Résumé en Français et résultats principaux

1 Introduction et motivations

1.1 La complexité bilinéaire de la multiplication dans les corps finis

Soit K un corps et $\mathcal{A}$ une K-algèbre (associative, commutative et unitère) de dimension finie. La loi de multiplication dans $\mathcal{A}$, $m_{\mathcal{A}}$, est vue comme une application K-bilinéaire:

$$m_{\mathcal{A}} : \quad \begin{array}{l} \mathcal{A} \times \mathcal{A} \longrightarrow \mathcal{A} \\ (X, Y) \longmapsto X \cdot Y \end{array} \tag{1.1}$$

Definition 1.1. Soit n un entier, un *algorithme de multiplication (non nécessairement symétrique) de longueur n dans $\mathcal{A}$* est la donnée de $2n$ formes linéaires $(\phi_i)_{i=1,\dots n}$, $(\phi'_i)_{i=1,\dots n}$ sur $\mathcal{A}$, ainsi que de n éléments $(w_1, \dots, w_n)$ de $\mathcal{A}$, tels que $m_{\mathcal{A}}$ est égal à

$$m_{\mathcal{A}} : (x, y) \longmapsto \sum_{i=1}^{n} \phi_i(x) \cdot \phi'_i(y) \cdot w_i \ . \tag{1.2}$$

L'algorithme est en outre dit *symétrique* si et seulement si $\phi_i = \phi'_i$ pour tout i.

La *complexité bilinéaire (non nécessairement symétrique)* de la multiplication $m_{\mathcal{A}}$ dans $\mathcal{A}$, notée $\mu(\mathcal{A}/K)$, est le plus petit entier n tel qu'il existe un algorithme de multiplication (non nécessairement symétrique) de longueur n. La *complexité bilinéaire symétrique* $\mu^{\mathrm{sym}}(\mathcal{A}/K)$ est définie de même.

Definition 1.2. Soit q une puissance d'un nombre premier et $\mathbf{F}_{q^n}[y]/y^l$ l'algèbre de polynômes sur $\mathbf{F}_q$ modulo y^l. La complexité bilinéaire symétrique de la multiplication dans $\mathbf{F}_{q^n}[y]/y^l$ est notée $\mu_q^{\mathrm{sym}}(n,l)$, tandis que $\mu_q(n,l)$ désigne la complexité bilinéaire (non nécessairement symétrique).

En particulier,

$$\mu_q^{\mathrm{sym}}(m) = \mu_q^{\mathrm{sym}}(m,1)$$

est la *complexité bilinéaire symétrique de la multiplication dans les extensions de corps finis* $\mathbf{F}_{q^m}/\mathbf{F}_q$, et de même $\mu_q(m)$ désigne la complexité bilinéaire.

Definition 1.3. Soit q une puissance d'un nombre premier, on définit:

$$m_q = \liminf_{n\to\infty} \frac{1}{n}\mu_q(n)$$
$$M_q = \limsup_{n\to\infty} \frac{1}{n}\mu_q(n)$$

ainsi que leurs analogues symétriques m_q^{sym} et M_q^{sym}.

D'autres mesures de complexité incluant aussi les additions seraient bien sûr pertinentes –en particulier au dessus du corps $\mathbf{F}_2$. On pourrait même tenir compte de la possibilité d'effectuer des opérations élémentaires sur des groupes de 32 ou 64 bits à la fois.

1.2 La méthode d'interpolation de Chudnovsky et Chudnovsky

La méthode d'interpolation de [Ch^2] fournit les algorithmes atteignant les plus petites complexités bilinéaires connues aujourd'hui, dans les extensions de corps finis de degré environ plus grand que 20.

Dans le contexte symétrique, la construction peut être résumée ainsi. Elle sera formalisée plus précisément dans le §1.1. Supposons que l'on veuille calculer la multiplication dans $\mathbf{F}_{q^m}$ de façon bilinéaire en $\mathbf{F}_q$. On part d'une courbe X sur $\mathbf{F}_q$, munie d'un point Q de degré m et de diviseurs D et G. Par exemple l'on choisit $G = \{P_1, \ldots, P_n\}$ égal à une somme de points P_i de degré un.

Supposons que D et G soient adaptés à l'interpolation, c'est à dire qu'on a l'injectivité et la surjectivité des flêches telles que représentées dans le diagramme ci-dessous. Alors la multiplication de x et y quelconques dans $\mathbf{F}_{q^m}$ peut être réalisée par les cinq étapes suivantes:

① *relever* x et y en des fonctions f_x et f_y dans l'espace des sections globales $L(D)$, de sorte que $f_x(Q) = x$ et $f_y(Q) = y$.

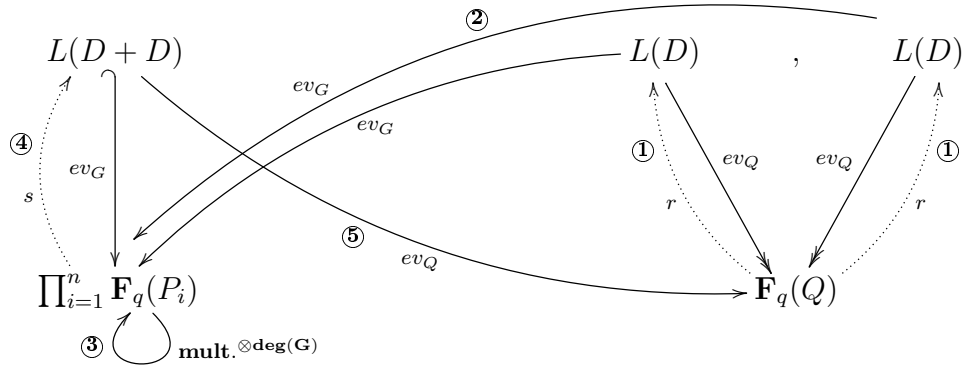
② *évaluer* f_x et f_y, séparément, en chaque point P_i du diviseur G.

③ *calculer*, pour chaque P_i, le produit des deux évaluations : $a_i = f_x(P_i) \cdot f_y(P_i)$. C'est l'étape coûteuse dans le contexte bilinéaire puisque elle nécessite $n = \deg G$ multiplications entre deux quantités variables. On obtient le n-uplet d'évaluations $(a_1, \ldots, a_n)$.

④ *interpoler* ce n-uplet en l'*unique* fonction $g \in L(2D)$ prenant les valeurs a_i aux points P_i;

⑤ *évaluer* g en Q pour retrouver le produit de x par y.

(1.3)



2 Résultats principaux et les conjectures qui se posent

2.1 Le théorème A sur les bornes asymptotiques

Étant principalement intéressés par la limite sup de la complexité, nous avons besoin de suffisamment de courbes différentes afin de traiter les pires cas. Donnons donc un nom à la qualité suivante, formalisée dans [STV, Claim p163]:

Definition 2.1. Soit X_s/k une famille de courbes sur un corps k de genres g_s. On dit que la famille $(X_s)_s$ est *dense* si et seulement si les genres g_s tendent vers l'infini et leur ratios consécutifs g_{s+1}/g_s tendent vers 1.

Les ratios asymptotiques β_r du nombre de places de degré r rapporté au genre, sont des quantités étudiées dans les corps de nombres (cf. [Leb] et [LZ] pour des progrés récents). De façon analogue, les algorithmes de multiplication par interpolation sur les courbes nécessitent, dans les cas qui nous intéressent, beaucoup de points de degré $r \geq 2$. D'où la définition suivante du meilleur ratio β_r que l'on puisse espérer :

Definition 2.2. Soit $r \geq 1$ un entier et q une puissance d'un nombre premier. Soit X une courbe sur $\mathbf{F}_q$ et $B_r(X)$ le nombre de points fermés de degré r. On appelle $A_r(q)$ et $\widetilde{A}_r(q)$ les plus grands nombres β_r et $\widetilde{\beta}_r$, tels qu'il existe une famille (respectivement une famille *dense*) de courbes X_s sur $\mathbf{F}_q$, de genres g_s tendant vers l'infini, qui satisfait:

$$\lim_{s\to\infty} \frac{B_r(X_s)}{g_s} = \beta_r \text{ (respectivement } \widetilde{\beta}_r)$$

Example 2.3. En particulier, $A_1(q) = A(q)$ est la constante d'Ihara. Cf. le tableau 2.2 et le théorème 2.5 dans le §2.2 pour des résultats récents dans les cas où q n'est pas un carré.

Plus généralement, Cascudo—Cramer—Xing et Yang ont montré que la borne de Drinfeld–Vladuts généralisée implique la majoration suivante (cf. le théorème 2.1):

$$\widetilde{A}_r(q) \leq A_r(q) \leq \frac{\sqrt{q^r}-1}{r}$$

Examples 2.4. Les tours de Garcia–Stichtenoth étant en fait définies sur leur corps premier $\mathbf{F}_p$, elles fournissent des exemples de familles non denses atteignant les bornes précédentes (cf. le §2.2):

$$A_r(q) = \frac{\sqrt{q^r}-1}{r} \text{ dès que } q^r \text{ est un carré.} \tag{2.1}$$

Pour toutes les valeurs de q qui seront utilisées dans ce travail, les courbes de Shimura fournissent des familles denses qui atteignent la borne de Drinfeld–Vladuts sur $\mathbf{F}_{q^2}$ cf. le §2.3. Les courbes modulaires de Drinfeld ont la même propriété. Voir [Gek, 8-9] pour l'optimalité (et [Gek$_2$, Th. 2.16] pour l'argument avec les points supersinguliers lorque q est pair). Tandis que la densité résulte de [Gek, 9.] et d'un argument communiqué par H. Randriam). Par conséquent on a l'égalité sur $\mathbf{F}_{q^2}$:

$$\widetilde{A}_1(q^2) = q - 1\ . \tag{2.2}$$

Mais on peut dire plus. Comme cela sera formalisé dans le corollaire 2.6, ces courbes sont définies sur $\mathbf{F}_q$ —et pas seulement sur $\mathbf{F}_{q^2}$. Donc par le corollaire de la borne de Drinfeld–Vladuts généralisée mentionné ci-dessus, cela implique aussi l'égalité:

$$\widetilde{A}_2(q) = \frac{q-1}{2} \tag{2.3}$$

On rappelle enfin que les courbes modulaires classiques sur $\mathbf{F}_p$ sont un cas particulier de courbes de Shimura.

Le théorème omnibus suivant généralise toutes les formules de la littérature fournissant les meilleures bornes asymptotiques connues pour la multiplication bilinéaire.

Theorem A. *Soit q une puissance d'un nombre premier et soient $r \geq 1$ et $l \geq 1$ deux entiers positifs. Alors on a la liste de majorations ci-dessous pour les constantes asymptotiques M_q. Elles sont valables sous les hypothèses énoncées dans chaque cas, et dès lors que les dénominateurs dans les formules concernées sont strictement positifs:*

(a)
$$M_q \leq \frac{2\mu_q(r,l)}{rl}\left(1 + \frac{1}{rl\widetilde{A}_r(q) - 1}\right).$$

(a') En outre sous l'une ou l'autre des deux hypothèses suivantes:

(i) $r = 1$ et q est tel que $\widetilde{A}_1(q) > 5$;

(ii) soit p un nombre premier tel que la conjecture Z est valable pour p. On demande également: $\{q = p$ et $r = 2\}$ ou $\{q = p^2$ et $r = 1\}$;

alors la borne précédente est en fait symétrique *:*

$$M_q^{\mathrm{sym}} \leq \frac{2\mu_q^{\mathrm{sym}}(r,l)}{rl}\left(1 + \frac{1}{rl\widetilde{A}_r(q) - 1}\right).$$

(b)
$$M_q^{\mathrm{sym}} \leq \frac{2\mu_q^{\mathrm{sym}}(r,l)}{rl}\left(1 + \frac{2}{rl\widetilde{A}_r(q) - 2}\right).$$

(c) si $2|q$

$$M_q^{\mathrm{sym}} \leq \frac{2\mu_q^{\mathrm{sym}}(r,l)}{rl}\left(1+\frac{1+\log_q(2)}{rl\widetilde{A}_r(q)-1-\log_q(2)}\right).$$

(c') si $2\nmid q$

$$M_q^{\mathrm{sym}} \leq \frac{2\mu_q^{\mathrm{sym}}(r,l)}{rl}\left(1+\frac{1+2\log_q(2)}{rl\widetilde{A}_r(q)-1-2\log_q(2)}\right).$$

Remarks 2.5. Voici les améliorations par rapport aux résultats connus:

- (c) et (c') autorisent désormais des évaluations en des points de degré r impair, ce que ne prenait pas en considération [CCX$_2$, Theorem 5.18] (bien que tous les arguments soient tirés de cet article);
- (b) autorise désormais des évaluations en des points de degré arbitraire, en comparaison de [BCP, Proposition 11];
- enfin, nous avons introduit des évaluations dérivées (le paramètre l) dans tous les résultats précédents. Cette possibilité était en fait connue depuis [Ar] et [Ran$_1$]. L'évaluation en des points de degré arbitraire ayant, elle, été introduite par [CO$_1$].

2.2 Le théorème B et les familles denses avec beaucoup de points de degré supérieur

Une courbe avec un nombre record de points

La famille dense de notre théorème B ci-dessous, provient de tours récursives de courbes de Shimura, définies sur le corps de nombres $\mathbf{Q}(\cos(\pi/7))$ de nombre de classes strict égal à un. L'étude d'une autre tour de courbes de Shimura, cette fois sur le corps $\mathbf{Q}(\sqrt{3})$ de nombre de classes strict égal à deux, conduit pour sa part à la bonne surprise détaillée dans le §V.4. En effet la réduction modulo (5) du quatrième étage de cette tour, de genre cinq, a un nombre de points dans$\mathbf{F}_{5^4}$: **871** plus grand que la valeur de 868 enregistrée dans les tables de manypoints.org[1]au moment de sa découverte. En sus nous obtenons des *équations définies dans* $\mathbf{F}_5$ pour cette courbe (définie a priori sur $\mathbf{F}_{5^2}$).

[1]Nous avons apris plus tard que S.E. Fischer avait soumis simultanément une courbe avec le même nombre de points et une équation encore plus simple.

La conjecture Y et son histoire (très) récente

La conjecture de folklore suivante pose la question de l'existence de *familles denses définies sur leur corps premier, et atteignant la borne de Drinfeld–Vladuts dans une extension de degré pair fixée.* Elle est énoncée dans [CCXY, Lemma IV.4], sous une forme équivalente à :

Conjecture Y. *Soit p un nombre premier et $t' = 2t \geq 2$ un entier pair*[2]*. L'égalité suivante est-elle satisfaite:*

$$\widetilde{A}_{2t}(p) = \frac{p^t - 1}{2t} \quad ? \tag{2.4}$$

Dit autrement (en vertu du théorème 2.1) : existe-il une famille $(X_s/\mathbf{F}_{p^{2t}})_{s\geq 1}$ de courbes de genres g_s tendant vers l'infini telles que:

(i) X_s *admet* $\mathbf{F}_p$ comme corps de définition *(descente);*

(ii) $g_{s+1}/g_s \xrightarrow[s\to\infty]{} 1$ *(*densité *de* $(X_s)_s$*)*

(iii) $|X_s(\mathbf{F}_{p^{2t}})|\,/g_s \xrightarrow[s\to\infty]{} p^t - 1$ *(*borne de Drinfeld–Vladuts sur $\mathbf{F}_{p^{2t}}$*)* *?*

Les premières tentatives ont consisté à rendre les tours de Garcia–Stichtenoth plus denses. Cela a commencé avec [Bal_2], puis [BR] a également traité le problème du corps de définition, et enfin [BBR] prouve un théorème de descente général. Ce dernier utilise le critère de la proposition A.1.2 (redécouvert par Randriam).

Ensuite, [CCXY, Lemma IV.4] ont proposé de résoudre la conjecture à l'aide de courbes de Shimura définies sur les rationnels. Le problème est que les courbes utilisées dans la preuve ne descendent pas nécessairement sur $\mathbf{Q}$. Ce problème fut remarqué pour la toute première fois par S. Ballet en tant que rapporteur de [CCXY], en réponse à une version préliminaire. L'article a ensuite été accepté avec une autre preuve, et l'énoncé de la conjecture utilisé comme s'il était un théorème, dans: [CCX_2, Lemma 5.17] et [PR, Lemma 5.2].

Plusieurs personnes ont ensuite remarqué que la preuve définitive contenait encore un problème de courbes qui ne descendent pas nécessairement

[2]Remarquons que les cas où $2t = 2$ sont en fait vérifiés avec les courbes modulaires classiques : voir [Mo, §5.6] pour une preuve. Tandis que les cas où $2t = 6$ sont traités dans le (nouveau) théorème B ci-dessous, et la conjecture X.

sur $\mathbf{Q}$. Tout d'abord, parce que la plupart n'ont même pas leur corps de modules égal à $\mathbf{Q}$: cf. §IV.5.5.

De façon plus sournoise, parce que *même les courbes de Shimura dont le corps des modules est égal à* $\mathbf{Q}$ *ne descendent pas toujours sur* $\mathbf{Q}$. Trois contre-exemples sont décrits dans §IV.5.6. Ils ont été initialement dégagés comme tels dans notre travail commun [BPRS, §3], parmi les courbes étudiées dans [Sij$_1$]. En particulier H. Randriam et J. Voight se doivent d'être crédités pour leur contribution.

Mais au regard du cas particulier ($p = 3$ et $2t = 6$) étudié dans ce travail, la proposition de [CCXY] d'utiliser les courbes de Shimura a porté ses fruits. Nous montrerons dans le prochain paragraphe comment construire une solution explicite.

La conjecture semble avoir été résolue début juillet 2017. Une communication privée de Bassa et Beelen établirait que les courbes modulaires de Drinfeld modulo T sur $\mathbf{F}_q$ ayant des niveaux dans $\mathbf{F}_p[T]$ (et pas seulement dans $\mathbf{F}_q[T]$), descendraient sur $\mathbf{F}_p$. De la formule des genres de Gekeler [Gek, 9.], H. Randriam déduit la densité de cette famille de courbes (nous avons enfin augmenté cette densité pour atteindre celle des tours de courbes de Shimura entrelacées).

Notre solution particulière

Theorem B. *On a:*

$$\widetilde{A}_6(3) = \frac{3^3 - 1}{6}. \tag{2.5}$$

Dit autrement : il existe X_s une famille de courbes définies sur $\mathbf{F}_3$ *avec des genres g_s tendant vers l'infini telle que:*

(i) $\dfrac{g_{s+1}}{g_s} \xrightarrow[s\to\infty]{} 1$ *(*densité *des genres)*

(ii) $\dfrac{|X_s(\mathbf{F}_{3^6})|}{g_s} \xrightarrow[s\to\infty]{} 3^3 - 1$ *(*optimalité *du nombre de points de degré* 6*)*

Nous explicitons aussi une solution dans le cas ($p = 5$ et $2t = 6$): entrelacer la tour d'équations V.(6.10), avec la réduction de la tour du Théorème C ci-dessous. Mais nos calculs pour vérifier l'étage supérieur n'ont pas encore abouti.

L'idée-clé de la preuve, due à N.D. Elkies, est qu'il est possible d'*entrelacer* deux tours modulaires récursives en une famille dense: voir §V.5.3. Une recherche dans les tables [Voi$_4$] de courbes de Shimura de petits genres, filtrée par les conditions sur les paramètres B, $\mathfrak{p}$ et $\mathfrak{N}$ du théorème IV.5.4 (dégagé dans la thèse de V. Ducet), aboutit aux candidats prometteurs suivants:

Proof Considérons la famille des surfaces de Riemann $X_0(\mathfrak{p}_2^i\mathfrak{p}_7^j)$ étudiées dans le §III.2.3 (et résumées dans le paragraphe suivant). En particulier les résultats du §2.5 montrent que leurs genres sont *denses*.

Par la théorie générale (théorème IV.5.4), ces courbes ont leurs modèles canoniques définis sur le corps $F = \mathbf{Q}(\cos(2\pi/3))$ avec bonne réduction modulo l'idéal premier (3). Ces réductions sont définies sur $\mathbf{F}_{3^3}$ et ont beaucoup de points dans l'extension quadratique $\mathbf{F}_{3^6}$.

Mais pour montrer qu'ils descendent sur $\mathbf{F}_3$, il faut *construire explicitement ces modèles canoniques.*

Or nous voulons montrer qu'il y a en outre *bonne réduction sur* $\mathbf{F}_3$. Pour le montrer nous *construisons de manière explicite ces modèles canoniques.* En vertu du deuxième énoncé de notre théorème IV.5.14, ces modèles sont caractérisés de manière unique par leur monodromie au dessus de $X(1)$.

Les deux tours $X_0(\mathfrak{p}_2^i)$ et $X_0(\mathfrak{p}_7^j)$ étant récursives par le §V.3, elles sont entièrement déterminées par *deux revêtements de Belyi depuis des courbes elliptiques.* Il s'agit des revêtements $X_0(\mathfrak{p}_7^2) \to X_0(\mathfrak{p}_7)$ et de $X_0(\mathfrak{p}_2^2) \to X_0(\mathfrak{p}_7)$, de degrés 7 et 8. leur monodromies sont calculées dans les exemples IV.3.4 et 3.6. Le calcul de leurs équations est décrit dans le §.V.5. Il a bénéficié de l'aide inestimable des résultats et méthodes numériques récents de J. Voight et J. Sijsling sur les courbes de Shimura, les opérateurs de Hecke, les groupes fuchsiens et les fonctions de Belyi.

Enfin nous *descendons à* $\mathbf{F}_3$ *le corps de définition* de la réduction modulo (3) de ces revêtements.

Comme vérification supplémentaire, nous avons pu calculer les étages supérieurs de ces tours: $X_0(\mathfrak{p}_7^3)$ et $X_0(\mathfrak{p}_2^3)$, de genres cinq et sept. Puis comparer leurs nombres de points dans $\mathbf{F}_{3^3}$ et $\mathbf{F}_{3^6}$ —$28; 1000$ pour $X_0(\mathfrak{p}_7^3)$ et $24; 1760$ pour $X_0(\mathfrak{p}_2^3)$—avec les nombres prédits par le théorème IV.5.5 (d'après les traces d'opérateurs de Hecke): $28; 1000$ et $24; 1760$. □

Remark 2.6. Pour des raisons techniques, le deuxième revêtement de Belyi a seulement été calculé dans l'extension quadratique $\mathbf{Q}(\sqrt{-7})$ (où il acquiert

un point de ramification rationnel). Par conséquent, même si la réduction modulo (3) de ce revêtement descend sur $\mathbf{F}_3$, le revêtement lui-même n'est isomorphe au revêtement canonique qu'après une *extension quadratique* par $\sqrt{-7}$: il pourrait s'agir d'un tordu. Heureusement, dans la mesure où nous ne sommes intéressés que par le *nombre de points après une extension quadratique de* $\mathbf{F}_{3^3}$, cela ne remet pas en cause notre preuve de ce cas particulier de la conjecture.

Remark 2.7. Le chapitre IV prouve en détail le théorème IV.5.14 de descente des modèles canoniques $\mathbf{Q}$. Ce résultat général n'intervient pas dans la preuve du théorème B. Mais donne des indices importants pour réaliser les calculs explicites de V.5 qui constituent la preuve. Le théorème IV.5.14 s'appuie sur les résultats généraux de descente des revêtements arithmétiques, et sur les résultats de Doi–Naganuma.

Remarquons que par la théorie générale, pour tous les nombres premiers différents de $p = 2$ and 7 et inertes dans le corps $\mathbf{Q}(\cos \pi/7)$ des modèles canoniques, les courbes $X_0(\mathfrak{p}_2^i \mathfrak{p}_7^j)_{\mathbf{Q}}$ ont aussi *potentielle bonne réduction* modulo p. Ces réductions ont lieu dans $\mathbf{F}_{p^3}$ et ont beaucoup de points dans l'extension quadratique $\mathbf{F}_{p^6}$. Donc bien entendu, un argument général qui prouverait la *bonne réduction* sur $\mathbf{F}_p$ (comme nous l'avons fait par le calcul pour $p = 3$) serait bienvenu.

Résumé des résultats effectifs sur les courbes de Shimura de la section §V.5.2 utilisés dans le théorème B

Rappelons les tours considérées dans V.5. Soit $F = \mathbf{Q}(\cos(\pi/7))$ le corps totallement réel de degré 3 et de nombre de classes restreint égal à un. Fixons une fois pour toutes un plongement réel $\iota : F \hookrightarrow \mathbf{R}$ (en fait ce choix n'a pas d'importance). Soit B l'algèbre de quaternions sur F ramifiée exactement en: les deux places infinies autres que ι, et aucune place finie.

B agit sur le demi plan supérieur à travers la place réelle ι qui scinde B: $\iota : B \hookrightarrow \mathrm{M}_2(\mathbf{R})$. Considérons les idéaux premiers $\mathfrak{p}_2$ et $\mathfrak{p}_7$ de F au dessus du premier inerte (2) et du premier ramifié (7). Définissons les familles emboîtées de groupes de congruence de $\mathrm{PSL}_2(\mathbf{R})$ qui leur correspondent: $\overline{\Gamma_0(\mathfrak{p}_2^i)}$ et $\overline{\Gamma_0(\mathfrak{p}_2^j)}$ (voir les définitions du II.5.1). Formons les quotients du demi plan supérieur par ces groupes: les inclusions de groupes successives donnent lieu à une succession de revêtements canoniques (voir le Théorème IV.5.1) sur F:

$$\ldots \xrightarrow{f_4} X_0(\mathfrak{p}_7^3) \xrightarrow{f_3} X_0(\mathfrak{p}_7^2) \xrightarrow{f_2} X_0(\mathfrak{p}_7) \xrightarrow{f_1} X_0(1)$$
$$\ldots \xrightarrow{f_4} X_0(\mathfrak{p}_2^3) \xrightarrow{f_3} X_0(\mathfrak{p}_2^2) \xrightarrow{f_2} X_0(\mathfrak{p}_2) \xrightarrow{f_1} X_0(1)$$

Theorem C. *(i) Le* revêtement canonique $f_{2,F} : X_0(\mathfrak{p}_7^2)_F \longrightarrow X_0(\mathfrak{p}_7)_F$ *descend à* $\mathbf{Q}$. *Son équation, ainsi que celles des involutions d'Atkin—Lehner, sont données par les équations V.*(5.11) *et V.*(5.12)–(5.15)*:*

$$\begin{aligned} X_0(\mathfrak{p}_7^2)_F &: y^2 + xy = x^3 - x^2 - 2x - 1 \\ f_{2,\mathbf{Q}}(x,y) &= 2x + 5x^2 - 3x^3 + (-3 + 3x + x^2)y \text{ , } \textit{branched over} \\ Q_3, Q_3' &= \pm\sqrt{-3}; \\ w_2 &: X_0(\mathfrak{p}_7^2)_{\mathbf{Q}} \ni P \longrightarrow (2,-1,1) - P \\ w_1 &: t \in \mathbf{P}^1_{\mathbf{Q}} \ni t \longrightarrow -1 - t \end{aligned}$$

(ii) L'extension quadratique à $F(\sqrt{-7})$ du modèle canonique $X_0(\mathfrak{p}_2^2)_F$ *est donnée par V.*(5.2)*:*

$$X_0(\mathfrak{p}_2^2)_{F(\sqrt{-7})} : y^2 = x^3 + x^2 - 114x - 127\,.$$

(ii') L'extension quadratique à $F(\sqrt{-7})$ du revêtement canonique

$$X_0(\mathfrak{p}_2^2)_F \longrightarrow X_0(\mathfrak{p}_2)_F = \mathbf{P}^1_F\,,$$

est donnée par V.(5.4)*:*

$$\begin{aligned} f_{2,F(\sqrt{-7})} =& \frac{1}{x - \frac{1}{32}(91z+169)}\Big[\frac{1}{12544}(-z+11)x^4 + \frac{1}{12544}(-27z-151)x^3 \\ &+ \frac{1}{3136}(71z-109)x^2 + \frac{1}{3136}(491z+4231)x + \frac{1}{3136}(-8411z-14971) \\ &+ y\Big(\frac{1}{614656}(-13z-49)x^3 + \frac{1}{153664}(205z+49)x^2 \\ &+ \frac{1}{76832}(-317z+1519)x + \frac{1}{153664}(-2613z+5831)\Big)\Big]. \end{aligned}$$

(iii) La réduction sur $\mathbf{F}_{3^6}$ *du* revêtement canonique après extension quadratique du corps de base $F(\sqrt{-7})$*:* $f_2 : X_0(\mathfrak{p}_2^2)_{F(\sqrt{-7})} \longrightarrow X_0(\mathfrak{p}_2)_{F(\sqrt{-7})} = \mathbf{P}^1_{F(\sqrt{-7})}$*, et de même pour les involutions d'Atkin—Lehner, est donnée par*

les équations suivantes V.(5.7) *to* (5.10). *Qui, heureusement pour nous, peuvent être descendues à* $\mathbf{F}_3$*:*

$$\begin{aligned} f_2(x,y) &= \frac{1+x^2+x^3+x^4+(x+2x^2)y}{2+x^2+x^3+x^4+x^2y} \\ X_0(\mathfrak{p}_2^2)_{\mathbf{F}_3} &: y^2 = x^3+x^2+2 \\ w_2 &: X_0(\mathfrak{p}_2^2)_{\mathbf{F}_3} \ni P \longrightarrow (1,2,1)-P \\ w_1 &: t \in \mathbf{P}^1_{\mathbf{F}_3} \ni t \longrightarrow -t \end{aligned}$$

Les conjectures X $\leq$ Y et Z qui subsistent

Pour traiter le cas restant $p = 2$*, on a besoin d'une autre tour* $X_0(\mathfrak{p}^k)$*, sur la même base* $X_0(1)$ *que dans le Théorèm B, qui descend sur* $\mathbf{F}_2$. En effet l'on pourrait alors entrelacer $X_0(\mathfrak{p}^k)_{\mathbf{F}_2}$ avec la tour $X_0(\mathfrak{p}_7^j)_{\mathbf{F}_2}$ trouvée dans le Théorème B (see V.(5.12)). Et donc produire une famille dense.

Un bon candidat est la tour $X_0(\mathfrak{p}_3^i)$, où $\mathfrak{p}_3$ est le premier (3). Par la théorie générale elle a bonne réduction modulo (2): $X_0(\mathfrak{p}_3^i)_{\mathbf{F}_{2^3}}$, et beaucoup de points dans $\mathbf{F}_{2^6}$. Mais nous ignorons si cette réduction descend sur $\mathbf{F}_2$. Par récursivité de la tour, cela résulterait de la conjecture suivante.

Conjecture X. *Soit* B *l'algèbre de quaternions sur* $F = \mathbf{Q}\big(\cos(2\pi/7)\big)$ *ramifiée en exactement deux des trois places réelles et aucune place finie. Soit* $\mathfrak{p}_3$ *l'idéal premier* (3)*, et* $X_0(\mathfrak{p}_3^2)$ *la courbe de Shimura sur* F *définie par le groupe* $\Gamma_0(\mathfrak{p}_3^2)$ *des unités de norme un de l'ordre d'Eichler de niveau* $\mathfrak{p}_3^2$.

Alors les morphismes suivantes descendent sur $\mathbf{F}_2$*:*

- *le revêtement ramifié canonique* $X_0(\mathfrak{p}_3^2)_{\mathbf{F}_{2^3}} \to X_0(\mathfrak{p}_3)_{\mathbf{F}_{2^3}}$,
- *et l'involution d'Atkin–Lehner sur* $X_0(\mathfrak{p}_3^2)_{\mathbf{F}_{2^3}}$.

Bien que ce soit un travail en cours, nous décrivons les calculs conduisant au quotient d'Atkin–Lehner $X_0(\mathfrak{p}_3^2)^*$ de genre deux dans I.4. En effet ils illustrent la théorie général et les algorithmes récents.

La dernière conjecture, comme proposée dans [Ran$_0$, Conjecture A] plus la condition de densité, pourrait combler l'écart entre les bornes symétriques et asymétriques pour les valeurs de q plus grandes. C'est à dire celles pour lesquelles l'interpolation sur les courbes modulaires classiques donne les meilleurs résultats. Cette conséquence est formalisée dans le théorème A, cas (a')(ii).

Conjecture Z. *Soit $p > 2$ un nombre premier impair. Existe-t-il une suite de nombres $(N_s)_s$, avec $N_{s+1}/N_s \xrightarrow[s\to\infty]{} 1$ (condition de densité), telle que l'opérateur de Hecke $T_p(N_s)$ sur l'espace des formes cuspidales $S_2(\Gamma_0(N_s))$ de poids deux, a un déterminant impair ?*

La conséquence suivante a été isolée dans [Ran$_0$]. Soit p un nombre premier, N un entier positif premier à p, $X_0(N)$ la courbe modulaire classique sur les rationnels, munie de l'opérateur de Hecke T_p sur l'espace $S_2(\Gamma_0(N))$ des formes cuspidales de poids deux. Alors la relation de congruence d'Eichler–Shimura implique (voir §5 pour la preuve):

$$|J_0(N)(\mathbf{F}_{p^2})| = \det(p^2 + 1 - T_p(N)^2) \tag{2.6}$$

On a en particulier la conséquence suivante sur le groupe rationnel des points de 2-torsion :

$$\dim J_0(N)(\mathbf{F}_{p^2})[2] \leq \mathrm{ord}_2\left(\det(p^2 + 1 - T_p(N)^2)\right) ,$$

où ord_2 désigne la valuation 2-adique. Le nombre premier p étant impair, le déterminant dans le membre de gauche a la même parité que $\det(T_p(N))$. Par conséquent la conjecture aurait comme conséquence la conjecture suivante plus faible:

Conjecture 2.8. *Existe-il une famille dense de courbes modulaires classiques $(X_0(N_s)/\mathbf{F}_p)_s$ telles que:*

$$(J_0(N)(\mathbf{F}_{p^2}))\,[2] = \{0\} \text{ pour tout } N_s?$$

Remarks 2.9. Remarquons que la condition de densité est $N_{s+1}/N_s \xrightarrow[s\to\infty]{} 1$, qui *n'implique pas* que l'ensemble des nombres $\{N_s\}_s$ ait une densité de Dirichlet positive (considérer $(N_s^2)_s$). L'implication opposée est aussi fausse.

Sans la condition de densité, le corollaire n'aurait d'effet que sur les bornes asymptotiques limites inf.:

- pour les valeurs de q dans le tableau 2.3: le seul effet de la conjecture Z serait alors de combler l'écart entre les bornes symétriques et asymétriques pour $q = 25$. En effet dans les trois autres cas où les bornes asymétriques sont meilleures que leurs pendants symétriques, il se trouve que les familles utilisées ne sont pas des courbes modulaires classiques.

- pour les valeurs de q plus grandes: la conjecture Z ne bénéficierait qu'aux valeurs pour lesquelles on ignore si la condition (a')(i) du théorème A ($\widetilde{A}_1(q) > 5$) est satisfaite. Donc seuls les grands nombres premiers q seraient concernés, parce que dans ces cas l'on aurait besoin d'interpoler sur les points de degré deux de courbes modulaires classiques.

2.3 Amélioration des bornes pour la multiplication bilinéaire

Multiplication symétrique dans les petites algèbres

La méthode d'interpolation de Chudnovsky et Chudnovsky sous sa forme généralisée (le théorème 1.1, au début du §1.1) utilise des évaluations en des points épaissis, qui prennent leurs valeurs dans de petites algèbres. Par conséquent, améliorer les algorithmes bilinéaires dans ces petites algèbres a un impact direct sur l'algorithme de multiplication global.

Dans le tableau 2.1 ci-dessous sont récapitulées les meilleures bornes supérieures et inférieures pour les complexités bilinéaires $\mu_2^{\mathrm{sym}}(m,l)$ de la multiplication dans les petites $\mathbf{F}_2$-algèbres $\mathbf{F}_{2^m}[x]/x^l$. Chaque paire de bornes inf.–sup. est notée "L–U". Lorsque la borne sup U est en fait optimale (donc L=U), alors une seule valeur est affichée.

Les trois bornes sup améliorées sont affichées en gras. Tandis que les deux nouvelles bornes inf. (pour $\mu_2^{\mathrm{sym}}(2,2)$ et $\mu_2^{\mathrm{sym}}(2,3)$, en plus de la valeur exacte de $\mu_2^{\mathrm{sym}}(3,2)$) sont simplement mises en valeur dans le tableau 3.1.

Les valeurs de toutes les bornes sup sont justifiées dans le tableau 3.1 du §3.1, et les nouvelles formules de multiplication dans l'annexe A.2. Les méthodes employées pour les trouver sont détaillées dans le §VI.2.

D'un autre côté on ne donne pas de justification pour la plupart des bornes inf. En particulier les trois nouvelles –évoquées ci-dessus– résultent de l'exhaustivité de la méthode de recherche (par orbites) décrite sous l'observation VI.2.2. Les autres bornes inf. non justifiées sont simplement déduites du résultat général [Ran_1, Lemma 1.9], ou en considérant une algèbre plus petite pour laquelle une borne inf. est connue.

Table 2.1: Bornes inf–sup sur les complexités $\mu_2^{\mathrm{sym}}(m,l)$

$l \backslash m$	1	2	3	4	5	6	7	8	9	10
1	1	3	6	9	13	15	$16-22$	$16-24$	$17-30$	$19-33$
2	3	9	**16**	$16-24$	.	.	.	.	.	.
3	5	15	$16-30$	.	.	.	.	.	.	.
4	8	$8-$ **21**	.	.	.	.	.	.	.	.
5	11	$11-$ **30**	.	.	.	.	.	.	.	.
6	14	.	.	.	.	.	.	.	.	.
7	$16-18$	.	.	.	.	.	.	.	.	.
8	$16-22$	.	.	.	.	.	.	.	.	.
9	$16-27$	.	.	.	.	.	.	.	.	.
10	$16-31$	.	.	.	.	.	.	.	.	.

Bornes asymptotiques limites supérieures dans les extensions de corps finis

Les valeurs affichées dans le tableau 2.2 ci-dessous sont justifiées dans le tableau 3.2 du §3.2. La première ligne est un état de l'art, la seconde tient compte de la contribution de notre théorème A, la troisième ajoute les nouvelles valeurs des $\widetilde{A}_r(q)$ démontrées par le théorème B. Les quatrième et cinquième ajoutent graduellement les valeurs de $\widetilde{A}_r(q)$ prédites par les conjectures X puis Y. À l'inverse la dernière ligne, valable sous la conjecture Z, ne dépend par contre pas des deux conjectures précédentes (ni du théorème B).

Remark 2.10. Insistons sur le fait que la ligne "Bornes (réparées)" du tableau 2.2 ne contient pas certaines bornes publiées dans la littérature car elles ne pouvaient pas être considérées comme prouvées à l'époque. Elles apparaissent dans [CCXY, Theorem IV.6, Theorem IV.7, Corollary IV.8], [CCX_2, Theorem 5.18, Corollary 5.19] et [PR, Theorem 5.3, Corollary 5.4, Corollary 5.5].

En effet elles reposent sur la conjecture Y, qui implique beaucoup de nouvelles valeurs de $\widetilde{A}_r(q)$.

Nous avons néanmoins tenu compte au maximum des résultats prou-

Table 2.2: Amélioration des bornes sup pour M_q^{sym} et M_q

Résultats utilisés \ q		2	3	4	5	7
Bornes (réparées)	Sym	$15,2$ [BP$_2$]	$7,73$ [BP$_2$]	6.00	$5,61$	$4,20$
	Asym	8.59	$6,00$	$4,50$	$4,00$	$3,60$
avec le th. A et Tab. 2.1	Sym	$\mathbf{10,0}$	$\mathbf{7,50}$	$\mathbf{5,33}$	$\mathbf{5,21}$	$\mathbf{4,08}$
	Asym	$\mathbf{7,00}$	—	—	—	—
+ le th. B	Sym	—	$\mathbf{5,42}$	—	*4,74*	—
	Asym	—	$\mathbf{5,20}$	—	—	—
Conj. X	Sym	7	—	4.24	—	—
	Asym	$5,83$	—	$3,89$	—	—
Conj. Y	Sym	$6,92$	$5,39$	—	$4,34$	3.63
	Asym	—	$5,14$	—	—	$3,57$
Conj. Z	Sym	—	—	—	*4, 00*	$3,60$

Résultats utilisés \ q		8	9	11	5^2
Bornes (réparées)	Sym	3.71	3.77	3.56	3
	Asym	3,50	3,43	3,33	2,67
Avec le th. A et Tab. 2.1	Sym	—	—	—	—
	Asym	—	—	—	—
+ le th. B	Sym	—	**3.56**	—	—
	Asym	—	—	—	—
Conj. X	Sym	—	—	—	—
	Asym	—	—	—	—
Conj. Y	Sym	3.58	—	3.55	—
	Asym	—	—	—	—
Conj. Z	Sym	—	—	$3,33$	$2,67$

vés dans ces articles dans les chiffres de la ligne "Bornes (réparées)" (d'où l'adjectif "réparé"). Simplement nous les avons appliqués avec les valeurs des $\widetilde{A}_r(q)$ connues à leur date de publication[3]. C'est à dire celles qui résultent de la théorie générale des courbes de Shimura[4], données par les équations (2.2) et (2.3).

Remark 2.11. [La remarque suivante perd de l'intérêt depuis que la conjecture Y a été démontrée]. La borne $M_2^{\mathrm{sym}} \leq 10,0$ semble pouvoir être légèrement améliorée avec les outils existants. En effet si la borne sup suivante s'avérait exacte : $\mu_2(2,6) \leq 39$ (au lieu de 42), alors le (b) du théorème A appliqué à $(r,l) = (2,6)$ impliquerait $M_2 \leq 9,75$. Nos raisons de penser que cette borne est accessible, est qu'elle pourrait être déduite de la borne conjecturale suivante: $\mu_4(1,6) \leq 13$ (au lieu de 14), qui est accessible avec les méthodes de recherche exhaustive. Or la valeur 14 est elle-même une borne sup. pour les deux complexités plus difficiles $\mu_2(1,6)$ et $\mu_4(6,1)$. Donc la borne conjecturale de 13 semble très crédible.

Remark 2.12. La colonne supplémentaire pour $q = 5^2$ met en valeur le record de longévité de la borne symétrique (qui tient toujours). En effet, bien que sa valeur n'ait jamais été publiée numériquement, elle peut être directement déduite d'une formule de Ballet–Pieltant, elle même basée sur un argument remontant à 1999. Cette exception sera discutée dans la remarque 3.2.

Les bornes asymptotiques limite inf dans les extensions de corps finis

Le tableau suivant regroupe à la fois : (i) les meilleures bornes connues pour les limites inf. m_q^{sym} des complexités symétriques pour les petites valeurs de q (cf. [CCX$_2$, V, table II],); et (ii) dans certains cas, propose des limites asymétriques légèrement meilleures (en gras)[5]:

Le fait que les bornes symétriques soient proches des bornes asymétriques résulte de la plus grande tolérance permise par la limite inf. En effet elle peut être calculée uniquement sur les valeurs avantageuses: voir le §3.3. Il subsiste néanmoins des possibilités d'améliorations :

[3]Mais par contre sans les généralités supplémentaires désormais autorisées par le théorème A.

[4]rappelée dans §2.3. Ce qui inclut les courbes modulaires classiques sur les corps premiers

[5]Qui résultent des tours du théorème 2.5 pour $q = 27$ et $q = 32$, et des courbes de Shimura pour $q = 16$.

Table 2.3: (nouvelles) Bornes sup pour m_q and m_q^{sym}

q	2	3	4	5	8
m_q^{sym}	$5,834$	$5,143$	$3,889$	$3,903$	$3,500$
m_q	$5,834$	$5,143$	$3,889$	$3,903$	$3,500$
q	9	16	25	27	32
m_q^{sym}	$3,429$	$3,026$	$2,779$	$3,120$	$2,667$
m_q	$3,429$	$\mathbf{3,000}$	$\mathbf{2,667}$	$\mathbf{2,909}$	$\mathbf{2,625}$

Remark 2.13. Supposons que l'on puisse abaisser à 17 (ou 18) la borne sup pour $\mu_2(7,1)$ (c'est à dire la complexité bilinéaire de la multiplication dans $\mathbf{F}_{2^7}$), dont on sait seulement qu'elle se situe entre 17 and 22. Alors la borne sup pour la complexité asymétrique m_2 serait abaissée à $5,426$ (ou, resp., $5,745$). Cela résulterait de l'emploi de la tour de Bassa & al. [BBGS] sur $\mathbf{F}_{2^7}$ (en utilisant l'astuce du lemme 3.4).

2.4 Aspects effectifs

Considérons une extension d'un corps premier, e.g. $\mathbf{F}_{2^m}/\mathbf{F}_2$ et une courbe fixée X de genre g. Alors l'équation (1.11) (du §1.3 ci-dessous) impliquerait qu'il existe un algorithme de multiplication utilisant $2m + 2g + 3$ points d'interpolation (comptés avec degrés et multiplicités) sur la courbe X.

En pratique on peut espérer mieux pour le même degré m et la même courbe X. À titre d'indication, la proposition VI.3.4 établit qu'on ne pourra pas trouver d'algorithme avec moins de $2m + g - 1$ points d'interpolation. Il semble donc rester de la marge pour diminuer le nombre de points nécessaires.

En fait la méthode VI.3.6 permet de construire un tel algorithme de multiplication avec le nombre minimum de points $2m + g - 1$, dès lors qu'il en existe un.

Et cela semble être souvent le cas en pratique, du moins sur tous les exemples traités. Le tableau suivant 2.4 considère la multiplication bilinéaire dans les extensions du [NIST] et compare les bornes de [BBT] avec nos bornes obtenues avec les courbes modulaires classiques. Les données sont une compression des tableaux VI.4.1 et VI.4.1.

Table 2.4: Amélioration des bornes sup dans les extensions du NIST $\mathbf{F}_{2^m}/\mathbf{F}_2$

m	163	233	283	409	571
before	906	1340	1668	2495	3566
after	**900**	**1335**	**1654**	**2486**	**3555**

Comme noté dans le paragraphe final du VI.4.2, ces calculs remontent à 2014. Et pourraient donc être améliorés aujourd'hui avec les quotients d'Atkin–Lehner et aussi une courbe de Shimura de genre 5 issue du théorème B.

3 Contenu des chapitres techniques et plan des principaux arguments

3.1 Chapitre II

Bien que ce chapitre contienne essentiellement des résultats bien connus sur les algèbres de quaternions, son but est de clarifier certains points:

- Les deux courbes de Shimura connexes $X_0^+(\mathfrak{N})$ et $X_0(\mathfrak{N})$ ne coincident que lorsque le nombre de classes restreint de F est un (Proposition 3.2). Seule la première est connue pour avoir un modèle canonique avec beaucoup de points (cf. V.4 pour un exemple intéressant où elles ne coincident pas). Tandis que la deuxième, bien que plus accessible pour les calculs en tant que courbe complexe, a en général plusieurs modèles canoniques possibles (cf. [Sij$_1$, sous la Prop. 3.2.4]).
- Le groupe d'Atkin–Lehner est défini par l'équation (4.4). L'enjeu du §II.4.2 est d'expliquer pourquoi dans le cadre de cette thèse, ce groupe est simplement décrit par l'équation (4.3).

  Au contraire dans le cas général (sans l'hypothèse de nombre de classes restreint égal à un), le groupe d'Atkin–Lehner peut être strictement plus gros que la description précédente. Ceci est détaillé dans les références données dans la note de bas de page 3 de la Proposition 4.1. Cette difficulté supplémentaire (que nous n'aurons donc pas) peut arriver même si le niveau de l'ordre d'Eichler se résume à une puissance d'un idéal premier;

- Le corollaire 2.5 donne une condition suffisante pour que tous les ordres d'Eichler de niveau donné soient conjugués (cf. [Sij$_1$, Proposition 2.6.2] pour une classification plus fine). This allows the descent data of Theorem IV.5.11.
- quant au dernier point, qui résume le §II.5, cette section a trois buts:
    - expliquer comment le groupe $\mathrm{PSL}_2(R)$ d'un anneau local fini R agit sur l'ensemble $\mathbf{P}^1(R)$: cf. le Lemme 5.2. C'est la clé des calculs de monodromie du §IV.3.2;
    - fournir les formules calcul d'indice: Proposition 5.4 et corollaire 5.6. Remarquons que cet dernier peut en fait se déduire directement du théorème d'approximation forte pour les groupes arithmétiques;
    - et d'insister sur le fait que le groupe de congruence pertinent dans notre thèse, qui a une signification galoisienne, est: $\Gamma'(\mathfrak{N})$. Il peut être strictement plus gros que le groupe de congruence principal classique: $\Gamma(\mathfrak{N})$. ceci se produit lorsque la norme de $\mathfrak{N}$ est paire.

      En réalité, la Proposition II.5.7 a pour seul but d'insister sur ce fait. Mais en tant que telle elle n'est pas utilisée ailleurs dans la thèse.

3.2 Leitfaden du chapitre IV

Les trois résultats suivants:

(a) Théorème 4.12 (ii): un revêtement ramifié avec un groupe d'automorphismes trivial et corps de modules $\mathbf{Q}$, descend en un revêtement sur $\mathbf{Q}$. (i): De plus le revêtement descendu est *unique*, à $\mathbf{Q}$-isomorphisme de revêtements près;

(b) Théorème 5.11 Soit $X_0(1)$ une courbe de Shimura uniformisée par un groupe triangulaire avec des indices distincts. On suppose en outre que ce groupe provient d'une algèbre de quaternions, dont le discriminant est stable sous l'action du groupe de Galois du centre F de l'algèbre. Soit enfin $\mathfrak{N}$ un idéal de F Galois-stable. Alors le revêtement $X_0(\mathfrak{N})_F \longrightarrow X_0(1)_F$ a un corps de modules égal à $\mathbf{Q}$;

(c) Proposition 5.12: les revêtements ramifiés $X_0(\mathfrak{N})_F \longrightarrow X_0(1)_F$ n'ont pas d'automorphismes;

. . . impliquent le résultat principal :

Théorème 5.14 : soit $X_0(1)$ uniformisée par un groupe triangulaire d'indices distincts, provenant d'une algèbre de quaternions de discriminant Galois-stable. Soit $\mathfrak{N}$ un idéal stable sous Galois. Alors le revêtement canonique: $X_0(\mathfrak{N})_F \longrightarrow X_0(1)_F$ descend en un revêtement sur $\mathbf{Q}$. De plus: ce modèle descendu sur $\mathbf{Q}$ est unique à $\mathbf{Q}$-isomorphisme de revêtements près.

3.3 Leitfaden du chapitre V

Détaillons l'enchaînement logique de ce chapitre et son rôle dans la preuve du Théorème B. Les résultats effectifs sur les revêtements canoniques dont on a besoin sont extraits du §V.4 et récapitulés dans le Théorème C énoncé précédemment.

(a) l'interprétation modulaire de l'involution d'Atkin–Lehner (§2.3 paragraphe "Atkin–Lehner");
implique que:

(b) la flêche en pointillés φ du diagramme (3.2) de V.3.2 est surjective;

On a également:

(c) φ est injective;

Preuve: résulte de §2.1, qui exprime l'involution d'Atkin-Lehner dans notre hypothèse de nombre de classes restreint égal à un. Ou, comme suggéré en haut de la page 111 : montré dans [Duc, Proposition IV.5.1].

Ensuite, (b) + (c) implique que φ est bijective. ce qui implique que:

(d) les tours de courbes de Shimura sont récursives;

On a également :

(e) les premiers étages des tours considérées dans le V.5 descendent sur $\mathbf{F}_3$;

Preuve: le Théorème IV.5.14(i) d'unicité montre que les revêtements candidats trouvés dans §5.2 sont bien les revêtements canoniques. Nous les avons récapitulés ci-dessus dans le Théorème C.

Par conséquent (d) + (e) implique:

(f) les tours descendent toutes entières sur $\mathbf{F}_3$;

Enfin, la possibilité d'entrelacer des tours récursives de niveaux premiers entre eux (§V.3.1) + la densité des genres de la famille obtenue (§III.2.5) impliquent que:

(g) le Théorème B s'obtient de façon explicite à partir de courbes de Shimura.