annule les termes devant les puissances non nulles de X.

Pour finir, on peut remarquer que l'on peut facilement en déduire un algorithme pour calculer une base de $\mathscr{L}(D)$ pour D quelconque : on commence par calculer une base de $\mathscr{L}(D_+)$ où D_+ est la partie positive de D. Ensuite, il suffit de chercher les fonctions qui s'annulent en chaque point $P \in \operatorname{supp} D_-$ avec la multiplicité n_P, de manière analogue à la première partie de la ligne 2 de l'algorithme ci-dessus.

3.3 Des courbes avec beaucoup de points rationnels.

3.3.1 Motivations.

Comme on l'a vu dans la section précédente, il apparaît fondamental de pouvoir trouver beaucoup de points rationnels sur une courbe : en effet, le code géométrique résultant en est d'autant plus long. Pour s'en convaincre, étudions un exemple qui met en confrontation un code de Reed–Solomon généralisé avec un traditionnel.

Exemple 3.34. On reprend en fait l'exemple 3.18, que l'on généralise. Soit $q = p^{2k}$ et $r = p^k$. Considérons la courbe $\mathcal{X}$ définie par le polynôme homogène $X^{r+1}+Y^{r+1}+Z^{r+1}$. Cette courbe est lisse puisque $r+1$ est premier à p. La formule de Plücker nous donne le genre de $\mathcal{X} : g(\mathcal{X}) = \frac{r(r-1)}{2}$. Montrons qu'elle possède $1 + q\sqrt{q}$ points rationnels, ce qui est en fait le maximum, comme on le verra ci-dessous.

En effet, si l'une des coordonnées est nulle disons x, alors $yz \neq 0$ et on peut choisir $y = 1$. On a alors à résoudre $1 + z^{r+1} = 0$: si ξ engendre $\mathbb{F}_q^*$ alors, on a les solutions $\xi^{\frac{r-1}{2}+k(r-1)}$ avec $0 \leqslant k < r + 1$. On a ainsi $3(r + 1)$ solutions dont l'une des coordonnées est nulle.

Sinon, on prend $z = 1$ et on cherche à résoudre $x^{r+1} + y^{r+1} + 1 = 0$: choisissons y tel que $a := y^{r+1} + 1 \neq 0$ et $y \neq 0$. Soit $x \in \overline{\mathbb{F}}_q$ tel que $x^{r+1} = a$; on a $x^q = xx^{q-1} = xa^{r-1}$. Or, $a^r = y^{r^2+r} + 1 = y^{1+r} + 1 = a$ et donc au final $x^q = x$, ce qui veut dire que $x \in \mathbb{F}_q$. Comme le polynôme $T^{r+1} - 1$ divise $T^q - T$, il est scindé à racines simples et on trouve donc $r + 1$ possibilités pour x.

Ainsi, au final, on a $3(r + 1) + (r^2 - 1 - (r + 1))(r + 1) = 1 + r^3$ points rationnels sur $\mathcal{X}$.

Soit $Q = [0 : 1 : \xi^{\frac{r-1}{2}}]$, $G = m(Q)$ et $D = \sum(Q_i)$ où les Q_i sont les $q\sqrt{q}$ autres points rationnels. On prend comme on l'a vu $2g - 2 = q - \sqrt{q} - 2 < m < q\sqrt{q}$. Le code $C(D, G)$ a pour longueur $q\sqrt{q}$, dimension $m - g + 1$, et distance supérieure à $n - m$.

On peut construire une base de $\mathscr{L}(G)$ très facilement en considérant les fonctions $f_{i,j} = \frac{x^i y^j}{(y+z)^{i+j}}$, avec $ri + (r + 1)j \leqslant m$ puisque $f_{i,j}$ a un pôle d'ordre $ri + (r + 1)j$ en Q.

On a donc construit un code pour lequel on sait facilement coder. En prenant $q = 16$ et $m = 37$, on obtient un code de rendement $R = \frac{64}{37-6+1} = \frac{1}{2}$. On peut montrer que sa distance minimale est exactement $64 - 37 = 27$. Le code de Reed–Solomon "standard" a une longueur maximale 16, et pour un rendement $\frac{1}{2}$ sur $\mathbb{F}_{16}$, la distance n'est que de 9.

Le choix des diviseurs D et G dans cet exemple est très général dans la construction de "bons" codes géométriques : en effet, plus D a un nombre de points distincts, plus la longueur du code est grande. Ensuite, seul le degré de G (pour un genre fixé) importe dans les formules donnant le taux d'information et la distance relative : c'est pourquoi on le choisit de la forme $m(P)$, afin de ne "consommer" qu'un point et ainsi garder tous les autres pour D.

Tout ceci justifie en quelque sorte la quête de courbes algébriques ayant beaucoup de points rationnels. Commençons par les définitions et notations suivantes.

Définition 3.35. *On note $N_q(g)$ le nombre maximum de points rationnels d'une courbe projective absolument irréductible, lisse, de genre g, définie sur $\mathbb{F}_q$. On note aussi*

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

La dernière quantité peut être motivée par la borne de Hasse–Weil qui généralise le théorème 2.34 en genre supérieur :

Théorème 3.36 (Hasse–Weil)**.** *Soit $\mathcal{X}$ une courbe projective lisse, absolument irréductible, de genre g définie sur $\mathbb{F}_q$. Alors, le nombre de points rationnels $|\mathcal{X}(\mathbb{F}_q)|$ vérifie les inégalités*

$$\big||\mathcal{X}(\mathbb{F}_q)| - (q+1)\big| \leqslant 2g\sqrt{q}.$$

Cette borne est atteinte dans le cas où q est un carré grâce à la courbe de l'exemple que l'on a détaillé ci-dessus

Maintenant, on peut s'intéresser d'une part aux résultats asymptotiques sur $A(q)$ et d'autre part aux quantités $N_q(g)$ à q et g fixées.

3.3.2 Résultats asymptotiques : la borne Tvz.

Le théorème de Hasse–Weil nous donne une première idée de $A(q)$ puisque l'on a facilement l'inégalité $A(q) \leqslant 2\sqrt{q}$. Néanmoins, cette borne n'est pas optimale. En fait, on a le théorème :

Théorème 3.37 (Drinfeld–Vlăduţ)**.** *On a l'inégalité*

$$A(q) \leqslant \sqrt{q} - 1,$$

qui est en fait une égalité si q est un carré.

On en déduit assez facilement la borne de Tsfasman–Vlăduţ–Zink (Tvz).

Théorème 3.38 (Borne Tvz)**.** *On fixe $q = p^{2k}$ un carré. Pour chaque R, il existe une asymptotiquement bonne famille de codes dont le taux d'information tend vers R et la distance relative tend vers un δ vérifiant*

$$R + \delta \geqslant 1 - \frac{1}{\sqrt{q}-1}.$$

Cette borne est meilleure que celle de Gilbert–Varshamov dès que $q \geqslant 49$, comme l'illustre la figure ci-dessous.

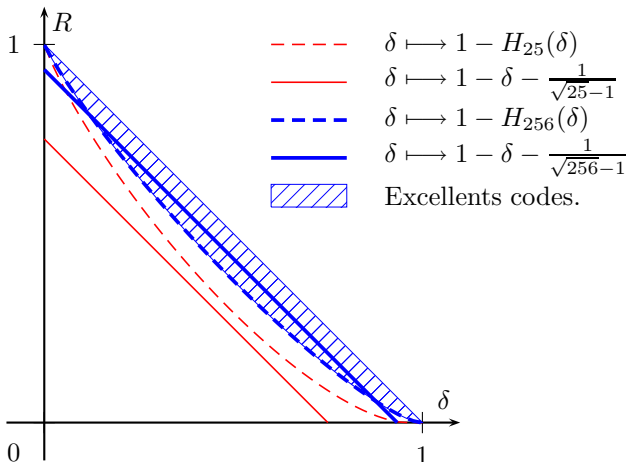


Figure 5: Borne Tvz pour $q = 25$ et $q = 256$.

Démonstration. Remarquons que si $R \geqslant 1 - \frac{1}{\sqrt{q}-1}$, tout code de rendement R convient ! On suppose alors $R < 1 - \frac{1}{\sqrt{q}-1}$.

Pour q carré, on a égalité dans le théorème de Drinfeld–Vlăduţ : il existe une suite de courbes $\mathcal{X}_l$ définies sur $\mathbb{F}_q$ de genre g_l ayant $n_l + 1$ points rationnels, $(P_0, \dots, P_{n_l})$, avec la propriété

$$\lim_{l\to\infty} \frac{n_l + 1}{g_l} = \sqrt{q} - 1.$$

Pour chacune de ces courbes, on choisit $D = \sum_{i=1}^{n_l}(P_i)$ et $G = m_l(P_0)$ avec m_l vérifiant $m_l < n_l$ et $\frac{m_l - g_l + 1}{n_l} \to R$ (ce qui est possible vu la supposition que l'on a faite sur R). Dès lors, le code $\mathcal{C}(D, G)$ de longueur n_l vérifie, si l'on note d_l sa distance minimale et k_l sa dimension,

$$k_l + d_l \geqslant n_l + 1 - g_l \Longrightarrow R_l + \delta_l \geqslant 1 - \frac{g_l - 1}{n_l}.$$

En faisant tendre l vers l'infini et quitte à extraire une sous-suite pour que $(\delta_l)_l$ converge, on a montré le résultat. □

On verra dans la section 3.3.3 une démonstration théorème 3.37 de Drinfeld–Vlăduţ, utilisant les *conjectures de Weil*. Pour l'instant on va seulement exhiber une suite de courbes dans le cas $q = p^{2k}$, qui va montrer que $A(q) \geqslant \sqrt{q} - 1$, ce qui suffit pour établir la borne Tvz.

Courbes Hermitiennes. On se place sur $\mathbb{F}_q$ avec $q = r^2 = p^{2k}$ et on considère le polynôme $F(X, Z) = X^{r+1} - Z^r - Z$. On construit une suite de courbes $\mathcal{X}_n$ définies par les idéaux †

$$\mathcal{I}_n = \langle F(X_1, X_2), F(X_2, X_3), \dots, F(X_{n-1}, X_n)\rangle \subset \mathbb{F}_q[X_1, X_2, \dots, X_n].$$

Ces idéaux sont premiers et définissent des variétés algébriques irréductibles ; comme elles sont de degré de transcendance 1, ce sont des courbes irréductibles.

Le genre de $\mathcal{X}_n$. Pour étudier ces courbes, il est plus pratique d'étudier leur corps de fonctions rationnelles $\mathcal{F}_n = \mathbb{F}_q(\mathcal{X}_n)$. Ces corps de fonctions sont reliés par la formule de récurrence $\mathcal{F}_1 = \mathbb{F}_q(z_1)$ et $\mathcal{F}_{n+1} = \mathcal{F}_n(z_{n+1})$ où

$$z_{n+1}^q + z_{n+1} = x_n^{q+1}$$

où $x_n = \frac{z_n}{x_{n-1}} \in \mathcal{F}_n$ et $x_1 = z_1$ et $x_0 = 1$.

Introduisons les notations classiques suivantes. Pour une description plus précise, on pourra par exemple voir [Sti09].

Notation 3.39.
- *On note $\mathscr{P}(\mathcal{F}_n)$ l'ensemble des places P de $\mathcal{F}_n$, c'est-à-dire les idéaux maximaux des anneaux de valuation (notés $\mathcal{O}_P$) de $\mathcal{F}_n$*
- *On note $\deg P = [\mathcal{O}_P/P : \mathbb{F}_q]$ le degré de P. Quand il est égal à 1, on dit que P est une place rationnelle.*
- *On note v_P la valuation discrète normalisée associée à la place P.*
- *On note $P'|P$ si P' est une place au-dessus de P ($\mathcal{O}_P \subset \mathcal{O}_{P'}$). On note $e(P'|P)$ l'entier vérifiant $v_{P'}(\cdot) = e(P'|P)v_P(\cdot)$.*

Afin de calculer le genre de $\mathcal{F}_n$ on souhaite utiliser la formule d'Hurwitz. Pour cela, il nous faut encore introduire une notion, afin de pouvoir écrire une formule générale en caractéristique positive.

Définition 3.40 (Module complémentaire)**.** *Soit P une place sur $\mathcal{F}$ et $\mathcal{O}_P$ son anneau de valuation. On pose*

$$\mathcal{O}'_P = \bigcap_{P'|P} \mathcal{O}_{P'}$$

la clôture intégrale de $\mathcal{O}_P$ dans $\tilde{\mathcal{F}}$.

On définit alors le module complémentaire *sur $\mathcal{O}_P$ comme le $\mathcal{O}'_P$–module*

$$\mathcal{C}_P = \{z \in \tilde{\mathcal{F}},\ \mathrm{Tr}_{\tilde{\mathcal{F}}/\mathcal{F}}(z\mathcal{O}'_P) \subset \mathcal{O}_P\}.$$

†. Il faudrait, pour être exact, homogénéiser les polynômes engendrant $\mathcal{I}_n$.

On peut montrer qu'il existe un élément $t \in \tilde{\mathcal{F}}$ tel que $\mathcal{C}_P = t\mathcal{O}'_P$. De plus, pour $P|P'$, la quantité $-v_{P'}(t)$ ne dépend que de P et P' : on l'appelle l'*exposant différentiel*, noté $d(P'|P)$.

Théorème 3.41 (Formule d'Hurwitz)**.** *Soit $\tilde{\mathcal{F}}$ une extension séparable et finie de $\mathcal{F}$, deux corps de fonctions algébriques. Soit $\tilde{\mathcal{K}}$ et $\mathcal{K}$ les corps des constantes correspondants. Alors, on a la relation*

$$2\tilde{g} - 2 = (2g-2) + \sum_{P \in \mathscr{P}(\mathcal{F})} \sum_{P'|P} d(P'|P) \deg(P').$$

Remarque 3.42. Dans le cas où $\mathrm{car}(\mathcal{K}) \nmid e(P'|P)$, on peut montrer la relation $d(P'|P) = e(P'|P) - 1$, ce qui permet de réécrire la formule d'Hurwitz sous sa forme plus "courante".

Donnons maintenant sans démonstration les propriétés générales d'une extension du type de $\mathcal{F}_n \subset \mathcal{F}_{n+1}$, dite d'*Artin–Schreier*.

Théorème 3.43. *Soit $\mathcal{F}/\mathbb{F}_q$ un corps de fonctions algébriques où $\mathbb{F}_q$ est algébriquement clos dans $\mathcal{F}$. Soit $x \in \mathcal{F}$ et $P \in \mathscr{P}(\mathcal{F})$ telle que $v_P(x) = -m$, $m > 0$ premier avec p.*

Alors, le polynôme $T^q + T - x \in \mathcal{F}[T]$ est absolument irréductible et si on note $\tilde{\mathcal{F}} = \mathcal{F}(z)$ où $z^r + z = x$ alors, on a :

(i) $\tilde{\mathcal{F}}/\mathcal{F}$ est une extension galoisienne de degré r et $\mathbb{F}_q$ est algébriquement clos dans $\tilde{\mathcal{F}}$.

(ii) La place P est totalement ramifiée dans $\tilde{\mathcal{F}}$, c'est-à-dire il existe une unique place P' au-dessus de P. On a $e(P'|P) = r$, $\deg P' = \deg P$ et $d(P'|P) = (r-1)(m+1)$.

(iii) Soit $Q \in \mathscr{P}(\mathcal{F})$ un zéro de x. L'équation $\alpha^r + \alpha = 0$ possède r racines distinctes α dans $\mathbb{F}_q$. Pour chaque α il existe une unique place $Q_\alpha \in \mathscr{P}(\tilde{\mathcal{F}})$ au-dessus de Q telle que $\deg Q_\alpha = \deg Q$ et Q_α est un zéro de $z - \alpha$.

Ce théorème nous donne des informations précieuses sur la tour d'extensions $\mathcal{F}_1 \subset \mathcal{F}_2 \subset \cdots \subset \mathcal{F}_n$.

Proposition 3.44. *(i) Supposons qu'il existe $P \in \mathscr{P}(\mathcal{F}_n)$ qui soit un pôle simple de x_n (c'est-à-dire $v_P(x_n) = -1$). Alors, $[\mathcal{F}_{n+1} : \mathcal{F}_n] = r$. De plus, P est totalement ramifiée et la place P' au-dessus de P est un pôle simple de x_{n+1}.*

(ii) Par ailleurs, il existe une unique place Q_n sur $\mathcal{F}_n$ qui est un zéro commun de $z_1, \ldots, z_n$. Cette place est rationnelle et se décompose totalement en r places rationnelles sur $\mathcal{F}_{n+1}$.

Démonstration. *(i)* Le théorème 3.43 *(i)* nous donne directement que $[\mathcal{F}_{n+1} : \mathcal{F}_n] = r$ et que P est totalement ramifiée. On a alors

$$v_{P'}(z_{n+1}^r + z_{n+1}) = v_{P'}(x_n^{r+1}) = e(P'|P)(r+1)v_P(x_n) = -r(r+1),$$

et ainsi P' est un pôle de z_{n+1} et $-r(r+1) = v_{P'}(z_{n+1}^r + z_{n+1}) = rv_{P'}(z_{n+1})$. On écrit :

$$v_{P'}(x_{n+1}) = v_{P'}(z_{n+1}) - v_{P'}(x_n) = -(r+1) - rv_P(x_n) = -1.$$

(ii) Il suffit de le vérifier pour $n = 1$ puis de dérouler une induction dont l'hérédité est directement assurée par le théorème 3.43 (iii). □

On note $P_\infty = \{f(x_1)/g(x_1),\ \deg f < \deg g\}$: c'est le pôle (rationnel) de $x_1 \in \mathcal{F}_1 = \mathbb{F}_q(x_1)$. On en déduit par récurrence qu'il existe toujours une place $P \in \mathcal{F}_n$ qui vérifie les conditions de la proposition ci-dessus.

On obtient aussi, avec le point *(i)* du théorème 3.43, que l'extension $\mathcal{F}_n \subset \mathcal{F}_{n+1}$ est galoisienne de degré r et que ces deux corps ont le même corps de constantes $(\mathbb{F}_q)$. Ainsi, pour utiliser la formule d'Hurwitz il ne nous reste "plus qu'à" déterminer les places qui sont ramifiées. Nous ne donnons pas la démonstration un peu technique, seulement les idées. On pourra par exemple voir [SG95] pour les détails.

Notation 3.45. *Pour une place $P \in \mathscr{P}(\mathcal{F}_n)$, on note $P \cap \mathcal{F}_k$ sa restriction à $\mathcal{F}_k$ pour $k \leqslant n$. Définissons ensuite les ensembles*

(i) Pour $n \geqslant 2$, on note $S_0^{(n)} = \{P \in \mathscr{P}(\mathcal{F}_n),\ P \cap \mathcal{F}_{n-1} = Q_{n-1}$ et $P \neq Q_n\}$.

(ii) *Pour* $1 \leqslant i \leqslant [\frac{n-3}{2}]$, $S_i^{(n)} = \{P \in \mathscr{P}(\mathcal{F}_n),\ P \cap \mathcal{F}_{n-1} \in S_{i-1}^{(n-1)}\}$.

(iii) $S^{(1)} = \{P_\infty\}$, $S^{(2)} = \{P \in \mathscr{P}(\mathcal{F}_2),\ P \in S_0^{(2)}$ *ou* $P \cap \mathcal{F}_1 = P_\infty\}$ *et*

$$S^{(n)} = \begin{cases} \{P \in \mathscr{P}(\mathcal{F}_n),\ P \cap \mathcal{F}_{n-1} \in S^{(n-1)}\} & \text{si } n \geqslant 3 \text{ est impair.} \\ \{P \in \mathscr{P}(\mathcal{F}_n),\ P \cap \mathcal{F}_{n-1} \in S^{(n-1)} \cup S_{\frac{n-4}{2}}^{(n-1)}\} & \text{si } n \geqslant 4 \text{ est pair.} \end{cases}$$

Proposition 3.46 (Ramifications des places de $\mathcal{F}_n$ sur $\mathcal{F}_{n+1}$)**.**

(i) *Les places de* $S_i^{(n)}$ *sont totalement décomposées dans l'extension* $\mathcal{F}_n \subset \mathcal{F}_{n+1}$.

(ii) *Pour une place* $P \in S^{(n)}$, *on a* $v_P(x_n) = -1$.

(iii) *Les seules places de* $\mathcal{F}_n$ *qui se ramifient dans* $\mathcal{F}_{n+1}$ *sont celles de* $S^{(n)}$.

On peut alors en déduire tout ce qu'il nous faut pour appliquer la formule d'Hurwitz. En effet, le point *(ii)* de la proposition ci-dessus et le théorème 3.43 *(ii)* nous assurent que $P \in S^{(n)}$ est totalement ramifiée et si l'on note P' la place au-dessus de P, ce même théorème nous donne l'exposant différentiel $d(P'|P) = (r-1)(r+2)$.

Pour conclure, il suffit de calculer le cardinal de $S^{(n)}$ pour $n \geqslant 2$. Montrons par récurrence que $|S^{(n)}| : r^{[n/2]}$. Si n est impair, puisque les places de $S^{(n)}$ sont totalement ramifiées, on a

$$|S^{(n)}| = |S^{(n-1)}| = r^{[(n-1)/2]} = r^{[n/2]}$$

Pour n pair, on vérifie que $|S_2| = r$. Pour $n \geqslant 4$, il nous faut d'abord calculer le cardinal de $S_i^{(n)}$, par récurrence : $|S_0^{(n)}| = r - 1$ par le point *(iii)* du théorème 3.43. Ensuite, chaque place $P \in S_{i-1}^{n-1}$ possède r places au-dessus d'elle par le point *(i)* de la proposition précédente : ainsi, $|S_i^n| = r^i(r-1)$ et

$$|S^{(n)}| = |S^{(n-1)}| + r|S_{\frac{n-4}{2}}^{(n-1)}| = r^{n/2-1} + r(r-1)r^{n/2-2} = r^{n/2} = r^{[n/2]}.$$

Proposition 3.47. *Le genre de* $\mathcal{F}_n$ *est donné par les formules*

$$g_n = \begin{cases} r^n + r^{n-1} - r^{\frac{n+1}{2}} - 2r^{\frac{n-1}{2}} + 1 & \text{si } n \text{ est pair.} \\ r^n + r^{n-1} - \frac{1}{2}r^{\frac{n}{2}+1} - \frac{3}{2}r^{\frac{n}{2}} - r^{\frac{n}{2}-1} + 1 & \text{si } n \text{ est impair.} \end{cases}$$

Démonstration. En effet, pour $n \leqslant 2$ on a $g_1 = 0$ et $g_2 = \frac{1}{2}r(r-1)$ comme on l'a vu dans l'exemple 3.34. Ensuite, il s'agit d'une simple récurrence en utilisant la formule d'Hurwitz $2g_{n+1} - 2 = r(2g_n - 2) + r^{[n/2]}(r-1)(r+2)$. □

Dans les deux cas, on retient que $g_n \leqslant r^n + r^{n-1}$.

Le nombre de points rationnels de $\mathcal{X}_n$. Afin de montrer que cette suite de corps de fonctions rationnelles (et donc de courbes) définit une *excellente famille de codes*, il nous faut minorer le nombre de places rationnelles. En fait, en revenant au langage des courbes, il nous faut calculer le nombre de points rationnels sur $\mathcal{X}_n$.

En fait, on a déjà fait la plus grande partie du travail dans l'exemple 3.34. En effet, il existe un changement de variables linéaire inversible qui transforme l'équation $U^{r+1} + V^{r+1} + W^{r+1} = 0$ en $X^{r+1} = Y^r Z + Y Z^r$:

$$\begin{pmatrix} 0 & 0 & 1 \\ b + ab & -a & 0 \\ b & -1 & 0 \end{pmatrix}$$

où $a, b \in \mathbb{F}_q$ vérifient $b^{r+1} + 1 = a^r + a + 1 = 0$. On rappelle que l'on note $F(X,Z) = X^{r+1} - Z^r - Z$. Ce polynôme vérifie la propriété que pour tout $x \in \mathbb{F}_q^*$, il existe r solutions différentes dans $\mathbb{F}_q$ à l'équation en z, $F(x,z) = 0$. En effet, le polynôme en z est séparable et si $z \in \overline{\mathbb{F}}_q$ est une racine, alors, $z^{r^2} + z^r = x^{(r+1)r} = x^{r+1} = z^r + z$ et donc $z \in \mathbb{F}_q$.

Par récurrence, on en déduit facilement que la courbe $\mathcal{X}_n$ possède au moins $(q-1)r^{n-1}$ points rationnels (qui ne sont pas à l'infini). On en déduit alors que

$$\frac{N_q(g_n)}{g_n} \geqslant \frac{(q-1)r^{n-1}}{r^n + r^{n-1}} = \frac{q-1}{r+1} = \sqrt{q} - 1,$$

ce qui montre le résultat annoncé : $A(q) \geqslant \sqrt{q} - 1$.

3.3.3 Estimations de $N_q(g)$.

Commençons par présenter les premiers résultats obtenus par Serre ([Ser84]). Tout d'abord, dans le cas où q n'est pas un carré, Serre améliore la borne de Weil :

Proposition 3.48 (Serre). *Soit $\mathcal{X}$ une courbe projective lisse absolument irréductible. Soit g son genre. Alors, son nombre de points rationnels sur $\mathbb{F}_q$ vérifie*

$$\big||\mathcal{X}(\mathbb{F}_q)| - (q+1)\big| \leqslant g[2\sqrt{q}],$$

où $[x]$ dénote la partie entière de x.

La démonstration de ce théorème fait intervenir les célèbres *conjectures de Weil* que l'on ne saurait passer sous silence dans la recherche du nombre de points rationnels sur les corps finis. On continue à les appeler *conjectures* bien qu'elles aient été démontrées en 1973 grâce aux travaux de Dwork, Grothendieck puis Deligne.

Théorème 3.49 (Conjectures de Weil). *Soit $\mathcal{X}$ une courbe définie sur $\mathbb{F}_q$, lisse, complètement irréductible et de genre g. Alors, si l'on note $|\mathcal{X}(\mathbb{F}_{q^n})|$ le nombre de points rationnels de $\mathcal{X}$ sur $\mathbb{F}_{q^n}$, la fonction zêta de $\mathcal{X}$ définie par*

$$Z_{\mathcal{X}}(T) \stackrel{\text{def}}{=} \exp\left(\sum_{n=1}^{\infty} |\mathcal{X}(\mathbb{F}_{q^n})| \frac{T^n}{n}\right),$$

est une fraction rationnelle à coefficients entiers. Plus précisément, il existe un polynôme $P_{\mathcal{X}}(T)$ de degré $2g$ à coefficients entiers et de terme constant 1 tel que

$$Z_{\mathcal{X}}(T) = \frac{P_{\mathcal{X}}(T)}{(1-T)(1-qT)}.$$

Enfin, si l'on note $P_X(T) = \prod(1-\omega_j T)(1-\overline{\omega}_j T)$ alors, $|\omega_j| = \sqrt{q}$.

En particulier, comme $|\mathcal{X}(\mathbb{F}_q)|$ est donné par la valeur en 0 de la dérivée logarithmique de $Z_{\mathcal{X}}$, on calcule

$$\frac{Z'_{\mathcal{X}}(T)}{Z_X(T)} = \frac{1}{1-T} + \frac{q}{1-qT} - \sum_{j=1}^{g}\left(\frac{\omega_j}{1-\omega_j T} + \frac{\overline{\omega}_j}{1-\overline{\omega}_j T}\right), \qquad (\diamondsuit)$$

ce qui donne $|\mathcal{X}(\mathbb{F}_q)| = q+1-\sum(\omega_j+\overline{\omega}_j)$. Ceci entraîne, avec la dernière assertion du théorème ci-dessus, la borne de Hasse–Weil (3.36). Néanmoins, Serre donne un résultat plus précis grâce au lemme suivant. Le théorème 3.48 en découlera immédiatement.

Lemme 3.50 (Serre, 1983). *Soient $P(T)$ un polynôme à coefficients entiers de degré n de la forme $\prod(1-\alpha_j T)(1-\overline{\alpha}_j T)$ tel que $|\alpha_j| = \sqrt{q}$. Alors, on a*

$$\left|\sum_{j=1}^{n}(\alpha_j + \overline{\alpha}_j)\right| \leqslant n[2\sqrt{q}].$$

Démonstration. Pour cela, on pose $x_j = [2\sqrt{q}] + 1 + \alpha_j + \overline{\alpha}_j$ et on considère le produit $\prod_{j=1}^{n} x_j$. C'est une expression symétrique en les racines du polynôme unitaire $T^{2n}P(1/T) \in \mathbb{Z}[T]$: c'est donc un entier relatif. Il est strictement positif car $x_j \geqslant [2\sqrt{q}] + 1 - 2\sqrt{q} > 0$. Dès lors, l'inégalité arithmético-géométrique nous donne

$$\frac{1}{n}\sum_{j=1}^{n} x_j \geqslant \left(\prod_{j=1}^{n} x_j\right)^n \geqslant 1,$$

et ainsi $\sum x_j \geqslant n$ ou encore $\sum(\alpha_j + \overline{\alpha}_j) \geqslant -n[2\sqrt{q}]$. On conclut en faisant le même travail avec $y_j = [2\sqrt{q}] + 1 - \alpha_j - \overline{\alpha}_j$, ce qui nous permet d'obtenir $\sum(\alpha_j + \overline{\alpha}_j) \leqslant n[2\sqrt{q}]$. □

Les genres 1 et 2. On appellera l'inégalité de la proposition 3.48, la borne de Weil–Serre. Celle-ci est presque optimale en petit genre. En effet, on a un théorème de Hasse et Deuring :

Théorème 3.51. *Soit $q = p^n$ et $m = [2\sqrt{q}]$. Alors,*

$$N_q(1) = q + 1 + m$$

sauf si $m \equiv 0 \mod p$, $n \geqslant 3$ et n est impair. Sous ces conditions, $N_q(1) = q + m$.

Le cas $g = 2$ est un peu plus délicat. Avec Serre, on note $m = [2\sqrt{q}]$ et on dit que $q = p^n$ avec n impair est *spécial* s'il vérifie l'une des conditions suivantes :

(i) $m \equiv 0 \mod p$.

(ii) il existe $x \in \mathbb{Z}$ tel que $q = x^2 + 1$.

(iii) il existe $x \in \mathbb{Z}$ tel que $q = x^2 + x + 1$.

(iv) il existe $x \in \mathbb{Z}$ tel que $q = x^2 + x + 2$.

On verra un peu plus loin une explication à ces trois dernières conditions un peu mystérieuses.

Théorème 3.52. *On a $N_4(2) = 10$, $N_9(2) = 20$. Sinon, si q n'est pas spécial alors,*

$$N_q(2) = q + 1 + 2m.$$

Si q est spécial alors,

$$N_q(2) = \begin{cases} q + 2m & \text{si } \{m\} > \frac{\sqrt{5}-1}{2}, \\ q + 2m - 1 & \text{sinon,} \end{cases}$$

où l'on a noté $\{x\} = x - [x]$ la partie fractionnaire de x.

Formule explicite de Serre. Avant de passer au genre 3, voyons un raffinement de la borne de Weil–Serre. Cette amélioration permet notamment à Serre, dans [Ser84], de trouver de très bonnes bornes supérieures pour les valeurs de $N_2(g)$. Par ailleurs, on verra comment on peut en déduire une démonstration théorème de Drinfeld–Vlăduţ que l'on a vu dans la section sur les *excellents* codes. On commence par considérer un polynôme trigonométrique pair de coefficient constant 1,

$$f(\theta) = 1 + 2\sum_{n \geqslant 1} a_n \cos(n\theta),$$

pour des coefficients réels a_n, nuls à partir d'un certain rang. On note ensuite α_d le nombre de points de $\mathcal{X}$ de degré d de telle sorte que

$$\sum_{d|n} d\alpha_d = |\mathcal{X}(\mathbb{F}_{q^n})|.$$

Enfin, écrivons $\psi_d(t) = \sum_{n \geqslant 1} a_{dn} t^{dn}$ et notons θ_j un réel vérifiant $\omega_j = \sqrt{q} e^{i\theta_j}$ où ω_j est défini en 3.49.

Proposition 3.53 (Formule explicite de Weil–Serre)**.** *On a la relation*

$$\sum_{j=1}^{g} f(\theta_j) + \sum_{d \geqslant 1} d\alpha_d \psi_d(1/\sqrt{q}) = g + \psi_1(\sqrt{q}) + \psi_1(1/\sqrt{q}).$$

Démonstration. Tout d'abord, en dérivant successivement ($\diamondsuit$), on obtient la formule bien connue :

$$|\mathcal{X}(\mathbb{F}_{q^n})| = q^n + 1 - \sum_{j=1}^{g} (\omega_j^n + \overline{\omega}_j^n).$$

On inverse l'ordre de sommation dans la deuxième somme du membre de gauche (les sommes sont finies) :

$$\begin{aligned}\sum_{d\geqslant 1} d\alpha_d \psi_d(1/\sqrt{q}) &= \sum_{n\geqslant 1}\left(\sum_{d|n} d\alpha_d\right) c_n(\sqrt{q})^{-n} = \sum_{n\geqslant 1} c_n|\mathcal{X}(\mathbb{F}_{q^n})|(\sqrt{q})^{-n}\\ &= \sum_{n\geqslant 1} c_n\left((\sqrt{q})^n + (\sqrt{q})^{-n} - \sum_{j=1}^{g}(e^{i\theta_j}+e^{-i\theta_j})\right)\\ &= \psi_1(\sqrt{q}) + \psi_1(1/\sqrt{q}) + g - \sum_{j=1}^{g} f(\theta_j),\end{aligned}$$

ce qui est la formule annoncée. □

Ensuite, Serre considère le cas particulier où les coefficients a_n sont choisis positifs et où f vérifie $f(\theta)\geqslant 0$ pour tout $\theta\in\mathbb{R}$. Alors, on a pour tout entier $k\geqslant 1$,

$$(|\mathcal{X}(\mathbb{F}_q)|-1)\psi_1(1/\sqrt{q}) + \sum_{d=2}^{k} d\alpha_d\psi_d(1/\sqrt{q}) \leqslant g + \psi_1(\sqrt{q}),$$

qui donne en particulier, pour $k=1$,

$$|\mathcal{X}(\mathbb{F}_q)| \leqslant ag+b$$

pour des constantes $a = 1/\psi_1(1/\sqrt{q})$ et $b = 1+\psi_1(\sqrt{q})/\psi_1(1/\sqrt{q})$ dépendantes uniquement de q et f. On retrouve par exemple la borne de Weil avec la fonction $f(\theta)=1+\cos\theta$.

Venons-en maintenant à l'application au théorème de Drinfeld–Vlăduţ. La dernière inégalité nous donne, en passant au sup à gauche,

$$\frac{N_q(g)}{g} \leqslant a + \frac{b}{g}.$$

En prenant la limite supérieure pour g tendant vers l'infini, on obtient $A(q)\leqslant a$. Comme on a maintenant tout choix sur f, du moment que $f\geqslant 0$ et $a_n\geqslant 0$, on peut arriver à une bonne majoration. Pour cela, l'idée est d'utiliser une suite de fonctions, g_k, 2π périodiques qui converge vers le "pic de Dirac". Elles sont représentées par la figure ci-contre et leur développement en séries de Fourier est

$$g_k(\theta) = 1 + 2\sum_{n=1}^{\infty} \frac{2k(k-1)\left(1-\cos\left(\frac{n\pi}{k}\right)\right)}{\pi^2 n^2}\cos(n\theta).$$

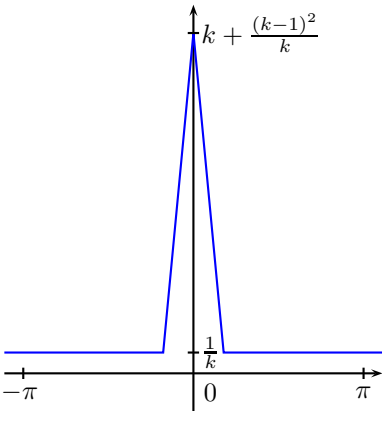


FIGURE 6: La fonction g_k complétée par 2π–periodicité.

On a $g_k\geqslant \frac{1}{k}$ et à k fixé, ses coefficients sont de l'ordre $O(\frac{1}{n^2})$: ainsi, on peut tronquer la série ci-dessus (tout en imposant de conserver au moins, disons, k termes) pour obtenir un polynôme trigonométrique $f_k\geqslant 0$. De plus, son coefficient constant est bien 1 et les autres sont positifs. Notons $\psi_1^{(k)}$ la fonction ψ_1 (définie un peu plus haut) associée à f_k. Si on fixe maintenant un entier M, alors, pour k assez grand, on aura

$$\psi_1^{(k)}(\sqrt{q}) \geqslant \sum_{n=1}^{M} \frac{2k(k-1)(1-\cos\left(\frac{n\pi}{k}\right))}{\pi^2 n^2}(\sqrt{q})^{-n},$$

et comme chacun des coefficients tend vers 1 quand $k\to\infty$, on en déduit que

$$A(q) \leqslant \frac{1}{\sum_{n=1}^{M}(\sqrt{q})^{-n}}$$

Ceci étant vrai pour tout entier M, on le fait tendre vers l'infini et on obtient $A(q)\leqslant \sqrt{q}-1$, ce qui constitue une preuve du théorème de Drinfeld–Vlăduţ (3.37), utilisant néanmoins les conjectures de Weil !

Le genre 3. Le cas $g = 3$ est bien plus compliqué et est toujours l'objet de recherches à l'heure actuelle. Un problème très naturel qui apparaît dans les cas $g = 2, 3$, est de savoir s'il existe une constante dépendante de g telle que pour tout q,

$$q + 1 + 2m - N_q(g) \leqslant C(g).$$

Par exemple, les deux théorèmes 3.51 et 3.52 nous donnent $C(1) = 2$ et $C(2) = 1 + \sqrt{5}$, mais on ne sait pas montrer l'existence d'une telle constante en genre 3 et encore moins en genre quelconque ! Voyons, sans rentrer dans tous les détails, ce que l'on peut dire du genre 3. On pourra notamment consulter [LR07] et [Lau02]. Le principal résultat général en genre 3 qui tente de répondre à la question précédente est le théorème suivant énoncé par Lauter :

Théorème 3.54. *Il existe une courbe (projective, lisse et absolument irréductible) de genre* 3 *sur* $\mathbb{F}_q$ *telle que*

$$\big||\mathcal{X}(\mathbb{F}_q)| - (q+1)\big| \geqslant 3m - 3,$$

où $m = [2\sqrt{q}]$.

Cela répondrait presque à la question de l'existence de $C(3)$, mais le problème est que l'on ne sait pas si la courbe donnée par ce théorème a le nombre maximal ou minimal de points ! A la différence des courbes elliptiques (ou hyperelliptiques), on ne peut résoudre cette complication seulement avec une tordue quadratique.

Pour arriver à ce théorème, on commence par prendre une courbe elliptique E qui possède le nombre maximal de points sur le corps $\mathbb{F}_q$. On considère ensuite naturellement la variété abélienne $E \times E \times E$ qui possède beaucoup de points rationnels.

Un exemple très important de variété abélienne est la jacobienne d'une courbe algébrique : si on a une courbe de genre g, sa jacobienne est une variété abélienne de dimension g. Ici , pour $g = 3$, c'est d'autant plus naturel que ce sont principalement les "seules" variétés abéliennes. En effet, une variété abélienne de dimension 3 est donnée par sa matrice des périodes, matrice symétrique 3×3 définie positive : c'est un ouvert (algébrique) de dimension 6. Une courbe lisse de genre 3, est donnée par une quartique projective plane, elle-même définie par $\binom{6}{2} = 15$ monômes de degré 4 en trois variables : en quotientant par le groupe linéaire de dimension 9, on obtient aussi 6 comme dimension.

Supposons maintenant que l'on ait une variété abélienne $A \simeq \mathrm{Jac}(C)$. Alors, les valeurs propres $(\omega_1, \overline{\omega}_1, \ldots, \omega_3, \overline{\omega}_3)$ du Frobenius sur A sont les mêmes sur $\mathrm{Jac}(C)$ et le nombre de points de C est donné par $q + 1 + \operatorname{tr} \mathrm{Fr}_A = q + 1 + \sum(\omega_i + \overline{\omega}_i)$. En effet le numérateur le la fonction zêta de C n'est autre que $x^6 P_\pi(1/x)$ où P_π est le polynôme caractéristique du Frobenius agissant sur $\mathrm{Jac}(C)$.

Malheureusement, ce n'est pas aussi simple que cela. En effet, même si on a vu que les variétés abéliennes de dimension 3 et les jacobiennes de courbes lisses de genre 3 ont même dimension, cela ne veut pas dire qu'une variété abélienne est nécessairement une jacobienne. Par exemple, en caractéristique nulle, on peut mentionner un théorème dû à Igusa pour la première partie et Klein pour la seconde.

Théorème 3.55. *Soient* $K \subset \mathbb{C}$ *et* A_τ *une variété abélienne définie par une matrice de Riemman*[†] τ. *Il existe une forme modulaire*[‡] χ_{18} *de poids* 18 *ainsi qu'une fonction* Σ_{140} *telles que*

(i) A_τ *est décomposable si* $\chi_{18}(\tau) = \Sigma_{240}(\tau) = 0$.

(ii) A_τ *est la jacobienne d'une courbe hyperelliptique si* $\chi_{18}(\tau) = 0$ *et* $\Sigma_{240}(\tau) \neq 0$.

(iii) A_τ *est la jacobienne d'une courbe non hyperelliptique si* $\chi_{18}(\tau) \neq 0$

De plus, si $A_\tau \simeq \mathrm{Jac}(C)$ *où* C *est une quartique d'équation* Q *alors,*

$$\chi_{18}(\tau) = (2\pi)^{-54} \operatorname{Disc}(Q)^2,$$

où $\operatorname{Disc}(Q)$ *est le résultant multivarié* $\operatorname{Res}(Q_X, Q_Y, Q_Z)$ *des trois dérivées partielles de* Q.

†. La variété abélienne est définie par une matrice des périodes $[\Omega_1, \Omega_2]$ et la matrice de Riemmann associée est $\tau = \Omega_2^{-1}\Omega_1$.

‡. Sur le demi-plan de Siegel $\mathscr{H}_g$ des matrices symétriques de partie imaginaire définie positive.

Ainsi, déjà en caractéristique nulle, on a des problèmes : la variété abélienne $E \times E \times E$ est loin d'être indécomposable comme il le faudrait dans les cas *(ii)* et *(iii)*. L'idée pour s'en sortir est de considérer une variété abélienne *isogène* à $E \times E \times E$ mais qui sera indécomposable. Néanmoins dans ce cas, la dernière affirmation du théorème ci-dessus indique que la courbe C trouvée sera définie sur les corps K seulement si† $\left(\frac{\pi}{2}\right)^{54} \chi_{18}(\tau)$ est un carré dans K.

Revenons à la caractéristique positive, ce qui est un peu plus délicat mais soulève les mêmes problèmes, à savoir l'indécomposabilité des jacobiennes et la définition sur le corps de base de la courbe dont la jacobienne sera isogène à $E \times E \times E$. Avant d'énoncer un théorème dû à Serre, introduisons quelques notions.

On fixe un entier a premier avec la caractéristique p du corps $\mathbb{F}_q$ et tel que $d = a^2 - 4q$ soit négatif : ce sera le discriminant de l'équation caractéristique du Frobenius d'une courbe elliptique E dont la trace est a. Avec le théorème 3.51 on peut prendre $a = -m$ où $-m + 1$. On pose $R = \mathbb{Z}[X]/(X^2 - aX + q)$ qui est un ordre (engendré par le Frobenius) dans le corps quadratique imaginaire $\mathbb{Q}(\sqrt{d})$. En fait, on va supposer que c'est l'ordre maximal, c'est-à-dire l'anneau des entiers. (Cette restriction ne pose pas de problèmes trop importants, comme on pourra le voir dans [Lau02]). On note $\mathrm{Ab}(a, q)$ la catégorie des variétés abéliennes isogènes sur $\mathbb{F}_q$ à un produit de copies de E et $\mathrm{Mod}(R)$ la catégorie des R–modules sans torsion de type fini. Par exemple, $\mathrm{Hom}(E, A)$ est un objet de cette catégorie.

Proposition 3.56. *Le foncteur $T : \mathrm{Ab}(a, q) \to \mathrm{Mod}(R)$, défini par $T(A) = \mathrm{Hom}(E, A)$, est une équivalence de catégorie. Le foncteur S inverse de T est donné par la variété abélienne $S(L) = L \otimes_R E$ que l'on abrègera en A_L.*

Munir A_L d'une polarisation revient exactement à faire de L un R–module hermitien et on peut énoncer le théorème suivant :

Théorème 3.57 (Serre)**.** *Une variété abélienne A_L principalement polarisée est indécomposable si et seulement si L est indécomposable comme module hermitien (de discriminant 1).*

Ainsi, pour obtenir une variété abélienne A indécomposable, isogène sur $\mathbb{F}_q$ à $E \times E \times E$, il faut et il suffit qu'il existe un R–module hermitien indécomposable. Notons que le fait que A soit seulement isogène à $E \times E \times E$ n'a pas d'influence sur le nombre de points : l'isogénie étant définie sur $\mathbb{F}_q$, elle commute avec les Frobenius et les polynômes caractéristiques sont les mêmes.

Un théorème, énoncé par Hoffmann, règle le cas des modules hermitens indécomposables en dimension 2 et 3 :

Théorème 3.58. *On rappelle que d est le discriminant de l'anneau R. Alors, il n'existe aucun R–module hermitien indécomposable de discriminant 1 si*

(i) on est en dimension 2 et si $d = -3, -4$ ou -7.

(ii) on est en dimension 3 et si $d = -3, -4, -8$ ou -11.

De plus, pour toutes les autres valeurs, il existe de tels modules indécomposables.

Cela ne pose donc pas tant de problèmes car il nous "suffit" de faire une étude de quelques cas particuliers. Par exemple, en dimension 2, on peut vérifier que ces cas correspondent exactement, outre le cas $m \equiv 0 \mod p$, aux discriminants qui apparaissent dans les cas *spéciaux* du théorème 3.52. En dimension 3, c'est ce qui explique, dans le théorème 3.54, le défaut de 3 par rapport à la borne de Weil–Serre.

Le problème vient du lien entre variétés abéliennes indécomposables et jacobiennes de courbes. L'existence ne pose pas trop de soucis, les complications viennent du fait que la courbe obtenue n'est pas forcément définie sur $\mathbb{F}_q$ mais sur sa clôture. Plus précisément, un théorème de Torelli permet de montrer le résultat suivant.

Théorème 3.59. *Soit L un R–module hermitien indécomposable de rang 3. Alors, il existe une courbe C définie sur $\mathbb{F}_q$ telle que $\mathrm{Jac}(C)$ est isomorphe sur $\mathbb{F}_q$ à A_L **ou** à sa tordue quadratique. De plus, si C n'est pas hyperelliptique, les deux cas s'excluent.*

On trouve ainsi une courbe de genre 3 dont le nombre de points rationnels sur $\mathbb{F}_q$ est soit $q + 1 + 3m$ soit $q + 1 - 3m$, ce qui, avec une étude détaillée des cas du théorème 3.58 en genre 3, conduit à une preuve du théorème 3.54.

†. En fait, on a équivalence, voir [LR07].

Bibliographie

[BP05] N. Brisebarre & G. Philibert – « Effective lower and upper bounds for the fourier coefficients of powers of the modular invariant j », *Journal of the Ramanujan Mathematical Society* **20** (2005), no. 4, p. 255–282.

[BSMS06] A. Bostan, B. Salvy, F. Morain & E. Schost – « Fast algorithms for computing isogenies between elliptic curves », `http://arxiv.org/abs/cs/0609020v1`, 2006.

[CF06] H. Cohen & G. Frey – *Handbook of elliptic and hyperelliptic curve cryptography*, Chapman & Hall/CRC, 2006.

[Coh00] H. Cohen – *A course in computational algebraic number theory*, GTM 138, Springer, 2000.

[Cox89] D. H. Cox – *Primes of the form $x^2 + ny^2$*, Wiley-Interscience, 1989.

[Ful89] W. Fulton – *Algebraic curves : an introduction to algebraic geometry*, Addison Wesley, 1989.

[GG03] J. Gathen & J. Gerhard – *Modern computer algebra*, Cambridge University Press, 2003.

[Lac85] G. Lachaud – « Les codes géométriques de Goppa », *Séminaire N. Bourbaki* (1984–1985), no. 641, p. 189–207.

[Lan87] S. Lang – *Elliptic functions*, GTM 112, Springer, 1987.

[Lau02] K. Lauter – « The maximum or minimum number of rational points on genus three curves over finite fields », avec un appendice de J.-P. Serre, *Compositio Mathematica* **134** (2002), p. 87–111.

[LBR88] D. Le Brigand & J. J. Risler – « Algorithme de Brill-Noether et codes de Goppa », *Bulletin de la S.M.F.* **116** (1988), no. 2, p. 231–253.

[LR07] G. Lachaud & C. Ritzenthaler – « On a conjecture of Serre on abelian threefolds », `http://arxiv.org/abs/0710.3303v1`, 2007.

[Mil90] J. S. Milne – « Modular functions and modular forms », `http://www.jmilne.org/math/CourseNotes/math678.pdf`, 1990.

[Mor95] F. Morain – « Calcul du nombre de points sur une courbe elliptique dans un corps fini : aspects algorithmiques », *Journal de la théorie des nombres de Bordeaux* **7** (1995), p. 255–287.

[Nit95] A. Nitaj – « L'algorithme de Cornacchia », *Expositiones Mathematicae* **13** (1995), p. 358–365.

[Sch85] R. Schoof – « Elliptic curves over finite fields and the computation of square roots mod p », *Mathematics of Computation* **44** (1985), no. 170, p. 483–494.

[Sch95] — , « Counting points on elliptic curves over finite fields », *Journal de la théorie des nombres de Bordeaux* **7** (1995), p. 219–254.

[Ser59] J.-P. Serre – *Groupes algébriques et corps de classes*, Hermann Paris, 1959.

[Ser70] — , *Cours d'arithmétique*, Presses Universitaires de France, 1970.

[Ser84] — , « Nombres de points des courbes algébriques sur $\mathbb{F}_q$ », in *Oeuvres – Collected papers*, vol. 3, Springer, 1972–1984, p. 664–668.

[SG95] H. Stichtenoth & A. Garcia – « A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vlăduţ bound », *Inventiones mathematicae* **121** (1995), p. 211–222.

[Sha73] D. Shanks – « Five number-theoretic algorithms », *Proceedings of the Second Manitoba Conference on Numerical Mathematics* (1973), no. VII, p. 51–70.

[Sho97] V. Shoup – « Lower bounds for discrete logarithms and related problems », *Lecture Notes in Computer Science* **1233** (1997), p. 256–266.

[Sil86] J. H. Silverman – *The arithmetic of elliptic curves*, GTM 106, Springer, 1986.

[Sil95] — , *Advanced topics in the arithmetic of elliptic curves*, GTM 151, Springer, 1995.

[Sti09] H. Stichtenoth – *Algebraic function fields and codes*, GTM 254, Springer, 2009.

[vL82] J. H. van Lint – *Introduction to coding theory*, GTM 86, Springer, 1982.

[Vél71] J. Vélu – « Isogénie entre courbes elliptiques », *Comptes-Rendus de l'Académie des Sciences, Série I* **273** (1971), p. 238–241.

Expose de maitrise
Factorisation dans $\mathbb{Z}[X]$

Abuaf Roland
Boyer Ivan

Sujet proposé par François Loeser

20 juin 2007

Table des matières

1 Précisions sur la complexité

Définition 1.1 *Un algorithme sur les entiers sera dit* polynomial en la taille des données *si le nombre d'opérations arithmétiques élémentaires est dominé par un polynôme en le logarithme du plus grand entier des données.*

Cette définition est raisonnable car un entier n est codé en base 2 et occupe donc un espace de $\log_2(n)$ en mémoire.

La majeure partie de cet exposé s'attache à montrer que le problème de la factorisation des polynômes à coefficients entiers est dans la classe **P**, c'est-à-dire qu'il existe un algorithme qui résout ce problème en temps polynomial (par rapport aux entiers des coefficients et au degré du polynôme)

Il ne s'agit pas de l'algorithme le plus efficace dans les cas courants et c'est pourquoi nous nous attacherons principalement au caractère polynomial de la complexité et non pas à l'optimalité.

2 Algorithme de Berlekamp

2.1 Lemme de Berlekamp

Dans cette section, nous allons considérer un algorithme de factorisation des polynômes à coefficients entiers dans les corps finis, celui de Berlekamp. C'est certainement la méthode la plus connue pour les corps finis car son implémentation est relativement aisée et son coût est polynomial en le degré du polynôme.

Plus précisément, il s'agit d'un algorithme de factorisation de polynômes sans facteurs carrés, dans $\mathbb{F}_p[X]$, pour p premier. En fait, l'idée générale marche pour tous les corps finis, mais les calculs de base (addition, multiplication, inverse) sont plus faciles dans $\mathbb{F}_p$.

Nous allons rappeler deux lemmes d'algèbre élémentaire, qui nous permettront d'établir le principe fondamental de l'algorithme. Dans la suite, on notera p un nombre premier.

Proposition 2.1.1 (Lemme Chinois) *Soit A un anneau principal et $x \in A$ avec $x = \prod_{i=1}^{k} p_i^{\alpha_i}$ sa décomposition en produit d'irréductibles, alors on a l'isomorphisme suivant :*

$$\begin{array}{ccc} A/(x) & \xrightarrow{\sim} & \prod_{i=1}^{k} A/(p_i^{\alpha_i}) \\ \overline{a}^x & \longmapsto & \left(\overline{a}^{p_1^{\alpha_1}}, \ldots, \overline{a}^{p_k^{\alpha_k}}\right). \end{array}$$

Proposition 2.1.2 (Lemme de Rupture) *Si f est un polynôme irréductible sur $\mathbb{F}_p$ alors le quotient $\mathbb{F}_p[X]/(f)$ est une extension finie de corps de $\mathbb{F}_p$ dans laquelle f admet une racine. On l'appelle corps de rupture de f sur $\mathbb{F}_p$.*

On en déduit le résultat suivant :

Soit f un polynôme à coefficients entiers sans facteurs carrés, alors $\mathbb{F}_p[X]/(f)$ est isomorphe à un produit direct de corps finis.

C'est une conséquence évidente des lemmes qui précèdent. Notons que l'isomorphisme chinois est un isomorphisme d'algèbre. Nous allons maintenant énoncer et démontrer le lemme de Berlekamp qui donne une expression intéressante du polynôme à factoriser.

Proposition 2.1.3 (Lemme de Berlekamp) *Soit f un polynôme sur $\mathbb{F}_p$ sans facteurs carrés, on note A l'algèbre $\mathbb{F}_p[X]/(f)$ et S l'endomorphisme de A comme espace vectoriel sur $\mathbb{F}_p$:*

$$\begin{array}{c} S : A \to A \\ a \mapsto a^p - a. \end{array}$$

Si $t \in \ker S$ alors on a l'égalité suivante :

$$f = \prod_{\alpha \in \mathbb{F}_p} \text{pgcd}(f, t - \alpha).$$

Preuve :
► On peut supposer $f \neq 0$. Grâce à l'isomorphisme chinois, on va pouvoir travailler sur le produit de corps pour déterminer le noyau de S. En effet si $t \in \ker S$ alors chaque composante t_i de t (vu comme vecteur du produit de corps) vérifie l'équation $t_i^p - t_i = 0$ dans une extension de $\mathbb{F}_p$. Or par définition même de $\mathbb{F}_p$, cela signifie que $t_i \in \mathbb{F}_p$. Dès lors, dans l'algèbre produit, $\ker S$ est le produit des $\mathbb{F}_p$.

Ainsi si on pose $f = \prod f_i$ où les f_i sont irréductibles sur $\mathbb{F}_p$ et tous distincts (décomposition sans facteurs carrés), $t - \alpha$ a pour $i^{\text{ème}}$ composante $t_i - \alpha$ dans l'algèbre produit. Donc si $\alpha = t_i$ alors $t - \alpha$ est divisible par f_i. Ceci prouve que f divise $\prod_{\alpha \in \mathbb{F}_p} \text{pgcd}(f, t - \alpha)$.

D'un autre côté une écriture de Bézout montre immédiatement que les $t - \alpha,\ \alpha \in \mathbb{F}_p$ sont deux à deux premiers entre eux. Ainsi les $\text{pgcd}(f, t - \alpha),\ \alpha \in \mathbb{F}_p$ sont deux à deux premiers entre eux et divisent f et donc $\prod_{\alpha \in \mathbb{F}_p} \text{pgcd}(f, t - \alpha)$ divise f. ◄

Notons que nous avons confondu t et un de ses représentants dans A (disons qu'à chaque fois que l'on écrivait $\text{pgcd}(f, t - \alpha)$, on évoquait un représentant de t). Le fait que t soit de degré strictement inférieur à f montre que, si on peut trouver t de degré supérieur à un, alors l'un des pgcd au moins sera un diviseur de f distinct de f et de degré supérieur à un.

2.2 Noyau de Berlekamp

La question se pose maintenant de savoir si l'on peut trouver un élément du noyau de S qui ne soit pas une constante. La démonstration du lemme de Berlekamp fait apparaître un résultat dans cette direction :

Porisme 2.2.1 *Si $f = f_1 \dots f_r$ est la décomposition sans facteurs carrés de f, alors la dimension de $\ker S$ comme $\mathbb{F}_p$ espace vectoriel est r.*

Ce résultat est important car il permet théoriquement de montrer que si f n'est pas irréductible, alors on peut trouver un polynôme non constant dans $\ker S$, et il donne pratiquement un critère de terminaison de l'algorithme.

Le calcul de l'endomorphisme S se fait via l'estimation des congruences suivantes :

$$x^{ip} - x^i \equiv \sum_{j=0}^{\deg f - 1} s_{ij} x^j \mod f,\ 0 \leq i \leq \deg f - 1$$

et donc si on représente un élément $t \in A$ par un vecteur colonne donnant ses coefficients dans la base $(1, x \dots x^{\deg f - 1})$, la relation $St = 0$ permet de trouver les éléments du noyau par résolution d'un système linéaire. (Les indéterminées étant bien sûr les composantes de t)

2.3 Coût de l'algorithme

Venons-en maintenant au coût de l'algorithme de Berlekamp. Trois étapes importantes interviennent pour trouver un facteur non constant ou prouver l'irréductibilité.

Tout d'abord, rappelons les coûts des opérations « élémentaires » :

Proposition 2.3.1 *Soient $f, g \in \mathbb{Z}[X]$, avec g unitaire.*

La division euclidienne de f par g peut se calculer en $O(\deg g \times (\deg f - \deg g + 1))$ opérations élémentaires.

Le pgcd *de f et g se calcule en $O(\deg f \times \deg g)$ opérations élémentaires.*

Preuve :
► L'algorithme de division euclidienne est très simple : il consiste à retirer à f un polynôme de la forme $cX^i g$ afin de faire disparaître le terme de degré le plus haut de f. Ceci coûte $O(\deg g)$ opérations. On recommence autant de fois que nécessaire mais au plus $\deg f - \deg g + 1$ fois.

Pour le calcul du pgcd, on déroule l'algorithme d'Euclide : en supposant $\deg f \geqslant \deg g$, on effectue la division euclidienne $f = ug + r_0$ et on recommence avec g et r_0. D'où une complexité de l'ordre de :

$$\begin{aligned}
&C\left(\deg g(\deg f - \deg g + 1) + \deg r_0(\deg g - \deg r_0 + 1) + \sum \deg r_i(\deg r_{i-1} - \deg r_i + 1)\right)\\
=&C\left(\deg f \deg g - \deg g(\deg g - \deg r) - \sum \deg r_i(\deg r_{i-1} - \deg r_i) + \deg g + \sum \deg r_i\right)\\
\leqslant&C\left(\deg f \deg g + (\deg g)^2\right) \leqslant 2C \deg f \deg g.
\end{aligned}$$

◄

Remarquons que les opérations dans $\mathbb{F}_p$ sont faciles, d'une complexité au plus $(\log p)^2$, ce que l'on assimilera à une constante pour la suite †.

L'algorithme de Berlekamp résulte de la combinaison des trois étapes :
– le calcul de l'endomorphisme S
– la résolution du système linéaire $St = 0$
– les calculs des $\text{pgcd}(Q, t - \alpha),\ \alpha \in \mathbb{F}_p$.

Dans la suite, on notera n le degré du polynôme Q. La première étape consiste essentiellement en n divisions euclidiennes de polynômes dont le degré est majoré par np : elle se fait donc en $O(n \times (n(np - n))=O(pn^3)$.

La deuxième est un pivot de Gauss sur un système de taille n, cela se fait donc en $O(n^3)$.

Enfin la troisième étape fait intervenir p divisions euclidiennes de polynômes de degré majoré par n, d'où un $O(p \times n^2)$.

Au total on a $O(p \times n^3)$ opérations pour trouver un facteur non constant ou pour prouver l'irréductibilité.

3 Lemme de Hensel

L'algorithme de Berlekamp nous permet d'obtenir la factorisation dans $\mathbb{Z}/p\mathbb{Z}$ (éventuellement l'irréductibilité) d'un polynôme à coefficients entiers. On cherche à remonter cette factorisation modulo $p^{2^k}, k \geq 1$. Le lemme de Hensel va exaucer ce souhait.

Lemme 3.1 *Soit P un polynôme à coefficients entiers unitaire, et soit :*

$$P = G_1 H_1 \mod p$$

une factorisation de P en produit d'éléments premiers entre eux. Notons U_1 et V_1 des polynômes unitaires vérifiant :

$$\deg U_1 < \deg H_1 \text{ et } \deg V_1 < \deg G_1,$$
$$U_1 G_1 + V_1 H_1 = 1 \mod p.$$

Alors pour tout $K = 2^k$ on a l'existence d'uniques G_K, H_K, U_K, V_K dans $\mathbb{Z}/p^K\mathbb{Z}[X]$ tels que :

$$G_K = G_{2K} \mod p^K, \text{ et de même pour } H, U, V,$$
$$G_K,\ H_K \text{ sont unitaires,}$$
$$P = G_K H_K \text{ dans } \mathbb{Z}/p^K\mathbb{Z},$$
$$U_K G_K + V_K H_K = 1 \text{ dans } \mathbb{Z}/p^K\mathbb{Z},$$
$$\deg U_K < \deg H_K,\ \deg V_K < \deg G_K.$$

†. Voir plus loin (paragraphe 5.1) pour le choix de p, qui en pratique n'excède pas 100.

Preuve :
► On va procéder par récurrence en supposant les polynômes H_K, G_K, V_K, U_K construits au rang K. Dès lors on pose le système d'équations :

$$\begin{cases} G_{2K} = G_K + p^K g_K \\ H_{2K} = H_K + p^K h_K \end{cases} \quad (1)$$

où $h_K, g_K \in \mathbb{Z}/p^K\mathbb{Z}[X]$ les inconnues. On réécrit l'égalité $P - G_K H_K = 0 \mod p^K$ en :

$$P - G_K H_K = p^K R_K \mod p^{2K}$$

En se rappelant qu'on veut $P = G_{2K} H_{2K} \mod p^{2k}$, le système (1) se réécrit en :

$$G_K h_K + H_K g_K = R_K \mod p^K$$

Il suffit donc de prendre :

$$\begin{cases} h_K = U_K R_K & \mod H_K, \\ g_K = V_K R_K & \mod G_K. \end{cases}$$

La construction de U_{2K} et V_{2K} se fait aussi de manière récursive. On remarque que U_K est l'inverse de G_K modulo H_K (et de même pour V_K et H_K). La question se ramène donc à trouver l'inverse de G_{2K} connaissant celui de G_K. Posons $U_{2K} = 2U_K - G_{2K}U_K^2 \mod H_{2K}$. On effectue les calculs suivant modulo p^{2K} et on a :

$$\begin{aligned} U_{2K}G_{2K} &= 2U_K G_{2K} - G_{2K}^2 U_K^2 && \mod H_{2K} \\ &= 1 - (U_K G_{2K} - 1)^2 && \mod H_{2K} \end{aligned}$$

or on a :

$$\begin{aligned} U_K G_{2K} &= U_K(G_K + p^K g_K) \\ &= 1 - H_K V_K + U_K p^K g_K \end{aligned}$$

ainsi

$$\begin{aligned} (U_K G_{2K} - 1)^2 &= (U_K p^K g_K - H_K V_K)^2 && \mod H_{2K} \\ &= (U_K p^K g_K - (H_{2K} - p^K h_K)V_K)^2 && \mod H_{2K} \\ &= 0 && \mod H_{2K} \end{aligned}$$

car $H_K = H_{2K} - p^K h_K$ et tous les calculs se font modulo p^{2K}. C'est ce que l'on voulait démontrer. On obtient des formules analogues pour V_K. ◄

Remarquons que le lemme de Hensel est un peu plus général puisqu'il affirme que l'on peut remonter une factorisation de $\mathbb{F}_p[X]$ dans $\mathbb{Z}/p^k\mathbb{Z}$ pour tout $k \in \mathbb{N}^*$. Néanmoins, ce relèvement quadratique sera amplement suffisant et la preuve présentée a l'avantage de donner directement un algorithme de relèvement :

Algorithme 1 HENSEL

Entrées : $f, g, h, u, v \in \mathbb{Z}[X]$, $p, k \in \mathbb{N}$ *p premier,* $f = gh[p^k]$ *et* $ug + vh = 1[p^k]$.
Sorties : $\tilde{g}, \tilde{h}, \tilde{u}, \tilde{v} \in \mathbb{Z}[X]$, $f = \tilde{g}\tilde{h}[p^{2k}]$ *et* $\tilde{u}\tilde{g} + \tilde{v}\tilde{h} = 1[p^{2k}]$.

$r \leftarrow \frac{1}{p^k}(f - gh)$
$\tilde{h} \leftarrow h + p^k \times$ DIV_EUCLIDE(ur, h)
$\tilde{g} \leftarrow g + p^k \times$ DIV_EUCLIDE(vr, g)
$\tilde{u} \leftarrow$ DIV_EUCLIDE$(2u - u^2\tilde{g}, \tilde{h})$
$\tilde{v} \leftarrow$ DIV_EUCLIDE$(2v - v^2\tilde{h}, \tilde{g})$
Retourner $\tilde{g}, \tilde{h}, \tilde{u}, \tilde{v}$

Proposition 3.2 *L'algorithme de relèvement présenté ci-dessus est polynomial en le logarithme des coefficients de f, en le degré de f, en p et en k.*

Preuve :
► En effet, tous les coefficients des polynômes sont majorés par $\max(|a_i|, p^{2k})$ où les a_i sont les coefficients de f. De plus, tous les degrés de ces polynômes sont majorés par n.

Ensuite, les seules opérations utilisées sont la multiplication, l'addition et la division euclidienne des polynômes, qui sont bien de coût polynomial en les données.

En supposant que $p^k > \max |a_i|$, ce qui correspond au cadre dans lequel on va utiliser l'algorithme, on peut estimer le coût de cet algorithme à $O(k^2 \times n^2)$ où la présence du k^2 s'explique par le fait que les opérations arithmétiques de base ne peuvent plus être considérées comme temps constant. ◄

Remarquons que l'on peut relever une factorisation de $\mathbb{F}_p[X]$ dans $\mathbb{Z}/p^{2^k}\mathbb{Z}$ en temps polynomial si 2^k est polynomial en les données : en effet toutes les remontées le seront et le nombre de remontées aussi.

4 L'algorithme LLL

Bien que de nature apparemment géométrique, l'algorithme LLL, du nom de ses inventeurs A. Lenstra, H. Lenstra et L. Lovász, a été initialement conçu pour la factorisation des polynômes. Étant donné un réseau de $\mathbb{Q}^n$,‡ son but est de trouver une base de vecteurs presque orthogonaux dont les normes sont graduellement petites.

Définition 4.0.2 (Réseaux) *Un réseau de $\mathbb{Q}^n$ est un sous $\mathbb{Z}-$module de $\mathbb{Q}^n$ de type fini.*
La dimension d'un réseau est le cardinal d'une partie génératrice minimale.

Généralement, un réseau est présenté comme un sous-groupe discret◇ de $\mathbb{R}^n$. Un résultat classique montre en fait que tout sous-groupe discret de $\mathbb{R}^n$ est isomorphe à $\mathbb{Z}^d$ avec $d \leqslant n$. La dimension est alors d et les deux visions sont essentiellement les mêmes. Notons qu'une partie génératrice minimale peut être de cardinal strictement plus grand que n.

Ceci dit, dans la suite, on confondra parfois une famille libre⋆ et le réseau qu'elle engendre et la dimension sera simplement le cardinal de la famille libre.

Définition 4.0.3 *Soit $m \leqslant n$. On appelle déterminant du réseau engendré par une famille libre $A = (a_1, \ldots, a_m)$ la quantité $\Delta = \det({}^tAA)$*

On vérifie facilement qu'il ne dépend pas de la base choisie.

4.1 Orthogonalisation de Gram–Schmidt

Dans toute la suite, nous noterons $\|.\|$ la norme euclidienne d'un vecteur. On identifiera le polynôme $f = \sum_{i=0}^{n} a_i X^i$ avec le vecteur formé de ces coefficients $(a_0, \ldots, a_n)$ et $\|f\| = \|(a_0, \ldots, a_n)\|$.

Rappelons brièvement le procédé d'orthogonalisation de Gram–Schmidt, afin de fixer des notations. Étant donné une famille libre de vecteurs $(b_1, \ldots, b_m)$ avec $m \leqslant n$, on veut trouver une famille orthogonale $(b_1^*, \ldots, b_m^*)$ vérifiant $b_k^* \in \underset{i \in [\![1,k]\!]}{\text{vect}}(b_i)$ pour tout k.

Proposition 4.1.1 (Orthogonalisation de Gram–Schmidt) *Une telle famille existe et s'obtient par l'algorithme suivant. On pose $b_1^* \leftarrow b_1$ et pour i allant de 2 à m on effectue :*

$$\mu_{ij} \leftarrow \frac{(b_i, b_j^*)}{(b_j^*, b_j^*)} \qquad (j = 1, \ldots, i-1)$$
$$b_i^* \leftarrow b_i - \sum_{j=1}^{i-1} \mu_{ij} b_j^*.$$

‡. On peut se placer sur $\mathbb{R}$ mais cela n'a que peu de sens d'un point de vue informatique.
◇. Un sous-groupe de $\mathbb{R}^n$ est discret si son intersection avec tout compact est finie.
⋆. On ne précise pas si la notion de liberté est dans $\mathbb{Q}^n$ ou en tant que $\mathbb{Z}-$module car les deux notions coïncident.

Il s'agit simplement de projeter le vecteur b_i sur la famille orthogonale déjà obtenue $(b_1^*, \ldots, b_{i-1}^*)$.

Cette procédure d'orthogonalisation prend un temps $O(n \times m)$ opérations élémentaires sur les rationnels. Si l'on note s le nombre de bits maximal qu'il faut pour stocker un numérateur ou un dénominateur d'une des données, la nouvelle base aura des numérateurs et dénominateurs dont la taille sera majorée en $O(m \times s)$, ce qui assure la complexité polynomiale de l'algorithme.

4.2 Bases faiblement réduites

Le but de l'algorithme LLL est de donner une base d'un réseau presque orthogonale, en fournissant des petits vecteurs.

Pour cela, on introduit des notions de bases réduites.

Définition 4.2.1 (Réduction faible) *Une base $B = (b_1, \ldots, b_m)$ sera dite faiblement réduite si en l'orthogonalisant, on obtient la condition pour tout $1 \leqslant j < i \leqslant m$:*

$$|\mu_{ij}| \leqslant \frac{1}{2}.$$

Cette condition est très naturelle car on ne peut faire que des combinaisons linéaires entières lors des changements de bases : on ne peut donc se rapprocher de «l'idéal» orthogonal qu'à $\frac{1}{2}$ près.

Proposition 4.2.2 *Toute base peut être faiblement réduite.*

Preuve :

► Soit (i_0, j_0) le plus grand couple pour l'ordre lexicographique qui ne vérifie pas $|\mu_{i_0 j_0}| \leqslant \frac{1}{2}$ (parmi les couples (i, j), $i > j$). Soit $c = \lfloor \mu_{i_0 j_0} \rceil$ l'entier le plus proche de $\mu_{i_0 j_0}$. On transforme B en la base $\overline{B}$ par l'opération :

$$\overline{b}_i = \begin{cases} b_i & si\ i \neq i_0 \\ b_{i_0} - c b_{j_0} & sinon. \end{cases}$$

Cette transformation ne change pas les vecteurs de l'orthogonalisée ($B^* = \overline{B}^*$). Seuls les coefficients μ_{ij} ont changé. En écrivant $b_{i_0} - c b_{j_0} = b_{i_0}^* + \sum_{j<i_0} \mu_{i_0 j} b_j^* - c b_{j_0}^* - c \sum_{j<j_0} \mu_{j_0 j} b_j^*$, on trouve :

$$\overline{\mu}_{ij} = \begin{cases} \mu_{ij} & si\ i \neq i_0\ ou\ si\ j > j_0 \\ \mu_{i_0 j} - c\mu_{j_0 j} & sinon. \end{cases}$$

En particulier les couples plus grands que (i_0, j_0) ne sont pas modifiés et $|\overline{\mu}_{i_0 j_0}| = |\mu_{i_0 j_0} - c| \leqslant \frac{1}{2}$.
En réitérant cette opération au plus $\binom{m}{2}$ fois, on peut donc faiblement–réduire la base B en $O(m^2 \times n)$ opérations. ◄

4.3 Bases réduites

Définition 4.3.1 *Une base B d'un réseau sera dite réduite si elle est faiblement réduite et vérifie de plus pour $1 \leqslant i < m$*

$$\|b_{i+1}^* + \mu_{i+1,i} b_i^*\|^2 \geqslant \frac{3}{4} \|b_i^*\|^2. \tag{2}$$

Rappelons qu'une réduction faible ne modifie pas l'orthogonalisée et donc peut intervenir à tout moment dans un algorithme de réduction, sans modifier ce qui a déjà été fait.

Le but de ce qui va suivre est de montrer le résultat suivant :

Théorème 4.3.2 *Toute base peut être réduite. De plus, le temps de la réduction est polynomiale en la taille des données.*

Pour cela, nous allons montrer quelques propriétés des bases réduites. Tout d'abord, introduisons des notations :

Notations 4.3.3 *Soit un réseau engendré par une $\mathbb{Z}-$base $B = (b_1, \ldots, b_m)$.*
Pour $1 \leqslant i \leqslant m$, on note Δ_i (ou $\Delta_i(B)$) le déterminant du réseau engendré par $B_i = (b_1, \ldots, b_i)$.
On note de plus $V(B) = \prod_{i=1}^{m} \Delta_i(B)$.

On remarque facilement, du fait que la matrice de changement de base vers l'orthogonalisée est triangulaire supérieure de diagonale $(1, \ldots, 1)$, que $\Delta_i = \prod_{j=1}^{i} \|b_j^*\|^2$.

Ainsi, une réduction faible donne une nouvelle base B' on a $V(B') = V(B)$.

Proposition 4.3.4 *On a l'inégalité :*

$$V(B) \leqslant \left(\max_i \|b_i\|\right)^{m(m+1)}.$$

Preuve :

► En écrivant $b_i = b_i^* + \sum_{j=1}^{i-1} \mu_{ij} b_j^*$ on obtient $\|b_i\| \geqslant \|b_i^*\|$ pour tout i. On a alors :

$$\begin{aligned} V(B) = \prod_{i=1}^{m} \Delta_i(B) = \prod_{i=1}^{m} \prod_{j=1}^{i} \|b_j^*\|^2 &= \prod_{i=1}^{m} \|b_i^*\|^{2(m-i+1)} \\ &\leqslant \prod_{i=1}^{m} \|b_i\|^{2(m-i+1)} \\ &\leqslant \left(\max_i \|b_i\|\right)^{m(m+1)}. \end{aligned}$$

◄

Voici enfin la proposition clé dans l'algorithme de réduction.

Proposition 4.3.5 *Si la base B du réseau est faiblement réduite et si les vecteurs b_i^* et b_{i+1}^* ne vérifient pas l'inégalité (2) alors la base $C = (b_1, \ldots, b_{i+1}, b_i, \ldots, b_m)$ vérifie :*

$$V(C) < \frac{3}{4} V(B).$$

Preuve :

► Il s'agit de faire le lien entre C^* et B^*. Il est clair que pour $j \neq i$ on a :

$$\Delta_j(B) = \Delta_j(C)$$

puisque les réseaux sont les mêmes. Ainsi $\frac{V(C)}{V(B)} = \frac{\Delta_i(C)}{\Delta_i(B)} = \frac{\|c_i^*\|^2}{\|b_i^*\|^2}$. Il faut alors relier $\|c_i^*\|$ à $\|b_i^*\|$.

On a $c_i = b_{i+1} = b_{i+1}^* + \sum_{j=1}^{i} \mu_{i+1,j} b_j^* = b_{i+1}^* + \mu_{i+1,i} b_i^* + \sum_{j=1}^{i-1} \nu_{ij} c_j^*$, où on a noté ν_{ij} les coefficients d'orthogonalisation de C. Ceci vient du fait que pour $j \leqslant i-1$, $c_j^* = b_j^*$ est orthogonal à $b_{i+1}^* + \mu_{i+1,i} b_i^*$. On a alors :

$$\begin{aligned} c_i^* &= c_i - \sum_{j=1}^{i-1} \nu_{ij} c_j^* \\ &= b_{i+1}^* + \mu_{i+1,i} b_i^* \end{aligned}$$

et par hypothèse $\|b_{i+1}^* + \mu_{i+1,i} b_i^*\|^2 < \frac{3}{4} \|b_i^*\|^2$. ◄

Cette proposition fournit alors une idée raisonnable d'algorithme pour réduire une base (au sens fort) : on trouve le plus petit indice qui ne vérifie pas la condition de réduction forte (2), on échange ces deux vecteurs et on réduit faiblement la base. On recommence alors récursivement.

C'est le facteur de réduction géométrique dans la proposition précédente qui fait marcher l'algorithme en temps polynomial . Notons que le point important est que $\frac{3}{4} < 1$ et que d'autres facteurs peuvent tout aussi bien marcher. ††

††. Le choix de $\frac{3}{4}$ est surtout motivé par le fait qu'il s'agit du facteur utilisé dans l'article original [1].

Algorithme 2 LLL

Entrée : $B \in \mathbb{Q}^{n\times m}$
Sortie : $\overline{B} \in \mathbb{Q}^{n\times m}$ *base réduite.*

$\overline{B} \leftarrow$REDUIT–FAIBLE (B)
Tant que $\overline{B}$ n'est pas réduite **Faire**
  $i \leftarrow \min_j \left(\|b_j^* + \mu_{j+1,j} b_{j+1}^*\|^2 < \frac{3}{4}\|b_j^*\|^2\right)$
  échanger $b_i \leftrightarrow b_{i+1}$
  $\overline{B} \leftarrow$REDUIT–FAIBLE $(\overline{B})$
Fin Tant que
Retourner $\overline{B}$

Proposition 4.3.6 (Terminaison et complexité) *La boucle « Tant que » ne s'exécute qu'un nombre de fois polynomial en la taille des données.*

Preuve :
► Soit d le pgcd des dénominateurs. On a $C = dB$ est à valeurs entières et donc $|V(\overline{C})| \geqslant 1$ à toutes les étapes de l'algorithme lancé sur C. La boucle « Tant que » ne peut donc s'exécuter plus que $\log_{\frac{3}{4}}(V(C))$ fois. Or $\Delta_i(C) = d^{2i}\Delta_i(B)$ et donc, avec la proposition 4.3.4 :

$$V(C) = d^{m(m+1)}V(B) \leqslant \left(d \max_i \|b_i\|\right)^{m(m+1)}.$$

Si s est le nombre maximal de bits nécessités par un numérateur ou dénominateu,r on a un nombre d'itérations en $O(m^2(s + \log d))$. ◄

Ceci permet d'énoncer le théorème suivant :

Théorème 4.3.7 *L'algorithme* LLL *s'exécute en temps polynomial en les données.*

Preuve :
► L'étape de réduction faible (qui consiste aussi à mettre à jour les μ_{ij}) ne nécessite pas d'être effectuée sur toute la matrice : en effet, les vecteurs $(b_1, \ldots, b_{i-1})$ ne sont pas changés et les coefficients μ correspondant non plus. Par ailleurs, on ne maîtrise rien de ce qui se passe aux rangs supérieurs à $i + 1$ et il ne sert à rien de réduire faiblement au delà de $i + 1$. Tout ceci permet de voir que l'étape de réduction faible ne peut coûter que $O(n^2)$ si elle est bien programmée.

On a donc une complexité totale de LLL en $O[m^2 \times n^2 \times (s + \log d)]$ qui est majorée au pire des cas (tous les dénominateurs sont grands et premiers entre eux ‡‡) par $O(m^4 \times n^2 \times s)$.

Ceci n'achève pas la preuve car on ne sait pas si les rationnels dans les calculs intermédiaires « n'explosent » pas en taille mémoire. C'est l'objet du lemme suivant. ◄

Lemme 4.3.8 *On suppose que le réseau est à valeurs dans $\mathbb{Z}^n$. Notons $M = \max\left(\max_i \|b_i\|, 1\right)$ et $s = \log M$. Alors les entiers intervenants dans les calculs ont leur logarithme borné par :*

$$O\left(n \log \max_i \|b_i\|\right) = O(ns).$$

Le cas des réseaux à valeurs dans $\mathbb{Q}$ s'en déduit mais nous nous contenterons de ce lemme car il correspond au cadre dans lequel on utilisera LLL.
Preuve : (idée)
► Un calcul facile montre que tout au long de l'algorithme $\|b_i^*\| \leqslant M$. Ensuite, si l'on note k le plus petit entier qui fait défaut à la condition de réduction forte, alors on a encore, au moment de l'échange de b_k et b_{k+1} et avant l'étape de réduction faible :

$$|\mu_{ij}| \leqslant \frac{1}{2},\ \forall 1 \leqslant j < i \leqslant k.$$

‡‡. On a alors $\log(d) = O(m^2 \times s)$.

Ainsi $\|b_i\|^2 \leqslant nM^2$ pour $i \leqslant k$. De plus, pour $i > k+1$ les vecteurs ne sont pas modifiés et par une induction facile, on montre que :

$$\forall i \neq k+1,\ \|b_i\|^2 \leqslant nM^2.$$

Il nous reste à traiter le cas $k+1$. Pour cela, on montre la propriété suivante par récurrence :

$$|\mu_{k+1,j}| \leqslant 2^{n-(k+1)} \left(M^{n-1}\right),\ j \leqslant k.$$

Au début de l'algorithme, on a pour tout couple (i,j) avec[◇◇] $j \leqslant n-1$:

$$\mu_{ij}^2 \leqslant \frac{\|b_i\|\|b_j^*\|}{\|b_j^*\|^2} \leqslant \frac{M^2}{\|b_j^*\|^2} \leqslant \frac{\Delta_{j-1}M^2}{\Delta_j} \leqslant \Delta_{j-1}M^2 \leqslant M^{2j} \leqslant M^{2(n-1)}.$$

On prouve alors l'hérédité. On note ν les nouveaux coefficients après l'échange de b_k et b_{k+1}. On a alors par un calcul simple, pour $j < k$:

$$\begin{aligned}
|\nu_{kj}| = |\mu_{k+1,j} - c\mu_{kj}| &< |\mu_{k+1,j}| + \frac{c}{2} \\
&< |\mu_{k+1,j}| + |\mu_{k+1,k}| \\
&< 2^{n-(k+1)} \left(M^{n-1}\right) + 2^{n-(k+1))} \left(M^{n-1}\right) \\
&< 2^{n-k} \left(M^{n-1}\right)
\end{aligned}$$

car $|c| \leqslant 2|\mu_{k+1,k}|$. Ceci est bien l'inégalité attendue car à la fin de l'étape, k devient $k-1$. Ceci termine la récurrence.
Dès lors on peut majorer b_{k+1} :

$$\begin{aligned}
\|b_{k+1}\|^2 &\leqslant \|b_{k+1}^*\|^2 + \sum_{j=1}^{k} |\mu_{k+1,j}|^2 \|b_j^*\|^2 \\
&\leqslant M^2 + k(2^{2n}M^{2(n-1)}M^2) \leqslant n2^{2n}M^{2n}.
\end{aligned}$$

Ainsi on a bien $\log \|b_i\| = O(n \log M)$. La formule des μ_{ij} rappelée au début de la section 4.1 assure que la taille de leur dénominateur[★★] est bornée par $\log M$ et celle de leur numérateur bornée par $O(n \log M + \log M) = O(n \log M)$. Ceci achève la démonstration du lemme. ◀

Dans notre application à la factorisation de polynômes, le réseau initial sera à valeurs dans $\mathbb{Z}^n$ avec $m = n$ et on pourra retenir une complexité en $O(n^4 \times s)$ opérations élémentaires. Comme de plus on travaille sur des grands entiers, il faut ajouter un facteur $(ns)^2$ pour tenir compte du temps des opérations arithmétiques élémentaires et on a un temps de l'ordre de $O(n^6 \times s^3)$.

Finissons la présentation de l'algorithme LLL par des propriétés intéressantes de la base réduite.

Proposition 4.3.9 *Si B est une base réduite de dimension n, on a :*

1. $\Delta_n(B) \leqslant \prod_{i=1}^n \|b_i\|^2 \leqslant 2^{\frac{n(n-1)}{2}} \Delta_n(B)$.
2. $\|b_1\|^2 \leqslant 2^{\frac{n(n-1)}{2}} \Delta_n(B)^{\frac{2}{n}}$.
3. $\|b_j\|^2 \leqslant 2^{i-1}\|b_i^*\|^2$ *pour* $1 \leqslant j \leqslant i \leqslant n$.
4. *Pour* $x \in \operatorname{vect} B$, $x \neq 0$, $\|b_1\|^2 \leqslant 2^{n-1}\|x\|^2$.

Preuve :
▶ La première inégalité du premier point est l'inégalité d'Hadamard et ne nécessite aucune propriété de réduction de la base B. Nous ne donnons une preuve que des deux derniers points car ce sont les seuls qui vont nous servir dans la suite. Toutes les références sur LLL les détaillent.

De la définition (2) des bases réduites, on tire $\|b_{i+1}^*\|^2 \geqslant \left(\frac{3}{4} - \mu_{i+1,i}\right)\|b_i\|^2 \geqslant \frac{1}{2}\|b_i^*\|^2$. Par une récurrence facile, on en tire pour tout $1 \leqslant j \leqslant i \leqslant n$:

$$\|b_j^*\|^2 \leqslant 2^{i-j}\|b_i^*\|^2. \tag{3}$$

◇◇. On prend $j \leqslant n-1$ car on l'applique à $j \leqslant k < k+1 \leqslant n$.
★★. *i.e.* leur logarithme.

Il suffit alors de décomposer b_i sur $(b_1^*, \ldots, b_i^*)$ et de calculer sa norme :

$$\begin{aligned}\|b_i\|^2 &= \|b_i^*\|^2 + \sum_{j=1}^{i-1} \mu_{ij}^2 \|b_j^*\|^2 \\ &\leqslant \|b_i^*\|^2 + \sum_{j=1}^{i-1} \frac{1}{4} 2^{i-j} \|b_i^*\|^2 \\ &\leqslant 2^{i-1} \|b_i^*\|^2.\end{aligned}$$

De cette inégalité et de 3, on tire $\|b_j\|^2 \leqslant 2^{j-1}\|b_j^*\|^2 \leqslant 2^{i-1}\|b_i^*\|^2$.

Il nous reste à établir le dernier point. Pour cela, on décompose x sur la base $(b_1, \ldots, b_n)$:

$$x = \sum_{i=1}^{j} n_i b_i = \sum_{i=1}^{j} r_i b_i^*$$

avec $r_j = n_j \neq 0$ et les n_i entiers. On en déduit $\|x\|^2 \geqslant n_i^2 \|b_j^*\|^2 \geqslant \|b_j^*\|^2$. En combinant avec le point précédent on a :

$$\begin{aligned}\|x\|^2 &\geqslant 2^{1-i}\|b_1\|^2 \\ &\geqslant 2^{1-n}\|b_1\|^2.\end{aligned}$$

◀

Cette dernière inégalité nous montre qu'à un facteur 2^{n-1} près, b_1 est un petit vecteur de réseau. Ceci est d'autant plus intéressant que trouver un plus petit vecteur d'un réseau ayant une base donnée est un problème soupçonné comme étant **NP**−complet.

5 Factorisation dans $\mathbb{Z}[X]$

5.1 Premières étapes

Tout d'abord, notons que le problème de la factorisation sur $\mathbb{Q}[X]$ est le même, quitte à multiplier par le dénominateur commun à tous les coefficients. Notons de plus que l'on peut supposer que le polynôme de départ est sans facteurs carrés car sinon on peut déjà factoriser par $\text{pgcd}(f, f')$ qui est non trivial. Finalement on peut supposer que le polynôme est unitaire. En effet on peut réécrire :

$$f(X) = \sum_{i=0}^{n} a_i X^i = \frac{1}{a_n^{n-1}} \left((a_n X)^n + \sum_{i=0}^{n-1} a_i a_n^{n-1-i} (a_n X)^i \right) = \frac{1}{a_n^{n-1}} \tilde{f}(a_n X).$$

Il suffit de factoriser $\tilde{f}$ qui est unitaire, pour pouvoir ensuite factoriser f.

Dans la suite, on supposera $f \in \mathbb{Z}[X]$ unitaire et sans facteurs carrés.
Il s'agit d'utiliser les différents algorithmes présentés ci-dessus pour aboutir à une factorisation de f. La première étape consiste à factoriser f dans $\mathbb{F}_p$ pour p choisi de telle façon que f n'ait pas de facteurs carrés dans ce corps. Pour cela, on calcule le résultant de f et f' (qui est non nul [†††]) et on choisit le plus petit p qui ne divise pas ce résultant. Remarquons que p n'est pas trop grand :

Proposition 5.1.1 *Pour n assez grand, $p \leqslant 4n \log(\max |a_i|) + 4n \log n$, où $f = \sum_{i=0}^{n} a_i X^i$.*

Preuve :
▶ En effet, on a par l'inégalité d'Hadamard :

$$|\text{res}(f, f')| \leqslant \|f\|^{n-1} \|f'\|^n \leqslant (\sqrt{n} \max |a_i|)^{n-1} (\sqrt{n} n \max |a_i|)^n \leqslant n^{2n} (\max |a_i|)^{2n}.$$

†††. $\text{res}(f, f') \neq 0 \Leftrightarrow f$ est sans facteurs carrés

Calculons le nombre maximal de facteurs premiers distincts qui peuvent diviser ce résultant. Pour cela, on utilise le théorème des nombres premiers qui affirme que :

$$\sum_{p \leqslant m} \log p \sim m.$$

Ainsi, pour m assez grand, $\prod_{p \leqslant m} p \geqslant e^{\frac{m}{2}}$ et on a donc l'implication

$$m \geqslant 4n \log n + 4n \log(\max |a_i|) \Longrightarrow \prod_{p \leqslant m} p > |\mathrm{res}(f, f')|.$$

Ainsi, $\mathrm{res}(f, f')$ ne peut admettre plus de $4n \log n + 4n \log(\max |a_i|)$ facteurs premiers distincts. On peut donc trouver un $p \nmid \mathrm{res}(f, f')$ dont la taille est polynomiale en les coefficients $(\log(\max |a_i|))$ et en le degré de f. En pratique, il est rare que p soit bien plus grand que 100. ◀

Une fois une factorisation effectuée de $f = gh$ dans $\mathbb{F}_p$, l'idée est de relever cette factorisation en $f = \hat{g}\hat{h}$ dans $\mathbb{Z}/p^k\mathbb{Z}$ grâce au lemme de Hensel pour un k bien choisi. On note $l = \deg g$ et on utilise ensuite LLL pour le réseau engendré par :

$$\{p^k X^i, 0 \leqslant i < l\} \cup \{\hat{g} X^i, 0 \leqslant i < n - l\}.$$

Dans la suite de cette section, on va s'attacher à montrer que le plus petit vecteur d'une base réduite de ce réseau a soit un facteur non trivial en commun avec f soit f est irréductible.

5.2 Propriétés du relèvement

Voyons tout d'abord un lemme tout à fait général qui commence à faire apparaître l'intérêt des petits vecteurs dans la recherche de facteurs non triviaux.

Lemme 5.2.1 *Soient $f, h \in \mathbb{Z}[X]$ de degrés respectifs n et l. Supposons par ailleurs qu'il existe $g \in \mathbb{Z}[X]$ unitaire et non constant qui divise f et h modulo $m \in \mathbb{N}^*$ avec $\|f\|^l \|h\|^n < m$. Alors,* $\mathrm{pgcd}(f, h)$ *n'est pas constant.*

Preuve :
▶ On sait qu'il existe des polynômes $u, v \in \mathbb{Z}[X]$ tels que $uf + vh = \mathrm{res}(f, h)$. En prenant cette relation modulo m, on a l'existence d'un polynôme $w \in \mathbb{Z}[X]$ tel que $gw = \mathrm{res}(f, h)[m]$. Comme g est unitaire et non constant, on a $w = 0[m]$ et donc m divise $\mathrm{res}(f, h)$.

D'un autre côté, l'inégalité d'Hadamard donne $|\mathrm{res}(f, h)| \leqslant \|f\|^l \|h\|^n < m$. Ainsi, $\mathrm{res}(f, h) = 0$ et donc $\mathrm{pgcd}(f, h)$ n'est pas constant. ◀

L'utilisation de ce lemme dans notre cadre est presque immédiate. Soit $g \in \mathbb{Z}[X]$ un polynôme unitaire irréductible dans $\mathbb{F}_p[X]$ facteur simple de f modulo p et facteur de f modulo p^k, via le lemme de Hensel. On note $l > 0$ son degré. On pose $m = p^k$ et on considère, comme annoncé, le réseau formé des polynômes de $\mathbb{Z}_{n-1}[X]$ qui modulo p^k sont multiples de g :

$$\{p^k X^i, 0 \leqslant i < l\} \cup \{g X^i, 0 \leqslant i < n - l\}. \tag{4}$$

Dans ces conditions, le lemme précédent permet d'affirmer :

Proposition 5.2.2 *Soit b un vecteur non nul de ce réseau vérifiant $\|b\|^n \|f\|^{n-1} < p^k$. Alors,* $\mathrm{pgcd}(f, b)$ *est un facteur non trivial de f dans $\mathbb{Z}[X]$.*

Preuve :
▶ C'est une conséquence triviale du lemme : il suffit de remarquer que b est bien divisible par g modulo p^k, que g est unitaire et non constant et que $\deg b \leqslant n - 1$. ◀

Cette proposition relativement élémentaire suffirait à construire un algorithme en temps polynomial. Voyons néanmoins une version plus avancée qui est en fait la propriété énoncée dans l'article historique de LLL. Même si elle ne permet pas de faire baisser la complexité au pire de l'algorithme, nous verrons que la complexité moyenne en est améliorée. Avant d'énoncer cette propriété, nous avons besoin d'un lemme sur les réseaux de $\mathbb{Z}^n$:

Lemme 5.2.3 *Soit Λ un réseau de $\mathbb{R}^n$ et $R \subset \Lambda$ un sous-réseau. Soit $(a_1, \ldots, a_n)$ une base de Λ. Alors on peut trouver une base $(b_1, \ldots, b_n)$ de R de la forme :*

$$\begin{array}{rcl} a_1 &=& \nu_{11} b_1 \\ a_2 &=& \nu_{21} b_1 + \nu_{22} b_2 \\ \vdots & \vdots & \vdots \quad \ddots \\ a_n &=& \nu_{n1} b_1 + \quad \ldots \quad + \nu_{nn} b_n. \end{array}$$

Preuve :

► Notons $B_k = \mathrm{vect}_{\mathbb{Z}}\{b_1, \ldots, b_k\}$.

Remarquons tout d'abord que si $x, y \in B_k$ alors on peut trouver $z \in B_{k-1}$. En effet, on écrit $x = x' + \alpha b_k$ et $y = y' + \beta b_k$ avec $x', y' \in B_{k-1}$, puis $d = \mathrm{pgcd}(\alpha, \beta) = u\alpha + v\beta$. Alors, $z = x - \frac{\alpha}{d}(ux + vy)$ convient.

Par une récurrence simple, on en déduit que pour tout $1 \leqslant k \leqslant n$ on a $B_k \cap R \neq \emptyset$. Choisissons donc des vecteurs de R de la forme :

$$a_i = \nu_{i1} b_1 + \ldots \nu_{ii} b_i$$

où les ν_{ik} sont entiers et $|\nu_{ii}| > 0$ est minimal. On va montrer par l'absurde que $(a_1, \ldots, a_n)$ convient. Soit donc $c \in R \backslash \mathrm{vect}_{\mathbb{Z}}\{a_1, \ldots, a_n\}$ tel que $c = t_1 b_1 + \ldots + t_k b_k$ pour k minimal puis pour $|t_k|$ minimal. Alors, comme $\nu_{kk} \neq 0$, on peut trouver $s \in \mathbb{N}$ tel que :

$$|t_k - s\nu_{kk}| < |\nu_{kk}|.$$

Soit alors $d = c - s a_k \in R \backslash \mathrm{vect}_{\mathbb{Z}}\{a_1, \ldots, a_n\}$. Par minimalité de k, d a une composante non nulle sur b_k mais celle-ci $(t_k - s\nu kk)$ est strictement plus petite en valeur absolue que ν_{kk}, ce qui contredit la construction de a_k. ◄

Corollaire 5.2.4 *Tout réseau R de $\mathbb{Z}^n$ a une base échelonnée $(b_1, \ldots, b_k)$ c'est-à-dire vérifiant :*

$$b_i \in \mathrm{vect}_{\mathbb{Z}}\{e_1, \ldots, e_{i_j}\} \text{ avec } 1 \leqslant i_1 < \ldots < i_k \leqslant n.$$

Preuve :

► Il suffit d'appliquer le lemme au réseau Λ engendré par $\{e_{\deg f},\ f \in R\}$ où $(e_1, \ldots, e_n)$ est la base canonique de $\mathbb{Z}^n$. ◄

Venons-en maintenant à la proposition principale, qui améliore la proposition 5.2.2. Rappelons que l'on considère le réseau :

$$\{p^k X^i, 0 \leqslant i < l\} \cup \{g X^i, 0 \leqslant i < n - l\}$$

où g est un facteur irréductible de degré l qui divise f modulo p^k. Il est clair que f est divisible par un unique polynôme g_1, irréductible unitaire, multiple de g modulo p^k.

Proposition 5.2.5 *Soit b un vecteur non nul de ce réseau vérifiant $\|b\|^n \|f\|^{n-1} < p^{kl}$. Alors, b est divisible par g_1 dans $\mathbb{Z}[X]$.*

Preuve :

► Soit $h = \mathrm{pgcd}(f, b) \in \mathbb{Z}[X]$. Il est clair qu'il suffit de montrer que g divise h dans $\mathbb{F}_p[X]$. Nous raisonnons par l'absurde. Comme g est irréductible dans $\mathbb{F}_p[X]$ on a l'existence de polynômes λ, μ et $\nu \in \mathbb{Z}[X]$ tels que :

$$\lambda g + \mu h = 1 - p\nu.$$

Remarquons qu'en multipliant par $1 + p\nu + \ldots + p^{k-1}\nu^{k-1}$ on a :

$$\lambda' g + \mu' h \equiv 1 [p^k]. \tag{5}$$

Du fait que g ne divise pas h, on en déduit aussi que g divise f/h dans $\mathbb{F}_p[X]$ et donc

$$\deg g \leqslant \deg f - \deg h. \tag{6}$$

Considérons le réseau engendré par :

$$R = \{\alpha f + \beta b,\ \deg\alpha < \deg b - \deg h,\ \deg\beta < \deg f - \deg h\}$$

et notons R' son projeté sur le réseau :

$$\mathbb{Z}X^{\deg h} + \ldots + \mathbb{Z}X^{\deg f + \deg b - \deg h - 1}.$$

Soit $c \in R$. Comme g divise f et b modulo p^k, g divise c modulo p^k. Or on a aussi h qui divise c dans $\mathbb{Z}[X]$. En multipliant (5) par c/h et en utilisant le fait que g divise c modulo p^k on a :

$$c/h \equiv 0[p^k, g].$$

Si $\deg c < \deg g + \deg h$ alors $c \in p^k\mathbb{Z}[X]$. Ceci permet de minorer le déterminant de R'. En effet, par le corollaire 5.2.4 on prend une base de R' triangulaire *i.e.* une base de polynômes dont les degrés s'échelonnent de $\deg h$ à $\deg f + \deg b - \deg h$. Or, par (6) $\deg f + \deg b - \deg h \geqslant \deg g + \deg b \geqslant \deg g + \deg h$. Ainsi, cette base contient au moins $\deg g$ vecteurs v vérifiant $\deg v < \deg g + \deg h$ et donc à coefficients dans $p^k\mathbb{Z}$. D'où en effectuant le produit des coefficients dominants des vecteurs de cette base :

$$\sqrt{\Delta R'} \geqslant (p^k)^{\deg g} = p^{kl}.$$

Ceci contredit l'inégalité d'Hadamard pour R'. En effet, montrons que les projections sur R' des vecteurs :

$$\{X^i f,\ 0 \leqslant i < \deg b - \deg h\} \cup \{X^j b,\ 0 \leqslant j < \deg f - \deg h\} \tag{7}$$

sont linéairement indépendants. En effet, si $\alpha f + \beta b$ se projette sur 0 dans R' alors $\deg(\alpha f + \beta b) < \deg h$ mais par ailleurs, h divise $\alpha f + \beta b$ dans $\mathbb{Q}[X]$. D'où $\alpha f + \beta b = 0$. On peut donc appliquer l'inégalité d'Hadamard à R' pour la base sont les projetés ‡‡‡ des vecteurs de (7) :

$$\sqrt{\Delta R'}| \leqslant \|f\|^{\deg b - \deg h}\|b\|^{\deg f - \deg h} \leqslant \|f\|^{n-1}\|b\|^n < p^{kl}.$$

◀

5.3 L'algorithme de factorisation

Voici maintenant le théorème principal qui permet de mettre en place un algorithme polynomial de la factorisation de polynômes :

Théorème 5.3.1 (LLL) *Choisissons k suffisamment grand pour que :*

$$\|f\|^{2n-1} n^{\frac{n}{2}} \binom{n-1}{\lfloor \frac{n-1}{2} \rfloor}^n 2^{\frac{n(n-1)}{2}} < p^{kl}. \tag{8}$$

Soit $(b_1, \ldots, b_n)$ une base LLL*–réduite de (4). Alors :*
- *soit* $\mathrm{pgcd}(b_1, f)$ *est un facteur non trivial de f,*
- *soit f est irréductible dans $\mathbb{Z}[X]$.*

Preuve :
▶ Supposons f réductible et montons que b_1 vérifie la condition de la proposition 5.2.5. Le facteur g_1, irréductible, unitaire et non trivial de f vérifie $g_1 \equiv 0[p^k, g]$ et donc g_1 est dans le réseau (4). Par la proposition 4.3.9 on a :

$$\|g_1\| \geqslant 2^{\frac{1-n}{2}}\|b_1\|.$$

Ainsi, $\|b_1\|^n\|f\|^{n-1} \leqslant \|f\|^{n-1}\|g_1\|^n 2^{\frac{n(n-1)}{2}}$. Il reste à relier $\|f\|$ et $\|g_1\|$. Pour cela, on utilise un résultat dû à Mignotte ◇◇◇ :

$$\|g_1\| \leqslant \sqrt{n}\binom{\deg g_1}{\lfloor \frac{\deg g_1}{2} \rfloor}\|f\|.$$

‡‡‡. Les projetés ont une norme euclidienne plus petite.
◇◇◇. Voir par exemple [2].

En combinant avec l'inégalité précédente, on tombe sur la condition (8) et $\|b\|^n \|f\|^{n-1} < p^{kl}$: $\text{pgcd}(f, b_1)$ fournit un facteur non trivial.

Sinon, f est irréductible. ◀

On peut trouver une borne plus petite, mais l'objectif ici n'est pas l'efficacité, mais le fait de montrer que l'on est dans la classe **P** :

Proposition 5.3.2 *On peut trouver un facteur irréductible unitaire (différent de 1) de f en temps polynomial.*

Algorithme 3 FACTORISER

Entrée : $f \in \mathbb{Z}[X]$ *unitaire sans facteurs carrés.*
Sortie : *Un facteur irréductible non trivial de f.*

$r \leftarrow \text{RES}(f, f')$
$p \leftarrow q$ où q premier, $r \not\equiv 0[q]$
$g, h \leftarrow$BERLEKAMP(f, p) ▷ $f = gh[p]$
$u, v \leftarrow$EUCLIDE_ETENDU(g, h) ▷ $ug + vh = 1[p]$
$k \leftarrow \left\lceil \frac{\log_p \left(\|f\|^{2n-1} n^{\frac{n}{2}} \binom{n-1}{\lfloor \frac{n-1}{2} \rfloor}^n 2^{\frac{n(n-1)}{2}} \right)}{\deg g} \right\rceil$
$l \leftarrow 0$
Tant que $2^l < k$ **Faire**
  $g, h, u, v \leftarrow$HENSEL(f, g, h, u, v)
  $l \leftarrow l + 1$
Fin Tant que
$R \leftarrow$réseau (4)
$B \leftarrow$LLL(R)
$g_0 \leftarrow \text{pgcd}(B_1, f)$
Si $g_0 = 1$ **Alors**
  Retourner f
Sinon
  Retourner g_0
Fin Si

Preuve :

▶ Montrons étape par étape que la complexité est polynomiale en les données.

Le calcul du résultant se fait par pivot de Gauss et sa valeur a un logarithme de l'ordre de $3n \log n + 2n(\log \|f\|)$.

Le calcul de p est lui aussi linéaire d'après la proposition 5.1.1. BERLEKAMP s'exécute en $O(p \times n^3)$, ce qui absorbe le temps demandé par EUCLIDE_ETENDU.

En utilisant la formule de Stirling, on voit que $k \times \log p = O(n^2 + n \log \|f\|)$: la boucle de remontée de HENSEL s'exécute $O(\log n + \log \log \|f\|)$ fois et son corps a une complexité en $O((k \log p)^2 n^2) = O(n^6 \log \|f\|^2)$ ce qui donne une complexité totale[⋆⋆⋆] en $O(n^6 \log n \times \log \|f\|)$.

De toute façon, c'est LLL qui absorbe toute la complexité : en effet, son temps d'exécution est de l'ordre de $O(n^6 \times (k \log p)^3) = O(n^{12} + n^9 (\log \|f\|)^3)$. En effet, les vecteurs du réseau ont une norme de l'ordre de $\sqrt{n} p^k$ et ont donc leur logarithme en $O(k \log p)$ car $\log n$ est négligeable devant k. ◀

6 Comment accélérer l'algorithme

Ce qui précède montre un résultat théorique important, à savoir que le problème de la factorisation des polynômes de $\mathbb{Q}[X]$ est dans la classe **P**. Néanmoins, l'algorithme décrit est loin d'être

⋆⋆⋆. On assimile $\log \log \|f\|$ à une constante.

efficace. En fait, les bornes utilisées dans la section 5 sont trop grandes pour espérer que les calculs, notamment ceux de l'orthogonalisation, soient réalisables rapidement. Voyons quelques améliorations qui accélèrent l'algorithme dans la plupart des cas.

6.1 Précision sur la complexité

Tout d'abord, notons que l'on peut baisser la complexité théorique annoncée en utilisant des algorithmes de multiplication rapide sur les entiers : multiplier deux entiers dont la taille en bits est de l'ordre de s peut être réduit à $O(s^{1+\varepsilon})$ pour tout $\varepsilon > 0$. Ceci permet de revoir la complexité de Lll à la baisse en $O(n^{5+\varepsilon}k^{2+\varepsilon})$ et donc une complexité totale en $O(n^{9+\varepsilon} + n^{7+\varepsilon}(\log \|f\|)^{2+\varepsilon})$. Néanmoins, cette amélioration n'est que théorique car l'efficacité de la multiplication rapide n'est atteinte que pour des entiers de l'ordre de 2^{1000}.

Notons que c'est la complexité au pire que nous avons calculée, en minorant le degré du facteur g par 1. Néanmoins, dans $\mathbb{F}_p[X]$ un polynôme de degré n a en moyenne $\log n$ facteurs irréductibles et on peut donc espérer un facteur g de degré $O\left(\frac{n}{\log n}\right) = O(n^{1-\varepsilon})$. Ceci permet d'obtenir une complexité en $O(n^{8+\varepsilon} + n^7(\log \|f\|)^{1+\varepsilon})$, qui est toujours entièrement déterminée par l'étape Lll.

Néanmoins, la complexité reste relativement élevée et en pratique, on peut trouver des astuces qui font chuter le temps de calcul dans la plupart des cas. La première est celle que l'on vient d'expliquer, qui consiste à chercher un facteur irréductible g pour des petits p tel que son degré soit le plus grand possible. Voyons quelques autres astuces.

6.2 Trouver un facteur non trivial

Deux questions se posent dans le problème de la factorisation : la première est de savoir si le polynôme est irréductible et la deuxième est de trouver un facteur non trivial pour pouvoir ensuite recommencer récursivement la factorisation. Il y a deux endroits dans l'algorithme présenté où l'on peut raisonnablement tester la divisibilité d'un facteur potentiel :

• Tout d'abord, lors de l'algorithme de relèvement de Hensel, il peut apparaître que le facteur considéré reste inchangé. Ainsi si pendant deux étapes du relèvement, le facteur n'est pas modifié, il est raisonnable qu'il s'agisse d'un facteur de f dans $\mathbb{Z}[X]$. Une stratégie de recherche d'un facteur irréductible consiste à relever chaque facteur un nombre de fois déterminé à l'avance [††††] et tester la divisibilité à chaque fois qu'un facteur est laissé inchangé pendant deux étapes.

• Lors du déroulement de Lll, il se peut que le premier vecteur devienne très petit par rapport aux autres : il y a des chances que ce petit vecteur ait en fait un pgcd avec f non trivial.

6.3 Prouver l'irréductibilité

La deuxième question naturelle est de savoir si le polynôme de départ f est irréductible. Evidemment, si en le factorisant dans $\mathbb{F}_p$ on ne trouve qu'un facteur, alors il est clair qu'il est irréductible. Néanmoins, on n'a pas forcément cette chance. L'idée est de factoriser f dans plusieurs $\mathbb{F}_p$ et de confronter les différentes factorisations obtenues.

Prenons un exemple pour montrer l'utilité de la méthode : supposons qu'un polynôme de degré 20 se factorise d'une part en des polynômes irréductibles de degrés 6, 6 et 7 et d'autre part de degrés 4, 6 et 10. Cela nous indique que f a un facteur irréductible de degré au moins 10 mais la première factorisation impose qu'il soit de degré 12. En reprenant la deuxième factorisation on minore son degré par 14 puis avec la première par 20 : f est en fait irréductible.

6.4 Essayer des combinaisons

Avant l'utilisation de Lll, les algorithmes de factorisation commençaient de la même façon. Cependant, après la remontée de Hensel, on teste toutes les combinaisons des facteurs irréductibles modulo p^k afin de trouver ou non un « vrai » facteur du polynôme. D'un point de vue théorique, il

[††††]. 5 paraît être raisonnable.

peut y avoir 2^n combinaisons et l'algorithme est exponentiel. Néanmoins, on peut espérer qu'à cette étape, le polynôme soit « presque » irréductible et que le nombre de combinaisons soit beaucoup plus petit. Dans la pratique, il est souvent plus rapide d'essayer toutes les combinaisons plutôt que d'utiliser LLL.

6.5 Accélérer LLL

Néanmoins, il peut arriver que notre polynôme ait trop de facteurs irréductibles modulo les p que l'on a essayés. Il est alors sage d'appliquer LLL.

Le moyen le plus couramment utilisé pour accélérer LLL est d'une part de modifier l'orthogonalisée de la base au fur et à mesure de l'algorithme, sans tout recalculer à chaque étape et d'autre part d'effectuer les calculs d'orthogonalisation en mode flottant dans un premier temps puis de finir avec des calculs exacts.

Néanmoins, ceci est assez dangereux car les calculs en mode flottant peuvent conduire à faire boucler l'algorithme : imaginons que l'on ait à réaliser le produit scalaire entre un vecteur b_j^* dont les coordonnées soient toutes inférieures à 100 et un vecteur b_i dont les coordonnées soient de l'ordre de 10^{50}. Le calcul en mode flottant donne un résultat avec une précision de l'ordre de 10^{40} qui est très supérieur à la norme du petit vecteur. Ainsi pendant le calcul de $\mu_{ij} = \frac{(b_i, b_j^*)}{(b_j^*, b_j^*)}$ on a seulement une précision que de l'ordre de 10^{40} et il est inconcevable de le comparer à $\frac{1}{2}$. Toutefois, on peut tourner cette situation à notre avantage car comme on l'a expliqué en 6.2, il se peut que $\text{pgcd}(f, b_j)$ soit non trivial.

Bibliographie

[1] A.K. Lenstra, H.W. Lenstra, L. Lovász. Factoring Polynomials with Rational Coefficients. In *Mathematische Annalen*, volume 261, pages 515–534. Springer 1982.

[2] C.K. Yap. *Fundamental Problems of Algorithmic Algebra.* Oxford University Press 2000.

[3] C.W.S. Cassels. *An introduction to the geometry of numbers.* Berlin, Heidelberg, New York : Springer 1971.

[4] J. Gathen, J. Gerhard. *Modern Computer Algebra.* Cambridge University Press 1999.

Parties de $\mathbb{N}$ reconnaissables
Théorème de Cobham

Ivan Boyer

12 février 2007

Table des matières

1 Définitions et notations

Soit A un alphabet fini et $k = |A|$. Grâce à une bijection $f : A \to [\![0,k-1]\!]$ on peut représenter un entier n écrit en base k à l'aide des lettres de A. On sous-entend par représentation, une représentation « propre », c'est-à-dire sans des $f^{-1}(0)$ à gauche des mots. Par exemple, nous écrivons communément les entiers en base 10 à l'aide de l'alphabet $A = \{0, \ldots, 9\}$ par des représentations propres : on n'écrit pas 007 mais simplement 7. Avec ces conventions, on introduit la notion principale :

Définition 1.1 (Ensemble k–rationnels)**.** *Soit $k > 1$.*

Une partie $P \subset \mathbb{N}$ est dite k–rationnelle s'il existe un alphabet A de taille k et un automate qui reconnaisse les entiers de P écrits en base k grâce aux lettres de A.

Pour $k = 1$ on prolonge cette définition en représentant un entier n sur un alphabet unaire, $A = \{a\}$, par le mot a^n. On dira simplement que P est rationnelle, plutôt que 1–rationnelle.

Notons que l'alphabet importe peu pour représenter des entiers en base k. En effet, pour une partie $P \subset \mathbb{N}$ représentée en base k dans deux alphabets A et B on a un morphisme naturel entre les représentations sur A et sur B. Ainsi, dans la suite, on ne mentionnera plus les alphabets. De plus, on assimilera 0 et la lettre représentant 0 dans une base quelconque. Enfin, on utilisera la notation :

Notation 1.2. *Soit P une partie de $\mathbb{N}$. On notera $(P)_k$ l'ensemble de ses représentations en base k.*

Donnons de plus une définition clé pour le théorème de Cobham :

Définition 1.3. *Deux entiers k et l sont dit multiplicativement indépendants s'il n'existe pas d'entiers $n, p > 0$ tels que $k^n = l^p$.*

Remarquons que c'est une notion assez « faible » puisque pour être multiplicativement dépendants il ne suffit pas que les facteurs premiers de l'un soient exactement les facteurs premiers de l'autre. Par exemple, 10 et 20 sont multiplicativement indépendants.

Théorème (Cobham)**.** *Soient k et l multiplicativement indépendants. Une partie $P \subset \mathbb{N}$ est k– et l–rationnelle si et seulement si elle est rationnelle.*

Notons que c'est le sens direct qui constitue généralement ce que l'on entend par théorème de Cobham. Le sens indirect est beaucoup plus facile et sera montré au paragraphe 2.

Exemple 1.1. L'ensemble $\{3, 5, 9, 17, 33, \ldots\}$ n'est certainement pas rationnel car le lemme de l'étoile impose d'avoir un sous ensemble en progression

arithmétique. Comme il est 2–rationnel (c'est 10^*1), il n'est donc pas 10–rationnel.

Rappelons par ailleurs une autre définition classique sur les parties de $\mathbb{N}$:

Définition 1.4. *Une partie $P \subset \mathbb{N}$ est dite ultimement périodique s'il existe des entiers N et $k > 0$ tels que*

$$\forall n \geqslant N,\ n \in P \Leftrightarrow n + k \in P.$$

Notons que toute partie finie est ultimement périodique et qu'une modification d'un nombre fini de nombres n'altère pas le caractère ultimement périodique.

Enfin, la démonstration du théorème de Cobham utilise le résultat suivant de densité :

Théorème 1.1. *Soient k, l deux entiers multiplicativement indépendants. Alors, $\left\{\frac{k^p}{l^q},\ (p,q) \in \mathbb{N}^2\right\}$ est dense dans $\mathbb{R}^+$.*

Pour montrer ce théorème, nous montrons auparavant le lemme suivant :

Lemme 1.2. *Soit α un irrationnel. Alors, l'ensemble $\{p - q\alpha,\ p, q \in \mathbb{N}\}$ est dense dans $\mathbb{R}$.*

Preuve :
▶ Soit $\alpha_n = \frac{p_n}{q_n}$ une suite de rationnels, sous forme irréductible, tendant vers α. Comme α est irrationnel, on peut choisir $(p_n)_{n\in\mathbb{N}}$ et $(q_n)_{n\in\mathbb{N}}$ strictement croissantes. On peut aussi supposer que $0 < \alpha_n - \alpha < \frac{1}{q_n}$. Ainsi, $\beta_n = p_n - \alpha q_n \in [0,1]$. Par Bolzano-Wierstrass, quitte à extraire une sous-suite, on supposera que β_n converge. Dès lors, en considérant $\beta_{n+1} - \beta_n$, on a trouvé $p_n, q_n > 0$ tels que $p_n - q_n\alpha$ converge vers 0, par valeurs positives. Soit $x \in \mathbb{R}^+$ un réel : on va l'approcher à $\epsilon > 0$. Il existe un rang N tel que $0 < p_N - q_N\alpha < \epsilon$ et on peut alors trouver un entier $k_N > 0$ tel que $0 < k_N p_N - k_N q_N \alpha - x < \epsilon$.

Si le réel x à approcher est négatif, on prend $q_0 > 0$ tel que $q_0\alpha > x$ et on approche comme ci-dessus $q_0\alpha - x$. ◀

Notons que quitte à choisir un plus petit ϵ, on peut prendre p_n et q_n aussi grands que l'on veut. Ceci nous sera utile plus tard. Montrons maintenant le théorème :

Preuve (du théorème) :
▶ On a $\frac{\log k}{\log l} = \frac{q}{p} \Leftrightarrow k^p = l^q$. Ainsi, si k et l sont multiplicativement indépendants, alors $\frac{\log k}{\log l}$ est irrationnel. Dès lors, pour $x > 0$, on peut trouver, grâce au lemme précédent, deux entiers p_n et q_n tels que :

$$p_n \log k - q_n \log l - \log x$$

soit aussi petit que l'on veut. ◀

2 Résultats préliminaires

Avant de s'attaquer au théorème de Cobham voyons quelques résultats plus élémentaires sur les parties de $\mathbb{N}$ k–rationnelles.

La première est une conséquence assez intuitive du lemme de l'étoile :

Proposition 2.1. *Une partie $P \subset \mathbb{N}$ est rationnelle si et seulement si elle est ultimement périodique.*

Preuve :

► Le sens indirect s'obtient par la construction évidente de l'automate.

Le sens direct est une conséquence du lemme de l'étoile : soit k le plus petit entier †, tel qu'il existe $n \geqslant 0$ vérifiant $a^n \left(a^k\right)^* \subset P$. Soit X l'ensemble des entiers $n < k$ vérifiant l'inclusion précédente. Alors,

$$P \setminus \bigcup_{n \in X} a^n \left(a^k\right)^*$$

est rationnel. Si jamais il n'est pas fini, on peut de nouveau appliquer le lemme de l'étoile qui fournit un entier $k' \notin k\mathbb{N}$ tel que $a^n \left(a^{k'}\right)^* \subset P$ et le pgcd de k et k' contredit la définition de k ◄

Montrons maintenant le sens indirect du théorème de Cobham :

Proposition 2.2. *Si $P \subset \mathbb{N}$ est rationnelle, elle est k–rationnelle pour $k \geqslant 1$.*

Preuve :

► Pour faciliter la rédaction, on se placera pour la k–rationnalité sur l'alphabet $[\![0,k-1]\!]$. D'après la proposition précédente, il suffit de montrer le résultat pour les ensembles d'entiers qui ont un reste égal à s modulo p. On construit un automate ayant pour ensemble d'états $[\![0,q-1]\!]$. L'état initial est 0 et l'état final s. On met les transitions $q \xrightarrow{a} r$ pour $r \equiv qk + a[p]$. ◄

Exemple 2.1.

Pour illustrer cette proposition, voici ci-contre l'automate construit comme dans la preuve pour la reconnaissance des multiples de 3 en base 10. On remarquera que l'on trouve l'automate basé sur le critère usuel de divisibilité par 3.

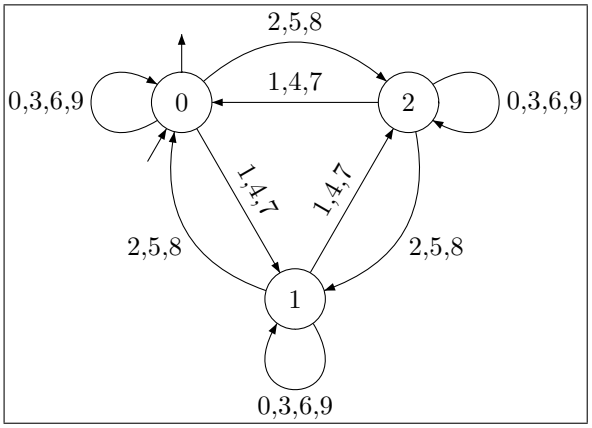


FIGURE 1 – Multiples de 3 en base 10.

†. k existe dès que P est infinie ; le cas P finie est trivial.

Voici enfin une proposition qui illustre l'enjeu des entiers multiplicativement indépendants :

Proposition 2.3. *Une partie $P \subset \mathbb{N}$ est k–rationnelle si et seulement si elle est k^p–rationnelle, pour $p > 0$ arbitraire.*

Preuve :
► Le passage de k^p à k est facile, en ajoutant pour chaque transition des états et transitions intermédiaires pour écrire les « chiffres » de la base k^p en base k.

Supposons que P soit k–rationnelle, reconnue par un automate $\mathcal{A}$. On construit un nouvel automate ayant les mêmes états que $\mathcal{A}$. Pour chaque suite de p transitions entre deux états q et q', on met une transition entre q et q' étiquetée par le chiffre de la base k^p représenté par les p transitions. ◄

Ainsi si k et l sont multiplicativement dépendants alors une partie de $\mathbb{N}$ est k–rationnelle si et seulement si elle est l–rationnelle.

3 Lemmes intermédiaires

La démonstration du théorème de Cobham présentée ci-dessous ‡ est assez longue, divisée en plusieurs lemmes. Le premier utilise la notion de densité à droite :

Définition 3.1. *Soit A un alphabet et L un langage sur A. L est dit dense à droite si tout mot $u \in A^*$ apparaît comme préfixe d'un mot de L.*

Lemme 3.1. *Soit $P \subset \mathbb{N}$ k–rationnelle et infinie. Alors, pour tout entier l multiplicativement indépendant, l'ensemble $0^*(P)_l$ est dense à droite.* ◇

Preuve :
► On peut appliquer le lemme de l'étoile à $(P)_k$ pour trouver $u, v, w \in A^*$ avec $v \neq \varepsilon$ tels que $uv^*w \subset (P)_k$. Soit x une représentation ⋆ en base k d'un entier arbitraire. Il faut montrer que x apparaît comme préfixe d'un mot de $0^*(P)_l$.

Notons n_x, n_u, n_v les entiers représentés respectivement par x, u et v. Notons $g = |v|$ et $h = |w|$. D'après le théorème 1.1 appliqué aux entiers k^g et l, on peut trouver p et q tels que :

$$\frac{n_x + \frac{1}{4}}{k^h} < \left(n_u + \frac{n_v}{k^g - 1}\right) \frac{k^{gp}}{l^q} < \frac{n_x + \frac{1}{2}}{k^h}$$

‡. due à G. Hansel.
◇. Les 0 ne sont là que pour les représentations impropres.
⋆. Pas forcément la représentation propre.

Notons, comme on l'a déjà dit dans le lemme 1.2, que l'on peut prendre p et q aussi grands que l'on veut. On peut donc choisir q suffisamment grand pour que :

$$-\frac{1}{4} < \frac{n_w - \frac{k^h n_v}{k^g-1}}{l^q} < \frac{1}{2}.$$

En remarquant que la quantité :

$$\left(n_u + \frac{n_v}{k^g-1}\right) k^{gp+h} + n_w - \frac{k^h n_v}{k^g-1} = n_u k^{pg+h} + n_v \frac{k^{gp}-1}{k^g-1} k^h + n_w$$
$$= n_u k^{pg+h} + \left(k^h \sum_{i=0}^{p-1} n_u k^{gi}\right) + n_w$$

n'est autre que l'entier représenté par $uv^p w$ (noté $n_{uv^p w}$), on obtient, en sommant les deux inégalités :

$$n_x l^q < n_{uv^p w} < (n_x+1) l^q.$$

Ceci montre l'existence de $j \in [\![1, l^q - 1]\!]$ tels que $n_x l^q + j = n_{uv^p w} \in P$. Ainsi x est bien le préfixe d'un mot de $(P)_l$, à savoir $uv^p w$. ◀

Pour le lemme suivant, on introduit une nouvelle notion :

Définition 3.2. *On dira qu'une partie non vide $P \subset \mathbb{N}$ est presque-périodique de période $d > 0$ si pour tout $x \in P$ on peut trouver $y \in P$ tels que $x < y \leqslant x + d$.*

Remarquons que si P est *presque-périodique* de période $d > 0$ alors, tout intervalle d'entiers supérieurs à $\min P$ de longueur d contient au moins un élément de P.

Lemme 3.2. *Soit $P \subset \mathbb{N}$ k–rationnelle. P est presque-périodique si et seulement si $0^*(P)_k$ est dense à droite.*

Preuve :

▶ Le sens direct n'utilise pas l'hypothèse : soit $n \in \mathbb{N}$ et u sa représentation propre en base k. Soit d la *presque-période* de P et p son nombre de lettres une fois écrite en base k. Il existe $p' \geqslant p$ tel que $k^{p'} \geqslant \min P$: on peut trouver $m \in P$ tel que $nk^{p'} < m < (n+1)k^{p'}$.

Le sens indirect est aussi rapide : pour tout n, il existe deux entiers p et $t < k^p$ tels que $nk^p + t \in P$. On note q le nombre d'états d'un automate reconnaissant $(P)_k$. Une fois que l'automate a lu u (représentant n), l'existence de t montre que l'on peut atteindre un état final. Comme on peut le faire sans repasser deux fois par le même état, on peut prendre $p \leqslant q$ et donc P est *presque-périodique*, de période k^q. ◀

Ceci montre déjà une version faible du théorème de Cobham, à savoir :

Proposition 3.3. *Soit $P \subset \mathbb{N}$ infini. Si P est k–rationnelle et l–rationnelle, pour k et l multiplicativement indépendants, alors P est presque périodique.*

Il nous faut donc étudier un peu plus les parties de $\mathbb{N}$ *presque-périodiques*. Voici un lemme, surtout technique, sur ces parties *presque-périodiques* :

Lemme 3.4. *Soit $P \subset \mathbb{N}$ presque-périodique de période d. Pour tout entier K, L et h, et pour tout réel $\eta > 0$ vérifiant $K < L < K + \eta$, il existe $x \in P$ et $y \in \mathbb{N}$ tels que :*

$$yL \leqslant xK + h \leqslant yL + \eta d.$$

Preuve :
► Soit $r = \min\{p \in \mathbb{N},\ pL > pK + h\}$. Soit $i \in [\![1,r-1]\!]$. On a d'une part $(r-i)L < (r-i)K + h$ et d'autre part :

$$(r-i)K + h = rK + h - iK < rL - iK < rL - iL + i\eta = (r-i)L + \eta i.$$

Remarquons que pour $i \geqslant r$ ces inégalités restent vraies. Soit j un entier vérifiant $jK + r - d \geqslant 0$ et $jL + r - d \geqslant \min P$. En ajoutant jKL aux différentes inégalités, on a finalement pour tout $i \in [\![1,d]\!]$:

$$(jK + r - i)L < (jL + r - i)K + h < (jK + r - i)L + \eta d.$$

Comme P a d comme *presque-période* alors, il existe un $i \in [\![1,d]\!]$ tel que $x := jL + r - i \in P$. En notant enfin $y := jK + r - i$, on a le résultat annoncé. ◄

Introduisons maintenant une notion clé dans cette preuve du théorème de Cobham :

Définition 3.3 (Facteurs récurrents)**.** *Soit x un mot infini et w un facteur de x c'est-à-dire $x = awb$. S'il existe une infinité de tels couples (a, b) vérifiant cette relation, le facteur w est dit récurrent.*
De plus, on dira qu'un mot $x_0x_1\ldots$ est ultimement périodique[††] *si :*

$$\exists N, p \in \mathbb{N}, \forall n \geqslant N,\ x_n = x_{n+p}.$$

Le lien entre les deux notions de cette définition est énoncé dans le lemme suivant :

Lemme 3.5. *Un mot x est ultimement périodique si et seulement si on peut trouver un entier $n > 0$ tel que x ait au plus n facteurs récurrents de longueur n.*

Preuve :
► Le sens direct est assez immédiat puisque pour un un mot ultimement périodique de période p, le nombre de facteurs récurrents de longueur p est bien au plus p.

††. On utilise le même vocabulaire car il n'y a pas d'ambiguïté possible.

Soit $r(n)$ le nombre de facteurs récurrents de longueur n. Chacun de ces facteurs apparaît une infinité de fois dans x et comme l'alphabet est fini, il y a encore une infinité de positions où le facteur est suivi d'une même lettre. Ainsi, $r(n) \leqslant r(n+1)$. Par hypothèse, il existe un plus petit entier $n_0 \geqslant 1$ tel que $r(n_0) = n_0$. Si $n_0 = 1$, le mot est constant à partir d'un certain rang et donc ultimement périodique. Sinon $n_0 \geqslant 2$. On a alors $r(n_0 - 1) = n_0$. Ainsi, au bout d'un moment, chaque facteur de longueur $n_0 - 1$ est suivi d'une unique lettre ne dépendant que du facteur : pour n assez grand et $w = x_n \dots x_{n+n_0-2}$ facteur récurrent, x_{n+n_0-1} est déterminé uniquement par w et $w' = x_{n+1} \dots x_{n+n_0-1}$ est encore un facteur récurrent qui détermine parfaitement x_{n+n_0}. On conclut ainsi que x est ultimement périodique.

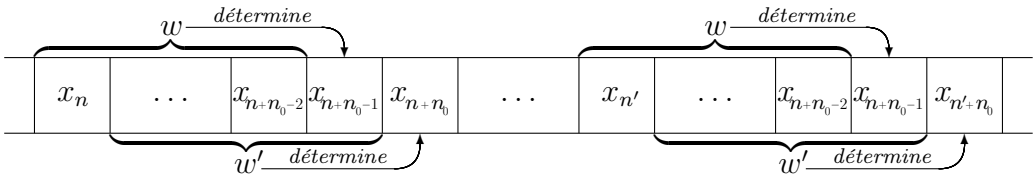


FIGURE 2 – x est ultimement périodique de période $n' - n$.

◀

4 Théorème de Cobham

Nous avons maintenant les outils nécessaires pour pouvoir prouver le sens direct le théorème de Cobham

Théorème (Cobham)**.** *Une partie $P \subset \mathbb{N}$ k– et l–rationnelle est rationnelle dès que k et l sont multiplicativement indépendants.*

Preuve :

▶ L'ensemble $E_{tj} = \{y,\ yk^j + t \in P\}$ est k–rationnel et aussi l–rationnel. En effet, la constante t n'affecte qu'un nombre fini d'états sur la droite et la division par k^j s'effectue classiquement en rajoutant une sortie sur les transitions de l'automate.

Ainsi, pour tout entier n, représenté en base k par un mot u, l'ensemble des entiers ayant une écriture en base k dans $(P)_k u^{-1} = \{v,\ vu \in (P)_k\}$ est l–rationnel, puisqu'il s'agit de $E_{n|u|}$

Soit $\sim$ la relation d'équivalence sur $\mathbb{N}$ définie par $x \sim y$ si et seulement si $(x)_k^{-1}(P)_k = (y)_k^{-1}(P)_k$. Notons que l'on a la propriété

$$x \sim y \Rightarrow xk^j + t \sim yk^j + t \tag{1}$$

pour tout j et tout t tels que $t < k^j$. Remarquons aussi que :

$$x \sim 0 \Leftrightarrow (x)_k^{-1}(P)_k = (P)_k \Leftrightarrow x \in P. \tag{2}$$

On vérifie facilement que la classe d'un entier x a pour représentation en base k :

$$([x]_\sim)_k = \left(\bigcap_{u \in (x)_k^{-1}(P)_k} (P)_k u^{-1} \right) \bigcap \left(\bigcap_{u \notin (x)_k^{-1}(P)_k} {}^c\big((P)_k u^{-1}\big) \right).$$

Comme le nombre de quotients à droite est fini, les classes d'équivalence de $\sim$ sont l–rationnelles.

Dès lors, pour chacune de ces classes écrite en base l, le nombre de quotients à droite est fini et on peut donc raffiner la relation $\sim$ en $\approx$ ayant toujours un nombre fini de classes, que l'on note c, telle que :

$$x \approx y \Rightarrow xl^j + t \approx yl^j + t \tag{3}$$

pour tout j et tout t tels que $t < l^j$.

On numérote alors les classes modulo $\sim$ et on note $num([k]_\sim)$ le numéro de la classe de k modulo $\sim$. On considère le mot infini R défini par $R_n = num([n]_\sim)$.
Soit w un facteur récurrent de longueur 2 et $P_w = \{n,\ R_n R_{n+1} = w\}$. P_w est k– et l–rationnel (en utilisant un automate produit où les transitions sont celles de la classe w_0, doublées de celle de la classe w_1). Ainsi, d'après le lemme 3.3, P_w est *presque-périodique* de période d_w : chaque occurrence de w est suivi d'une autre dans un intervalle d'au plus d_w. Comme le nombre de facteurs récurrents de longueur 2 est fini, on peut définir $d = \max d_w$. Soit alors ϵ un réel vérifiant $0 < \epsilon < 1$ ainsi que $c\frac{\epsilon}{1-\epsilon} < \frac{1}{2}$. Grâce théorème 1.1 on trouve deux entiers p et q tels que :

$$1 < \frac{l^q}{k^p} < 1 + \frac{\epsilon}{d}.$$

Soit maintenant $K = k^p$, $L = l^q$ et $m = \lfloor K(1-\epsilon) \rfloor$. Nous avons besoin d'un dernier lemme :

Lemme 4.1. *Soit w un facteur récurrent de longueur m de R. Il existe un entier y tel que $R_{yL} \dots R_{(y+1)L-1} = swt$ et $|s| \leqslant \epsilon K$.*
Preuve :
▶ Il existe une infinité d'entiers x tel que $R_{xK} \dots R_{(x+2)K-1}$ ait w pour facteur. On peut de plus imposer que w commence toujours à la même position. Notons que la relation $\sim$ vérifie la propriété 1 et donc que le sous mot $R_{xK} \dots R_{(x+2)K-1}$ est entièrement défini par le facteur $R_x R_{x+1}$ et par K. Parmi tous les facteurs $R_x R_{x+1}$, il y en a nécessairement un qui est récurrent : on est en mesure de construire une suite strictement croissante $(x_n)_{n\in\mathbb{N}}$ vérifiant :

$$\begin{cases} \forall n,\ x_{n+1} - x_n \leqslant d \\ R_{x_n K} \dots R_{(x_n+2)K-1} = w'_n w w''_n \end{cases}$$

avec $|w'_n| = h$ constant. On peut maintenant utiliser le lemme 3.4 avec h ainsi défini, $\eta = K\frac{\epsilon}{d}$ et l'ensemble P *presque-périodique*‡‡. On vérifie que l'on a bien $K < L < K + \eta$. On a donc l'existence d'un entier y tel que $yL < xK + h < yL + \eta d < (y+1)L$. Ainsi, on a :

$$R_{yL} \dots R_{(y+1)L-1} = swt$$

avec $|s| < yL + \eta d - yL$. La figure suivante aide à se retrouver parmi tous ces indices.

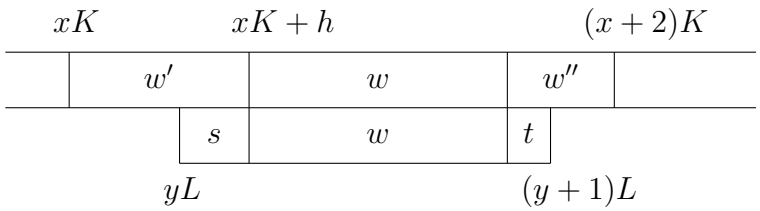


FIGURE 3 – Localisation de w. ◀

Les facteurs de la forme $R_{yL} \dots R_{(y+1)L-1}$ seraient parfaitement définis par R_y et L si $\sim$ possédait la propriété 3. Or $\approx$ possède précisément cette propriété. Ainsi, il y a au plus c possibilités de facteurs $R_{yL} \dots R_{(y+1)L-1}$, correspondants à la classe de R_y modulo $\approx$. Comme L ne dépend pas de w, un majorant du nombre de facteurs récurrents de R de longueur m est donné par un facteur de la forme $R_{yL} \dots R_{(y+1)L-1}$ ainsi que par le point de départ de w dans ce facteur. Ce point de départ étant fourni par $|s|$, on a donc au plus

$$\epsilon K \times c \leqslant \frac{1}{2}K(1-\epsilon) \leqslant \frac{1}{2}(m+1) \leqslant m$$

facteurs récurrents de R de longueur m. Ainsi, d'après le lemme 3.5, le mot R est ultimement périodique. Or, vu la propriété 2, P est précisément la classe de 0 modulo $\sim$ c'est-à-dire $P = \{n,\ R_n = num([0]_\sim)\}$. Ainsi, il est clair que P est elle-même ultimement périodique, ce qui veut dire, d'après la proposition 2.1 que P est rationnelle. ◀

5 Autres résultats de reconnaissabilité

5.1 Reconnaissance par substitution

La notion de partie k–rationnelle peut être définie d'une autre façon à l'aide de morphismes substitutifs.

‡‡. D'après la proposition 3.3

Définition 5.1. *Une (k–)substitution est un morphisme $\alpha : A \to A^k$ tel qu'au moins une lettre $a \in A$ soit la première lettre de $\alpha(a)$. Un point fixe de α est un mot infini, w, tel que $\alpha(w) = w$.*

Notons que pour chaque lettre $a \in A$ qui est la première lettre de $\alpha(a)$ il existe un unique point fixe w commençant par a, à savoir $\alpha^\omega(a)$. Nous avons la proposition suivante :

Proposition 5.1. *Une partie $P \subset \mathbb{N}$ est k–rationnelle si, et seulement si, il existe un alphabet fini A et une k–substitution ayant un point fixe w tel que :*

$$P = \bigcup_{a \in A_P} \{n \geqslant 0,\ w_n = a\}$$

où $A_P \subset A$ est la partie de A qui "détermine" P.

Preuve :
▶ Supposons P k–rationnelle sur l'alphabet $[\![0,k-1]\!]$, reconnue par un automate déterministe complet (Q, q_i, T, F). On considère la substitution α définie sur l'alphabet Q par $\alpha(q) = s_0 \dots s_{k-1}$ avec $s_0 = q$ et $q \xrightarrow{i} s_i$. On considère le point fixe $w = \alpha^\omega(q_i)$. Pour un entier n écrit en base k $n_0 \dots n_p$, la lettre $w_{[n_0 \dots n_j]}$ représente[◇◇] l'état dans lequel se trouve l'automate après avoir lu les $j+1$ premières lettres. On a donc :

$$w_n \in F \Leftrightarrow n \in P.$$

Pour la réciproque, on construit l'automate suivant le morphisme selon le schéma montré ci-dessus. ◀

Exemple 5.1. La 2–substitution α définie par $\alpha(a) = ab$ et $\alpha(b) = ba$ a pour point fixe m, le mot de Thue-Morse et l'on vérifie facilement que $\{n, m_n = a\}$ est 2–rationnel.

5.2 Morphismes substitutifs primitifs

Ces morphismes substitutifs donnent lieu à un autre résultat similaire au théorème de Cobham. Ici, les morphismes substitutifs seront à valeurs non pas dans A^k mais dans A^*.

Définition 5.2. *Pour un tel morphisme α on note M_α la matrice carrée définie par $m_{ij} = |\alpha(j)|_i$, c'est-à-dire le nombre d'occurrences de la lettre i dans le mot $\alpha(j)$. Le morphisme α est dit primitif si une puissance de M_α a tous ses coefficients strictement positifs.*

La multiplication de telles matrices est compatible avec la composition des

◇◇. On note $[n_0 \dots n_j] = \sum_{i=0}^{j} n_i k^{j-i}$.

morphismes. Ainsi, d'après le théorème de Perron-Frobenius, un morphisme primitif a une matrice possédant une valeur propre simple et réelle λ, de module strictement plus grand que les autres, possédant un vecteur propre de composantes strictement positives. Le morphisme est alors dit *λ–primitif substitutif*. On a le théorème suivant :

Théorème 5.2. *Soit x un mot infini point fixe de deux morphismes λ– et κ–primitifs substitutifs. Si x n'est pas ultimement périodique alors λ et κ sont multiplicativement dépendants.*

Ce théorème peut d'une certaine manière être vu comme une généralisation du théorème de Cobham. Soit en effet une partie $P \subset \mathbb{N}$ k– et l–rationnelle. Considérons les morphismes substitutifs α_k et α_l définis comme dans la preuve de la proposition 5.1. Les deux points fixes associés, sur les alphabets K et L, peuvent être reliés par un morphisme lettre à lettre φ, pourvu que $\varphi(K_P) \subset \varphi(L_P)$ et $\varphi({}^cK_P) \subset \varphi({}^cL_P)$. On suppose maintenant que les deux morphismes sont primitifs. Alors, ils sont respectivement k– et l– primitifs substitutifs. En effet, la somme des éléments sur une ligne de ${}^tM_K$ est égale à k qui est donc une valeur propre pour le vecteur $(1, \ldots, 1)$. Soit μ une autre valeur propre et $n = |A|$. μ est aussi une valeur propre de ${}^tM_K = \left(m'_{ij}\right)$. Soit $(x_1, \ldots, x_n)$ un vecteur propre associé. Pour tout i on a :

$$\sum_{j=1}^{n} m'_{ij} x_j = \mu x_i.$$

En sommant sur i on obtient $k \sum x_i = \mu \sum x_i$. Si μ est la valeur propre dominante alors $\sum x_i \neq 0$ et $k = \mu$. Ceci montre que k est la valeur propre dominante. Le théorème de Cobham donne, dans ce cas, le même résultat que le théorème 5.2.

Bibliographie

[1] D. Perrin. Finite Automata. In *Handbook of Theoretical Computer Science*, volume B, chapter 1, pages 1–57. 1990.

[2] F. Durand. Sur les ensembles d'entiers reconnaissables. In *Journal de Théorie des Nombres de Bordeaux*, pages 65–84. 1998.

La référence majeure utilisée ici est la première, qui contient une bibliographie très complète. La deuxième référence concerne la dernière section.

Algorithmique
Multiplication efficace de matrices

Ivan Boyer

14 janvier 2007

1 Multiplication matricielle par la méthode de Strassen

1.1 Algorithme

Rappelons tout d'abord l'algorithme récursif de Strassen en mettant en avant l'utilisation de la mémoire. Cet algorithme, basé sur le paradigme divisé pour régner, utilise la multiplication « naïve »des matrices, Mult, lorsqu'une des matrices a une dimension égale à 1. Nous supposerons qu'avant l'appel de Strassen les tailles des matrices utilisées sont « suffisamment » divisibles par 2.

Algorithme 1 Strassen(M, N, P) — Calcule $M \times N$ et place le résultat dans P.

Si $A_1 \to li = 1$ **ou** $A_1 \to co = 1$ **ou** $A_2 \to co = 1$ **Alors**
  $P \leftarrow$ Mult(M,N)
Sinon
  allouer $T_1,\ T_2,\ T_3$ #(*de tailles moitié de M, resp. N resp. P*)
  $T_1 \leftarrow M_{11} + M_{22}$; $T_2 \leftarrow N_{11} + N_{22}$; Strassen(T_1,T_2,T_3) ; $P_{11} \leftarrow T_3$; $P_{22} \leftarrow T_3$
  $T_1 \leftarrow M_{21} + M_{22}$; $T_2 \leftarrow N_{11}$; Strassen(T_1,T_2,T_3) ; $P_{21} \leftarrow T_3$; $P_{22} \leftarrow P_{22} - T_3$
  $T_1 \leftarrow M_{11}$; $T_2 \leftarrow N_{12} - N_{22}$; Strassen(T_1,T_2,T_3) ; $P_{12} \leftarrow T_3$; $P_{22} \leftarrow P_{22} + T_3$
  $T_1 \leftarrow M_{22}$; $T_2 \leftarrow N_{21} - N_{11}$; Strassen(T_1,T_2,T_3) ; $P_{11} \leftarrow P_{11} + T_3$; $P_{21} \leftarrow P_{21} + T_3$
  $T_1 \leftarrow M_{11} + M_{12}$; $T_2 \leftarrow N_{22}$; Strassen(T_1,T_2,T_3) ; $P_{11} \leftarrow P_{11} - T_3$; $P_{12} \leftarrow P_{12} + T_3$
  $T_1 \leftarrow M_{21} - M_{11}$; $T_2 \leftarrow N_{11} + N_{12}$; Strassen(T_1,T_2,T_3) ; $P_{22} \leftarrow P_{22} + T_3$;
  $T_1 \leftarrow M_{12} - M_{22}$; $T_2 \leftarrow N_{21} + N_{22}$; Strassen(T_1,T_2,T_3) ; $P_{11} \leftarrow P_{11} + T_3$;
  libérer $T_1,\ T_2,\ T_3$
Fin Si

Tout l'avantage de cet algorithme repose sur une astuce de calcul qui permet d'effectuer 7 multiplications matricielles au lieu de 8. Voyons maintenant la complexité en temps de la méthode de Strassen, pour la multiplication de matrices de tailles $m \times n$ et $n \times p$, où l'on supposera que m, n et p sont des puissances de deux.

1.2 Complexité en temps

Soit $T(m, n, p)$ le coût en multiplications et additions de l'algorithme de Strassen. Le coût de reconstruction et des additions matricielles en dehors des appels récursifs est en $O(mn + np + mp)$. On a donc la relation de récurrence, pour C constante :

$$T(m, n, p) \leqslant 7T\left(\frac{m}{2}, \frac{n}{2}, \frac{p}{2}\right) + C(mn + np + mp)$$

Par une résolution classique on obtient :

$$T(m, n, p) = O\left(\frac{mn + np + mp}{\min(m, n, p)^2}\big(\min(mn + np + mp)\big)^{\log(7)}\right)$$

On vérifie que pour $m = n = p$, on retrouve le résultat habituel. De plus, dans le cas où $\min(m, n, p)$ est une puissance de 2 divisant les autres dimensions, on peut montrer que le nombre cumulé d'additions et multiplications est, en notant $r = \min(m, n, p) = 2^k$:

$$\frac{1}{3}\left(7^k - r^2\right)\left(5\frac{m}{r} + 5\frac{mp}{r^2} + 8\frac{p}{r}\right) + 7^k\frac{mp}{r^2}$$

Cette complexité est asymptotiquement meilleure que celle du calcul naïf, mais malgré tout, pour des dimensions assez petites, la constante cachée dans le « O »influe beaucoup. Par exemple, voyons pour $m = n = p = 2^k$, le nombre d'additions et de multiplications effectuées par les deux algorithmes :

$$\begin{aligned} add_{naif}(k) &= 2^{2k}(2^k - 1) \\ add_{Strassen}(k) &= 7add_{Strassen}(k-1) + 18 \times 2^{2k-2} = 6\left(7^k - 4^k\right) \\ mult_{naif}(k) &= 2^{3k} = 8^k \\ mult_{Strassen}(k) &= 7mult_{Strassen}(k-1) = 7^k \end{aligned}$$

Dans le cas où le coût de l'addition est négligeable devant celui de la multiplication, l'algorithme de Strassen est toujours plus performant. Sinon, il faut que $n \geqslant 1024$ ($k \leqslant 10$) pour que le coût cumulé en additions et multiplications soit meilleur. Voici ci-dessous la courbe montrant la différence entre le nombre d'opérations de l'algorithme naïf et de l'algorithme de Strassen.

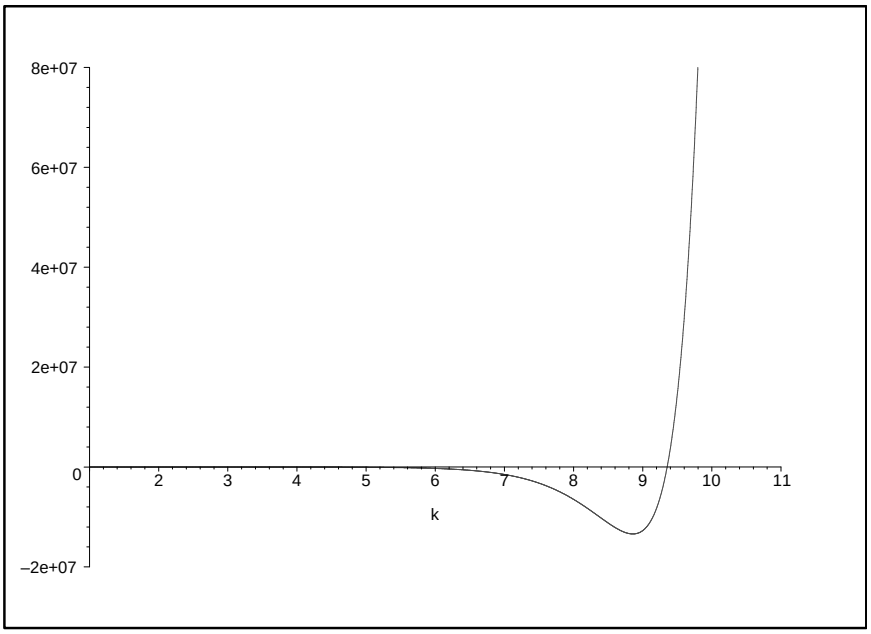


FIGURE 1 – Différence des coûts.

1.3 Complexité en espace

La complexité en espace de l'algorithme de Strassen est toujours plus mauvaise que celle de l'algorithme naïf.

Tout d'abord deux possibilités s'offrent à nous pour implanter la récursivité : la première consiste à rajouter une ligne et/ou une colonne pour obtenir des tailles paires : ceci entraîne de réallouer la mémoire à chaque fois qu'une des dimensions est impaire ainsi qu'une recopie des données. La deuxième solution consiste à recopier une seule fois au début les matrices initiales dans des matrices aux dimensions « suffisamment » divisibles par 2 : la plus petite des dimensions est augmentée en une puissance de 2 et les autres sont augmentées en le plus petit entier divisible par cette puissance. Ceci peut entraîner, dans le pire des cas, un surcroît de mémoire dans un facteur 4.

Un autre problème de l'algorithme est la gestion de la mémoire : néanmoins, il n'est pas si problématique. Comme le montre l'algorithme 1, les calculs intermédiaires peuvent s'effectuer en allouant trois tableaux de dimensions deux fois plus petites. Dans le cas où $m = n = p = 2^k$, on peut

évaluer facilement la mémoire utilisée :

$$M(n) = M\left(\frac{n}{2}\right) + \frac{3}{4}n^2 = O(n^2)$$

En effet, à la fin de chaque appel de la fonction, on libère l'espace alloué aux trois tableaux, ce qui fait que les sept appels récursifs peuvent se resservir de la mémoire allouée. Néanmoins, le nombre d'allocations en mémoire est, lui, de l'ordre de $O\left(n^{\log(7)}\right)$ ce qui augmente la constante dans la complexité en temps et mitige d'autant plus l'utilisation de l'algorithme pour les petites matrices.

2 Calcul du parenthésage

Par un algorithme dynamique, on peut déterminer le coût optimum de la multiplication d'une série de matrices : on met simplement en œuvre l'idée intuitive récursive. Pour effectuer $A_i \times \ldots \times A_j$, il suffit de déterminer un indice $k \in [\![i, j-1]\!]$ tel que le parenthésage $(A_i \times \ldots \times A_k)(A_{k+1} \times \ldots \times A_j)$ soit optimal. En faisant varier i et j dans le bon ordre, on peut utiliser les calculs déjà effectués :

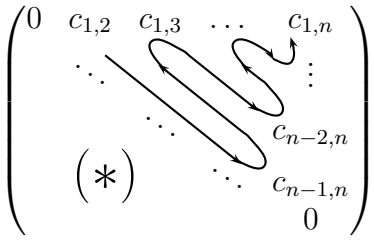


FIGURE 2 – L'ordre de parcours dans l'algorithme dynamique.

Néanmoins, cet algorithme ne donne pas explicitement le bon parenthésage. Pour cela, il suffit de créer un autre tableau (appelé dans la suite *optimum*) de taille $n \times n$ qui à la case d'indice (i, j), $i < j$ redonne le k optimal du parenthésage. Dès lors, on peut effectivement se servir de ce parenthésage en l'affichant ou en calculant le produit :

Algorithme 2 CALCUL-PARENTHÉSÉ(*matrices,optimum,i,j*) — Calcule $A_i \times \ldots \times A_j$.

```
Si i = j Alors
  retourner matrices[i]
Sinon
  k ← optimum[i, j]
  M ← CALCUL-PARENTHÉSÉ(matrices,optimum,i,k)
  N ← CALCUL-PARENTHÉSÉ(matrices,optimum,k+1,j)
  retourner MULTIPLIER(M, N)
Fin Si
```

Finissons en rappelant les complexités de l'algorithme de parenthésage : la complexité en temps est cubique (trois boucles **pour** imbriquées) et la complexité en espace est quadratique, puisqu'il faut créer deux tableaux (les coûts et l'optimum) de taille $n \times n$.

Enfin, le nombre d'appels récursifs de CALCUL-PARENTHÉSÉ est linéaire en le nombre de matrices à multiplier (car l'appel de MULTIPLIER n'est effectué que $n-1$ fois). En le modifiant légèrement, on peut faire en sorte de ramener ce nombre d'appels en dessous de n.

3 Comparaisons avec l'algorithme naïf

Déjà dans les calculs théoriques de complexité, nous avons vu que l'algorithme de Strassen n'était pas aussi efficace que l'on pouvait l'espérer. Le tableau 1 ci-après regroupe des temps moyens d'exécution (sur 10 tirages) obtenus lors de la multiplication de deux matrices carrées aléatoires de dimensions fixées à une puissance de deux [†].

†. Afin que STRASSEN ne soit pas pénalisé par l'augmentation des dimensions.

Tailles	2^8	2^9	2^{10}	2^{11}
Srassen	1.81	12.67	89.83	621.70
Naïf	0.25	2.12	65.77	536.93

TABLE 1 – Problème de l'algorithme de Strassen.

A partir de 2^{10} on observe que les deux algorithmes ont des temps d'exécution comparables, ce qui semble en accord avec ce que l'on a dit précédemment (voir figure 1).

Ceci incite à modifier l'algorithme de Strassen en utilisant un paramètre N qui représente la dimension des matrices en deçà de laquelle on fait appel à l'algorithme naïf. Voici dans le tableau 2 un comparatif des temps d'exécution en faisant varier ce paramètre.

Tailles / Algorithmes		256 (2^8)	512 (2^9)	1024 (2^{10})	2048 (2^{11})
Naïf		0.25	2.12	65.77	536.93
Strassen	N=1	1.81	12.67	89.83	621.70
	N=2	0.74	5.24	36.80	257.15
	N=4	0.41	2.91	20.42	160.72
	N=8	0.28	1.94	13.72	96.12
	N=16	0.21	1.52	10.68	75.11
	N=32	0.19	1.34	9.50	66.76
	N=64	0.18	1.33	9.32	65.67
	N=128	0.23	1.61	11.33	79.46

TABLE 2 – Amélioration de l'algorithme de Strassen.

Ce tableau montre clairement l'utilité du paramètre N, qui permet l'implantation d'un algorithme effectivement plus efficace. Notons de plus que ce paramètre joue à la fois sur l'efficacité en temps, mais aussi sur l'efficacité en mémoire : la plus petite des tailles ne doit plus simplement être une puissance de 2, mais simplement suffisamment divisible par 2 (de la forme $p2^i$ où $p \leqslant N$).

Pour la machine sur laquelle ces comparatifs ont été effectués, il semble intéressant de prendre comme paramètre $N = 64$. Notons que ceci dépend beaucoup du matériel, notamment de la mémoire cache. C'est, semble-t-il, la raison du temps anormalement élevé d'exécution de l'algorithme naïf entre les tailles 512 et 1024. Notons par ailleurs que dans les domaines testés pour N, l'algorithme naïf n'a pas ce problème et donc l'algorithme de Strassen dépend moins des limites de la mémoire cache (les temps d'exécution d'une colonne à l'autre sont bien multipliés par un facteur de l'ordre de 7 pour l'algorithme de Strassen).

Finissons par comparer les multiplications ‡ avec le parenthésage gauche et le parenthésage calculé par l'algorithme dynamique. Ici, les temps d'exécution pour des paramètres donnés varient beaucoup puisque les tailles des matrices sont générées aléatoirement : ils ne sont là qu'à titre de comparatif.

Paramètres				Parenthésage	
nb [a]	inf [b]	sup [c]	N	Optimal	Naïf
50	1	512	64	0.28	17.81
100	1	512	64	0.34	15.24
200	1	512	64	0.61	47.05
50	1	1024	64	2.86	27.28
100	1	1024	64	6.21	103.35

a. Nombre de matrices
b. Taille minimale
c. Taille maximale

TABLE 3 – L'efficacité du parenthésage.

‡. En utilisant l'algorithme de Strassen.