N° d'ordre :02/2010-D/MT

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université des Sciences et de la Technologie
Houari Boumedienne

Faculté de Mathématiques

THÈSE

Présentée pour l'obtention du diplôme de DOCTORAT

En : **MATHEMATIQUES**

Spécialité : **Algèbre et Théorie des Nombres**

Par **BAAZIZ Houria**

Thème

Sur l'Arithmétique des Courbes de Genre Un et Deux

soutenue publiquement le 14/03/2010 devant le jury composé de :

Mr. B. BENZAGHOU	Professeur, USTHB	*Président*
Mr. J. BOXALL	Professeur, U.Caen	*Directeur de thèse*
Mr. M. AIDER	Professeur, USTHB	*Examinateur*
Mr. N. M. BENKAFADAR	Professeur, U.Constantine	*Examinateur*
Mr. M.O. HERNANE	Maître de Conférences, USTHB	*Examinateur*
Mme. O. LECACHEUX	Maître de Conférences, Paris VI	*Examinatrice*
Mr. M. ZITOUNI	Professeur, USTHB	*Examinateur*

Remerciements

J'aimerais exprimer mes sincères remerciements à mon directeur de thèse le professeur John BOXALL de m'avoir encadrée et initiée à la recherche pour sa disponibilité, sa patience, sa rigueur et son esprit critique.

Je suis trés reconnaissante au professeur Mohamed ZITOUNI qui m'a guidé tout au long de ma thèse et a accepté d'être membre du jury.

Ma gratitude au professeur Benali BENZAGHOU d'avoir accepté d'être le pésident du jury.

Je remercie vivement, d'avoir accepter d'être membres du jury :

les professeurs Meziane AIDER (USTHB), N. Mohamed BENKAFADAR (Université de Constantine),

M. Ouamer HERNANE, Maître de Conférences (USTHB) et

Odile LECACHEUX, Maître de Conférences (Université Paris VI).

Je remercie le laboratoire de mathématiques NICOLAS ORESME de l'université de Caen pour l'aide et les facilités qui m'ont permis de réaliser cette thèse.

Je remercie mes parents, mes frères et soeurs pour leurs encouragements durant l'élaboration de cette thèse.

Table des matières

Introduction

Cette thèse est consacrée à l'étude de quelques propriétés des courbes modulaires, des courbes elliptiques et des courbes de genre deux. Elle est divisée en 3 chapitres. Le premier regroupe quelques définitions et notions de base qui seront utilisées par la suite.

Le but du chapitre 2 est de présenter un nouvel algorithme pour obtenir des équations de la courbe modulaire $X_1(N)$ dont les points paramètrent les classes d'isomorphismes des couples (E, P) où E est une courbe elliptique et P est un point d'ordre N de E.

Soit $N \geq 2$ un entier naturel et K un corps de caractéristique première à N. Les points K-rationnels de la courbe modulaire $X_1(N)$ (dépourvue de ses pointes) paramètrent les classes de K-isomorphismes des couples (E, P) où E est une courbe elliptique et P est un point de torsion d'ordre N de E. Deux tels couples (E, P) et (E', P') sont isomorphes s'il existe un isomorphisme $\phi : E \to E'$ tel que $\phi(P) = P'$. Reichert [27] a calculé des équations pour $X_1(N)$ lorsque $N = 11$ et $13 \leq N \leq 18$. Lecacheux [17] et Washington [35] ont déterminé des équations pour $X_1(13)$ et $X_1(16)$, liées à la construction des familles d'extensions cycliques de $\mathbb{Q}$. Dans [8], Darmon a étudié $X_1(25)$. Leurs méthodes ne se généralisent pas à une valeur arbitraire de N. Ishida et Ishii [13] ont développé des méthodes pour trouver des équations de $X_1(N)$ pour N arbitraire en construisant explicitement deux fonctions modulaires qui engendrent le corps de fonctions de $X_1(N)$, ils donnent une liste des équations obtenues lorsque $N \leq 20$. Yang [37] donne une méthode pour construire des générateurs du corps de fonctions en utilisant des produits construits à partir de la fonction eta de Dedekind généralisée. Dans son papier, Yang obtient des modèles explicites de $X_1(N)$ lorsque $N = 1$ et $13 \leq N \leq 22$. À l'exception de Reichert, ces auteurs ne montrent pas comment retrouver un modèle explicite du couple (E, P) à partir du point correspondant sur leurs modèles de $X_1(N)$.

Nous nous proposons de présenter un nouvel algorithme pour obtenir des équations de $X_1(N)$ qui nous permettent en même temps de déterminer explicitement le couple correspondant (E, P). Pour cela, nous utilisons les polynômes de division pour caractériser les courbes elliptiques d'équation

$$(E) \qquad y^2 + (a_1x + a_3)y = x^3 + a_2x^2$$

sur lesquelles le point $(0, 0)$ de (E) est de torsion d'ordre donné $N \geq 4$. Ces polynômes de N-division peuvent être calculés rapidement par récurrence. Nous constatons alors que ces polynômes de division sont divisibles par des grandes puissances de a_3. Ce coefficient a_3 est aussi un facteur du discriminant de la courbe elliptique (E).

Chaque courbe elliptique (E) est isomorphe à une courbe elliptique d'équation

$$y^2 + ((1+g)x + f)y = x^3 + fx^2$$

via un isomorphisme qui applique $(0,0)$ sur $(0,0)$. Lorsque le point $(0,0)$ est d'ordre N, les coefficients f et g sont des formes modulaires sur le groupe modulaire $\Gamma_1(N)$. Nous montrons qu'ils engendrent le corps de fonctions $\mathbb{C}(X_1(N))$ sur $X_1(N)$. En simplifiant les polynômes de division nous obtenons une première équation $\Phi_N^{(f,g)}(f,g) = 0$ de $X_1(N)$. Le degré de cette équation est nettement plus grand que celui des équations obtenues par les auteurs précédents. Dans § 2.4, nous définissons, en termes de f et g, deux autres couples de fonctions modulaires $\{s,t\}$ et $\{q,r\}$ sur $\Gamma_1(N)$, chaque couple étant un système de générateurs de $\mathbb{C}(X_1(N))$, il en résulte une équation de plus petit degré. La Table 2.1 permet de comparer les équations obtenues pour $N \leq 15$. Le couple $\{q,r\}$ donne le meilleur résultat. Nos équations sont de degré plus petit que celle de [13] et [37] en les deux variables individuellement, mais de degré total un peu plus grand. Il est intéressant de calculer des équations qui sont de petit degré en une des deux fonctions, ce qui donne une meilleure borne supérieure pour la gonalité de la courbe (voir la fin de § 2.5).

Nous avons calculé les équations de $X_1(N)$ pour tout $N \leq 51$. Lorsque N approche 50, chacune des équations obtenue occupe une page environs. Si $N = 50$, l'équation en termes de q et r est de degré 23 en r et 32 en q et de degré total 48 (Table 2.3). La valeur absolue du plus grand coefficient est 109037417. La Table 2.2 présente quelques équations particulières de $X_1(N)$ pour $11 \leq N \leq 20$ et exprime les fonctions u et v utilisées en fonction de s et t. Notons que tous ces résultats sont présentés dans le chapitre 2.

Présentons maintenant le contenu du chapitre 3. Soit C est une courbe projective lisse ou une variété abélienne sur un corps de nombres K et $\mathfrak{p}$ est un idéal premier de K. La courbe C a bonne réduction tordue en $\mathfrak{p}$ s'il existe une tordue de C qui a bonne réduction en $\mathfrak{p}$. Dans le § 3.2, nous développons quelques propriétés simples de la bonne réduction tordue. En particulier, nous montrons qu'il n'existe pas de courbes elliptiques sur $\mathbb{Q}$ ayant bonne réduction tordue partout et que si K est un corps de nombres et si Σ est un ensemble fini de nombres premiers de K, alors il n'existe qu'un nombre fini d'invariants modulaires $j \in K$ de courbes elliptiques ayant bonne réduction tordue partout en tout premier n'appartenant pas à Σ. Dans le § 3.6, nous construisons deux familles de courbes de genre deux C_w où $w = -107$ ou -109, à bonne réduction partout sur des corps quartiques et à bonne réduction tordue partout sur des corps quadratiques. Dans le § 3.3, nous étudions brièvement la courbe C_w où w est une indéterminée.

En particulier, nous montrons que la jacobienne J_w de C_w est isogène au produit de deux courbes elliptiques sur une extension cubique de $\mathbb{Q}(w)$. Dans le § 3.4. Nous étudions les courbes de genre deux obtenues de la courbe (3.5) spécialisée en $w^2 = -107$ et nous donnons une première construction qui est une démonstration du Theorème 3.1.

La partie § 3.5 est consacrée à une étude similaire de C_w spécialisée en $w^2 = -109$. Finalement, dans le § 3.6, nous expliquons brièvement comment nous avons découvert la famille (3.2) et nous montrons comment, en appliquant une stratégie similaire aux courbes elliptiques, nous avons retrouvé des courbes elliptiques de Setzer ayant bonne réduction partout sur des corps quadratiques imaginaires.

Chapitre 1

Courbes modulaires, courbes elliptiques et hyperelliptiques.

Nous examinons les fonctions, les formes et les courbes modulaires. Dans la suite N désigne un entier naturel.

1.1 Fonctions, formes et courbes modulaires.

Notons $\mathcal{H} = \{z \in \mathbb{C}, \Im(z) > 0\}$ le demi-plan supérieur de Poincaré et posons $\mathcal{H}^* = \mathcal{H} \cup \mathbb{Q} \cup \{\infty\}$.

Le groupe $SL_2(\mathbb{R})$ opère à gauche sur $\mathbb{C} \cup \{\infty\}$ par la transformation homographique

$$\gamma(z) = \frac{az+b}{cz+d}, \text{ où } z \in \mathbb{C} \cup \{\infty\} \quad \text{et} \quad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{R}),$$

$$\text{avec} \qquad \gamma(\frac{-d}{c}) = \infty \qquad \text{et} \qquad \gamma(\infty) = \begin{cases} \frac{a}{c}, & \text{si } c \neq 0 \\ \infty, & \text{si } c = 0. \end{cases}$$

Les matrices scalaires $I_2 = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$, $a \in \mathbb{R}^\times$ opèrent trivialement sur $\mathbb{C} \cup \{\infty\}$.

Définition 1.1. *1. Le groupe modulaire spécial linéaire des 2×2 matrices est égal à*

$$SL_2(\mathbb{Z}) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a,b,c,d \in \mathbb{Z},\ ad-bc=1\}$$

2. Le groupe spécial linéaire projectif $PSL_2(\mathbb{Z}) = SL_2(\mathbb{Z})/\{\pm I_2\}$.

3. Le sous groupe de congruence principal de niveau N de $SL_2(\mathbb{Z})$ est égal à

$$\Gamma(N) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \mid b \equiv c \equiv 0 \pmod N, a \equiv d \equiv 1 \pmod N\}.$$

Définition 1.2. *un sous-groupe de congruence de niveau N est un sous-groupe contenant $\Gamma(N)$ pour un entier N. Le plus petit entier N est le niveau du sous-groupe. Les sous groupes $\Gamma_0(N)$, $\Gamma_1(N)$ de $SL_2(\mathbb{Z})$, sont égaux à*

$$\Gamma_0(N) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \mid c \equiv 0 \pmod N\},$$
$$\Gamma_1(N) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \mid c \equiv 0 \pmod N,\ a \equiv d \equiv 1 \pmod N\}.$$

L'action par homographies d'un sous-groupe de $SL_2(\mathbb{Z})$ stabilise $\mathcal{H}^*$. Ces sous groupes vérifient la relation

$$\Gamma(N) \subseteq \Gamma_1(N) \subset \Gamma_0(N) \subset SL_2(\mathbb{Z}).$$

et une suite exacte

$$1 \longrightarrow \Gamma(N) \longrightarrow SL_2(\mathbb{Z}) \longrightarrow SL_2(\mathbb{Z}/N\mathbb{Z}) \longrightarrow 1.$$

Définition 1.3. *Une fonction elliptique est une fonction méromorphe sur $\mathbb{C}$, invariante par translation par un réseau Ω.*

Les fonctions elliptiques sont définies sur le tore complexe $\mathbb{C}/\Omega$ et permettent de paramétrer les courbes elliptiques définies sur $\mathbb{C}$. Citons la fonction de Weierstrass associée à un réseau Ω

$$\wp(z,\Omega) = \frac{1}{z^2} + \sum_{\substack{\omega\in\Omega \\ \omega\neq 0}} \Big(\frac{1}{(z-\omega)^2} + \frac{1}{\omega^2}\Big). \tag{1.1}$$

Théorème 1.1. *Le corps des fonctions elliptiques associées à un réseau Ω est engendré par $\wp(z,\Omega)$ et sa dérivée $\wp'(z,\Omega)$.*

Preuve. Les singularités de $\wp(z,\Omega)$ sont les points doubles aux points de Ω. Pour plus de détails, cf [7], Théorème 10.2. [30] Proposition 1.38 et Proposition 1.39. □

Définition 1.4. *Soit une matrice* $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{R})$*, alors un point* $z \in \mathbb{C} \cup \{\infty\}$ *est un point fixe pour* γ *s'il vérifie la relation* $\gamma(z) = z$*. La matrice* $\gamma \neq \pm I_2$ *est*

1. *Elliptique si elle admet deux points fixes qui sont des conjugués complexes.*
2. *Hyperbolique si elle admet deux points fixes réels.*
3. *Parabolique si elle admet un seul point fixe.*

Définition 1.5. *Soit* $\tilde{\Gamma}$ *un sous-groupe de congruence de* $PSL_2(\mathbb{Z})$*.*

1. *Une pointe de* $\tilde{\Gamma}$ *est un point fixé par une transformation parabolique de* $\tilde{\Gamma}$*.*
2. *Un élément de* $\mathcal{H}$ *est elliptique d'ordre* 2 *(respectivement d'ordre* 3*) s'il est fixé par une transformation elliptique d'ordre* 2 *(respectivement d'ordre* 3*) de* $\tilde{\Gamma}$*.*

Notons que les pointes de $\tilde{\Gamma}$ appartiennent à $\mathbb{Q} \cup \{\infty\}$. Elles forment un nombre fini d'orbites sous $PSL_2(\mathbb{Z})$ puisque les sous groupes de congruences sont d'indice fini et l'opération de $PSL_2(\mathbb{Z})$ sur $\mathbb{Q} \cup \{\infty\}$ est transitive.

Définition 1.6. *Une fonction modulaire* $f : \mathcal{H} \mapsto \mathbb{C}$ *par rapport à* Γ *est une fonction méromorphe qui satisfait aux conditions :*

1. $f(\gamma(z)) = f(z)$ *pour toute matrice* $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$*.*
2. *Pour toute matrice* $\gamma \in SL_2(\mathbb{Z})$*, il existe un entier* $\ell \geq 1$ *tel que* $f \circ \gamma$ *admet un développement en série de Fourier de la forme*

$$f(\gamma(z)) = \sum_{n=m}^{\infty} c(n) q^{n/\ell} \quad \text{où} \quad q = exp(2\pi i z).$$

Définition 1.7. *Soit un entier pair $2k$ où $k \in \mathbb{Z}$. Une forme modulaire $f : \mathcal{H} \mapsto \mathbb{C}$ de poids $2k$ sur Γ est une fonction holomorphe sur $\mathcal{H}$ qui satisfait aux conditions :*

1. *$f(\gamma(z)) = (cz+d)^{2k} f(z)$ pour tout $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$.*
2. *Pour tout $\gamma \in SL_2(\mathbb{Z})$, il existe un entier $\ell \geq 1$ tel que $f \circ \gamma$ admet un développement en série de Fourier de la forme*

$$f(\gamma(z)) = \sum_{n=0}^{\infty} c(n) q^{n/\ell} \text{ où } q = exp(2\pi i z).$$

3. *La forme modulaire f est parabolique si elle s'annule en toutes les pointes, alors $c(0) = 0$.*

Soit Γ un sous-groupe de congruence de $SL_2(\mathbb{Z})$. La courbe modulaire X_Γ est alors définie comme le quotient du demi-plan de Poincaré complété $\mathcal{H}^*$ par l'action du groupe Γ. Ce quotient peut être muni de la structure d'une surface de Riemann compacte connexe, et donc d'une courbe projective lisse.

Théorème 1.2. *Le genre g de X_Γ est égal à*

$$g = 1 + \frac{\nu}{12} - \frac{\nu_2}{4} - \frac{\nu_3}{3} - \frac{\nu_\infty}{2}$$

où ν est l'indice de $\tilde{\Gamma}$ dans $PSL_2(\mathbb{Z})$.
ν_2 est le nombre de points elliptiques d'ordre 2 de X_Γ,
ν_3 est le nombre de points elliptiques d'ordre 3 de X_Γ,
ν_∞ est le nombre de pointes de X_Γ.

Preuve. Cf [30] p.25. □

Exemple 1.1. Considérons le cas où $N = 50$, alors $\nu = 900$. Le sous groupe $\Gamma_1(50)$ n'a aucun point elliptique et possède 56 pointes. D'après le Théorème 1.2, le genre de $X_1(50)$ est donné par la formule $1 + \frac{900}{12} - \frac{0}{4} - \frac{0}{3} - \frac{56}{2} = 48$ comme indiqué dans la Table 2.3 (page 50).

Dans le Chapitre 1, nous considérons le sous groupe $\Gamma = \Gamma_1(N)$ et la courbe $X_1(N)$. Notons par $Y_1(N)$ le quotient de $\mathcal{H}$ par $\Gamma_1(N)$, il s'agit alors de l'ouvert de $X_1(N)$ obtenu en enlevant les pointes. La courbe $X_1(N)$ classifie les couples de courbes elliptiques munies d'un point de torsion d'ordre N, à isomorphismes près.

1.2 Réductions des courbes elliptiques.

Soit K un corps commutatif et soit K^{alg} une clôture algébrique de K.

Définition 1.8. *Une courbe elliptique E/K est une courbe algébrique, plane, irréductible, projective, lisse, de genre* 1*, munie d'un point O_E rationnel sur K.*

Toute courbe elliptique est représentée dans le plan projectif par une cubique plane d'équation de Weierstrass

$$E: \quad Y^2Z+(a_1x+a_3)YZ = X^3+a_2X^2Z+a_4XZ^2+a_6Z^3 \in K[X,Y,Z] \quad (1.2)$$

Cette courbe intersecte la droite à l'infini $Z=0$ en un unique point dont les coordonnées projectives sont $(0,1,0)$, qui est rationnel sur K. Prennons alors pour O_E le point $(0,1,0)$. En substituant $x=X/Z$, $y=Y/Z$, nous obtenons le modèle affine de E

$$E_1: \quad y^2+(a_1x+a_3)y = x^3+a_2x^2+a_4x+a_6 \in K[x,y]. \quad (1.3)$$

Posons $F(x,y) = y^2+(a_1x+a_3)y - x^3 - a_2x^2 - a_4x - a_6$.

Lorsque la caractéristique $car(K) \neq 2$, la substitution

$$(x,y) \mapsto \big(x, (y-a_1x-a_3)/2\big) \quad (1.4)$$

transforme l'équation (1.3) en

$$E_3: \quad y^2 = 4x^3+b_2x^2+b_4x+b_6, \quad b_i \in \mathbb{Z}[a_1,a_2,a_3,a_4,a_6], \quad (1.5)$$

avec les coefficients

$$b_2 = a_1^2+4a_2, \quad b_4 = a_1a_3+2a_4, \quad b_6 = a_3^2+4a_6, \quad 4b_8 = b_2b_6-b_4^2. \quad (1.6)$$

Lorsque $car(K) \neq 2,\ 3$, la substitution $(x,y) \mapsto \big((x-3b_2)/36, y/108\big)$ transforme l'équation (1.5) en

$$y^2 = x^3 - 27c_4x - 216c_6, \quad c_4, c_6 \in \mathbb{Z}[b_2,b_4,b_6]. \quad (1.7)$$

$$\text{où} \quad c_4 = b_2^2-24b_4 \quad \text{et} \quad c_6 = -b_2^3+36b_2b_4-216b_6. \quad (1.8)$$

Le discriminant $\Delta(E)$ de E est égal à

$$\Delta(E) = -b_2^2b_8-8b_4^3-27b_6^2+9b_2b_4b_6 = (c_4^3-c_6^2)/1728, \quad \Delta(E) = 16\Delta_f. \quad (1.9)$$

où Δ_f est le discriminant du polynôme $x^3+a_2x^2+a_4x+a_6+\frac{1}{4}(a_1x+a_3)^2$.

La courbe (1.2) représente une courbe elliptique si et seulement si elle est lisse, une condition équivalente à $\Delta(E) \neq 0$.

L'invariant modulaire de E est égal à $j(E) = c_4^3/\Delta(E)$.

L'invariant différentiel est égal à

$$\omega(E) = \frac{dx}{2y + a_1x + a_3} = -\frac{dy}{a_1y - 3x^2 - 2a_2x - a_4} \tag{1.10}$$

Il est obtenu de la forme différentielle $df = f'_x dx + f'_y dy$.

Soit K un corps de caractéristique différente de 2 et 3. L'équation d'une courbe elliptique E/K peut se mettre sous la forme de Legendre

$$E : y^2 = x(x-1)(x-\lambda), \quad \lambda \neq 0, 1.$$

L'invariant modulaire $j(E)$ de E et le paramètre λ sont liés par la relation

$$2^8\big(1 - \lambda(1-\lambda)\big)^3 - j(E)\lambda^2(1-\lambda)^2 = 0$$

Pour plus de détails, voir [32], III.1.6.

Soit une cubique de Weierstrass projective, plane E/K d'équation (1.2).

Soit $F(X, Y, Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3$.

Une cubique plane singulière de genre 0 possède un seul point singulier, solution du système des équations algébriques :

$$\begin{aligned} F(X,Y,Z) &= 0, \quad \frac{\partial F}{\partial X}(X,Y,Z) = 0, \\ \frac{\partial F}{\partial Y}(X,Y,Z) &= 0, \quad \frac{\partial F}{\partial Z}(X,Y,Z) = 0. \end{aligned}$$

Proposition 1.1. *Soit une cubique plane E/K d'équation de Weierstrass (1.3) et de discriminant $\Delta(E)$. Alors E est non-singulière si et seulement si $\Delta(E) \neq 0$.*

Preuve. Cf [32] Chapitre III, Proposition 1.4 (i). □

Si une cubique E d'équation de Weierstrass est singulière, il existe deux possibilités pour le point singulier.

Proposition 1.2. *Soit une cubique plane E d'équation de Weierstrass (1.3) et de discriminant $\Delta(E) = 0$ et d'invariant c_4. Alors*

1. *E possède un point double si et seulement si $c_4 \neq 0$.*
2. *E possède un point de rebroussement si et seulement si $c_4 = 0$.*

Preuve. Cf [32], Chap III, Proposition 1.4. □

Soit E une courbe elliptique sur un corps de nombres K, munie du point K-rationnel $O_E = (\infty, \infty) = (0, 1, 0)$. Il existe une structure de groupe commutative sur $E(K)$ dont les lois (composition et symétrie) sont données par des fonctions algébriques à coefficients dans K. Cette loi a une interprétation géométrique qui se résume par la formule « trois points colinéaires ont une somme nulle ». Prenons une équation de Weierstrass de E

$$E : y^2 + (a_1x + a_3)y = x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in K, \qquad O_E = (0, 1, 0).$$

Soient $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ deux points de E tels que P_1, $P_2 \neq O_E$. Les coordonnées de la somme $P_1 + P_2 = P_3 = (x_3, y_3)$ sont définis par

(1) Si $x_1 \neq x_2$

$$x_3 = m^2 + a_1m - a_2 - x_1 - x_2,$$
$$y_3 = -m^3 - a_1m^2 + (a_2 - a_1^2 + 2x_1 + x_2)m + a_1(a_2 + x_1 + x_2) - a_3 - y_1,$$
$$\text{où } m = \frac{y_2 - y_1}{x_2 - x_1}.$$

(2) Si $x_1 = x_2$ et si $2y_1 + a_1x_1 + a_3 \neq 0$

$$x_3 = m^2 + a_1m - a_2 - 2x_1,$$
$$y_3 = -m^3 - 2a_1m^2 + (a_2 - a_1^2 + 3x_1)m + a_1(a_2 + 2x_1) - a_3 - y_1$$
$$\text{où } m = \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x + a_3}.$$

(3) Si $x_1 = x_2$ et si $2y_1 + a_1x_1 + a_3 = 0$, alors $y_2 = y_1$, $P_2 = P_1$ et $P_3 = O_E$.

La structure de l'ensemble $E(K)$ des points K-rationnels d'une courbe elliptique E définie sur un corps K est donnée par le théorème

Théorème 1.3. *Soit une courbe elliptique E/K. Alors l'ensemble $E(K)$ muni de la loi « trois points colinéaires ont une somme nulle » est un groupe abélien d'élément neutre le point à l'infini O_E.*

Preuve. Cf [32], chapitre VIII théorème 6.7. □

Le groupe $E(K)$ est appelé le groupe de Mordell-Weil de E/K.

Théorème 1.4 (Mordell-Weil)**.** *Soit K un corps de nombres et soit E/K une courbe elliptique. Alors le groupe $E(K)$ est un groupe abélien de type fini. Il est isomorphe au produit de groupes abéliens*

$$E(K) \simeq E_{tors}(K) \times \mathbb{Z}^r,$$

l'entier r est le rang de E/K et $E_{tors}(K)$ est le sous groupe de torsion du groupe $E(K)$.

Preuve. Cf [32]. □

Les points de torsion d'une courbe elliptique E/K sont définis par

Définition 1.9. *Soit E/K une courbe elliptique. Un point de n-torsion de E est un point $P \in E(K)$ tel que $nP = O_E$ où*

$$nP = \begin{cases} P + ... + P, & n \text{ fois } P \text{ si } n \text{ est un entier positif,} \\ -P - ... - P, & -n \text{ fois } -P \text{ si } n \text{ est un entier négatif,} \\ O_E, & \text{si } n = 0. \end{cases}$$

pour tout entier rationnel n premier à la caractéristique du corps K.

La structure du sous groupe de torsion d'une courbe elliptique sur $\mathbb{Q}$ est détérminée par le théorème

Théorème 1.5 (théorème de Mazur)**.** *Le groupe de torsion $E_{tors}(\mathbb{Q})$ d'une courbe elliptique $E/\mathbb{Q}$ est isomorphe aux 15 groupes abéliens additifs*

$$E_{tors}(\mathbb{Q}) = \begin{cases} \mathbb{Z}/d\mathbb{Z}, & \text{avec } 1 \leq d \leq 10 \quad \text{ou} \quad d = 12 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2d\mathbb{Z}, & \text{avec } 1 \leq d \leq 4. \end{cases}$$

Preuve. Cf [22]. □

Proposition 1.3. *Soient deux courbes elliptiques E/K et E'/K d'équations de Weierstrass*

$$\begin{aligned} E: \quad & y^2 + (a_1x + a_3)y = x^3 + a_2x^2 + a_4x + a_6 \quad \in K[x, y], \\ E': \quad & y^2 + (a'_1x + a'_3)y = x^3 + a'_2x^2 + a'_4x + a'_6 \quad \in K[x, y]. \end{aligned}$$

Soit $f : E(K) \longrightarrow E'(K)$ un homomorphisme. Alors il existe des nombres r, s, t, $u \in K$ et $u \neq 0$ tels que

$$f(x, y) = (u^2x + r, u^3y + u^2sx + t). \tag{1.11}$$

est un isomorphisme.

Preuve. Les invariants de E/K et E'/K sont liés par les formules

$$\begin{aligned}
&ua_1' = a_1 + 2s, \quad u^2a_2' = a_2 - sa_1 + 3r - s^2, \quad u^3a_3' = a_3 + ra_1 + 2t,\\
&u^4a_4' = a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st,\\
&u^6a_6' = a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1,\\
&u^2b_2' = b_2 + 12r, \quad u^4b_4' = b_4 + rb_2 + 6r^6,\\
&u^6b_6' = b_6 + 2rb_4 + r^2b_2 + 4r^3, \quad u^8b_8' = b_8 + 3rb_6 + 3r^2b_4 + r^3b_2 + 3r^4,\\
&u^4c_4' = c_4, \quad u^6c_6' = c_6, \quad u^{12}\Delta(E') = \Delta(E) \quad \text{et} \quad j(E') = j(E).
\end{aligned}$$

□

L'invariant modulaire permet de classifier les courbes elliptiques.

Proposition 1.4. *Soit K un corps et soit K^{alg} une clôture algébrique de K.*

1. *Deux courbes elliptiques définies sur K sont isomorphes sur K^{alg} si et seulement si leurs invariants modulaires sont égaux.*
2. *Tout nombre $\lambda \in K^{alg}$ est l'invariant modulaire d'une classe de courbes elliptiques définies sur $K(\lambda)$.*

Preuve. Cf [32] Chap III. Proposition 1.4. □

Définition 1.10. *Le conducteur d'une courbe elliptique E définie sur $\mathbb{Q}$ est un entier rationnel défini par*

$$N(E) = \prod_{p|\Delta(E)} p^{f_p}, \tag{1.12}$$

où l'entier $f_p = ord_p\big(\Delta(E)\big) + 1 - n_p$ et n_p est le nombre des composantes irréductible de la fibre spéciale du modèle minimal de Néron et $\Delta = \Delta(E)$ est le discriminant d'un modèle minimal de E.

Notons que $f_p = 0$ si et seulement si E a bonne réduction en p.
Lorsque $p \geq 5$,

$$f_p = \begin{cases} 1 & \text{lorsque } E \text{ a réduction multiplicative en } p,\\ 2 & \text{lorsque } E \text{ a réduction additive en } p. \end{cases} \tag{1.13}$$

Pour plus de détails et notamment les cas $p = 2$ et $p = 3$, cf [26].

Définition 1.11. *Soit K un corps commutatif et E/K, E'/K deux courbes elliptiques. Une isogénie de E/K vers E'/K est un homomorphisme surjectif non-nul de $E(K) \longrightarrow E'(K)$ de noyau fini.*

Définition 1.12. *Soit E/K, E'/K deux courbes elliptiques.*

1. *Le degré d'une isogénie $f : E(K) \longrightarrow E'(K)$ est l'ordre du noyau $Kerf = \{P \in E(K), f(P) = O_E\}$.*
2. *La relation « E isogène à E' » est une relation d'équivalence.*
3. *A une isogénie de courbes elliptiques $f : E \longrightarrow E'$ de degré n correspond une isogénie duale unique $\tilde{f} : E' \longrightarrow E$ de degré n de l'isogénie f.*
4. *L'isogénie $\tilde{f}$ satisfait les conditions : $\tilde{f} \circ f = n_E$ et $f \circ \tilde{f} = n_{E'}$ où n est la multiplication par n définie dans (1.9).*

Proposition 1.5. *Deux courbes elliptiques E et E' isogènes sur $\mathbb{Q}$ ont le même conducteur.*

Proposition 1.6. *Soit K un corps de nombres et une courbe elliptique E/K. Alors, il n'existe qu'un nombre fini de classes de K-isomorphismes de courbes elliptiques isogènes à E/K.*

Preuve. Cf [32], Chap IX. Corollaire 6.2. □

Soit K un corps muni d'une valuation discrète v et une courbe elliptique E/K d'équation de Weierstrass

$y^2 + (a_1x + a_3)y = x^3 + a_2x^2 + a_4x + a_6$ où $a_i \in K$ et de discriminant $\Delta(E)$.

La réduction de la courbe elliptique E modulo v est une cubique $\tilde{E}$ d'équation

$$\tilde{E} : y^2 + (\tilde{a_1}x + \tilde{a_3})y = x^3 + \tilde{a_2}x^2 + \tilde{a_4}x + \tilde{a_6},$$

où $\tilde{a_i}$ est la réduction modulo $\mathfrak{p}$ de a_i pour tout $i \in \{1, 2, 3, 4, 6\}$. Alors

$$v(a_i) \geq 0 \quad \text{pour} \quad i \in \{1, 2, 3, 4, 6\} \quad \text{et} \quad v\big(\Delta(E)\big) \geq 0.$$

La courbe réduite $\tilde{E}$ dépend de v.

Définition 1.13. *Soit E/K une cubique et v une valuation de K.*

1. *E a bonne réduction si $\tilde{E}$ est une courbe elliptique.*
2. *E a une réduction multiplicative en v si $\tilde{E}$ est singulière et le point singulier est un point double.*
3. *E a une réduction additive en v si $\tilde{E}$ est singulière et le point singulier est un point de rembroussement.*

Le type de réduction d'une courbe elliptique est déterminé par

Théorème 1.6. *Soit E/K une courbe elliptique d'équation de Weierstrass minimale $y^2+(a_1x+a_3)y = x^3+a_2x^2+a_4x+a_6, \quad a_i \in K$, de discriminant $\Delta(E)$ et d'invariant c_4. Alors*

1. *La courbe E a bonne réduction si et seulement si $v\big(\Delta(E)\big) = 0$.*
2. *La courbe E a réduction multiplicative si $\big(\Delta(E)\big) > 0$ et $v(c_4) = 0$.*
3. *La courbe E a réduction additive si $\big(\Delta(E)\big) > 0$ et $v(c_4) > 0$.*

Preuve. Cf [32], Chap VII, Proposition 5.1. □

Proposition 1.7. *Soit deux courbes elliptiques E/K et E'/K isogènes sur K. Alors E et E' ont le même type de réduction sur K.*

Preuve. Cf [32] Chapitre VII, Corollaire 7.2. □

Soit un corps K muni d'une valuation discrète v et $\mathcal{O}_K$ son anneau d'entiers.

Définition 1.14. *L'équation de Weierstrass (1.3) de la courbe elliptique E est minimale si les coefficients a_i, $i \in \{1,2,3,4,6\}$ appartiennent à $\mathcal{O}_K$ et $v(\Delta(E))$ est minimal parmi tous les modèles de Weierstrass de cette forme.*

Proposition 1.8. *Soit K un corps de valuation discrète.*

1. *Toute courbe elliptique sur K admet un modèle minimal de Weierstrass.*
2. *Le changement de variables*

$$(x,y) \mapsto (u^2x+r, u^3y+u^2sx+t) \text{ où } r,s,t,u \in K \text{ et } u \neq 0$$

transforme l'équation (1.3) en une équation d'invariants

$$\Delta = u^{12}\Delta'(E), \quad c_4 = u^4c_4' \quad \text{et} \quad c_6 = u^6c_6'.$$

3. *En particulier, tout modèle de Weierstrass peut être transformer en un modèle minimal par un changement de variables de cette forme.*

Preuve. Cf [32] Chapitre VII, Proposition 1.3. □

Il en résulte que l'équation de Weierstrass (1.3) est minimale si l'une des trois assertions suivantes est satisfaite :

1. $a_i \in \mathcal{O}_K$ pour tout $i \in \{1,2,3,4,6\}$ et $v\big(\Delta(E)\big) < 12$.
2. $a_i \in \mathcal{O}_K$ pour tout $i \in \{1,2,3,4,6\}$ et $v(c_4) < 4$.
3. $a_i \in \mathcal{O}_K$ pour tout $i \in \{1,2,3,4,6\}$ et $v(c_6) < 6$.

La réciproque est vraie lorsque $car(K) \neq 2, 3$.

Exemple 1.2. L'équation de Weirstrass sur $\mathbb{Q}_p$

$$E_{65} : y^2 + xy = x^3 + x^2 - 23x - 44$$

d'invariants $\Delta = 5^3.13^3$ et $c_4 = 5.13.17$, est minimale en p pour tout premier $p \in \mathbb{Z}$.

L'algorithme de Tate [34], permet d'en déduire si une équation de Weierstrass est minimale ou non.

Soit K un corps de nombres, $\mathcal{O}_K$ l'anneau des entiers de K et soit E/K une courbe elliptique d'équation de Weierstrass

$$E : \quad y^2 + (a_1x + a_3)y = x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in \mathcal{O}_K, \tag{1.14}$$

de discriminant $\Delta(E)$.

Définition 1.15. *Le discriminant minimal de E/K est l'ideal entier $\mathfrak{D}_E$ de K, défini par*

$$\mathfrak{D}_E = \prod_{v \in M_K} \mathfrak{p}^{ord_v(\Delta_v)}.$$

où Δ_v est le discriminant d'une équation minimale de E associée à v et $\mathfrak{p}$ est l'ideal premier de $\mathcal{O}_K$ associé à v. L'ensemble M_K désigne l'ensemble des places non archimédiennes de K.

Pour toute valuation $v \in M_K$, le changement de variables

$$(x, y) \mapsto (u_v^2 x_v + r_v, u_v^3 y_v + u_v^2 s_v x_v + t_v) \text{ où } r_v, s_v, t_v \in K \text{ et } u_v \in K^\times$$

transforme l'équation (1.14) en un modèle minimal

$$y_v^2 + (a_{1,v}x_v + a_{3,v})y_v = x_v^3 + a_{2,v}x_v^2 + a_{4,v}x_v + a_{6,v}, \quad a_i \in K \tag{1.15}$$

de discriminant Δ_v.

Les deux discriminants $\Delta(E)$ et Δ_v sont liés par la relation $\Delta(E) = u_v^{12}\Delta_v$.

Soit l'ideal

$$\mathfrak{a} = \prod_{v \in M_K} \mathfrak{p}^{-ord_v(u_v)}. \tag{1.16}$$

Alors le discriminant minimal est égal à

$$\mathfrak{D}_{E/K} = \big(\Delta(E)\big)\mathfrak{a}^{12}. \tag{1.17}$$

Bonne réduction potentielle.

Dans ce paragraphe, nous allons expliquer le comportement du type de réduction d'une courbe elliptique suivant l'extension de corps ; une courbe elliptique E/K à mauvaise réduction, peut acquérir bonne réduction sur une extension finie de K.

Soit K un corps de valuation discrète v, $\mathcal{O}_K$ son anneau d'entiers et $\mathfrak{m}$ son ideal maximal.

Définition 1.16. *Une courbe elliptique E/K a bonne réduction potentielle s'il existe une extension finie de K sur laquelle E acquiert bonne réduction.*

La bonne réduction potentielle est caractérisée par le résultat suivant :

Proposition 1.9. *Une courbe elliptique E/K a bonne réduction potentielle si et seulement si son invariant modulaire est entier (c'est-à-dire $j_E \in \mathcal{O}_K$).*

Preuve. Supposons que E a bonne réduction potentielle.

Soit L une extension finie de K sur laquelle E acquiert bonne réduction et $\mathcal{O}_K$ l'anneau de valuation de K. Supposons que

$$y^2 + (a_1x + a_3)y = x^3 + a_2x^2 + a_4x + a_6,$$

est une équation minimale de E sur L, de discriminant Δ' et d'invariant c'_4. L'hypothèse E a bonne réduction sur L implique

$$\Delta' \in \mathcal{O}'^{\times}_K \quad \text{et} \quad j_E = (c'_4)^3/\Delta' \in \mathcal{O}^{\times}_K.$$

L'hypothèse E est définie sur K entraîne $j_E \in K$. D'où le résultat $j_E \in \mathcal{O}_K$.

Réciproquement : Supposons que $j_E \in \mathcal{O}_K$.

1. Premier cas : $car(K) \neq 2$.
   Soit L' une extension de K sur laquelle E possède un modèle de Legendre

   $$E : y^2 = x(x-1)(x-\mu), \quad \mu \in L', \quad \mu \neq 0, 1. \tag{1.18}$$

   L'hypothèse $j_E \in \mathcal{O}_K$ et l'équation $2^8\big(1-\mu(1-\mu)\big)^3 - j\mu^2(1-\mu)^2 = 0$ entraîne que μ est entier sur $\mathcal{O}_K$. La clôture intégrale de $\mathcal{O}_K$ dans L' est l'anneau de valuation $\mathcal{O}'_K$ de L' et $\mathfrak{m}'$ son idéal maximal. Il s'en suit que $\mu \in \mathcal{O}'_K$ et que μ non congru à 0 ou 1 (mod $\mathfrak{m}'$).
   Il en résulte que l'équation (1.18) est à coefficients entiers et donc E a bonne réduction.

2. Deuxième cas : $car(K) = 2$.
   Dans ce cas, la courbe E possède une équation normale de Deuring

$$E : y^2 + \nu xy + y = x^3, \quad \nu \in K' \quad \text{et} \quad \nu^3 \neq 27,$$

   de discriminant $\Delta = \nu^3 - 27$ et d'invariant modulaire

$$j_E = \nu^3(\nu^3 - 24)^3/(\nu^3 - 27) = \nu^6/(\nu^3 - 1).$$

   (Pour plus de détails, voir [32], Appendice A).
   Comme $j_E \in \mathcal{O}_K$, la relation

$$\nu^6 - j_E(\nu^3 - 1) = 0$$

   entraîne $\nu \in \mathcal{O}'_K$ et $\nu^3 \not\equiv 1 \pmod{\mathfrak{m}'}$. Il s'ensuit que l'équation normale de Deuring est à coefficients entiers et donc E a bonne réduction.

□

Proposition 1.10. *Soit une courbe elliptique E/K.*

1. *Soit L une extension non-ramifiée de K. Si E a bonne réduction, (multiplicative, ou additive) alors E a le même type de réduction sur L.*
2. *Soit L une extension finie de K. Si E a bonne réduction ou réduction multiplicative alors E a le même type de réduction sur L.*
3. *Il existe une extension finie L de K sur laquelle E a bonne réduction ou réduction multiplicative.*

Preuve. Cf [32], VII. Proposition 5.4. □

Proposition 1.11. *Soit L une extension finie de $\mathbb{Q}_p$ et soit une courbe elliptique E sur L à multiplication complexe. Alors E a bonne réduction potentielle.*

Preuve. Cf [32], VII. Exercice 7.10. □

Bonne réduction partout

Soit K un corps de nombres, $\mathcal{O}_K$ l'anneau des entiers de K, $\mathfrak{p}$ un idéal premier de K et v la place de K associée à $\mathfrak{p}$. Une courbe elliptique E/K a bonne réduction en $\mathfrak{p}$ si E a bonne réduction sur K. Alors E a bonne réduction en $\mathfrak{p}$ si et seulement si, il existe un modèle de Weierstrass de E à coefficients dans $\mathcal{O}_K$ et de discriminant

$$\Delta(E) \not\equiv 0 \pmod{\mathfrak{p}}.$$

Définition 1.17. *Une courbe elliptique E/K a bonne réduction partout si E a bonne réduction en tout idéal premier de l'anneau des entiers de K.*

Proposition 1.12. *Soit une courbe elliptique E/K à bonne réduction partout sur K. Alors l'idéal engendré par $\Delta(E)$ est la puissance douzième d'un idéal de K.*

Preuve. E possède une équation de Weierstrass à coefficients $a_i \in \mathcal{O}_K$ et de discriminant $\Delta(E)$ vérifiant

$$\mathfrak{D}_E = \big(\Delta(E)\big)\mathfrak{a}^{12},$$

où $\mathfrak{D}_E$ est le discriminant minimal de E. Mais l'hypothèse de bonne réduction partout entraîne que l'idéal entier $\mathfrak{D}_E$ n'est divisible par aucun idéal premier de K et donc que $\mathfrak{D}_E = \mathcal{O}_K$. Par conséquent, $(\Delta(E)) = \mathfrak{a}^{-12}$ est une puissance douzième. □

Soit K un corps de nombres et L une extension finie de K.

Définition 1.18. *Soit E/K une courbe elliptique. Une tordue de E par L est une courbe elliptique E'/K isomorphe à E sur L.*

Soit une courbe elliptique E/K de modèle de Weierstrass

$$y^2 = x^3 + a_2x^2 + a_4x + a_6, \qquad a_2,\ a_4,\ a_6 \in K. \tag{1.19}$$

Soit $m \in K^\times$. Le changement de variables $(x, y) \mapsto (x/m, y/\sqrt{m})$ et la simplification par m^3 transforment le modèle (1.19) en

$$m^2y^2 = x^3 + a_2mx^2 + a_4m^2x + a_6m^3, \qquad a_2,\ a_4,\ a_6 \in K. \tag{1.20}$$

En substituant $(x, y) \mapsto (x, y/m)$ dans (1.20) nous obtenons l'équation de la tordue E_m de la courbe elliptique E

$$E_m \quad : y^2 = x^3 + a_2mx^2 + a_4m^2x + a_6m^3, \tag{1.21}$$

de discriminant $\Delta(E_m) = m^6\Delta(E) = (\sqrt{m})^{12}\Delta(E)$.

Exemple 1.3. Soit E une courbe elliptique sur K, de modèle de Weiestrass

$$y^2 = x^3 + ax + b, \qquad a,\ b \in K. \tag{1.22}$$

Il y a trois cas ;

1. Premier cas : $ab \neq 0$

   Une tordue de E admet un modèle de Weierstrass de la forme

   $$E_m : y^2 = x^3 + m^2ax + m^3b \quad \text{où} \quad m \in K^\times$$

   Deux tordues E_m et $E_{m'}$ sont K-isomorphes si et seulement si m'/m est un carré dans K.

   En général, E_m est isomorphe à E sur le corps quadratique $K(\sqrt{m})$. Par conséquent, E_m est une $K(\sqrt{m})$-tordue de E.

2. Deuxième cas : $a = 0$

   Une tordue de E a pour équation

   $$y^2 = x^3 + mb \quad \text{avec} \quad m \in K^\times$$

   et devient isomorphe à E sur $K(\sqrt[6]{m})$.

   Ce cas correspond aux courbes elliptiques d'invariant modulaire j égal à 1728.

3. Troisième cas : $b = 0$

   Une tordue de E a pour modèle

   $$y^2 = x^3 + max \quad \text{avec} \quad m \in K^\times$$

   et devient isomorphe à E sur $K(\sqrt[4]{m})$.

   Ce cas correspond aux courbes elliptiques d'invariant modulaire $j = 0$.

1.3 Courbes hyperelliptiques.

Soit K un corps algébriquement clos et C/K une courbe projective lisse.

Définition 1.19. *Un diviseur D de la courbe C est une somme formelle finie de points de $C(K)$, définie par*

$$D = \sum_{P \in C(K)} m_P P \quad \text{où} \quad m_P \in \mathbb{Z}.$$

Le degré de D, est l'entier $\sum_{P \in C(K)} m_P$. Le diviseur D est effectif (ou positif) si $m_P \geq 0$ pour tout $P \in C(K)$. Si $D' = \sum_{P \in C(K)} m'_P P$ est un second diviseur, on écrit $D \geq D'$ lorsque $m_P \geq m'_P$ pour tout $P \in C(K)$.

L'ensemble $Div(C)$ des diviseurs de la courbe C muni de l'addition forme un groupe abélien. L'ensemble $Div^0(C)$ des diviseurs de degré 0 de C est un sous groupe de $Div(C)$.

Proposition 1.13. *Soit une courbe projective, lisse C/K et P un point de C. L'ensemble des fonctions rationnelles sur C qui sont définies au point P est un anneau de valuation discrète noté $\mathcal{O}_P$. Son unique idéal maximal est l'ensemble $\{f \in K(C) \mid f(P) = 0\}$ et son corps de fractions est $K(C)$.*

Preuve. Cf [11], p. 70. □

A toute fonction $f \in K(C)$ correspond un diviseur de f

$$\mathrm{div}(f) = \sum_{P \in C(K)} ord_P(f)P$$

où $ord_P(f)$ est la valuation en P de la fonction f pour tout point $P \in C(K)$:

$$ord_P(f) = \begin{cases} 0, & \text{si } f \text{ est définie en } P \text{ et si } f(P) \neq 0 \\ v_P(f), & \text{si } f \text{ est définie en } P \text{ et si } f(P) = 0 \\ -v_P(1/f), & \text{si } f \text{ a un pôle en } P, \end{cases}$$

où v_P est la valuation de l'anneau local $\mathcal{O}_P$.

Définition 1.20. *Un diviseur D sur C est principal s'il existe une fonction f sur C telle que $D = \mathrm{div}(f)$.*

Comme f a autant de zéros que de pôles alors $\deg(\mathrm{div}(f)) = 0$, et donc tout diviseur principal est de degré 0. L'ensemble $Div^{Princ}(C)$ des diviseurs principaux de C est un sous groupe de $Div^0(C)$.

Deux diviseurs D_1 et D_2 de C sont dans la même classe ; $D_1 \sim D_2$ s'il existe une fonction $f \in K(C)$ tel que $D_1 - D_2 = \mathrm{div}(f)$.

Le groupe quotient $Div(C)/Div^{Princ}(C)$ appelé le groupe de Picard de C et est noté $Pic(C)$. Notons par $Pic^0(C)$ son sous-groupe $Div^0(C)/Div^{Princ}(C)$.

Lemme 1.1. *Soit $f \in K(C)^\times$. Alors $\mathrm{div}(f) = 0$ si et seulement si $f \in K$.*

Le théorème de Riemann-Roch permet de calculer, ou au moins de majorer, la dimension de certains espaces de fonctions rationnelles sur C.

Soit $D \in Div(C)$. Notons par $l(D)$ la dimension du K-espace vectoriel

$$L(D) = \{f \in K(C)^\times \mid \mathrm{div}(f) \geq -D\} \cup \{0\}. \tag{1.23}$$

Lemme 1.2. *Soit $D \in Div(C)$.*

1. *Si $\deg D < 0$, alors $l(D) = 0$.*
2. *Supposons $\deg D = 0$. Alors $l(D) = 1$ si $D \in Div^{Princ}(C)$ et $l(D) = 0$ sinon.*

Théorème 1.7 (Riemann-Roch)**.** *Soit $D \in Div(C)$. Alors $l(D)$ est fini et*

$$l(D) - l(D_{ca} - D) = 1 - g + \deg(D),$$

où D_{ca} est un diviseur canonique de C et l'entier g est le genre de C.

Preuve. Cf [11], p. 192. □

Le résultat suivant, montre que chaque classe de diviseurs dans $Pic^0(C)$ possède un représentant simple.

Proposition 1.14. *Soit une courbe C/K de genre $g \geq 1$ et soit $P_\infty \in C(K)$. Alors tout diviseur de degré zéro est équivalent à un diviseur de la forme $D - gP_\infty$, où D est un diviseur effectif de degré g.*

Preuve. Soit un point fixé $P_\infty \in C(K)$ et un diviseur D de degré 0. Posons $D' = D + gP_\infty$. D'après le théorème de Riemann-Roch,

$$l(D') = 1 + l(D_{ca} - D) \geq 1 \tag{1.24}$$

Il existe alors une fonction $f \in K(C)$ telle que le diviseur $D'' = \mathrm{div}(f) + D'$ est effectif et de degré g. Par définition, les diviseurs D et $D'' - gP_\infty$ sont dans la même classe. □

Définition 1.21. *Un diviseur réduit est un diviseur de la forme $D - gP_\infty$ où D est un diviseur effectif de degré g.*

Le théorème de Riemann-Hurwitz permet de calculer le genre d'une courbe.

Théorème 1.8 (Riemann-Hurwitz)**.** *Soit un homomorphisme non constant $\phi : C \mapsto C'$ de deux courbes projectives lisses C et C' définies sur un corps K de caractéristique ne divisant pas les degrés de ramification $e_\phi(P)$ de ϕ pour tout point $P \in C(K)$. Alors*

$$2g_C - 2 = \deg(\phi)\big(2g_{C'} - 2\big) + \sum_{P \in C(K)} (e_\phi(P) - 1)$$

en particulier $g_C \geq g_{C'}$ où g_C est le genre de C et $g_{C'}$ est le genre de C'.

Preuve. Cf [9], p 21. □

Soit K un corps et soit K^{alg} une clôture algébrique de K.

Définition 1.22. *Une courbe projective lisse C/K de genre $g \geq 2$ est hyperelliptique s'il existe un morphisme $\varphi : C \longrightarrow \mathbb{P}^1_K$ de degré 2 défini sur K.*

Une courbe hyperelliptique lisse C admet un modèle affine

$$y^2 + Q(x)y = P(x) \quad \text{avec } P(x) \text{ et } Q(x) \in K[x], \tag{1.25}$$

où $\deg Q \leq g+1$ et $\deg P \leq 2g+2$ avec P et Q sans racines multiples.

Dans ce cas, la courbe C admet une involution hyperelliptique

$$i : K^{alg}(C) \longrightarrow K^{alg}(C)$$

qui envoie un élément (x, y) sur $i(x, y) = (x, -y - Q(x))$ et vérifie

$$\varphi(P) = \varphi \circ i(P) \quad \text{pour tout point} \quad P \in C(K^{alg}).$$

Lorsque la caractéristique de K est différente de 2, nous pouvons compléter le carré de l'équation (3.32) pour obtenir un modèle affine de la forme

$$y^2 = f(x) \quad \text{avec} \quad f = P + \frac{1}{4}Q^2 \tag{1.26}$$

de degré $2g+1$ ou $2g+2$ sans racines multiples. Il existe donc un ou deux points à l'infini suivant que $P + \frac{1}{4}Q^2$ est de degré $2g+1$ ou de degré $2g+2$.

En appliquant la transformation linéaire $(x, y) \mapsto (a^2x, a^{2g+1}y)$ où a est le coefficient de x^{2g+1} dans $P(x)$ de l'équation (1.26), nous obtenons un polynôme unitaire.

Définition 1.23. *Le discriminant d'une courbe hyperelliptique C de genre $g \geq 2$, de modèle (1.25) est le polynôme*

$$\Delta_C = 2^{4g} disc(P(x) + \frac{1}{4}Q(x)^2) \tag{1.27}$$

à coefficients dans K.

Lorsque la caractéristique de K est égale à 2, nous interprétons cette définition de la manière suivante ; si nous considérons les coefficients du modèle (1.25) comme des variables indépendantes, alors Δ_C tel qu'il est défini par la formule (1.27) devient un polynôme en ces variables et à coefficients entiers. Nous obtenons alors la formule pour Δ_C en caractéristique 2 en réduisant ce polynôme modulo 2.

Lemme 1.3. *La courbe C est non-singulière si et seulement si $\Delta_C \neq 0$.*

Définition 1.24. *les points de Weierstrass sont les points de ramification du morphisme φ et sont aussi les points fixes de l'involution hyperelliptique.*

Lorsque la caractéristique du corps K est différente de 2, il y a $2g+2$ points de Weierstrass et lorsque la caractéristique de K est égale à 2, il y a au moins un et au plus $g+1$.

Si l'un des points de Weierstrass est rationnel sur K, en composant φ avec une transformation projective qui envoie un point de Weierstrass sur l'infini, nous pouvons supposer que ce point est un point à l'infini. Ainsi nous obtenons un modèle affine de la forme (1.25) avec Q de degré inférieur ou égale à g et P de degré $2g+1$.

Exemple 1.4. Les points de Weierstrass de la courbe C de modèle (3.32) sont le point à l'infini et les points d'abscisses les racines de $Q(x)$.

Soit K un corps de caractéristique différente de 2.

Proposition 1.15. *Une courbe C/K de genre deux est birationnellement équivalente sur K à une courbe de modèle affine plan*

$$y^2 = f(x) \tag{1.28}$$

où

$$f(x) = a_6x^6 + a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 \in K[x] \tag{1.29}$$

sans facteur carré.

L'équation (1.28) est unique à transformations homographiques près

$$(x, y) \mapsto \big(\frac{ax+b}{cx+d}, \frac{\lambda y}{(cx+d)^3}\big) \tag{1.30}$$

où a, b, c, $d \in K$, $ad - bc \neq 0$ et $\lambda \in K^\times$.

Supposons que le corps K est algébriquement clos et que le polynôme $f(x)$ possède une racine $\alpha \in K$. Alors, la substitution

$$(x, y) \mapsto \big(\frac{1}{(x-\alpha)}, \frac{y}{(x-\alpha)^3}\big) \tag{1.31}$$

transforme le modèle (1.28) en l'équation

$$y^2 = F(x) \quad \text{avec} \quad F(x) \in K[x] \quad \text{de degré 5.} \tag{1.32}$$

Supposons que le corps K est de caractéristique différente de 2 et que $y^2 = F(x)$ est un modèle hyperelliptique de C, où $F(x) \in K[x]$ est de degré 5 ou 6 sans racines multiples.

Le conjugué d'un point $P = (x, y)$ de C par l'involution hyperelliptique i est le point $\overline{P} = (x, -y)$.

Il existe un ou deux points à l'infini selon que F est de degré 5 ou 6, notés ∞ et $\overline{\infty}$, où $\overline{\infty} = \infty$ lorsque F est de degré 5.

Proposition 1.16. *Les diviseurs de degré* 2 *de la forme* $P+\overline{P}$ *sont linéairement équivalents.*

Preuve. La formule

$$\mathrm{div}(x - x(P)) = P + \overline{P} - \infty - \overline{\infty}$$

entraîne $P + \overline{P}$ est équivalent à $\infty + \overline{\infty}$. Il en résulte que

$$\mathrm{div}((x - x(P)/(x - x(Q)) = P + \overline{P} - Q - \overline{Q}$$

lorsque P et Q ne sont pas des points à l'infini et donc que $P+\overline{P} \sim Q+\overline{Q}$. □

La classe canonique $\mathcal{D}$ contient $\infty+\overline{\infty} = \mathrm{div}(dx)$ et donc tous les diviseurs de la forme $P+\overline{P}$. D'après le théorème de Riemann-Roch, toute classe $\mathcal{U} \neq \mathcal{D}$ de diviseurs de degré 2 de $Pic(C)$ contient un seul diviseur effectif, qui est donc de la forme $P_1 + P_2$ avec P_1, $P_2 \in C(K)$ et $P_2 \neq \overline{P_1}$. Réciproquement, tout diviseur de cette forme représente une classe de degré 2 différente de $\mathcal{D}$.

Proposition 1.17. *Soit deux points* P_1 *et* P_2 *de* $C(K)$. *Alors le diviseur* $P_1 + P_2$ *est rationnel sur* K *si, ou bien*

1. P_1 *et* P_2 *sont rationnels sur* K, *ou bien*
2. P_1 *et* P_2 *sont rationnels sur une extension quadratique de* K *et conjugués sur* K.

Soient deux diviseurs effectifs de degré 2, rationnels sur K :

$$U = (a_1, \alpha_1) + (a_2, \alpha_2) \quad \text{et} \quad V = (b_1, \beta_1) + (b_2, \beta_2)$$

Il existe un unique polynôme $P(x) \in K[x]$ de degré 3 telle que la courbe $Y = P(x)$ passe par les quatre points (a_1, α_1), (a_2, α_2), (b_1, β_1) et (b_2, β_2). Le polynôme $F(x) - P(x)^2$ est alors de degré 6, et les coefficients a_1, a_2, b_1, b_2 sont des racines.

Notons par c_1 et c_2 les deux autres racines et soit $\gamma_1 = P(c_1)$, $\gamma_2 = P(c_2)$. En posant $W = (c_1, \gamma_1) + (c_2, \gamma_2)$, nous remarquons que

$$\mathrm{div}(y - P(x)) = U + V + W - 3(\infty + \overline{\infty}).$$

Par conséquent, si $\mathcal{U}$ désigne la classe de $U - (\infty + \overline{\infty})$ dans $Pic^0(C)$ et si nous définissons $\mathcal{V}$ et $\mathcal{W}$ de la même manière, alors $\mathcal{U} + \mathcal{V} = \overline{\mathcal{W}}$, et donc le diviseur W est rationnel sur K si U et V sont rationnels sur K.

Le symétrique de la classe $\mathcal{U}$ est la classe $\overline{\mathcal{U}}$ de

$$(a_1, -\alpha_1) + (a_2, -\alpha_2) - (\infty + \overline{\infty}).$$

En effet, le diviseur

$$P_1 + P_2 + \overline{P_1} + \overline{P_2} - 2(\infty + \overline{\infty})$$

est principal, égal à

$$\mathrm{div}(x - (x(P_1))(x - x(P_2)).$$

Lemme 1.4. *La classe $\mathcal{U}$ est d'ordre 2 si et seulement si*

$$U = (a_1, 0) + (a_2, 0) \quad \text{où} \quad a_1 \text{ et } a_2 \text{ sont des racines distinctes de } F(x).$$

Il s'ensuit qu'il existe 15 éléments d'ordre 2 de $Pic^0(C)$ qui ne sont pas nécessairement définis sur K.

Théorème 1.9. *Soit une courbe plane lisse projective C/K de genre g. Alors il existe une variété abélienne de dimension g, appelée la jacobienne J_C de C et un isomorphisme de groupes $J_C(K) \simeq Pic^0(C)$.*

Si, de plus, la courbe C est définie sur un sous-corps K_0 de K, alors J_C est définie sur K_0. Si, en plus, l'extension K/K_0 est séparable, alors l'isomorphisme $J_C(K) \simeq Pic^0(C)$ est un isomorphisme de $Gal(K/K_0)$-modules.

Soit $P_\infty \in C(K)$. D'après la proposition 1.14, toute classe de $Pic^0(C)$ est représentée par un diviseur réduit, c'est-à-dire par un diviseur de la forme $(P_1 + P_2 + \cdots + P_g) - gP_\infty$, avec $(P_1, P_2, \ldots, P_g) \in C(K)^g$.

Proposition 1.18. *Supposons que le genre de la courbe C est non nul et fixons $P_\infty \in C(K)$.*

1. *L'application $C(K)^g \to Pic^0(C)$ qui envoie $(P_1, P_2, \ldots, P_g)$ sur la classe du diviseur $(P_1 + P_2 + \cdots + P_g) - gP_\infty$ est induite par un morphisme dominant $C^g \to J_C$.*
2. *L'application $C(K) \to Pic^0(C)$ qui envoie $P \in C(K)$ sur la classe du diviseur $P - P_\infty$ est induite par une immersion fermée $C \to J_C$.*

Lorsque C est définie sur un sous-corps K_0 de K, les morphismes

$$C^g \to J_C \quad \text{et} \quad C \to J_C$$

sont rationnels sur K_0.

Soit C/K une courbe de genre deux et J_C sa jacobienne. Le noyau de la multiplication [2] par 2 sur J_C est d'ordre 16. L'application [2] peut alors se factoriser comme produit de deux isogénies de variétés abéliennes, chacune de noyau d'ordre 4. La variété isogène est la jacobienne d'une courbe $\widehat{C}$ qui peut être déterminée. Par exemple, la courbe de genre deux C_w du chapitre 3 est isogène au produit de deux courbes elliptiques.

Soit V une variété abélienne sur K et soit N un entier supérieur ou égal à 2. Notons par $V[N]$ le groupe des points de torsion de $V(K^{alg})$ dont l'ordre divise N.

$$V[N] = \{P \in V(K^{alg}) \mid NP = 0\}.$$

La structure du groupe $V[N]$ est donnée par le théorème suivant.

Théorème 1.10. *Soit V une variété abélienne sur K de dimension g. Si N est un entier premier à la caractéristique de K, alors*

$$V[N] \simeq (\mathbb{Z}/N\mathbb{Z})^{2g}. \tag{1.33}$$

Preuve. Cf [25]. □

1.4 Nombre de points d'une courbe de genre $g \leq 2$ sur un corps fini.

Soit q une puissance d'un nombre premier p et $\mathbb{F}_q$ le corps fini à q éléments. L'automorphisme de Frobenius est l'application $\pi : \mathbb{F}_q^{alg} \to \mathbb{F}_q^{alg}$ définie par $\pi(x) = x^q$, laissant fixe $\mathbb{F}_q$. Si X est une variété sur $\mathbb{F}_q$, π induit un morphisme $X \to X$. Lorsque A est une variété abélienne et ℓ est un nombre premier différent de p, π induit un endomorphisme du groupe $A[\ell^r]$ pour tout entier r, d'où un endomorphisme du module de Tate $T_\ell(A) = \varprojlim A[\ell^r]$ et enfin un endomorphisme du $\mathbb{Q}_\ell$-espace vectoriel $V_\ell(A) = T_\ell(A) \otimes \mathbb{Q}_\ell$. Puisque $\ell \neq p$, le Théorème 1.10 entraîne que $V_\ell(A)$ est de dimension $2g$, où g désigne la dimension de A.

Théorème 1.11. *Soit A une variété abélienne de dimension g sur $\mathbb{F}_q$, soit ℓ un nombre premier différent de la caractéristique de $\mathbb{F}_q$ et soit $\chi_A(x)$ le polynôme caractéristique de l'endomorphisme de Frobenius de $V_\ell(A)$ sur $\mathbb{F}_q$.*

1. *$\chi_A(x)$ est un polynôme unitaire de degré $2g$ à coefficients dans $\mathbb{Z}$.*
2. *$\chi_A(x)$ est indépendant du choix du nombre premier ℓ.*
3. *$\chi_A(x)$ ne dépend que de la classe d'isogénies de A.*
4. *Supposons que A est $\mathbb{F}_q$-isogène à un produit $B\times C$ de variétés abéliennes. Alors $\chi_A(x) = \chi_B(x)\chi_C(x)$.*
5. *$\#A(\mathbb{F}_q) = \chi_A(1)$.*
6. *Si α est une racine complexe de $\chi_A(x)$, alors $\alpha\overline{\alpha} = q$. Par conséquent, $|\alpha| = \sqrt{q}$ et le coefficient constant de $\chi(x)$ est q^g.*
7. *Soit $r \geq 1$ un entier. Si la factorisation complexe du polynôme $\chi_A(x)$ est $\prod_\alpha(x-\alpha)$, alors celle du polynôme caractéristique de A sur l'extension de degré r de $\mathbb{F}_q$ est $\prod_\alpha(x-\alpha^r)$.*

Le polynôme χ_A est appelé *le polynôme caractéristique* de A.

Corollaire 1.1. *Soit A une variété abélienne de dimension g sur $\mathbb{F}_q$. Alors*

$$(\sqrt{q}-1)^{2g} \leq \#A(\mathbb{F}_q) \leq (\sqrt{q}+1)^{2g}.$$

Preuve. Soit α une racine de $\chi_A(x)$. D'après le Théorème (1.11),

$$|\alpha| = \sqrt{q}.$$

Par conséquent,

$$\sqrt{q}-1 \leq |1-\alpha| \leq \sqrt{q}+1.$$

Il en résulte que

$$(\sqrt{q}-1)^{2g} \leq \prod_{\{\alpha|\chi_A(\alpha)=0\}} |1-\alpha| \leq (\sqrt{q}+1)^{2g},$$

où le produit parcourt l'ensemble des racines de χ_A. Et enfin,

$$\#A(\mathbb{F}_q) = \chi_A(1) = \prod_{\{\alpha|\chi_A(\alpha)=0\}} |1-\alpha|.$$

D'où le résultat suivant : □

Théorème 1.12. *Soit C une courbe projective lisse de genre g sur $\mathbb{F}_q$, soit J_C la jacobienne de C et soit $\chi(x) = x^{2g} - sx^{2g-1} + \cdots$ le polynôme caractéristique de l'endomorphisme de Frobenius de $V_\ell(J_C)$. Alors $\#C(\mathbb{F}_q) = q+1-s$ et, par conséquent,*

$$q+1-2g\sqrt{q} \leq \#C(\mathbb{F}_q) \leq q+1+2g\sqrt{q}.$$

Pour plus de détails sur le polynôme caractéristique $\chi(x)$ de l'endomorphisme de Frobenius, voir [36], [33] ou [32].

En genre 0

Le polynôme caractéristique (de la jacobienne) d'une courbe C de genre 0 sur $\mathbb{F}_q$ est

$$\chi(x) = 1 \quad \text{et} \quad \#C(\mathbb{F}_q) = q + 1.$$

Dans ce cas, la courbe C est isomorphe à la droite projective sur $\mathbb{F}_q$.

En genre 1

Lorsque C est de genre un, le polynôme caractéristique de Frobenius de J_C est alors donné par

$$\chi(x) = x^2 - sx + q = (x - \alpha)(x - \overline{\alpha})$$

où α et $\overline{\alpha}$ sont des conjugués complexes, de valeur absolue $\sqrt{q}$,

$$s = \alpha + \overline{\alpha}, \quad \text{avec } |s| \leq 2\sqrt{q}.$$

et

$$q + 1 - 2g\sqrt{q} = q + 1 - 2\sqrt{q} = (\sqrt{q} - 1)^2 > 0.$$

Par conséquent, $C(\mathbb{F}_q)$ est non-vide d'après le théorème 1.12. En particulier, toute courbe C de genre un sur un corps fini possède un point rationnel sur ce corps et est donc munie de la structure d'une courbe elliptique. On en tire que C est isomorphe à J_C.

En genre 2

Soit C une courbe de genre deux définie sur $\mathbb{F}_q$, déquation $y^2 = f(x)$ où le polynôme f est de degré 5 ou 6 et sans facteur carré. Le polynôme caractéristique de l'endomorphisme de Frobenius π de $V_\ell(J_C)$ est un polynôme de degré 4 de la forme

$$\chi_p(x) = x^4 - sx^3 + tx^2 - qsx + q^2 = (x - \alpha)(x - \overline{\alpha})(x - \beta)(x - \overline{\beta})$$

où $\alpha\overline{\alpha} = \beta\overline{\beta} = q$. Par conséquent,

$$\begin{aligned} \#C(\mathbb{F}_q) &= q + 1 - (\alpha + \overline{\alpha} + \beta + \overline{\beta}) = q + 1 - s, \\ \#C(\mathbb{F}_{q^2}) &= q^2 + 1 - (\alpha^2 + \overline{\alpha}^2 + \beta^2 + \overline{\beta}^2) = q^2 + 1 - (s^2 - 2t). \end{aligned}$$

Les coefficients s et t (et donc $\chi(1)$, le cardinal de $J_C(\mathbb{F}_q)$), sont donc déterminés par les équations

$$N_1 = \#C(\mathbb{F}_q), \qquad N_2 = \#C(\mathbb{F}_{q^2}), \tag{1.34}$$

$$s = q + 1 - N_1, \qquad t = \frac{(N_1^2 + N_2)}{2} + q - N_1 - qN_1. \tag{1.35}$$

Quant au calcul de N_1, il peut se faire (lorsque $p \neq 2$) à l'aide de la formule

$$N_1 = N_{1,\infty} + \sum_{x \in \mathbb{F}_q} (1 + f(x)^{\frac{q-1}{2}}), \tag{1.36}$$

Il en résulte que $f(x)^{(q-1)/2} = 0$ si x est une racine de f et, si $f(x) \neq 0$ alors $f(x)^{(q-1)/2} = 1$ ou -1 selon que $f(x)$ soit un carré de $\mathbb{F}_q^\times$ ou non.

Enfin, $N_{1,\infty}$ désigne le nombre de points à l'infini de la courbe qui sont rationnels sur $\mathbb{F}_q$. Il s'ensuit que $N_{1,\infty} = 1$ si f est de degré 5 et, lorsque f est de degré 6, $N_{1,\infty} = 2$ ou 0 selon que le coefficient de x^6 dans f est un carré de $\mathbb{F}_q$ ou non. Notons qu'il y a une formule semblable pour N_2.

Nous allons utiliser ces formules dans le § 3.6 pour calculer les Tables 3.3 et 3.2). Pour plus de détails, voir [32], Chapitre V. Théorème 2.4 en genre 1 et [23] ou [18] en genre 2.

Chapitre 2

Equations de la courbe modulaire $X_1(N)$.

Dans ce chapitre nous présentons un nouvel algorithme pour obtenir des équations de modèles affines des courbes modulaires $X_1(N)$.

2.1 Quelques fonctions elliptiques.

Soit K un corps commutatif et une courbe elliptique E/K, d'équation de Weierstrass

$$E: \quad y^2 + (a_1x + a_3)y = x^3 + a_2x^2 + a_4x + a_6, \quad \in K[x, y]. \tag{2.1}$$

Supposons que $E(K)$ contient un point $P = (a, b)$ autre que l'origine O_E. Alors, en remplaçant x par $x - a$ et y par $y - b$, nous pouvons supposer que $P = (0, 0)$. Cela implique que $a_6 = 0$. Donc, chaque couple (E, P) est formé par une courbe elliptique E sur K et un point $P \in E(K)$ autre que l'origine peut être representé sous la forme

$$y^2 + (a_1x + a_3)y = x^3 + a_2x^2 + a_4x, \qquad P = (0, 0). \tag{2.2}$$

Lemme 2.1. *Supposons que (2.2) défini une courbe elliptique et que P est un point de torsion.*

1. *Si P est d'ordre $N \geq 3$, alors $a_3 \neq 0$ et, après un changement de variables, nous pouvons supposer que $a_4 = 0$.*
2. *Si $a_3 \neq 0$ et $a_4 = 0$, alors P est d'ordre 3 si et seulement si $a_2 = 0$.*

Preuve. (1) Soit $Q \neq O_E$ un point d'abscisse $x(Q) = 0$. Alors

$$y(Q)^2 + a_3y(Q) = 0$$

Si $a_3 = 0$, alors $Q = P$ et donc x n'a pas d'autre zéro que P. Il s'ensuit que x doit avoir un zéro d'ordre 2 en P et donc le point P est d'ordre 2, contrairement aux hypothèses. D'où $a_3 \neq 0$, et nous vérifions facilement qu'en substituant $y + \frac{a_4}{a_3}x$ pour y nous obtenons un modèle avec $a_4 = 0$.

(2) Supposons que $a_4 = 0$. Soit un point $Q \neq O_E$ avec $y(Q) = 0$. Alors

$$x(Q)^3 + a_2 x(Q)^2 = 0,$$

ainsi $a_2 = 0$ si et seulement si la seule possibilité pour Q est P, et donc le point P est d'ordre 3 si et seulement si $a_2 = 0$. □

A partir de maintenant, nous considérons les couples (E, P) representés par

$$y^2 + (a_1 x + a_3)y = x^3 + a_2 x^2, \qquad a_2 a_3 \neq 0, \qquad P = (0, 0). \tag{2.3}$$

Le discriminant de ce modèle est

$$\Delta(E) = a_3^2(-a_2 a_1^4 + a_3 a_1^3 - 8a_2^2 a_1^2 + 36 a_3 a_2 a_1 - 16 a_2^3 - 27 a_3^2).$$

Supposons toujours que (2.3) définie une courbe elliptique, donc $\Delta(E) \neq 0$.

Lemme 2.2. *Soit (E, P) et (E', P') deux couples d'équations*

$$(E) : y^2 + (a_1 x + a_3)y = x^3 + a_2 x^2, \quad a_2 a_3 \neq 0, \quad P = (0, 0), \text{ et} \tag{2.4}$$
$$(E') : y^2 + (a_1' x + a_3')y = x^3 + a_2' x^2, \quad a_2' a_3' \neq 0, \quad P' = (0, 0). \tag{2.5}$$

Alors (E, P) et (E', P') sont K-isomorphes si et seulement s'il existe $\lambda \in K^\times$ tel que $a_i' = \lambda^i a_i$ pour tout $i \in \{1, 2, 3\}$. Lorsque c'est le cas, λ est unique.

Preuve. Si un tel λ existe, alors $(x, y) \mapsto (\lambda^2 x, \lambda^3 y)$ est un isomorphisme de (E, P) sur (E', P'). Un K-isomorphisme ϕ de la courbe elliptique E vers E' envoie (x, y) sur

$$(\lambda^2 x + r, \lambda^3 y + ux + v), \qquad \text{où } \lambda \in K^\times,\ u,\ v \in K.$$

Pour avoir $\phi(0, 0) = (0, 0)$, nous devons avoir $r = v = 0$. Puisque les coefficients de x sur E et E' s'annulent, nous devons avoir $u = 0$. Donc ϕ doit être de la forme

$$(x, y) \mapsto (\lambda^2 x, \lambda^3 y).$$

Cela implique que $a_i' = \lambda^i a_i$ pour $i \in \{1, 2, 3\}$. Puisque $a_2' = \lambda^2 a_2$, $a_3' = \lambda^3 a_3$ et $a_2 a_3 a_2' a_3' \neq 0$, nous devons avoir $\lambda = a_3' a_2 / a_3 a_2'$. D'où λ est unique. □

Proposition 2.1. *Supposons que $N \geq 4$. Alors toute classe de K-isomorphismes des couples (E, P) avec E une courbe elliptique sur K et $P \in E(K)$ un point de torsion d'ordre N, contient un unique modèle de la forme*

$$y^2 + ((1+g)x + f)y = x^3 + fx^2, \quad P = (0,0). \tag{2.6}$$

avec $f \in K^\times$, $g \in K$.

Preuve. Posons $f = a_2^3/a_3^2$ et $g = (a_1a_2 - a_3)/a_3$, alors le modèle

$$y^2 + (a_1x + a_3)y = x^3 + a_2x^2$$

devient isomorphe à

$$y^2 + ((1+g)x + f)y = x^3 + fx^2,$$

via l'isomorphisme

$$x \mapsto (a_2/a_3)^2 x, y \mapsto (a_2/a_3)^3 y.$$

La relation $a_2a_3 \neq 0$ entraîne $f \neq 0$.

Si la classe d'isomorphismes contient aussi

$$\big(y^2 + ((1+g')x + f')y = x^3 + f'x^2, (0,0)\big)$$

avec $f' \in K^\times$ et $g' \in K$ alors, en considérant les coefficients de y et de x^2, le Lemme 2.2 entraîne qu'il existe $\lambda \in K^\times$ tel que

$$f' = \lambda^2 f \quad \text{et} \quad f' = \lambda^3 f$$

La relation $f \neq 0$ implique $\lambda = 1$. □

Pour le reste de cette section, nous supposons que $K = \mathbb{C}$. Nous nous proposons de paramétrer le modèle (2.3) en utilisant les fonctions elliptiques associées au réseau

$$\Omega = \{\int_\gamma \frac{dx}{2y + a_1x + a_3} \mid \gamma \in H_1(E(\mathbb{C}), \mathbb{Z})\}.$$

Plus précisement, en fixant $z_0 \in \mathbb{C}/\Omega$, nous voulons décrire explicitement l'isomorphisme

$$\xi : \mathbb{C}/\Omega \to E(\mathbb{C}) \qquad \text{tel que} \quad \xi(z_0) = P.$$

Soit Ω un réseau quelconque dans $\mathbb{C}$. La fonction elliptique de Weierstrass est définie par la formule

$$\wp(z) = \wp(z,\Omega) = \frac{1}{z^2} + \sum_{\substack{\omega\in\Omega\\ \omega\neq 0}} \Big(\frac{1}{(z-\omega)^2} + \frac{1}{\omega^2}\Big), \tag{2.7}$$

et satisfait l'équation différentielle

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3, \tag{2.8}$$

où

$$g_2 = g_2(\Omega) = 60\sum_{\substack{\omega\in\Omega\\ \omega\neq 0}} \frac{1}{\omega^4} \quad \text{et} \quad g_3 = g_3(\Omega) = 140\sum_{\substack{\omega\in\Omega\\ \omega\neq 0}} \frac{1}{\omega^6} \tag{2.9}$$

sont les séries usuelles d'Eisenstein, ainsi que la formule de duplication

$$\wp(2z) = -2\wp(z) + \frac{1}{4}\frac{\wp''(z)^2}{\wp'(z)^2}. \tag{2.10}$$

En complétant le carré de l'équation (2.3), nous obtenons

$$Y^2 = 4x^3 + (4a_2 + a_1^2)x^2 + 2a_3a_1x + a_3^2$$

avec

$$Y = 2\big(y + \frac{1}{2}(a_1x + a_3)\big).$$

En remplaçant x par $X - \frac{1}{12}(a_1^2 + 4a_2)$ nous obtenons

$$Y^2 = 4X^3 - g_2X - g_3, \qquad g_2^3 - 27g_3^2 \neq 0 \tag{2.11}$$

et cette courbe est parametrée par

$$X = \wp(z), \qquad Y = \wp'(z).$$

Il est facile d'écrire

$$a = \frac{1}{12}(a_1^2 + 4a_2), \tag{2.12}$$

tel que

$$\begin{aligned} g_2 &= \frac{1}{12}(a_1^4 + 8a_2a_1^2 - 24a_3a_1 + 16a_2^2) = 12a^2 - 2a_1a_3 \\ g_3 &= -(2^3a^3 - 2a_1a_3a + a_3^2). \end{aligned} \tag{2.13}$$

Le point $P = (0, 0)$ correspond au point (a, a_3) sur la courbe

$$Y^2 = 4X^3 - g_2X - g_3,$$

tel que la condition $\xi(z_0) = P$ signifie que

$$a = \wp(z_0), \qquad a_3 = \wp'(z_0). \tag{2.14}$$

Comme $a_3 \neq 0$, la première équation de (2.13) entraîne

$$a_1 = \frac{12a^2 - g_2}{2a_3} = \frac{12\wp(z_0)^2 - g_2}{2\wp'(z_0)} = \frac{\wp''(z_0)}{\wp'(z_0)}, \tag{2.15}$$

où la dernière équation résulte en dérivant (2.8) et en remplaçant z par z_0. Ces équations aussi avec (2.12) nous permettent de déterminer a_2.

En résumant la discussion précédente, nous obtenons le résultat

Théorème 2.1. *Soit Ω un réseau dans $\mathbb{C}$ et soit $z_0 \in \mathbb{C}$ tel que $2z_0 \notin \Omega$. Définissons les fonctions elliptiques*

$$a_1(z) = \frac{\wp''(z)}{\wp'(z)}, \quad a_2(z) = 3\wp(z) - \frac{1}{4}\frac{\wp''(z)^2}{\wp'(z)^2}, \quad a_3(z) = \wp'(z), \tag{2.16}$$

de sorte que $\wp(z) = (a_1(z)^2 + 4a_2(z))/12$. Alors la courbe elliptique

$$y^2 + (a_1(z_0)x + a_3(z_0))y = x^3 + a_2(z_0)x^2 \tag{2.17}$$

est paramétrée par les fonctions elliptiques

$$x(z) = \wp(z) - \wp(z_0), \qquad y(z) = \frac{1}{2}\big(\wp'(z) - a_1(z_0)x(z) - a_3(z_0)\big) \tag{2.18}$$

et nous avons $\big(x(z_0), y(z_0)\big) = (0, 0)$.

Inversement, tout couple de la forme (2.3) peut être parametré de cette façon en utilisant le réseau

$$\Omega = \{\int_\gamma \frac{dx}{2y + a_1x + a_3} \mid \gamma \in H_1(E(\mathbb{C}), \mathbb{Z})\},$$

le point z_0 étant la solution unique (mod Ω) *de (2.14).*

Définition 2.1. *Le diviseur d'une fonction elliptique non-nulle f associée à un réseau de périodes Ω est la somme formelle $\sum_{x\in\mathbb{C}/\Omega} v_x(f)[x]$, où $v_x(f)$ est l'ordre du zéro (ou du pôle compté negativement) de f en $z \in \mathbb{C}$ quelconque telle que sa classe* (mod Ω) *est x. (Puisque $\mathbb{C}/\Omega$ est compact, $v_x(f)$ s'annule en dehors d'un ensemble fini).*

L'ordre de f est l'entier non-negatif $\sum_x \max(v_x(f), 0)$.

Proposition 2.2. *Les diviseurs des fonctions a_2, a_3 et $a_1a_2-a_3$ sont donnés par les formules*

$$\operatorname{div}(a_2) = \sum_{\substack{3x=0\\x\neq 0}} [x] - 2\sum_{2x=0}[x], \qquad \operatorname{div}(a_3) = \sum_{\substack{2x=0,\\x\neq 0}} [x] - 3[0],$$
$$\operatorname{div}(a_1a_2 - a_3) = \sum_{\substack{4x=0\\2x\neq 0}} [x] - 3\sum_{2x=0}[x]$$

Preuve. Le cas de $a_3(z) = \wp'(z)$ est bien connu. Dans le cas de $a_2(z)$, nous utilisons la formule de duplication (2.10) pour obtenir

$$a_2(z) = -\wp(2z) + \wp(z), \tag{2.19}$$

à partir duquel nous obtenons facilement le résultat puisque $\wp(z)$ est une fonction paire. De la même manière, un calcul simple en utilisant (2.8) et (2.10) montre que

$$a_1(z)a_2(z) - a_3(z) = \wp'(2z) \tag{2.20}$$

à partir duquel nous obtenons le dernier résultat. □

Corollaire 2.1. *Soit F et G les fonctions elliptiques définies par*

$$F(z) = F(z,\Omega) = \frac{a_2(z)^3}{a_3(z)^2}, \qquad G(z) = G(z,\Omega) = \frac{a_1(z)a_2(z) - a_3(z)}{a_3(z)}.$$

Alors

$$\operatorname{div}(F) = 3\sum_{\substack{3x=0\\x\neq 0}} [x] - 8\sum_{\substack{2x=0\\x\neq 0}}[x], \tag{2.21}$$

$$\operatorname{div}(G) = \sum_{\substack{4x=0\\2x\neq 0}} [x] - 4\sum_{\substack{2x=0\\x\neq 0}}[x]. \tag{2.22}$$

2.2 Polynômes de division.

Revenons au modèle (2.3) et considérons x, a_1, a_2, et a_3 comme indéterminées. Soit l'anneau $A = \mathbb{Z}[x, a_1, a_2, a_3, y]$ où y satisfait l'équation

$$y^2 + (a_1x + a_3)y = x^3 + a_2x^2.$$

Par la division euclidienne, tout élément de A sécrit de façon unique sous la forme

$$P + Qy \qquad \text{avec} \qquad P, Q \in \mathbb{Z}[x, a_1, a_2, a_3].$$

Pour tout entier $n \geq 1$, considérons le polynôme de n-division ψ_n, élément de A défini récursivement par les formules

$$\begin{aligned}
&\psi_1 = 1, \qquad \psi_2 = a_1x + a_3 + 2y,\\
&\psi_3 = 3x^4 + (4a_2 + a_1^2)x^3 + 3a_1a_3x^2 + 3a_3^2x + a_3^2a_2,\\
&\psi_4 = \psi_2(2x^6 + (a_1^2 + 4a_2)x^5 + 5a_3a_1x^4 + 10a_3^2x^3 + 10a_3^2a_2x^2 +\\
&\quad (a_3^2a_2a_1^2 - a_3^3a_1 + 4a_3^2a_2^2)x + a_3^3a_2a_1 - a_3^4)
\end{aligned}$$

et

$$\begin{aligned}
&\psi_{2n+1} = \psi_{n+2}\psi_n^3 - \psi_{n-1}\psi_{n+1}^3, \text{ si } n \geq 2\\
&\psi_2\psi_{2n} = \psi_n(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2), \text{ si } n \geq 3.
\end{aligned} \tag{2.23}$$

Définissons de plus ϕ_n et ω_n par

$$\phi_n = x\psi_n^2 - \psi_{n+1}\psi_{n-1}, \qquad 2\psi_n\omega_n = \psi_{2n} - \psi_n^2(a_1\phi_n + a_3\psi_n^2). \tag{2.24}$$

Nous pouvons en déduire par récurrence que ψ_n, ω_n, $\phi_n \in A$ pour tout n.

Théorème 2.2. *Soit une courbe elliptique E de modèle (2.3). Le point $P = (x_0, y_0)$ de E est d'ordre divisant n si et seulement si $\psi_n(x_0, y_0) = 0$. Si ce n'est pas le cas, alors*

$$nP = \Big(\frac{\phi_n(x_0, y_0)}{\psi_n(x_0, y_0)^2}, \frac{\omega_n(x_0, y_0)}{\psi_n(x_0, y_0)^3}\Big).$$

De plus, si nous attribuons à x, y, a_1, a_2 et a_3 respectivement les poids 2, 3, 1, 2 et 3 et nous consiérons $\mathbb{Z}[x, y, a_1, a_2, a_3]$ comme un anneau gradué, alors ψ_n, ϕ_n et ω_n sont homogènes de poids respectifs $n^2 - 1$, $2n^2$ et $3n^2$.

Preuve. C'est un variant des formules bien connues des courbes de la forme

$$y^2 = x^3 + Ax + B,$$

qui sont discutées par exemple dans Cassels [5]. Voir aussi Lercier et Morain [19]. □

Nous nous intéressons à ce résultat seulement lorsque $P = (0, 0)$ et, à partir de maintenant, nous écrivons ψ_n à la place de $\psi_n(0, 0)$ et la même chose pour ϕ_n et ω_n. Donc ψ_n, ϕ_n et ω_n sont des éléments homogènes de $\mathbb{Z}[a_1, a_2, a_3]$ de poids respectifs $n^2 - 1$, $2n^2$ et $3n^2$.

Nous obtenons

$$\psi_1 = 1, \quad \psi_2 = a_3, \quad \psi_3 = a_3^2 a_2, \quad \psi_4 = a_3^4(a_1 a_2 - a_3), \tag{2.25}$$

aussi bien que les relations

$$\begin{aligned} \psi_{2n+1} &= \psi_{n+2}\psi_n^3 - \psi_{n-1}\psi_{n+1}^3, \text{ si } n \geq 2 \\ a_3\psi_{2n} &= \psi_n(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2), \text{ si } n \geq 3. \end{aligned} \tag{2.26}$$

De plus, nous avons

$$\begin{aligned} \phi_n &= -\psi_{n+1}\psi_{n-1}, \\ 2\psi_n\omega_n &= \psi_{2n} - \psi_n^2(a_1\phi_n + a_3\psi_n^2). \end{aligned} \tag{2.27}$$

Corollaire 2.2. *Soit P le point $(0, 0)$ sur la courbe elliptique (2.3) et soit un entier $n \geq 2$. Alors $nP = O_E$ si et seulement si $\psi_n = 0$. Lorsque ce n'est pas le cas, alors*

$$nP = \left(\frac{\phi_n}{\psi_n^2}, \frac{\omega_n}{\psi_n^3}\right).$$

Les relations (2.27) sont faciles à implémenter et permettent de calculer ψ_n et les coordonnées de nP rapidement par récurrence. En pratique, nous aurons besoin de substituer des polynômes variés pour a_1, a_2 et a_3. Le lemme suivant montre que ψ_n est divisible par une grande puissance de a_3, et nous pouvons améliorer l'implémentation en la simplifiant.

Lemme 2.3. *Soit $v_{a_3}(n)$ l'exposant de la puissance de a_3 divisant ψ_n. Alors*

$$v_{a_3}(n) = \begin{cases} \dfrac{n^2}{4}, & \text{si } n \text{ pair} \\ \dfrac{n^2 - 1}{4}, & \text{si } n \text{ impair.} \end{cases} \tag{2.28}$$

Preuve. Quand $n \leq 4$, c'est clair d'après (2.25). En général, en posant

$$\zeta_n = a_3^{-v_{a_3}^*(n)}\psi_n$$

où $v^*_{a_3}(n)$ est définie comme étant le membre droit de (2.28). Puis, à partir de (2.26) nous obtenons :

$$\zeta_{2n+1} = \begin{cases} a_3\zeta_{n+2}\zeta_n^3 - \zeta_{n-1}\zeta_{n+1}^3 & \text{si } n \text{ est pair} \\ \zeta_{n+2}\zeta_n^3 - a_3\zeta_{n-1}\zeta_{n+1}^3 & \text{si } n \text{ est impair} \end{cases} \tag{2.29}$$

pour tout $n \geq 2$.

Dans le cas où $n \geq 3$, alors

$$\zeta_{2n} = \zeta_n(\zeta_{n+2}\zeta_{n-1}^2 - \zeta_{n-2}\zeta_{n+1}^2). \tag{2.30}$$

Puisque

$$\zeta_1 = \zeta_2 = 1, \quad \zeta_3 = a_2 \quad \text{et} \quad \zeta_4 = a_1a_2 - a_3$$

nous déduisons par récurrence que $\zeta_n \in \mathbb{Z}[a_1, a_2, a_3]$ pour tout n, en d'autres termes que

$$v_{a_3}(n) \geq v^*_{a_3}(n) \quad \text{pour tout } n$$

Pour montrer l'égalité, il suffit de montrer que le terme constant $\zeta_n(0)$ de ζ_n, considéré comme un polynôme à coefficients dans $\mathbb{Z}[a_1, a_2]$, est non nul. En fait, en posant $\epsilon_n = (-1)^{n(n-1)/2}$, nous constatons que

$$\zeta_{2n+1}(0) = \epsilon_n a_2^{n(n+1)/2}, \quad \text{pour tout } n \geq 0$$

et, quand $n \geq 1$, que $\zeta_{2n}(0)$ est de la forme

$$\zeta_{2n}(0) = \epsilon_{n-1} \sum_{i=0}^{\lfloor \frac{n-1}{2} \rfloor} c_{n,i} a_1^{n-1-2i} a_2^{n(n-1)/2+i},$$

où $c_{n,i} \in \mathbb{Z}$ et $c_{n,0} = 1$ pour tout n. À nouveau, cela peut être vérifié par récurrence en utilisant les équations obtenues en substituant $a_3 = 0$ dans (2.29) et (2.30). □

Puisque a_3 est de poids 3, nous constatons que ζ_n est de poids $\frac{1}{4}n^2 - 1$ ou $\frac{n^2-1}{4}$ selon que n est pair ou impair. Ce qui représente une amélioration considérable. Par exemple, a_3^{625} divise ψ_{50}, alors que ζ_{50} est de poids 624 et donc de degré au plus 208 en a_3. Il est donc préférable d'implémenter (2.29) et (2.30) au lieu de (2.26). En utilisant (2.27) nous pouvons calculer la puissance de a_3 divisant ϕ_n et ω_n et accélérer le calcul de nP lorsque $nP \neq O_E$.

Cependant, comme nous le verrons dans la section suivante, la poursuite de la simplification est possible dans le cas nécessaire pour calculer les équations de $X_1(N)$.

2.3 Une première équation de $X_1(N)$.

Soit un entier $N \geq 4$ fixé. Notons par $\mathcal{H}$ le demi-plan supérieur

$$\mathcal{H} = \{\tau \in \mathbb{C} \mid \Im(\tau) > 0\}.$$

Soit $\tau \in \mathcal{H}$, notons par Ω_τ le réseau dans $\mathbb{C}$ de base $(\tau, 1)$. Lorsque $i \in \{1, 2, 3\}$ nous écrivons $a_i(\tau)$ au lieu de $a_i(1/N, \Omega_\tau)$ où $z \mapsto a_i(z, \Omega)$ est la fonction elliptique utilisée dans le Théorème 2.1. Posons

$$f(\tau) = F(1/N, \Omega_\tau) \quad \text{et} \quad g(\tau) = G(1/N, \Omega_\tau)$$

où F et G sont les fonctions définies dans le corollare 2.1. Donc, d'après (2.19) et (2.20),

$$f(\tau) = \frac{(\wp(1/N, \Omega_\tau) - \wp(2/N, \Omega_\tau))^3}{\wp'(1/N, \Omega)^2},$$
$$g(\tau) = \frac{\wp'(2/N, \Omega_\tau)}{\wp'(1/N, \Omega_\tau)}.$$

Lemme 2.4. *Soient les polynômes homogènes $\psi_n \in \mathbb{Z}[a_1, a_2, a_3]$ introduits dans le § 2.2. Alors*

$$\psi_N\big(a_1(\tau), a_2(\tau), a_3(\tau)\big) = 0 \quad \textit{pour tout } \tau \in \mathcal{H}. \tag{2.31}$$

Preuve. Cela résulte du Théorème 2.1 et du Corollaire 2.2. □

Théorème 2.3. *Soit un entier $N \geq 4$.*

1. *Les fonctions f et g sont des fonctions modulaires sur $\Gamma_1(N)$ et engendrent le corps de toutes les fonctions modulaires sur $\Gamma_1(N)$.*
2. *Nous avons*
$$\psi_N(1 + g, f, f) = 0. \tag{2.32}$$

Preuve. Les fonctions

$$\tau \mapsto \wp(1/N, \Omega_\tau), \qquad \tau \mapsto \wp'(1/N, \Omega_\tau) \quad \text{et} \quad \tau \mapsto \wp''(1/N, \Omega_\tau)$$

sont des formes modulaires sur $\Gamma_1(N)$ de poids 2, 3 et 4. Il s'ensuit que $a_i(\tau)$, $i \in \{1, 2, 3\}$ est une forme modulaire de poids i. Donc f et g sont des fonctions modulaires sur $\Gamma_1(N)$.

Pour montrer que f et g engendrent $\mathbb{C}(X_1(N))$, nous les interprétons comme des fonctions méromorphes sur la surface de Riemann compacte $X_1(N)$.

Rappelons que si X est une surface de Riemann compacte quelconque et S un sous-ensemble du corps $\mathbb{C}(X)$ des fonctions méromorphes sur S, alors S engendre $\mathbb{C}(X)$ si et seulement s'il existe un sous ensemble U ouvert non-vide de X tel que si P et Q sont deux points de U tels que $\varphi(P) = \varphi(Q)$ pour tout $\varphi \in S$, alors $P = Q$.

Appliquons ce qui précède en prenant $X = X_1(N), U = X_1(N)$ dépourvue des pointes et $S = \{f, g\}$, l'assertion résulte alors du Lemme 2.1. Ce qui prouve (1). L'assertion (2) résulte du Lemme 2.4 et la Proposition 2.1.

□

Remarque 2.4. Comme le référé nous l'a indiqué, les fonctions $a_i(\tau)$ sont en fait des formes modulaires holomorphes partout (c'est à dire, y compris aux pointes). Pour voir cela, nous utilisons le fait que les fonctions

$$\tau \mapsto \left(\wp^{(k)}(z, \Omega_\tau)\right)_{z=1/N}$$

sont holomorphes pour tout $k \geq 0$. Puisque $a_3(\tau) = \wp'(1/N, \Omega_\tau)$, cela entraîne que a_3 est holomorphe. Pour montrer que a_1 et a_2 sont holomorphes, nous constatons que

$$3\wp(1/N, \Omega_\tau) - \tfrac{1}{4}a_1(\tau)^2 = a_2(\tau) = \wp(1/N, \Omega_\tau) - \wp(2/N, \Omega_\tau),$$

où la deuxième égalité résulte de (2.19). Ce qui entraîne que a_2 et a_1^2 sont holomorphes. Puisque a_1 est méromorphe et son carré a_1^2 est holomorphe, nous pouvons conclure que a_1 est elle-même holomorphe.

Nous pouvons utiliser le Théorème 2.3 pour obtenir un modèle affine plan de $X_1(N)$ comme suit ; nous savons que si

$$y^2 + ((1+g)x + f)y = x^3 + fx^2 \tag{2.33}$$

est une courbe elliptique et si $P = (0, 0)$, alors $NP = O$ si et seulement si $\psi_N(1 + g, f, f) = 0$.

Le discriminant de cette courbe elliptique est

$$\Delta = -f^3(16f^2 + (8g^2 - 20g - 1)f + g(g+1)^3). \tag{2.34}$$

Par conséquent, nous pouvons simplifier de $\psi_N(1+g, f, f)$ les facteurs communs avec ce discriminant. Notons par $\Psi_N^{(f,g)} \in \mathbb{Z}[f, g]$ le polynôme ainsi obtenu, normalisé (au signe près) en supposant que les coefficients sont des entiers premiers entre eux.

Notons que, si M divise N, alors $MP = O$ entraîne $NP = O$, de sorte que $\Psi_M^{(f,g)}$ divise $\Psi_N^{(f,g)}$.

Donc $\Psi_N^{(f,g)}$ se factorise sous la forme

$$\Psi_N^{(f,g)} = \prod_{M|N} \Phi_M^{(f,g)}, \tag{2.35}$$

où $\Phi_M^{(f,g)}(f,g)$ s'annule si et seulement si l'ordre de $(0,0)$ est exactement M. Alors, le Théorème 2.3 entraîne que $\Phi_N^{(f,g)} = 0$ est l'équation d'un modèle affine plan de $X_1(N)$.

D'après le Lemme 2.3, le terme $f^{v_{a_3}(\psi_n)}$ divise $\psi_n(1+g,f,f)$. En fait, nous pouvons faire mieux que cela.

Théorème 2.5. *Soit*

$$v_f^*(n) = \begin{cases} 3k^2 & si \quad n = 3k \\ 3k^2 + 2k & si \quad n = 3k+1 \\ 3k^2 + 4k + 1 & si \quad n = 3k+2. \end{cases} \tag{2.36}$$

Alors, pour tout $n \geq 1$, nous avons $\Psi_n^{(f,g)} = f^{-v_f^*(n)}\psi_n(1+g,f,f)$ (au signe près).

Preuve. Soit $\theta_n = f^{-v_f^*(\psi_n)}\psi_n(1+g,f,f)$. Montrons que $\Psi_n^{(f,g)} = \theta_n$ pour tout $n \geq 1$.

Les formules (2.25) et (2.26) entraînent

$$\theta_1 = \theta_2 = \theta_3 = 1, \quad \theta_4 = g, \quad \theta_5 = g - f \tag{2.37}$$

et, quand $N \geq 6$,

$$\theta_N = \begin{cases} \theta_{3n}(\theta_{3n+2}\theta_{3n-1}^2 - \theta_{3n-2}\theta_{3n+1}^2) & \text{si} \quad N = 6n, \\ f\theta_{3n+2}\theta_{3n}^3 - \theta_{3n-1}\theta_{3n+1}^3 & \text{si} \quad N = 6n+1, \\ \theta_{3n+1}\big(f\theta_{3n+3}\theta_{3n}^2 - \theta_{3n-1}\theta_{3n+2}^2\big) & \text{si} \quad N = 6n+2, \\ \theta_{3n+3}\theta_{3n+1}^3 - \theta_{3n}\theta_{3n+2}^3 & \text{si} \quad N = 6n+3, \\ \theta_{3n+2}\big(\theta_{3n+4}\theta_{3n+1}^2 - f\theta_{3n}\theta_{3n+3}^2\big) & \text{si} \quad N = 6n+4, \\ \theta_{3n+4}\theta_{3n+2}^3 - f\theta_{3n+1}\theta_{3n+3}^3 & \text{si} \quad N = 6n+5. \end{cases} \tag{2.38}$$

Il en résulte que $\theta_n \in \mathbb{Z}[f,g]$ pour tout n. En effet, si $n \leq 5$ ceci résulte de (2.37) et pour des grandes valeurs de n il résulte de (2.38) par récurrence.

Pour conclure, nous avons besoin de monter que θ_n est premier au discriminant (2.34) de la courbe elliptique (2.33), et que les coefficients de θ_n sont deux à deux premiers entre eux. Montrons d'abord que f ne divise pas θ_n en montrant que le terme constant $\theta_n(0)$ de θ_n, considéré comme un polynôme en f à coefficients dans $\mathbb{Z}[g]$, n'est pas nul (comparer avec la démonstration du lemme 2.3). En effet, nous obtenons

$$\theta_N(0) = \begin{cases} \epsilon_m \sum_{i=1}^{m} (-1)^i g^{m(m+1)/2-i} = \epsilon_{m-1} g^{m(m-1)/2} \dfrac{g^m+1}{g+1} & \text{si } N = 3m \\ \epsilon_m g^{m(m+1)/2} \quad \text{si} \quad N = 3m+1 \quad \text{ou} \quad \text{si} \quad N = 3m+2, \end{cases} \tag{2.39}$$

où encore

$$\epsilon_m = (-1)^{m(m-1)/2}.$$

Ceci peut être montrer par récurrence sur l'entier naturel N en utilisant la formule obtenue en substituant $f = 0$ dans (2.37) et (2.38).

Pour monter que $16f^2+(8g^2-20g-1)f+g(g+1)^3$ ne divise pas θ_n, nous remarquons que dans le cas contraire, $g(g+1)^3$ diviserait $\theta_n(0)$, ce qui n'est pas le cas d'après (2.39). Finalement, (2.39) montre aussi que ± 1 apparait comme un coefficient dans θ_n ce qui termine la démonstration.

□

D'après la discussion précédente, il s'ensuit que les relations (2.37) et (2.38) donnent une procédure récursive permettant de calculer $\Psi_N^{(f,g)}$, et par conséquent $\Phi_N^{(f,g)}$, en principe pour tout $N \geq 1$. La première colonne de la Table 2.1 donne les polynômes $\Phi_N^{(f,g)}$ pour tout N, $4 \leq N \leq 15$.

2.4 Une équation améliorée de $X_1(N)$.

Il est naturel de se demander si d'autres choix de générateurs de $\mathbb{C}(X_1(N))$ donnent des equations plus simples, c'est à dire de degré plus petit que celui de $\Phi_N^{(f,g)}$. En général, si deux éléments x et y de $\mathbb{C}(X_1(N))$ engendrent $\mathbb{C}(X_1(N))$, notons par $\Phi_N^{(x,y)}$ un polynôme de plus petit degré tel que

$$\Phi_N^{(x,y)}(x,y) = 0$$

(c'est défini seulement à une constante multiplicative non-nulle près). En particulier, si x et y engendrent $\mathbb{C}(X_1(N))$, alors $\Phi_N^{(x,y)} = 0$ est un modèle affine plan de $X_1(N)$.

En particulier, on peut se demander si de tels générateurs peuvent être définis en termes de f et g d'une manière uniforme, c'est à dire par une formule qui est indépendente de N. Ce cas a été initialement observé expérimentalement, et nous n'avons pas d'explications satisfaisantes ni pourquoi les choix suivants marchent, ni pourquoi cela produit des équations plus simples que d'autres substitutions similaires qui ont été essayées.

Avant d'aller plus loin, nous énonçons le Lemme suivant.

Lemme 2.5. *Notons par F et G les fonctions elliptiques utilisées au Corollaire 2.1. Alors*

$$\begin{aligned}
\operatorname{div}(G-F) &= \sum_{\substack{5x=0\\x\neq 0}}[x] - 8\sum_{\substack{2x=0\\x\neq 0}}[x],\\
\operatorname{div}(G^2-G+F) &= \sum_{\substack{6x=0\\2x\neq 0,3x\neq 0}}[x] - 8\sum_{\substack{2x=0\\x\neq 0}}[x],\\
\operatorname{div}(G^3-GF+F^2) &= \sum_{\substack{7x=0\\x\neq 0}}[x] - 16\sum_{\substack{2x=0\\x\neq 0}}[x],\\
\operatorname{div}((F+1)G^2-3FG+2F^2) &= \sum_{\substack{8x=0\\4x\neq 0}}[x] - 16\sum_{\substack{2x=0\\x\neq 0}}[x].
\end{aligned}$$

Preuve. D'après le Corollaire 2.1, le diviseur polaire d'un monôme de la forme F^kG^ℓ est donné par

$$(8k+4\ell)\sum_{\substack{2x=0\\x\neq 0}}[x],$$

où k et ℓ sont des entiers positifs.

Considérons par exemple le cas de la fonction G^2-G+F. D'après ce que nous venons d'énonçer, le diviseur polaire de cette fonction est supporté par les trois points x_1, x_2, x_3 d'ordre 2 et s'écrit sous la forme

$$a[x_1]+b[x_2]+c[x_3]$$

avec a, b et c positifs et ne dépassant pas 8. Donc G^2-G+F est d'ordre au plus 24. D'autre part, G^2-G+F s'annule aux points d'ordre 6 sur $\mathbb{C}/\Omega$. Cela peut être déduit du fait que $\Phi_6^{(f,g)} = g^2-g+f$. (voir la Table 2.1). Comme il y a 24 points d'ordre 6, nous en déduisons que l'ordre de G^2-G+F est au moins 24. Donc il n'y a pas d'autres zéros ni pôles et $\operatorname{div}(G^2-G+F)$ est comme prévu. Un argument similaire marche dans les autres cas. □

Revenons à notre discussion sur les équations de $X_1(N)$. Supposons que $N \geq 6$. Alors le Lemme précédent entraîne que $g - f$ ne s'annule pas identiquement sur $X_1(N)$ et le même procédé est vrai pour g par le Corollaire 2.1. Donc

$$t = f/g \quad \text{et} \quad s = g^2/(f-g)$$

sont des fonctions bien définies sur $X_1(N)$ et nous pouvons résoudre pour f et g pour obtenir

$$f = t(t-1)s \quad \text{et} \quad g = (t-1)s.$$

Par conséquent, s et t engendrent $\mathbb{C}(X_1(N))$ quand $N \geq 6$.

Dans la deuxième colonne de la Table 2.1, $\Phi_N^{(s,t)}$ est déterminé pour tout N, $6 \leq N \leq 15$.

D'autres calculs suggèraient un autre choix de générateurs. Soit

$$r = \frac{t-1}{s+1}, \qquad q = \frac{(s+1)(t-1)}{t+s}. \tag{2.40}$$

En termes de f et g, nous avons

$$r = \frac{(f-g)^2}{g(g^2-g+f)}, \qquad q = \frac{(g^2-g+f)(f-g)}{g^3-fg+f^2}. \tag{2.41}$$

En utilisant Lemme 2.5, nous remarquons que q et r sont bien définis lorsque $N \geq 8$, et nous pouvons résoudre pour t et s pour obtenir

$$t = q(r+1)+1 \quad \text{et} \quad s = q(r+1)/r - 1.$$

Il s'ensuit que q et r constituent un ensemble de générateurs de $\mathbb{C}(X_1(N))$ lorsque $N \geq 8$.

Il en résulte que

$$f = \frac{q(1+r)(1+q+qr)(q+qr-r)}{r}, \; g = \frac{(q(r+1)+1)f}{r},$$

qui nous permet d'écrire l'équation de la courbe elliptique correspondante.

A nouveau, dans la colonne de droite de la Table 2.1, nous présentons le polynôme $\Phi_N^{(q,r)}$ pour tout N, $8 \leq N \leq 15$.

Remarque 2.6. Comme nous avons déjà expliqué, nous n'avons pas d'explications complètes pourquoi les paires de générateurs $\{f, g\}$, $\{s, t\}$ et $\{q, r\}$ mènent succéssivement à des équations plus simples de $X_1(N)$. Nous remarquons que, puisque dans les travaux de plusieurs auteurs, les fonctions modulaires qui apparaîssent dans les équations ont leurs diviseurs supportés par les pointes, et sont donc des unités modulaires (voir par exemple [15]). En outre, certaines combinaisons simples de nos fonctions modulaires sont des unités modulaires. Par exemple, s, t et aussi $s+1$, $t-1$ et $s+t$ sont des unités modulaires quand $N \geq 8$ et nous avons

$$r = (t-1)/(s+1) \quad \text{et} \quad q = (s+1)(t-1)/(t+s),$$

et donc $q+1$ et $r-q$ sont aussi des unités modulaires quand $N \geq 10$. Tout ce qui précéde peut être vérifié en utilisant le Lemme 2.5.

2.5 Commentaires sur les tables.

Nous présentons trois tables donnants des informations concernant les équations de $X_1(N)$ que nous avons obtenu. Dans chaque table, la première colonne indique la valeur de N sous considération et dans la seconde, g rappele le genre de $X_1(N)$.

Pour trouver les équations, premièrement, nous calculons $\psi_N(1+g, f, f)$ en utilisant les relations de récurrence (2.25), (2.26) et (2.27) ainsi que les relations :

$$-\frac{N}{2}P = \frac{N}{2}P \quad \text{si } N \text{ est pair} \qquad \text{et} \qquad \frac{N-1}{2}P = \frac{N+1}{2}P \quad \text{si } N \text{ est impair.}$$

A partir de cela, nous déterminons $\Phi_N^{(f,g)}$ en enlevant les facteurs communs avec $\psi_M(1+g, f, f)$ quand M est un diviseur propre de N et avec le discriminant de la courbe. Nous calculons alors $\Phi_N^{(s,t)}$ en substituant

$$f = t(t-1)s \quad \text{et} \quad g = (t-1)s$$

dans $\Phi_N^{(f,g)}$ et en enlevant les facteurs inutiles. Nous obtenons $\Phi_N^{(q,r)}$ de $\Phi_N^{(s,t)}$ d'une manière similaire. Nous remarquons qu'il est extrêmement important d'enlever les facteurs inutiles de $\psi_N(1+g, f, f)$ *avant* de substituer. Par exemple, d'après le Lemme 2.5, nous savons que f^{833} divise $\psi_{50}(1+g, f, f)$, de sorte qu'en substituant $f = t(t-1)s$, il résulte un facteur inutile de $(t-1)^{833}$ qui, une fois développé devient trés grand devant

$$\Phi_{50}^{(f,g)}(1+(t-1)s, t(t-1)s, t(t-1)s).$$

Comme nous l'avons déjà indiqué, les trois colonnes à droite de la Table 2.1 donnent les équations de $X_1(N)$ pour les ensembles de générateurs $\{f, g\}$, $\{s, t\}$ et $\{q, r\}$ pour ces valeurs de N entre 4 et 15 pour lesquels les deux membres de l'ensemble sont définis, et une entrée vide indiquant que ce n'est pas le cas. Cela montre clairement, que pour les valeurs indiqués de N, la simplification obtenue en passant de l'ensemble $\{f, g\}$ à l'ensemble $\{s, t\}$ et après à $\{q, r\}$, est considérable.

Plus loin, les calculs révèlent des simplifications similaires pour des valeurs plus grandes de N.

La troisième colonne de la Table 2.2 présente des modèles de $X_1(N)$ pour $11 \leq N \leq 20$, dont la plus part sont bien connus.

Ces équations sont données en termes de deux fonctions u et v. Les deux dernières colonnes donnent s et t en termes de u et v. Ces équations sont pour la plus part trouvées par tatonnement en essayant des substitutions variées dans $\Phi_N^{(s,t)}$.

En substituant pour s et t en les coefficients de la courbe elliptique

$$y^2 + (1 + (t-1)sx + t(t-1)s)y = x^3 + t(t-1)sx^2,$$

nous obtenons l'équation de la courbe elliptique correspondante en termes de u and v. Puisque le polynôme $\Phi_N^{(q,r)}$ est obtenu par une procédure récursive comme nous l'avons expliqué avant et qui est facile à implémenter, et il devient rapidement grand lorsque N augmente, il semble de les reproduire en détail ici.

Dans la Table 2.3, nous présentons les degrés $\deg_r \Phi_N^{(q,r)}$ et $\deg_q \Phi_N^{(q,r)}$ ainsi que le degré total $\deg_{\text{total}} \Phi_N^{(q,r)}$ de $\Phi_N^{(q,r)}$ pour tout N de 16 à 51.

Rappelons que la gonalité d'une courbe algébrique projective irréductible X est le plus petit degré d'un morphisme surjectif de X sur la droite projective. C'est aussi la plus petite valeur possible du degré en termes de l'une des variables de l'équation affine plane de X. En particulier, si $\gamma(N)$ désigne la gonalité de $X_1(N)$, alors

$$\gamma(N) \leq \min\left(\deg_r \Phi_N^{(q,r)}, \deg_q \Phi_N^{(q,r)}\right).$$

Cependant, cette borne n'est pas toujours la meilleure possible. Par exemple les degrés en u et v des équations dans la Table 2.2 sont également des bornes supérieures, et sont parfois plus petites.

Le corps de fonctions de la courbe modulaire $X_1(N)$ possède deux générateurs f et g lorsque $N \geq 4$, s et t lorsque $N \geq 6$ et q et r lorsque $N \geq 8$.

Remarque 2.7. Le genre de $X_1(12)$ étant égal à 0, $\mathbb{C}(X_1(12))$ est un corps de fonctions rationnels. Voici une autre méthode pour déterminer un générateur. Nous remarquons que l'équation de $X_1(12)$ en termes de t et s peut s'écrire sous la forme :

$$(2s + t(t+1))^2 = (t-1)^2(t^2 + 4t - 4).$$

En écrivant

$$d = (2s + t(t+1))/(t-1),$$

nous remarquons que la conique

$$d^2 = t^2 + 4t - 4$$

est aussi un modèle de $X_1(12)$. Nous obtenons ainsi un paramètre rationnel en prennant le gradient u de la droite joignant le point $\big(-3, 5/3\big)$ à un point arbitaire (t, d) de la conique, ce qui montre que :

$$u = \frac{d-1}{t-1} = \frac{t^2 + 2s + 1}{(t-1)^2} \tag{2.42}$$

est un générateur de $\mathbb{C}\big(X_1(12)\big)$.

TAB. 2.1 – Les polynômes $\Phi_N^{(f,g)}$, $\Phi_N^{(t,s)}$, $\Phi_N^{(q,r)}$, $4 \leq N \leq 15$

N	g	$\Phi_N^{(f,g)}$	$\Phi_N^{(t,s)}$	$\Phi_N^{(q,r)}$
4	0	g		
5	0	$g-f$		
6	0	g^2-g+f	$s+1$	
7	0	g^3-fg+f^2	$t+s$	
8	0	$(f+1)g^2-3fg+2f^2$	$(s+2)t-1$	$q+1$
9	0	$g^5-g^4+(f+1)g^3-$ $3fg^2+3f^2g-f^3$	$t-(s^2+s+1)$	$r-q$
10	0	$g^5+fg^4-3fg^3+$ $(3f^2+f)g^2-2f^2g+f^3$	$(s^2+3s+1)t+s^2$	$(q^2+q-1)r$ $+q(q+2)$
11	1	$fg^7-(3f+1)g^6+3f(f+2)g^5$ $-9f^2g^4+f^2(4f-1)g^3+$ $3f^3g^2-3f^4g+f^5$	$t^2+s(s^2+3s+4)t-s$	$r^2+q^2r+(q^2+q)$
12	0	$g^6-(f-1)g^4-5fg^3+$ $f^2(f+10)g^2-9f^3g+3f^4$	$(s+3)t^2+(s-3)t+$ s^2+1	$(q+2)r+1$
13	2	$g^{10}+f^2g^9-6f(f+1)g^8$ $+f(5f^2+21f+3)g^7-$ $f(24f^2+13f+1)g^6+$ $3f^2(f+2)(3f+1)g^5-$ $15f^3(f+1)g^4+4f^4(f+5)g^3$ $-15f^5g^2+6f^6g-f^7$	t^3- $(s^4+5s^3+9s^2+4s+2)t^2$ $+(s^3+6s^2+3s+1)t+s^3$	$r^2-(q^3+q^2-1)r$ $-q(q+1)^2$
14	1	$fg^9-3fg^8+(4f^2+6f+1)g^7$ $-f(f^2+17f+10)g^6+$ $f(16f^2+30f+1)g^5-$ $5f^2(f^2+8f+1)g^4+$ $5f^3(5f+2)g^3-2f^4(3f+5)g^2$ $+f^5(5g-f)$	$(s^3+5s^2+6s+1)t^2$ $-(s^4+3s^3+6s^2+7s+1)t+s$	$(q^3+2q^2-q-1)r^2$ $+q(3q+2)r-$ $q^2(q+1)$
15	1	$g^{13}+(f-1)g^{12}+(f^2-3f+1)g^{11}$ $-(3f^2+2f+1)g^{10}+$ $(7f^3+19f^2+8f+1)g^9-$ $f(36f^2+37f+9)g^8+$ $f^2(18f^2+73f+36)g^7-$ $2f^3(31f+37)g^6+$ $f^3(19f^2+81f-1)g^5-$ $5f^4(9f-1)g^4+10f^5(f-1)g^3$ $+10f^6g^2-5f^7g+f^8$	t^3+ $s(s^4+7s^3+18s^2+19s+10)t^2$ $+s(s^4+4s^3-5s-5)t+$ $s(s^4+s^3+s^2+s+1)$	r^2+ $q(q-1)(q^2+3q+3)r$ $+q^2(q^2+3q+3)$

TAB. 2.2 – Les polynômes $\Phi_N^{(u,v)}$, $11 \leq N \leq 20$.

N	g	$\Phi_N(u,v)$	t	s
11	1	$v^2 - v - u^3 + u^2$	v	$-\dfrac{v+u-1}{u}$
12	0	$v^2 + 2uv + u$	$\dfrac{v^2+v+u}{u}$	$\dfrac{v-u+1}{u}$
13	2	$u^2 - (v^3+v+1)u - v^4(v+1)$	$\dfrac{v}{u^4}+1$	$\dfrac{(1-u)v+u^4}{vu-u^4}$
14	1	$v^2 + uv - (u^3 - 3u^2 + 2u)$	$\dfrac{(v^4+3uv^3-u^2(u-6)v^2-u^3(2u-7)v-u^4(u-2))}{(uv^3+5u^2v^2+6u^3v+u^4)}$	$\dfrac{v}{u}$
15	1	$v^2 + (u+1)v - u^2(u+1)$	$\dfrac{u^6+u^5-vu^4-2v^2u^3+v^3u+v^4}{u^5}$	$\dfrac{v^2-u^3-u^2}{u^2+vu}$
16	2	$v^2 + (u-1)(u^2-2u-1)v -$ $u^2(u-1)(u^2-2u-1)$	$-\dfrac{v^2-(u-1)(2u+1)v+u^4-u^3}{v}$	$\dfrac{v-u^2+1}{u-1}$
17	5	$v^4 + (2u^2-3u-3)v^3 + (u^4-4u^3+6u+3)v^2$ $-(u^5-2u^4-u^3+u^2+4u+1)v + u$	$\dfrac{v+u^2-u}{v}$	$\dfrac{2u-v-u^2}{v-u}$
18	2	$v^2 - (u^3+2u^2+3u+1)v + u(u+1)^2$	$\dfrac{(u+1)^2+uv}{(u+1)^2+(2u+1)v-v^2}$	$-\dfrac{(u+1)^2-v}{v^2-uv-(u+1)^2}$
19	7	$v^5 + (u^6+4u^5+3u^4-5u^3-4u^2+2)v^4 +$ $(2u^6+11u^5+18u^4-u^3-12u^2-4u+1)v^3 +$ $u(u^5+7u^4+21u^3+15u^2-2u-3)v^2 -$ $u^2(u+1)(u^2-4u-3)v - u^3(u+1)^2$	$\dfrac{(v^3+v^2-(u-1)v+(u-1)^2}{(v^2+u-1)(u-1)}$	$\dfrac{v^2+v-u+1}{u-1}$
20	3	$v^3 - u(2u-3)v^2 + (u-1)(u^3-2u^2-u-1)v$ $+u(u-1)(u^2-u-1)$	$\dfrac{(u^2-u+1)v+u^2}{v(u-1)^2}$	$\dfrac{-uv-2u+1}{(u-1)(v+1)}$

TAB. 2.3 – Le degré en r, en q et le degré total de $\Phi_N^{(q,r)}$, $16 \leq N \leq 51$.

N	g	$\deg_r \Phi_N^{(q,r)}$	$\deg_q \Phi_N^{(q,r)}$	$\deg_{\text{total}} \Phi_N^{(q,r)}$	N	g	$\deg_r \Phi_N^{(q,r)}$	$\deg_q \Phi_N^{(q,r)}$	$\deg_{\text{total}} \Phi_N^{(q,r)}$
16	2	3	3	5	34	21	11	16	23
17	5	4	5	8	35	25	15	21	32
18	2	3	4	6	36	17	11	16	23
19	7	5	6	10	37	40	18	24	37
20	3	3	5	6	38	28	14	20	29
21	5	5	7	11	39	33	18	24	37
22	6	4	7	11	40	25	16	20	32
23	12	7	9	14	41	51	22	30	45
24	5	6	7	11	42	25	15	20	30
25	12	8	11	16	43	57	24	33	49
26	10	7	9	15	44	36	19	25	39
27	13	8	12	17	45	41	23	31	47
28	10	7	10	15	46	45	21	29	44
29	22	11	15	22	47	70	29	39	59
30	9	8	9	15	48	37	19	28	41
31	26	13	17	26	49	69	31	42	64
32	17	10	14	21	50	48	23	32	48
33	21	12	17	26	51	65	30	41	62

Chapitre 3

Courbes de genre deux à bonne réduction partout.

Dans ce chapitre, nous nous proposons de construire des courbes de genre deux à bonne réduction partout sur des corps quartiques et à bonne réduction tordue partout sur des corps quadratiques. Il découle des travaux de Fontaine et d'Abrashkin [1], [10] qu'il n'existe pas de telles courbes sur $\mathbb{Q}$.

3.1 Premiers résultats

Soit C une courbe (projective, lisse) de genre deux sur un corps de nombres K. Alors C admet un modèle affine de la forme $y^2 = P(x)$ où P est un polynôme de degré 5 ou 6 à coefficients dans K et toutes les racines sont simples. Soit $\mathfrak{p}$ un idéal premier de caractéristique résiduelle impaire d'un corps de nombres K. La courbe C a bonne réduction en $\mathfrak{p}$ si et seulement si nous pouvons choisir $P(x)$ à coefficients dans l'anneau local $\mathcal{O}_\mathfrak{p}$ en $\mathfrak{p}$ de sorte qu'il reste sans facteur carré après réduction (mod $\mathfrak{p}$). Ce qui est équivalent à : le discriminant de P est un élément inversible de $\mathcal{O}_\mathfrak{p}$. Lorsque la caractéristique résiduelle de $\mathfrak{p}$ est 2, nous aurons besoin d'utiliser un modèle de la forme

$$y^2 + Q(x)y = P(x), \tag{3.1}$$

où les polynômes P et Q sont à coefficients dans $\mathcal{O}_\mathfrak{p}$ et $P + Q^2/4$ est de degré 5 ou 6 sans facteur carré et sans racines multiples. La courbe C a bonne réduction en $\mathfrak{p}$ si et seulement si nous pouvons choisir P et Q de sorte que 2^8 fois le discriminant de $P + Q^2/4$ est un élément inversible de $\mathcal{O}_\mathfrak{p}$.

Afin d'avoir une notation uniforme, nous écrivons Δ_C pour 2^8 fois le discriminant de $P + Q^2/4$ (Pour plus de détails, voir l'article de Lockhart [21]).

Le discriminant Δ_C dépend du choix des polynômes P et Q et non seulement de la courbe C.

Un modèle de la forme (3.1) est appelé un modèle de Weierstrass de la courbe C de genre deux.

Notons par $\mathcal{O}_K$ l'anneau des entiers de K. D'après le paragraphe précédent, si la courbe C a un modèle de Weierstrass (3.1) avec P et Q à coefficients dans $\mathcal{O}_K$ tels que Δ_C est un élément inversible de $\mathcal{O}_K$, alors C a bonne réduction partout.

Nous nous proposons de construire des courbes de genre deux à bonne réduction partout sur des corps quartiques et à bonne réduction tordue partout sur des corps quadratiques.

Proposition 3.1. *Soit p, $b \in K$ et soit C de modèle de Weierstrass*

$$y^2 + (px^2 + px)y = x^5 + \left(\tfrac{b+5}{2}\right)x^4 + bx^3 + \left(\tfrac{b-5}{2}\right)x^2 - x. \tag{3.2}$$

Alors $\Delta_C = ((p^2 + 2b)^2 + 108)^2$.

Ce résultat se vérifie par un calcul, et mène à la construction suivante d'une famille infinie de courbes de genre deux à bonne réduction partout sur des corps de nombres quartiques.

Proposition 3.2. *Soient un entier impair b et un nombre algébrique p tels que ou bien $(p^2 + 2b)^2 = -107$ ou bien $(p^2 + 2b)^2 = -109$ est vérifiée. Soit un corps de nombres K engendré sur $\mathbb{Q}$ par p. Alors la courbe* (3.2) *a bonne réduction partout sur K.*

Puisque b est un entier rationnel, il est clair que p appartient à $\mathcal{O}_K$ et, puisque b est impair, (3.2) est à coefficients dans $\mathcal{O}_K$. La condition suivante

$$(p^2 + 2b)^2 = -107 \quad \text{ou} \quad -109 \tag{3.3}$$

entraîne $\Delta_C = 1$.

Le corps K est une extension quartique de $\mathbb{Q}$. Le groupe de Galois de sa clôture galoisienne est le groupe diédral d'ordre 8. Puisque nous ne connaissons pas d'exemples de courbes de genre deux à bonne réduction partout sur un corps de nombres de degré 2 ou 3, les corps K de la proposition 3.2 semblent être des corps de plus petit degré connus sur lesquels nous connaissons des exemples de courbes de genre deux à bonne réduction partout.

Le reste de ce chapitre est consacré à l'étude des propriétés diverses de ces courbes ainsi que leur utilisation pour construire des courbes de genre deux avec différentes propriétés arithmétiques.

En écrivant

$$w = p^2 + 2b \qquad \text{et} \qquad Y = y + \frac{1}{2}(px^2 + px), \tag{3.4}$$

nous remarquons que la courbe C d'équation (3.2) est isomorphe à

$$Y^2 = x(x+1)\big(x^3 + \tfrac{1}{4}(w+6)x^2 + \tfrac{1}{4}(w-6)x - 1\big). \tag{3.5}$$

De plus, $\Delta_C = (w^2 + 108)^2$.

Définition 3.1. *Soit X est une variété projective lisse sur un corps de nombres K. Une tordue de X est une seconde variété projective lisse sur K isomorphe à X sur une extension finie de K.*

Définition 3.2. *Soit X une variété projective lisse sur un corps de nombres K. La variété X a bonne réduction tordue partout si, pour un premier donné $\mathfrak{p}$ de K, il existe une tordue de X qui a bonne réduction en $\mathfrak{p}$.*

En se spécialisant aux cas $w^2 = -107$, et $w^2 = -109$, nous donnerons deux constructions qui mènent au résultat suivant :

Théorème 3.1. *Il existe une infinité de courbes de genre deux sur des corps quadratiques à bonne réduction tordue partout.*

3.2 Bonne réduction tordue.

Soit K un corps de nombres et $\mathfrak{p}$ un idéal premier de K. Comme dans l'introduction, la variété projective lisse X définie sur K a *bonne réduction tordue* en $\mathfrak{p}$ s'il existe une tordue de X à bonne réduction en $\mathfrak{p}$. D'après le critère de la jacobienne appliqué à n'importe quel modèle lisse de X, la variété X a bonne réduction en dehors d'un ensemble fini de premiers. Si X n'a pas bonne réduction en $\mathfrak{p}$ et si l'une des tordues X' de X a bonne réduction en $\mathfrak{p}$, alors X' devient isomorphe à X sur une extension finie de K, pour que X acquiert bonne réduction sur K. Cela signifie que X a *bonne réduction potentielle* en $\mathfrak{p}$.

Soit Σ un ensemble de premiers de K. En réitérant cette procédure, nous déduisons que si X a bonne réduction tordue en tout premier de K qui n'appartient pas à Σ, alors X a *bonne réduction potentielle* en dehors de Σ,

c'est-à-dire qu'elle acquiert bonne réduction en tout premier de K sur une extension finie de K.

Dans toute la suite, nous désignons par C soit une courbe soit une variété abélienne.

Soit C une courbe de genre $g \geq 1$. Si la courbe C a bonne réduction en $\mathfrak{p}$, alors la variété jacobienne J_C de C a bonne réduction en $\mathfrak{p}$. La réciproque est fausse en général ; si C est une courbe de genre deux, alors J_C a bonne réduction lorsque C est la réunion de deux courbes de genre un se coupant en un point. Par conséquent, nous ne pouvons pas utiliser des surfaces abéliennes à bonne réduction partout pour construire des courbes de genre deux à bonne réduction partout.

Soit une courbe elliptique E/K, et fixons un modèle de Weiestrass

$$E : y^2 = x^3 + ax + b, \qquad a,\ b \in K. \tag{3.6}$$

Nous savons que, si $ab \neq 0$, chaque tordue de E a un modèle de Weierstrass de la forme

$$E_d : y^2 = x^3 + d^2ax + d^3b \quad \text{où} \quad d \in K^\times. \tag{3.7}$$

Deux tordues E_d et $E_{d'}$ sont K-isomorphes si et seulement si d'/d est un carré dans K. En général, E_d est isomorphe à E sur $K(\sqrt{d})$, et E_d est appelée *tordue de E par $K(\sqrt{d})$*.

Lorsque $a = 0$, chaque tordue de E a un modèle de la forme

$$y^2 = x^3 + db \quad \text{avec} \quad d \in K^\times \tag{3.8}$$

et devient isomorphe à E sur $K(\sqrt[6]{d})$.

Lorsque $b = 0$, chaque tordue de E a un modèle de la forme

$$y^2 = x^3 + dax \quad \text{avec} \quad d \in K^\times \tag{3.9}$$

et devient isomorphe à E sur $K(\sqrt[4]{d})$.

Ces cas correspondent respectivement aux courbes elliptiques dont l'invariant j est égal soit à 1728 soit à 0.

Soit un premier $\mathfrak{p}$ de K et soit $\mathcal{O}_\mathfrak{p}$ l'anneau des entiers de K en $\mathfrak{p}$. Soit E/K une courbe elliptique d'équation de Weierstrass généralisée

$$E : \quad y^2 + (a_1x + a_3)y = x^3 + a_2x^2 + a_4x + a_6 \tag{3.10}$$

où $a_i \in \mathcal{O}_\mathfrak{p}$ pour tout $i \in \{1, 2, 3, 4, 6\}$.

Notons par $\Delta_\mathfrak{p} \in \mathcal{O}_\mathfrak{p}$ le discriminant de ce modèle et par $v_E(\mathfrak{p})$ la valuation $\mathfrak{p}$-adique de $\Delta_\mathfrak{p}$. Si $\Delta'_\mathfrak{p}$ est le discriminant d'un second modèle de Weierstrass sur $\mathcal{O}_\mathfrak{p}$ et $v'_E(\mathfrak{p})$ sa valuation $\mathfrak{p}$-adique, alors $v'_E(\mathfrak{p}) \equiv v_E(\mathfrak{p}) \pmod{12}$. La courbe elliptique E a bonne réduction en $\mathfrak{p}$ si et seulement si, il existe un modèle (3.10) avec $v_E(\mathfrak{p}) = 0$.

Supposons que E a un modèle de Weierstrass (3.6), et que l'invariant modulaire j de E est différent de 0 et de 1728. Si E a bonne réduction tordue en $\mathfrak{p}$, alors E acquiert bonne réduction sur une extension quadratique L de K. Si $\mathfrak{P}$ est un premier de L divisant $\mathfrak{p}$ alors, d'après ce qui précède

$$v_E(\mathfrak{P}) \equiv 0 \pmod{12}.$$

Il s'ensuit que $v_E(\mathfrak{p}) \equiv 0 \pmod 6$ (et en effet, $v_E(\mathfrak{p}) \equiv 0 \pmod{12}$ si $\mathfrak{p}$ est non-ramifié dans L).

Lorsque $\mathfrak{p}$ parcourt tous les premiers de K, nous obtenons le résultat

Lemme 3.1. *Soit un ensemble fini Σ de premiers de K et soit une courbe elliptique E d'équation (3.6), et de discriminant $D = 16(4a^3+27b^2)$. Supposons que $ab \neq 0$ et que E a bonne réduction tordue partout, alors D est la puissance sixième d'un $\mathcal{O}_{K,\Sigma}$-ideal fractionnaire de K.*

Notons par $\mathcal{O}_{K,\Sigma}$ l'anneau des éléments de K qui sont entiers en tout premier de K qui n'appartient pas à Σ. Nous utilisons le lemme précédent pour démontrer les résultats suivants, en utilisant l'argument de Shafarevich [29] qui montre qu'il n'existe pas de courbes elliptiques à bonne réduction partout sur $\mathbb{Q}$ et que seulement un nombre fini de classes d'isomorphismes de courbes elliptiques sur un corps de nombres K a bonne réduction partout en dehors d'un ensemble fini de premiers de K.

Théorème 3.2. *Il n'existe pas de courbes elliptiques sur $\mathbb{Q}$ à bonne réduction tordue partout.*

Preuve. Considérons à nouveau les courbes elliptiques de modèle de Weierstrass (3.6). Supposons (dans la preuve) que a, $b \in \mathbb{Q}$ et que Σ est vide.

Si $a = 0$, alors chaque tordue de E est de la forme $y^2 = x^3 + b$, et le discriminant est $16 \cdot 27b^2$. Mais une telle courbe ne peut avoir bonne réduction en 3, puisque la valuation 3-adique de $16 \cdot 27b^2$ est impaire pour tout $b \in \mathbb{Q}^\times$ et, par conséquent, elle ne peut pas être divisible par 12.

Si $b = 0$, alors chaque tordue de E est de la forme

$$y^2 = x^3 + ax \quad \text{avec} \quad a \in \mathbb{Q}^\times. \tag{3.11}$$

Posons $a = 2^m A$, avec A une unité en 2 et supposons que $0 \leq m \leq 3$. Le discriminant est maintenant $2^{6+3m}A^3$. Puisque $v_E(2) \equiv 0 \pmod{12}$, alors $m = 2$. L'algorithme de Tate [34] montre que E ne peux avoir bonne réduction en 2.

Supposons alors que $ab \neq 0$. Le Lemme 3.1 montre qu'il existe $d \in \mathbb{Q}^\times$ tel que $D = \epsilon d^6$ et

$$16(4a^3 + 27b^2) = \epsilon d^6 \quad \text{où} \quad \epsilon \in \{\pm 1\}. \tag{3.12}$$

En posant

$$\xi = -(3 \cdot 2^2 \cdot a)/d^2, \quad \eta = (3^3 \cdot 2^2 \cdot b)/d^3, \tag{3.13}$$

nous obtenons

$$\eta^2 = \xi^3 + 27\epsilon \quad \text{où} \quad \epsilon \in \{\pm 1\}. \tag{3.14}$$

Donc (ξ, η) est un point rationnel sur l'une des courbes elliptiques

$$y^2 = x^3 + 27\epsilon.$$

Le rang de ces deux courbes est 0 et que la torsion rationnelle est d'ordre 2. Il en résulte que $(\xi, \eta) = (3\epsilon, 0)$ où $\epsilon \in \{\pm 1\}$ et par conséquent $b = 0$, un cas qui a été déjà exclu. □

Puisque deux courbes elliptiques sont des tordues l'une de l'autre si et seulement si leurs invariants modulaires sont égaux, il est naturel donc de considérer la bonne réduction tordue comme une propriété de l'invariant modulaire.

Théorème 3.3. *Soit K un corps de nombres et Σ un ensemble fini d'idéaux premiers de K. Alors, il n'existe qu'un nombre fini de $j \in K$ qui sont des invariants modulaires de courbes elliptiques à bonne réduction tordue en tout idéal premier de K n'appartenant pas à Σ.*

Preuve. Commençons par élargir Σ de sorte que l'anneau $\mathcal{O}_{K,\Sigma}$ des Σ-entiers soit un anneau principal.

Soit E/K une courbe elliptique, à bonne réduction tordue en dehors de Σ. Alors E a un modèle de Weierstrass de la forme (3.6) sur $\mathcal{O}_{K,\Sigma}$. Nous pouvons supposer que $ab \neq 0$. En effet, si $ab = 0$ alors l'invariant j est soit 0 soit 1728.

D'après le Lemme 3.1, le discriminant D de la courbe elliptique E est de la forme ϵd^6, où ϵ appartient au groupe des éléments inversibles $\mathcal{O}_{K,\Sigma}^{\times}$ de $\mathcal{O}_{K,\Sigma}$, et $0 \neq d \in \mathcal{O}_{K,\Sigma}$.

Comme dans la preuve du Théorème 3.10, en posant

$$\xi = -(3 \cdot 2^2 \cdot a)/d^2 \quad \text{et} \quad \eta = -(3^3 \cdot 2^2 \cdot b)/d^3, \tag{3.15}$$

de sorte que

$$\eta^2 = \xi^3 + 27\epsilon \tag{3.16}$$

et tel que (ξ, η) soit un point K-rationnel de la courbe elliptique C_ϵ d'équation $y^2 = x^3 + 27\epsilon$.

Maintenant, si ϵ' appartient à $\mathcal{O}_{K,\Sigma}^{\times}$, alors les deux courbes C_ϵ et $C_{\epsilon'}$ sont K-isomorphes si et seulement si ϵ'/ϵ est une puissance sixième dans K.

Nous aurons besoin seulement de considérer les courbes C_ϵ lorsque ϵ parcourt un ensemble de représentants du groupe fini $\mathcal{O}_{K,\Sigma}^{\times}/(\mathcal{O}_{K,\Sigma}^{\times})^6$, (il s'agit d'un ensemble fini de courbes).

Choisissons ϵ tel que $(\xi, \eta) \in C_\epsilon$.

Nous rappelons que l'invariant j_E de E est défini par la formule

$$j_E = 1728(64a^3)/D \tag{3.17}$$

Il s'ensuit que

$$j_E = -2^6\xi^3/\epsilon.$$

De plus, puisque E a bonne réduction potentielle en dehors de Σ, alors j_E appartient à $\mathcal{O}_{K,\Sigma}$.

Puisque les premiers de K divisant 2 appartiennent à Σ, nous constatons que $\xi \in \mathcal{O}_{K,\Sigma}$. Mais, par un théorème de Siegel [31], C_ϵ n'a qu'un nombre fini de points (ξ, η) tels que $\xi \in \mathcal{O}_{K,\Sigma}$. Il s'ensuit qu'il n'existe qu'un nombre fini de possibilités pour j_E. □

Il est naturel de se demander si les Théorèmes 3.10 et 3.3 peuvent se généraliser aux courbes de genre supérieur ou aux variétés abéliennes de dimension supérieure. Dans § 3.4 et § 3.5 nous allons construire des exemples de courbes de genre deux à bonne réduction tordue partout sur certains corps quadratiques.

3.3 La courbe C_w sur $K(w)$.

Soit un corps K de caractéristique différente de 2 et 3. Soit w une indeterminée et $\mathcal{F}$ le corps de fonctions rationnelles de $K(w)$.

Dans cette section, nous citons quelques propriétés de la courbe de genre deux (3.5) de l'introduction, vue comme courbe sur $\mathcal{F}$. Fixons une clôture algébrique Ω de $\mathcal{F}$. Il est commode de remplacer x par $x-1$ de sorte que l'équation de C_w devient

$$y^2 = x(x-1)W(x) \quad \text{où} \qquad W(x) = x^3 + \frac{1}{4}(w-6)x^2 - \frac{1}{4}(w+6)x + 1 \tag{3.18}$$

Le discriminant de W est $(w^2+108)^2$. Si α est l'une des racines de W dans Ω, alors les autres racines sont $1/(1-\alpha)$ et $1-1/\alpha$. En utilisant le fait que le coefficient de x^2 dans W est moins la somme des racines de W, nous obtenons

$$w = 2\frac{(\alpha-2)(\alpha+1)(2\alpha-1)}{\alpha(\alpha-1)}, \qquad w^2+108 = \frac{(\alpha^2-\alpha+1)^3}{\alpha^2(\alpha-1)^2} \tag{3.19}$$

Lemme 3.2. *Le polynôme W est irréductible et séparé sur $\mathcal{F}$ avec un groupe de Galois cyclique.*

Preuve. Supposons que W est réductible. Puisque W est de degré 3, l'une de ses racines, α par exemple, appartient à $\mathcal{F}$. Il s'ensuit alors que les autres racines $1/(1-\alpha)$ et $1-1/\alpha$ appartiennent aussi à $\mathcal{F}$.

D'autre part, W est un polynôme unitaire à coefficients dans l'anneau $K[w]$ qui est intégralement clos dans F. Il s'ensuit que α et $1-1/\alpha$ sont toutes les deux des polynômes en w, et cela ne peut arriver que si $\alpha \in K$. Donc

$$W(\alpha) = (\frac{\alpha^2}{4} - \frac{\alpha}{4})w + (\alpha^3 - \frac{3}{2}\alpha^2 - \frac{3}{2}\alpha + 1) \tag{3.20}$$

est le polynôme identiquement nul.

La comparaison des coefficients de w montre que soit $\alpha = 0$ soit $\alpha = 1$, aucun des deux n'annule le coefficient constant. Ce qui montre que W est irréductible. Puisque son discriminant est un carré non-nul, il s'ensuit que W est séparable de groupe de Galois cyclique. □

La courbe C_w possède un automorphisme d'ordre 3, défini par

$$(x,y) \mapsto \big(\frac{1}{1-x}, \frac{y}{(1-x)^3}\big) \tag{3.21}$$

D'aprés Bolza [3], la courbe C_w a aussi un automorphisme ι d'ordre deux, différent de l'involution hyperelliptique. Un tel automorphisme transforme l'ensemble des points de Weierstrass $\{\infty, (0,0), (1,0)\}$ en l'ensemble des points de Weierstrass $\{(\alpha,0), (1/(1-\alpha),0), (1-1/\alpha,0)\}$.

Cet automorphisme est défini, à composition près avec l'involution hyperelliptique, par

$$x \mapsto \frac{\alpha x + 1 - \alpha}{x - \alpha}, \qquad y \mapsto \frac{4y}{(\alpha(\alpha-1)u)^3} \tag{3.22}$$

où u est une racine carrée de $4w^2/(w^2+108)$ dans Ω. Puisque K est de caractéristique différente de 2 et 3, w^2+108 n'est pas un carré de $\mathcal{F}$. Donc, $\mathcal{F}(u)$ est une extension quadratique de $\mathcal{F}$ et $\mathcal{F}(\alpha,u)$ est une extension galoisienne de degré 6 de $\mathcal{F}$, dont le groupe de Galois est cyclique.

Proposition 3.3. *Nous conservons les notations introduites dans le paragraphe précédent.*

1. *Soit J_w la variété jacobienne de C_w. Alors J_w devient isogène, sur l'extension cyclique de degré 6, $\mathcal{F}(\alpha,u)$ de $\mathcal{F}$, au produit de deux courbes elliptiques.*
2. *Lorsque $K = \mathbb{Q}$, J_w n'est pas isogène au produit de deux courbes elliptiques sur aucune extension de $\mathcal{F}$ de degré strictement inférieur à 6.*

Preuve. (1) Nous avons déjà vu que $\mathcal{F}(\alpha,u)$ est une extension cyclique de degré 6 de $\mathcal{F}$. Soit ι l'automorphisme d'ordre 2 de la courbe C_w définie par (3.22), alors ι est rationnel sur $\mathcal{F}(\alpha,u)$. La courbe quotient E_w de C_w par le groupe engendré par ι est de genre un, et puisque $C_w(\mathcal{F})$ et, par conséquent, $C_w(\mathcal{F}(\alpha,u))$ est non vide, alors $E_w(\mathcal{F}(\alpha,u))$ est non vide. Donc E_w peut être munie d'une structure de courbe elliptique. D'après la propriété d'Albanese des jacobiennes, l'application des quotients $C_w \to E_w$ peut être prolongée en un homomorphism $\phi : J_w \to E_w$. Mais alors J_w est isogène sur $\mathcal{F}(\alpha,u)$ à $E_w \times E'_w$, où E'_w est la composante connexe de l'identité de $\ker\phi$, qui est une courbe elliptique.

(2) Il suffit de montrer que J_w admet une spécialisation J_{w_0} qui n'est pas isogène au produit de courbes elliptiques sur une extension de $\mathbb{Q}(w_0)$ de degré strictement inférieur à 6.

En effet, prennons $w_0 = \sqrt{-109}$. Le premier 11 se décompose dans $\mathbb{Q}(\sqrt{-109})$ et la courbe $C_{\sqrt{-109}}$ a bonne réduction aux premiers de $\mathcal{F}$ au dessus de 11.

Le même procédé est encore vrai pour $J_{\sqrt{-109}}$. Soit L une extension finie de $\mathbb{Q}(\sqrt{-109})$, soit $\mathfrak{P}$ un premier de L divisant 11, et soit $K_{\mathfrak{P}}$ le corps résiduel de L en $\mathfrak{P}$.

Soit $\phi : J_{w_0} \to E \times E'$ une isogénie définie sur L, avec E et E' des courbes elliptiques sur L, alors E et E' auront bonne réduction en $\mathfrak{P}$ et ϕ induirait une isogénie entre les fibres

$$J_{\mathfrak{P}} \quad \text{de} \quad J_{\sqrt{-109}} \quad \text{et} \quad E_{\mathfrak{P}} \times E'_{\mathfrak{P}} \quad \text{de} \quad E \times E' \quad \text{sur } K_{\mathfrak{P}}.$$

Maintenant, $K_{\mathfrak{P}}$ est un corps fini. D'après la théorie des endomorphismes de Frobenius, deux variétés abéliennes isogènes sur un corps fini ont le même polynôme caractéristique. Par conséquent, l'existence d'une isogénie

$$J_{\mathfrak{P}} \to E_{\mathfrak{P}} \times E'_{\mathfrak{P}}$$

entraîne que le polynôme caractéristique $\chi_{L,\mathfrak{P}}(t) \in \mathbb{Q}[t]$ de l'endomorphisme de Frobenius de $J_{\mathfrak{P}}$ est le produit de celui de $E_{\mathfrak{P}}$ et de celui de $E'_{\mathfrak{P}}$. Ce qui à son tour entraîne que $\chi_{L,\mathfrak{P}}(t)$ se factorise dans $\mathbb{Q}[t]$ en produit de deux polynômes quadratiques.

Une méthode pour calculer $\chi_{L,\mathfrak{P}}(t)$ est expliquée dans [18] et rappelée dans le § 1.4. En l'appliquant lorsque $L = \mathbb{Q}(\sqrt{-109})$, nous obtenons

$$\chi_{\mathbb{Q}(\sqrt{-109}),\mathfrak{P}}(t) = t^4 + 9t^3 + 38t^2 + 99t + 121,$$

qui est irréductible dans $\mathbb{Q}[t]$. (Voir l'Appendice § 3.6 pour plus de détail sur ces calculs).

Soit L une extension finie de $\mathbb{Q}(\sqrt{-109})$, et soit d le degré de la classe résiduelle de L sur $\mathbb{Q}(\sqrt{-109})$ en $\mathfrak{P}$.

Supposons le polynôme $\chi_{\mathbb{Q}(\sqrt{-109}),\mathfrak{P}}(t)$ se factorise sous la forme

$$\chi_{\mathbb{Q}(\sqrt{-109}),\mathfrak{P}}(t) = (t-\alpha)(t-\beta)(t-\gamma)(t-\delta),$$

où α, β, γ, $\delta \in \mathbb{C}$, alors

$$\chi_{L,\mathfrak{P}}(t) = (t-\alpha^d)(t-\beta^d)(t-\gamma^d)(t-\delta^d).$$

Les coefficients de $\chi_{L,\mathfrak{P}}(t)$ sont alors calculés comme fonctions symétriques de α, β, γ et δ et les calculs montrent que $\chi_{L,\mathfrak{P}}(t)$ est irréductible lorsque $d \leq 5$.

□

TAB. 3.1 – Invariants d'Igusa de la courbe C_w.

C	$J_2^5 J_{10}^{-1}$	$J_4^5 J_{10}^{-2}$	$J_6^5 J_{10}^{-3}$	$J_8^5 J_{10}^{-4}$
C_w	$\frac{(w^2+120)^5}{(w^2+108)^2}$	$243\frac{(w^2+110)^5}{(w^2+108)^4}$	$-\frac{(3w^2+320)^5}{(w^2+108)^6}$	$-\frac{(3w^4+665w^2+36825)^5}{(w^2+108)^8}$
$C_{\sqrt{-107}}$	13^5	3^{10}	1	-17^5
$C_{\sqrt{-109}}$	11^5	3^5	7^5	17^5

Terminons cette section en remarquant que C_w a une tordue définie sur $K(w^2)$. En effet, notons que la substitution de x par $x+\frac{1}{2}$ dans $x(x-1)W(x)$ montre que C_w possède aussi un modèle de la forme

$$y^2 = x^5 + \frac{1}{4}wx^4 - \frac{5}{2}x^3 - \frac{1}{8}wx^2 + \frac{9}{16}x + \frac{1}{64}w. \tag{3.23}$$

En remplaçant x par x/w, en multipliant par w^5 et enfin en remplaçant w^2 par v nous obtenons le résultat suivant

Proposition 3.4. *Soit $v = w^2$. La courbe projective lisse $\mathcal{X}_v$ sur $K(v)$ définie par l'équation affine*

$$\mathcal{X}_v : \quad y^2 = x^5 + \frac{1}{4}vx^4 - \frac{5}{2}vx^3 - \frac{1}{8}v^2x^2 + \frac{9}{16}v^2x + \frac{1}{64}v^3$$

est isomorphe à C_w sur $\mathcal{F}(\sqrt{w})$.

Remarque 3.4. Lorsque le corps $\mathcal{F}$ est égale à $\mathbb{C}$, un résultat classique de Bolza [3], montre qu'il existe $u \in \Omega$ telle que C_w est isomorphe à la courbe

$$y^2 = x^6 + ux^3 + 1.$$

Un calcul montre que c'est vrai dans notre situation, avec

$$u^2 = 4w^2/(w^2+108)$$

comme ci-dessus.

Remarque 3.5. Pour montrer que les deux courbes de genre deux C_{107} et C_{109} ne sont pas isomorphes, nous calculons les invariants d'Igusa, qui sont définis dans [12]. Leur calcul a été effectué à l'aide d'un programme sous Pari-gp préparé par F. Rodriguez-Villegas. Rappelons que les j-invariants d'Igusa déterminent la courbe à K^{alg}-isomorphismes près.

D'après la Table 3.1, les invariants d'Igusa de la courbe C_w où

$$w \in \{\sqrt{-107}, \sqrt{-109}\}$$

sont des entiers et donc en particulier des entiers algébriques, une propriété qui caractérise les courbes de genre deux sur $\mathbb{Q}^{alg}$ à bonne réduction potentielle partout.

Les invariants d'Igusa des courbes $C_{\sqrt{-107}}$ et $C_{\sqrt{-109}}$ sont différents, donc ces deux courbes ne sont pas isomorphes.

3.4 La courbe $C_{\sqrt{-107}}$ et ses tordues.

Dans cette section, nous restreignons l'étude au cas $w = \sqrt{-107}$, et nous écrivons $C_{\sqrt{-107}}$ pour la courbe correspondante (3.5) ou (3.23) qui est définie sur $\mathbb{Q}(\sqrt{-107})$, et a pour discriminant 1. Puisque ces coefficients sont des entiers algébriques en dehors de 2, la courbe $C_{\sqrt{-107}}$ a bonne réduction en dehors de 2.

D'autre part, nous pouvons détérminer la $\sqrt[4]{-107}$-tordue de $C_{\sqrt{-107}}$ comme dans la Proposition 3.4. Ce qui donne la courbe $\mathcal{X}_{-107}$ définie sur $\mathbb{Q}$ par l'équation

$$\mathcal{X}_{-107}: \quad y^2 = x^5 - \frac{107}{4}x^4 + \frac{535}{2}x^3 - \frac{11449}{8}x^2 + \frac{103041}{16}x - \frac{1225043}{64}$$

qui a bonne réduction en dehors de 2 et 107. Tordre $\mathcal{X}_{-107}$ par $\sqrt{-1}$, donne la courbe $\mathcal{X}'_{-107}$

$$\mathcal{X}'_{-107}: \quad y^2 = x^5 + \frac{107}{4}x^4 + \frac{535}{2}x^3 + \frac{11449}{8}x^2 + \frac{103041}{16}x + \frac{1225043}{64}$$

avec $\Delta_{\mathcal{X}'_{-107}} = 107^{10}$.

L'avantage est que cette courbe a bonne réduction en 2. En effet, en remplaçant x by $x - \frac{1}{2}$ et y par $y + \frac{x^2+x+1}{2}$ nous obtenons l'équation

$$y^2 + (x^2 + x + 1)y = x^5 + 24x^4 + 216x^3 + 1068x^2 + 5196x + 16247 \quad (3.24)$$

avec des coefficients entiers.

Puisque la courbe $C_{\sqrt{-107}}$ a bonne réduction en dehors de $\sqrt{-107}$, et $\mathcal{X}'_{-107}$, vue comme une courbe sur $\mathbb{Q}(\sqrt{-107})$, est une tordue de $C_{\sqrt{-107}}$ et a bonne réduction en dehors de 2, nous en déduisons que $C_{\sqrt{-107}}$ a bonne réduction tordue partout sur $\mathbb{Q}(\sqrt{-107})$.

Nous pouvons généraliser cette construction et démontrer le résultat suivant

Théorème 3.6. *Soit m un entier sans facteur carré non nul, premier à 107 et soit $\mathcal{F}=\mathbb{Q}(\sqrt{-107m})$. Alors $\mathcal{X}_{-107}$ acquiert bonne réduction tordue partout sur $\mathcal{F}$.*

Preuve. Puisque $\mathcal{X}'_{-107}$ est une tordue de $\mathcal{X}_{-107}$ qui a bonne réduction en dehors de 107, nous avons besoin de considérer seulement les premiers de $\mathcal{F}$ au dessus de 107. Soit $\alpha=\sqrt{-107m}$. Alors la tordue $\mathcal{X}^{(\alpha)}_{-107}$ de $\mathcal{X}_{-107}$ par $\sqrt{\alpha}$ sur $\mathcal{F}$ a une équation de la forme

$$\mathcal{X}^{(\alpha)}_{-107}: \quad y^2=x^5-\frac{107}{4\alpha}x^4+\frac{535}{2\alpha^2}x^3-\frac{11449}{8\alpha^3}x^2+\frac{103041}{16\alpha^4}x-\frac{1225043}{64\alpha^5} \quad (3.25)$$

de sorte que $\Delta_{\mathcal{X}^{(\alpha)}_{-107}}=107^{10}/\alpha^{20}=1/m^{10}$. D'après la construction de α, ce modèle est entier en 107 et $\Delta_{\mathcal{X}^{(\alpha)}_{-107}}$ est une unité en 107. Par conséquent $\mathcal{X}^{(\alpha)}_{-107}$ a bonne réduction en 107. □

Remarque 3.7. Lorsque $w=\sqrt{-107}$, une racine du polynôme $W(x)$ de (3.18) engendre le corps de classes de Hilbert du corps $\mathbb{Q}(\sqrt{-107})$. Par conséquent, la 2-torsion sur la Jacobienne de $C_{\sqrt{-107}}$ est rationnelle sur le corps de classes de Hilbert L de $\mathbb{Q}(\sqrt{-107})$. Dans ce cas, la Jacobienne de $C_{\sqrt{-107}}$ aussi devient isogène au produit de deux courbes elliptiques sur L.

En effet, lorsque $w=\sqrt{-107}$, u se spécialise en un carré de $\mathbb{Q}(\sqrt{-107})$, de sorte que la spécialisation de l'isogénie de la Proposition 3.3 est définie sur le corps $\mathbb{Q}(\sqrt{-107},\alpha)=L$.

3.5 La courbe $C_{\sqrt{-109}}$ et ses tordues.

Cette fois, nous nous restreignons au cas $w=\sqrt{-109}$, et notons par $C_{\sqrt{-109}}$ la courbe correspondante (3.5) ou (3.23). Commençons avec le modèle obtenu en substituant $w=\sqrt{-109}$ dans (3.5)

$$C_{\sqrt{-109}}: \quad y^2=x(x+1)\big(x^3+\tfrac{1}{4}(\sqrt{-109}+6)x^2+\tfrac{1}{4}(\sqrt{-109}-6)x-1\big).$$

Cette courbe est définie sur $\mathbb{Q}(\sqrt{-109})$, et son discriminant vaut 1. Puisque ces coefficients sont des entiers algébriques en dehors de 2, la courbe $C_{\sqrt{-109}}$ a bonne réduction en dehors de 2.

Tordre $C_{\sqrt{-109}}$ par $\sqrt{2+\sqrt{-109}}$ donne la courbe $C_{\sqrt{-109}}^{(2+\sqrt{-109})}$ d'équation

$$y^2 = x^5 + \big(\frac{12\sqrt{-109}-89}{4}\big)x^4 - \big(\frac{105\sqrt{-109}+436}{2}\big)x^3 + \big(\frac{324\sqrt{-109}+17033}{4}\big)x^2 + (840\sqrt{-109}-9281)x,$$

qui a aussi le modèle entier

$$y^2 + (\sqrt{-109}x^2+x)y = x^5 + (3\sqrt{-109}+5)x^4 - (53\sqrt{-109}+218)x^3 + (81\sqrt{-109}+4258)x^2 + (840\sqrt{-109}-9281)x.$$

Puisque $2+\sqrt{-109}$ est l'un des premiers de $\mathbb{Q}(\sqrt{-109})$ au dessus de 113, la courbe $C_{\sqrt{-109}}^{(2+\sqrt{-109})}$ a bonne réduction en dehors de $2+\sqrt{-109}$ et, en particulier, au premiers de $\mathbb{Q}(\sqrt{-109})$ au dessus de 2. Il s'ensuit que $C_{\sqrt{-109}}$ a bonne réduction tordue partout sur $\mathbb{Q}(\sqrt{-109})$.

D'après la Proposition 3.4, la $\sqrt[4]{-109}$-tordue $\mathcal{X}_{-109}$ de $C_{\sqrt{-109}}$ a une équation de la forme

$$\mathcal{X}_{-109}: \quad y^2 = x^5 - \frac{109}{4}x^4 + \frac{545}{2}x^3 - \frac{11881}{8}x^2 + \frac{106929}{16}x - \frac{1295029}{64} \quad (3.26)$$

qui a bonne réduction en dehors de 2 et 109.

Théorème 3.8. *Soit m un entier sans facteur carré, premier à 109 et tel que $m \equiv 1 \pmod 8$ et soit $\mathcal{F}=\mathbb{Q}(\sqrt{m})$. Alors la courbe $\mathcal{X}_{-109}$ a bonne réduction tordue partout sur $\mathcal{F}$.*

Preuve. Puisque $\mathcal{X}_{-109}$ a bonne réduction en dehors de 2 et 109, nous avons besoin seulement de construire des tordues à bonne réduction aux idéaux premiers de $\mathcal{F}$ divisant 2 et 109. Soit $\beta = \sqrt{-109m}$. Alors la tordue $\mathcal{X}_{-109}^{(\beta)}$ de $\mathcal{X}_{-109}$ sur $\mathcal{F}$ a une équation

$$\mathcal{X}_{-109}^{(\beta)}: \quad y^2 = x^5 - \frac{109}{4\beta}x^4 + \frac{545}{2\beta^2}x^3 - \frac{11881}{8\beta^3}x^2 + \frac{106929}{16\beta^4}x - \frac{1295029}{64\beta^5} \quad (3.27)$$

de discriminant $\Delta_{\mathcal{X}_{-109}}^{(\beta)} = 1/m^2$. Puisque m est premier à 109, la courbe $\mathcal{X}_{-109}^{(\beta)}$ a bonne réduction aux premier de $\mathcal{F}$ au dessus de 109.

Pour conclure, nous avons besoin de montrer que $\mathcal{X}_{-109}$ a une tordue sur $\mathcal{F}$ qui a bonne réduction au premier au dessus de 2. Puisque $m \equiv 1 \pmod 8$, m est un carré de $\mathbb{Q}_2$, et donc $\mathbb{Q}_2(\sqrt{-109}) = \mathbb{Q}_2(\sqrt{-109m})$ (dans une clôture algébrique fixée de $\mathbb{Q}_2$).

Par conséquent, $\mathcal{X}_{-109}^{(\beta)}$ est isomorphe à C_{-109} sur $\mathbb{Q}_2(\sqrt{-109})$.

De plus, puisque $2+\sqrt{-109m}$ est inversible comme un entier 2-adique, la condition $m \equiv 1 \pmod 8$ entraîne

$$(2+\sqrt{-109m})/(2+\sqrt{-109}) \equiv 1 \pmod 8$$

qui est donc un carré de $\mathbb{Q}_2(\sqrt{-109})$. Il s'ensuit que la tordue $\mathcal{X}_{-109}^{(\beta,2+\beta)}$ de $\mathcal{X}_{-109}^{(\beta)}$ par $\sqrt{2+\beta}$ est isomorphe sur $\mathbb{Q}_2(\sqrt{-109})$ à la courbe $C_{\sqrt{-109}}^{(2+\sqrt{-109})}$.

Puisque cette dernière courbe a bonne réduction en l'idéal premier de $\mathbb{Q}(\sqrt{-109})$ divisant 2 et, par conséquent, aussi sur $\mathbb{Q}_2(\sqrt{-109})$, nous concluons que $\mathcal{X}_{-109}^{(\beta,2+\beta)}$ a bonne réduction sur $\mathbb{Q}_2(\sqrt{-109})$.

Puisque la bonne réduction en un idéal premier d'un corps de nombres est équivalente à la bonne réduction sur la complétion, nous concluons que $\mathcal{X}_{-109}^{(\beta,2+\beta)}$ a bonne réduction en l'idéal premier de au dessus de 2. □

Remarque 3.9. Quand $w=\sqrt{-109}$, les racines du polynôme $W(x)$ de (3.18) engendrent une extension cubique cyclique L de $\mathbb{Q}(\sqrt{-109})$ qui est partout non ramifiée. Il s'ensuit que la 2-torsion sur la jacobienne de $C_{\sqrt{-109}}$ est rationnelle sur L et que $u=\pm 2\sqrt{109}$. Notons que $L(u)$ est le corps de classes de Hilbert de $\sqrt{-109}$. En spécialisant à partir de la Proposition 3.3, nous concluons que la jacobienne de $C_{\sqrt{-109}}$ devient isogène au produit de deux courbes elliptiques sur $L(u)$.

3.6 Reconstruction des courbes de Setzer.

Comme nous l'avons indiqué dans l'introduction, dans cette partie, nous expliquons brièvement comment la courbe de genre deux (3.2) a été trouvée. Soit L un corps de nombres. Nous cherchons les courbes de genre deux sur L à bonne réduction partout. Inspirés par le fait que les courbes elliptiques de Setzer à bonne réduction partout sur des corps quadratiques imaginaires K ont un point de 2-torsion K-rationnel, nous avons décidé de commencer avec des courbes de genre deux possédant deux points de Weierstrass L-rationnels. Ces courbes ont un modèle de la forme

$$y^2+(px^2+qx)y = x^5+ax^4+bx^3+cx^2+dx, \quad a,\, b,\, c,\, d,\, p,\, q \in L,$$

les points de Weierstrass étant l'unique point à l'infini et $(0,0)$. Quand $q=p$, il s'avère que le discriminant Δ_C est de degré 10 comme un polynôme en p ne contenant que des puissances paires de p.

En outre, le coefficient de p^{10} est $d^2(d+1-a+b-c))$, qui s'annule si et seulement si $d = a-b+c-1$. (Notons que si $d=0$, alors $(0,0)$ est un point singulier de C, qui ne serait alors pas de genre 2).

La substitution de cette valeur de d dans Δ_C donne un polynôme de degré 4 en p^2 dont le coefficient dominant est

$$(a-b+c-1)^2(3a-2b+c-4)^2.$$

Une simple vérification montre que

$$\text{si} \quad a-b+c-1=0 \quad \text{ou bien si} \quad 3a-2b+c-4=0, \quad \text{alors} \quad \Delta_C = 0,$$

donc le degré de Δ_C en p ne peut être réduit davantage.

Supposons alors que le coefficient dominant de Δ_C soit une unité. Dans ce cas, si a, b et c sont des entiers algébriques, si $\epsilon \in L$ est une unité et si p est une racine de $\Delta_C = \epsilon$, alors C a bonne réduction partout sur L.

Pour simplifier, nous supposons donc que

$$a-b+c-1=\epsilon \quad \text{et} \quad 3a-2b+c-4=\epsilon' \quad , \text{ où } \epsilon,\, \epsilon' \in \{\pm 1\}.$$

Ces conditions sont équivalentes à

$$d \in \{\pm 1\} \quad \text{et} \quad 2a-b \in \{1,3,5\}.$$

Le calcul de Δ_C pour chacune de ces possibilités pour d et $2a-b$ montre que, à des simples transformations près, il y a deux cas, l'un menant aux courbes (3.2) dont le discriminant est un carré et l'autre mène à une famille de courbes à bonne réduction partout sur un corps de nombres de degré 8 dont le discriminant a une forme plus compliquée.

Une fois que ces calculs ont été achevés, nous avons décidé de faire une recherche similaire pour les courbes elliptiques à bonne réduction partout. Ce qui a conduit à la famille paramétrée de courbes elliptiques d'équation de Weierstrass

$$E = E^{\epsilon}_{p,a}: \qquad y^2 + pxy = x^3 + ax^2 + \epsilon x \quad \text{où} \quad \epsilon \in \{\pm 1\} \tag{3.28}$$

de discriminant

$$\Delta = (p^2+4a)^2 + 64\epsilon \qquad \text{et d'invariant modulaire} \qquad j = (\Delta + 16\epsilon)^3/\Delta.$$

À nouveau, si $a \in \mathbb{Z}$ et si p est une racine de l'un des quatre polynômes

$$(t^2 + 4a)^2 + 64\epsilon = \epsilon' \quad \text{où} \qquad \epsilon,\, \epsilon' \in \{\pm 1\},$$

alors E acquiert bonne réduction partout sur tout corps L contenant p.

Rappelons que Setzer [28] a déterminé toutes les courbes elliptiques (munies d'un point d'ordre deux rationnel sur K) à bonne réduction partout sur les corps quadratiques imaginaires $K = \mathbb{Q}(\sqrt{-m})$, où m est un entier positif.

Théorème 3.10. *(Setzer). Il existe une courbe elliptique E sur K, à bonne réduction partout, munie d'un point K-rational d'ordre deux si et seulement si $m = 65m_1$, où m_1 est un carré* $\pmod 5$ *et* $\pmod{13}$ *et* 65 *est un carré* $\pmod{m_1}$.

Nous allons donner une description alternative des courbes de Setzer à partir des courbes $E = E^{\epsilon}_{p,a}$ où $\epsilon \in \{\pm 1\}$.

Considérons la courbe $E^{-}_{p,a}$ et supposons que le discriminant vaut 1. Alors

$$(p^2 + 4a)^2 = 65 \quad \text{et} \quad j = 17^3$$

et E a bonne réduction partout sur le corps $\mathbb{Q}(p)$ quand $a \in \mathbb{Z}$.

En posant $Y = y + \frac{1}{2}px$, nous obtenons le modèle

$$E' : \quad Y^2 = x^3 + \frac{\sqrt{65}}{4}x^2 + x \tag{3.29}$$

sur $\mathbb{Q}(\sqrt{65})$, qui a bonne réduction sur ce corps en dehors des premiers divisant 2.

En tordant la courbe E' par $\sqrt[4]{65}$ nous obtenons une courbe elliptique d'équation

$$Y^2 = x^3 + \frac{65}{4}x^2 + 65x, \tag{3.30}$$

à coefficient rationnels. En réécrivant (3.30) sous la forme

$$E_{65} : y^2 + xy = x^3 + 16x^2 + 65x \tag{3.31}$$

nous remarquons que la courbe E_{65} a maintenant un discriminant égale à 65^3 et, en particulier, que E_{65} a bonne réduction en 2.

En fait, le conducteur de E_{65} est $65^2 = 4225$ et nous pouvons l'identifier dans les tables de Cremona [6] comme étant la courbe elliptique $4225m_1$, bien que nous n'utiliserons pas ce résultat.

Par construction, la courbe elliptique E_{65} acquiert bonne réduction partout sur $\mathbb{Q}(\sqrt[4]{65})$.

Proposition 3.5. *Soit un corps quadratique imaginaire K satisfaisant aux conditions suivantes :*

1. *K et $\mathbb{Q}(\sqrt{65})$ ont les mêmes completions F_5 et F_{13} en 5 et en 13.*
2. *K a une extension quadratique L, non ramifiée en dehors de 5 et 13, telle que L et $\mathbb{Q}(\sqrt[4]{65})$ ont les mêmes completions en 5 et en 13.*

Alors la tordue C de E_{65} par L (vue comme courbe elliptique sur K) a bonne réduction partout sur K.

Preuve. Comme L est non ramifiée en dehors de 5 et 13, et E_{65} a bonne réduction en dehors de 5 et 13, alors la courbe C a aussi bonne réduction en dehors des idéaux premiers de K divisant 5 et 13.

Pour montrer que C a bonne réduction au dessus de 5, nous rappelons d'abord que E' est la tordue de E_{65} par $\sqrt[4]{65}$ et que C est la tordue par L de E_{65}. Les conditions (1) et (2) entraînent que E' et C sont en fait isomorphes sur F_5 et donc elles ont le même type de réduction sur ce corps.

Puisque E_{65} a bonne réduction, il s'ensuit que C a aussi bonne réduction. Un argument similaire montre que C a bonne réduction au dessus de 13. □

Soit K un corps quadratique dans lequel 5 et 13 sont ramifiés et notons par $\mathfrak{p}_5$ et $\mathfrak{p}_{13}$ les premiers de K au dessus de 5 et 13. La condition (2) de la proposition montre que L est ramifiée en $\mathfrak{p}_5$ et en $\mathfrak{p}_{13}$. Ce qui entraîne qu'il existe $\theta \in \mathcal{O}_K$ telle que $L = K(\sqrt{\theta})$ et

$$\theta\mathcal{O}_K = \mathfrak{p}_5\mathfrak{p}_{13}\mathfrak{a}^2$$

où $\mathfrak{a}$ est un idéal entier de K. D'autre part, si L/K est non ramifiée en 2, alors $\mathfrak{a}$ est premier à $2\mathcal{O}_K$ et θ est un carré $(\mathrm{mod}\ 4\mathcal{O}_K)$.

Réciproquement, si $\theta \in \mathcal{O}_K$ vérifie ces conditions, et si $L = K(\sqrt{\theta})$, alors L/K est ramifiée en $\mathfrak{p}_5$ et en $\mathfrak{p}_{13}$, et non ramifiée ailleurs. Ces conditions sont déjà citées dans [28] et, comme expliquées dans cette référence, d'après la théorie du genre, elles sont équivalentes au fait que le corps K soit de la forme décrite dans le Théorème 3.10. Donc la Proposition 3.5 donne une démonstration de la partie « si » du Théorème 3.10.

Remarque 3.11. En fait, non seulement Setzer démontre la partie « seulement si » du théorème 3.10, mais montre également que lorsque K est de la forme citée dans le théorème, il existe exactement 2^t classes d'isomorphismes de courbes elliptiques à bonne réduction partout sur K, où $t \geq 2$ est le nombre des premiers ramifiés dans K. Rappelons que le sous-groupe d'exposant 2 du groupe de classes de K est alors isomorphe au produit de $t-1$ groupes d'ordre 2.

Considérons une courbe C comme dans la Proposition 3.5, alors C et les tordues de C par les $2^{t-1}-1$ extensions quadratiques non ramifiées de K sont mutuellement non isomorphes et ont bonne réduction partout sur K. Cela représente la moitié des courbes de Setzer. Les autres sont obtenues en appliquant le même argument au quotient de C par le sous groupe engendré par ses sous groupes K-rationnels d'ordre 2.

Appendice

1. Polynômes caractéristiques de J_w.

Définition 3.3. *Une variété abélienne est simple si elle n'admet pas de sous variété abélienne autre que* $\{0\}$ *et elle même.*

En général, une variété abélienne qui est simple sur un corps K ne l'est pas forcément sur une clôture algébrique de K.

Le résultat suivant montre qu'une variété abélienne peut se décomposer de manière unique en produit de variétés abéliennes simples à isogénies près.

Proposition 3.6. *Soit A une variété abélienne et B une sous variété propre de A. Alors il existe une variété abélienne C telle que A est isogène au produit $B \times C$.*

Preuve. Cf [16], p. 28. □

Soit à nouveau C/K une courbe projective et lisse de genre deux.

Proposition 3.7. *La jacobienne J_C de C est décomposée si et seulement si J_C est isogène au produit de deux courbes elliptiques sur un corps de nombres K.*

Preuve. Découle de la proposition 3.6. □

Supposons que C est définie sur un corps fini $\mathbb{F}_q$. Lorsque la jacobienne de C est isogène au produit de deux courbes elliptiques $E \times E'$ sur $\mathbb{F}_q$, le polynôme caractéristique de Frobenius de J_C se factorise en deux polynômes de degré 2, les polynômes caractéristiques de E et de E' (voir le Théorème 1.11)).

Proposition 3.8. *Soit C une courbe de genre deux sur le corps fini $\mathbb{F}_q$ de caractéristique différente de deux et soit C' la tordue de C par l'extension quadratique de $\mathbb{F}_q$. Alors les polynômes caractéristiques de Frobenius $\chi(x)$ et $\chi'(x)$ de C et de C' sont liés par la formule $\chi'(-x) = \chi(x)$.*

Preuve. Écrivons

$$\chi(x) = x^4 - sx^3 + tx^2 - qsx + q^2 \quad \text{et} \quad \chi'(x) = x^4 - s'x^3 + t'x^2 - qs'x + q^2$$

et posons $N_1 = \#C(\mathbb{F}_q)$ et $N_1' = \#C'(\mathbb{F}_q)$ (voir (1.34)).

Il s'agit de vérifier que $s' = -s$ et $t' = t$. Si $y^2 = f(x)$ est un modèle affine de C, alors un modèle affine de C' est $y^2 = af(x)$, où $a \in \mathbb{F}_q^\times$ n'est pas un carré.

Il en résulte que si $x \in \mathbb{F}_q$ et si $f(x) \neq 0$, alors $af(x)$ est un carré si et seulement si $f(x)$ n'est pas un carré, et donc que

$$(af(x))^{(q-1)/2} = -f(x)^{(q-1)/2} \quad \text{pour tout } x \in \mathbb{F}_q.$$

En outre, si $f(x)$ est de degré 6 et si b est son coefficient de x^6, alors ab est le coefficient de x^6 dans $af(x)$ et b et un carré si et seulement si ab n'est pas un carré. Le nombre de points à l'infini de $C'(\mathbb{F}_q)$ est donc égal à 2 moins le nombre de points à l'infini de $C(\mathbb{F}_q)$.

En appliquant (1.36), nous obtenons

$$\begin{aligned} N_1 + N_1' =& 2 + \sum_{x\in\mathbb{F}_q}(1 + f(x)^{\frac{q-1}{2}}) + \sum_{x\in\mathbb{F}_q}(1 + (af(x))^{\frac{q-1}{2}}) \\ =& 2 + \sum_{x\in\mathbb{F}_q}(1 + f(x)^{\frac{q-1}{2}}) + \sum_{x\in\mathbb{F}_q}(1 - f(x)^{\frac{q-1}{2}}) \\ =& 2 + \sum_{x\in\mathbb{F}_q} 2 = 2(q+1). \end{aligned}$$

Les relations $N_1 = q + 1 - s$ et $N_1' = q + 1 - s'$, entraînent $s' = -s$.

Par hypothèse, C' devient isomorphe à C sur $\mathbb{F}_{q^2}$, d'où $\#C(\mathbb{F}_{q^2}) = \#C'(\mathbb{F}_{q^2})$. En utilisant (1.34), nous concluons que $t' = t$.

□

Reprenons les courbes C_w de genre deux définies sur $\mathbb{Q}(w)$ par l'équation

$$C_w : y^2 = x(x+1)(x^3 + \frac{w+6}{4}x^2 + \frac{w-6}{4}x - 1) \tag{3.32}$$

où $w \in \{\sqrt{-107}, \sqrt{-109}\}$.

Notons par $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, $K = \mathbb{Q}(\sqrt{-107})$, $K' = \mathbb{Q}(\sqrt{-109})$ et L (respectivement L') le corps de décomposition du polynôme caractéristique de Frobenius sur K (respectivement K').

Les Tables 3.2 et 3.3 donnent la décomposition du polynôme caractéristique $\chi_p(x)$ de l'endomorphisme de Frobenius de J_w sur l'un des corps résiduels $\mathcal{O}_{\mathbb{Q}(w)}/\mathfrak{p}$, dans chacun des cas $w = \sqrt{-107}$ et $w = \sqrt{-109}$, pour tout nombre premier $p \leq 101$ décomposé dans $\mathbb{Q}(w)$ et pour tout idéal premier $\mathfrak{p}$ de $\mathbb{Q}(w)$ divisant p. Notons que ces calculs ont été faits avec le logiciel Pari-gp. Lorsque $p \equiv 1 \mod 4$, ce polynôme ne dépend pas du choix de $\mathfrak{p}$. Par contre, lorsque $p \equiv 3 \mod 4$, l'un de ces polynômes est obtenu de l'autre en remplaçant x par $-x$. Ceci est une conséquence de la Proposition 3.8 et les deux propriétés suivantes :

(i) La courbe C_{-w} est la tordue par i de C_w en appliquant la substitution $(x, y) \mapsto (-x, iy)$ dans le modèle (3.23).

(ii) Le corps à p éléments (p un nombre premier impair) contient un élément i vérifiant $i^2 = -1$ si et seulement si $p \equiv 1 \pmod 4$.

La décomposition du polynôme caractéristique χ_p permet de citer les propriétés suivantes de la courbe C_w où $w \in \{\sqrt{-107}, \sqrt{-109}\}$.

1. Dans les deux cas, nous pouvons choisir p de telle manière que $\chi_p(x)$ soit irréductible. Nous en déduisons que la fibre en $\mathfrak{p}$ de la jacobienne J_w de la courbe C_w est simple sur $\mathcal{O}_{\mathbb{Q}(w)}$ puis, par un argument de spécialisation, que J_w est $\mathbb{Q}(w)$-simple.
2. Soit $\chi_{p^r}(x)$ le polynôme caractéristique de Frobenius de J_w sur l'extension de degré r de $\mathcal{O}_{\mathbb{Q}(w)}/\mathfrak{p}$. Lorsque $r = 2$, nous obtenons dans les deux cas encore des exemples où $\chi_{p^2}(x)$ est irréductible, ce qui entraîne que J_w est simple sur toute extension quadratique de $\mathbb{Q}(w)$. Il en est de même lorsque $r = 3$ et $w = \sqrt{-109}$. Par contre, lorsque $r = 3$ et $w = \sqrt{-107}$, $\chi_{p^3}(x)$ est toujours réductible, ce qui est à prévoir à partir de la Remarque 3.7, car l'existence d'une isogénie avec un produit de courbes elliptiques sur le corps L se spécialise en une isogénie analogue sur chaque fibre. De même, $\chi_{p^6}(x)$ est toujours réductible, en conformité avec la Proposition 3.3.
3. Nous remarquons aussi que le nombre de points de $J_w(\mathbb{F}_p)$ est divisible par 4. En fait, quelque soit le corps K de caractéristique différente de 2, $J_w(K)$ contient un sous-groupe isomorphe à un produit de deux groupes d'ordre deux. Celui-ci est engendré par les classes des diviseurs

$$(0,0) - \infty \quad \text{et} \quad (-1,0) - \infty \quad \text{de} \quad C_w.$$

TAB. 3.2 – Le polynôme caractéristique de la courbe $C_{\sqrt{-107}}$.

p	$\#J(\mathbb{F}_p)$	$\chi_p(x)$
3	$2^2.3$	$x^4+x^3-2x^2+3x+9$
11	$2^2.3.7$	$x^4-3x^3-2x^2-33x+121$
13	$2^4.3^2$	$x^4-x^3-12x^2-13x+169$
19	$2^2.67$	$x^4-5x^3+6x^2-95x+361$
23	$2^2.3.7$	$x^4-3x^3-14x^2-69x+529$
29	$(2.3)^4$	$(x^2+6x+29)^2$
37	$2^4.73$	$x^4-5x^3-12x^2-185x+1369$
41	$2^6.3.7$	$x^4-9x^3+40x^2-369x+1681$
47	$2^8.3^2$	$(x^2+47)^2$
53	$2^4.3.7^2$	$x^4-9x^3+28x^2-477x+2809$
61	$2^4.3^2.31$	$x^4+11x^3+60x^2+671x+3721$
79	$2^2.7.223$	$x^4+x^3-78x^2+79x+6241$
83	$2^{12}.3^2$	$(x^2+12x+83)^2$
89	$2^6.3.37$	$x^4-9x^3-8x^2-801x+7921$
101	$2^4.3.7.31$	$x^4+3x^3-92x^2+303x+10201$

TAB. 3.3 – Le polynôme caractéristique de la courbe $C_{\sqrt{-109}}$.

p	$\#J(\mathbb{F}_p)$	$\chi_p(x)$
5	$2^4.3$	$x^4+3x^3+4x^2+15x+25$
11	$2^2.67$	$x^4+9x^3+38x^2+99x+121$
19	$2^2.3.19$	$(x^2-8x+19)(x^2-x+19)$
23	$2^2.11^2$	$x^4-3x^3+26x^2-69x+529$
29	$2^4.3.19$	$x^4+3x^3-20x^2+87x+841$
47	$2^2.349$	$x^4-21x^3+194x^2-987x+2209$
59	$2^4.211$	x^4-106x^2+3481
61	$2^4.7.37$	$x^4+7x^3-12x^2+427x+3721$
67	$2^4.3^2.31$	x^4-26x^2+4489
73	$2^4.307$	$x^4-5x^3-48x^2-365x+5329$
79	$2^4.3^2.43$	x^4-50x^2+6241
89	$2^6.3.7^2$	$x^4+15x^3+136x^2+1335x+7921$
97	$2^6.157$	$x^4+7x^3-48x^2+679x+9409$
103	$2^2.3.7.97$	$(x^2-20x+103)(x^2-7x+103)$

TAB. 3.4 – Décomposition de $\chi_q(x)$ de la courbe $C_{\sqrt{-107}}$ sur $\mathbb{F}_{p^2}$, $\mathbb{F}_{p^3}$ et $\mathbb{F}_{p^6}$.

p	χ_{p^2}	χ_{p^3}	χ_{p^6}
3	irréductible	$(x^2+8x+27)^2$	$(x^2-10x+729)^2$
11	irréductible	$(x^2-72x+1331)^2$	$(x^2-2522x+1771561)^2$
13	irréductible	$(x^2-38x+2197)^2$	$(x^2+2950x+4826809)^2$
19	irréductible	$(x^2-160x+6859)^2$	$(x^2-11882x+47045881)^2$
23	irréductible	$(x^2-180x+12167)^2$	$(x^2-8066x+148035889)^2$
29	$(x^2+22x+841)^2$	$(x^2-306x+24389)^2$	$(x^2-44858x+594823321)^2$
37	irréductible	$(x^2-430x+50653)^2$	$(x^2-83594x+2565726409)^2$
41	irréductible	$(x^2-378x+68921)^2$	$(x^2-5042x+4750104241)^2$
47	$(x+47)^4$	$(x^2+103823)^2$	$(x+103823)^4$
53	irréductible	$(x^2-702x+148877^2$	$(x^2-195050x+22164361129)^2$
61	irréductible	$(x^2+682x+226981)^2$	$(x^2-11162x+51520374361)^2$
79	irréductible	$(x^2+236x+493039)^2$	$(x^2+930382x+243087455521)^2$
83	$(x^2+22x+6889)^2$	$(x^2-1260x+571787)^2$	$(x^2-444026x+326940373369)^2$
89	irréductible	$(x^2-1674x+704969)^2$	$(x^2-1392338x+496981290961)^2$
101	irréductible	$(x^2+882x+1030301)^2$	$(x^2+1282678x+1061520150601)^2$

TAB. 3.5 – Décomposition de $\chi_q(x)$ de la courbe $C_{\sqrt{-109}}$ sur $\mathbb{F}_{p^2}$, $\mathbb{F}_{p^3}$ et $\mathbb{F}_{p^6}$.

p	χ_{p^2}	χ_{p^3}	χ_{p^6}
5	irréductible	$(x^2+18x+125)^2$	$(x^2-74x+15625)^2$
11	irréductible	irréductible	$(x^2-1690x+1771561)^2$
19	$(x^2-26x+361)(x^2+37x+361)$	$(x^2-56x+6859)(x^2+56x+6859)$	$(x^2+10582x+47045881)^2$
23	irréductible	irréductible	$(x^2-11266x+148035889)^2$
29	irréductible	$(x^2+234x+24389)^2$	$(x^2-5978x+594823321)^2$
47	irréductible	irréductible	$(x^2-202354x+10779215329)^2$
59	$(x^2-106x+3481)^2$	irréductible	$(x^2-84058x+42180533641)^2$
61	irréductible	$(x^2+938x+226981)^2$	$(x^2-425882x+51520374361)^2$
67	$(x^2-26x+4489)^2$	irréductible	$(x^2+332566x+90458382169)^2$
73	irréductible	$(x^2-970x+389017)^2$	$(x^2-162866x+151334226289)^2$
79	$(x^2-50x+6241)^2$	irréductible	$(x^2+811150x+243087455521)^2$
89	irréductible	$(x^2+630x+704969)^2$	$(x^2+1013038x+496981290961)^2$
97	irréductible	$(x^2+1694x+912673)^2$	$(x^2-1044290x+832972004929)^2$

Conclusion.

Dans cette thèse, nous avons en premier lieu, présenté un nouvel algorithme de calcul des équations des courbes modulaires $X_1(N)$. L'objectif est d'obtenir des équations de $X_1(N)$ permettant de déterminer explicitement le couple correspondant (E, P) où E est une courbe elliptique et P est un point de torsion d'ordre N sur E.

La première démarche est d'utiliser les polynômes de division pour caractériser les couples $\big(E, (0,0)\big)$ où $E : y^2 + (a_1x + a_3)y = x^3 + a_2x^2$ et le point $(0,0)$ est de torsion d'ordre N sur E.

Nous avons constaté que chaque courbe elliptique de la forme (E) est isomorphe à une courbe elliptique de modèle $y^2 + \big((1+g)x + f\big)y = x^3 + fx^2$ via un isomorphisme qui envoie $(0,0)$ sur $(0,0)$ (voir la proposition 2.1). Ces coefficients f et g sont en fait des formes modulaires définies sur le groupe modulaire $\Gamma_1(N)$ et ils engendrent le corps de fonctions $\mathbb{C}(X_1(N))$ sur $X_1(N)$ (voir § 2.3).

Notre deuxième démarche est de définir en fonction de f et g deux autres couples de fonctions modulaires $\{s, t\}$ et $\{q, r\}$ sur $\Gamma_1(N)$, chaque couple étant un système de générateurs de $\mathbb{C}(X_1(N))$. Nous obtenons ainsi des équations de $X_1(N)$ de plus petit degré.

Nous avons abordé des nouvelles approches pour calculer ces équations, en s'appuyant sur le fait que les polynômes de division sont divisibles par des grandes puissances de a_3 qui est aussi un facteur du discriminant de la courbe elliptique E. Nous avons obtenu une simplification considérable en enlevant ces puissances de a_3. Les calculs effectués reposent sur des procédures récursives et peuvent être facilement implémentés.

Nous avons montré que cet algorithme peut être amélioré de sorte que ces équations soient de plus petit degré en les deux variables, et ainsi que lorsque N est petit, elles se comparent favorablement avec les équations des auteurs précedents.

Des équations particulièrement simples de $X_1(N)$ ont été calculées pour tout $N \leq 51$.

Il est naturel de tenter d'améliorer encore cet algorithme pour obtenir des équations de $X_1(N)$ de plus petit degré possible.

D'autre part, dans le chapitre 3, nous avons développé quelques notions simples de la bonne réduction tordue partout.

Nous avons démontré deux résultats fondamentaux :

1. Il n'existe pas de courbes elliptiques sur $\mathbb{Q}$ à bonne réduction tordue partout.
2. Si K est un corps de nombres et Σ est un ensemble fini de premiers de K, alors il n'existe qu'un nombre fini d'invariants $j \in K$ de courbes elliptiques à bonne réduction tordue partout en tout premier n'appartenant pas à Σ.

Nous avons construit deux familles de courbes de genre deux C_w où $w^2 = -107$ ou $w^2 = -109$, à bonne réduction partout sur des corps quartiques et à bonne réduction tordue partout sur certains corps quadratiques et nous avons montré que la jacobienne J_w de C_w est isogène au produit de deux courbes elliptiques sur une extension cubique de $\mathbb{Q}(w)$.

En appliquant une stratégie similaire aux courbes elliptiques, nous avons retrouvé les exemples des courbes de Setzer à bonne réduction partout sur des corps quadratiques imaginaires.

Il serait intéressant de construire d'autres exemples de courbes de genre deux à bonne réduction tordue partout sur des corps quadratiques et de déterminer le lien avec des courbes elliptiques à bonne réduction partout sur des corps quadratiques.

Bibliographie

[1] **V. ABRASHKIN.** *Galois modules of period p group schemes over the ring of Witt vectors.* Izv. Akad. Nauk SSSR, ser. matem., **51** (1987), pp.691-736 ; English translation in Math. USSR Izv. **31**, (1988), 1-46.

[2] **H. BAAZIZ.** *Equations for the modular curve $X_1(N)$ and models of elliptic curves with torsion points.* Accepté pour publication dans le journal Mathematics of Computation.

[3] **O. BOLZA.** *On binary sextics with linear transformations into themselves.* Amer. Math. **10**, 1888, 47-70.

[4] **G. CARDONA, J. GONZALEZ, J. C. LARIO and A. RIO.** *On curves of genus 2 with jacobian of GL_2-type.* Manuscripta Math. **72**, (1999), no. 1, 37-54.

[5] **J. W. S. CASSELS.** *Lectures on elliptic curves.* London Mathematical Society. Student Texts 24, Cambridge University Press, 1991.

[6] **J. E. CREMONA.** *Algorithms for modular elliptic curves.* Combridge University Press (1997).

[7] **D. H. COX.** *Primes of the form $x^2 + ny^2$.* Wiley-Interscience (1989).

[8] **H. DARMON.** Note on a polynomial of Emma Lehmer. Math. Comput. **56** (194) (1991) 795–800.

[9] **H. M. FARKAS, I. KRA.** *Riemann Surfaces.* Springer. 1991.

[10] **J. M. FONTAINE.** *Il n'y a pas de variété abélienne sur $\mathbb{Z}$.* Invent. Math. **81**, (1985), 515-538.

[11] **W. FULTON.** *Algebraic Curves.* Math. Lec. Note Series. A. A. Benjamin Inc.1969.

[12] **J. IGUSA.** *Arithmetic variety of moduli for genus two.* Annals of Mathematics. **72** (1960), 612-649.

[13] **N. ISHIDA, N. ISHII.** *Generators and defining equation of the modular function field of the group $\Gamma_1(N)$.* Acta. Arithmetica. **101**. 4. (2002), 301–320.

[14] **K. KIOZUMI, G. SHIMURA.** *On specializations of abelian varieties.* Scientific papers of the college of general education, University of Tokyo **9** (1959), 187-211.

[15] **D. S. KUBERT, S. LANG.** *Modular units.* Springer-Verlag. New York Heidelberg. Berlin, 1981.

[16] **S. LANG.** *Abelian varieties.* Intersciences Tracs in Pure and Applied Mathematics, no. **7**, Intersciences Publishers, 1959.

[17] **O. LECACHEUX.** *Unités d'une famille de corps cycliques réels de degré* 6 *liés à la courbe modulaire* $X_1(13)$. J. Num. Theory. **31** (1989), 54–63.

[18] **F. LEPREVOST.** *Jacobiennes de certaines courbes de genre deux : torsion et simplicité.* Journal de Théorie des Nombres de Bordeaux **7** (1995), 283-306.

[19] **R. LERCIER and F. MORAIN.** *Counting points on elliptic curves over* $\mathbb{F}_{p^n}$ *using Couveignes's algorithm.* Rapport de Recherche LIX/RR/95/09, Ecole Polytechnique, septembre 1995. ftp ://lix.polytechnique.fr/pub/submissions/morain/Preprints/seac-gfpn.960125.ps.Z

[20] **Q. LIU.** *Courbes stables de genre* 2 *et leur schéma de modules.* Math Ann. **295** (1993), 201-222.

[21] **P. LOCKHART.** *On the discriminant of a hyperelliptic curve.* Transactions of the American Mathematical Society. **342, 2** (1994), 729-752.

[22] **B. MAZUR.** *Modular curves and the Eisenstein ideal.* Publications mathématiques de l'IHES **47** (1977), 33-186.

[23] **J. R. MERRIMAN, N. P. SMART.** *Curves of genus* 2 *with good reduction away from* 2 *with a Weierstrass rational point.* Math. Proc. Camb. Phil. Soc. **88**, (1993), 114, 203.

[24] **J. F. MESTRE** *Construction de courbes de genre 2 à partir de leurs modules, effective Methods in Algebraic Geometry (Castiglioncello, 1990).* Progr. Math., Birkhauser **94**, (1991), 313-334.

[25] **D. MUMFORD.** *Abelian Varieties*, Oxford University Press (1970).

[26] **A. NÉRON.** *Modèles minimaux des variétés abéliennes sur les corps locaux et globeaux.* IHES Publ. Math. **21** (1964), 361-482.

[27] **M. A. REICHERT.** *Explicit determination of non-trivial torsion structures of elliptic curves over quadratic number fields.* Math. Comp. **46** (1986), 637–658.

[28] **B. SETZER.** *Elliptic curves over complex quadratic fields.* Pacific. J. Math. **74, 1** (1978), 235-250.

[29] **I. R. SHAFAREVICH.** *Algebraic number fields.* Proc. Int. Cong. Stockholm (1962). AMS Transactions 2^{nd} Series. **31**, (25-39).

[30] **G. SHIMURA.** *Introduction to the arithmetic theory of automorphic functions.* Princeton Univ Press (1971).

[31] **C. L. SIEGEL.** *Über einige Anwendungen diophantischer Approximationen.* Abh. Pr. Akad. Wiss. (1929), no 1 (= Collected Works **I**, 209-266).

[32] **J. H. SILVERMAN.** *The Arithmetic of Elliptic Curves.* Springer-Verlag (1986).

[33] **H. STICHTENOTH.** *Algebraic function fields and codes.* Springer-Verlag, 1993.

[34] **J. TATE.** *Algorithm for determining the type of a singular fiber in an elliptic pencil.* Modular functions of one variable IV. Lecture Notes in Mathematics **476**. Springer-Verlag, Berlin (1975).

[35] **L. C. WASHINGTON.** *A family of cyclic quartic fields arising from modular curves.* Math. Comput. **57**. 196. (1991), 763–775.

[36] **A. WEIL.** *Courbes algébriques et variétés abéliennes.* Hermann, Paris (1948).

[37] **Y. YANG.** *Defining equations of modular curves.* Advances. Math. **204** (2006), 481–508.