N° d'ordre : 4374

THÈSE

présentée à

L'UNIVERSITÉ BORDEAUX I

ÉCOLE DOCTORALE DE MATHÉMATIQUES ET INFORMATIQUE

par **Florence Gillibert**

POUR OBTENIR LE GRADE DE

DOCTEUR

SPÉCIALITÉ : **Mathématiques Pures**

****

SURFACES ABÉLIENNES À MULTIPLICATION QUATERNIONIQUE ET POINTS RATIONNELS DE QUOTIENTS D'ATKIN-LEHNER DE COURBES DE SHIMURA

****

Soutenue le 2 décembre 2011 à l'Institut de Mathématiques de Bordeaux

Après avis de :

Victor ROTGER	Professeur, Universitat Politècnica de Catalunya	**Rapporteur**
Andrei YAFAEV	Reader, University College London	**Rapporteur**

Devant la commission d'examen composée de :

Pascal AUTISSIER	Professeur, Université Bordeaux I	
Yuri BILU	Professeur, Université Bordeaux I	**Co-directeur**
Pierre PARENT	Maître de Conférences, Université Bordeaux I	**Directeur**
Marusia REBOLLEDO	Maître de Conférences, Université Clermont-Ferrand 2	
Damian RÖSSLER	Directeur de Recherche CNRS, Université Toulouse 2	
Andrei YAFAEV	Reader, University College London	**Rapporteur**

– 2011 –

Table des matières

1 Introduction **4**
1.1 Courbes de Shimura et involutions d'Atkin-Lehner 5
1.2 Lien avec une conjecture de Coleman 7
1.3 Points rationnels sur les quotients d'Atkin-Lehner de courbes de Shimura de niveau 1 8
1.4 Surfaces abéliennes à multiplication potentiellement quaternionique munies d'une structure de niveau $\Gamma_0(N)$ 10

2 Points rationnels sur les quotients d'Atkin-Lehner de courbes de Shimura de discriminant pq **13**
2.1 Introduction 13
2.2 Vecteurs de Gross 15
2.2.1 Vecteurs de Gross sur le graphe modulaire 16
2.2.2 Vecteurs de Gross sur le graphe de Shimura 19
2.3 Groupe des composantes de $\mathrm{Jac}(X^{pq}/w_q)_{\mathbb{F}_p}$ 25
2.4 Points rationnels sur les courbes de Shimura 40

3 Surfaces abéliennes à multiplication quaternionique munies d'une structure de niveau $\Gamma_0(N)$ **44**
3.1 Introduction 44
3.2 Représentations associées aux surfaces abéliennes de type GL_2 48
3.3 Congruences satisfaites par les traces des substitutions de Frobenius 52
3.4 Preuve des résultats principaux 55

Remerciements

Je tiens à adresser à Pierre Parent mes remerciements les plus sincères. Pendant ces années de thèse il a encadré mon travail, répondu à mes questions, et m'a encouragée dans mes efforts. Je me réjouis d'avoir pu bénéficier de ses conseils avisés et de ses connaissances mathématiques, ainsi que de sa grande disponibilité. Merci d'avoir relu avec patience les versions successives des manuscripts de mes articles.

Je remercie également Victor Rotger et Andrei Yafaev pour avoir accepté de rapporter cette thèse, et pour l'intérêt qu'ils ont porté à mon travail. Je suis très reconnaissante à Victor et Andrei pour avoir répondu à mes questions.

Merci à Yuri Bilu avec lequel j'ai eu le plaisir de travailler pendant mon Master et qui a très gentiment accepté de co-encadrer ma thèse.

Marusia Rebolledo a eu l'amabilité de lire et de commenter entièrement le manuscript de mon premier article, je tiens à l'en remercier chaleureusement.

Pascal Autissier et Damian Rössler ont accepté de faire partie de ce jury, je les remercie de l'intérêt qu'ils portent à mon travail.

Je remercie Federico Pellarin pour avoir guidé mes premiers pas dans le domaine de la théorie des nombres. Je remercie également tous ceux qui m'ont accompagné pendant mes études à Caen et ma thèse à Bordeaux : les membres du LMNO de Caen, de l'IMB de Bordeaux, ainsi que Éva Bayer et les membres du MathGeom à Lausanne qui m'ont accueillie dans leur institut lors des derniers mois de ma thèse.

Je voudrais aussi saluer tous les doctorants et ATERs de l'IMB qui étaient à mes cotés durant ces années.

Je dois également exprimer ma gratitude à l'égard de ma famille pour m'avoir encouragée, durant tout ce temps. Enfin je remercie Gabriele pour son indéfectible soutien.

Chapitre 1

Introduction

Dans cette thèse nous abordons deux problèmes :

- l'absence de points rationnels non spéciaux sur certains quotients d'Atkin-Lehner de courbes de Shimura ;
- les structures de niveau possibles sur les surfaces abéliennes rationnelles à potentielle multiplication quaternionique.

Ces deux questions sont étroitement liées. Les courbes de Shimura peuvent être vues comme une généralisation des courbes modulaires : tout comme celles-ci paramétrisent les courbes elliptiques munies d'une structure de niveau, les courbes de Shimura paramétrisent les surfaces abéliennes à multiplication quaternionique munies d'une structure de niveau.

Nous nous intéressons plus précisément aux quotients d'Atkin-Lehner pour la raison suivante. Une surface abélienne $A/\mathbb{Q}$ peut acquérir multiplication quaternionique sur une extension $K/\mathbb{Q}$ mais n'a jamais multiplication quaternionique sur $\mathbb{Q}$. Une telle surface abélienne A correspond à un point K-rationnel d'une courbe de Shimura, se réduisant en un point rationnel sur l'un des quotients d'Atkin-Lehner de cette courbe de Shimura, et c'est pourquoi ces quotients sont les « espaces de modules » naturels pour nous.

L'étude des points des courbes de Shimura sur des corps de nombres, principalement sur des corps quadratiques imaginaires a fait l'objet de nombreux travaux, notament ceux de Jordan [9]. L'absence de points $\mathbb{Q}$-rationnels sur les quotients d'Atkin-Lehner de courbes de Shimura a été étudiée par Clark [3], Rotger, Skorobogatov et Yafaev [24], Bruin, Flynn, González et Rotger [2], ainsi que Parent et Yafaev [17] entre autres. Une première motivation pour démontrer l'absence de points rationnels sur ces quotients est de trouver des courbes, voire des familles infinies de courbes, contredisant le principe de Hasse sur $\mathbb{Q}$ (cf. [24]). Une autre motivation (peut-être plus profonde, car liée à des conjectures générales discutées plus loin), est de répondre à la question suivante : existe-t-il des surfaces abéliennes rationnelles ayant multiplication potentiellement quaternionique par une algèbre de quaternions fixée, éventuellement munies d'une structure de niveau ? Lorsque la réponse à cette question est négative, cette absence de surfaces abéliennes

peut-elle être expliquée par l'absence de points rationnels sur le quotient d'Atkin-Lehner de la courbe de Shimura correspondant à ce problème de modules ?

Ce sont ces deux questions qui ont retenu notre attention. Ainsi, l'objet de notre chapitre 2 est de montrer que certaines familles de quotients d'Atkin-Lehner de courbes de Shimura sont sans points rationnels (non spéciaux). Dans le chapitre 3, nous allons « dans l'autre sens ». Sachant l'absence de points rationnels sur des quotients d'Atkin-Lehner de courbes de Shimura de niveau N pour N supérieur à une borne non effective (ce qui découle des résultats de Falings et Ohta), nous déterminons des bornes effectives pour les structures de niveau en travaillant directement sur l'arithmétique des surfaces abéliennes rationnelles à multiplication quaternionique.

1.1 Courbes de Shimura et involutions d'Atkin-Lehner

Rappelons d'abord brièvement la construction des courbes modulaires $X_0(N)$ sur $\mathbb{C}$ pour $N \geq 1$. On associe à l'entier $N \geq 1$ le groupe de congruence $\Gamma_0(N)$, sous-groupe de $\mathrm{SL}_2(\mathbb{Z})$ défini par :

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \ : \ c \equiv 0 \mod N \right\}.$$

Le groupe $\mathrm{SL}_2(\mathbb{Z})$ agit par homographie sur le demi-plan de Poincaré. On note $Y_0(N)$ la surface de Riemann obtenue en quotientant le demi-plan de Poincaré par l'action de $\Gamma_0(N)$. Cette surface de Riemann non compacte paramétrise les classes d'isomorphismes de courbes elliptiques $E/\mathbb{C}$ munies d'une isogénie cyclique de degré N. La courbe modulaire $X_0(N)/\mathbb{C}$, est la surface de Riemann obtenue en compactifiant $Y_0(N)/\mathbb{C}$ par l'ajout de pointes.

La construction des courbes de Shimura et leur interprétation comme espace de module est analogue, comme nous allons le voir. Soit B_D une algèbre de quaternions sur $\mathbb{Q}$, de discriminant D et O_D un ordre maximal de B_D. On suppose que B_D est indéfinie, c'est à dire $B_D \otimes \mathbb{R} \simeq \mathrm{M}_2(\mathbb{R})$. Dans ce cas le discriminant D de B_D est le produit d'un nombre pair de nombres premiers. Soit N un entier premier à D. Les ordres d'Eichler de niveau N de B_D sont tous conjugués. Fixons O un tel ordre d'Eichler et O^1 le groupe multiplicatif constitué des éléments de norme réduite 1 de O. On peut associer au couple (D, N) un groupe Fuchsien image de O^1 par l'inclusion $B_D \hookrightarrow B_D \otimes \mathbb{R} \simeq \mathrm{M}_2(\mathbb{R})$. On considère la surface de Riemann obtenue en effectuant le quotient du demi-plan de Poincaré par ce groupe. Lorsque $D \neq 1$ ce quotient est compact. Par définition, c'est la courbe de Shimura $X_0^D(N)/\mathbb{C}$ de discriminant D et de niveau N. Lorsque $D = 1$, l'algèbre de quaternions B_1 est l'algèbre de matrices $M_2(\mathbb{Q})$, et le groupe O^1 est le sous-groupe de congruence $\Gamma_0(N)$ de $\mathrm{SL}_2(\mathbb{Z})$. Le quotient est la surface de Riemann $Y_0(N)/\mathbb{C}$, la surface de Riemann obtenue en compactifiant $Y_0(N)$ est la courbe de Shimura $X_0^1(N)/\mathbb{C}$ déjà vue comme courbe modulaire $X_0(N)/\mathbb{C}$. Les courbes de Shimura sont des espaces de modules pour le problème de modules énoncé dans la proposition 1.1.1 ci-dessous :

Proposition 1.1.1. *La courbe de Shimura $X_0^D(N)/\mathbb{C}$ est un espace de modules paramétrisant les triplet (A, ι, Q_N) à isomorphisme près, constitués d'une surface abélienne $A/\mathbb{C}$, d'un plongement $\iota\colon O_D \to \mathrm{End}_{\mathbb{C}}(A)$ et d'une N^2-isogénie de A de noyau $Q_N \simeq \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ qui est O_D-cyclique, c'est-à-dire il existe $P \in Q_N$ tel que $Q_N = O_D \cdot P$.*

Dans la suite, nous appellerons une surface abélienne A munie d'un tel plongement ι et d'un tel sous-groupe Q_N, une surface abélienne à multiplication quaternionique munie d'une structure de niveau $\Gamma_0(N)$. Certaines de ces surfaces abéliennes ne sont pas des surfaces abéliennes simples. Elles sont alors isogènes au carré d'une courbe elliptique ayant multiplication complexe par un ordre dans un corps quadratique imaginaire K tel que B_D se plonge dans $M_2(K)$.

Définition 1.1.2. Un point de la courbe de Shimura $X_0^D(N)$ est appelé spécial ou CM si la surface abélienne sous-jacente est isogène au carré d'une courbe elliptique ayant multiplication complexe.

On peut définir un modèle de $X_0^D(N)$ sur $\mathbb{Q}$, qui est un espace de modules pour le problème de modules correspondant sur $\mathbb{Q}$. La courbe modulaire $X_0^1(N)$ est un espace de modules pour les couples (E, C_N) à isomorphisme près, constitué d'une courbes elliptiques E munies d'une N-isogénie cyclique C_N. Cet espace de modules jouit de la propriété suivante : pour un couple $(E, C_N)/\overline{\mathbb{Q}}$ et un corps de nombre K, si (E, C_N) correspond à un point K-rationnel de $X_0^1(N)$, alors il existe un modèle de (E, C_N) sur K. Pour $D > 1$, l'espace de module $X_0^D(N)$ n'a pas ces propriétés : pour tout point x de $X_0^D(N)(K)$, il existe un triplet $(A, \iota, Q_N)_{\overline{\mathbb{Q}}})$ associé à une surface abélienne à multiplication quaternionique munie d'une structure de niveau $\Gamma_0(N)$ comme dans la Proposition 1.1.1, tels que (A, ι, Q_N) correspond à x, mais on n'a pas nécessairement de modèle de (A, ι, Q_N) sur K. C'est pourquoi nous devons distinguer le corps de modules et les corps de définitions. C'est l'objet de la définition 1.1.3 ci-dessous.

Définition 1.1.3. Soit $(A, \iota, Q_N)/\overline{\mathbb{Q}}$ un triplet constitué d'une surface abélienne $A/\overline{\mathbb{Q}}$, d'un plongement $\iota\colon O_D \to \mathrm{End}_{\overline{\mathbb{Q}}}(A)$ et d'une N^2-isogénie de A de noyau $Q_N \simeq \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ qui est O_D-cyclique.

- Un corps de définition de (A, ι, Q_N) est un corps L tel que (A, ι, Q_N) admet un modèle sur L.
- Le corps de modules de (A, ι, Q_N) est le plus petit corps M tel que le point de $X_0^D(N)$ correspondant à (A, ι, Q_N) est défini sur M.

Un corps de définition contient le corps de modules. Par contre en général le corps de modules n'est pas un corps de définition. Le problème de la différence entre le corps de modules et le corps de définition est étudié par Jordan dans l'article [9].

Il découle des travaux de Drinfeld que pour tout nombre premier p, l'on peut également définir un modèle de $X_0^D(N)$ sur $\mathbb{Z}_p$ attaché au problème de modules correspondant sur $\mathbb{Z}_p$. En particulier nous nous intéresserons dans le chapitre 2 au cas décrit par Cerednick et Drinfeld, c'est à dire au cas où p divise D.

Pour un discriminant D et un niveau N fixé, on peut définir un groupe d'involutions sur $X_0^D(N)/\mathbb{Q}$, appelé groupe des involutions d'Atkin-Lehner. Ce groupe est engendré par deux types d'involutions, comme nous allons l'expliquer. À un nombre premier p divisant N, on associe l'involution d'Atkin-Lehner w_{p^k}, où $k \in \mathbb{N}$ est tel que $p^k \,||\, N$. Les involutions de ce type sont définies de manière analogue aux involutions d'Atkin-Lehner de la courbe modulaire $X_0(N)$. Pour un nombre premier p divisant D, on définit également une involution d'Atkin-Lehner w_p. Décrivons l'action de ces deux types d'involution sur l'espace de modules. Soit $(A, \iota, Q_N)/\overline{\mathbb{Q}}$ un triplet comme dans la proposition 1.1.1 ci-dessus. Pour un nombre premier p divisant le niveau N, tel que $p^k \,||\, N$, on a :

$$w_{p^k}(A, \iota, Q_N) = (A/Q_{p^k}, \pi_{p^k} \circ \iota, (A[p^k] + Q_N)/Q_{p^k}),$$

où Q_{p^k} désigne l'unique sous-groupe de Q_N de cardinal p^{2k} et π_{p^k} est le morphisme $\mathrm{End}_{\overline{\mathbb{Q}}}(A) \to \mathrm{End}_{\overline{\mathbb{Q}}}(A/Q_{p^k})$ induit par l'isogénie de noyau Q_{p^k}. Pour un nombre premier p divisant D, on a :

$$w_p(A, \iota, Q_N) = (A, \alpha_p^* \circ \iota, Q_N),$$

où $\alpha_p^* \colon O_D \to O_D$ est l'automorphisme de O_D donné par la conjugaison par un élément α_p de norme p appartenant au normalisateur de O_D. Pour $n \mid DN$ et $m \mid DM$ premiers entre eux on a $w_{mn} = w_n w_m$. Dans cette thèse nous nous intéressons uniquement aux involutions de la forme w_m pour m divisant D.

1.2 Lien avec une conjecture de Coleman

Soit B_D l'algèbre de quaternions sur $\mathbb{Q}$ indéfinie de discriminant D et O_D un ordre maximal de B_D. Fixons un corps de nombre L. À la question : « Existe-t-il des surfaces abéliennes A/L à multiplication quaternionique par O_D ? » correspond la question : « Existe-t-il des points L-rationnels sur $X_0^D(1)$? » L'absence de points L-rationnels sur $X_0^D(1)$ est en fait une propriété plus forte que la non-existence de surfaces abéliennes A/L munies d'une structure de niveau $\Gamma_0(N)$ à cause de la différence entre corps de modules et corps de définition discutée plus haut. Comme on l'a évoqué encore, c'est un fait bien connu que les courbes de Shimura n'ont pas de point rationnel, ni même de point réel. Tout comme le fait que pour une surface abélienne $A/\mathbb{R}$, l'anneau $\mathrm{End}_{\mathbb{R}}(A)$ ne contient pas d'ordre dans une algèbre de quaternions. Ce qui nous amène à nous intéresser aux surfaces abéliennes rationnelles $A/\mathbb{Q}$ ayant *potentiellement multiplication quaternionique*, c'est-à-dire telle que $\mathrm{End}_{\overline{\mathbb{Q}}}(A) \otimes \mathbb{Q}$ est une algèbre de quaternions. Considérons donc la nouvelle question : « Existe-t-il des surfaces abéliennes rationnelles simples $A/\mathbb{Q}$ à multiplication potentiellement quaternionique par O_D ? » Grâce aux travaux de Bruin, Flynn, Gonzáles et Rotger [2, thm 4.5] (ou théorème 1.2.1 ci-dessous) on sait que le point correspondant à une telle surface abélienne simple sur la courbe de Shimura $X_0^D(1)(\overline{\mathbb{Q}})$ se réduit en un point rationnel non spécial d'un quotient d'Atkin-Lehner $X_0^D(1)/w_m$ pour un certain m divisant D.

Théorème 1.2.1. *(Bruin, Flynn, Gonzales, Rotger) Soit B_D une algèbre de quaternions sur $\mathbb{Q}$, indéfinie de discriminant D. Soit O_D un ordre maximal de B_D. Il existe une surface abélienne $A/\mathbb{Q}$ telle que $\mathrm{End}_{\overline{\mathbb{Q}}}(A) \simeq O_D$ si et seulement s'il existe un point rationnel non spécial Q sur le quotient $X_0^D(1)/w_m$ de la courbe de Shimura de discriminant D et de niveau 1 par l'involution d'Atkin-Lehner w_m, où m est tel que $\mathrm{End}_{\mathbb{Q}}(A) \otimes \mathbb{Q} \simeq \mathbb{Q}(\sqrt{m})$, satisfaisant les conditions suivantes : le point Q est la projection sur $X_0^D(1)/w_m$ d'un point de $X_0^D(1)(K)$ pour un corps $K = \mathbb{Q}(\sqrt{-d})$ quadratique imaginaire satisfaisant :*

$$B_D \simeq \left(\frac{-d, m}{\mathbb{Q}}\right).$$

Autrement dit B_D est l'algèbre de quaternions donnée par $B_D \simeq \mathbb{Q} \oplus \mathbb{Q}i \oplus \mathbb{Q}j \oplus \mathbb{Q}k$ avec $i^2 = -d$, $j^2 = m$ et $ij = -ji = k$.

On dit qu'une variété abélienne simple $A/\mathbb{Q}$ est de type GL_2 si son algèbre d'endomorphisme $\mathrm{End}_{\mathbb{Q}}(A) \otimes \mathbb{Q}$ est un corps de nombre de degré $\dim(A)$. L'étude de l'existence et de la non-existence de points rationnels non-spéciaux sur les quotients d'Atkin-Lehner de courbes de Shimura $X_0^D(1)$ permet de déterminer les corps de quaternions contenant un ordre maximal isomorphe à l'anneau des endomorphismes d'une surface abélienne $A/\mathbb{Q}$ et d'aborder une conjecture de Coleman, énoncée ainsi par Clark et Mazur :

Conjecture 1.2.1. (Coleman, Clark, Mazur) Soit $g \geq 1$ un entier fixé. Il existe un nombre fini de classes d'isomorphismes d'anneaux d'endomorphismes sur $\overline{\mathbb{Q}}$ de variété abéliennes $A/\mathbb{Q}$ de type GL_2 de dimension g.

Lorsque la dimension g est 1, une telle variété abélienne est une courbe elliptique, et la conjecture est vraie dans ce cas par les résultats classiques, mais non triviaux, de la multiplication complexe. En effet l'anneau des endomorphismes d'une courbe elliptique rationnelle est soit $\mathbb{Z}$, soit un ordre de nombre de classes 1 dans un corps quadratique imaginaire. La liste de ces 13 ordres est bien connue (cf.[30, p. 483]). Lorsque $g \geq 2$, la conjecture est ouverte. Si A est une variété abélienne simple, on sait que l'anneau $\mathrm{End}_{\overline{\mathbb{Q}}}(A) \otimes \mathbb{Q}$ peut être isomorphe à un corps de nombres totalement réel, à une algèbre de quaternions sur un corps de nombre totalement réel, ou bien un corps gauche ayant pour centre un corps à multiplication complexe. L'étude des points rationnels sur les quotients d'Atkin-Lehner de courbes de Shimura permet donc d'aborder le problème dans le cas $g = 2$ pour les surfaces abéliennes à multiplication potentiellement quaternionique par un ordre maximal dans une algèbre de quaternions indéfinie.

1.3 Points rationnels sur les quotients d'Atkin-Lehner de courbes de Shimura de niveau 1

Dans ce paragraphe nous allons expliquer les résultats du premier chapitre de notre thèse. Le problème étudié est le suivant : trouver des familles les plus grandes possibles

de quotients $X_0^D(N)/w_m$ de courbes de Shimura de discriminant D et de niveau N par des involutions d'Atkin-Lehner w_m, où $m \mid D$, sans point rationnel non spécial. Si la conjecture de Coleman est vraie, sauf pour un nombre fini de discriminants, le quotient $X_0^D(N)/w_m$ ne contient que des points « non modulaires », c'est-à-dire des points associés à des surfaces abéliennes ayant un corps de module différent de leur corps de définition. En fait, il est également conjecturé que ces quotients sont vides sauf pour un nombre fini de discriminants. C'est cette question que nous aborderons, en considérant toutefois un cas non modulaire.

Nous nous restreignons dans le premier chapitre au cas où D est le produit de deux nombres premiers impairs distincts ($N = 1$). Un théorème de Ogg donne des conditions pour l'existence de points locaux au quotient $X_0^D(N)/w_m$. Nous énonçons ici un corollaire de ce résultat dans ce cas particulier (cf. [24, thm 3.1]).

Proposition 1.3.1. *(Ogg) Soient p et q deux nombres premiers impairs distincts. Si $X_0^{pq}(1)/w_q(\mathbb{Q})$ est non vide, alors $\left(\frac{p}{q}\right) = -1$, et une des deux conditions suivantes est satisfaite*

(1) $p \equiv 3 \mod 4$; (cas ramifié)
(2) $p \equiv 1 \mod 4$ et $q \equiv 3 \mod 4$ (cas non ramifié).

Il découle des travaux de Rotger (cf [23]) que lorsque $p \equiv 1 \mod 4$ il n'y a pas de surfaces abéliennes $A/\mathbb{Q}$ telle que $\mathrm{End}_{\mathbb{Q}}(A)$ est l'anneau des entiers de $\mathbb{Q}(\sqrt{p})$ et $\mathrm{End}_{\overline{\mathbb{Q}}}(A)$ est isomorphe à un ordre maximal dans l'algèbre de quaternions B_{pq} de discriminant pq. Ce qu'on peut traduire par : il n'y a pas de point rationnel non spécial et « modulaire » sur le quotient d'Atkin-Lehner $X_0^{pq}(1)/w_q$ dans le cas non ramifié de Ogg. On se pose la question de l'existence de points rationnels non spéciaux sur le quotient $X_0^{pq}(1)/w_q$ dans ce cas. Parent et Yafaev donnent un critère dans le cas non ramifié de Ogg pour la non-existence de points rationnels non-spéciaux sur le quotient d'Atkin-Lehner $X_0^{pq}(1)/w_q$ (voir théorème 2.4.3 ci-dessous). Pour cela l'article [17] considère la réduction d'un éventuel point rationnel sur la fibre spéciale $(X_0^{pq}(1)/w_q)_{\mathbb{F}_p}$ du modèle de Cerednick-Drinfeld de $(X_0^{pq}(1)/w_q)/\mathbb{Z}_p$. Cette fibre est une union de courbes de genre 0 se coupant transversalement. Cet objet combinatoire est entièrement déterminé par la donnée de son graphe dual. Les sommets de ce graphe, noté $\mathcal{G}((X_0^{pq}(1)/w_q)_{\mathbb{F}_p})$, sont les composantes de la fibre $(X_0^{pq}(1)/w_q)_{\mathbb{F}_p}$ et ses arêtes sont les points d'intersections entre ces composantes. Dans le cas d'une courbe de Shimura dont le discriminant est le produit de deux nombres premiers, le graphe $\mathcal{G}((X_0^{pq}(1)/w_q)_{\mathbb{F}_p})$ a été décrit de manière précise par Ribet dans [21]. Pour vérifier le critère de Parent et Yafaev, il faut construire un chemin sur le graphe $\mathcal{G}((X_0^{pq}(1)/w_q)_{\mathbb{F}_p})$, satisfaisant certaines propriétés. Ce critère leur permet de donner des familles infinies de quotients d'Atkin-Lehner de courbes de Shimura sans point rationnel non spécial, comme par exemple, celle des courbes de la forme $X^{251p}(1)/w_{251}$. Mais la vérification de ce critère n'était jusqu'alors possible que dans de tels cas particuliers.

L'objet de notre premier chapitre est d'expliquer comment vérifier ce critère de façon plus générale. Nous y arrivons pour presque tous les couples (p, q) à q fixé. L'idée essentielle

est de développer la comparaison entre les propriétés du graphe $\mathcal{G}((X_0^{pq}(1)/w_q)_{\mathbb{F}_p})$ et du graphe dual de la fibre en q de la courbe modulaire $X_0(q)$, ce qui nous permet de démontrer le résultat suivant :

Théorème 1.3.2. *Soit $q > 245$ un nombre premier avec $q \equiv 3 \mod 4$. Il existe une borne B_q dépendant de q telle que si p est un nombre premier vérifiant $p \equiv 1 \mod 4$, $\left(\frac{p}{q}\right) = -1$ et $p \geq B_q$, alors la courbe $X_0^{pq}(1)/w_q$ est sans point rationnel non spécial.*

La nature de notre preuve semble exclure de déterminer la borne B_q de façon effective. À cette réserve près, on vérifie donc le critère principal de [17] en généralité presque maximale.

1.4 Surfaces abéliennes à multiplication potentiellement quaternionique munies d'une structure de niveau $\Gamma_0(N)$

Dans notre second chapitre nous étudions le problème suivant : soit B_D une algèbre de quaternions de discriminant D et O_D un ordre maximal de B_D. Quelles sont les structures de niveau possibles du type $\Gamma_0(N)$, avec N premier, pour les surfaces abéliennes rationnelles ayant multiplication potentiellement quaternionique par O_D ? Remarquons que le cas $D = 1$ correspond au cas des courbes elliptiques munies d'une isogénie rationnelle cyclique, et l'ensemble des degrés de ces isogénies est fini. Dans son célèbre article [12], Mazur décrit en effet l'ensemble des isogénies rationnelles de degré premier entre courbes elliptiques rationnelles.

Comme nous l'avons expliqué ci-dessus (cf. théorème 1.2.1) une surface abélienne $A/\mathbb{Q}$ admettant multiplication quaternionique sur $\overline{\mathbb{Q}}$ par un ordre maximal dans l'algèbre de quaternions indéfinie B_D de discriminant D correspond à un point rationnel sur un le quotient d'Atkin-Lehner $X_0^D(1)/w_m$ pour un certain nombre premier m divisant D. D'après le théorème 1.2.1 on sait que m est tel que l'anneau $\mathrm{End}_{\mathbb{Q}}(A)$ des endomorphismes sur $\mathbb{Q}$ de A est un ordre dans le corps $\mathbb{Q}(\sqrt{m})$. Supposons qu'en outre A est munie d'une structure de niveau $\Gamma_0(N)$, c'est à dire A admet une N^2-isogénie O_D-cyclique de noyau $Q_N \simeq \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$. Alors le point rationnel de $X_0^D(1)/w_m$ associé à A se relève en un point rationnel de $X_0^D(N)/w_m$. Une première approche pour répondre à notre question consiste à regarder pour quelles valeurs de N des points de $(X_0^D(1)/w_m)(\mathbb{Q})$ peuvent se relever en des points de $(X_0^D(N)/w_m)(\mathbb{Q})$. Lorsque le genre de $X_0^D(N)/w_m$ est > 1, il découle du théorème de Faltings que $X_0^D(1)/w_m(\mathbb{Q})$ est fini. Il résulte en outre d'un théorème d'Ohta que chacun des points de $X_0^D(1)/w_m(\mathbb{Q})$ ne se relève en un point de $X_0^D(N)/w_m(\mathbb{Q})$ que pour un nombre fini de N. On en déduit le théorème suivant, énoncé par Clark dans sa thèse :

Théorème 1.4.1. *(Faltings, Ohta). Soit D le discriminant d'une algèbre de quaternions B_D indéfinie et m un diviseur de D. On suppose que le genre de $X_0^D(1)/w_m$ est ≥ 2. Pour tout corps de nombres F, il existe une borne M telle que pour $N \geq M$, la courbe $X_0^D(N)/w_m$ n'a pas de point F-rationnel.*

En employant des méthodes similaires à la méthode de Mazur, Clark prouve dans sa thèse [3, Main Theorem 4] le résultat partiel ci-dessous. Ce théorème affine le résultat du théorème 1.4.1 dans le cas $m = D$ en supprimant la condition sur le genre de $X_0^D(1)/w_D$.

Théorème 1.4.2. *(Clark) Soit D le discriminant d'une algèbre de quaternions B_D sur $\mathbb{Q}$ indéfinie. Pour tout corps de nombres F, et pour tout corps quadratique imaginaire K, il existe une borne absolue M telle que pour un nombre premier $N \geq M$ satisfaisant $N \equiv 1 \mod 4$ et N reste premier dans F, il n'existe pas de point F-rationnel de $X_0^D(N)/w_D$ provenant d'un point de $X_0^D(N)(K)$.*

Mentionnons également des travaux récents (non encore publiés) de Momose et Arai : pour un corps quadratique fixé, il n'y a pas de point K-rationnel non spécial sur la courbe de Shimura $X_0^D(p)$ pour p assez grand.

Un corollaire de ces résultats est l'existence d'une borne sur les structures de niveau possibles sur les surfaces abéliennes $A/\mathbb{Q}$ ayant multiplication quaternionique par un ordre maximal de B_D sur une extension $K/\mathbb{Q}$ fixée. Mais même le résultat du théorème 1.4.1 est non effectif, le théorème de Faltings étant non-effectif. Nous nous proposons de rendre la borne le plus explicite possible. Nous parvenons à démontrer l'existence d'une borne effective dans le résultat suivant :

Théorème 1.4.3. *Il existe une constante absolue et effective C, telle que pour toute algèbre de quaternions sur $\mathbb{Q}$ indéfinie B_D, de discriminant D, pour tout corps quadratique imaginaire $K = \mathbb{Q}(\sqrt{-d})$, où d est un entier sans facteurs carré, pour toute surface abélienne $A/\mathbb{Q}$, telle que $\mathrm{End}_K(A) \simeq O_D$ est un ordre maximal de B_D et pour tout nombre premier $N \geq C(\mathrm{ppcm}(D,d))^{22}$, la surface A n'admet pas d'isogénie O_D-cyclique de noyau $\simeq \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$.*

Cette borne dépend du corps de nombres K sur lequel A acquiert multiplication quaternionique. Nous savons, d'après le théorème 1.4.1, que lorsque le genre de $X_0^D(1)/w_m$ est > 1, il existe une borne sur le nombre de structures de niveau possibles pour les surfaces abéliennes $A/\mathbb{Q}$ telles que $\mathrm{End}_{\mathbb{Q}}(A) \otimes \mathbb{Q} \simeq \mathbb{Q}(\sqrt{m})$ et $\mathrm{End}_{\overline{\mathbb{Q}}}(A) \simeq O_D$ qui est indépendante du corps de nombres K sur lequel A acquiert multiplication quaternionique. Il serait particulièrement intéressant de pouvoir calculer cette borne. On remarque que ceci est possible lorsque $m \neq D$ car dans ce cas il y a un nombre fini de possibilités pour K, ce qui nous permet d'obtenir le théorème 1.4.4 ci-dessous.

Théorème 1.4.4. *Soit C la constante donnée par le théorème 1.4.3. Soient B_D une algèbre de quaternions sur $\mathbb{Q}$ indéfinie, de discriminant D, et O_D un ordre maximal de B_D.*

Soit $E = \mathbb{Q}(\sqrt{m})$ un corps quadratique réel. On suppose qu'il existe un nombre premier impair $p \mid D$ et $p \nmid m$. Alors pour toute surface abélienne $A/\mathbb{Q}$ telle que $\mathrm{End}_{\overline{\mathbb{Q}}}(A) \simeq O_D$, et $\mathrm{End}_{\mathbb{Q}}(A) \simeq R_E$ soit l'anneau des entiers de E, pour tout nombre premier $N \geq CD^{22}$, la surface A n'admet pas d'isogénie O_D-cyclique de noyau $\simeq \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$.

Rappelons que les deux chapitres suivants, dont les contenus viennent d'être discutés, correspondent à deux articles (ce qui implique certaines répétitions, entre eux et avec la présente introduction). Le premier article est actuellement soumis, le second le sera prochainement.

Chapitre 2

Points rationnels sur les quotients d'Atkin-Lehner de courbes de Shimura de discriminant pq

2.1 Introduction

La recherche de quotients d'Atkin-Lehner de courbes de Shimura sans point rationnel non spécial a été l'objet de plusieurs travaux notamment de Clark [3], Rotger [23], Rotger, Skorobogatov et Yafaev [24], Bruin, Flynn, González et Rotger [2], ainsi que de Parent et Yafaev [17]. Pour des équations de ces courbes, on peut aussi consulter les travaux (à paraître) de Molina [13]. Ce problème est lié à une conjecture (attribuée à Coleman) sur les anneaux d'endomorphismes potentiels de variétés abéliennes de type GL_2 (cf. [2]). On dit qu'une variété abélienne $A/\mathbb{Q}$ est de type GL_2 si son algèbre d'endomorphisme $\mathrm{End}_{\mathbb{Q}}(A) \otimes \mathbb{Q}$ est un corps de nombre de degré $\dim(A)$. La conjecture est énoncée ainsi par Clark et Mazur : pour toute dimension g fixée, il y a un nombre fini de classes d'isomorphismes d'anneaux d'endomorphismes sur $\overline{\mathbb{Q}}$ de variétés abéliennes $A/\mathbb{Q}$ de type GL_2 de dimension g. Dans le cas $g = 1$, ces variétés abéliennes sont les courbes elliptiques, et la liste finie des anneaux d'endomorphismes possibles est connue. L'étude des courbes de Shimura permet d'aborder cette conjecture dans le cas de la dimension $g = 2$. En effet, étant donnés une algèbre de quaternion B_D de discriminant D, et un entier sans facteur carré m, toute surface abélienne $A/\mathbb{Q}$, telle que $\mathrm{End}_{\mathbb{Q}}(A) \otimes \mathbb{Q} = \mathbb{Q}(\sqrt{m})$ et $\mathrm{End}_{\overline{\mathbb{Q}}}(A)$ soit un ordre maximal de B_D, est associée à un point rationnel non spécial sur le quotient X^D/w_m de la courbe de Shimura de discriminant D par l'involution d'Atkin-Lehner w_m (cf. [2, thm 4.5]). L'absence de point rationnel non spécial sur X^D/w_m est en fait un problème plus fort que l'absence de telles surfaces abéliennes $A/\mathbb{Q}$; en effet de tels points rationnels peuvent correspondre à des surfaces abéliennes à multiplication quaternionique définies sur une extension de $\mathbb{Q}$ et admettant $\mathbb{Q}$ comme corps de module.

Dans cet article, nous nous restreignons au cas où le discriminant D de la courbe de

Shimura est le produit de deux nombres premiers p et q. L'existence de points rationnels sur X^{pq}/w_q peut se produire dans deux cas décrits par Ogg (cf. proposition 2.2.1) : le « cas ramifié » et le « cas non ramifié ». Nous nous plaçons dans le cas non ramifié de Ogg. Remarquons que dans ce cas l'absence de surfaces abéliennes à multiplication quaternionique découle d'un résultat de Rotger : [23, thm 1.4]. Dans leur article [17], Parent et Yafaev donnent un critère, pour l'absence de point rationnel non spécial sur un quotient d'Atkin-Lehner X^{pq}/w_q de courbe de Shimura dont le discriminant est le produit de deux nombres premiers. Nous rappelons leur énoncé dans la proposition 2.4.3. Une application immédiate de ce critère leur permet de déterminer un exemple de famille infinie de quotients d'Atkin-Lehner de courbes de Shimura sans point spécial, de la forme X^{251p}/w_{251}, mais la vérification de ce critère n'était jusqu'alors possible que dans de tels cas particuliers. Dans cet article nous appliquons ce critère à des courbes X^{pq}/w_q beaucoup plus générales. En fait pour presques toutes à q fixé : pour tout nombre premier $q > 245$, et tout nombre premier p supérieur à une borne (non effective) dépendant de q, si la condition du cas non ramifié de Ogg est satisfaite (cf. proposition 2.2.1 ci-dessous), alors nous pouvons appliquer le critère.

Théorème 2.1.1. *Soit $q > 245$ un nombre premier avec $q \equiv 3 \mod 4$. Il existe une borne B_q dépendant de q telle que si p est un nombre premier vérifiant $p \equiv 1 \mod 4$, $\left(\frac{p}{q}\right) = -1$ et $p \geq B_q$, alors la courbe X^{pq}/w_q est sans point rationnel non spécial.*

Résumons ici la preuve (on renvoie au texte pour les définitions et énoncés précis) : Le critère de Parent et Yafaev proposition 2.4.3 ne peut être appliqué qu'à des couples de nombres premiers (p, q) satisfaisant les conditions du cas non ramifié de Ogg ((2) proposition 2.2.1) et la condition supplémentaire $p \equiv -1 \mod 3$. Nous généralisons ce théorème dans la proposition 2.4.4 en supprimant cette dernière condition. Celle-ci apparaît dans un lemme de Parent et Yafaev sur le groupe des composantes de $\mathrm{Jac}(X^{pq}/w_q)_{\mathbb{F}_p}$. On considère $\widetilde{(X^{pq}/w_q)}_{\mathbb{F}_p}$ la fibre en p du modèle régulier de X^{pq}/w_q, obtenu par éclatement aux points singuliers du modèle décrit par Cherednik et Drinfeld. Supposons que p et q satisfont les conditions du cas non ramifié de Ogg, et que q est « assez grand ». Soit $\mathcal{J}$ la composante exceptionnelle de $\widetilde{(X^{pq}/w_q)}_{\mathbb{F}_p}$ apparaissant après éclatement de l'unique point singulier d'épaisseur 2, et $J \neq \mathcal{J}$ une autre composante irréductible de $\widetilde{(X^{pq}/w_q)}_{\mathbb{F}_p}$. Parent et Yafaev prouvent que si $p \equiv -1 \mod 3$, pour $p \gg q$, on a $(p+1)(J - \mathcal{J}) \neq 0$ dans le groupe des composantes de $\mathrm{Jac}(X^{pq}/w_q)_{\mathbb{F}_p}$ (cf. [17, lemma 3.1.3]). Dans le troisième paragraphe nous généralisons ce lemme en montrant que le résultat reste valable si $p \equiv 1 \mod 3$ (cf. lemme 2.3.2).

Dans le quatrième paragraphe, nous appliquons le critère de Parent-Yafaev (théorème 2.4.4) pour prouver le théorème 2.1.1. Pour cela il suffit de construire un cycle sur le graphe $\mathscr{G}(X^{pq}_{\mathbb{F}_p}/w_q)$ constitué de vecteurs de Gross contenant l'arête exceptionnelle de longueur 2 avec une multiplicité première à p. Le chemin que nous construisons utilise également le vecteur d'Eisenstein qui appartient à l'espace engendré par les vecteurs de

Gross. Comme les vecteurs de Gross sont invariants par l'action de w_q, nous travaillons sur $\mathscr{G}(X^{pq}_{\mathbb{F}_p})$. Nous utilisons la description du graphe de $\mathscr{G}(X^{pq}_{\mathbb{F}_p})$ donnée par Ribet. Le groupe des chemins $\mathcal{L}$ sur $\mathscr{G}(X^{pq}_{\mathbb{F}_p})$ est isomorphe au groupe des diviseurs sur les p-isogénies entre courbes elliptiques supersingulières en caractéristique q à isomorphisme près. D'autre part le groupe des chemins $\mathcal{P}_S$ sur le graphe $\mathscr{G}(X_0(q)_{\mathbb{F}_q})$ est isomorphe au groupe des diviseurs sur les courbes elliptiques supersingulières en caractéristique q à isomorphisme près. Le groupe des cycles sur $\mathscr{G}(X^{pq}_{\mathbb{F}_p})$ est l'intersection des noyaux de deux morphismes naturels s_* et t_* de $\mathcal{L}$ dans $\mathcal{P}_S$.

Pour éviter la confusion entre les vecteurs de Gross sur le graphe $\mathscr{G}(X_0(q)_{\mathbb{F}_q})$ et les vecteurs de Gross sur le graphe $\mathscr{G}(X^{pq}_{\mathbb{F}_p})$, nous les désignons respectivement par vecteurs de Gross-modulaire (cf. définition 2.2.4) et vecteurs de Gross-Shimura (cf. définition 2.2.11). De même, le vecteur d'Eisenstein sur $\mathscr{G}(X_0(q)_{\mathbb{F}_q})$ et le vecteur d'Eisenstein sur $\mathscr{G}(X^{pq}_{\mathbb{F}_p})$ sont appelés respectivement vecteur d'Eisenstein-modulaire et vecteur d'Eisenstein-Shimura.

Nous prouvons (sous certaines condition sur l'ordre O_D de discriminant D) que l'image d'un vecteur de Gross-Shimura $\gamma_D \in \mathcal{L}$ par l'application s_* (ou t_*) est le vecteur de Gross-modulaire $\Gamma_D \in \mathcal{P}_S$ correspondant au même discriminant. Construire un cycle C constitué de vecteurs de Gross-Shimura, revient à construire un chemin nul en vecteurs de Gross-modulaire. Pour trouver un cycle contenant les arêtes exceptionnelles avec une multiplicité λ première à p, nous construisons un cycle de la forme $C_0 = C + \lambda a_E$ où C est un chemin en vecteurs de Gross ne contenant pas l'arête exceptionnelle et a_E est le vecteur d'Eisenstein-Shimura. Pour cela, nous nous ramenons à construire une combinaison linéaire de vecteurs de Gross-modulaires égale au vecteur d'Eisenstein-modulaire en utilisant uniquement des vecteurs associés à des « bons » ordres.

2.2 Vecteurs de Gross

Pour toute la suite, p et q sont deux nombres premiers distincts, tous deux ≥ 5. Dans ce paragraphe, nous allons rappeler la notion de vecteurs de Gross sur le graphe dual de la fibre en q de la courbe modulaire de niveau q, et sur le graphe dual de la fibre en p d'une courbe de Shimura de discriminant pq. Nous invitons le lecteur à se référer à [3] et [21] pour une introduction aux courbes de Shimura, à [6] pour la définition des vecteurs de Gross sur les courbes modulaires de niveau premier, et à [17, §4] pour le cas des vecteurs de Gross sur les courbes de Shimura de discriminant pq.

Dans les paragraphes suivants, on considérera l'existence éventuelle de points rationnels du quotient de la courbe de Shimura X^{pq} par l'involution d'Atkin-Lehner w_q. Cette existence de points rationnels ne peut se produire que dans les deux cas décrits par Ogg dans la proposition suivante.

Proposition 2.2.1. *Si $X^{pq}/w_q(\mathbb{Q})$ est non vide, alors $\left(\frac{p}{q}\right) = -1$, et une des deux conditions suivante est satisfaite*

(1) $p \equiv 3 \mod 4$; (cas ramifié)

(2) $p \equiv 1 \mod 4$ *et* $q \equiv 3 \mod 4$ *(cas non ramifié).*

Démonstration. Consulter [24, thm 3.1]. □

Nous nous placerons pour ce travail dans le cas non ramifié.

2.2.1 Vecteurs de Gross sur le graphe modulaire

D'après le travail de Deligne et Rapoport (cf. [4, théorème 6.9 et exemple 6.16]) la fibre en q de la courbe modulaire $X_0(q)$ est constituée de deux composantes irréductibles s_1 et s_2 isomorphes à $\mathbb{P}^1(\mathbb{F}_q)$ se coupant transversalement. Il découle de cette description que le graphe dual de la fibre en q de la courbe modulaire $X_0(q)$, noté $\mathscr{G}((X_0(q))_{\mathbb{F}_q})$, est constitué de deux sommets s_1 et s_2 et d'arêtes entre s_1 et s_2. Ces arêtes correspondent à l'ensemble S des classes d'isomorphismes de courbes elliptiques supersingulières sur $\overline{\mathbb{F}}_q$. On note $E_{j_1}, \ldots, E_{j_{g+1}}$ un système de représentants de S, où les j_k parcourent le sous-ensemble de $\mathbb{F}_{q^2}$ constitué par les j-invariants supersinguliers, et g est le genre de $X_0(q)$. Soit $B_{q\infty}$ l'algèbre de quaternions sur $\mathbb{Q}$ ramifiée en q et l'infini. À la classe d'isomorphismes de la courbe elliptique E_{j_k}, on associe l'ordre maximal $\Omega_k = \mathrm{End}(E_{j_k}) \subseteq B_{q\infty}$.

Le cardinal de $(\Omega_k^*/\{\pm 1\})$ est appelé la longueur de l'arête de $\mathscr{G}((X_0(q))_{\mathbb{F}_q})$ correspondant à E_{j_k}. D'après [30, theorem 10.1 p. 103], si $j_k \neq 0, 1728$ ce cardinal est égal à 1. Il y a donc au plus deux arêtes de longueur > 1.

On désigne par $\mathcal{P}_S$ l'ensemble des chemins sur le graphe $\mathscr{G}((X_0(q))_{\mathbb{F}_q})$, c'est le $\mathbb{Z}$-module des diviseurs sur S. On définit le degré d'un chemin par : $\mathrm{degré}(\sum_{k=1}^{g+1} \lambda_{j_k} E_{j_k}) = \sum_{k=1}^{g+1} \lambda_{j_k}$. On note $\mathcal{P}_S^0$ le $\mathbb{Z}$-module des diviseurs de degré 0 sur S. La $\mathbb{Z}$-algèbre $\mathbb{T}_{\Gamma_0(q)}$ engendrée par les opérateurs de Hecke T_l, pour $l \neq q$ premier, agit sur les groupes $\mathcal{P}_S$ et $\mathcal{P}_S^0$ par l'action $T_l(E) = \sum_{C_l \subset E} E/C_l$, où $E \in S$ et C_l parcourt l'ensemble des sous-groupes d'ordre l de E.

Définition 2.2.2. L'accouplement de monodromie (Cf. [7, Exposé 9 §9]) est la forme bilinéaire non dégénérée $\langle \cdot, \cdot \rangle$ sur $\mathcal{P}_S$ définie par :

$$\langle E_{j_k}, E_{j_l} \rangle = \delta_{j_k, j_l} \,\mathrm{card}(\Omega_k^*/\{\pm 1\}),$$

où δ_{j_k,j_l} est le symbole de Kronecker. Ainsi $E_{j_1}, \ldots E_{j_{g+1}}$ est une base orthogonale pour cet accouplement. Chaque E_{j_k} est de norme 1 pour cet accouplement, sauf si $j_k = 0$ ou 1728.

Définition 2.2.3. Le vecteur d'Eisenstein (ou vecteur d'Eisenstein-modulaire) $A_E \in \frac{1}{6}\mathcal{P}_S$ est :

$$A_E = \sum_{k=1}^{g+1} \frac{1}{\mathrm{card}(\Omega_k^*/\{\pm 1\})} E_{j_k}.$$

Le vecteur d'Eisenstein A_E forme une base de $(\mathcal{P}_S^0)^\perp$, l'espace orthogonal à $\mathcal{P}_S^0$ pour cet accouplement. Il est choisi de telle sorte que, pour $v \in \mathcal{P}_S$, le degré de v est $\langle v, A_E \rangle$.

Définition 2.2.4. Soit O_D l'ordre quadratique imaginaire de discriminant D. On lui associe un vecteur $\Gamma_D \in \frac{1}{12}\mathcal{P}_S$, appelé *vecteur de Gross sur le graphe modulaire* (ou vecteur de Gross-modulaire) :

$$\Gamma_D = \frac{1}{2u(D)} \sum_{k=1}^{g+1} H_k(D) E_{j_k},$$

où $H_k(D)$ est le nombre de plongements optimaux de O_D dans Ω_k modulo conjugaison par Ω_k^* (cf. [6, §1, p 122]), et $u(D) = \mathrm{card}(O_D^*/\{\pm 1\})$. On a $u(D) = 1$, sauf pour $D = -3$ ou -4. De plus on a $u(-3) = 3$, $u(-4) = 2$.

Par la formule des traces d'Eichler, lorsque q est scindé dans O_D ou lorsque q divise le conducteur de O_D, il n'existe pas de plongement de O_D dans $B_{q\infty}$ (voir [6, §1, p 122]). Le vecteur Γ_D est non nul si q est inerte ou ramifié dans O_D et q^2 ne divise pas D. La proposition suivante donne une interprétation des vecteurs de Gross en terme de réduction modulo q des courbes elliptiques définies sur $\overline{\mathbb{Q}}$ ayant multiplication complexe par O_D. Nous nous plaçons dans le cas où q est inerte dans O_D, car nous ne manipulerons dans la suite que de tels vecteurs de Gross.

Proposition 2.2.5. *Soit O_D un ordre quadratique imaginaire de discriminant D et de nombre de classe $h(D)$, tel que q soit inerte dans O_D. Fixons $\mathcal{Q}$ une place de $\overline{\mathbb{Q}}$ au dessus de q. Le vecteur $u(D)\Gamma_D$ est constitué de la somme des réductions (non forcément distinctes) modulo $\mathcal{Q}$ des $h(D)$ courbes elliptiques sur $\overline{\mathbb{Q}}$ ayant multiplication complexe par O_D.*

Démonstration. Par la formule des traces d'Eichler (cf. [35, thm 5.11, p 92]), le nombre de plongements optimaux de O_D dans les ordres maximaux de $B_{q\infty}$ est

$$\sum_{i=1}^{g+1} H_i(D) = \left(1 - \left(\frac{D}{q}\right)\right) h(D) = 2h(D).$$

D'autre part, d'après le théorème fondamental de la multiplication complexe, il existe $h(D)$ courbes elliptiques $E_1/\overline{\mathbb{Z}}$,$E_2/\overline{\mathbb{Z}}$,...,$E_{h(D)}/\overline{\mathbb{Z}}$ à $\overline{\mathbb{Q}}$-isomorphisme près ayant multiplication complexe par O_D. Pour chacune de ces courbes elliptiques, il existe deux isomorphismes conjugués $f_1, f_2 \colon O_D \to \mathrm{End}(E)$. La place $\mathcal{Q}$ définit une inclusion de $\overline{\mathbb{Z}}$ dans une clôture algébrique de $O_D \otimes \mathbb{Z}_q$. Soit W un anneau de valuation discrète complet contenant $O_D \otimes \mathbb{Z}_q$, de corps résiduel $\overline{\mathbb{F}}_q$, et tel que $E_1, \ldots, E_{h(D)}$ sont définies sur W. On note q' l'uniformisante de W. On considère l'ensemble des couples (E, g) constitués d'une courbe elliptique E/W à multiplication complexe par O_D sur W, muni d'un isomorphisme fixé $g \colon O_D \to \mathrm{End}(E)$. On dit que les couples (E, g) et (E', g') sont équivalents s'il existe un isomorphisme $i \colon (E \mod q') \to (E' \mod q')$ tel que $(g'(\alpha) \mod q') \circ i = i \circ (g(\alpha) \mod q')$ pour tout $\alpha \in O_D$. D'après Gross [6, fin du §2 pp. 128-129], les plongements

optimaux de O_D dans les ordres maximaux de $B_{q\infty}$ correspondent aux couples (E, g), à équivalence près. Le plongement optimal associé à un tel couple (E, g) est obtenu par composition de $g\colon O_D \to \mathrm{End}(E)$ et de la réduction $\mathrm{End}(E) \to \mathrm{End}(E \mod q')$. Toute courbe elliptique E/W à multiplication complexe par O_D est une tordue d'une des courbes $E_1, \dots E_{h(D)}$. Donc tout couple $(E, g)/W$ est équivalent à un des couples $(E_l, f)/W$. Ainsi chacun des $2h(D)$ plongement optimaux de O_D dans les ordres maximaux de $B_{q\infty}$ correspond à d'un des $2h(D)$ couples $(E_l, f)/\overline{\mathbb{Z}}$. Cette correspondance est bijective par égalité des cardinaux. Pour conclure il suffit de voir que :

$$2u(D)\Gamma_D = \sum_{k=1}^{g+1} \sum_{\substack{O_D \to \Omega_k \\ \text{optimal}}} E_{j_k}.$$

Donc on a

$$2u(D)\Gamma_D = \sum_{\substack{(E,g)/W \\ \text{à équiv. près}}} (E \mod q') = 2(E_1 + \cdots + E_{h(D)}) \mod \mathcal{Q}.$$

□

Proposition 2.2.6. *Toute arête est de longueur* 1 *sauf dans les deux cas suivants :*

- *si q est inerte dans O_{-4}, alors* $1728 \mod q$ *est un j-invariant supersingulier et l'arête associée à la courbe elliptique E_{1728} de j-invariant* $1728 \mod q$ *est de longueur* 2. *Plus précisément $O_{-4} = \mathbb{Z}[\zeta_4]$ se plonge dans* $\mathrm{End}\, E_{1728}$.
- *Si q est inerte dans O_{-3}, alors* $0 \mod q$ *est un j-invariant supersingulier et l'arête associée à la courbe elliptique E_0 de j-invariant* 0 *est de longueur* 3. *Plus précisément $O_{-3} = \mathbb{Z}[\zeta_6]$ se plonge dans* $\mathrm{End}\, E_0$.

Démonstration. Découle de [29, thm 10.1 p. 103] et du fait qu'une arête de longueur 2 (respectivement de longueur 3) correspond à un ordre maximal de $B_{q\infty}$ dans lesquels se plonge O_{-4} (respectivement O_{-3}).

□

L'algèbre de Hecke $\mathbb{T}_{\Gamma_0(q)}$ agit sur l'espace $S_2(\Gamma_0(q))$ des formes modulaires paraboliques primitives f de poids 2 sur $\Gamma_0(q)$. On désigne par I_e l'idéal d'enroulement de $\mathbb{T}_{\Gamma_0(q)}$, c'est-à-dire l'ensemble des opérateurs de $\mathbb{T}_{\Gamma_0(q)}$ annulant toutes les formes modulaires de $S_2(\Gamma_0(q))$ telles que $L(f, 1) \neq 0$. Pour une forme modulaire primitive f, la formule de Gross [6, Cor. 11.6, p. 167] et de façon plus générale un théorème de Waldspurger [11, p 397], relie la valeur de $L(f, 1)$ à la norme de l'image $\Gamma_{f,D}$ du vecteur de Gross Γ_D par l'idempotent primitif $1_f \in \mathbb{T}$ associé à f. On en déduit la proposition suivante.

Proposition 2.2.7. *L'espace engendré par les projections orthogonales des vecteurs de Gross de discriminant D premier à q sur $\mathcal{P}_S \otimes \mathbb{Q}$ est $\mathcal{P}_S[I_e] \otimes \mathbb{Q}$.*

Démonstration. Consulter [16, prop 4,2]. □

On rappelle finalement que le vecteur d'Eisenstein appartient au $\mathbb{Q}$-espace engendré par les vecteurs de Gross. Cela découle de la proposition 2.2.8 ci-dessous.

Proposition 2.2.8. *Soient D le discriminant de l'ordre maximal O_D d'un corps quadratique imaginaire, tel que q soit inerte ou ramifié dans O_D et $l \neq q$ un nombre premier. On a :*

$$\lim_{n\to\infty} \frac{\langle A_E, A_E\rangle}{\langle A_E, \Gamma_{l^{2n}D}\rangle}\Gamma_{l^{2n}D} = A_E.$$

Il en découle que A_E appartient au $\mathbb{Q}$-espace vectoriel engendré par les $\Gamma_{l^{2n}D}$, pour $n \geq 1$.

Démonstration. Consulter [16, thm 4.3]. □

On peut remarquer de la même façon que le vecteur d'Eisenstein-Shimura sur le graphe dual de la fibre en p de la courbe de Shimura X^{pq} (cf. Définition 2.2.9) s'exprime lui aussi comme combinaison linéaire de vecteurs de Gross.

2.2.2 Vecteurs de Gross sur le graphe de Shimura

Soit X^{pq} la courbe de Shimura de discriminant pq. Ribet donne la description de $\mathscr{G}(X^{pq}_{\mathbb{F}_p})$, le graphe dual de la fibre en p de cette courbe de Shimura, dans [21, Propositions 4.4 et 4.7]. L'ensemble de ses sommets est constitué de deux copies $S_1 \sqcup S_2$ de l'ensemble S des classes d'isomorphismes de courbes elliptiques supersingulières $\overline{\mathbb{F}}_q$. L'ensemble de ses arêtes est l'ensemble $\{e_1, \ldots, e_n\}$ des classes d'isomorphismes de $p-$isogénies entre ces courbes elliptiques. Chacune de ces isogénies $e_i \colon E_{j_1} \to E_{j_2}$ s'interprète comme une arête reliant le sommet de S_1 correspondant à E_{j_1} au sommet de S_2 correspondant à E_{j_2}. De manière équivalente l'ensemble des arêtes du graphe s'identifie avec l'ensemble des couples (E, C_p), où E est une courbe elliptique supersingulière à isomorphisme près sur $\overline{\mathbb{F}}_q$, et C_p est un sous-groupe d'ordre p de E défini à action de $\mathrm{End}(E)^*$ près. On munit ce graphe d'une orientation en considérant que toutes les arêtes sont orientées d'un sommet de S_1 vers un sommet de S_2. À chaque arête $e = (E, C_p)$ on associe l'ordre d'Eichler $\mathrm{End}(e) = \{\alpha \in \mathrm{End}(E) \ : \ \alpha(C_p) \subseteq C_p\}$ de niveau p dans $B_{q\infty}$. On définit la longueur d'une arête $e = (E, C_p)$ comme le cardinal de $\mathrm{End}(e)^*/\{\pm 1\}$. Comme pour le graphe modulaire, les arêtes ont toutes une longueur 1, sauf peut-être les quatre arêtes décrites dans le corollaire 2.2.15 ci-après.

Les involutions d'Atkin Lehner w_p et w_q agissent sur le graphe de la manière suivante : l'involution w_p échange chaque sommet de S_1 (respectivement S_2) avec le sommet de S_2 (respectivement S_1) correspondant à la même courbe elliptique à isomorphisme près, et échange l'arête correspondant à une isogénie (E, C_p) avec l'opposé de l'arête correspondant à son isogénie duale $(E/C_p, E[p]/C_p)$. L'involution w_q agit comme le Frobenius sur le graphe, c'est-à-dire qu'elle échange chaque sommet de S_1 (respectivement S_2) avec le sommet de S_1 (respectivement S_2) correspondant à l'image par le Frobenius en q de la

courbe elliptique correspondante, et échange l'arête correspondant à l'isogénie (E, C_p) avec l'arête correspondant à l'image de cette isogénie par le Frobenius.

Comme dans le paragraphe précédent, on considère $\mathcal{L}$ le $\mathbb{Z}$-module des diviseurs sur les arêtes du graphe $\mathscr{G}(X^{pq}_{\mathbb{F}_p})$. On appelle les éléments de $\mathcal{L}$ les chemins sur le graphe. Notons $\mathcal{L}^0$ le $\mathbb{Z}$-module des diviseurs de degré 0. La $\mathbb{Z}$-algèbre $\mathbb{T}_{\Gamma_0(pq)}$ engendrée par les opérateurs de Hecke T_l, pour $l \neq p, q$ premier, agit sur ces groupes par l'action :

$$T_l((E, C_p)) = \sum_{C_l \subset E} (E/C_l, (C_p + C_l)/C_l),$$

où C_l parcourt les sous-groupes d'ordre l de E.

On définit l'accouplement de monodromie sur $\mathcal{L}$ par :

$$\langle e_i, e_j \rangle = \delta_{i,j} \operatorname{card}(\operatorname{End}(e_i)^*/\{\pm 1\}).$$

On remarque que les $(e_i)_{i=1\ldots n}$ forment une base orthogonale de $\mathcal{L}$ pour cet accouplement, et que presque tous les e_i sont de norme 1.

Définition 2.2.9. Le vecteur d'Eisenstein (ou vecteur d'Eisenstein-Shimura) est défini par :

$$a_E = \sum_{i=1}^{n} \frac{1}{\operatorname{card}(\operatorname{End}(e_i)^*/\{\pm 1\})} e_i.$$

Il forme une base de $(\mathcal{L}^0)^\perp$, l'espace orthogonal à $\mathcal{L}^0$ pour l'accouplement de monodromie.

On remarque que le module $\mathcal{L}$ s'identifie naturellement avec le groupe des diviseurs des points supersinguliers de $X_0(pq)(\mathbb{F}_{q^2})$. Le vecteur d'Eisenstein sur $\mathscr{G}(X^{pq}_{\mathbb{F}_p})$ correspond donc à un vecteur d'Eisenstein pour la courbe modulaire de niveau non premier $X_0(pq)_{\mathbb{F}_q}$. De la même façon, les vecteurs de Gross sur $\mathscr{G}(X^{pq}_{\mathbb{F}_p})$ qui seront introduits dans la définition 2.2.11 ci-dessous, correspondent à des vecteurs de Gross pour la courbe modulaire $X_0(pq)_{\mathbb{F}_q}$.

Définition 2.2.10. On note par s l'application qui a une arête $e = (E_{j_k}, C_p)$ de $\mathscr{G}(X^{pq}_{\mathbb{F}_p})$ associe la courbe $E_{j_k} \in S$. On a :

$$s_* \colon \mathcal{L} \to \mathcal{P}_S$$
$$\sum_{i=1}^{n} \lambda_i e_i \mapsto \sum_{i=1}^{n} \lambda_i s(e_i).$$

De manière similaire on définit l'application t qui a l'arête $e = (E_{j_k}, C_p)$ associe la courbe $E_{j_k}/C_p \in S$. On a :

$$t_* \colon \mathcal{L} \to \mathcal{P}_S$$
$$\sum_{i=1}^{n} \lambda_i e_i \mapsto \sum_{i=1}^{n} \lambda_i t(e_i).$$

Soit Y l'intersection des noyaux de s_* et t_*. C'est un sous $\mathbb{Z}$-module de $\mathcal{L}^0$. D'après [21, corollary 4.5], Y est isomorphe à $H_1(\mathscr{G}(X^{pq}_{\mathbb{F}_p}), \mathbb{Z})$. On appelle les éléments de Y les cycles ou chemins fermés de $\mathscr{G}(X^{pq}_{\mathbb{F}_p})$.

Définition 2.2.11. Soit O_D un ordre quadratique imaginaire de discriminant D. On définit le *vecteur de Gross sur le graphe dual de la fibre en p de la courbe de Shimura*, (ou vecteur de Gross-Shimura), $\gamma_D \in \frac{1}{12}\mathcal{L}$, par :

$$\gamma_D = \sum_{i=1}^{n} \frac{h_i(D)}{\mathrm{card}(\mathrm{End}(e_i)^*/\{\pm 1\})} e_i,$$

où $h_i(D)$ est le nombre de plongements optimaux de O_D dans l'ordre d'Eichler $R_i = \mathrm{End}(e_i)$.

Lorsque q est scindé (ou p est inerte) dans l'ordre O_D, d'après la formule des traces d'Eichler, il n'existe aucun plongement de O_D dans les ordres d'Eichler de niveau p de $B_{q\infty}$, et le vecteur γ_D est nul (cf. [35, thm 5.11, p 92]). Lorsque q est inerte (ou ramifié et ne divisant pas le conducteur de O_D) et p scindé (ou ramifié et ne divisant pas le conducteur de O_D) dans O_D, le vecteur γ_D est non nul. De manière similaire à la proposition 2.2.5, la proposition suivante donne une description des arêtes du vecteur γ_D en terme de réduction modulo q des isogénies entre courbes elliptiques sur $\overline{\mathbb{Q}}$ à multiplication complexe par O_D. Nous nous restreignons au cas où q est inerte et p scindé dans O_D, car nous ne manipulerons dans la suite que des vecteurs satisfaisant ces hypothèses.

Proposition 2.2.12. *Soit O_D un ordre quadratique imaginaire de discriminant D et de nombre de classe $h(D)$, tel que q soit inerte et p scindé dans O_D. Fixons $\mathcal{Q}$ une place de $\overline{\mathbb{Q}}$ au dessus de q. Le vecteur γ_D est constitué de $2h(D)$ arêtes, chacune de ces arêtes e pondérée par $2/(\mathrm{card}(\mathrm{End}(e)^*/\{\pm 1\}))$. Ces arêtes correspondent aux réductions modulo $\mathcal{Q}$ des $2h(D)$ p-isogénies entre les $h(D)$ courbes elliptiques sur $\overline{\mathbb{Q}}$ ayant multiplication complexe par O_D.*

Démonstration. Par la formule des traces d'Eichler, le nombre de plongements optimaux de O_D dans les ordres d'Eichler de niveau p de $B_{q\infty}$ est

$$\sum_{i=1}^{n} h_i(D) = \left(1 - \left(\frac{D}{q}\right)\right)\left(1 + \left(\frac{D}{p}\right)\right) h(D) = 4h(D).$$

Les ordres d'Eichler $R_1, \ldots, R_n$ de niveau p correspondent aux $\mathrm{End}(E_{j_i}, C_p)$, où $i = 1, \ldots, g+1$ et C_p parcourt les sous-groupes d'ordre p de E_{j_i} à isomorphisme près.

Soit $\Phi\colon O_D \to \mathrm{End}(E_{j_i}, C_p)$ un plongement optimal. Le plongement induit $\Phi'\colon O_D \to \mathrm{End}(E_{j_i})$ est également optimal. D'après la proposition 2.2.5, ce plongement Φ' provient d'un couple (E, g), où $E/\overline{\mathbb{Q}}$ est une courbe elliptique à multiplication complexe par O_D munie d'un isomorphisme $g\colon O_D \to \mathrm{End}(E)$, de telle sorte que $(E \mod \mathcal{Q}) = E_{j_i}$. Comme

la réduction modulo $\mathcal{Q}$ réalise un isomorphisme $E[p] \to E_{j_i}[p]$, il existe un sous-groupe C d'ordre p de E tel que $(C \mod \mathcal{Q}) = C_p$. Pour des raisons de compatibilité, on a $g(O_D)$ inclus dans $\mathrm{End}(E, C)$, c'est-à-dire $\mathrm{End}(E) = \mathrm{End}(E, C) \simeq O_D$. L'isogénie $E \to E/C$ de noyau C est une p-isogénie entre E et une courbe elliptique E/C à multiplication complexe par O_D. Par la théorie de la multiplication complexe, une telle isogénie correspond à un idéal P de O_D au dessus de p. Comme p est scindé dans O_D, il existe deux isogénies distinctes de E dans des courbes elliptiques à multiplication complexe par O_D, et C est le noyau d'une de ces deux isogénies. Finalement un plongement optimal Φ de O_D dans un ordre d'Eichler $R = \mathrm{End}(E_{j_i}, C_p)$ correspond à un des $4h(D)$ couples $((E, C), g)$ constitués d'une p-isogénie à isomorphisme près (E, C) entre courbes elliptiques sur $\overline{\mathbb{Q}}$ ayant multiplication complexe par O_D, et d'un isomorphisme $g \colon O_D \to \mathrm{End}(E, C)$. Ici Φ est la composée de g et de la réduction modulo $\mathcal{Q}$ de $\mathrm{End}(E, C) \to \mathrm{End}(E_{j_i}, C_p)$. Cette correspondance est bijective par égalité des cardinaux.

□

La proposition suivante décrit l'action des involutions d'Atkin-Lehner sur les vecteurs de Gross.

Proposition 2.2.13. *Avec les hypothèses de la proposition 2.2.12, on a $w_p(\gamma_D) = -\gamma_D$, et $w_q(\gamma_D) = \gamma_D$.*

Démonstration. Prouvons d'abord que $w_p(\gamma_D) = -\gamma_D$. Soit τ une permutation de l'ensemble $\{1, \ldots, n\}$ telle que, pour chaque arête e_i, l'arête $e_{\tau(i)}$ est son isogénie duale. L'involution w_p agit sur les arêtes du graphe en envoyant e_i sur $-e_{\tau(i)}$. Ainsi on a

$$w_p(\gamma_D) = \sum_{i=1}^{n} \frac{h_i(D)}{\mathrm{card}(\mathrm{End}(e_i)^*/\{\pm 1\})}(-e_{\tau(i)}),$$

or $\mathrm{End}(e_i) \simeq \mathrm{End}(e_{\tau(i)})$ donc $w_p(\gamma_D) = -\gamma_D$.

Rappelons que w_q agit comme le Frobenius sur les sommets et les arêtes du graphe. Soit $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ tel que σ se réduit en le Frobenius de $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$. Considérons $\mathcal{I}_{\overline{\mathbb{Q}}}$ l'ensemble des p-isogénies à isomorphismes près entre courbes elliptiques sur $\overline{\mathbb{Q}}$ à multiplication complexe par O_D. D'après la proposition 2.2.12,

$$\gamma_D = \sum_{g \in \mathcal{I}_{\overline{\mathbb{Q}}}} \frac{1}{\mathrm{card}(\mathrm{End}(g \mod q)^*/\{\pm 1\})}(g \mod q),$$

donc

$$w_q(\gamma_D) = \sum_{g \in \mathcal{I}_{\overline{\mathbb{Q}}}} \frac{1}{\mathrm{card}(\mathrm{End}(g \mod q)^*/\{\pm 1\})}(\sigma(g) \mod q).$$

Or σ réalise une bijection de $\mathcal{I}_{\overline{\mathbb{Q}}}$ dans $\mathcal{I}_{\overline{\mathbb{Q}}}$ telle que pour tout $g \in \mathcal{I}_{\overline{\mathbb{Q}}}$, on a $\mathrm{End}(\sigma(g) \mod q) \simeq \mathrm{End}(g \mod q)$ donc $w_q(\gamma_D) = \gamma_D$. □

La proposition 2.2.12 nous permet de décrire l'image de γ_D par les applications s_* et t_*, en comparant le vecteur γ_D sur $\mathscr{G}(X^{pq}_{\mathbb{F}_p})$ au vecteur Γ_D sur $\mathscr{G}((X_0(q))_{\mathbb{F}_q})$.

Corollaire 2.2.14. *Avec les hypothèses de la proposition 2.2.12, les arêtes du vecteur de Gross γ_D sur le graphe $\mathscr{G}(X^{pq}_{\mathbb{F}_p})$ sont distribuées de la façon suivante : de chaque sommet E_{j_k} dans S_1 partent $H_k(D)$ arêtes de γ_D. Chacune de ces arêtes est précédée du coefficient $2/l$, où l est la longueur de l'arête. En particulier, si le vecteur γ_D ne contient pas d'arêtes de longueur 2 ou 3, on a :*

$$s_*(\gamma_D) = t_*(\gamma_D) = 4\Gamma_D.$$

Démonstration. Dans la démonstration de la proposition 2.2.12, nous avons montré que les $H_k(D)$ plongements optimaux de O_D dans l'ordre maximal $\mathrm{End}(E_{j_k})$ définissent $2H_k(D)$ plongements optimaux de O_D dans des ordres d'Eichler de la forme $\mathrm{End}(E_{j_k}, C_p)$ qui correspondent à des arêtes de $\mathscr{G}(X^{pq}_{\mathbb{F}_p})$ partant du sommet $E_{j_k} \in S_1$. Cela se traduit par la formule suivante :

$$\sum_{\substack{i=1\ldots n \\ e_i=(E_{j_k},C_p)}} h_i(D) = 2H_k(D).$$

Si le vecteur γ_D ne contient pas d'arêtes de longueur 2 ou 3, on a :

$$\gamma_D = \sum_{i=1}^{n} h_i(D) e_i.$$

On en déduit que

$$s_*(\gamma_D) = \sum_{k=1}^{g+1} 2H_k(D) E_{j_k} = 4\Gamma_D.$$

D'autre part pour chaque arête $e = (E_{j_k}, C_p)$, on a

$$s_*(-w_p(e)) = s_*((E_{j_k}/C_p, E_{j_k}[p]/C_p)) = E_{j_k}/C_p = t_*(e).$$

Ce qui implique que $t_*(\gamma_D) = s_*(-w_p(\gamma_D))$. Or d'après la proposition 2.2.13, on a $\gamma_D = -w_p(\gamma_D)$. En conséquence $t_*(\gamma_D) = s_*(\gamma_D)$, ce qui achève la preuve de la proposition. □

En appliquant la proposition 2.2.12, on décrit les arêtes de longueur $\neq 1$.

Corollaire 2.2.15. *Toutes les arêtes du graphe $\mathscr{G}(X^{pq}_{\mathbb{F}_p})$ sont de longueur 1 sauf dans les cas suivants :*

- *Si q est inerte et p scindé dans O_{-4}, il existe exactement deux arêtes de longueur 2. Ces deux arêtes relient le sommet $E_{1728} \in S_1$ au sommet $E_{1728} \in S_2$ et sont échangées par w_q.*

– *Si q est inerte et p scindé dans O_{-3}, il existe exactement deux arêtes de longueur 3. Ces deux arêtes relient le sommet $E_0 \in S_1$ au sommet $E_0 \in S_2$ et sont échangées par w_q.*

En particulier si on se place dans le cas non ramifié de Ogg (voir proposition 2.2.1), il existe deux arêtes exceptionnelles de longueur 2 sur $\mathscr{G}(X^{pq}_{\mathbb{F}_p})$. Donc une seule arête exceptionnelle de longueur 2 sur $\mathcal{G}((X^{pq}/w_q)_{\mathbb{F}_p})$.

Démonstration. Comme dans la proposition 2.2.6, on voit que les arêtes de longueur 2 sont les arêtes de γ_{-4} et les arêtes de longueur 3 sont les arêtes de γ_{-3}.

D'après la formule des traces d'Eichler, si q est scindé ou p est inerte dans O_{-4}, le vecteur γ_{-4} est nul. Supposons que q est inerte et p scindé dans O_{-4}. Soit $E/\overline{\mathbb{Q}}$ l'unique courbe elliptique ayant multiplication par O_{-4}. On sait que le j-invariant de E est 1728. D'après la proposition 2.2.12, les arêtes de γ_{-4} correspondent aux réductions modulo q des 2 p-isogénies entre courbes elliptiques à multiplication complexe par O_{-4}. Soit $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ qui se réduit en le Frobenius modulo q. Le morphisme σ agit comme la conjugaison complexe sur O_{-4}, car q est inerte dans O_{-4}. Comme p est scindé dans O_{-4}, l'idéal pO_{-4} se décompose en le produit de deux idéaux P et $\sigma(P)$ dans O_D. Par la théorie de la multiplication complexe, ces idéaux correspondent à deux p-isogénies conjuguées par σ, notées $[P]$ et $[\sigma(P)]$, de $E \to E$. Ces deux p-isogénies se réduisent en deux arêtes du graphe $\mathscr{G}(X^{pq}_{\mathbb{F}_p})$ reliant le sommet $E_{1728} \in S_1$ au sommet $E_{1728} \in S_2$. Ces deux arêtes sont échangées par w_q qui agit comme le Frobenius sur le graphe, ce qui nous donne la forme annoncée de l'ensemble des arêtes de γ_{-4}.

On traite le cas des arêtes de longueur 3 de manière similaire.

□

Proposition 2.2.16. *Soient O_{D_1} et O_{D_2} deux ordres quadratiques imaginaires de discriminant respectifs D_1 et D_2 premiers à q. Supposons aussi que q soit inerte dans O_{D_1} et O_{D_2}. Il existe une borne B dépendant de q telle que, pour $p \geq B$, si p est scindé dans ces deux ordres, les vecteurs de Gross γ_{D_1} et γ_{D_2} sur le graphe dual de la fibre en p de la courbe de Shimura X^{pq} sont sans arêtes communes.*

Démonstration. Soient α_1 et α_2 tels que $O_{D_i} = \mathbb{Z}[\alpha_i]$, pour $i = 1, 2$. Soient $\phi_i \colon O_{D_i} \to \Omega$ des plongements optimaux des ordres O_{D_i} dans un même ordre maximal $\Omega = \mathrm{End}(E)$, où $E/\mathbb{F}_q$ est une courbe elliptique supersingulière.

Remarquons d'abord que $\phi_1(\alpha_1)$ et $\phi_2(\alpha_2)$ ne commutent pas. En effet, s'ils commutent, $\mathbb{Q}[\phi_1(\alpha_1), \phi_2(\alpha_2)]$ est un sous-corps commutatif de $B_{q\infty}$ strictement plus grand que $\mathbb{Q}$. Donc il est de degré 2 sur $\mathbb{Q}$ et est isomorphe à $\mathbb{Q}[\phi_1(\alpha_1)]$ et à $\mathbb{Q}[\phi_2(\alpha_2)]$, ce qui n'est possible que si ces deux derniers corps sont égaux. Comme les plongements ϕ_i sont optimaux, $\mathbb{Q}[\phi_i(\alpha_i)] \cap \Omega = \mathbb{Z}[\phi_i(\alpha_i)] = \phi_i(O_{D_i})$, ce qui est impossible car, par hypothèse, $O_{D_1} \neq O_{D_2}$.

Comme dans le corollaire 2.2.14, chacun de ces plongements ϕ_i définit deux plongements optimaux $O_{D_i} \to \mathrm{End}(E, C^i_{p,j})$ dans des ordres d'Eichler de niveau p, où $i = 1, 2$,

$j = 1, 2$ et $C^i_{p,j}$ est un sous-groupe d'ordre p de E. Plus précisément $C^i_{p,1}$ et $C^i_{p,2}$ sont les deux sous-espaces propres du morphisme restreint $\phi_i(\alpha_i)|_{E[p]}$. Pour prouver que pour p assez grand il n'y a pas de plongement optimal de O_{D_1} et O_{D_2} dans un même ordre d'Eichler de niveau p, il suffit de prouver que pour p assez grand $\phi_1(\alpha_1)|_{E[p]}$ et $\phi_2(\alpha_2)|_{E[p]}$ n'ont pas d'espace propre commun. On identifie ces restrictions avec $(\phi_1(\alpha_1) \mod p)$ et $(\phi_2(\alpha_2) \mod p)$ qui sont des éléments de $\Omega \otimes \mathbb{F}_p \simeq M_2(\mathbb{F}_p)$. Comme $\phi_1(\alpha_1)$ et $\phi_2(\alpha_2)$ ne commutent pas dans $B_{q\infty}$, on a $\mathbb{Q}[\phi_1(\alpha_1), \phi_2(\alpha_2)] = B_{q\infty}$. Donc il existe une constante $M \in \mathbb{Z}$ ne dépendant que de $\phi_1(\alpha_1), \phi_2(\alpha_2)$, telle que $\Omega \subseteq \frac{1}{M}\mathbb{Z}[\phi_1(\alpha_1), \phi_2(\alpha_2)]$. Pour p ne divisant pas M, on a $\mathbb{Z}[\phi_1(\alpha_1), \phi_2(\alpha_2)] \otimes \mathbb{F}_p = M_2(\mathbb{F}_p)$. Dans ce cas $(\phi_1(\alpha_1) \mod p)$ et $(\phi_2(\alpha_2) \mod p)$ n'ont pas d'espace propre commun, sinon ils engendreraient un sous-groupe de Borel de $M_2(\mathbb{F}_p)$.

Lorsque ϕ_1 et ϕ_2 parcourent les ensembles finis des plongements optimaux de O_{D_1} et O_{D_2} dans les ordres maximaux, M prend un nombre fini de valeurs. Donc pour p supérieur à toutes ces valeurs, les vecteurs γ_{D_1} et γ_{D_2} sont sans arête commune.

□

2.3 Groupe des composantes de $\mathrm{Jac}(X^{pq}/w_q)_{\mathbb{F}_p}$

On considère le modèle régulier $\widetilde{X^{pq}/w_q}$ sur $\mathbb{Z}_p$ du quotient d'Atkin-Lehner X^{pq}/w_q, obtenu par éclatement aux points singuliers du modèle décrit par Cherednik et Drinfeld. Parent et Yafaev ont prouvé le présent lemme sur le groupe des composantes de la fibre en p de la jacobienne du quotient d'Atkin-Lehner X^{pq}/w_q.

Lemme 2.3.1. *Soient p, q deux nombres premiers tels que $g(X_0(q)) \geq 5$, $q \equiv 3 \mod 4$, $p \equiv 5 \mod 12$ et $\left(\frac{q}{p}\right) = -1$. Soient $\mathcal{J}$ la composante irréductible exceptionnelle de $\widetilde{X^{pq}/w_q}$ provenant de la multiplication par ζ_4 et $J \neq \mathcal{J}$ une autre composante irréductible de $\widetilde{X^{pq}/w_q}$. Pour $p \gg q$, on a $(p+1)(\mathcal{J} - J) \neq 0$ dans le groupe des composantes de $\mathrm{Jac}(X^{pq}/w_q)_{\mathbb{F}_p}$.*

Démonstration. Cela découle du lemme [17, lemma 3.2.3]. □

Le but de ce paragraphe est de généraliser le lemme 2.3.1 en supprimant la condition $p \equiv -1 \mod 3$. Nous allons prouver le lemme ci-dessous :

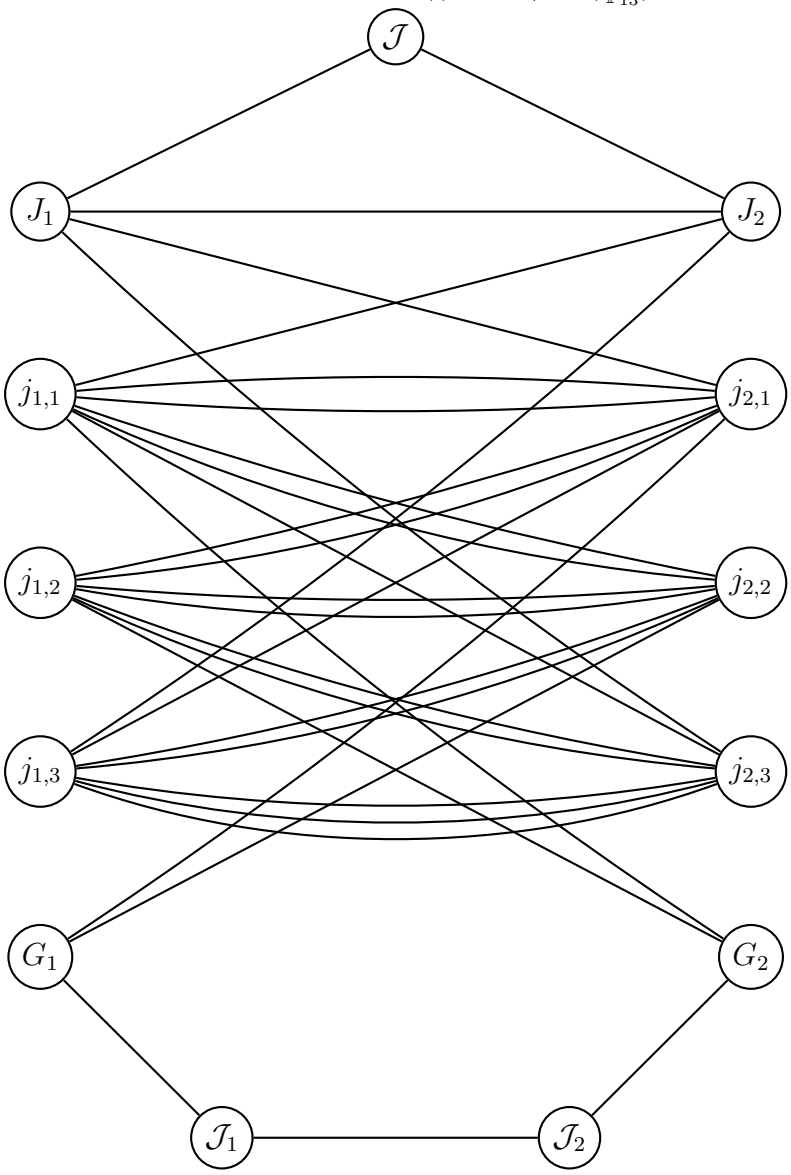
Lemme 2.3.2. *Soient p, q deux nombres premiers tels que $g(X_0(q)) \geq 6$, $q \equiv 3 \mod 4$, $p \equiv 1 \mod 4$ et $\left(\frac{q}{p}\right) = -1$. Soient $\mathcal{J}$ la composante irréductible exceptionnelle de $\widetilde{X^{pq}/w_q}$ provenant de la multiplication par ζ_4 et $J \neq \mathcal{J}$ une autre composante irréductible de $\widetilde{X^{pq}/w_q}$. Pour $p \gg q$, on a $(p+1)(\mathcal{J} - J) \neq 0$ dans le groupe des composantes de $\mathrm{Jac}(X^{pq}/w_q)_{\mathbb{F}_p}$.*

Remarque 2.3.3. D'après [28, Prop. 1.43], le genre de $X_0(q)$ est la partie entière $\lfloor \frac{q+1}{12} \rfloor$ de $\frac{q+1}{12}$ si $q \not\equiv 1 \mod 12$ et $\lfloor \frac{q+1}{12} \rfloor - 1$ si $q \equiv 1 \mod 12$. On en déduit que si $q \geq 79$ alors $g(X_0(q)) \geq 6$. D'autre part d'après la définition 2.2.3, le poids du vecteur d'Eisenstein modulaire est $w(A_E) = \sum_{k=1}^{g+1} (\mathrm{card}(\mathrm{End}(E_{j_k})^*/\{\pm 1\}))^{-1}$, où $g = g(X_0(q))$. Comme, d'après le corollaire 2.2.6, $\mathrm{card}(\mathrm{End}(E_{j_k})^*/\{\pm 1\}) = 1$ sauf au plus pour deux valeurs de j_k, on a $w(A_E) > g(X_0(q)) - 1 \geq 5$.

Notations 2.3.4. Pour faciliter la compréhension des notations qui suivent, nous invitons le lecteur à consulter l'exemple 2.3.5 ci-dessous. On note $\mathcal{G}((\widetilde{X^{pq}/w_q})_{\mathbb{F}_p})$ le graphe dual de la fibre en p de $\widetilde{X^{pq}/w_q}$. Rappelons que ce graphe est le graphe obtenu à partir du graphe $\mathcal{G}((X^{pq}/w_q)_{\mathbb{F}_p})$ en remplaçant chaque arête exceptionnelle de longueur l par une chaîne de l arêtes de longueur 1. On renvoie au corollaire 2.2.15 pour une description de ces arêtes. On désigne par $S_1' = S_1/w_q$ et $S_2' = S_2/w_q$ les deux partitions du graphe $\mathcal{G}((X^{pq}/w_q)_{\mathbb{F}_p})$. L'ensemble des sommets de $\mathcal{G}((\widetilde{X^{pq}/w_q})_{\mathbb{F}_p})$ est l'union disjointe de S_1', S_2' et de l'ensemble des sommets exceptionnels que nous allons décrire. On note $\mathcal{J}$ le sommet exceptionnel de $\mathcal{G}((\widetilde{X^{pq}/w_q})_{\mathbb{F}_p})$ provenant de l'éclatement de $(X^{pq}/w_q)/\mathbb{Z}_p$ en l'unique point singulier d'épaisseur 2. Le sommet $\mathcal{J}$ est relié par une arête à chacun des deux sommets $J_1 \in S_1'$ et $J_2 \in S_2'$ correspondant au j-invariant $1728 \mod q$. Lorsque $q \equiv -1 \mod 3$ et $p \equiv 1 \mod 3$, on note $G_1 \in S_1'$ et $G_2 \in S_2'$ les deux sommets correspondant à la classe du j-invariant $0 \mod q$. Les sommets G_1 et G_2 sont reliés à deux sommets exceptionnels $\mathcal{J}_1$ et $\mathcal{J}_2$ provenant de l'unique point singulier d'épaisseur 3 après éclatements successifs. On note par $j_{1,1}, j_{1,2}, \ldots, j_{1,l}$ les sommets de S_1' distincts de J_1 et G_1. De même $j_{2,1}, j_{2,2}, \ldots, j_{2,l}$ désignent les sommets de S_2' distincts de J_2 et G_2.

Soient a et b deux sommets du graphe. On note $N(a,b)$ le nombre d'arêtes entre les deux sommets a et b, et $N(a)$ la puissance du sommet a (*i. e.* le nombre d'arêtes qui partent du sommet a ou arrivent au sommet a).

Exemple 2.3.5. Graphe de $\mathcal{G}((X^{\widetilde{13*47}}/w_{47})_{\mathbb{F}_{13}})$.



Nous invitons le lecteur à se référer au présent exemple pour faciliter la compréhension des calculs qui suivent. (On note cependant que ce graphe ne satisfait pas à la condition du corollaire 2.3.9 ci-dessous. En effet dans cet exemple certains des sommets de S'_1 ne sont pas reliés à tous les sommets de S'_2).

La preuve du lemme 2.3.1 repose sur la description du groupe des composantes donnée par Raynaud [1, thm 1, p 274].

Lemme 2.3.6. *(« Loi K »). Avec les notations du lemme 2.3.2, on a $(p+1)(\mathcal{J}-J)=0$ dans le groupe des composantes de $\mathrm{Jac}(X^{pq}/w_q)_{\mathbb{F}_p}$, si et seulement s'il existe une fonction ν de l'ensemble des sommets S de $\mathcal{G}(\widetilde{(X^{pq}/w_q)}_{\mathbb{F}_p})$ dans $\mathbb{Z}$ telle que pour chaque sommet C de $\mathcal{G}(\widetilde{(X^{pq}/w_q)}_{\mathbb{F}_p})$, on a l'égalité :*

$$\sum_{D\mapsto C}\nu(C)-\nu(D)=\begin{cases}p+1 \text{ si } C=\mathcal{J};\\ -(p+1) \text{ si } C=J;\\ 0 \text{ sinon.}\end{cases}$$

Où $\sum_{D\mapsto C}$ désigne la somme faite sur tous les sommets D voisins du sommet C avec une multiplicité égale au nombre d'arêtes entre D et C. C'est-à-dire :

$$\sum_{D\in S}N(C,D)(\nu(C)-\nu(D))=\begin{cases}p+1 \text{ si } C=\mathcal{J};\\ -(p+1) \text{ si } C=J;\\ 0 \text{ sinon.}\end{cases}$$

Démonstration. Consulter [17, Sublemma 3.1.3.1]. □

Le lemme 2.3.6 peut se traduire de manière électrodynamique, on pourra consulter à ce sujet [17, §3.1] ou [5, II.1]. Identifions le graphe $\mathcal{G}(\widetilde{(X^{pq}/w_q)}_{\mathbb{F}_p})$ à un circuit électrique de la manière suivante : les sommets du graphe sont les nœuds du circuit et les arêtes du graphe sont des fils reliant ces nœuds. Chacun de ces fils étant d'une résistance de 1 Ohm. Supposons que les nœuds $\mathcal{J}$ et J soient reliées aux pôles d'un générateur électrique, et qu'un courant de $p+1$ Ampères entre dans le circuit en le nœud J et quitte le circuit au nœud $\mathcal{J}$. Soit ν une répartition des potentiels, exprimée en Volts, sur l'ensemble des nœuds du circuit, définie à une répartition constante près. La différence de potentiel entre deux nœuds reliés par un fil A et B est $u(A,B)=\nu(A)-\nu(B)$. Chaque fil entre A et B est parcouru par un courant (éventuellement d'intensité nulle) dirigé de A vers B si $u(A,B)\geq 0$ et de B vers A si $u(A,B)\leq 0$. La loi d'Ohm affirme que si le fil c, de résistance $r(c)$ est parcouru par un courant dirigé de A vers B, dont l'intensité est $i(c)$ Ampères, alors la différence de potentiel $u(A,B)$ est égale à $r(c)i(c)$ Volts. Dans le cas qui nous intéresse $i(c)=u(A,B)=\nu(A)-\nu(B)$ comme $r(c)=1$. La loi des nœuds de Kirchhoff affirme que pour chaque nœud A, la somme des intensité des courants arrivant au nœud A est égale à la somme des intensités des courants partant du sommet A. En combinant la loi de Kirchhoff en un nœud C avec la loi d'Ohm sur tous les fils partant de C, on retrouve les équations du lemme 2.3.6. Or d'après [1, thm 1, p 274] la solution ν de ce système est unique à une fonction constante près. Donc prouver que $(p+1)(\mathcal{J}-J)\neq 0$

revient à prouver que le circuit électrique décrit ne peut pas admettre de répartition de potentiel ν à valeurs entières.

Les lemmes suivants décrivent la répartition des arêtes de $\mathcal{G}(\widetilde{(X^{pq}/w_q)_{\mathbb{F}_p}})$.

Lemme 2.3.7. *Avec les hypothèses du lemme 2.3.2, fixons $j \in \mathbb{F}_{q^2}$ un j-invariant supersingulier défini à action de $\mathrm{Gal}(\mathbb{F}_{q^2}/\mathbb{F}_q)$ près, et soit C le sommet de S_1' ou S_2' associé à ce j-invariant. Le nombre $N(C)$ d'arêtes qui partent de C dans le graphe $\mathcal{G}(\widetilde{(X^{pq}/w_q)_{\mathbb{F}_p}})$ est donné par :*

$(p+1)$ *si j appartient à $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$;*
$(p+1)/2$ *si j appartient à $\mathbb{F}_q$ et $j \not\equiv 0,\ 1728$;*
$(p+3)/4$ *si $j \equiv 1728$;*
$(p+1)/6$ *si $j \equiv 0$ et $p \equiv -1 \mod 3$;*
$(p+5)/6$ *si $j \equiv 0$ et $p \equiv 1 \mod 3$.*

Démonstration. Le nombre d'arêtes partant de chaque sommet non exceptionnel du graphe $\mathcal{G}(\widetilde{(X^{pq}/w_q)_{\mathbb{F}_p}})$ est égal au nombre d'arêtes partant du sommet correspondant dans le graphe $\mathcal{G}((X^{pq}/w_q)_{\mathbb{F}_p})$. Le lemme [17, lemma 3.1.2] et sa preuve donnent le résultat. □

Lemme 2.3.8. *Soient $j_1, j_2 \in \mathbb{F}_{q^2}$ deux j-invariants supersinguliers définis à action de $\mathrm{Gal}(\mathbb{F}_{q^2}/\mathbb{F}_q)$ près. On note $C_1 \in S_1'$ et $C_2 \in S_2'$ les sommets associés à ces j-invariants. On note $\epsilon(C_1, C_2) = 2$ si $j_1 \in \mathbb{F}_q$ et $j_2 \in \mathbb{F}_q$ et $\epsilon(C_1, C_2) = 1$ si $j_1 \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ ou $j_2 \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. Le nombre d'arêtes $N(C_1, C_2)$ entre les sommets C_1 et C_2 dans le graphe $\mathcal{G}(\widetilde{(X^{pq}/w_q)_{\mathbb{F}_p}})$ est :*

$$\frac{p+1}{w(A_E)} \times \frac{1}{\epsilon(C_1, C_2) w(C_1) w(C_2)} + O_q(\sqrt{p}).$$

Où $w(A_E) = \sum_{k=1}^{g+1} (\mathrm{card}(\mathrm{End}(E_{j_k})^*/\{\pm 1\}))^{-1}$ est le degré du diviseur $A_E \in \mathcal{P}_S$, et $w(C_i) = \mathrm{card}(\mathrm{End}(E_{j_i})^*/\{\pm 1\})$.

Démonstration. Il suffit d'appliquer le lemme [17, lemma 3.1.2] qui donne le nombre d'arêtes N entre les deux sommets C_1 et C_2 dans $\mathcal{G}((X^{pq}/w_q)_{\mathbb{F}_p})$. Le nombre d'arêtes $N(C_1, C_2)$ liant les deux sommets non exceptionnels C_1 et C_2 dans $\mathcal{G}(\widetilde{(X^{pq}/w_q)_{\mathbb{F}_p}})$ étant égal à N, ou à $N-1$ si $\{C_1,\ C_2\} = \{J_1,\ J_2\}$ ou $\{C_1,\ C_2\} = \{G_1,\ G_2\}$ et $p \equiv 1 \mod 3$. □

Une conséquence utile du lemme 2.3.8 est le corollaire suivant.

Corollaire 2.3.9. *Pour $p \gg q$, on a $N(C_1, C_2) > 0$ pour tout $C_1 \in S_1'$ et $C_2 \in S_2'$.*

Dans la suite nous supposerons que cette condition est satisfaite.

Pour prouver le lemme 2.3.2, nous devons traiter le cas où $p \equiv 1 \mod 3$. Si $q \equiv 1 \mod 3$, la seule composante exceptionnelle est $\mathcal{J}$ et la preuve de [17, lemma 3.1.3] reste valable. On se place dans le cas où $q \equiv -1 \mod 3$. Supposons d'abord que J n'est pas une des composantes exceptionnelles $\mathcal{J}_1$ ou $\mathcal{J}_2$. Soient i et j tels que $\{i, j\} = \{1, 2\}$. On

note $I(G_i) = 0$ si $J \neq G_i$ et $I(G_i) = p+1$ si $J = G_i$. En appliquant la loi K (lemme 2.3.6) successivement aux sommets $\mathcal{J}_i$ et $\mathcal{J}_j$, on trouve :

$$(\nu(\mathcal{J}_i) - \nu(\mathcal{J}_j)) + (\nu(\mathcal{J}_i) - \nu(G_i)) = 0,$$

$$(\nu(\mathcal{J}_j) - \nu(\mathcal{J}_i)) + (\nu(\mathcal{J}_j) - \nu(G_j)) = 0.$$

Soit :

$$\nu(G_i) - \nu(\mathcal{J}_i) = \nu(\mathcal{J}_i) - \nu(\mathcal{J}_j) = \nu(\mathcal{J}_j) - \nu(G_j).$$

Donc :

$$\nu(G_i) - \nu(G_j) = 3(\nu(G_i) - \nu(\mathcal{J}_i)). \tag{2.1}$$

D'autre part en appliquant la loi K au sommet G_i, on trouve :

$$N(G_i, G_j)(\nu(G_i) - \nu(G_j)) + (\nu(G_i) - \nu(\mathcal{J}_i)) + \sum_{D \in S'_j \setminus \{G_j\}} N(G_i, D)(\nu(G_i) - \nu(D)) = I(G_i).$$

En combinant avec l'égalité (2.1) (ou directement en appliquant la loi des résistances en série), on trouve :

$$(N(G_i, G_j) + \frac{1}{3})(\nu(G_i) - \nu(G_j)) + \sum_{D \in S'_j \setminus \{G_j\}} N(G_i, D)(\nu(G_i) - \nu(D)) = I(G_i).$$

Pour C_1 et C_2 différents de $\mathcal{J}_1$ et de $\mathcal{J}_2$ on pose :

$$N'(C_1, C_2) = \begin{cases} N(C_1, C_2) + 1/3 \text{ si } \{C_1, C_2\} = \{G_1, G_2\}; \\ N(C_1, C_2) \text{ sinon.} \end{cases}$$

Ceci nous permet de considérer un système d'équations dont les inconnues sont les $\nu(C)$ où $C \in S'_1 \sqcup S'_2 \sqcup \{\mathcal{J}\}$, c'est-à-dire $C \neq \mathcal{J}_1, \mathcal{J}_2$, et dont les coefficients sont les $N'(C_1, C_2)$ pour $C_1, C_2 \in S'_1 \sqcup S'_2 \sqcup \{\mathcal{J}\}$. Pour prouver que ce système est sans solution entière, reprenons la preuve de [17, lemma 3.1.3] en remplaçant dans toutes les équations $N(C_1, C_2)$ par $N'(C_1, C_2)$. La preuve de [17, lemma 3.1.3] utilise les valeurs asymptotiques (à $O_q(\sqrt{p})$ près) de $N(C_1, C_2)$. Ces valeurs étant conservées lorsque on remplace $N(C_1, C_2)$ par $N'(C_1, C_2)$. On obtient une preuve du lemme 2.3.2 dans le cas où $J \neq \mathcal{J}_1, \mathcal{J}_2$.

Il reste à prouver le lemme 2.3.2 dans le cas où $J = \mathcal{J}_1$ ou $\mathcal{J}_2$. Comme l'involution w_p échange $\mathcal{J}_1$ et $\mathcal{J}_2$ et laisse invariant $\mathcal{J}$, il suffit de prouver le lemme suivant :

Lemme 2.3.10. *Avec les notations du lemme 2.3.2, supposons que* $q \equiv -1 \mod 3$ *et* $p \equiv 1 \mod 3$. *Pour* $p \gg q$, *on a* $(p+1)(\mathcal{J} - \mathcal{J}_1) \neq 0$ *dans le groupe des composantes de* $\mathrm{Jac}(X^{pq}/w_q)_{\mathbb{F}_p}$.

Démonstration. On suppose qu'il existe une répartition de potentiels entiers ν, sur les sommets de $\mathcal{G}(\widetilde{(X^{pq}/w_q)_{\mathbb{F}_p}})$, tel qu'un courant de $p+1$ Ampères entre dans le circuit au sommet $\mathcal{J}_1$ et le quitte en $\mathcal{J}$.

Nous allons prouver que pour $p \gg q$ les potentiels $\nu(j_{1,1})$, $\nu(j_{1,2}), \ldots, \nu(j_{1,l})$ et $\nu(j_{2,1})$, $\nu(j_{2,2}), \ldots, \nu(j_{2,l})$ sont tous égaux (cf. sous-lemme 2.3.16). Puis nous obtiendrons une contradiction (cf. sous-lemmes 2.3.17 et 2.3.18). Fixons J_M un sommet ayant un potentiel maximal dans $S_1' \cup S_2' \setminus \{G_1, G_2\}$. Ainsi que J_m un sommet ayant un potentiel minimal dans $S_1' \cup S_2' \setminus \{J_1, J_2\}$.

Sous-lemme 2.3.11. Soient i, j tels que $\{i, j\} = \{1, 2\}$ et $J_M \in S_j'$. On a la majoration suivante pour l'intensité du courant que J_M reçoit de G_i :

$$N(J_M, G_i)(\nu(G_i) - \nu(J_M)) \leq \frac{6(p+1)}{(3w(A_E) - 1)\epsilon(G_i, J_M)w(J_M)} + O_q(\sqrt{p}).$$

Démonstration. Remarquons que si $\nu(G_i) \leq \nu(J_M)$ la proposition est évidente. On va donc supposer $\nu(G_i) > \nu(J_M)$. Par la loi K exprimée en le sommet G_i,

$$\sum_{D \mapsto G_i} (\nu(G_i) - \nu(D)) = 0,$$

c'est-à-dire

$$\sum_{\substack{D \mapsto G_i \\ D \neq G_j, \mathcal{J}_i}} (\nu(G_i) - \nu(D)) = N(G_j, G_i)(\nu(G_j) - \nu(G_i)) + (\nu(\mathcal{J}_i) - \nu(G_i)). \tag{2.2}$$

Nous allons majorer $N(G_j, G_i)(\nu(G_j) - \nu(G_i)) + (\nu(\mathcal{J}_i) - \nu(G_i))$. En appliquant la loi K au sommet $\mathcal{J}_1$ on trouve :

$$(\nu(\mathcal{J}_1) - \nu(G_1)) + (\nu(\mathcal{J}_1) - \nu(\mathcal{J}_2)) = p + 1;$$

et en appliquant la loi K au sommet $\mathcal{J}_2$ on obtient

$$\nu(\mathcal{J}_1) - \nu(\mathcal{J}_2) = \nu(\mathcal{J}_2) - \nu(G_2). \tag{2.3}$$

Donc on a

$$(\nu(\mathcal{J}_1) - \nu(G_1)) + (\nu(\mathcal{J}_2) - \nu(G_2)) = p + 1. \tag{2.4}$$

D'après [17, Sublemma 3.1.3.2], on a $\nu(\mathcal{J}_1) \geq \nu(G_1), \nu(\mathcal{J}_2)$ donc $\nu(\mathcal{J}_1) - \nu(G_1) \geq 0$ et $\nu(\mathcal{J}_2) - \nu(G_2) = \nu(\mathcal{J}_1) - \nu(\mathcal{J}_2) \geq 0$ d'après l'égalité (2.3). On a donc

$$\nu(\mathcal{J}_i) - \nu(G_i) \leq p + 1, \tag{2.5}$$

On applique la loi K au sommet G_j :

$$\sum_{\substack{D \mapsto G_j \\ D \neq G_i, \mathcal{J}_j}} (\nu(D) - \nu(G_j)) = N(G_j, G_i)(\nu(G_j) - \nu(G_i)) + (\nu(G_j) - \nu(\mathcal{J}_j)).$$

Si on suppose $\nu(G_j) > \nu(G_i)$, on a par hypothèse $\nu(G_i) > \nu(J_M) \geq \nu(D)$ pour tout $D \in (S_1' \sqcup S_2') \setminus \{G_1, G_2\}$, on en déduit $\nu(G_j) > \nu(D)$ et

$$N(G_i, G_j)(\nu(G_j) - \nu(G_i)) \leq \nu(\mathcal{J}_j) - \nu(G_j). \tag{2.6}$$

En combinant l'égalité (2.4) avec l'inégalité (2.6) si $\nu(G_j) > \nu(G_i)$ et en considérant l'inégalité (2.5) si $\nu(G_j) \leq \nu(G_i)$, on trouve l'inégalité suivante :

$$N(G_j, G_i)(\nu(G_j) - \nu(G_i)) + (\nu(\mathcal{J}_i) - \nu(G_i)) \leq p + 1. \tag{2.7}$$

En combinant l'égalité (2.2) avec la majoration (2.7), on trouve :

$$\sum_{\substack{D \mapsto G_i \\ D \neq G_j, \mathcal{J}_i}} (\nu(G_i) - \nu(D)) \leq p + 1.$$

Comme J_M a un potentiel maximal parmi tous les sommets adjacents à G_i différents de G_j et $\mathcal{J}_i$, on a

$$\sum_{\substack{D \mapsto G_i \\ D \neq G_j, \mathcal{J}_i}} (\nu(G_i) - \nu(J_M)) \leq p + 1.$$

Soit :

$$\big(N(G_i) - N(G_i, G_j) - N(G_i, \mathcal{J}_i)\big)(\nu(G_i) - \nu(J_M)) \leq p + 1$$

Soit C l'intensité du courant que J_M reçoit de G_i, on a l'inégalité :

$$C = N(G_i, J_M)(\nu(G_i) - \nu(J_M)) \leq N(G_i, J_M)\frac{(p+1)}{(N(G_i) - N(G_i, G_j) - 1)}.$$

On utilise les lemmes 2.3.7 et 2.3.8 :

$$C \leq \frac{p+1}{(p+5)/6 - 1 - (p+1)/(18w(A_E)) + O_q(\sqrt{p})}\left(\frac{p+1}{w(A_E)\epsilon(G_i, J_M)3w(J_M)} + O_q(\sqrt{p})\right).$$

$$\leq \left(\frac{18w(A_E)}{3w(A_E) - 1} + \frac{O_q(\sqrt{p})}{p+1}\right)\left(\frac{p+1}{w(A_E)\epsilon(G_i, J_M)3w(J_M)} + O_q(\sqrt{p})\right).$$

Finalement :

$$C \leq \frac{6(p+1)}{(3w(A_E) - 1)\epsilon(G_i, J_M)w(J_M)} + O_q(\sqrt{p}).$$

□

On démontre un résultat similaire pour J_m.

Sous-lemme 2.3.12. Soient i, j tels que $\{i, j\} = \{1, 2\}$ et $J_m \in S_j'$. On a la majoration suivante pour le courant que J_m donne à J_i :

$$N(J_m, J_i)(\nu(J_m) - \nu(J_i)) \leq \frac{4(p+1)}{(2w(A_E) - 1)\epsilon(J_i, J_m)w(J_m)} + O_q(\sqrt{p}).$$

Démonstration. Remarquons que si $\nu(J_i) \geq \nu(J_m)$ la proposition est évidente, nous supposerons dans la suite que $\nu(J_i) < \nu(J_m)$. Par la loi K exprimée en le sommet J_i,

$$\sum_{\substack{D \mapsto J_i \\ D \neq J_j, \mathcal{J}}} \nu(D) - \nu(J_i) = N(J_i, J_j)(\nu(J_i) - \nu(J_j)) + (\nu(J_i) - \nu(\mathcal{J})). \tag{2.8}$$

Nous allons majorer la quantité $N(J_i, J_j)(\nu(J_i) - \nu(J_j)) + (\nu(J_i) - \nu(\mathcal{J}))$. En appliquant la loi K au sommet $\mathcal{J}$, on trouve :

$$(\nu(J_i) - \nu(\mathcal{J})) + (\nu(J_j) - \nu(\mathcal{J})) = p + 1 \tag{2.9}$$

D'après [17, Sublemma 3.1.3.2] on a $\nu(\mathcal{J}) \leq \nu(J_j)$, donc

$$\nu(J_i) - \nu(\mathcal{J}) \leq p + 1 \tag{2.10}$$

On applique la loi K au sommet J_j :

$$\sum_{\substack{D \mapsto J_j \\ D \neq J_i, \mathcal{J}}} \nu(D) - \nu(J_j) = N(J_i, J_j)(\nu(J_j) - \nu(J_i)) + \nu(J_j) - \nu(\mathcal{J}).$$

Si $\nu(J_j) < \nu(J_i)$, alors comme par hypothèse $\nu(J_i) < \nu(J_m) \leq \nu(D)$ pour tout sommet $D \in S_1' \sqcup S_2' \setminus \{J_1, J_2\}$, on a $\nu(J_j) \leq \nu(D)$ et

$$N(J_i, J_j)(\nu(J_i) - \nu(J_j)) \leq \nu(J_j) - \nu(\mathcal{J}) \tag{2.11}$$

En combinant l'inégalité (2.11) avec l'égalité (2.9) si $\nu(J_j) < \nu(J_i)$ et en considérant l'inégalité (2.10) si $\nu(J_j) \geq \nu(J_i)$, on trouve la majoration :

$$N(J_i, J_j)(\nu(J_i) - \nu(J_j)) + (\nu(J_i) - \nu(\mathcal{J})) \leq p + 1 \tag{2.12}$$

En combinant cette inégalité (2.12) avec l'égalité (2.8), on trouve :

$$\sum_{\substack{D \mapsto J_i \\ D \neq J_j, \mathcal{J}}} \nu(D) - \nu(J_i) \leq p + 1.$$

Comme J_m a un potentiel minimal parmi tous les sommets adjacents à J_i différents de J_j et $\mathcal{J}$, on a

$$(N(J_i) - N(J_i, \mathcal{J}) - N(J_i, J_j))(\nu(J_m) - \nu(J_i)) \leq p + 1,$$

donc

$$\nu(J_m) - \nu(J_i) \leq \frac{p+1}{N(J_i) - 1 - N(J_i, J_j)}.$$

On utilise les lemmes 2.3.7 et 2.3.8 :

$$\nu(J_m) - \nu(J_i) \leq \frac{p+1}{(p+3)/4 - 1 - (p+1)/(w(A_E)8) + O_q(\sqrt{p})}$$

Soit

$$\nu(J_m) - \nu(J_i) \leq \frac{8w(A_E)}{2w(A_E)-1} + \frac{O_q(\sqrt{p})}{p+1}.$$

D'autre part, le courant C que J_m donne à J_i est :

$$C = N(J_i, J_m)(\nu(J_m) - \nu(J_i)).$$

$$= \left(\frac{p+1}{w(A_E)2\epsilon(J_i,J_m)w(J_m)} + O_q(\sqrt{p})\right)(\nu(J_m) - \nu(J_i)).$$

D'où l'inégalité :

$$C \leq \frac{4(p+1)}{(2w(A_E)-1)\epsilon(J_i,J_m)w(J_m)} + O_q(\sqrt{p}).$$

□

Nous allons prouver que J_M ne peut pas être égal à J_1 ou J_2 et que J_m ne peut pas être G_1 ou G_2.

Sous-lemme 2.3.13. Pour $p \gg q$, on a les inégalités : $\nu(J_1), \nu(J_2) < \nu(J_M)$ et $\nu(G_1)$, $\nu(G_2) > \nu(J_m)$.

Démonstration. Supposons que pour $j = 1$ ou 2 on a $J_j = J_M$, nous allons obtenir une contradiction pour $p \gg q$. En appliquant la loi de Kirchhoff au sommet J_j on obtient :

$$\sum_{\substack{D \mapsto J_j \\ D \neq \mathcal{J}, G_i}} \nu(D) - \nu(J_j) = N(J_j, G_i)(\nu(J_j) - \nu(G_i)) + \nu(J_j) - \nu(\mathcal{J});$$

où i est tel que $\{i, j\} = \{1, 2\}$. Par hypothèse, pour tout sommet D adjacent à J_j et différent de $\mathcal{J}$ et de G_i, on a $\nu(D) \leq \nu(J_j)$. D'où :

$$N(J_j, G_i)(\nu(G_i) - \nu(J_j)) \geq \nu(J_j) - \nu(\mathcal{J}). \tag{2.13}$$

On applique le sous-lemme 2.3.11 à $J_j = J_M$:

$$N(J_j, G_i)(\nu(G_i) - \nu(J_j)) \leq \frac{3(p+1)}{2(3w(A_E)-1)} + O_q(\sqrt{p}). \tag{2.14}$$

D'autre part en appliquant la loi K à $\mathcal{J}$ on trouve :

$$\nu(\mathcal{J}) - \nu(J_1) + \nu(\mathcal{J}) - \nu(J_2) = -(p+1),$$

comme $\nu(J_1), \nu(J_2) \leq \nu(J_j)$ on en déduit que :

$$\nu(J_j) - \nu(\mathcal{J}) \geq (p+1)/2. \tag{2.15}$$

En combinant ces trois inégalités (2.13), (2.14) et (2.15) on trouve :

$$\frac{p+1}{2} \leq \frac{3(p+1)}{2(3w(A_E)-1)} + O_q(\sqrt{p}).$$

Ce qui est contradictoire pour $p \gg q$ comme $w(A_E) > 4/3$ d'après la remarque 2.3.3.

Supposons que pour $j = 1$ ou 2 on a $G_j = J_m$, nous allons obtenir une contradiction pour $p \gg q$. En appliquant la loi de Kirchhoff au sommet G_j on obtient :

$$\sum_{\substack{D \mapsto G_j \\ D \neq \mathcal{J}_j, J_i}} \nu(D) - \nu(G_j) = N(G_j, J_i)(\nu(G_j) - \nu(J_i)) + \nu(G_j) - \nu(\mathcal{J}_j);$$

où i est tel que $\{i, j\} = \{1, 2\}$. Par hypothèse, pour tout sommet D adjacent à G_j et différent de $\mathcal{J}_j$ et de J_i, on a $\nu(D) \geq \nu(G_j)$. D'où :

$$\nu(\mathcal{J}_j) - \nu(G_j) \leq N(G_j, J_i)(\nu(G_j) - \nu(J_i)),$$

on applique le sous-lemme 2.3.12 à $G_j = J_m$:

$$\nu(\mathcal{J}_j) - \nu(G_j) \leq \frac{2(p+1)}{3(2w(A_E)-1)} + O_q(\sqrt{p}). \tag{2.16}$$

D'autre part, en appliquant la loi K au sommet $\mathcal{J}_1$

$$\nu(\mathcal{J}_1) - \nu(G_1) + \nu(\mathcal{J}_1) - \nu(\mathcal{J}_2) = p + 1, \tag{2.17}$$

et en appliquant la loi K au sommet $\mathcal{J}_2$

$$\nu(\mathcal{J}_2) - \nu(G_2) + \nu(\mathcal{J}_2) - \nu(\mathcal{J}_1) = 0,$$

soit

$$\nu(\mathcal{J}_1) - \nu(G_2) = 2(\nu(\mathcal{J}_1) - \nu(\mathcal{J}_2). \tag{2.18}$$

En combinant les deux égalités (2.17) et (2.18), on obtient :

$$\nu(\mathcal{J}_1) - \nu(G_1) + \frac{1}{2}(\nu(\mathcal{J}_1) - \nu(G_2)) = p + 1. \tag{2.19}$$

Comme $\nu(G_j) \leq \nu(G_1), \nu(G_2)$, on a l'inégalité : $3/2(\nu(\mathcal{J}_1) - \nu(G_j)) \geq p + 1$. Si $j = 1$ on en déduit que $\nu(\mathcal{J}_1) - \nu(G_1) \geq 2/3(p + 1)$. Si $j = 2$, en utilisant (2.18), on obtient $\nu(\mathcal{J}_2) - \nu(G_2) \geq 1/3(p + 1)$. Dans tous les cas on a :

$$\nu(\mathcal{J}_j) - \nu(G_j) \geq \frac{1}{3}(p+1).$$

En combinant avec l'inégalité (2.16) :

$$\frac{1}{3}(p+1) \leq \frac{2(p+1)}{3(2w(A_E)-1)} + O_q(\sqrt{p}).$$

Ce qui est impossible si $p \gg q$ comme $w(A_E) > 3/2$ d'après la remarque 2.3.3. □

On suppose dans la suite que les hypothèses du sous-lemme 2.3.13 ci-dessus sont satisfaites.

Sous-lemme 2.3.14. Soient i, j tels que $\{i, j\} = \{1, 2\}$ et $J_M \in S'_j$. Pour $p \gg q$, le potentiel $\nu(J_M)$ ne peut pas être strictement supérieur au potentiel de 3 sommets ou plus de S'_i.

Démonstration. D'après les hypothèses, $\nu(J_M)$ est supérieur aux potentiels de tous les sommets de $S'_i \setminus \{G_i\}$. Supposons que $\nu(J_M)$ est strictement supérieur au potentiel de 3 sommets D_1, D_2, D_3 de S'_i. On applique la loi K au sommet J_M en remarquant que $J_M \neq J_j$ d'après le sous-lemme 2.3.13 :

$$\sum_{\substack{D \mapsto J_M \\ D \neq G_i}} \nu(J_M) - \nu(D) = N(J_M, G_i)(\nu(G_i) - \nu(J_M)).$$

Comme $\nu(J_M) - \nu(D) \geq 0$ pour $D \in S'_i \setminus \{G_i\}$, on a $\nu(G_i) - \nu(J_M) \geq 0$, donc $G_i \notin \{D_1, D_2, D_3\}$. On a donc

$$\sum_{k=1}^{3} N(J_M, D_k)(\nu(J_M) - \nu(D_k)) \leq N(J_M, G_i)(\nu(G_i) - \nu(J_M)). \tag{2.20}$$

Par hypothèse, $\nu(J_M) - \nu(D_k) \geq 1$, on en déduit l'inégalité :

$$\sum_{k=1}^{3} N(J_M, D_k) \leq N(J_M, G_i)(\nu(G_i) - \nu(J_M)).$$

On rappelle que

$$N(J_M, D_k) = \frac{p+1}{w(A_E)\epsilon(J_M, D_k)w(J_M)w(D_k)} + O_q(\sqrt{p}).$$

Comme $\epsilon(J_M, D_k) \leq \epsilon(G_i, J_M)$ et $w(D_k) = 1$ sauf pour $D_k = J_i$, auquel cas $w(J_i) = 2$.

$$\sum_{k=1}^{3} N(J_M, D_k) \geq \frac{5}{2} \times \frac{(p+1)}{w(A_E)\epsilon(G_i, J_M)w(J_M)} + O_q(\sqrt{p}).$$

En combinant avec l'inégalité (2.20) et le sous-lemme 2.3.11 on obtient :

$$\frac{5(p+1)}{2w(A_E)\epsilon(G_i, J_M)w(J_M)} + O_q(\sqrt{p}) \leq \frac{6(p+1)}{(3w(A_E)-1)w(J_M)\epsilon(G_i, J_M)} + O_q(\sqrt{p}).$$

Comme d'après la remarque 2.3.3 $w(A_E) > 5/2$, on obtient une contradiction pour $p \gg q$. □

On démontre un résultat similaire pour J_m.

Sous-lemme 2.3.15. Soient i, j tels que $\{i, j\} = \{1, 2\}$ et $J_m \in S'_j$. Le potentiel $\nu(J_m)$ ne peut pas être strictement inférieur au potentiel de 3 sommets ou plus de S'_i.

Démonstration. D'après les hypothèses, $\nu(J_m)$ est inférieur à tous les potentiels des sommets de $S'_i \setminus \{J_i\}$. Supposons en outre que $\nu(J_m)$ est strictement inférieur au potentiel de 3 sommets D_1, D_2, D_3 de S'_i. On applique la loi K au sommet J_m en notant que $J_m \neq J_j$ par le sous-lemme 2.3.13 :

$$\sum_{\substack{D \mapsto J_m \\ D \neq J_i}} \nu(D) - \nu(J_m) = N(J_m, J_i)(\nu(J_m) - \nu(J_i)).$$

Comme $\nu(D) - \nu(J_m) \geq 0$ pour tout $D \in S'_2 \setminus \{J_i\}$, on a $\nu(J_m) - \nu(J_i) \geq 0$, donc $J_i \notin \{D_1, D_2, D_3\}$. On a :

$$\sum_{k=1}^{3} N(D_k, J_m)(\nu(D_k) - \nu(J_m)) \leq N(J_m, J_i)(\nu(J_m) - \nu(J_i)).$$

Comme par hypothèse, $\nu(D_k) - \nu(J_m) \geq 1$ pour $i = 1, 2, 3$, on a :

$$\sum_{k=1}^{3} N(D_k, J_m) \leq N(J_m, J_i)(\nu(J_m) - \nu(J_i)).$$

Soit en appliquant le lemme 2.3.8

$$\sum_{k=1}^{3} \frac{p+1}{w(A_E)\epsilon(J_m, D_k)w(J_m)w(D_k)} + O_q(\sqrt{p}) \leq N(J_m, J_i)(\nu(J_m) - \nu(J_i)).$$

Remarquons que $\epsilon(J_m, D_k) \leq \epsilon(J_i, J_m)$ et $w(D_k) = 1$ sauf pour $D_k = G_i$, auquel cas $w(G_i) = 3$. On en déduit :

$$\frac{(7/3)(p+1)}{w(A_E)w(J_m)\epsilon(J_i, J_m)} + O_q(\sqrt{p}) \leq N(J_m, J_i)(\nu(J_m) - \nu(J_i)).$$

En utilisant la majoration donnée par le sous-lemme 2.3.12, on obtient :

$$\frac{(7/3)(p+1)}{w(A_E)w(J_m)\epsilon(J_i, J_m)} + O_q(\sqrt{p}) \leq \frac{4(p+1)}{(2w(A_E)-1)w(J_m)\epsilon(J_i, J_m)} + O_q(\sqrt{p}).$$

Ce qui est contradictoire pour $p \gg q$ comme $w(A_E) > 7/2$ d'après la remarque 2.3.3.

□

Sous-lemme 2.3.16. Sous l'hypothèse que $g(X_0(q)) \geq 6$, pour $p \gg q$ les potentiels $\nu(j_{1,1})$, $\nu(j_{1,2}), \ldots, \nu(j_{1,l})$ et $\nu(j_{2,1})$, $\nu(j_{2,2}), \ldots, \nu(j_{2,l})$ sont tous égaux. En particulier $\nu(J_M) = \nu(J_m)$.

Démonstration. Notons n le cardinal de S_1' (et S_2'). On rappelle que $S_1' = S_1/w_q$ (cf. notations 2.3.4), que le cardinal de S_1 est $g(X_0(q)) + 1$, et que w_q laisse fixe au moins les deux sommets J_1 et G_1 de S_2. Donc $n \geq 2 + (g(X_0(q)) - 1)/2$, on en déduit $n \geq 5$.

Pour $i = 1, 2$, on fixe $J_{i,M}$ un sommet ayant un potentiel maximal dans l'ensemble $S_i' \setminus \{G_i\}$. Ainsi que $J_{i,m}$ un sommet dans l'ensemble $S_i' \setminus \{J_i\}$ ayant un potentiel minimal. Supposons que $\nu(J_{1,M}) \neq \nu(J_{2,M})$, alors J_M a un potentiel strictement supérieur au potentiel de $n-1$ sommets ou plus de la répartition opposée. Pour $p \gg q$ cela contredit le sous-lemme 2.3.14. De même si $\nu(J_{1,m}) \neq \nu(J_{2,m})$, alors J_m a un potentiel strictement inférieur au potentiel de $n-1$ sommets ou plus de la répartition opposée ce qui contredit le sous-lemme 2.3.15 pour $p \gg q$. On a donc $\nu(J_{1,M}) = \nu(J_{2,M})$ et $\nu(J_{1,m}) = \nu(J_{2,m})$ pour $p \gg q$.

Supposons que $\nu(J_{1,m}) = \nu(J_{2,m}) < \nu(J_{1,M}) = \nu(J_{2,M})$. Si $\nu(J_{1,M})$ est strictement supérieur au potentiel de 3 sommets ou plus de S_2' on peut appliquer le sous-lemme 2.3.14 pour $J_M = J_{1,M}$. Sinon il y a au plus 2 sommets D_1, D_2 de S_2' de potentiel strictement inférieur à $\nu(J_{1,M})$, tous les sommets de $S_2' \setminus \{D_1, D_2\}$ sont de potentiel supérieur ou égal à $\nu(J_{1,M})$, et strictement supérieur à $J_{1,m}$. Il y a donc $n-2$ sommets ou plus de S_2' de potentiel strictement supérieur au potentiel de $J_m = J_{1,m}$. Ceci contredit le sous-lemme 2.3.15. Finalement pour $p \gg q$ on doit avoir $\nu(J_{1,m}) = \nu(J_{2,m}) = \nu(J_{1,M}) = \nu(J_{2,M})$, ce qui démontre la proposition. □

Dans toute la suite nous supposons que les hypothèses du sous-lemme 2.3.16 sont satisfaites. Les potentiels $\nu(j_{1,1}), \nu(j_{1,2}), \ldots, \nu(j_{1,l})$ et $\nu(j_{2,1}), \nu(j_{2,2}), \ldots, \nu(j_{2,l})$ sont donc tous égaux à $\nu(J_m) = \nu(J_M)$.

Sous-lemme 2.3.17. On a $\nu(J_1) \equiv \nu(J_2) \mod 2$. En outre $\nu(J_1) \neq \nu(J_2)$.

Démonstration. En appliquant la loi K au sommet $\mathcal{J}$ on obtient :

$$\nu(J_1) - \nu(\mathcal{J}) + \nu(J_2) - \nu(\mathcal{J}) = p + 1.$$

En considérant cette égalité modulo 2 on trouve :

$$\nu(J_1) \equiv \nu(J_2) \mod 2,$$

ce qui démontre le premier point.

Supposons que $\nu(J_1) = \nu(J_2)$. En appliquant la loi K au sommet J_1 on trouve :

$$\sum_{k=1}^{l} N(J_1, j_{2,k})(\nu(j_{2,k}) - \nu(J_1)) + N(J_1, G_2)(\nu(G_2) - \nu(J_1)) + (\nu(\mathcal{J}) - \nu(J_1)) = 0.$$

En appliquant la loi K au sommet J_2 on trouve :

$$\sum_{k=1}^{l} N(J_2, j_{1,k})(\nu(j_{1,k}) - \nu(J_2)) + N(J_2, G_1)(\nu(G_1) - \nu(J_2)) + (\nu(\mathcal{J}) - \nu(J_2)) = 0.$$

Or $N(J_1, j_{2,k}) = N(J_2, j_{1,k})$, et $N(J_2, G_1) = N(J_1, G_2)$. En outre pour $p \gg q$, par le sous-lemme 2.3.16, on a $\nu(j_{2,k}) = \nu(j_{1,k})$ et, par le corollaire 2.3.9, $N(J_1, G_2) > 0$. On en déduit : $\nu(G_1) = \nu(G_2)$. D'autre part en appliquant successivement la loi K aux sommets $\mathcal{J}_1$ et $\mathcal{J}_2$, on trouve (voir preuve du sous-lemme 2.3.13 formule (2.19) ou appliquer la loi des résistances en série) :

$$\nu(\mathcal{J}_1) - \nu(G_1) + \frac{1}{2}(\nu(\mathcal{J}_1) - \nu(G_2)) = p + 1$$

En considérant cette égalité modulo 3, comme par hypothèse $p \equiv 1 \mod 3$, on a :

$$\nu(G_2) - \nu(G_1) \equiv 2 \mod 3,$$

En particulier $\nu(G_1) \neq (G_2)$ ce qui est contradictoire. On a donc $\nu(J_1) \neq \nu(J_2)$. □

Le sous-lemme 2.3.18 suivant nous permet de conclure à une contradiction avec le sous-lemme 2.3.17 pour $p \gg q$, ce qui achève la preuve du lemme 2.3.10. □

Sous-lemme 2.3.18. On a $|\nu(J_1) - \nu(J_2)| < 2$.

Démonstration. Soient i et j tels que $\{i, j\} = \{1, 2\}$ et $\nu(J_i) \leq \nu(J_j)$. Supposons que $\nu(J_j) - \nu(J_i) \geq 2$. D'après le sous-lemme 2.3.13, $\nu(J_M) > \nu(J_j)$, donc $\nu(J_M) \geq \nu(J_i) + 3$. En outre d'après les sous-lemmes 2.3.13 et 2.3.16, on a $\nu(G_j) > \nu(J_m) = \nu(J_M) \geq \nu(J_i)+3$. Donc pour tout sommet $D \in S_j$, on a $\nu(D) - \nu(J_i) \geq 3$. En appliquant la loi K à J_i on trouve :

$$\sum_{\substack{D \mapsto J_i \\ D \neq \mathcal{J}}} (\nu(D) - \nu(J_i)) = \nu(J_i) - \nu(\mathcal{J}),$$

Soit :

$$\sum_{\substack{D \mapsto J_i \\ D \neq \mathcal{J}}} 3 \leq \nu(J_i) - \nu(\mathcal{J}),$$

c'est-à-dire :

$$3(N(J_i) - 1) \leq \nu(J_i) - \nu(\mathcal{J}),$$

soit d'après le lemme 2.3.7,

$$\frac{3(p-1)}{4} \leq \nu(J_i) - \nu(\mathcal{J}).$$

D'autre part en appliquant le loi K à $\mathcal{J}$

$$\nu(J_1) - \nu(\mathcal{J}) + \nu(J_2) - \nu(\mathcal{J}) = p + 1$$

et en utilisant l'inégalité : $\nu(J_i) \leq \nu(J_j)$, on trouve

$$\nu(J_i) - \nu(\mathcal{J}) \leq \frac{p+1}{2}.$$

On en déduit : $3(p-1)/4 \leq (p+1)/2$ ce qui est impossible pour $p > 5$ (on a $p > 5$ car les hypothèses faites sur p impliquent $p \equiv 1 \mod 12$). □

2.4 Points rationnels sur les courbes de Shimura

Le critère de [17] repose sur une description du groupe des caractères du quotient d'enroulement de la composante neutre de la fibre en p du modèle de Néron sur $\mathbb{Z}_p$ de la jacobienne $\mathrm{Jac}(X^{pq})^0_{\mathbb{F}_p}$ de la courbe de Shimura X^{pq}. D'après un théorème de Raynaud (cf [7, 12.4]), le groupe des caractères de $\mathrm{Jac}(X^{pq})^0_{\mathbb{F}_p}$ est isomorphe au groupe des cycles sur le graphe dual de la fibre en p de la courbe de Shimura $\mathscr{G}(X^{pq}_{\mathbb{F}_p})$. À l'aide d'une généralisation de la formule de Gross, Parent et Yafaev prouvent que le groupe des caractère du quotient d'enroulement de $\mathrm{Jac}(X^{pq})^0_{\mathbb{F}_p}$ est isomorphe au groupe des cycles sur $\mathscr{G}(X^{pq}_{\mathbb{F}_p})$ constitués de projections orthogonales pour l'accouplement de monodromie de vecteurs de Gross sur l'espace des diviseurs de degré 0 sur les arêtes du graphe $\mathscr{G}(X^{pq}_{\mathbb{F}_p})$.

Rappelons que $\mathcal{L}$ et Y (introduits dans le paragraphe 2) désignent respectivement les $\mathbb{Z}$-modules des chemins et des cycles sur le graphe $\mathscr{G}(X^{pq}_{\mathbb{F}_p})$. On considère également les $\mathbb{Q}$-espaces vectoriels $\mathcal{L}_{\mathbb{Q}} = \mathcal{L} \otimes \mathbb{Q}$ et $Y_{\mathbb{Q}} = Y \otimes \mathbb{Q}$.

On note $I_{pq,e}$ l'idéal d'enroulement de $\mathbb{T}_{\Gamma_0(pq)}$, c'est-à-dire l'ensemble des opérateurs de $\mathbb{T}_{\Gamma_0(pq)}$ annulant toutes les formes modulaires primitives f de poids 2 pour $\Gamma_0(pq)$ telles que $L(f,1) \neq 0$. On a la proposition suivante qui généralise la proposition 2.2.7.

Proposition 2.4.1. *On note par $\mathbb{E}$ l'espace engendré par les projections orthogonales des vecteurs de Gross sur $\mathcal{L}_{\mathbb{Q}}$. On a l'égalité : $\mathbb{E} = \mathcal{L}_{\mathbb{Q}}[I_{pq,e}]$.*

Consulter [17, prop 4.2]. En combinant la proposition 2.4.1 avec le théorème de Raynaud décrivant le groupe des caractères de $\mathrm{Jac}(X^{pq})^0_{\mathbb{F}_p}$ comme groupe des cycles sur $\mathscr{G}(X^{pq}_{\mathbb{F}_p})$, on obtient la proposition suivante :

Proposition 2.4.2. *L'espace $\mathbb{E} \cap Y_{\mathbb{Q}}$ est le groupe des caractères du quotient d'enroulement de $\mathrm{Jac}(X^{pq})^0_{\mathbb{F}_p}$.*

Consulter [17, prop 4.3].

Théorème 2.4.3. *Soient p et q deux nombres premiers tels que $q > 245$, $q \equiv 3 \mod 4$, $p \equiv 5 \mod 12$, $\left(\frac{q}{p}\right) = -1$, et $p \gg q$. S'il existe $C \in Y \cap \mathbb{E}$, un chemin fermé sur le graphe $\mathscr{G}(X^{pq}_{\mathbb{F}_p})$ constitué de projections orthogonales de vecteurs de Gross sur $\mathcal{L}^0$, qui contient les deux arêtes exceptionnelles de longueur 2 avec une multiplicité première à p, alors la courbe quotient X^{pq}/w_q est sans point rationnel non spécial.*

Démonstration. Consulter [17, Theorem 5.3]. L'énoncé que nous donnons est légèrement différent : nous remplaçons l'hypothèse « C est un chemin fermé fait de vecteurs de Gross » par « C est un chemin fermé constitué de projection orthogonales de vecteurs de Gross ». En consultant la preuve de Parent et Yafaev, on voit que C correspond à un caractère du quotient d'enroulement de $\mathrm{Jac}(X^{pq})^0_{\mathbb{F}_p}$, ce qui est équivalent, d'après la proposition 2.4.2, au fait que C est dans $Y \cap \mathbb{E}$.

On peut aussi noter que le vecteur d'Eisenstein appartient à l'espace engendré par les vecteurs de Gross, et donc que la projection orthogonale sur $\mathcal{L}^0$ d'un chemin en vecteurs de Gross est également constitué de vecteurs de Gross.

□

Nous allons utiliser le travail du troisième paragraphe pour généraliser ce critère en supprimant la condition $p \equiv -1 \mod 3$. Ainsi les hypothèses de congruences sur p et q sont équivalentes aux conditions du cas non ramifié de Ogg ((2) théorème 2.2.1).

Théorème 2.4.4. *Soient p et q deux nombres premiers tel que $q > 245$, $q \equiv 3 \mod 4$, $p \equiv 1 \mod 4$, $\left(\frac{q}{p}\right) = -1$, et $p \gg q$. S'il existe $C \in Y \cap \mathbb{E}$, un chemin fermé sur le graphe $\mathscr{G}(X^{pq}_{\mathbb{F}_p})$ constitué de projections orthogonales de vecteurs de Gross sur $\mathcal{L}^0$, qui contient les deux arêtes exceptionnelles de longueur 2 avec une multiplicité première à p, alors la courbe quotient X^{pq}/w_q est sans point rationnel non spécial.*

Démonstration. Dans la preuve de [17, Theorem 5.3] l'hypothèse $p \equiv -1 \mod 3$ n'est utilisée que dans la preuve du lemme [17, lemma 3.1.3]. Or nous avons généralisé ce lemme (cf. lemme 2.3.2) en supprimant cette condition. □

Pour la preuve du théorème 2.1.1, nous utiliserons la présente proposition décrivant l'image du vecteur d'Eisenstein-Shimura a_E par les applications s_* et t_*.

Proposition 2.4.5. *Si A_E et a_E désignent respectivement les vecteurs d'Eisenstein sur le graphe modulaire $\mathscr{G}(X_0(q)_{\mathbb{F}_q})$ et le graphe de Shimura $\mathscr{G}(X^{pq}_{\mathbb{F}_p})$ (cf. définitions 2.2.3 et 2.2.9), on a : $s_*(a_E) = (p+1)A_E$, et $t_*(a_E) = (p+1)A_E$.*

Démonstration. Par définition :

$$a_E = \sum_{i=1}^{n} \frac{1}{\mathrm{card}(\mathrm{End}(e_i)^*/\{\pm 1\})} e_i = \sum_{\substack{(E,C_p) \\ \text{à isom. près}}} \frac{1}{(\mathrm{End}(E,C_p)^*/\{\pm 1\})} (E, C_p).$$

Où (E, C_p) parcourt l'ensemble des couples constitué d'une courbe elliptique supersingulière E en caractéristique q et d'un sous groupe d'ordre p de E

$$s_*(a_E) = \sum_{k=1}^{g+1} \Bigg(\sum_{\substack{(E_{j_k}, C_p) \\ \text{à isom. près}}} \frac{1}{\text{card}(\text{End}(E_{j_k}, C_p)^*/\{\pm 1\})} \Bigg) E_{j_k}.$$

Pour k fixé, il y a $p+1$ couples de la forme (E_{j_k}, C_p). Par la formule des classes pour le groupe $\text{End}(E_{j_k})^*/\{\pm 1\}$ opérant sur l'ensemble des (E_{j_k}, C_p), on a :

$$\sum_{\substack{(E_{j_k}, C_p) \\ \text{à isom. près}}} \frac{1}{\text{card}(\text{End}(E_{j_k}, C_p)^*/\{\pm 1\})} = \frac{p+1}{\text{card}(\text{End}(E_{j_k})^*/\{\pm 1\})}.$$

Donc $s_*(a_E) = (p+1)A_E$. On montre de même que $t_*(a_E) = (p+1)A_E$.

□

Prouvons maintenant notre résultat principal : le théorème 2.1.1 dont l'énoncé est rappelé ci-dessous.

Théorème 2.4.6. *Soit $q > 245$ un nombre premier avec $q \equiv 3 \mod 4$. Il existe une borne B_q dépendant de q telle que si p est un nombre premier vérifiant $p \equiv 1 \mod 4$, $\left(\frac{p}{q}\right) = -1$ et $p \geq B_q$, alors la courbe X^{pq}/w_q est sans point rationnel non spécial.*

Démonstration. Soit $l \neq p, q$ un nombre premier. D'après la proposition 2.2.8, le vecteur d'Eisenstein modulaire A_E sur $\mathscr{G}((X_0(q))_{\mathbb{F}_q})$ appartient au $\mathbb{Q}-$espace engendré par les vecteurs de Gross de la forme Γ_D, pour $D = -4l^{2n}$, où $n \geq 1$. Ces vecteurs Γ_D correspondent à des sous-ordres stricts O_D de l'ordre O_{-4} de conducteurs l^n. On peut donc écrire A_E comme combinaison linéaire de ces vecteurs :

$$\lambda_0 A_E = \sum_{n=1}^{N} \lambda_n \Gamma_{-4l^{2n}},$$

avec $\lambda_n \in \mathbb{Z}$ et $\lambda_0 \neq 0$. Pour ne pas avoir de dénominateurs on choisit tous les λ_n multiples de 12. D'après la proposition 2.2.16, il existe B une borne telle que, pour $p \geq B$, chacun des vecteurs $\gamma_{-4l^{2n}}$ soit sans arête commune avec les vecteurs γ_{-4} et γ_{-3}. On suppose dans la suite $p \geq B$, de telle sorte que les vecteurs $\Gamma_{-4l^{2n}}$ ne contiennent pas d'arête exceptionnelle de longueur 2 ou 3. On impose en outre que p ne divise pas λ_0. On suppose également que $p \gg q$ de telle sorte qu'on puisse appliquer le théorème 2.4.4.

Considérons le chemin en vecteurs de Gross $C = \sum_{n=1}^{N} \lambda_n \gamma_{-4l^{2n}}$ sur le graphe dual de la fibre en p de la courbe de Shimura X^{pq}. D'après l'hypothèse, $p \equiv 1 \mod 4$, p est scindé dans O_{-4} et dans tous ses sous-ordres stricts $O_{-4l^{2n}}$. En outre chacun de ces vecteurs ne contient que des arêtes de longueur 1. On peut appliquer le corollaire 2.2.14 :

$$s_*(C) = \sum_{n=1}^{N} \lambda_n s_*(\gamma_{-4l^{2n}}) = \sum_{n=1}^{N} \lambda_n 4\Gamma_{-4l^{2n}} = 4\lambda_0 A_E.$$

De même $t_*(C) = 4\lambda_0(A_E)$. D'autre part d'après la proposition 2.4.5, on a : $s_*(a_E) = t_*(a_E) = (p+1)A_E$. Le chemin $C_0 = (p+1)C - 4\lambda_0 a_E$, est un chemin fermé. Pour cela il suffit de voir que $s_*(C_0) = t_*(C_0) = 0$.

D'autre part, le chemin C_0 est la projection orthogonale pour l'accouplement de monodromie du chemin en vecteurs de Gross $(p+1)C$ sur l'espace $\mathcal{L}^0$ des diviseurs de degré 0. Donc C_0 appartient à $\mathbb{E}$. Finalement C_0 est un chemin de $\mathbb{E} \cap Y$. D'après les hypothèses faites sur p, les vecteurs du chemin C ne contiennent pas d'arête exceptionnelle de longueur 2. D'autre part le vecteur d'Eisenstein a_E contient chacune des deux arêtes exceptionnelle de longueur 2 avec multiplicité 1/2. Le chemin C_0 passe par chacune de ces arêtes exceptionnelles avec multiplicité $2\lambda_0$. Donc on peut appliquer le théorème de Parent-Yafaev à ce chemin. On en déduit que la courbe de Shimura X^{pq}/w_q est sans point rationnel non spécial.

□

Chapitre 3

Surfaces abéliennes à multiplication quaternionique munies d'une structure de niveau $\Gamma_0(N)$

3.1 Introduction

Les degrés possibles des isogénies cycliques rationnelles de courbes elliptiques, sont bien connus. Les travaux de Mazur [12] ont abouti à une description complète des isogénies de degré premier. Nous nous intéressons à un problème analogue dans le cas de certaines surfaces abéliennes de type GL_2 à multiplication quaternionique. Fixons B_D une algèbre de quaternions sur $\mathbb{Q}$ de discriminant D et O_D un ordre maximal de B_D. Considérons une surface abélienne $A/\mathbb{Q}$ telle que l'anneau $\mathrm{End}_{\overline{\mathbb{Q}}}(A)$ des endomorphismes de A sur $\overline{\mathbb{Q}}$ est isomorphe à O_D. On se demande pour quelles valeurs de $N \in \mathbb{N}$, premier à D, la surface abélienne $A/\mathbb{Q}$ admet une structure de niveau $\Gamma_0(N)$ c'est-à-dire une isogénie rationnelle O_D-cyclique de degré N^2 de noyau $Q_N \simeq \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$. On s'intéresse aux valeurs possibles des couples (D, N) tels qu'il existe une telle surface abélienne $A/\mathbb{Q}$. Remarquons que le cas $D = 1$ correspond aux courbes elliptiques et a été traité par Mazur comme expliqué ci-dessus. Le cas $N = 1$ est lié à une conjecture de Coleman, énoncée ainsi par Clark et Mazur : pour tout entier $g \geq 1$ fixé, il existe un ensemble fini d'anneaux d'endomorphismes sur $\overline{\mathbb{Q}}$ à isomorphisme près pour les variétés abéliennes $A/\mathbb{Q}$ de dimension g. Une réponse positive à cette conjecture dans le cas $g = 2$ impliquerait que pour tout discriminant D sauf un nombre fini, il n'existe pas de surface abélienne $A/\mathbb{Q}$ ayant multiplication quaternionique par B_D (i.e telle que $\mathrm{End}_{\overline{\mathbb{Q}}}(A) \otimes \mathbb{Q} \simeq B_D$). Il découle de notre théorème principal (cf. théorème 2.1.1) que pour D fixé il y a un nombre fini effectif de couples (D, N) possibles. On note que, si la conjecture de Coleman est vraie, il existe même un nombre fini de couples (D, N) possibles, D variant.

Ce problème est aussi lié à l'existence de points rationnels sur certains quotients d'Atkin-Lehner de courbes de Shimura. Soit $X_0^D(N)$ la courbe de Shimura de discri-

minant D et de niveau N. Cette courbe de Shimura est un espace de module grossier pour les triplets $(A, \iota, Q_N)/\overline{\mathbb{Q}}$ constitué d'une surface abélienne $A/\overline{\mathbb{Q}}$ d'un morphisme $\iota\colon O_D \hookrightarrow \mathrm{End}_{\overline{\mathbb{Q}}}(A)$ et de $Q_N \simeq \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ un sous-groupe O_D-cyclique de $A[N]$. D'après [2, thm 4.5], une surface abélienne $A/\mathbb{Q}$ comme ci-dessus correspond à un point rationnel sur le quotient $X_0^D(N)/w_m$ de la courbe de Shimura de discriminant D par l'involution d'Atkin-Lehner w_m, où $m \mid D$ est tel que $\mathrm{End}_{\mathbb{Q}}(A) \otimes \mathbb{Q} \simeq \mathbb{Q}(\sqrt{m})$. On suppose que $\mathrm{End}_{\overline{\mathbb{Q}}}(A)$ est isomorphe à un ordre maximal de B_D. Alors la surface abélienne A est simple et le point correspondant à A sur $X_0^D(N)/w_m$ est non-spécial. En effet les points spéciaux de $X_0^D(N)/w_m$ sont les points associés aux surfaces abéliennes isogènes au carré d'une courbe elliptique à multiplication complexe. L'existence de telles surfaces abéliennes est donc liée à l'existence de points rationnels non spéciaux sur certains quotients d'Atkin-Lehner de courbes de Shimura. L'absence de point rationnel non spécial sur $X_0^D(N)/w_m$ est en fait une propriété plus forte que l'absence de surfaces abéliennes $A/\mathbb{Q}$ à multiplication par B_D sur $\overline{\mathbb{Q}}$ et munies d'une structure de niveau $\Gamma_0(N)$. En effet des points de $X_0^D(N)/w_m(\mathbb{Q})$ peuvent correspondre à des surfaces abéliennes définies sur une extension de $\mathbb{Q}$ et admettant $\mathbb{Q}$ comme corps de module.

Fixons une algèbre de quaternions sur $\mathbb{Q}$ indéfinie B_D de discriminant D, ainsi que m un diviseur de D et K un corps quadratique imaginaire. On se pose la question suivante : Peut-on trouver une borne (dépendant de D et K) sur les nombres premiers N tels qu'il existe des surfaces abéliennes $A/\mathbb{Q}$ telles que $\mathrm{End}_K(A) \simeq O_D$ et A est munie d'une structure de niveau $\Gamma_0(N)$? Clark pose une question similaire dans sa thèse (cf. [3, Conjecture 111] et la discussion qui suit) : peut-on trouver une borne sur les nombres premiers N tels qu'il existe des points de $X_0^D(N)(K)$ se réduisant en des points de $X_0^D(N)/w_m(\mathbb{Q})$? Une réponse positive à la question de Clark sur les courbes de Shimura entrainerait une réponse positive à notre première question. Un corollaire d'un théorème de Ohta et du théorème de Faltings (cf. théorème 3.1.1 ci-dessous) donne une réponse partielle à cette seconde question, en prouvant l'existence d'une telle borne sous la condition que le genre de $X_0^D(1)/w_m$ est ≥ 2. Ce théorème est énoncé par Clark (cf. [3, cor 119]) dans le cas $m = D$:

Théorème 3.1.1. *(Faltings, Ohta). Soit D le discriminant d'une algèbre de quaternions B_D indéfinie et m un diviseur de D. On suppose que le genre de $X_0^D(1)/w_m$ est ≥ 2. Pour tout corps de nombres F, il existe une borne M telle que pour $N \geq M$, la courbe $X_0^D(N)/w_m$ n'a pas de point F-rationnel.*

Rappellons comment on peut déduire ce théorème des résultats de Faltings et de Ohta. D'après le théorème de Faltings, lorsque le genre de $X_0^D(1)/w_m$ est ≥ 2, pour tout corps de nombres F l'ensemble $X_0^D(1)/w_m(F)$ est fini. Nous allons expliquer comment déduire du théorème de Ohta [15] que pour chacun de ces points $P \in X_0^D(1)/w_m(F)$, il existe un nombre fini de nombres premiers N tels que P se relève en un point de $X_0^D(N)(F)$. Ce théorème de Ohta est un analogue pour les surfaces abéliennes à multiplication quaternionique du théorème de Serre sur la « grosse image » de la représentation de Galois

adélique associée à une courbe elliptique (cf. [25, thm. 3 et cor. au thm. 5]). Fixons un point de $X_0^D(1)/w_m(F)$, ce point correspond à une surface abélienne A/K définie sur une extension K de F (dépendante de A) telle que $\mathrm{End}_{\overline{K}}(A) \simeq O_D$ un ordre maximal de B_D. Quitte à remplacer K par une extension finie, on peut supposer que tous les endomorphismes de $A/\overline{K}$ sont définis sur K de telle sorte que $\mathrm{End}_K(A) \simeq O_D$. Pour un nombre premier $N \nmid D$, le module de Tate $T_N(A) \simeq \mathbb{Z}_N^4$ associé à A est un O_D-module isomorphe à $O_D \otimes \mathbb{Z}_N \simeq M_2(\mathbb{Z}_N)$ muni d'une action du groupe de Galois $\mathrm{Gal}(\overline{K}/K)$. On a donc une représentation :

$$\mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}_{O_D}(T_N(A)) \simeq (O_D \otimes \mathbb{Z}_N)^* \simeq \mathrm{GL}_2(\mathbb{Z}_N),$$

(cf. [15, prop. 1.1]). D'après [15, §0 Theorem], pour tout nombre premier N, sauf peut-être un nombre fini, cette représentation est surjective. Or si A admet une structure de niveau $\Gamma_0(N)$, l'image de la représentation ci-dessus est d'indice $\geq N$ dans $\mathrm{GL}_2(\mathbb{Z}_N)$. Ceci n'est donc possible que pour un nombre fini de nombres premiers N.

En employant des méthodes similaires à la méthode de Mazur, Clark prouve dans sa thèse [3, Main Theorem 4] le théorème 3.1.2 ci-dessous. Ce théorème affine le résultat du théorème 3.1.1 dans le cas $m = D$ en supprimant la condition sur le genre de $X_0^D(1)/w_D$.

Théorème 3.1.2. *(Clark) Soit D le discriminant d'une algèbre de quaternions B_D sur $\mathbb{Q}$ indéfinie. Pour tout corps de nombres F, et pour tout corps quadratique imaginaire K, il existe une borne absolue M telle que pour un nombre premier $N \geq M$ satisfaisant $N \equiv 1 \mod 4$ et N reste premier dans F, il n'existe pas de point F-rationnel de $X_0^D(N)/w_D$ provenant d'un point de $X_0^D(N)(K)$.*

On a également un résultat récent d'Arai et Momose : pour un corps quadratique fixé, il n'y a pas de point K-rationnel non spécial sur la courbe de Shimura $X_0^D(p)$ pour p assez grand. Un corollaire immédiat est l'existence d'une borne sur les structures de niveau possibles sur les surfaces abéliennes $A/\mathbb{Q}$ ayant multiplication quaternionique par un ordre maximal de B_D sur une extension $K/\mathbb{Q}$ fixée.

Le théorème de Faltings étant non effectif, la borne donnée par le théorème 3.1.1 est non effective. On ne peut donc en déduire qu'une réponse non effective à la question de l'existence d'une borne supérieure sur les structures de niveau premier N possibles sur les surfaces abéliennes $A/\mathbb{Q}$ ayant multiplication quaternionique par un ordre maximal de B_D. La borne donnée par le théorème de Clark peut-être rendue effective, mais elle n'est pas valable pour tout les nombres premiers. Dans le théorème 3.1.3 ci-dessous nous donnons une borne effective pour ce problème, en fonction de D et du corps K sur lequel tous les endomorphismes de A sont définis.

Théorème 3.1.3. *Il existe une constante absolue C, telle que pour toute algèbre de quaternions sur $\mathbb{Q}$ indéfinie B_D, de discriminant D et pour tout corps quadratique imaginaire $K = \mathbb{Q}[\sqrt{-d}]$, où d est un entier sans facteurs carré, pour toute surface abélienne*

$A/\mathbb{Q}$, telle que $\mathrm{End}_K(A) \simeq O_D$ un ordre maximal de B_D et pour tout nombre premier $N \geq C(\mathrm{ppcm}(D,d))^{22}$, la surface A n'admet pas d'isogénie O_D-cyclique de noyau $\simeq \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$.

La constante C qui apparaît dans l'énoncé dépend des constantes donnés par le théorème de Linnik, (cf [8, thm 18.1] ou théorème 3.4.2 ci-dessous) qui sont explicitement calculables. Nous donnons un moyen plus précis pour calculer la borne dans le lemme 3.4.1. Au passage, dans le corollaire 3.3.3 nous améliorons la borne donnée par le théorème de Clark, en trouvant une borne indépendante de D, m et K, valable uniquement pour les nombres premiers N satisfaisants la condition supplémentaire $N \equiv 1 \mod 4$. Ces résultats 3.1.3 et 3.3.3 sont valables quel que soit le genre de $X_0^D(1)/w_D$. Il serait particulièrement intéressant de pouvoir trouver une telle borne qui soit indépendante du corps de nombre K. Ceci est possible lorsque $m \neq D$, car dans ce cas, il y a un nombre fini de possibilité pour K, comme nous le remarquons dans le théorème 3.1.4 ci-dessous. On rappelle que $\mathrm{End}_{\mathbb{Q}}(A) \otimes \mathbb{Q}$ est un corps quadratique réel.

Théorème 3.1.4. *Soit C la constante donnée par le théorème 3.1.3. Soient B_D une algèbre de quaternions sur $\mathbb{Q}$ indéfinie, de discriminant D, et O_D un ordre maximal de B_D. Soit $E = \mathbb{Q}(\sqrt{m})$ un corps quadratique réel. On suppose qu'il existe un nombre premier impair $p \mid D$ et $p \nmid m$. Alors pour toute surface abélienne $A/\mathbb{Q}$ telle que $\mathrm{End}_{\overline{\mathbb{Q}}}(A) \simeq O_D$, et $\mathrm{End}_{\mathbb{Q}}(A) \simeq R_E$ soit l'anneau des entiers de E, pour tout nombre premier $N \geq CD^{22}$, la surface A n'admet pas d'isogénie O_D-cyclique de noyau $\simeq \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$.*

Décrivons maintenant la stratégie de la preuve, inspirée des travaux de Mazur, développés notamment par Clark, Rotger, Jordan, Arai et Momose. Soit $A/\mathbb{Q}$ une surface abélienne telle que $\mathrm{End}_K(A) \simeq O_D$. La variété abélienne $A/\mathbb{Q}$ est de type GL_2, son anneau d'endomorphismes sur $\mathbb{Q}$, $\mathrm{End}_{\mathbb{Q}}(A)$ est un ordre dans un corps de nombre E de degré 2 sur $\mathbb{Q}$, d'anneau des entiers R_E. Pour un nombre premier N, et $\mathcal{N}$ un premier de E au-dessus de N, soit $E_{\mathcal{N}}$ le complété de E en $\mathcal{N}$. D'après ces hypothèses, la surface abélienne A est de type GL_2, donc l'action de $G_{\mathbb{Q}}$ sur le module de Tate $V_N(A)$ définit une représentation $\mathcal{R}_{\mathcal{N}} \colon G_{\mathbb{Q}} \to \mathrm{GL}_2(E_{\mathcal{N}})$. Nous étudions $r_{\mathcal{N}} \colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_N)$, la réduction modulo $\mathcal{N}$ de cette représentation, qui est donnée par l'action du groupe de Galois sur $A[\mathcal{N}]$ l'ensemble des points de $\mathcal{N}$-torsion de A. Supposons que A admet une structure de niveau $\Gamma_0(N)$, c'est-à-dire $A[N]$ admet un sous-groupe O_D-cyclique $Q_N \simeq \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ stable par l'action de $G_{\mathbb{Q}}$. La représentation $r_{\mathcal{N}}$ de $G_{\mathbb{Q}}$ sur $A[\mathcal{N}]$ est alors réductible. On note par $\alpha_{\mathcal{N}} \colon G_{\mathbb{Q}} \to \overline{\mathbb{F}}_N$ le caractère d'isogénie, donnée par l'action de $G_{\mathbb{Q}}$ sur le sous-groupe $A[\mathcal{N}] \cap Q_N$. La représentation $r_{\mathcal{N}}$ s'écrit sous la forme :

$$r_{\mathcal{N}} \colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_N)$$

$$\sigma \mapsto \begin{pmatrix} \alpha_{\mathcal{N}}(\sigma) & * \\ 0 & \chi_N(\sigma)(\alpha_{\mathcal{N}}(\sigma))^{-1} \end{pmatrix},$$

où χ_N est le N-ième caractère cyclotomique (cf. lemme 3.2.3).

Pour un nombre premier $\ell \neq N$, on considère $a_\ell \in R_E$ la trace de $R_{\mathcal{N}}(\phi_\ell)$, où ϕ_ℓ est une substitution de Frobenius en ℓ (élément de $G_{\mathbb{Q}}$ se réduisant en le Frobenius en ℓ). Ce coefficient a_ℓ est bien défini à condition que ℓ soit un nombre premier de bonne réduction. Comme la surface A a multiplication quaternionique, elle admet partout potentiellement bonne réduction d'après un résultat de Shimura (voir par exemple [19, thm 3]), ce qui nous permet de définir des coefficients a_ℓ pour tout $\ell \neq N$. Pour connaître a_ℓ modulo $\mathcal{N} = r_N(\phi_\ell)$, nous étudions le caractère $\alpha_{\mathcal{N}}$. Pour cela nous étudions la ramification du caractère $\alpha_{\mathcal{N}}$ en ℓ pour tout nombre premier $\ell \neq N$. Nous démontrons (lemme 3.2.5) que $\alpha_{\mathcal{N}}$ peut s'écrire sous la forme $\chi_N^{k'}\beta_{\mathcal{N}}$, où $k' \in \mathbb{Z}/(N-1)\mathbb{Z}$ et $\beta_{\mathcal{N}}^{24}$ est partout non ramifié, donc égal à 1. En outre on peut restreindre l'ensemble des valeurs possibles de k' à une liste finie indépendante de N. On en déduit (proposition 3.3.1) que pour tout $\ell \neq N$ il existe une racine 24-ième de l'unité $\zeta(\ell)$ telle que :

$$a_\ell \equiv \ell^k\zeta(\ell) + \ell^{1-k}\zeta(\ell)^{-1} \mod \overline{\mathcal{N}},$$

pour $\overline{\mathcal{N}}$ une place de $\overline{\mathbb{Q}}$ au-dessus de $\mathcal{N}$ et $k \in \{0, 1, 1/2, 1/3, 2/3\}$. Pour $N \gg \ell$ cette congruence est une égalité. On a donc un nombre restreint de valeurs possibles pour a_ℓ. Maintenant nous utilisons les propriétés des coefficients a_ℓ pour obtenir une contradiction à l'existence d'une telle N^2-isogénie. Sous certaines conditions sur ℓ, nous prouvons (lemme 3.4.1) que le coefficient a_ℓ ne peut pas être écrit sous une telle forme. Ces conditions nous permettent de trouver de tels premiers ℓ à partir de K et de D, et d'en déduire une borne M (en fonction de ℓ) telle que pour $M \geq N$, il ne peut pas exister de structure de niveau $\Gamma_0(N)$ sur A.

3.2 Représentations associées aux surfaces abéliennes de type GL_2

Dans ce paragraphe nous allons étudier la représentation de $G_{\mathbb{Q}}$ dans les points de N-torsion d'une surface abélienne à multiplication quaternionique, admettant une structure de niveau $\Gamma_0(N)$ pour un nombre premier N. Soit $A/\mathbb{Q}$ une surface abélienne, on fait les hypothèses suivantes :

Hypothèses 3.2.1. On suppose que $\mathrm{End}_{\overline{\mathbb{Q}}}(A)$ l'anneau des endomorphismes sur $\overline{\mathbb{Q}}$ de A est isomorphe à un ordre maximal O_D d'une algèbre de quaternions sur $\mathbb{Q}$ indéfinie B_D de discriminant D.

D'après [23, Lemma 2.3], ces hypothèses impliquent que $\mathrm{End}_{\mathbb{Q}} A \otimes \mathbb{Q}$ est un corps de nombres E totalement réel et que le corps K sur lequel tous les endomorphismes de A sont définie est un corps quadratique imaginaire. En outre d'après [24, thm 3.1] on a $E = \mathbb{Q}(\sqrt{m})$ avec $m = D$ ou $m = D/p$ pour un certain nombre premier p divisant D.

Comme $A/\mathbb{Q}$ est de type GL_2, pour tout nombre premier ℓ on peut lui associer une représentation linéaire de $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ dans $\mathrm{GL}_2(R_E \otimes \mathbb{Z}_\ell)$, où R_E est l'anneau des

entiers de E. En effet le module de Tate $T_\ell(A)$ est un $\mathrm{End}_{\mathbb{Q}} A \otimes \mathbb{Z}_\ell$-module libre de dimension 2. L'action de $G_{\mathbb{Q}}$ sur $T_\ell(A)$ définit une action :

$$G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathrm{End}_{\mathbb{Q}} A \otimes \mathbb{Z}_\ell) \to \mathrm{GL}_2(R_E \otimes \mathbb{Z}_\ell).$$

Pour $\mathcal{N}$ premier de E au-dessus de N, on note $R_{E,\mathcal{N}}$ le complété de R_E en $\mathcal{N}$. On a une représentation :

$$\mathcal{R}_{\mathcal{N}} \colon G_{\mathbb{Q}} \to \mathrm{GL}_2(R_{E,\mathcal{N}}).$$

En réduisant la représentation $\mathcal{R}_{\mathcal{N}}$ modulo $\mathcal{N}$, on obtient une représentation :

$$r_{\mathcal{N}} \colon G_{\mathbb{Q}} \to \mathrm{GL}_2(R_{E,\mathcal{N}}/\mathcal{N}) \subseteq \mathrm{GL}_2(\overline{\mathbb{F}}_N),$$

où $R_{E,\mathcal{N}}/\mathcal{N} = \mathbb{F}_N$ si N est scindé ou ramifié dans E, et $R_{E,\mathcal{N}}/\mathcal{N} = \mathbb{F}_{N^2}$ si N est inerte dans E. Il s'agit de la représentation donnée par l'action de $G_{\mathbb{Q}}$ sur l'ensemble $A[\mathcal{N}]$ défini par :

$$A[\mathcal{N}] = \{x \in A(\mathbb{Q}) \ : \ \forall \beta \in \mathcal{N} \cap \mathrm{End}_{\mathbb{Q}}(A),\ \beta x = 0\} \subseteq A[N].$$

D'après [19, thm 3], la surface A a potentiellement partout bonne réduction. Cela nous permet de définir les traces des images par $\mathcal{R}_{\mathcal{N}}$ des substitutions de Frobenius en ℓ pour tout nombre premier ℓ. D'après [27, p. 498], pour tout nombre premier ℓ, il existe une extension totalement ramifiée $L_\ell/\mathbb{Q}_\ell$ où $A/\mathbb{Q}_\ell$ admet bonne réduction de degré $[L_\ell/\mathbb{Q}_\ell]$ majoré par le cardinal de $\mathrm{GL}_2(\mathbb{F}_3) < 3^8$. On a la majoration plus précise $[L_\ell/\mathbb{Q}_\ell] \leq 24$ d'après [9, prop 3.3 et 2.8]. On fixe un plongement de $\overline{\mathbb{Q}}$ dans $\overline{\mathbb{Q}}_l$, ce qui définit une inclusion de $G_{\mathbb{Q}_\ell}$ dans $G_{\mathbb{Q}}$. On choisit un élément $\phi_\ell \in G_{\mathbb{Q}_\ell} \subseteq G_{\mathbb{Q}}$ qui se réduit en le Frobenius de $\overline{\mathbb{F}}_\ell/\mathbb{F}_\ell$ et tel que $\phi_\ell|_{L_\ell} = \mathrm{id}$. Pour $\ell \neq N$, par le critère [27, thm. 1] l'image de ϕ_ℓ par $R_{\mathcal{N}}$ ne dépend que de ℓ, et c'est un élément de $\mathrm{GL}_2(R_E)$. La trace de $R_{\mathcal{N}}(\phi_\ell)$ est notée $a_\ell \in R_E$. On a la majoration ci-dessous pour les coefficients a_ℓ (borne de Weil, cf. [27, theorem 3]) : pour tout plongement $\tau \colon E \to \mathbb{R}$ on a : $|\tau(a_\ell)| \leq 2\sqrt{\ell}$.

Pour résumer on pose les notations suivantes :

Notations 3.2.2. On note K le corps sur lequel tous les endomorphismes de $A/\overline{\mathbb{Q}}$ sont définis. On note $E = \mathrm{End}_{\mathbb{Q}}(A) \otimes \mathbb{Q}$, on a $E = \mathbb{Q}(\sqrt{m})$ pour un certain entier $m \mid D$. On note par R_E l'anneau des entiers de E. On fixe $\mathcal{N}$ un premier de E au-dessus de N et $\overline{\mathcal{N}}$ un premier de $\overline{\mathbb{Q}}$ au-dessus de $\mathcal{N}$. On note $\mathcal{R}_{\mathcal{N}} \colon G_{\mathbb{Q}} \to \mathrm{GL}_2(R_{E,\mathcal{N}})$ la représentation de type GL_2 définie ci-dessus, par $r_{\mathcal{N}}$ sa réduction modulo $\mathcal{N}$ et $\alpha_{\mathcal{N}}$ le caractère d'isogénie donné par l'action de $G_{\mathbb{Q}}$ sur $A[\mathcal{N}] \cap Q_N$. Pour tout nombre premier $\ell \neq N$, on fixe une inclusion $G_{\mathbb{Q}_\ell}$ dans $G_{\mathbb{Q}}$. On dénote par $\phi_\ell \in G_{\mathbb{Q}_\ell} \subset G_{\mathbb{Q}}$ une substitution de Frobenius telle que $\phi_\ell|_{L_\ell} = \mathrm{id}$ pour L_ℓ une extension totalement ramifiée de $\mathbb{Q}_\ell$ où $A/\mathbb{Q}_\ell$ admet bonne réduction. On appelle $a_\ell \in R_E$ la trace de $\mathcal{R}_{\mathcal{N}}(\phi_\ell)$.

Lemme 3.2.3. *Avec les conditions et notations de 3.2.1 et 3.2.2, il existe un plongement de* $\mathrm{GL}_2(R_E/\mathcal{N}R_E)$ *dans* $\mathrm{M}_2(\overline{\mathbb{F}}_N)$, *pour lequel la représentation* $r_{\mathcal{N}}$ *est triangulaire supérieure de la forme :*

$$r_{\mathcal{N}} \colon \sigma \mapsto \begin{pmatrix} \alpha_{\mathcal{N}}(\sigma) & * \\ 0 & \chi_N(\sigma)(\alpha_{\mathcal{N}}(\sigma))^{-1} \end{pmatrix},$$

où $\alpha_{\mathcal{N}} \colon G_{\mathbb{Q}} \to R_E/\mathcal{N}R_E \to \overline{\mathbb{F}}_N$ donne l'action de $G_{\mathbb{Q}}$ sur $A[\mathcal{N}] \cap Q_N$.

Démonstration. Le sous-espace $A[\mathcal{N}] \cap Q_N$ est stable par l'action de $G_{\mathbb{Q}}$ et strictement inclus dans $A[\mathcal{N}]$. La représentation $r_{\mathcal{N}}$ peut donc s'écrire sous la forme :

$$r_{\mathcal{N}} \colon \sigma \mapsto \begin{pmatrix} \alpha_{\mathcal{N}}(\sigma) & * \\ 0 & * \end{pmatrix},$$

avec $\alpha_{\mathcal{N}}$ comme dans l'énoncé. D'après [22, Lemma 3.1] le déterminant de $r_{\mathcal{N}}$ est χ_N si E est totalement réel, ce qui est le cas (voir par exemple [23, Lemma 2.3]), ce qui nous permet de déterminer l'autre coefficient diagonal de $r_{\mathcal{N}}$. □

Pour calculer la trace de $r_{\mathcal{N}}$ et les coefficients $a_\ell \mod \mathcal{N}$, nous allons étudier le caractère $\alpha_{\mathcal{N}}$. Les lemmes 3.2.4 et 3.2.5 ci-dessous permettent de contrÃ´ler la ramification de $\alpha_{\mathcal{N}}$ en tout premier.

Lemme 3.2.4. *Avec les conditions et notations de 3.2.1 et 3.2.2, le caractère $\alpha_{\mathcal{N}}^{24}$ est non ramifié en dehors de N.*

Démonstration. Il découle de [9, prop 3.3 and prop 2.8] que pour $\ell \neq N$ l'ordre du groupe $r_{\mathcal{N}}(I_\ell)$ divise 24. Donc pour tout $\ell \neq N$, on a $r_{\mathcal{N}}^{24}(I_\ell) = \{1\}$ et $r_{\mathcal{N}}^{24}$ est non ramifié en dehors de N. Il en est de même de $\alpha_{\mathcal{N}}^{24}$. □

Lemme 3.2.5. *Avec les conditions et notations de 3.2.1 et 3.2.2, on suppose $N > 3$. Le caractère $\alpha_{\mathcal{N}}$ peut être écrit sous la forme $\alpha_{\mathcal{N}} = \chi_N^{k'}\beta_{\mathcal{N}}$, où $k' \in \mathbb{Z}$, $\beta_{\mathcal{N}}^{24}$ est partout non ramifié et $\chi_N \colon G_{\mathbb{Q}} \to \mathbb{F}_N^*$ est le N-ième caractère cyclotomique. En outre il existe $k \in \{0, 1, 1/2, 1/3, 2/3\}$ tel que $12k' \equiv 12k \mod N-1$.*

L'argument de la preuve est tiré de [12, prop 5.1]. Dans toute la suite on fixe une telle décomposition.

Démonstration. On fixe une place de $\overline{\mathbb{Q}}$ au-dessus de N, ce qui définit un plongement $G_{\mathbb{Q}_N} \to G_{\mathbb{Q}}$. On note par I le groupe d'inertie de $G_{\mathbb{Q}_N}$, par I_N le groupe d'inertie sauvage et $I_t \simeq I/I_N$ le groupe d'inertie modérée. La restriction de α_N à I est triviale sur I_N, donc elle se factorise par I_t. Les caractères du groupe d'inertie modérée I_t qui peuvent être étendus en une action de $G_{\mathbb{Q}_N}$ sont les caractères de niveau 1 (cf. [26, 2.2 p. 183]) donc $\alpha_{\mathcal{N}}|_{I_t}$ est de la forme $\theta_{N-1}^{k'}$, pour un certain $k' \in \{0, \ldots, N-2\}$.

Soit χ_N le N-ième caractère cyclotomique. Comme $\chi_N|_{I_t} = \theta_{N-1}$, le caractère $\alpha_{\mathcal{N}}$ peut-être écrit sous la forme $\chi_N^{k'}\beta_{\mathcal{N}}$, avec $\beta_{\mathcal{N}}$ non ramifié en N. D'après le lemme 3.2.4, on a $\beta_{\mathcal{N}}^{24} = 1$.

D'après [9, prop 3.4], il existe une extension totalement ramifiée $L_N/\mathbb{Q}_N$ sur laquelle $A \times_{\mathbb{Q}} \mathbb{Q}_N$ acquiert bonne réduction, dont le degré $e = [L_N : \mathbb{Q}_N]$ divise 4 ou 6. On peut donc supposer que le degré de $L_N/\mathbb{Q}_N$ est 4 ou 6. Soit $\mathcal{A}$ le modèle de Néron de $A \times_{\mathbb{Q}} L_N$ sur O_{L_N} l'anneau des entiers de L_N. Le groupe Q_N s'identifie à un sous-groupe

de $\mathcal{A}[N]$ stable par l'action de G_{L_N}. On considère le schéma $Q_N \cap \mathcal{A}[\mathcal{N}]$ sur O_{L_N}. C'est un schéma en groupes fini et plat sur O_{L_N}. Ce schéma en groupes est de type (N, N) si N est inerte dans E (et $\mathcal{A}[\mathcal{N}] = \mathcal{A}[N]$) ou de type (N) si N est scindé ou ramifié dans E (et $\mathcal{A}[\mathcal{N}] \subsetneq \mathcal{A}[N]$). On considère la représentation donnée par l'action de G_{L_N} sur $Q_N \cap \mathcal{A}[\mathcal{N}]$:

$$G_{L_N} \to \mathrm{Aut}(Q_N \cap \mathcal{A}[\mathcal{N}]),$$

où $\mathrm{Aut}(Q_N \cap \mathcal{A}[\mathcal{N}]) \simeq \mathbb{F}_N^*$ si N est scindé ou ramifié dans E, ou $\mathrm{Aut}(Q_N \cap \mathcal{A}[\mathcal{N}]) \simeq \mathrm{GL}_2(\mathbb{F}_N)$ si N est inerte dans E.

D'autre part d'après le lemme 3.2.3, le $\mathbb{F}_N$-espace vectoriel $Q_N = Q_N \cap \mathcal{A}[\mathcal{N}]$ peut-être muni d'une structure de $R_E/\mathcal{N}R_E$-espace vectoriel de dimension 1, compatible avec l'action de G_{L_N} sur Q_N. L'action de G_{L_N} sur ce $R_E/\mathcal{N}R_E$-espace vectoriel est donnée par $\alpha_{\mathcal{N}}|_{G_{L_N}}$.

Dans le cas où N est scindé ou ramifié dans E, par le théorème de Raynaud [18, cor 3.4.4], l'action de $I_t(\overline{\mathbb{Q}}_N/L_N)$ sur $Q_N \cap \mathcal{A}[\mathcal{N}]$ est donnée par un caractère de niveau 1 de la forme $\theta_{N-1}^{e_1}$, avec $0 \leq e_1 \leq e = [L_N : \mathbb{Q}_N]$. On a donc $\alpha_{\mathcal{N}}|_{G_{L_N}} = \theta_{N-1}^{e_1}$.

Dans le cas où N est inerte dans E, le $\mathbb{F}_N$-espace vectoriel $Q_N = Q_N \cap \mathcal{A}[\mathcal{N}]$ est muni d'une structure de $R_E/NR_E \simeq \mathbb{F}_{N^2}$-espace vectoriel de dimension 1, l'action de G_{L_N} sur ce $\mathbb{F}_{N^2}$-espace vectoriel est donnée par $\alpha_{\mathcal{N}}|_{G_{L_N}}$. D'après ce que nous avons dit plus haut, le caractère $\alpha_{\mathcal{N}}|_I$ est une puissance de θ_{N-1}. Donc $I(G_{L_N})$ agit sur Q_N par homothétie. En particulier la représentation $I(G_{L_N}) \to \mathrm{GL}_2(\mathbb{F}_N)$ donnant cette action est diagonale (donc une représentation réductible) donnée par deux caractères identiques $\psi_1 = \psi_2 = \alpha_{\mathcal{N}}|_{I(G_{L_N})}$.

D'autre part, par le théorème de Raynaud [18, cor 3.4.4], cette représentation de $I(G_{L_N})$ dans $\mathrm{GL}_2(\mathbb{F}_N)$ étant réductible, les caractères diagonaux de sa semi-simplifiée $\psi_1 = \psi_2 \colon I(G_{L_N}) \to \mathbb{F}_N^*$ sont de la forme : $\theta_{N-1}^{e_1}$ avec $0 \leq e_1 \leq e$.

Dans tous les cas, on a prouvé que $\alpha_{\mathcal{N}}|_{I(G_{L_N})} = \theta_{N-1}^{e_1}$, avec $0 \leq e_1 \leq e$. D'après [25, prop 8], on a l'égalité $(\chi_N|_{I(G_{L_N})}) = \theta_{N-1}^{e}$. Comme $\alpha_{\mathcal{N}} = \chi^{k'}\beta_{\mathcal{N}}$ et $\beta_{\mathcal{N}}|_{I(G_{L_N})} = 1$, on a la congruence :

$$k'e \equiv e_1 \mod N - 1.$$

On rappelle que $e = 4$ ou 6. Si e_1 était impair, la congruence $k'e \equiv e_1 \mod N - 1$ impliquerait que $N - 1$ est impair, ce qui n'est pas le cas car $N > 3$ par hypothèse. On a donc e_1 pair. En multipliant les deux termes de cette égalité par $12/e$, on obtient :

$$12k' \equiv 12k \mod N - 1,$$

pour un certain $k = e_1/e \in \{0, 1, 1/2, 1/3, 2/3\}$.

□

3.3 Congruences satisfaites par les traces des substitutions de Frobenius

Nous allons utiliser les résultats de ramification de la représentation $r_{\mathcal{N}}$ du précédent paragraphe pour déterminer un ensemble très restreint de valeurs possibles modulo $\mathcal{N}$ pour la trace a_ℓ d'une substitution de Frobenius en un nombre premier $\ell \neq N$.

On remarque qu'étant donné un nombre premier ℓ et $k \in \{0, 1, 1/2, 1/3, 2/3\}$, on peut définir ℓ^k une puissance k-ième de ℓ à une racine 6-ième de l'unité près.

Proposition 3.3.1. *Avec les notations et conditions de 3.2.5, soit $\ell \neq N$ un nombre premier, soit $\overline{\mathcal{N}}$ un premier de $\overline{\mathbb{Q}}$ au-dessus de $\mathcal{N}$. On fixe ℓ^k une puissance k-ième de ℓ dans $\overline{\mathbb{Z}}$. Il existe une racine 24-ième de l'unité $\zeta(\ell) \in \overline{\mathbb{Z}}$ telle que :*

$$a_\ell \equiv \ell^k \zeta(\ell) + \ell^{1-k} \zeta(\ell)^{-1} \mod \overline{\mathcal{N}}.$$

Démonstration. Soit $\phi_\ell \in G_{\mathbb{Q}}$ une substitution de Frobenius en ℓ, choisi comme expliqué dans les notations 3.2.2. D'après le lemme 3.2.3, la trace de la représentation $r_{\mathcal{N}}$ est : $\alpha_{\mathcal{N}} + \chi_N \alpha_{\mathcal{N}}^{-1}$. Ce qui donne pour ϕ_ℓ :

$$a_\ell \equiv \alpha_{\mathcal{N}}(\phi_\ell) + \chi_N(\phi_\ell)(\alpha_{\mathcal{N}}(\phi_\ell))^{-1} \mod \mathcal{N}.$$

On utilise la décomposition du lemme 3.2.5 :

$$a_\ell \equiv \chi_N^{k'}(\phi_\ell)\beta_{\mathcal{N}}(\phi_\ell) + \chi_N^{1-k'}(\phi_\ell)(\beta_{\mathcal{N}}(\phi_\ell))^{-1} \mod \mathcal{N}.$$

Pour $\ell \neq N$ on a $\chi_N(\phi_\ell) \equiv \ell \mod N$, et d'après le lemme 3.2.5 on a $12k' \equiv 12k \mod N - 1$ donc il existe une racine 12-ième de l'unité $\zeta' \in \overline{\mathbb{Z}}$ telle que

$$\chi_N^{k'}(\phi_\ell) \equiv \ell^{k'} \equiv \zeta' \ell^k \mod \overline{\mathcal{N}}.$$

D'autre part d'après le lemme 3.2.4, le caractère $\beta_{\mathcal{N}}^{24}$ est partout non ramifié, donc est trivial et il existe $\zeta \in \overline{\mathbb{Z}}$ une racine $24-$ième de l'unité telle que $\beta_{\mathcal{N}}(\phi_\ell) \equiv \zeta \mod \overline{\mathcal{N}}$. Posons $\zeta(\ell) = \zeta\zeta'$, c'est une racine 24-ième de l'unité pour laquelle on a :

$$a_\ell \equiv \ell^k \zeta(\ell) + \ell^{1-k} \zeta(\ell)^{-1} \mod \overline{\mathcal{N}}.$$

□

Proposition 3.3.2. *Avec les notations du lemme 3.2.5, soit*

$$M = (199^{1/6} + 199^{-1/6} + 2)^{48} 199^{24} \leq 10^{84.1}.$$

Pour tout nombre premier $N > M$ et pour tout $\ell \neq N$, il existe une racine 24-ième de l'unité $\zeta(\ell)$ telle que :

$$a_\ell \equiv \sqrt{\ell}\left(\zeta(\ell) + \zeta(\ell)^{-1}\right) \mod \overline{\mathcal{N}}.$$

Démonstration. D'après la proposition 3.3.1, on sait que pour tout $\ell \neq N$, il existe $\zeta(\ell) \in \overline{\mathbb{Z}}$ une racine 24-ième de l'unité telle que :

$$a_\ell \equiv \ell^k \zeta(\ell) + \ell^{1-k}\zeta(\ell)^{-1} \mod \overline{\mathcal{N}}.$$

D'autre part le coefficient a_ℓ satisfait l'inégalité : $|\tau(a_\ell)| \leq 2\sqrt{\ell}$ pour tout plongement $\tau\colon E \to \mathbb{R}$. On fixe $k_0 \in \{0, 1, 1/3, 2/3\}$ ($k_0 \neq 1/2$), on va prouver que pour N assez grand on ne peut pas avoir $k = k_0$. Soit ℓ le nombre premier :

$$\ell = \ell_{k_0} = \begin{cases} 7 & \text{si } k_0 = 0 \text{ ou } 1, \\ 199 & \text{si } k_0 = 1/3 \text{ ou } 2/3; \end{cases}$$

on a pour ce nombre premier ℓ :

$$\min_{\substack{\xi\in\mathbb{C} \\ \xi^{24}=1}} \{|\ell^{k_0-1/2}\xi + \ell^{1/2-k_0}\xi^{-1}|\} = |\ell^{k_0-1/2} - \ell^{1/2-k_0}| > 2.$$

On en déduit que :

$$\min_{\substack{\xi\in\mathbb{C} \\ \xi^{24}=1}} \{|\ell^{k_0}\xi + \ell^{1-k_0}\xi^{-1}|\} > 2\sqrt{\ell}.$$

On pose :

$$M_{k_0} = \max_{\substack{\xi\in\mathbb{C} \\ \xi^{24}=1}} \{|\ell^{k_0-1/2}\xi + \ell^{1/2-k_0}\xi^{-1}|\},$$

c'est-à-dire

$$M_{k_0} = \ell^{k_0-1/2} + \ell^{1/2-k_0};$$

On fixe $\zeta_{24} \in \overline{\mathbb{Q}}$ une racine primitive 24-ième de l'unité. On considère le corps :

$$F = \mathbb{Q}(\zeta_{24}, \ell^{k_0}, a_\ell).$$

On a la majoration suivante pour le degré de F sur $\mathbb{Q}$:

$$[F : \mathbb{Q}] \leq [\mathbb{Q}(\zeta_{24}) : \mathbb{Q}][\mathbb{Q}(a_l) : \mathbb{Q}][\mathbb{Q}(\ell^{k_0}) : \mathbb{Q}] \leq 8 * 2 * \varepsilon = 16\varepsilon,$$

avec $\epsilon = 1$ si $k_0 = 0, 1$ et $\epsilon = 3$ si $k_0 = 1/3, 2/3$ (on rappelle que $a_\ell \in E$ et $[E : \mathbb{Q}] = 2$). Pour tout plongement $\tau\colon F \to \mathbb{C}$, on a les inégalités

$$|\tau(a_\ell)| \leq 2\sqrt{\ell} \quad \text{(borne de Weil)} \tag{3.1}$$

$$|\tau\left(\ell^{k_0}\zeta(\ell) + \ell^{1-k_0}\zeta(\ell)^{-1}\right)| > 2\sqrt{\ell}, \tag{3.2}$$

$$|\tau\left(\ell^{k_0}\zeta(\ell) + \ell^{1-k_0}\zeta(\ell)^{-1}\right)| \leq M_{k_0}\sqrt{\ell} \tag{3.3}$$

On déduit de (3.1) et de (3.3) que pour tout plongement $\tau\colon F \to \mathbb{C}$, on a :

$$|\tau\left(\ell^{k_0}\zeta(\ell) + \ell^{1-k_0}\zeta(\ell)^{-1} - a_\ell\right)| \leq (M_{k_0} + 2)\sqrt{\ell}.$$

Donc pour $N_{F/\mathbb{Q}}$ la norme de F sur $\mathbb{Q}$, on a :

$$\left|N_{F/\mathbb{Q}}\left(\ell^{k_0}\zeta(\ell)+\ell^{1-k_0}\zeta(\ell)^{-1}-a_\ell\right)\right| \leq ((M_{k_0}+2)\sqrt{\ell})^{16\varepsilon}.$$

Supposons maintenant que $N > ((M_{k_0}+2)\sqrt{\ell})^{16\varepsilon}$. Prouvons par contraposée qu'on ne peut pas avoir $k = k_0$. En effet si $k = k_0$, on a :

$$a_\ell \equiv \ell^{k_0}\zeta(\ell)+\ell^{1-k_0}\zeta(\ell)^{-1} \mod \overline{\mathcal{N}}, \tag{3.4}$$

$$\text{donc } N \text{ divise } \left|N_{F/\mathbb{Q}}\left(\ell^{k_0}\zeta(\ell)+\ell^{1-k_0}\zeta(\ell)^{-1}-a_\ell\right)\right| \leq ((M_{k_0}+2)\sqrt{\ell})^{16\varepsilon} < N.$$

On en déduit que la congruence (3.4) est une égalité :

$$a_\ell = \ell^{k_0}\zeta(\ell)+\ell^{1-k_0}\zeta(\ell)^{-1},$$

ce qui est contradictoire avec les égalités (3.1) et (3.2).

On a :

$$((M_{k_0}+2)\sqrt{\ell})^{16\varepsilon} = \begin{cases} (7+7^{-1}+2)^{16}7^8 & \text{si } k_0 = 0,\ 1 \\ (199^{1/6}+199^{-1/6}+2)^{48}199^{24} & \text{si } k_0 = 1/3,\ 2/3. \end{cases}$$

On en déduit une borne $M = (199^{1/6}+199^{-1/6}+2)^{48}199^{24}$ telle que pour $N > M$, on ne peut pas avoir $k \in \{0, 1, 1/3, 2/3\}$. On en déduit que $k = 1/2$. On a donc :

$$a_\ell \equiv \sqrt{\ell}\left(\zeta(\ell)+\zeta(\ell)^{-1}\right) \mod \overline{\mathcal{N}}.$$

□

Un corollaire de cette proposition est une version de [3, Main Theorem 4] avec des constantes explicites :

Corollaire 3.3.3. *Soit $A/\mathbb{Q}$ une surface abélienne telle que $\mathrm{End}_{\overline{\mathbb{Q}}}(A)$ est un ordre maximal dans une algèbre de quaternions sur $\mathbb{Q}$. Pour tout nombre premier $N \equiv 1 \mod 4$ tel que $N > (199^{1/6}+199^{-1/6}+2)^{48}199^{24}$, il n'existe pas de structure de niveau $\Gamma_0(N)$ sur A.*

En outre pour tout nombre premier $N \equiv 1 \mod 12$ tel que $N > (7+7^{-1}+2)^{16}7^8$, il n'existe pas de structure de niveau $\Gamma_0(N)$ sur A.

Démonstration. Supposons que A soit munie d'une structure de niveau $\Gamma_0(N)$. D'après la proposition 3.2.5 il existe $k \in \{0, 1, 1/2, 1/3, 2/3\}$ et $k' \in \mathbb{Z}$ satisfaisant la congruence $12k' \equiv 12k \mod N-1$. D'après les propositions 3.3.1 et 3.3.2 pour $N > (199^{1/6}+199^{-1/6}+2)^{48}199^{24}$ on a $k = 1/2$. En particulier la congruence $12k' \equiv 12k \equiv 6 \mod N-1$ implique alors que $N \not\equiv 1 \mod 4$.

Si en outre $N \equiv 1 \mod 3$, on ne peut pas avoir $12k' \equiv 12k \equiv 4$ ou $8 \mod N-1$. On en déduit que k ne peut pas être $1/3$ ou $2/3$. Dans la preuve de la proposition 3.3.2, on peut utiliser la borne plus petite : si $N > (7+7^{-1}+2)^{16}7^8$, on doit avoir $k = 1/2$ et $N \not\equiv 1 \mod 4$, donc $N \not\equiv 1 \mod 12$. □

3.4 Preuve des résultats principaux

Lemme 3.4.1. *Soient B_D une algèbre de quaternions sur $\mathbb{Q}$ indéfinie, de discriminant D. Soit K un corps quadratique imaginaire, on suppose qu'il existe ℓ un nombre premier tel que :*

- *ℓ est scindé ou ramifié dans K ;*
- *il existe un nombre premier $p \mid D$ décomposé dans $\mathbb{Q}(\sqrt{-\ell})$;*
- *$\ell > 3$.*

Soit $M = \max\{4^8\ell^4, 10^{84.1}\}$, alors pour toute surface abélienne $A/\mathbb{Q}$ telle que $\mathrm{End}_K(A)$ est un ordre maximal de B_D, et pour tout nombre premier $N \geq M$, la surface A n'admet pas d'isogénie O_D-cyclique de noyau $\simeq \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$.

Démonstration. Soit ℓ un tel nombre premier, comme ℓ est scindé ou ramifié dans K, on a : $a_\ell \in \mathbb{Q}$, d'après [22, thm 5.5]. Soit $A/\mathbb{Q}$ une surface abélienne à multiplication quaternionique par B_D, et admettant une N^2-isogénie O_D-cyclique de noyau isomorphe à $\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$. D'après la proposition 3.3.2 pour $N \geq 10^{84.1}$, on a :

$$a_\ell \equiv \sqrt{\ell}(\zeta + \zeta^{-1}) \mod \overline{\mathcal{N}}, \tag{3.5}$$

avec $\zeta \in \overline{\mathbb{Z}}$ tel que $\zeta^{24} = 1$. On a : $\zeta + \zeta^{-1} \in \{0, 1, \pm\sqrt{2}, \pm\sqrt{3}, \pm\sqrt{2 \pm \sqrt{3}}\}$. Soit F le corps $\mathbb{Q}(\sqrt{\ell}, \zeta + \zeta^{-1})$. Le degré de F sur $\mathbb{Q}$ est inférieur à 8. Pour tout plongement $\tau \colon F \to \mathbb{R}$ on a :

$$\left|\tau\left(a_\ell - \sqrt{\ell}(\zeta + \zeta^{-1})\right)\right| \leq 4\sqrt{\ell}.$$

On en déduit que pour $N_{F/\mathbb{Q}}$ la norme de F sur $\mathbb{Q}$, on a :

$$\left|N_{F/\mathbb{Q}}\left(a_\ell - \sqrt{\ell}(\zeta + \zeta^{-1})\right)\right| \leq 4^8\ell^4.$$

D'après la congruence (3.5), cette norme est divisible par N. On en déduit que pour N tel que $N > 4^8\ell^4$ cette congruence (3.5) est une égalité :

$$a_\ell = \sqrt{\ell}(\zeta + \zeta^{-1}).$$

Comme par hypothèse $\ell > 3$, on a $\sqrt{\ell}(\zeta + \zeta^{-1}) = 0$ ou $\sqrt{\ell}(\zeta + \zeta^{-1}) \notin \mathbb{Q}$. Or $a_\ell \in \mathbb{Q}$, on a donc $a_\ell = 0$.

On considère l'extension totalement ramifiée $L_\ell/\mathbb{Q}_\ell$ où $A/\mathbb{Q}_\ell$ admet bonne réduction. On note $\mathcal{A}$ le modèle de Néron de $A \times_{\mathbb{Q}} L_\ell$ sur l'anneau des entiers de L_ℓ et $\tilde{A}/\mathbb{F}_\ell$ la fibre spéciale de $\mathcal{A}$. D'après [32, Theorem 2 (a)] et [33, Theorem 1 (1)], l'anneau $\mathrm{End}_{\mathbb{F}_\ell}(\tilde{A}) \otimes \mathbb{Q}$ est isomorphe à $M_{2r}(\tilde{F})$ où $\tilde{F}$ est le corps de décomposition de $T^2 - a_\ell T + \ell$ et $r = 2/[\tilde{F} : \mathbb{Q}]$. Comme $a_\ell = 0$, on a : $\tilde{F} = \mathbb{Q}(\sqrt{-\ell})$ et $r = 1$.

D'autre part pour $\mathcal{L}$ premier de K au-dessus de ℓ, on a $R_K/\mathcal{L} \simeq \mathbb{F}_\ell$ car ℓ n'est pas inerte dans K par hypothèse. On en déduit que $\mathrm{End}_K(A)$ se plonge dans $\mathrm{End}_{\mathbb{F}_\ell}(\tilde{A})$. Donc que B_D se plonge dans $M_2(\tilde{F}) = M_2(\mathbb{Q}(\sqrt{-\ell}))$. Nous allons montrer que l'existence d'un

tel plongement est impossible. Par hypothèse il existe un nombre premier p divisant D qui est décomposé dans $\mathbb{Q}(\sqrt{-\ell})$. Soient $\mathcal{P}_1$ et $\mathcal{P}_2$ les deux premiers de $\mathbb{Q}(\sqrt{-\ell})$ au-dessus de p. Pour $i = 1, 2$ on note $\tilde{F}_{\mathcal{P}_i} \simeq \mathbb{Q}_p$ le complété de $\tilde{F}$ en $\mathcal{P}_i$. Le corps de quaternions $B_D \otimes \mathbb{Q}_p$ sur $\mathbb{Q}_p$ se plonge dans $M_2(\tilde{F}) \otimes \mathbb{Q}_p \simeq M_2(\tilde{F}_{\mathcal{P}_1}) \times M_2(\tilde{F}_{\mathcal{P}_2})$. Or comme $p \mid D$ l'algèbre de quaternionss $B_D \otimes \mathbb{Q}_p$ ne se plonge pas dans $M_2(\tilde{F}_{\mathcal{P}_i}) \simeq M_2(\mathbb{Q}_p)$. On en déduit une contradiction, il ne peut donc pas exister de telle isogénie sur A. □

Maintenant nous allons prouver qu'un tel nombre premier ℓ existe quel que soit le discriminant D et le corps quadratique imaginaire K. Nous allons en outre prouver qu'un tel nombre premier est inférieur à une borne ne dépendant que de D et de K. Pour cela nous utilisons le théorème suivant qui est une version effective du théorème de Dirichlet :

Théorème 3.4.2. *(Linnik, Heath-Brown). Il existe des constantes c et $L = 5.5$ telle que quel pour tout couple d'entiers premiers entre eux (d, a), il existe un nombre premier ℓ tel que*

$$\ell \equiv a \mod d,$$

satisfaisant $\ell \leq cd^L$.

Démonstration. Consulter [8, Thm 18.1]. □

Nous allons maintenant prouver le théorème 3.1.3. La constante C mentionnée dans ce résultat peut être calculée explicitement en fonction de la constante c donnée par le théorème 3.4.2.

Théorème 3.4.3. *Il existe une constante absolue C, telle que pour toute algèbre de quaternions sur $\mathbb{Q}$ indéfinie B_D, de discriminant D et pour tout corps quadratique imaginaire $K = \mathbb{Q}[\sqrt{-d}]$, où d est un entier sans facteurs carré, pour toute surface abélienne $A/\mathbb{Q}$, telle que $\mathrm{End}_K(A) \simeq O_D$ un ordre maximal de B_D et pour tout nombre premier $N \geq C(\mathrm{ppcm}(D, d))^{22}$, la surface A n'admet pas d'isogénie O_D-cyclique de noyau $\simeq \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$.*

Démonstration. Il suffit de prouver l'existence d'un nombre premier ℓ tel que

$$\ell \leq c(24\,\mathrm{ppcm}(D, d))^{5.5},$$

où c est la constante donnée par le théorème 3.4.2, tel que ℓ satisfait aux conditions du lemme 3.4.1 :

- ℓ est décomposé ou ramifié dans K ;
- il existe un nombre premier $p \mid D$ décomposé dans $\mathbb{Q}(\sqrt{-\ell})$;
- $\ell > 3$.

En effet supposons qu'un tel nombre premier existe, soit $C = \max\{4^8((24c)^{5.5})^4, 10^{84.1}\}$. Pour tout nombre premier $N \geq C(\mathrm{ppcm}(D, d))^{22}$, on a $N \geq \max\{4^8\ell^4, 10^{84.1}\}$ donc on peut appliquer le lemme 3.4.1, il n'existe pas de surface abélienne $A/\mathbb{Q}$, telle que $\mathrm{End}_K(A) \simeq O_D$ un ordre maximal de B_D qui admet de structure de niveau $\Gamma_0(N)$.

Prouvons l'existence d'un tel nombre premier ℓ. Soit $d \in \mathbb{N}$ sans facteurs carrés, tel que $K = \mathbb{Q}(\sqrt{-d})$. Il existe p_1 et p_2 deux nombres premiers distincts divisant D tels qu'une au moins des trois hypothèses suivantes est satisfaite :

(1) $p_1 \nmid d$ et $p_1 \neq 2$.

(2) $p_1 \nmid d$ et $p_1 = 2$ et $d \neq 1$.

(3) $p_1 \mid d$ et $p_2 \mid d$ et $p_2 \neq 2$.

On suppose d'abord qu'on est dans le cas (1). D'après le théorème 3.4.2, il existe un nombre premier $\ell \leq c(3 * 4dp_1)^{5.5} \leq c(24 \operatorname{ppcm}(D, d))^{5.5}$ tel que :

$$\begin{cases} \left(\frac{-\ell}{p_1}\right) = 1, \\ \left(\frac{-d}{\ell}\right) = 1, \\ \ell \neq 3. \end{cases}$$

Si on est dans le cas (2), d'après le théorème 3.4.2, il existe un nombre premier ℓ, tel que $\ell \leq c(3 * 8d)^{5.5} \leq (3 * 8 \operatorname{ppcm}(D, d))^{5.5}$ et :

$$\begin{cases} \ell \equiv -1 \mod 8, \\ \left(\frac{-d}{\ell}\right) = 1, \\ \ell \neq 3. \end{cases}$$

Dans ces deux cas (1) et (2), pour un tel nombre premier $\ell > 3$, on a ℓ décomposé dans $K = \mathbb{Q}(\sqrt{-d})$ et p_1 est décomposé dans $\mathbb{Q}(\sqrt{-\ell})$.

Si on est dans le cas (3), d'après le théorème 3.4.2, il existe un nombre premier ℓ, tel que $\ell \leq c(3 * 8d) \leq (24 \operatorname{ppcm}(D, d))^{5.5}$ et :

$$\begin{cases} \ell \equiv -1 \mod 8, \\ \left(\frac{-\ell}{p_1}\right) = 1 \text{ si } p_1 \neq 2, \\ \left(\frac{p_2}{\ell}\right) = -1, \\ \left(\frac{p}{\ell}\right) = 1 \text{ pour tout nombre premier } p \mid d, p \nmid 2p_1p_2, \\ \ell \neq 3. \end{cases}$$

D'après les deux premières conditions, p_1 est décomposé dans $\mathbb{Q}(\sqrt{-\ell})$ (qu'il soit égal à 2 ou non). En outre, on a en utilisant la loi de réciprocité quadratique :

$$\left(\frac{-p_1}{\ell}\right) = -(-1)^{\frac{(p_1-1)(\ell-1)}{4}}(-1)^{\frac{p_1-1}{2}}\left(\frac{-\ell}{p_1}\right).$$

Or comme $\ell \equiv -1 \mod 8$, les entiers $\frac{(p_1-1)(\ell-1)}{4}$ et $\frac{p_1-1}{2}$ ont la même parité, donc : $\left(\frac{-p_1}{\ell}\right) = -\left(\frac{-\ell}{p_1}\right) = -1$. Par hypothèse $\left(\frac{p_2}{\ell}\right) = -1$ et $\left(\frac{2}{\ell}\right) = 1$ et $\left(\frac{p}{\ell}\right) = 1$ pour tout nombre premier $p \nmid 2p_1p_2$. Finalement $\left(\frac{-d}{\ell}\right) = 1$. On en déduit que ℓ est décomposé dans $K = \mathbb{Q}(\sqrt{-d})$.

□

Lorsque l'anneau d'endomorphismes $\mathrm{End}_{\mathbb{Q}}(A)$ est l'anneau des entiers d'un corps de nombre $E = \mathbb{Q}(\sqrt{m})$, rappellons que d'après [24, Thm 3.1] on a $m = D$ ou $m = D/p$ pour un certain nombre premier p. Dans le cas $m \neq D, D/2$, d'après le théorème 3.4.4 ci-dessous le corps de nombre K où A acquiert tous ses endomorphismes peut prendre un nombre fini de valeurs, ce qui permet de supprimer la dépendance de la borne M du théorème 3.1.3 en le corps K.

Théorème 3.4.4. *Soit D le discriminant d'une algèbre de quaternions indéfinie B_D et $m \mid D$ un entier positif, tels que $D = pm$ avec p un nombre premier impair. Soit K un corps quadratique imaginaire. S'il existe $A/\mathbb{Q}$ une variété abélienne telle que $\mathrm{End}_K(A)$ est un ordre maximal de B_D et $\mathrm{End}_{\mathbb{Q}}(A)$ est l'anneau des entiers de $\mathbb{Q}(\sqrt{m})$, alors K est non ramifié en dehors de D.*

Démonstration. L'énoncé de ce théorème paraît dans [23, thm 1.1]. Pour une preuve de ce théorème, consulter [34, Prop. 7.8], en remarquant que la condition supplémentaire $p \equiv 3 \mod 4$ qui apparaît dans cette dernière proposition est toujours satisfaites sous les hypothèses du présent théorème 3.4.4 d'après [23, cor 3.7].

□

Corollaire 3.4.5. *Soit C la constante donnée par le théorème 3.1.3. Soient B_D une algèbre de quaternions sur $\mathbb{Q}$ indéfinie, de discriminant D, et O_D un ordre maximal de B_D. Soit $E = \mathbb{Q}(\sqrt{m})$ un corps quadratique totalement réel. On suppose qu'il existe un nombre premier impair $p \mid D$ et $p \nmid m$. Alors pour toute surface abélienne $A/\mathbb{Q}$ telle que $\mathrm{End}_{\overline{\mathbb{Q}}}(A) \simeq O_D$, et $\mathrm{End}_{\mathbb{Q}}(A) \simeq R_E$ soit l'anneau des entiers de E, pour tout nombre premier $N \geq CD^{22}$, la surface A n'admet pas d'isogénie O_D-cyclique de noyau $\simeq \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$.*

Démonstration. D'après le théorème 3.4.4, le corps K sur lequel tous les endomorphismes de $A/\overline{\mathbb{Q}}$ sont définis est non ramifié en dehors de D. Donc K est de la forme $\mathbb{Q}(\sqrt{-d})$ avec d un entier sans facteur carré divisant D. D'après le théorème 3.1.3 pour tout nombre premier $N \geq C\,\mathrm{ppcm}(d, D)^{22} = CD^{22}$, la surface A n'admet pas d'isogénie O_D-cyclique de noyau $\simeq \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$. □

Bibliographie

[1] S. Bosch, W. Lütkebohmert, M. Raynaud, *Néron Models* Springer, Ergeb. Math. Grenz. **21** (1990).

[2] N. Bruin, E.V. Flynn, J. González, V. Rotger, *On finiteness conjecture for modular quaternion algebras.* Math. Proc. Camb. Phil. Soc. **141**(3), 383-408 (2006).

[3] P. Clark, *Local and global points on moduli spaces of potentially quaternionic abelian surfaces.* Ph.D. Thesis, Harvard University, (2003). Available at http ://math.uga.edu/ pete/thesis.pdf

[4] P. Deligne, M. Rapoport, *Les schémas de modules de courbes elliptiques.*Proc. Int. Summer School on modular functions. Antwerp 1972, vol II, Springer, LMNO **349** (1973).

[5] B. Edixhoven *On Néron models, divisors and modular curves.* J. Ramanujan Math. Soc. **13**(2), pp. 157-194 (1998).

[6] B. Gross, *Heights and the special values of L-séries.* Canadian Math. Soc. Conference Proceedings 7, Am. Math. Soc., Providence, pp. 115-187 (1987).

[7] A. Grothendieck, M. Raynaud, D. Rim, *Groupes de monodromie en géométrie algébrique (SGA7-I).* Springer, Lecture Notes in Math. **288**, (1972).

[8] H. Iwaniec and E. Kowalski, *Analytic Number Theory.* Colloquium Publications **53**, (2004).

[9] B. Jordan *Points on Shimura curves rationals over number fields.* J. Reine Angew. Math. **371** (1986), pp 92-114.

[10] C. Khare, J.-P. Wintenberger *On Serre's conjecture for 2-dimensional mod p representations of the absolute Galois group of the rationals* à paraître dans Annals of Math.

[11] W. Luo, D. Ramakrishnan, *Determination of modular forms by twists of critical L-values.* Invent. Math. **130** pp. 371-398 (1997).

[12] B. Mazur *Rational isogenies of prime degree.* Invent. Math. **44** (1978), no. 2, pp. 129-162.

[13] S. Molina, *Specialisation of Heegner points and applications.* Ph.D. Thesis, Universitat Politècnica de Catalunya, (2010).

[14] A. P. Ogg, *Mauvaise réduction des courbes de Shimura*

[15] M. Ohta *On ℓ-adic representations of Galois groups obtained from certain two-dimensional abelian varieties.* J. Fac. Sci. Univ. Tokyo Sect. IA Math. **21** (1974), pp. 299-308

[16] P. Parent, *Towards the triviality of $X_0^+(p^r)(\mathbb{Q})$ for $r > 1$.* Compositio Math. **141**(3), pp. 561-572 (2005)

[17] P. Parent, A. Yafaev, *Proving the triviality of rational points on Atkin-Lehner quotients of Shimura curves.* Math. Ann. **339** pp. 915-935 (2007).

[18] M. Raynaud, *Schémas en groupes de type (p,...,p).* Bull. Soc. Math. France **102** (1974), pp. 241-280.

[19] K. A. Ribet, *Endomorphism algebras of abelian varieties attached to newforms of weight 2.* Progress in Math. **12**, pp. 263-276 (1981).

[20] K. A. Ribet, *On l-adic representations attached to modular forms. II* Glasgow Math. J. 27 (1985), pp. 185–194.

[21] K. Ribet, *On modular representations of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *arising from modular forms.* Invent. Math. **100**, pp. 431-476 (1990).

[22] K. A. Ribet, *Abelian varieties over Q and modular forms.* in Modular curves and abelian varieties, J. Cremona, J.-C. Lario, J. Quer, K. Ribet (eds.), Progress in Mathematics **224**, Birkhäuser (2004), pp. 241-261.

[23] V. Rotger, *Which quaternion algebras act on a modular abelian variety ?* Mathematical Research Letters **15** (2008), pp. 251-263.

[24] V. Rotger, A. Skorobogatov, A. Yafaev, *Failure of the Hasse principle for Atkin-Lehner quotients of Shimura curves over* $\mathbb{Q}$. Moscow Math. J. **5**(2) (2005), pp 463-476.

[25] J.-P. Serre, *Propriétés galoisiennes des points d'ordre finis des courbes elliptiques.* Invent. Math. **15** (1972), pp. 259-331.

[26] J.-P. Serre, *Sur les représentations modulaires de degré 2 de* $\mathrm{Gal}\,\overline{\mathbb{Q}}/\mathbb{Q}$. Duke Math. J. **54**, no. 1 (1987), 179-230.

[27] J.-P. Serre, J. Tate, *Good reduction of abelian varieties.* Ann. Math. **88** (1968), 492-517.

[28] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions* Kanô Memorial Lectures, No. 1. Publications of the Mathematical Society of Japan, No. 11. Iwanami Shoten Publishers, Tokyo, Princeton University Press, Princeton, NJ, pp. xiv+267 (1971).

[29] J. H. Silverman, *The Arithmetic of Elliptic Curves.* Springer-Verlag, GTM **106**, (1992).

[30] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves.* Springer-Verlag, GTM **151**, (1994).

[31] A. Skorobogatov *Shimura coverings of Shimura curves and the Manin obstruction* Math. Res. Lett. 12 (2005), **5-6**, pp 779-788

[32] J. Tate, *Endomorphisms of abelian varieties over finite fields* Invent. Math. **2** (1966) pp. 134-144.

[33] J. Tate, *Classes d'isogénie des variétés abéliennes sur un corps fini*, Séminaire Bourbaki **352** (1968-69), pp 95-110.

[34] C. de Vera *Rational points on Atkin-Lehner quotients of Shimura curves* MSc Thesis, Universitat Politècnica de Catalunya, (2011). Available at http ://www-ma2.upc.edu/vrotger/docs/students/deVeraMSc.pdf

[35] M.-F. Vignéras, *Arithmétique des Algèbres de Quaternions.* Lecture Note in Math **800**, (1980).

Résumé

Dans cette thèse nous étudions deux problèmes. Le premier est la non-existence de points rationnels non spéciaux sur des quotients d'Atkin-Lehner de courbes de Shimura. Le second est l'absence de surfaces abéliennes rationnelles à multiplication potentiellement quaternioniques munies d'une structure de niveau. Ces deux problèmes sont liés car une surface abélienne rationnelle simple à multiplication potentiellement quaternionique correspond à un point rationnel non spécial sur un certain quotient d'Atkin-Lehner de courbe de Shimura.

Dans une première partie nous expliquons comment vérifier un critère de Parent et Yafaev en grande généralité pour prouver que dans les conditions du cas non ramifié de Ogg, et si p est assez grand par rapport à q, alors le quotient X^{pq}/w_q n'a pas de point rationnel non spécial.

Dans une seconde partie nous determinons une borne effective pour les structures de niveaux possibles pour une surface abélienne rationnelle acquérant sur un corps quadratique imaginaire fixé multiplication par un ordre fixé dans une algèbre de quaternion.

Mots clefs : Courbes de Shimura, surfaces abéliennes

Abstract

In this thesis we study two problems. The first one is the non-existence of rational non-specila points on Atkin-Lehner quotients of Shimura curves. The second one is the absence of rational abelian surfaces with potential quaternionique multiplication endowed with a level structure. These two problems are linked because a simple rational abelian surface with potential quaternionique multiplication is associated to a rational non-special point on an Atkin-Lehner quotients of Shimura curve.

In a first part of our work we explain how to verify in wide generality a criterium of Parent and Yafaev in order to prove that in the conditions of Ogg's non ramified case, and if p is big enough compared two q, then the quotient X^{pq}/w_q has no non-special rational point.

In a second part we determine an effective born for possible level structures on rational abelian surfaces having, over a fixed quadratic field, multiplication by a fixed order in a quaternion algebra.

Key words : Shimura curves, abelian surfaces.