G. Ligozat
Nagoya Math. J.
Vol. 76 (1979), 115-152

COURBES ELLIPTIQUES AYANT BONNE RÉDUCTION EN DEHORS DE 3

GÉRARD LIGOZAT

Introduction

Le résultat principal de ce travail est le suivant: les courbes elliptiques définies sur $\boldsymbol{Q}$, et ayant bonne réduction en dehors de 3, vérifient la conjecture de Weil (cf. [2], Th. 2).

La démonstration de ce fait découle d'une construction explicite des formes paraboliques de poids 2 sur les groupes de congruence $\Gamma_0(3^\nu)$, $\nu = 3, 4, 5$. La méthode utilisée pour faire cette construction, ainsi que la façon d'en déduire la validité de la conjecture de Weil, sont celles employées par Honda et Miyawaki dans leur article [2] relatif au cas analogue des courbes ayant bonne réduction en dehors de 2.

Ces questions sont traitées dans les deux premiers paragraphes.

Dans un troisième paragraphe, on utilise les symboles modulaires pour donner une description de la jacobienne $J_0(3^4)$, associée au groupe de congruence $\Gamma_0(3^4)$, en termes de réseaux complexes. On montre dans le quatrième paragraphe comment on peut déduire des résultats obtenus: d'une part, certaines propriétés galoisiennes des points de 3-division des courbes elliptiques de conducteur 27; d'autre part, les propriétés galoisiennes des points de 3-division d'une certaine courbe elliptique considérée par Koike dans [3], § 3. Ces propriétés sont démontrées par Koike par une autre méthode, et lui servent à déterminer une équation explicite de cette courbe. Notre démonstration montre qu'elles ont une origine "modulaire".

Je tiens à remercier ici le Professeur Koike qui a bien voulu s'intéresser aux résultats de la première partie de ce travail, et dont l'article cité plus haut a motivé la seconde partie.

Received October 16, 1978.

1. Construction de formes paraboliques

Notons $\langle \Gamma_0(3^\nu), 2\rangle_0$ l'espace des formes paraboliques de poids 2 sur le groupe de congruence $\Gamma_0(3^\nu)$, $\nu = 3, 4, 5$, resp. Cet espace est de dimension 1, 4, 19 resp. Le sous-espace engendré par les formes primitives est de dimension 1, 2, 12 resp.

Soit $\mathfrak{H} = \{z \in \boldsymbol{C} \mid \mathrm{Im}\,(z) > 0\}$ le demi-plan de Poincaré. On notera $\mathfrak{H}^*$ le demi-plan de Poincaré complété:

$$\mathfrak{H}^* = \mathfrak{H} \cup \boldsymbol{Q} \cup \{\infty\}\,.$$

On désigne par $X_0(3^\nu)$, $\nu = 3, 4, 5$, la courbe modulaire associée à $\Gamma_0(3^\nu)$. Cette courbe est lisse, projective, définie sur $\boldsymbol{Q}$, et de genre égal à la dimension de $\langle \Gamma_0(3^\nu), 2\rangle_0$. Enfin, on note $J_0(3^\nu)$ la jacobienne de $X_0(3^\nu)$.

Soit $\eta(z)$ la fonction êta de Dedekind, définie par

$$\eta(z) = e^{\pi i z/12} \prod_{n=1}^{\infty} (1-q^n)\,,$$

où $z \in \mathfrak{H}$, et où l'on pose $q = e^{2\pi i z}$.

1.1. Formes sur $\Gamma_0(3^\nu)$, $\nu = 3, 4$

Proposition 1.1.1. a) *La fonction*:

$$F_1^{(3)}(z) = \eta(3z)^2\eta(9z)^2 \equiv q - 2q^4 - q^7 + 5q^{13} + 4q^{16} - 7q^{19} - 5q^{25} + 2q^{28} - 4q^{31} \pmod{q^{37}}\,,$$

est l'unique forme primitive normalisée de $\langle \Gamma_0(3^3), 2\rangle_0$.

b) *Soient*:

$$G_1^{(4)}(z) = \eta(3z)\eta(9z)^2\eta(27z) \equiv q^2 - q^5 - q^8 - 2q^{11} + 2q^{14} + 3q^{17} - q^{20} + 2q^{23} - q^{26} + q^{29} - 3q^{32} - 2q^{35} \pmod{q^{38}}\,,$$

et

$$G_2^{(4)}(z) = \eta(3z)^{-1}\eta(9z)^6\eta(27z)^{-1} \equiv q + q^4 + 2q^7 - 3q^{10} - q^{13} - 5q^{16} + 2q^{19} - 6q^{22} - 2q^{25} + 2q^{28} + 8q^{31} + 9q^{34} \pmod{q^{37}}\,.$$

Les fonctions $G_1^{(4)}, G_2^{(4)}$ *constituent une base de l'espace engendré dans* $\langle \Gamma_0(3^4), 2\rangle_0$ *par les formes primitives. Les deux formes primitives normalisées sont*:

$$F_1^{(4)} = G_2^{(4)} + \sqrt{3}\cdot G_1^{(4)}$$

et

$$F_2^{(4)} = G_2^{(4)} - \sqrt{3} \cdot G_1^{(4)} .$$

Démonstration. Le Théorème 1 de [2] montre que $F_1^{(3)}$ est un élément (non nul) de $\langle \Gamma_0(3^3), 2 \rangle_0$ (cf. aussi [4], Prop. 3.1.1); on en déduit la partie (a); le même théorème entraîne que $G_1^{(4)}$ et $G_2^{(4)}$ sont des éléments non nuls de $\langle \Gamma_0(3^4), 2 \rangle_0$.

Soit S la matrice:

$$S = \begin{pmatrix} 1 & 0 \\ 27 & 1 \end{pmatrix} .$$

Toujours d'après [2], Th. A, on a, avec les conventions de loc. cit.:

$$\eta(3 \cdot Sz) = (27z + 1)^{1/2} \cdot e^{-3\pi i/4} \cdot \eta(3z) ,$$
$$\eta(9 \cdot Sz) = (27z + 1)^{1/2} \cdot e^{-\pi i/4} \cdot \eta(9z) ,$$
$$\eta(27 \cdot Sz) = (27z + 1)^{1/2} \cdot e^{-\pi i/12} \cdot \eta(27z) .$$

Il en résulte:

$$G_1^{(4)} |_2 S = e^{-4\pi i/3} \cdot G_1^{(4)} ,$$
$$G_2^{(4)} |_2 S = e^{-2\pi i/3} \cdot G_2^{(4)} .$$

Ceci entraîne (cf. [2], p. 368) que $G_1^{(4)}$ et $G_2^{(4)}$ sont orthogonaux à $\langle \Gamma_0(27), 2 \rangle_0$ pour le produit scalaire de Petersson; ce sont donc des combinaisons linéaires de formes primitives de $\langle \Gamma_0(3^4), 2 \rangle_0$.

Enfin, l'action de l'opérateur de Hecke $T(2)$ est la suivante:

$$G_1^{(4)} | T(2) = G_2^{(4)} ,$$
$$G_2^{(4)} | T(2) = 3G_1^{(4)} .$$

On obtient $F_1^{(4)}, F_2^{(4)}$ en diagonalisant.

1.2. Formes sur $\Gamma_0(3^5)$

Considérons maintenant l'espace $\langle \Gamma_0(3^5), 2 \rangle_0$, et cherchons à déterminer les éléments de cet espace qui s'écrivent comme produits de fonctions êta. On obtient le résultat suivant:

PROPOSITION 1.2.1. *La fonction*:

$$\eta(z)^{n_1}\eta(3z)^{n_2}\eta(3^2z)^{n_3}\eta(3^3z)^{n_4}\eta(3^4z)^{n_5}\eta(3^5z)^{n_6} , \tag{1.2.1.1}$$

où $n_1, \cdots, n_6 \in \boldsymbol{Z}$, *est une forme parabolique de poids* 2 *sur* $\Gamma_0(3^5)$ *si et seulement si* $(n_1, \cdots, n_6)$ *prend l'une des seize valeurs données dans le tableau suivant.*

https://doi.org/10.1017/S0027763000018547 Published online by Cambridge University Press

$(n_1, n_2, n_3, n_4, n_5, n_6)$	notation de la fonction correspondante
$(0, -1, 3, 3, -1, 0)$	$G_1^{(5)}$
$(0, -1, 5, -1, 1, 0)$	$G_2^{(5)}$
$(0, -1, 4, -1, 2, 0)$	$G_3^{(5)}$
$(0, 2, 1, 0, 1, 0)$	$G_4^{(5)}$
$(0, 2, 0, 0, 2, 0)$	$G_5^{(5)}$
$(0, 2, -1, 4, -1, 0)$	$G_6^{(5)}$
$(0, 1, -1, 5, -1, 0)$	$G_8^{(5)}$
$(0, 1, 1, 1, 1, 0)$	$G_9^{(5)}$
$(0, 1, 0, 1, 2, 0)$	$G_{10}^{(5)}$
$(0, 2, 2, 0, 0, 0)$	$F_1^{(3)}$
$(0, 0, 2, 2, 0, 0)$	
$(0, 0, 0, 2, 2, 0)$	
$(0, 1, 2, 1, 0, 0)$	$G_1^{(4)}$
$(0, 0, 1, 2, 1, 0)$	
$(0, -1, 6, -1, 0, 0)$	$G_2^{(4)}$
$(0, 0, -1, 6, -1, 0)$	

Les formes $G_i^{(5)}$, $1 \leq i \leq 10$, $i \neq 7$, *sont linéairement indépendantes, et appartiennent à l'espace engendré dans* $\langle \Gamma_0(3^5), 2 \rangle_0$ *par les formes primitives.*

Démonstration. Utilisons les résultats de [4], 3.2. D'après la Prop. 3.2.8 de loc. cit., l'ordre de la fonction définie par (1.2.1.1) en une pointe de niveau 3^{j-1} $(1 \leq j \leq 6)$ est donné par la j-ième ligne de la matrice:

$$\frac{1}{24}\Omega\begin{pmatrix} n_1 \\ \vdots \\ n_6 \end{pmatrix} = \begin{pmatrix} m_1 \\ \vdots \\ m_6 \end{pmatrix}, \tag{1.2.1.2}$$

https://doi.org/10.1017/S0027763000018547 Published online by Cambridge University Press

où l'on désigne par Ω la matrice de terme:

$$\Omega_{i,j} = 3^{5+2\inf(i,j)-\inf(i-1,6-i)-(i+j)} . \qquad 1 \leq i, j \leq 6 .$$

Le raisonnement fait dans la démonstration de la Prop. 3.1.1 de [4] montre que les conditions suivantes sont nécessaires et suffisantes pour que la fonction associée à $(n_1, \cdots, n_6)$ soit une forme parabolique de poids 2 sur $\Gamma_0(3^5)$:

(i) $n_1 + \cdots + n_6 = 4$;
(ii) $m_1, \cdots, m_6 \in \boldsymbol{Z}$;
(iii) $m_1, \cdots, m_6 > 0$;
(iv) $n_1 + n_3 + n_5 \equiv 0 \pmod 2$.

S'il en est ainsi, le diviseur de la forme différentielle associée à la forme parabolique est de degré 36; ceci s'exprime par la formule:

(v) $m_1 + m_6 + 2(m_2 + m_5) + 6(m_3 + m_4) = 54$.

Pour déterminer les solutions du système (i, ii, iii, iv), il est commode d'utiliser (v). Plus précisément, posons:

$$u = m_1 + m_6 ; \quad v = m_2 + m_5 ; \quad w = m_3 + m_4 .$$

La condition (iii) entraîne:

(iii)′ $u, v, w \geq 2$.

D'autre part, on tire de (1.2.1.2):

$$\begin{aligned} 24u &= 244n_1 + 84n_2 + 36n_3 + 36n_4 + 84n_5 + 244n_6 , \\ 24v &= 28n_1 + 84n_2 + 36n_3 + 36n_4 + 84n_5 + 28n_6 , \\ 24w &= 4n_1 + 12n_2 + 36n_3 + 36n_4 + 12n_5 + 4n_6 , \end{aligned}$$

d'où:

$$\text{(vi)} \quad \begin{cases} n_1 + n_6 = \dfrac{u - v}{9} \\ n_3 + n_4 = \dfrac{-v + 7w}{9} . \end{cases}$$

Dans un premier temps, on détermine les triplets (u, v, w) vérifiant simultanément:

(v) $u + 2v + 6w = 54$;

https://doi.org/10.1017/S0027763000018547 Published online by Cambridge University Press

(iii)′ $u, v, w \geq 2$;

(vi)′ $u \equiv v \pmod 9$; $v \equiv 7w \pmod 9$.

On trouve ainsi les neuf solutions suivantes:

(2, 2, 8); (4, 4, 7); (6, 6, 6); (8, 8, 5); (10, 10, 4); (12, 12, 3); (14, 14, 2); (30, 3, 3); (32, 5, 2).

Pour chacune de ces neuf valeurs, on est ramené à résoudre un système ne faisant intervenir que la moitié des inconnues. Montrons comment on traite le cas $u = 2$, $v = 2$, $w = 8$.

On a; $m_1 + m_6 = 2$; $m_2 + m_5 = 2$; $m_3 + m_4 = 8$,

soit (*): $n_1 + n_6 = 0$; $n_2 + n_5 = -2$; $n_3 + n_4 = 6$.

Comme $m_1, \cdots, m_6 \geq 1$, on a nécessairement:

$$m_1 = m_2 = m_5 = m_6 = 1 .$$

On tire alors de (1.2.1.2) et (*):

$$24 = 242n_1 + 78n_2 + 18n_3 + 48 ,$$
$$24 = 6n_1 + 78n_2 + 18n_3 + 48 ,$$

soit $n_1 = 0$, donc $n_6 = 0$, et (**) $13n_2 + 3n_3 + 4 = 0$. D'autre part, on tire de (1.2.1.2):

$$24m_3 = 6n_2 + 18n_3 + 48 .$$

On a donc, utilisant (**):

$$3n_2 = 1 - m_3 ,$$

donc

$$m_3 \equiv 1 \pmod 3; \qquad \text{comme } 1 \leq m_3 \leq 7 ,$$

m_3 peut prendre une des trois valeurs 1, 4 ou 7, donc $n_2 = 0$, -1 ou -2.

Enfin, (**) entraîne: $n_2 \equiv 2 \pmod 3$.

Par conséquent, $n_2 = -1$, d'où $n_3 = 3$, et $m_3 = 4$. On a ainsi obtenu la solution:

$$n_1 = 0,\ n_2 = -1,\ n_3 = 3,\ n_4 = 3,\ n_5 = -1,\ n_6 = 0$$

du système (i, ii, iii).

On procède de façon analogue pour les autres cas. On constate que la condition (iv) est vérifiée par chacune des solutions de (i, ii, iii).

1.2.2. Donnons les premiers coefficients des développements en série de Fourier des formes $G_i^{(5)}$, $1 \leq i \leq 10$, $i \neq 7$:

$$G_1^{(5)} \equiv q + q^4 + 2q^7 + 2q^{13} + q^{16} + 2q^{19} + q^{25} - q^{28} - q^{31} - 6q^{34} \pmod{q^{37}};$$

$$G_2^{(5)} \equiv q^4 + q^7 + 2q^{10} - 2q^{13} - 3q^{19} + q^{22} - 5q^{25} - 3q^{28} + q^{31} + 3q^{34} \pmod{q^{37}};$$

$$G_3^{(5)} \equiv q^7 + q^{10} + 2q^{13} - q^{16} + q^{19} - q^{22} + q^{25} - 3q^{28} - 2q^{31} + q^{34} \pmod{q^{37}};$$

$$G_4^{(5)} \equiv q^4 - 2q^7 - q^{10} + q^{13} + 3q^{16} + 3q^{19} - 5q^{22} + q^{25} - 3q^{28} - 2q^{31} \pmod{q^{37}};$$

$$G_5^{(5)} \equiv q^7 - 2q^{10} - q^{13} + 2q^{16} + q^{19} + 2q^{22} - 2q^{25} - 2q^{31} - 2q^{34} \pmod{q^{37}};$$

$$G_6^{(5)} \equiv q - 2q^4 - q^7 + 3q^{10} - q^{13} + q^{16} + 2q^{19} - 3q^{22} - 2q^{25} - q^{28} + 5q^{31} + 3q^{34} \pmod{q^{37}};$$

$$G_8^{(5)} \equiv q^2 - q^5 - q^8 + q^{11} - q^{14} + 2q^{20} - q^{23} - q^{26} - 2q^{29} + 3q^{32} + 4q^{35} \pmod{q^{38}};$$

$$G_9^{(5)} \equiv q^5 - q^8 - q^{11} - q^{14} + q^{17} + 2q^{20} - q^{23} + 2q^{26} - q^{32} \pmod{q^{44}};$$

$$G_{10}^{(5)} \equiv q^8 - q^{11} - q^{14} + q^{23} + q^{29} - q^{35} \pmod{q^{38}}.$$

1.2.3. On démontre comme en 1.1 que ces neuf formes sont orthogonales à $\langle \Gamma_0(3^4), 2 \rangle_0$ pour le produit scalaire de Petersson (cf. [2], p. 368); plus précisément, cela résulte de ce que la matrice:

$$\begin{pmatrix} 1 & 0 \\ 3^4 & 1 \end{pmatrix}$$

opère sur la forme parabolique de poids 2:

$$\eta(3z)^{n_2}\eta(3^2z)^{n_3}\eta(3^3z)^{n_4}\eta(3^4z)^{n_5}$$

en la multipliant par

$$e^{-((3n_2+9n_3+3n_4+n_5)/12)\pi i}$$

comme il résulte immédiatement de [2], Th. A; or, pour chacune des neuf formes considérées,

$$3n_2 + 9n_3 + 3n_4 + n_5 \equiv \pm 4 \pmod{24}.$$

Les neuf formes considérées sont donc des éléments de l'espace engendré

https://doi.org/10.1017/S0027763000018547 Published online by Cambridge University Press

par les formes primitives dans $\langle \Gamma_0(3^5), 2\rangle_0$.

1.2.4. Soient:

$$G_7^{(5)} = G_8^{(5)} \mid T(2) ,$$
$$G_{11}^{(5)} = \tfrac{1}{3} G_1^{(5)} \mid T(2) ,$$
$$G_{12}^{(5)} = G_2^{(5)} \mid T(2) .$$

Ces trois formes sont combinaisons linéaires de formes primitives. On a:

$$G_7^{(5)} \equiv q + q^4 - q^7 - q^{13} + q^{16} - q^{19} + q^{25} - 4q^{28} - 4q^{31} + 3q^{34} \pmod{q^{37}} ;$$

$$G_{11}^{(5)} \equiv q^2 + q^8 + q^{14} - 2q^{17} - 2q^{20} - 2q^{23} + q^{26} - 2q^{29} - q^{32} - 2q^{35} \pmod{q^{38}} ;$$

$$G_{12}^{(5)} \equiv q^2 + 2q^5 + 2q^8 + q^{11} - q^{14} + 3q^{17} - q^{20} + 2q^{23} - 4q^{26} + 4q^{29} - 2q^{35} \pmod{q^{38}} .$$

L'examen des coefficients de Fourier montre que les douze formes $G_i^{(5)}$, $1 \leq i \leq 12$ sont linéairement indépendantes. On peut donc conclure:

Proposition 1.2.5. *Les formes $G_i^{(5)}$, $1 \leq i \leq 12$, constituent une base de l'espace engendré par les formes primitives dans $\langle \Gamma_0(3^5), 2\rangle_0$.*

1.3. Diagonalisation

Pour déterminer les formes primitives elles-mêmes, nous allons utiliser la diagonalisation de $T(2)$. Remarquons tout d'abord que l'espace engendré par les formes $G_i^{(5)}$, $1 \leq i \leq 12$, est somme directe de l'espace V engendré par $G_i^{(5)}$, $1 \leq i \leq 7$, et de W, engendré par $G_i^{(5)}$, $8 \leq i \leq 12$, et que $T(2)$ est somme directe de:

$$T' = T(2)|_V : V \to W$$

et

$$T'' = T(2)|_W : W \to V$$

qui sont deux opérateurs de rang 5.

On est donc ramené, pour déterminer les valeurs propres de $T(2)$, à calculer celles de

$$T' \circ T'' : W \to W$$

où W est de dimension 5.

https://doi.org/10.1017/S0027763000018547 Published online by Cambridge University Press

L'action de $T(2)$ sur les formes $G_i^{(5)}$, $1 \leq i \leq 12$, est la suivante:

$$G_1^{(5)} \mid T(2) = 3G_{11}^{(5)} ;$$
$$G_2^{(5)} \mid T(2) = G_{12}^{(5)} ;$$
$$G_3^{(5)} \mid T(2) = G_9^{(5)} ;$$
$$G_4^{(5)} \mid T(2) = G_8^{(5)} + 6G_{10}^{(5)} ;$$
$$G_5^{(5)} \mid T(2) = -2G_9^{(5)} ;$$
$$G_6^{(5)} \mid T(2) = 3G_9^{(5)} ;$$
$$G_7^{(5)} \mid T(2) = 2G_8^{(5)} + 3G_{10}^{(5)} + G_{12}^{(5)} ;$$
$$G_8^{(5)} \mid T(2) = G_7^{(5)} ;$$
$$G_9^{(5)} \mid T(2) = -\tfrac{1}{3}G_1^{(5)} + G_3^{(5)} - G_5^{(5)} + \tfrac{1}{3}G_6^{(5)} ;$$
$$G_{10}^{(5)} \mid T(2) = \tfrac{1}{3}G_2^{(5)} + \tfrac{2}{3}G_4^{(5)} ;$$
$$G_{11}^{(5)} \mid T(2) = \tfrac{5}{3}G_1^{(5)} - 2G_3^{(5)} - G_5^{(5)} - \tfrac{2}{3}G_6^{(5)} ;$$
$$G_{12}^{(5)} \mid T(2) = 2G_2^{(5)} + G_4^{(5)} + G_7^{(5)} .$$

On en déduit la matrice de $T' \circ T''$, par rapport à la base $G_i^{(5)}$, $8 \leq i \leq 12$:

$$\begin{pmatrix} 2 & 0 & 3 & 0 & 1 \\ 0 & 4 & 0 & -1 & 0 \\ \frac{2}{3} & 0 & 4 & 0 & \frac{1}{3} \\ 0 & -2 & 0 & 5 & 0 \\ 3 & 0 & 9 & 0 & 3 \end{pmatrix} .$$

Le polynôme caractéristique de cette matrice est:

$$-(X-3)(X-6)(X^3 - 9X^2 + 18X - 9) .$$

Soient $\alpha_1, \alpha_2, \alpha_3$ les racines du polynôme:

$$X^3 - 3X^2 + 3 .$$

On a (cf. [3], § 7):

$$\alpha_i = 1 + \zeta_i + \zeta_i^{-1} , \qquad (i = 1, 2, 3) ,$$

où ζ_i est une racine primitive neuvième de l'unité.

Les valeurs propres de $T' \circ T'' : W \to W$ sont:

$$3, 6, \alpha_i^2 , \qquad i = 1, 2, 3 .$$

Les valeurs propres de $T(2)$, par conséquent, sont:

$$0, 0, \pm\sqrt{3}, \pm\sqrt{6}, \pm\alpha_i , \qquad 1 \leq i \leq 3 .$$

https://doi.org/10.1017/S0027763000018547 Published online by Cambridge University Press

Les espaces propres correspondant à chacune des valeurs propres non nulles sont de dimension 1. L'espace propre associé à la valeur propre 0 est de dimension 2. Il est facile de voir qu'il est engendré par les deux formes primitives normalisées $G_6^{(5)} - 3G_3^{(5)}$ et $G_6^{(5)} + 3(G_3^{(5)} + G_5^{(5)})$. On détermine sans peine les autres formes primitives. Le résultat est le suivant:

PROPOSITION 1.3.1. *Les formes primitives normalisées de* $\langle \Gamma_0(3^5), 2\rangle_0$ *sont les douze formes* $F_i^{(5)}$, $1 \leq i \leq 12$:

(a) $F_1^{(5)} = G_6^{(5)} - 3G_3^{(5)}$

$$\equiv q - 2q^4 - 4q^7 - 7q^{13} + 4q^{16} - q^{19} - 5q^{25} + 8q^{28} + 11q^{31} \pmod{q^{37}} ;$$

$$F_2^{(5)} = G_6^{(5)} + 3(G_3^{(5)} + G_5^{(5)})$$

$$\equiv q - 2q^4 + 5q^7 + 2q^{13} + 4q^{16} + 8q^{19} - 5q^{25} - 10q^{28} - 7q^{31} \pmod{q^{37}} ;$$

(b) $F_3^{(5)} = G_1^{(5)} - 3G_5^{(5)} + \sqrt{3}\,[2G_9^{(5)} + G_{11}^{(5)}]$

$$\equiv q + \sqrt{3}\cdot q^2 + q^4 + 2\sqrt{3}\cdot q^5 - q^7 - \sqrt{3}\cdot q^8 + 6q^{10} - 2\sqrt{3}\cdot q^{11} + 5q^{13} - \sqrt{3}\cdot q^{14} - 5q^{16} - q^{19} + 2\sqrt{3}\cdot q^{20} - 6q^{22} - 4\sqrt{3}\cdot q^{23} \pmod{q^{24}} ;$$

$F_4^{(5)} = G_1^{(5)} - 3G_5^{(5)} - \sqrt{3}\,[2G_9^{(5)} + G_{11}^{(5)}]$;

(c) $F_5^{(5)} = 2G_1^{(5)} - 3G_3^{(5)} - G_6^{(5)} + \sqrt{6}\,(-G_9^{(5)} + G_{11}^{(5)})$,

$F_6^{(5)} = 2G_1^{(5)} - 3G_3^{(5)} - G_6^{(5)} - \sqrt{6}\,(-G_9^{(5)} + G_{11}^{(5)})$;

(d) $F_{6+i}^{(5)} = (\alpha_i - 1)(G_2^{(5)} + G_8^{(5)}) + (\alpha_i^2 - \alpha_i - 2)(G_4^{(5)} + 3G_{10}^{(5)}) + G_7^{(5)} + G_{12}^{(5)}$, $1 \leq i \leq 3$.

(e) $F_{9+i}^{(5)} = (\alpha_i - 1)(G_2^{(5)} - G_8^{(5)}) + (\alpha_i^2 - \alpha_i - 2)(G_4^{(5)} - 3G_{10}^{(5)}) + G_7^{(5)} - G_{12}^{(5)}$, $1 \leq i \leq 3$.

2. Courbes elliptiques de conducteur une puissance de 3

2.1. Conjecture de Weil

Soit $f(z)$ un élément de $\langle \Gamma_0(3^\nu), 2\rangle_0$ qui est fonction propre des opérateurs de Hecke $T(p)$, pour tout $p \neq 3$, et supposons que les valeurs propres associées soient des entiers rationnels. D'après Shimura ([8], Th. 1), il existe alors un morphisme canonique, surjectif, défini sur $\boldsymbol{Q}$:

$$\varphi_f : J_0(3^\nu) \to E_f ,$$

où E_f est une courbe elliptique, définie sur $\boldsymbol{Q}$. De plus, la série L de la

courbe E_f coïncide, au facteur local en 3 près, avec la série de Dirichlet associée à f.

On a déterminé dans le paragraphe 1 les formes primitives de poids 2 normalisées sur $\Gamma_0(3^\nu)$, pour $\nu = 3, 4, 5$ resp. Trois d'entre elles ont des coefficients entiers rationnels. Ce sont:

$F_1^{(3)}$, qui est l'unique forme primitive normalisée de poids 2 sur $\Gamma_0(3^3)$;

$F_1^{(5)}$, $F_2^{(5)}$, qui sont primitives sur $\Gamma_0(3^5)$.

Considérons les trois courbes elliptiques associées. Ces courbes ne sont pas isogènes sur $\boldsymbol{Q}$, puisque leurs séries L sont distinctes. En outre, chacune d'entre elles a bonne réduction en dehors de 3.

D'autre part, on connait toutes les courbes elliptiques définies sur $\boldsymbol{Q}$ qui ont bonne réduction en dehors de 3, cf. [1], appendice. Ces courbes se partagent en trois classes de $\boldsymbol{Q}$-isogénie; l'une de ces classes a pour conducteur 3^3, les deux autres ont pour conducteur 3^5; en particulier, le facteur local de la fonction L en 3 est 1 pour chacune des trois classes.

La comparaison de ces renseignements montre que les trois courbes associées à $F_1^{(3)}$ d'une part, $F_1^{(5)}$ et $F_2^{(5)}$ d'autre part, représentent les trois classes de $\boldsymbol{Q}$-isogénie en question. L'examen des premiers coefficients du développement de Fourier permet de reconnaître la classe correspondant à $F_1^{(5)}$ et celle correspondant à $F_2^{(5)}$.

On a ainsi démontré:

THÉORÈME 2.1.1 (*Conjecture de Weil pour les courbes de conducteur une puissance de* 3). *Soit* $L(s) = \sum_{n=1}^{\infty} a_n \cdot n^{-s}$ *la fonction L d'une courbe elliptique définie sur* $\boldsymbol{Q}$, *de conducteur* 3^ν (*donc* $\nu = 3$ *ou* 5). *Alors la série de Fourier*:

$$f(z) = \sum_{n=1}^{\infty} a_n \cdot q^n$$

est une forme primitive normalisée sur $\langle \Gamma_0(3^\nu), 2 \rangle_0$, *donc coïncide avec* $F_1^{(3)}$ *si* $\nu = 3$, *avec* $F_1^{(5)}$ *ou* $F_2^{(5)}$ *si* $\nu = 5$. *De plus, il existe un* $\boldsymbol{Q}$*-morphisme surjectif de* $J_0(3^\nu)$ *sur la courbe considérée.*

La courbe associée à $F_1^{(3)}$ est la courbe $X_0(27)$, d'équation:

$$y^2 + y = x^3 - 7$$

(cf. [1], table p. 209).

La classe d'isogénie correspondant à $F_1^{(5)}$, resp. $F_2^{(5)}$ est représentée par la courbe:

https://doi.org/10.1017/S0027763000018547 Published online by Cambridge University Press

$$y^2 + y = x^3 + 20 ,$$

resp.

$$y^2 + y = x^3 + 2$$

(loc. cit).

2.2. Multiplications complexes

Considérons les endomorphismes $R^*_{3,\pm}$ de $\langle \Gamma_0(3^\nu), 2\rangle_0$, $\nu = 3, 4, 5$, définis par:

$$R^*_{3,\pm} : f(z) \mapsto f(z \pm \tfrac{1}{3}) .$$

Soit $R^*_3 = R^*_{3,+} - R^*_{3,-}$.

Lorsque $f(z)$ est une forme primitive normalisée:

$$f | R^*_3 = i\sqrt{3} \cdot f_\chi ,$$

où f_χ note la forme tordue par le caractère de Legendre modulo 3 (cf. [5], I.3.4).

L'espace $\langle \Gamma_0(3^\nu), 2\rangle_0$ s'identifie de façon canonique à l'espace cotangent à l'origine à la variété $J_0(3^\nu)$. Les opérateurs $R^*_3, R^*_{3,\pm}$ sont induits par des endomorphismes $R_3, R_{3,\pm}$ de $J_0(3^\nu)$; ces endomorphismes sont définis sur $\boldsymbol{Q}(\sqrt{-3})$ (cf. [8], § 4; [5], I, 3.4).

Soit f l'une des trois formes primitives $F_1^{(3)}, F_1^{(5)}, F_2^{(5)}$; soit E_f la courbe elliptique associée à f (cf. [8], Prop. 3). Soit R l'un des endomorphismes $R_3, R_{3,\pm}$. Il existe un endomorphisme de la courbe E_f, noté encore R, qui rend commutatif le diagramme suivant:

$$\begin{array}{ccc} J_0(3^\nu) & \xrightarrow{R} & J_0(3^\nu) \\ {\scriptstyle \varphi_f}\downarrow & & \downarrow{\scriptstyle \varphi_f} \\ E_f & \xrightarrow{R} & E_f . \end{array}$$

L'anneau des endomorphismes de E_f contient donc $R_3, R_{3,\pm}$, qui vérifient:

$$R_3^2 = -3; \quad R_{3,+} + R_{3,-} = -1; \quad R_{3,+} - R_{3,-} = R_3 .$$

Par conséquent, la courbe E_f admet une multiplication complexe par l'anneau des entiers de $\boldsymbol{Q}(\sqrt{-3})$:

PROPOSITION 2.2.1. *Soit f l'une des trois formes primitives $F_1^{(3)}, F_1^{(5)}, F_2^{(5)}$. La courbe E_f associée à f admet une multiplication complexe par*

https://doi.org/10.1017/S0027763000018547 Published online by Cambridge University Press

l'anneau des entiers de $\boldsymbol{Q}(\sqrt{-3})$. *En particulier, son invariant est nul.*

Soit toujours f l'une des formes $F_1^{(3)}, F_1^{(5)}, F_2^{(5)}$, et considérons la courbe E_f. D'après Deuring, et la Prop. 2.2.1, la série L de E_f est associée à un Grössencharakter. Montrons comment cette remarque permet de déterminer *a priori* les formes $F_1^{(3)}, F_1^{(5)}$ et $F_2^{(5)}$.

Utilisons les notations de Shimura [7]. Soit $\omega = e^{2\pi i/3}$, et $K = \boldsymbol{Q}(\omega)$. Soit $\boldsymbol{m}$ un idéal entier de K, et λ un Grössencharakter modulo $\boldsymbol{m}$. La série L associée à λ est par définition:

$$L(\lambda, s) = \sum_{\mathfrak{a}} \lambda(\mathfrak{a}) \cdot N(\mathfrak{a})^{-s} ,$$

$\mathfrak{a}$ parcourant les idéaux entiers de K premiers à $\boldsymbol{m}$.

Le lemme 3 de [7] montre que les Grössencharaktere susceptibles de correspondre à des formes de poids 2 sont ceux qui vérifient:

$$\lambda((\alpha)) = \alpha \tag{2.2.2}$$

pour tout $\alpha \in K^\times$ tel que $\alpha \equiv 1 \bmod^\times \boldsymbol{m}$.

On note:

$$f_\lambda(z) = \sum_{\mathfrak{a}} \lambda(\mathfrak{a}) \cdot e^{2\pi i N(\mathfrak{a}) z} ,$$

$\mathfrak{a}$ parcourant les idéaux entiers de K premiers à $\boldsymbol{m}$. On dit que f_λ est la forme associée à λ. Enfin, on associe à λ un caractère de Dirichlet modulo $3 \cdot N(\boldsymbol{m})$:

$$\varepsilon_\lambda(a) = \left(\frac{-3}{a}\right) \cdot \frac{\lambda((a))}{a} ,$$

pour tout $a \in \boldsymbol{Z}$ premier à $\boldsymbol{m}$.

LEMME 2.2.3. a) *Il existe un unique Grössencharakter* $\lambda_1^{(3)}$ *de* K *de conducteur* 3, *et vérifiant* (2.2.2).

b) *Il existe exactement deux Grössencharaktere* $\lambda_1^{(5)}$ *et* $\lambda_2^{(5)}$ *de* K, *de conducteur* 9, *vérifiant* (2.2.2), *et tels que le caractère de Dirichlet associé soit le caractère unité. On a*:

$$\lambda_i^{(5)}((1 + 3\omega)) = \omega^i , \qquad i = 1, 2 .$$

Démonstration. Soit α un entier de K premier à 3. Alors un et un seul des trois nombres $\pm\alpha$, $\pm\omega\alpha$, $\pm\omega^2\alpha$ est congru à 1 (mod) 3, et $\lambda_1((\alpha))$ est le nombre en question; d'où (a).

https://doi.org/10.1017/S0027763000018547 Published online by Cambridge University Press

Soit α un entier de K, congru à $1 \pmod 3$. Alors un et un seul des neuf nombres $4^i(1+3\omega)^j\alpha$, $0 \leq i, j \leq 2$ est congru à $1 \pmod 9$. Par conséquent, la connaissance d'un Grössencharakter (mod 9) est déterminée par celle de $\lambda((4))$ et $\lambda((1+3\omega))$, qui sont nécessairement des racines cubiques de l'unité. La condition sur ε_λ entraîne que $\lambda((4)) = 1$. Les possibilités $\lambda((1+3\omega)) = 1, \omega, \omega^2$ resp. donnent $\lambda_1^{(3)}, \lambda_1^{(5)}, \lambda_2^{(5)}$ resp.

Nous pouvons maintenant utiliser le Lemme 3 de [7]. Ce dernier montre que $F_1^{(3)}$ est un élément normalisé de $\langle \Gamma_0(3^3), 2\rangle_0$, et $F_1^{(5)}$, $F_2^{(5)}$ des éléments normalisés de $\langle \Gamma_0(3^5), 2\rangle_0$; on vérifie sans peine:

PROPOSITION 2.2.4. *Les formes $F_1^{(3)}, F_1^{(5)}, F_2^{(5)}$ resp. sont associées aux Grössencharaktere $\lambda_1^{(3)}, \lambda_1^{(5)}, \lambda_2^{(5)}$ resp.*

3. Description de $J_0(3^4)$

Le but de ce paragraphe est la description des courbes elliptiques qui sont des quotients de $J_0(3^4)$ en termes de réseaux complexes. La technique employée pour ce faire est celle décrite dans [5], I, § 4. Nons nous contenterons ici de rappeler brièvement les notations utilisées, en renvoyant à loc. cit. pour plus de détails.

3.1. Détermination des réseaux

Soit $\mathscr{H}(3^4)$ le groupe défini par [5], I, Prop. 3.2.3. Un premier calcul, élémentaire, permet de montrer:

LEMME 3.1.1. *Le groupe $\mathscr{H}(3^4)$ admet pour base sur Z les huit éléments suivants*:

$$(\tilde{c}\colon \tilde{1}), \qquad c \in \mathscr{B},$$

où $\mathscr{B} = \{2, 4, 7, 13, 25, 31, 34, 58\}$.

L'expression de $(\tilde{c}\colon \tilde{1})$, $1 \leq c < 3^4$, $(c, 3) = 1$, en fonction de cette base est donnée par la table 1.

Posons:

$$\text{(3.1.1.1)} \qquad \begin{cases} f_1 = F_1^{(3)}\ ; \\ f_2 = F_1^{(3)}(z) - 3F_1^{(3)}(3z)\ ; \\ f_3 = F_1^{(4)}\ ; \\ f_4 = F_2^{(4)}\ ; \end{cases}$$

https://doi.org/10.1017/S0027763000018547 Published online by Cambridge University Press

(cf. 1.1.1).

Les formes f_i, $1 \leq i \leq 4$ constituent une base de l'espace $\langle \Gamma_0(3^4), 2\rangle_0$; de plus, ce sont des vecteurs propres normalisés des opérateurs de Hecke; enfin, f_3 et f_4 sont primitives.

Soient $z_0, z_1 \in \mathfrak{H}^*$. On note:

$$\{z_0, z_1\}$$

le vecteur de $\boldsymbol{C}^4$ de coordonnées:

$$\{z_0, z_1\}_{f_i} = \int_{z_0}^{z_1} f_i(t)dt\,, \qquad (1 \leq i \leq 4)\,.$$

L'application

$$\xi : \mathscr{H}(3^4) \to \boldsymbol{C}^4$$

définie par:

$$\xi((\tilde{c} : \tilde{d})) = \left\{\frac{b}{d}, \frac{a}{c}\right\},$$

où $a, b, c, d \in \boldsymbol{Z}$ vérifient $ad - bc = 1$, et $\tilde{c} \equiv c \pmod{3^4}$, $\tilde{d} \equiv d \pmod{3^4}$, définit un isomorphisme

$$\xi : \mathscr{H}(3^4) \to L$$

où L est un réseau de $\boldsymbol{C}^4$.

D'après Shimura, cf. [8], § 3, les points de la jacobienne $J = J_0(3^4)$ à valeurs dans $\boldsymbol{C}$ s'identifient au quotient $\boldsymbol{C}^4/L$. L'application:

$$\varphi : \mathfrak{H}^* \to \boldsymbol{C}^4$$
$$z \mapsto \{0, z\}$$

définit par passage au quotient un plongement de $X_0(3^4)(\boldsymbol{C}) \simeq \mathfrak{H}^*/\Gamma_0(3^4)$ dans la jacobienne $J(\boldsymbol{C}) \simeq \boldsymbol{C}^4/L$; ce plongement envoie la pointe $z = 0$ de $X_0(3^4)$ sur l'origine de J.

Les formes f_1, f_2 ont des coefficients entiers rationnels; ceux de f_3 sont des entiers du corps $\boldsymbol{Q}(\sqrt{3})$, et ceux de f_4 se déduisent des précédents par conjugaison. D'après Shimura [8], Prop. 3, il existe donc trois morphismes canoniques, définis sur $\boldsymbol{Q}$, et surjectifs:

$$\varphi_1 : J \to E_1\,,$$
$$\varphi_2 : J \to E_2\,,$$
$$\varphi_A : J \to A\,,$$

https://doi.org/10.1017/S0027763000018547 Published online by Cambridge University Press

où E_1, E_2 sont des courbes elliptiques définies sur $\boldsymbol{Q}$, et A une variété abélienne de dimension 2, définie sur $\boldsymbol{Q}$.

Soient π_1, π_2, π_A les projections canoniques de $\boldsymbol{C}^4$ sur $\boldsymbol{C}, \boldsymbol{C}, \boldsymbol{C}^2$ correspondant à l'isomorphisme:

$$\boldsymbol{C}^4 \simeq \boldsymbol{C} \times \boldsymbol{C} \times \boldsymbol{C}^2 .$$

Posons

$$L_i = \pi_i(L) , \qquad i = 1, 2,$$

et

$$L_A = \pi_A(L) .$$

Si l'on identifie $J(C)$ à $\boldsymbol{C}^4/L$, les morphismes, φ_i, φ_A, i $= 1, 2$, s'obtiennent à partir de π_i, π_A par passage au quotient.

La conjugaison complexe opère sur L (cf. [5], I, Prop. 3.2.5). On note $L^{\pm}$ les sous-réseaux de L correspondant aux valeurs propres ± 1.

En termes des générateurs choisis au Lemme 3.1.1, la conjugaison complexe se traduit par les formules de la table 2. On en déduit:

LEMME 3.1.2. *Le réseau $L^{\pm}$ est engendré par les vecteurs*:

$$\gamma_1^{\pm} = \left\{0, \frac{1}{4}\right\} \pm \left\{0, -\frac{1}{4}\right\} ;$$

$$\gamma_2^{\pm} = \left\{0, \frac{1}{7}\right\} \pm \left\{0, -\frac{1}{7}\right\} ;$$

$$\gamma_3^{\pm} = \left\{0, \frac{1}{13}\right\} \pm \left\{0, -\frac{1}{13}\right\} ;$$

$$\gamma_4^{\pm} = \left\{0, \frac{1}{31}\right\} \pm \left\{0, -\frac{1}{31}\right\} .$$

La table 3 donne l'expression de $\gamma_k^{\pm}$, $k = 1, \cdots, 4$, en fonction des générateurs définis en 3.1.1, et inversement.

L'examen de la table 3 montre en particulier:

PROPOSITION 3.1.3. *Le réseau L est un sous-réseau d'indice 2^4 du réseau $\frac{1}{2}L^+ \oplus \frac{1}{2}L^-$. Plus précisément, soit*

$$z = \frac{1}{2} \sum_{k=1}^{4} (x_k \gamma_k^+ + y_k \gamma_k^-) , \qquad x_k, y_k \in \boldsymbol{Z} ,$$

un élément du réseau $\frac{1}{2}L^+ \oplus \frac{1}{2}L^-$. Alors

$$z \in L$$

si et seulement si $x_k \equiv y_k \pmod 2$, $1 \leq k \leq 4$.

3.1.4. Notons $\underline{c}$ la matrice diagonale qui représente l'action de $T(2)$ sur la base $\{f_1, \cdots, f_4\}$ de l'espace $\langle \Gamma_0(3^4), 2\rangle_0$:

$$\underline{c} = \operatorname{diag}(c_1, \cdots, c_4) .$$

(On sait, du reste, que $\underline{c} = \operatorname{diag}(0, 0, \sqrt{3}, -\sqrt{3})$, cf. 1.1).

L'action de $T(2)$ se traduit par la formule:

$$\underline{c}\cdot\{0, z\} = \{0, 2z\} + \left\{0, \frac{z+1}{2}\right\} + \left\{0, \frac{z}{2}\right\} - \left\{0, \frac{1}{2}\right\} , \tag{3.1.4.1}$$

pour tout $z \in \mathfrak{H}^*$; cf. [5].

Notons $\gamma^{\pm}_{k,i}$ la i-ième coordonnée de $\gamma^{\pm}_k$, $1 \leq i,\ k \leq 4$.

Procédant comme dans [5], I, 4.9, on écrit la formule (3.1.4.1), pour $\pm z = \frac{1}{4}, \frac{1}{7}, \frac{1}{13}, \frac{1}{31}$. On obtient ainsi, séparant les parties correspondant aux valeurs $+1$ et -1 de la conjugaison complexe, les deux systèmes suivants de quatre équations aux inconnues $\gamma^{\pm}_{k,i}$:

$$\begin{cases} (c_i - 2)\gamma^+_{1,i} + 2\gamma^+_{2,i} - 2\gamma^+_{3,i} = 0 ; \\ -\gamma^+_{1,i} + (c_i + 1)\gamma^+_{2,i} - \gamma^+_{3,i} = 0 ; \\ -\gamma^+_{2,i} + (c_i + 1)\gamma^+_{3,i} + \gamma^+_{4,i} = 0 ; \\ \gamma^+_{1,i} - \gamma^+_{2,i} + \gamma^+_{3,i} + c_i\cdot\gamma^+_{4,i} = 0 . \end{cases} \tag{3.1.4.2}$$

resp.

$$\begin{cases} c_i\cdot\gamma^-_{1,i} = 0 ; \\ -\gamma^-_{1,i} + (c_i + 1)\gamma^-_{2,i} - \gamma^-_{3,i} = 0 ; \\ -\gamma^-_{2,i} + (c_i - 1)\gamma^-_{3,i} + \gamma^-_{4,i} = 0 ; \\ \gamma^-_{1,i} - \gamma^-_{2,i} + \gamma^-_{3,i} + c_i\cdot\gamma^-_{4,i} = 0 . \end{cases} \tag{3.1.4.3}$$

Le système (3.1.4.2) resp. (3.1.4.3) n'a de solutions non triviales que pour $c_i \in \{0, \pm\sqrt{3}\}$. Pour $c_i = \pm\sqrt{3}$, le système est de rang 3, ce qui détermine $\gamma^+_{k,i}$ resp. $\gamma^-_{k,i}$ à une constante multiplicative près.

Lorsque $c_i = 0$, les systèmes considérés sont de rang 2. On doit alors utiliser l'identité:

$$f_2(z) = f_1(z) - 3f_1(3z) , \qquad \text{cf. (3.1.1.1)}$$

qui entraîne:

$$\{0, z\}_{f_2} = \{0, z\}_{f_1} - \{0, 3z\}_{f_1} .$$

https://doi.org/10.1017/S0027763000018547 Published online by Cambridge University Press

Les résultats obtenus sont rassemblés dans la table 4. On a posé

$$\omega_1^+ = \gamma_{1,1}^+;\ \omega_2^+ = -3\omega_1^+;\ \omega_3^+ = \gamma_{2,3}^+;\ \omega_4^+ = \gamma_{2,4}^+;$$
$$\omega_1^- = \gamma_{1,1}^-;\ \omega_2^- = \gamma_{1,1}^-;\ \omega_3^- = \gamma_{2,3}^-;\ \omega_4^- = \gamma_{2,4}^- .$$

3.2. Pointes de $X_0(3^4)$

Soit z une pointe de $X_0(3^4)$. Pour calculer $\{0, z\}$, nous procéderons comme dans [5], I, 4.10. Plus précisément, on utilise la formule (3.1.4.1), ainsi que [5], Prop. 3.2.4.

Montrons comment se fait le calcul pour la pointe à l'infini. La formule (3.1.4.1) s'écrit:

$$(\underline{c} - 3)\cdot\{0, \infty\} = -\{0, \tfrac{1}{2}\} = -\gamma_1^+ + \gamma_2^+ - \gamma_3^+ - \gamma_4^+$$

(en utilisant la table 3).

D'après la table 4, on a donc:

$$\{0, \infty\}_{f_1} = \tfrac{1}{3}\omega_1^+ ;$$
$$\{0, \infty\}_{f_2} = 0 ;$$
$$\{0, \infty\}_{f_3} = (\sqrt{3}/3)\omega_3^+ ;$$
$$\{0, \infty\}_{f_4} = -(\sqrt{3}/3)\omega_4^+ .$$

Les résultats obtenus sont rassemblés dans la table 5, où l'on a posé:

$$\{0, \pm z\} = \tfrac{1}{2}[X(z, k)\cdot\omega_k^+ \pm Y(z, k)\cdot\omega_k^-] , \qquad 1 \leq k \leq 4 .$$

3.3. Utilisation de R_3^*

Considérons à nouveau l'opérateur R_3^*, cf. 2.2. On a:

$$f_1 | R_3^* = i\sqrt{3}\cdot f_1 = i\sqrt{3}\cdot f_{1,\chi} ;$$
$$f_3 | R_3^* = i\sqrt{3}\cdot f_4 = i\sqrt{3}\cdot f_{3,\chi} ;$$
$$f_4 | R_3^* = i\sqrt{3}\cdot f_3 = i\sqrt{3}\cdot f_{4,\chi} .$$

(On note f_χ la forme tordue de f par le caractère de Legendre modulo 3).

Appliquons à f_1, f_3, f_4 l'analogue de [5], I, Lemme 4.11.3.1. On a:

$$\{0, z\}_{f_\chi} = -\frac{i\sqrt{3}}{3}\left[\left\{\frac{1}{3}, z + \frac{1}{3}\right\}_f - \left\{\frac{2}{3}, z + \frac{2}{3}\right\}_f\right] .$$

Faisons $z = \infty$ dans cette formule; compte tenu des résultats de la table 5, ceci donne, pour f_1:

https://doi.org/10.1017/S0027763000018547 Published online by Cambridge University Press

(3.3.1) $$\omega_1^+ = \frac{i\sqrt{3}}{3}\omega_1^- \ ;$$

et pour f_3, f_4:

(3.3.2) $$\begin{cases} \omega_4^+ = -\dfrac{i\sqrt{3}}{3}\cdot\omega_3^- \ ; \\ \omega_3^+ = -\dfrac{i\sqrt{3}}{3}\cdot\omega_4^- \ . \end{cases}$$

La Prop. 3.1.3, et le fait que L soit un réseau dans $\boldsymbol{C}^4$, entraînent que tout vecteur $z = (z_1, \cdots, z_4)$ de $\boldsymbol{C}^4$ s'écrit de façon unique:

$$z = \frac{1}{2}\sum_{k=1}^{4}(x_k\gamma_k^+ + y_k\gamma_k^-) \ , \qquad \text{où } x_k, y_k \in \boldsymbol{R} \ .$$

Soient $L_i = \pi_i(L)$, $i = 1, 2$. Soient:

$$z_i = \tfrac{1}{2}(a_i\omega_i^+ + b_i\omega_i^-) \ , \qquad i = 1, 2 \ .$$

Tout vecteur de $\boldsymbol{C}$ s'écrit de façon unique sous cette forme, avec a_i, $b_i \in \boldsymbol{R}$.

Soit enfin $L_A = \pi_A(L)$. Notons:

(3.3.3) $$M_k(a, b, c, d) = \tfrac{1}{2}[a\omega_k^+ + b\omega_k^- + \sqrt{3}\,(c\omega_k^+ + d\omega_k^-)] \ , \qquad k = 3, 4 \ .$$

PROPOSITION 3.3.4. a) *Pour que $z_i \in \boldsymbol{C}$ soit un élément du réseau L_i $(i = 1, 2)$, il faut et il suffit qu'il existe $a_i, b_i \in \boldsymbol{Z}$, $a_i \equiv b_i \pmod 2$, tels que*

$$z_i = \tfrac{1}{2}(a_i\omega_i^+ + b_i\omega_i^-) \ .$$

b) *Pour que $(z_3, z_4) \in \boldsymbol{C}^2$ soit un élément du réseau L_A, il faut et il suffit qu'il existe $a, b, c, d \in \boldsymbol{Z}$, $a \equiv b \pmod 2$, $c \equiv d \pmod 2$, tels que:*

$$(z_3, z_4) = (M_3(a, b, c, d), M_4(a, b, -c, -d)) \ .$$

Démonstration. Soit $z \in \boldsymbol{C}^4$ un vecteur de L, que nous écrivons:

$$z = \frac{1}{2}\sum_{k=1}^{4}(x_k\gamma_k^+ + y_k\gamma_k^-) \ , \quad x_k, y_k \in \boldsymbol{Z} \ , \quad x_k \equiv y_k \pmod 2 \ .$$

On a donc:

$$z_i = \frac{1}{2}\sum_{k=1}^{4}(x_k\gamma_{k,i}^+ + y_k\gamma_{k,i}^-) \ , \qquad 1 \leq i \leq 4 \ .$$

Tirant de la table 4 les valeurs de $\gamma_{k,i}^{\pm}$ en fonction de $\omega_i^{\pm}$, et tenant compte des identités (3.3.2), on obtient la nécessité des conditions de la proposition.

https://doi.org/10.1017/S0027763000018547 Published online by Cambridge University Press

On a porté dans la table 6 l'expression de a_i, b_i $(i = 1, 2)$, a, b, c, d, en fonction de x_k, y_k, $1 \leq k \leq 4$, et réciproquement. Inversement, il est clair que $z_i = \frac{1}{2}(a_i\omega_1^+ + b_i\omega_1^-)$, $i = 1, 2$, $a_i, b_i \in \boldsymbol{Z}$, $a_i \equiv b_i \pmod 2$, est la i-ième projection du vecteur $\frac{1}{2}(a_i\gamma_i^+ + b_i\gamma_i^-) \in L$.

Enfin $(M_3(a, b, c, d), M_4(a, b, -c, -d))$ est l'image par π_A du vecteur $\frac{1}{2}(a\gamma_2^+ + b\gamma_2^- + c\gamma_3^+ + d\gamma_3^-)$ qui est un élément de L; d'où la suffisance.

Corollaire. Tout vecteur de $\boldsymbol{C}^2$ s'écrit de façon unique

$$(z_3, z_4) = (M_3(a, b, c, d), M_4(a, b, -c, -d)) ,$$

où $a, b, c, d \in \boldsymbol{R}$.

Nous allons également tirer de la table 6 le résultat suivant:

PROPOSITION 3.3.5. *Le noyau du morphisme canonique*

$$J \to E_1 \times E_2 \times A$$

est produit de deux groupes cycliques d'ordre 3. *Plus précisément, identifiant les points de J au quotient de $\boldsymbol{C}^4$ par L, ce noyau est engendré par les vecteurs*:

$$\tfrac{1}{3}(\gamma_1^+ - \gamma_4^+) + \tfrac{1}{3}(\gamma_1^- - 2\gamma_2^- - \gamma_4^-)$$

et

$$\tfrac{2}{3}(\gamma_1^- + \gamma_2^- + \gamma_4^-) \qquad \text{de } \boldsymbol{C}^4 .$$

Démonstration. Il résulte immédiatement de l'examen de la table 6 que le noyau considéré est annulé par la multiplication par 3. C'est donc un espace vectoriel sur $\boldsymbol{F}_3$, de dimension égale au rang du système de la table 6 (sur $\boldsymbol{F}_3$); ce rang est 2; le calcul explicite donne aisément le résultat annoncé.

Il est commode d'exprimer les coordonnées des pointes de $X_0(3^4)$ en fonction de a_i, b_i, $i = 1, 2$, a, b, c, d; ceci est fait dans la table 7.

4. Applications

4.1. Courbes elliptiques de conducteur 27

On sait (par ex. [1], appendice) qu'il existe quatre courbes elliptiques définies sur $\boldsymbol{Q}$, de conducteur 27, et que ces courbes sont $\boldsymbol{Q}$-isogènes entre elles. Nous allons retrouver l'existence de ces courbes et des isogénies qui les relient en utilisant les résultats du paragraphe 3.

https://doi.org/10.1017/S0027763000018547 Published online by Cambridge University Press

4.1.1. Rappelons quelle est l'action du groupe de Galois $G_Q = \mathrm{Gal}(\bar{Q}/Q)$ sur les pointes de la courbe $X_0(3^4)$; toutes ces pointes sont rationnelles sur le corps des racines neuvièmes de l'unité $Q(e^{2\pi i/9}) = K'$. Soit:

$$n \mapsto [n]$$
$$(Z/9Z)^\times \to \mathrm{Gal}(K'/Q) = G$$

l'isomorphisme canonique. Alors G est engendré par l'élément [2]. Si $z = a/d$, ($a \in Z$, d divise 3^4) représente une pointe de $X_0(3^4)$, la transformée par [2] de cette pointe est représentée par $z' = 5a/d$ (cf. [5], II, § 3). En particulier, [2] laisse stables les pointes 0 et ∞, et échange $\pm 1/3$, resp. $\pm 1/27$.

Enfin, soit N un entier > 1, et μ_N le G_Q-module galoisien formé des racines N-ièmes de l'unité. On note $\mu_N^{\otimes k}$ le produit tensoriel de k copies de μ_N, muni de sa structure de G_Q-module. Cette notation ne dépend que de $k \bmod \varphi(N)$. En particulier, on note $Z/NZ = \mu_N^{\otimes 0}$; cf. [5], I, 2.5.

4.1.2. Considérons les courbes E_1, E_2 associées aux formes f_1, f_2, cf. 3.1.1.1. Ces deux courbes elliptiques sont de conducteur 27, la courbe E_1 n'étant rien d'autre que la courbe modulaire $X_0(27)$.

Soient C_1, C_2 resp. les sous-groupes engendrés dans E_1, resp. E_2 par les images des pointes de $X_0(3^4)$; le groupe G permute les pointes, et fait ainsi de C_1, C_2 des G_Q-modules galoisiens. Le lemme suivant détermine leur structure:

LEMME 4.1.2.1.

$$C_1 \cong Z/3Z \oplus \mu_3 ; \qquad C_2 \cong \mu_9^{\otimes 2} \oplus \mu_3 .$$

Démonstration. Posons $\omega_i^+/\omega_i^- = 2\tau_i - 1$, $i = 1, 2$. D'après la Prop. 3.3.4, a), les points de E_i à valeurs dans C s'identifient au quotient C/L_i, où

$$L_i = \omega_i^- \cdot [1, \tau_i] , \qquad i = 1, 2 .$$

La table 7 montre que les coordonnées des images des pointes dans le parallélogramme fondamental du réseau $[1, \tau_i]$, construit sur $1, \tau_i$, sont les suivantes:

https://doi.org/10.1017/S0027763000018547 Published online by Cambridge University Press

pointes	réseau $[1,\tau_1]$
0	(0, 0)
∞, $\pm\frac{1}{27}$	$(\frac{2}{3}, \frac{2}{3})$
$\frac{1}{3}$	$(\frac{2}{3}, 0)$
$-\frac{1}{3}$	$(\frac{1}{3}, 0)$
$\frac{1}{9}$, $\frac{4}{9}$, $\frac{7}{9}$	$(\frac{1}{3}, \frac{2}{3})$
$-\frac{1}{9}$ $-\frac{4}{9}$ $-\frac{7}{9}$	$(0, \frac{2}{3})$

pointes	réseau $[1, \tau_2]$
0, ∞	(0, 0)
$\frac{1}{3}$, $-\frac{1}{27}$	$(\frac{1}{3}, \frac{2}{3})$
$-\frac{1}{3}$, $\frac{1}{27}$	$(0, \frac{2}{3})$
$\pm\frac{1}{9}$	$(\frac{7}{9}, \frac{4}{9})$
$\pm\frac{2}{9}$	$(\frac{4}{9}, \frac{1}{9})$
$\pm\frac{4}{9}$	$(\frac{1}{9}, \frac{7}{9})$

L'image de ∞ engendre dans E_1 un groupe d'ordre 3 formé de points $\boldsymbol{Q}$-rationnels, donc isomorphe à $Z/3Z$.

L'image de $\frac{1}{3}$ engendre dans E_1 un groupe d'ordre 3 formé de points rationnels sur le corps $\boldsymbol{Q}(\omega)$ des racines cubiques de l'unité; l'élément non-trivial du groupe de Galois permute les images des pointes $\frac{1}{3}$ et $-\frac{1}{3}$; d'où un $G_{\boldsymbol{Q}}$-module isomorphe à $\boldsymbol{\mu}_3$. Enfin, la somme directe des deux groupes considérés contient les images de toutes les pointes.

Soient P, P' les images dans E_2 des pointes $\frac{1}{9}, \frac{1}{3}$. Les images dans E_2 des pointes $-\frac{1}{3}, \frac{2}{9}, \frac{4}{9}$ resp. sont $3P + 2P'$, $7P$, $4P$ resp. Soit

$$Q = 3P + P' .$$

On a:

$$P^{[2]} = 4P ;$$
$$Q^{[2]} = -Q .$$

Ceci montre: le groupe engendré par P est isomorphe à $\boldsymbol{\mu}_9^{\otimes 2}$; le groupe engendré par Q est isomorphe à $\boldsymbol{\mu}_3$; C_2 est la somme directe de ces deux groupes.

Le groupe $\boldsymbol{\mu}_9^{\otimes 2}$ s'insère dans une suite exacte canonique de G-modules:

$$0 \to Z/3Z \to \boldsymbol{\mu}_9^{\otimes 2} \to Z/3Z \to 0$$

(le sous-groupe de $\boldsymbol{\mu}_9^{\otimes 2}$ formé des points annulés par 3 est isomorphe à $Z/3Z$).

4.1.3. Soient E_2', E_2'', E_2''' resp. le quotient de E_2 par $Z/3Z$, $\boldsymbol{\mu}_9^{\otimes 2}$, $\boldsymbol{\mu}_3$ resp. On obtient un diagramme canonique formé d'isogénies de degré 3 définies

sur $\boldsymbol{Q}$:

$$E_2''' \leftarrow E_2 \rightarrow E_2' \rightarrow E_2'' .$$

PROPOSITION 4.1.3.1. a) *Les courbes* E_2, E_2', E_2''' *contiennent un point d'ordre* 3 *rationnel sur* $\boldsymbol{Q}$.

b) *L'anneau des endomorphismes de* E_2, E_2', *resp.* E_2'', E_2''' *est isomorphe à l'anneau* O_K *des entiers du corps* K *des racines cubiques de l'unité, resp. à un ordre d'indice* 3 *dans* O_K; *en particulier*:

$$j(E_2) = j(E_2') = 0 ; \qquad j(E_2'') = j(E_2''') = -3 \cdot 2^{15} \cdot 5^3$$

j *désignant la fonction invariant modulaire.*

c) *Les quatre courbes* E_2, E_2', E_2'', E_2''' *appartiennent à quatre classes de* $\boldsymbol{Q}$*-isomorphie distinctes. La courbe* E_2' *est isomorphe sur* $\boldsymbol{Q}$ *à la courbe* E_1.

Démonstration. a) Le groupe des points de E_2 annulé par 3 est isomorphe à $\boldsymbol{Z}/3\boldsymbol{Z} \oplus \boldsymbol{\mu}_3 \subseteq \boldsymbol{\mu}_9^{\otimes 2} \oplus \boldsymbol{\mu}_3$.

Le quotient E_2' de E_2 par le sous-groupe isomorphe à $\boldsymbol{Z}/3\boldsymbol{Z}$ contient $\boldsymbol{\mu}_9^{\otimes 2}/(\boldsymbol{Z}/3\boldsymbol{Z}) \cong \boldsymbol{Z}/3\boldsymbol{Z}$.

Enfin, le quotient E_2''' de E_2 par $\boldsymbol{\mu}_3$ contient $\boldsymbol{Z}/3\boldsymbol{Z} \subseteq \boldsymbol{\mu}_9^{\otimes 2}$.

b) La courbe E_2 est associée au réseau L_2, où

$$L_2 = \omega_2^- \cdot [1, \tau_2] .$$

D'après (3.3.1), et $\omega_2^+ = -3\omega_1^+$, $\omega_2^- = \omega_1^-$

$$\tau_2 = -\omega ,$$

ce qui montre que $[1, \tau_2]$ est isomorphe à O_K.

La courbe E_2' est associée au réseau:

$$L_2' = \omega_2^- \cdot \left[1, \frac{1-\omega}{3}\right]$$
$$= \frac{1-\omega}{3} \cdot \omega_2^- [1, \omega] ;$$

par conséquent, L_2' est homothétique au réseau O_K.

La courbe E_2'' est associée au réseau:

$$L_2'' = \omega_2^- \cdot \left[1, \frac{4-\omega}{9}\right]$$

https://doi.org/10.1017/S0027763000018547 Published online by Cambridge University Press

$$= \omega_2^- \cdot \left(\frac{2\omega + 1}{9}\right) \cdot [1, 3\omega] .$$

Enfin, la courbe E_2''' est associée au réseau:

$$L_2''' = \omega_2^- \cdot \left[\frac{1}{3}, \omega\right] = \frac{\omega_2^-}{3}[1, 3\omega] .$$

On a donc: $j(E_2) = j(E_2') = 0$;

$$j(E_2'') = j(E_2''') = -3 \cdot 2^{15} \cdot 5^3 .$$

c) La courbe E_2 n'est pas isomorphe sur $\boldsymbol{Q}$ à la courbe E_2'. En effet, le quotient de E_2 par le sous-groupe $Z/3Z$ qu'elle contient est E_2', d'invariant nul, alors que le quotient de E_2' par son sous-groupe isomorphe à $Z/3Z$ est E_2'', dont l'invariant est non nul.

On sait que le graphe des 3-isogénies entre les courbes de conducteur 27 ne contient pas de cycle; donc E_2'' et E_2''' ne sont pas $\boldsymbol{Q}$-isomorphes.

La courbe E_1 est associée au réseau:

$$L_1 = \omega_1^- \cdot [1, \tau_1] ;$$

d'après (3.3.1), on a:

$$\tau_1 = \frac{1}{2}\left(1 + i\frac{\sqrt{3}}{3}\right) ,$$

d'où

$$L_1 = \frac{\omega_1^-}{3}(2 + \omega) \cdot [1, \omega] .$$

La courbe E_1 coïncide donc avec la courbe E_2 ou la courbe E_2' (on pourrait aussi remarquer que le groupe des points de E_1 annulé par 3 est isomorphe à $Z/3Z \oplus \boldsymbol{\mu}_3$, pour obtenir la même conclusion).

Le quotient de E_1 par le sous-groupe isomorphe à $\boldsymbol{\mu}_3$ est associé au réseau:

$$\frac{\omega_1^-}{3}[1, 3\tau_1] = \frac{\omega_1^-}{3}[1, \omega] .$$

Ce quotient a donc un invariant nul. Ceci montre que E_1 est isomorphe à E_2', et non à E_2.

4.2. La variété abélienne A

Considérons la variété abélienne A associée aux formes f_3, f_4, cf. 3.1.1.1.

https://doi.org/10.1017/S0027763000018547 Published online by Cambridge University Press

Cette variété est définie sur $\boldsymbol{Q}$, de dimension 2. On a:

$$A(\boldsymbol{C}) \cong \boldsymbol{C}^2/L_A .$$

L'opérateur de Hecke $T(2)$ définit un endomorphisme de A, défini sur $\boldsymbol{Q}$.

L'opérateur R_3^* (cf. 2.2) définit un endomorphisme R_3 de A, défini sur le corps $K = \boldsymbol{Q}(\omega)$. Soit ε l'automorphisme non trivial de K.

On a:

$$R_3^\varepsilon = -R_3 ;$$
$$R_3 \circ T(2) + T(2) \circ R_3 = 0$$
$$R_3^2 = -3 ; \qquad T(2)^2 = 3 .$$

Soit $\lambda = T(2) - R_3$, $\lambda^\varepsilon = T(2) + R_3$.

Soit $B = \operatorname{Im} \lambda$, $B^\varepsilon = \operatorname{Im} \lambda^\varepsilon$. Alors B et B^ε sont des courbes elliptiques définies sur K.

Notons $K' = \boldsymbol{Q}(e^{2\pi i/9})$.

Nous allons montrer:

PROPOSITION 4.2.1. a) *On a* $B = \operatorname{Ker} \lambda$, $B^\varepsilon = \operatorname{Ker} \lambda^\varepsilon$.

b) *Les points de 3-division de la courbe elliptique* B (*resp.* B^ε) *sont rationnels sur* K'. *Il existe une base des points de 3-division de* B *telle que l'action de* $\operatorname{Gal}(K'/K)$ *soit donnée par la matrice*

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

de $GL_2(\boldsymbol{F}_3)$.

c) *Soit* C *le sous-groupe d'ordre* 3 *de* B *formé de points rationnels sur* K. *Alors* $B \cap B^\varepsilon$ *est le produit de* C *par le groupe des points de 2-division de* B (*resp.* B^ε).

d) *On a*:

$$B/C \cong B^\varepsilon ,$$
$$B^\varepsilon/C \cong B ;$$

e) *Soit* $i: B \cap B^\varepsilon \to B \times B^\varepsilon$ *l'application* $b \mapsto (b, -b)$

et

$$j: B \times B^\varepsilon \to A$$
$$(b, b') \mapsto b + b' .$$

https://doi.org/10.1017/S0027763000018547 Published online by Cambridge University Press

La suite exacte:

$$0 \longrightarrow B \cap B^s \xrightarrow{i} B \times B^s \xrightarrow{j} A \longrightarrow 0$$

fait de A *la somme amalgamée de* B *et* B^s *le long de* $B \cap B^s$. *Le morphisme*:

$$B \times B^s \xrightarrow{\mathrm{pr}_2} B^s \longrightarrow B^s/B \cap B^s ,$$

resp.

$$B \times B^s \xrightarrow{\mathrm{pr}_1} B \longrightarrow B/B \cap B^s ,$$

se factorise à travers $j: B \times B^s \to A$.

Identifiant $B^s/B \cap B^s$ *à* B, *resp.* $B/B \cap B^s$ *à* B^s, *le morphisme obtenu*:

$$A \to B$$

resp.

$$A \to B^s$$

s'identifie à λ, *resp.* λ^s.

Remarque. La partie de (b) concernant le corps de rationalité des points de 3-division de B est démontrée par Koike dans [3], en utilisant les traces des opérateurs de Hecke. Dans ce qui suit, nous démontrons la Prop. 4.2.1.

4.2.2. D'après 1.1, l'opérateur de Hecke $T(2)$ est induit par l'application:

$$(z_3, z_4) \mapsto (\sqrt{3} \cdot z_3, -\sqrt{3} \cdot z_4)$$

de C^2 dans lui-même.

De:

$$f_3 | R_3^* = i\sqrt{3} \cdot f_4 ,$$
$$f_4 | R_3^* = i\sqrt{3} \cdot f_3 ,$$

résulte que R_3 est induit par l'application:

$$(z_3, z_4) \mapsto (i\sqrt{3} \cdot z_4, i\sqrt{3} \cdot z_3)$$

de C^2 dans lui-même.

On en déduit que λ est induit par l'application $\tilde{\lambda}$:

$$\tilde{\lambda}: C^2 \to C^2$$
$$(z_3, z_4) \mapsto (\sqrt{3}(z_3 - iz_4), -\sqrt{3}(z_4 + iz_3)) .$$

Il en résulte en particulier que l'image de $\tilde{\lambda}$ est isomorphe à $\boldsymbol{C}$, et formée des couples $(z_3, -iz_3)$, où $z_3 \in \boldsymbol{C}$.

Utilisons maintenant les notations de (3.3.3). Un calcul facile, utilisant les identités (3.3.2) montre que $\tilde{\lambda}$ correspond à l'application:

$$M(a, b, c, d) \mapsto M(3(b + c), 3d - a, a - 3d, b + c) .$$

Rappelons que le réseau L_A est défini par les conditions:

$$a, b, c, d \in \boldsymbol{Z} ;$$
$$a \equiv b \pmod 2;$$
$$c \equiv d \pmod 2 .$$

On vérifie que

$$\tilde{\lambda}(L_A) \subseteq L_A .$$

On voit aussi que l'image de $\tilde{\lambda}$ est caractérisée par les équations:

(4.2.2.0)
$$\begin{cases} a, b, c, d \in \boldsymbol{R} ; \\ a = 3d ; \qquad b + c = 0 . \end{cases}$$

Posons

$$2\tau_B - 1 = \sqrt{3} \cdot \frac{\sqrt{3} \cdot \omega_3^+ + \omega_3^-}{\sqrt{3} \cdot \omega_3^+ - \omega_3^-} .$$

On a alors:

$$M_3(3d, b, -b, d) = (\sqrt{3} \cdot \omega_3^+ - \omega_3^-) \cdot \left(-\frac{b + d}{2} + d \cdot \tau_B \right) .$$

Enfin, pour que $M(3d, b, -b, d)$ soit un vecteur de L_A, il faut et il suffit que le vecteur $-(b + d)/2 + d \cdot \tau_B$ appartienne au réseau $[1, \tau_B]$. Ceci montre que la courbe B est associée au réseau $[1, \tau_B]$.

Nous aurons besoin plus loin de l'expression de $\tilde{\lambda}^\varepsilon$. Procédant comme pour $\tilde{\lambda}$, on montre que $\tilde{\lambda}^\varepsilon$ correspond à l'application:

$$M(a, b, c, d) \mapsto M(3(c - b), a + 3d, a + 3d, b - c) .$$

Posons:

$$2\tau_{B^\varepsilon} - 1 = \sqrt{3} \cdot \frac{\sqrt{3} \cdot \omega_3^+ - \omega_3^-}{\sqrt{3} \cdot \omega_3^+ + \omega_3^-} .$$

On a alors:

https://doi.org/10.1017/S0027763000018547 Published online by Cambridge University Press

$$M_3(-3d, b, b, d) = (\sqrt{3}\cdot\omega_3^+ + \omega_3^-)\cdot\left(\frac{b+d}{2} - d\cdot\tau_{B^6}\right).$$

Pour que $M(-3d, b, b, d)$ soit un vecteur de L_A, il faut et il suffit que le vecteur $(b+d)/2 - d\cdot\tau_{B^6}$ appartienne au réseau $[1, \tau_{B^6}]$; la courbe B^6 est donc associée à ce réseau.

Remarquons que l'on a l'identité:

$$(2\tau_B - 1)(2\tau_{B^6} - 1) = 3\,. \tag{4.2.2.1}$$

Il en résulte:

$$\begin{cases} [1, \tau_{B^6}] = (2\tau_{B^6} - 1)\cdot\left[1, \dfrac{1+\tau_B}{3}\right]; \\ [1, \tau_B] = (2\tau_B - 1)\cdot\left[1, \dfrac{1+\tau_{B^6}}{3}\right]. \end{cases} \tag{4.2.2.2}$$

4.2.3. On sait que le noyau de λ contient B, puisque $\lambda^2 = 0$. Montrons que $\operatorname{Ker}\lambda = B$.

On a:

$$M^{-1}(\tilde{\lambda}^{-1}(L_A)) = \left\{(a, b, c, d) \in \boldsymbol{R}^4 \;\middle|\; \begin{array}{l} a - 3d \in \boldsymbol{Z} \\ b + c \in \boldsymbol{Z} \\ a - 3d \equiv b + c \pmod 2 \end{array}\right\}.$$

Pour tout élément $M(a, b, c, d)$ de $\tilde{\lambda}^{-1}(L_A)$, on a:

$$M(a - 3d, b + c, 0, 0) \in L_A\,.$$

Par conséquent, tout élément de $\tilde{\lambda}^{-1}(L_A)$ est congru, modulo L_A, à un élément de la forme:

$$M(3d, -c, c, d)$$

c'est-à-dire, d'après (4.2.2.0), à un élément de l'image de $\tilde{\lambda}$. En d'autres termes:

$$\tilde{\lambda}(\boldsymbol{C}^2) + L_A = \tilde{\lambda}^{-1}(L_A)\,.$$

On a donc:

$$\operatorname{Ker}\lambda = \tilde{\lambda}^{-1}(L_A)/L_A \cong \tilde{\lambda}(\boldsymbol{C}^2)/\tilde{\lambda}(\boldsymbol{C}^2) \cap L_A = B\,, \qquad d'\text{où (a)}\,.$$

4.2.4. La table 7 montre que les projections des pointes $0, \frac{1}{3}, \frac{2}{3}, \frac{1}{9}, \frac{4}{9}, \frac{7}{9}$ de $X_0(3^4)$ sur A sont dans le noyau de λ, donc dans B. Ramenées dans le parallélogramme construit sur $1, \tau_B$, ces projections ont les coordonnées

https://doi.org/10.1017/S0027763000018547 Published online by Cambridge University Press

indiquées dans le tableau suivant:

pointe	0	$\frac{1}{3}$	$\frac{2}{3}$	$\frac{1}{9}$	$\frac{4}{9}$	$\frac{7}{9}$
coordonnées	(0, 0)	$(\frac{1}{3}, \frac{1}{3})$	$(\frac{2}{3}, \frac{2}{3})$	$(\frac{2}{3}, \frac{1}{3})$	$(\frac{1}{3}, 0)$	$(0, \frac{2}{3})$

On voit que les images de ces pointes engendrent le groupe des points de B annulés par 3. Plus précisément, soient P, Q resp. les images de $\frac{1}{3}, \frac{1}{9}$ resp. Soit $K' = \boldsymbol{Q}(e^{2\pi i/9})$; rappelons que $K = \boldsymbol{Q}(\omega)$, avec $\omega = e^{2\pi i/3}$. L'action du générateur [4] de $\mathrm{Gal}\,(K'/K)$ sur les pointes est la suivante, cf. 4.1.1:

[4] laisse fixes $0, \frac{1}{3}, \frac{2}{3}$, et permute cycliquement les pointes $\frac{1}{9}, \frac{7}{9}, \frac{4}{9}$.

On a donc:

$$P^{[4]} = P\,;$$
$$Q^{[4]} = P + Q\,,$$

et, par rapport à la base $\{P, Q\}$, [4] est représenté par la matrice $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

On a ainsi démontré (b). Ce résultat permet à Koike de déterminer une équation de la courbe B (à ε-automorphisme près); cf. [3].

4.2.5. Soit C le sous-groupe d'ordre 3 engendré par l'image de la pointe $\frac{1}{3}$. Les autres points annulés par 3 ne sont pas rationnels sur K.

Déterminons $B \cap B^{\varepsilon}$.

On doit déterminer:

$$\tilde{\lambda}^{-1}(L_A) \cap (\tilde{\lambda}^{\varepsilon})^{-1}(L_A) \qquad (\text{modulo } L_A)\,.$$

Pour que $M(a, b, c, d)$ soit dans cette intersection, il faut et il suffit que l'on ait:

$$\text{(A)} \quad \begin{cases} a, b, c, d \in \boldsymbol{R}^4\,; \\ a - 3d \in \boldsymbol{Z}\,; \\ b + c \in \boldsymbol{Z}\,; \\ a + 3d \in \boldsymbol{Z}\,; \\ b - c \in \boldsymbol{Z}\,; \\ a - 3d \equiv b + c \pmod 2\,; \\ a + 3d \equiv b - c \pmod 2\,. \end{cases}$$

Enfin, pour que $M(a, b, c, d)$ soit dans L_A, il faut et il suffit que:

https://doi.org/10.1017/S0027763000018547 Published online by Cambridge University Press

$$(B)\quad \begin{cases} a, b, c, d \in \boldsymbol{Z} ; \\ a \equiv b \pmod 2 ; \\ c \equiv d \pmod 2 . \end{cases}$$

LEMME 4.2.5.1. *L'intersection* $B \cap B^{\epsilon}$ *est formée des classes* mod L_A *des douze vecteurs* $M(a, b, c, d)$, *où* (a, b, c, d) *est donné par le tableau suivant*:

$(0, 0, 0, 0)$	$(0, 1, 1, 0)$
$(\frac{1}{2}, \frac{1}{2}, \frac{3}{2}, \frac{1}{6})$	$(\frac{1}{2}, \frac{3}{2}, \frac{1}{2}, \frac{1}{6})$
$(0, 0, 1, \frac{1}{3})$	$(0, 1, 0, \frac{1}{3})$
$(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2})$	$(\frac{1}{2}, \frac{3}{2}, \frac{3}{2}, \frac{1}{2})$
$(0, 0, 0, \frac{2}{3})$	$(0, 1, 1, \frac{2}{3})$
$(\frac{1}{2}, \frac{1}{2}, \frac{3}{2}, \frac{5}{6})$	$(\frac{1}{2}, \frac{3}{2}, \frac{1}{2}, \frac{5}{6})$

Démonstration. On déduit des conditions (A): $2a, 2b, 2c, 6d \in \boldsymbol{Z}$. Posons:

$$2a = \alpha , \quad 2b = \beta , \quad 2c = \gamma , \quad 6d = \delta .$$

Les conditions (A) s'écrivent:

$$\alpha \equiv \beta \equiv \gamma \equiv \delta \pmod 2 ,$$
$$\delta \equiv \alpha - \beta - \gamma \pmod 4 .$$

Ces congruences admettent 16 solutions (mod 4).

Pour que $M(a, b, c, d)$ soit un élément de L_A, il faut et il suffit que:

$$\alpha \equiv \beta \equiv \gamma \equiv 0 \pmod 2 ; \qquad \delta \equiv 0 \pmod 6 ;$$
$$\alpha + \beta \equiv 0 \pmod 4 ; \qquad 3\gamma + \delta \equiv 0 \pmod{12} .$$

Ces congruences admettent 108 solutions (mod 12).

Par conséquent, $B \cap B^{\epsilon}$ contient $(16 \cdot 81)/108 = 12$ éléments.

Il est facile de déterminer des représentants, en utilisant le fait que, quitte à modifier $M(a, b, c, d)$ par un vecteur de L_A, on peut supposer:

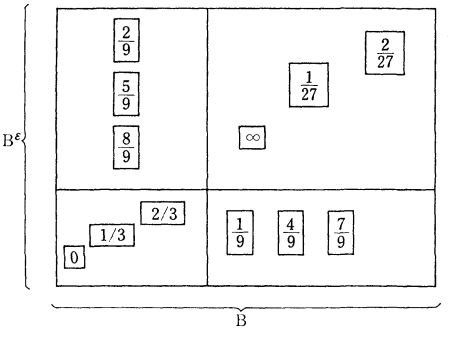
$$0 \leq \alpha \leq 1 ; \quad 0 \leq \beta, \gamma \leq 3 ; \quad 0 \leq \delta \leq 5 .$$

Rappelons que la courbe B est associée au réseau $[1, \tau_B]$, cf. (4.2.2). Dans le parallélogramme construit sur $1, \tau_B$, les douze points de $B \cap B^{\epsilon}$ ont pour coordonnées respectives:

$(0, 0)$	$(\frac{1}{2}, 0)$
$(\frac{2}{3}, \frac{1}{6})$	$(\frac{1}{6}, \frac{1}{6})$
$(\frac{5}{6}, \frac{1}{3})$	$(\frac{1}{3}, \frac{1}{3})$
$(\frac{1}{2}, \frac{1}{2})$	$(0, \frac{1}{2})$
$(\frac{2}{3}, \frac{2}{3})$	$(\frac{1}{6}, \frac{2}{3})$
$(\frac{1}{3}, \frac{5}{6})$	$(\frac{5}{6}, \frac{5}{6})$

On constate ainsi que $B \cap B^\varepsilon$ contient les points d'ordre 2 de B, ainsi que les images des pointes $\frac{1}{3}$ et $\frac{2}{3}$; ces dernières engendrent le groupe C, qui est cyclique d'ordre 3, cf. (4.2.4).

Par conséquent, $B \cap B^\varepsilon$ est le produit de C par le groupe des points de 2-torsion de B, resp. de C par le groupe des points de 2-torsion de B^ε. On peut schématiser comme suit la position des images des pointes de $X_0(3^4)$ dans A:



4.2.6. Considérons le quotient B/C. La courbe obtenue possède un point d'ordre 3 rationnel sur K, à savoir l'image de la pointe $\frac{1}{9}$, cf. (4.2.4). Elle vérifie donc les conditions du lemme du § 3 de [3]. D'autre part, sa série L coïncide avec celle de B. Les raisonnements de [3] montrent que cette courbe coïncide avec B ou B^ε. Ce ne peut pas être B, car $\mathrm{End}(B) = Z$. C'est donc B^ε.

Une vérification de ce résultat consiste à remarquer que le réseau définissant B/C est, d'après 4.2.4, le réseau $[1, (1 + \tau_B)/3]$. Or ce dernier est homothétique au réseau $[1, \tau_{B^\varepsilon}]$, cf. (4.2.2.2).

On peut aussi vérifier que le quotient de la courbe:

$$y^2 - 3xy + \omega y = x^3 , \qquad \omega = e^{2\pi i/3} ,$$

https://doi.org/10.1017/S0027763000018547 Published online by Cambridge University Press

par le sous-groupe engendré par le point $(0, 0)$ est la courbe

$$y^2 - 3xy + \omega^2 y = x^3 \ ;$$

(on utilise les formules de [9]; on obtient ainsi l'equation:

$$y'^2 - 3x'y' + \omega y' = x'^3 + 15\omega x' + (7 + 34\omega)$$

d'où, posant:

$$x = -\frac{1}{3}x' - 1 \ , \qquad y = -\frac{1}{3i\sqrt{3}}y' - \frac{1}{3}(\omega + 2)x' + \frac{4\omega - 10}{9}$$

l'équation

$$y^2 - 3xy + \omega^2 y = x^3) \ .$$

On a ainsi montré l'assertion (d) de la Prop. 4.2.1.

4.2.7. Considérons le morphisme:

$$j: B \times B^s \to A \ .$$

Ce morphisme est surjectif. Son noyau est l'ensemble des couples $(b, -b)$, $b \in B \cap B^s$, donc l'image de i.

Considérons le morphisme composé:

$$B \times B^s \xrightarrow{\mathrm{pr}_2} B^s \longrightarrow B^s/B \cap B^s \ ;$$

il est clair que son noyau contient l'image de i, d'où, par passage au quotient, un morphisme:

$$A \to B^s/B \cap B^s \ .$$

Ce dernier est visiblement surjectif. D'autre part, son noyau est l'image par j de $B \times (B \cap B^s)$, qui n'est autre que B.

L'unicité (à isomorphisme près) du quotient A/B entraîne, tenant compte de l'assertion (a), l'existence d'un isomorphisme:

$$\iota: B \cong B^s/B \cap B^s \ ,$$

ce qui fournit une nouvelle preuve de (d); d'autre part, le morphisme $A \to B^s/B \cap B^s$ s'identifie à λ, pour un choix convenable de ι.

https://doi.org/10.1017/S0027763000018547 Published online by Cambridge University Press

Table 1

Expression de $(\tilde{c}\colon \tilde{1})$, $1 \leq c < 81$, $(c, 3) = 1$, en fonction de $(\tilde{c}\colon \tilde{1})$, $c \in \mathscr{B}$, où

$$\mathscr{B} = \{2, 4, 7, 13, 25, 31, 34, 58\}\ .$$

On note simplement (c) l'élément $(\tilde{c}\colon \tilde{1})$; cf. 3.1

$(1) = 0$	$(43) = -(31)$
(2)	$(44) = 0$
(4)	$(46) = 0$
$(5) = (4)$	$(47) = -(31)$
(7)	$(49) = -(34)$
$(8) = 0$	$(50) = -(34)$
$(10) = 0$	$(52) = -(13)$
$(11) = (7)$	$(53) = 0$
(13)	$(55) = 0$
$(14) = (13)$	$(56) = -(13)$
$(16) = -(4)$	(58)
$(17) = 0$	$(59) = (58)$
$(19) = 0$	$(61) = -(2) + (4) - (7) + (13) - (25) + (31) - (34) + (58)$
$(20) = -(4)$	$(62) = 0$
$(22) = -(7)$	$(64) = 0$
$(23) = -(7)$	$(65) = -(2) + (4) - (7) + (13) - (25) + (31) - (34) + (58)$
(25)	$(67) = -(25)$
$(26) = 0$	$(68) = -(25)$
$(28) = 0$	$(70) = -(58)$
$(29) = (25)$	$(71) = 0$
(31)	$(73) = 0$
$(32) = (31)$	$(74) = -(58)$
(34)	$(76) = (2) - (4) + (7) - (13) + (25) - (31) + (34) - (58)$
$(35) = 0$	$(77) = (2) - (4) + (7) - (13) + (25) - (31) + (34) - (58)$
$(37) = 0$	$(79) = (2)$
$(38) = (34)$	$(80) = 0$
$(40) = -(2)$	
$(41) = -(2)$	

https://doi.org/10.1017/S0027763000018547 Published online by Cambridge University Press

Table 1′

Expression de $(\tilde{c}:\tilde{3})$, $1 \leq c < 27$, $(c, 3) = 1$, en fonction de $(\tilde{1}:\tilde{3})$, $(\tilde{2}:\tilde{3})$ et $(\tilde{c}:\tilde{1})$, $c \in \mathscr{B}$; cf. Table 1 et 3.1.

$$(\tilde{4}:\tilde{3}) = (\tilde{1}:\tilde{3}) + (2) - (4) + (7) - (13) + (25) - (31) + (34) - (58)$$
$$(\tilde{5}:\tilde{3}) = (\tilde{2}:\tilde{3}) + (34)$$
$$(\tilde{7}:\tilde{3}) = (\tilde{1}:\tilde{3}) + (2) - (4) + (7) - (13) + (25) - (31) + (34)$$
$$(\tilde{8}:\tilde{3}) = (\tilde{2}:\tilde{3}) - (31) + (34)$$
$$(\widetilde{10}:\tilde{3}) = (\tilde{1}:\tilde{3}) + (2) - (4) + (7) - (13) - (31) + (34)$$
$$(\widetilde{11}:\tilde{3}) = (\tilde{2}:\tilde{3}) + (25) - (31) + (34)$$
$$(\widetilde{13}:\tilde{3}) = (\tilde{1}:\tilde{3}) + (2) - (4) - (13) - (31) + (34)$$
$$(\widetilde{14}:\tilde{3}) = (\tilde{2}:\tilde{3}) - (2) + (4) - (7) + (13) + (58)$$
$$(\widetilde{16}:\tilde{3}) = (\tilde{1}:\tilde{3}) + (2) - (13) - (31) + (34)$$
$$(\widetilde{17}:\tilde{3}) = (\tilde{2}:\tilde{3}) - (2) + (4) - (7) + (13)$$
$$(\widetilde{19}:\tilde{3}) = (\tilde{1}:\tilde{3}) + (2) - (31) + (34)$$
$$(\widetilde{20}:\tilde{3}) = (\tilde{2}:\tilde{3}) - (2) + (4) - (7)$$
$$(\widetilde{22}:\tilde{3}) = (\tilde{1}:\tilde{3}) + (2) - (31)$$
$$(\widetilde{23}:\tilde{3}) = (\tilde{2}:\tilde{3}) - (2) + (4)$$
$$(\widetilde{25}:\tilde{3}) = (\tilde{1}:\tilde{3}) + (2)$$
$$(\widetilde{26}:\tilde{3}) = (\tilde{2}:\tilde{3}) - (2)$$

Table 2

Conjugaison complexe (cf. 3.1).

On note $(\tilde{c}:\tilde{1}) = (c)$.

$$(\overline{2}) = (2)$$
$$(\overline{4}) = (2) - (4) + (7) - (13) + (25) - (31) + (34) - (58)$$
$$(\overline{7}) = -(58)$$
$$(\overline{13}) = -(25)$$
$$(\overline{25}) = -(13)$$
$$(\overline{31}) = -(34)$$
$$(\overline{34}) = -(31)$$
$$(\overline{58}) = -(7)$$

https://doi.org/10.1017/S0027763000018547 Published online by Cambridge University Press

Table 3

On désigne par (c) le vecteur $\xi((\tilde{c}:\tilde{1}))$; cf. 3.1.

$$\gamma_1^+ = (2) + (7) - (13) + (25) - (31) + (34) - (58)$$
$$\gamma_2^+ = (7) - (58)$$
$$\gamma_3^+ = (13) - (25)$$
$$\gamma_4^+ = (31) - (34)$$
$$\gamma_1^- = -(2) + 2(4) - (7) + (13) - (25) + (31) - (34) + (58)$$
$$\gamma_2^- = (7) + (58)$$
$$\gamma_3^- = (13) + (25)$$
$$\gamma_4^- = (31) + (34)$$

$$(2) = \gamma_1^+ - \gamma_2^+ + \gamma_3^+ + \gamma_4^+$$
$$(4) = \tfrac{1}{2}\gamma_1^+ + \tfrac{1}{2}\gamma_1^-$$
$$(7) = \tfrac{1}{2}\gamma_2^+ + \tfrac{1}{2}\gamma_2^-$$
$$(13) = \tfrac{1}{2}\gamma_3^+ + \tfrac{1}{2}\gamma_3^-$$
$$(25) = -\tfrac{1}{2}\gamma_3^+ + \tfrac{1}{2}\gamma_3^-$$
$$(31) = \tfrac{1}{2}\gamma_4^+ + \tfrac{1}{2}\gamma_4^-$$
$$(34) = -\tfrac{1}{2}\gamma_4^+ + \tfrac{1}{2}\gamma_4^-$$
$$(58) = -\tfrac{1}{2}\gamma_2^+ + \tfrac{1}{2}\gamma_2^-$$

Table 4

On note:

$$\omega_1^+ = \gamma_{1,1}^+ ; \qquad \omega_1^- = \gamma_{1,1}^- ;$$
$$\omega_2^+ = -3\omega_1^+ ; \qquad \omega_2^- = \omega_1^- ;$$
$$\omega_3^+ = \gamma_{2,3}^+ ; \qquad \omega_3^- = \gamma_{2,3}^- ;$$
$$\omega_4^+ = \gamma_{2,4}^+ ; \qquad \omega_4^- = \gamma_{2,4}^- .$$

cf. 3.1.4.

https://doi.org/10.1017/S0027763000018547 Published online by Cambridge University Press

$\gamma^+_{1,1} = \omega^+_1$	$\gamma^+_{1,2} = 0$	$\gamma^+_{1,3} = 2\omega^+_3$	$\gamma^+_{1,4} = 2\omega^+_4$
$\gamma^+_{2,1} = -\omega^+_1$	$\gamma^+_{2,2} = \omega^+_2$	$\gamma^+_{2,3} = \omega^+_3$	$\gamma^+_{2,4} = \omega^+_4$
$\gamma^+_{3,1} = -2\omega^+_1$	$\gamma^+_{3,2} = \omega^+_2$	$\gamma^+_{3,3} = (\sqrt{3} - 1)\omega^+_3$	$\gamma^+_{3,4} = -(1 + \sqrt{3})\omega^+_4$
$\gamma^+_{4,1} = \omega^+_1$	$\gamma^+_{4,2} = 0$	$\gamma^+_{4,3} = -\omega^+_3$	$\gamma^+_{4,4} = -\omega^+_4$
$\gamma^-_{1,1} = \omega^-_1$	$\gamma^-_{1,2} = 2\omega^-_2$	$\gamma^-_{1,3} = 0$	$\gamma^-_{1,4} = 0$
$\gamma^-_{2,1} = \omega^-_1$	$\gamma^-_{2,2} = \omega^-_2$	$\gamma^-_{2,3} = \omega^-_3$	$\gamma^-_{2,4} = \omega^-_4$
$\gamma^-_{3,1} = 0$	$\gamma^-_{3,2} = -\omega^-_2$	$\gamma^-_{3,3} = (\sqrt{3} + 1)\omega^-_3$	$\gamma^-_{3,4} = (1 - \sqrt{3})\omega^-_4$
$\gamma^-_{4,1} = \omega^-_1$	$\gamma^-_{4,2} = 0$	$\gamma^-_{4,3} = -\omega^-_3$	$\gamma^-_{4,4} = -\omega^-_4$

Table 5

On pose:

$$\{0, \pm z\} = \tfrac{1}{2}[X(z, k)\cdot\omega^+_k \pm Y(z, k)\cdot\omega^-_k] , \qquad 1 \leq k \leq 3 ;$$

cf. 3.2.

pointe	∞	$\frac{1}{3}$	$\frac{1}{9}$	$\frac{2}{9}$	$\frac{4}{9}$	$\frac{1}{27}$
$X(z, 1)$	$\frac{2}{3}$	1	$-\frac{1}{3}$	$\frac{2}{3}$	$\frac{5}{3}$	$\frac{2}{3}$
$Y(z, 1)$	0	$\frac{1}{3}$	$\frac{1}{3}$	$\frac{2}{3}$	$\frac{1}{3}$	0
$X(z, 2)$	0	$-\frac{1}{3}$	$\frac{4}{9}$	$\frac{1}{9}$	$-\frac{2}{9}$	$-\frac{1}{3}$
$Y(z, 2)$	0	$\frac{1}{3}$	0	1	0	$-\frac{1}{3}$
$X(z, 3)$	$\frac{2\sqrt{3}}{3}$	$\sqrt{3}$	$\frac{\sqrt{3}}{3}$	$\frac{1+\sqrt{3}}{\sqrt{3}}$	$\frac{4-\sqrt{3}}{\sqrt{3}}$	$-\frac{\sqrt{3}}{3}$
$Y(z, 3)$	0	$\frac{\sqrt{3}}{3}$	$\frac{2+\sqrt{3}}{3}$	$\frac{1+\sqrt{3}}{3}$	$-\frac{1}{3}$	$\frac{\sqrt{3}}{3}$

Table 6

Soit $z \in \boldsymbol{C}^4$; z s'écrit de façon unique:

$$z = \tfrac{1}{2}\sum_{k=1}^{4}(x_k\gamma^+_k + y_k\gamma^-_k) ,$$

où $x_k, y_k \in \boldsymbol{R}$, $1 \leq k \leq 4$.

https://doi.org/10.1017/S0027763000018547 Published online by Cambridge University Press

On note:

$$\pi_i(z) = \tfrac{1}{2}(a_i\omega_i^+ + b_i\omega_i^-) , \qquad i = 1, 2 ,$$

et

$$\pi_A(z) = (M_3(a, b, c, d), M_4(a, b, -c, -d))$$

(cf. 3.3).

$a_1 = x_1 - x_2 - 2x_3 + x_4;$	$3x_1 = a_1 + a + 3c;$
$b_1 = y_1 + y_2 + y_4;$	$3x_2 = 3a_2 - 3c;$
$a_2 = x_2 + x_3;$	$3x_3 = 3c;$
$b_2 = 2y_1 + y_2 - y_3;$	$3x_4 = 2a_1 + 3a_2 - a$
$a = 2x_1 + x_2 - x_3 - x_4;$	$3y_1 = -b_1 + 2b_2 - b + 3d;$
$b = y_2 + y_3 - y_4;$	$3y_2 = 2b_1 - b_2 + 2b - 3d;$
$c = x_3;$	$3y_3 = 3d;$
$d = y_3 .$	$3y_4 = 2b_1 - b_2 - b.$

Table 7

Soit $z \in \mathfrak{H}^*$ une pointe de $X_0(3^4)$.
On note:

$$\{0, z\}_{f_j} = \tfrac{1}{2}(a_j\omega_j^+ + b_j\omega_j^-) , \qquad j = 1, 2 .$$
$$(\{0, z\}_{f_3}, \{0, z\}_{f_4}) = M(a, b, c, d) ,$$

cf. (3.3.3).

pointe	a_1	b_1	a_2	b_2	a	b	c	d
∞	$\frac{2}{3}$	0	0	0	0	0	$\frac{2}{3}$	0
$\frac{1}{3}$	1	$\frac{1}{3}$	$-\frac{1}{3}$	$\frac{1}{3}$	0	0	1	$\frac{1}{3}$
$\frac{1}{9}$	$-\frac{1}{3}$	$\frac{1}{3}$	$\frac{4}{9}$	0	0	$\frac{2}{3}$	$\frac{1}{3}$	$\frac{1}{3}$
$\frac{2}{9}$	$\frac{2}{3}$	$\frac{2}{3}$	$\frac{1}{9}$	1	1	$\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{3}$
$\frac{4}{9}$	$\frac{5}{3}$	$\frac{1}{3}$	$-\frac{2}{9}$	0	-1	$-\frac{1}{3}$	$\frac{4}{3}$	0
$\frac{1}{27}$	$\frac{2}{3}$	0	$-\frac{1}{3}$	$-\frac{1}{3}$	0	0	$-\frac{1}{3}$	$\frac{1}{3}$

https://doi.org/10.1017/S0027763000018547 Published online by Cambridge University Press

Bibliographie

[1] T. Hadano, On the conductor of an elliptic curve with a rational point of order 2. Nagoya Math. J., **53** (1974), 199–210.

[2] T. Honda and I. Miyawaki, Zeta-functions of elliptic curves of 2-power conductor. J. Math. Soc. Japan, **26**, n° 2 (1974), 362–373.

[3] M. Koike, On certain Abelian varieties obtained from newforms of weight 2 on $\Gamma_0(3^4)$ and $\Gamma_0(3^5)$, Nagoya Math. J., **62** (1976), 29–39.

[4] G. Ligozat, Courbes modulaires de genre 1. Bull. Soc. Math. France, Suppl., Mém. N° **43**, 80 p (1975).

[5] ——, Courbes modulaires de niveau 11, in Modular Functions of one variable V. Lecture Notes in Math. **601**, 149–237, Berlin-Heidelberg-New York, Springer 1977.

[6] G. Shimura, Introduction to the arithmetic theory of automorphic functions. Publ. Math. Soc. Japan, N° **11**, Iwanami Shoten and Princeton University Press (1971).

[7] ——, On elliptic curves with complex multiplication as factors of the jacobians of modular function fields. Nagoya Math. J., **43** (1971), 199–208.

[8] ——, On the factors of the jacobian variety of a modular function field. J. Math. Soc. Japan, **25**, N° 3 (1973), 523–544.

[9] J. Vélu, Isogénies entre courbes elliptiques. C. R. Acad. Sci. Paris, **273** (1971), 238–241.

Université de Paris-Sud