Sur la courbe modulaire $\mathrm{X}_{\mathrm{ndép}}(11)$

Emmanuel Halberstadt

TABLE DES MATIÈRES

La courbe modulaire $\mathrm{X}_{\mathrm{ndép}}(11)$ classifie les courbes elliptiques E telles que l'image de la représentation de Galois dans le groupe des points de 11-torsion de E soit contenue dans le normalisateur d'un sous-groupe de Cartan non déployé. On sait que $\mathrm{X}_{\mathrm{ndép}}(11)$ est de genre 1. Nous donnons ici une paramétrisation de cette courbe par une certaine courbe elliptique sur $\mathbb{Q}$, de conducteur 121. Nous en déduisons des exemples explicites de couples de courbes elliptiques sur $\mathbb{Q}$ non isogènes sur $\mathbb{Q}$ mais donnant des représentations de Galois modulo 11 symplectiquement isomorphes.

The modular curve $\mathrm{X}_{\mathrm{ndép}}(11)$ (or $\mathrm{X}_{\mathrm{nonsplit}}(11)$) classifies the elliptic curves E such that Galois acts on the group of 11-torsion points of E through the normaliser of a non-split Cartan subgroup. It is known that this curve has genus 1. We give here a parametrisation of this curve by a certain elliptic curve over $\mathbb{Q}$ with conductor 121. As an application, we give explicit examples of couples of elliptic curves over $\mathbb{Q}$ nonisogenous over $\mathbb{Q}$ but giving symplectically isomorphic modulo 11 Galois representations.

1. INTRODUCTION

Soit p un nombre premier ; nous supposerons $p \geq 5$ pour simplifier. Soit $X(p)$ la courbe modulaire classifiant les courbes elliptiques munies d'une base de leurs points de p-torsion [Deligne et Rapoport 1973]. Le groupe $\mathrm{GL}_2(\mathbb{F}_p)$ opère naturellement sur $X(p)$ [Deligne et Rapoport 1973; Shimura 1971]. Soit G un sous-groupe de $\mathrm{GL}_2(\mathbb{F}_p)$ tel que le morphisme $\det : G \to \mathbb{F}_p^*$ soit surjectif. Le quotient $X_G = G\backslash X(p)$ est alors une courbe (projective et lisse) absolument irréductible sur $\mathbb{Q}$. Les points de X_G sur un corps K (de caractéristique 0 par exemple) correspondent aux courbes elliptiques E sur K telles que, $\bar{K}$ étant une clôture algébrique de K, l'opération du groupe $\mathrm{Gal}(\bar{K}/K)$ sur les points de p-torsion de E se factorise par G. Pour tous ces

1058-6458/1998 $0.50 per page
Experimental Mathematics **7**:2, page 163

faits la référence est encore [Deligne et Rapoport 1973]. Lorsque G est le normalisateur d'un sous-groupe de Cartan déployé de $\mathrm{GL}_2(\mathbb{F}_p)$ [Serre 1972], on note $X_{\text{dép}}(p)$ la courbe modulaire X_G. On définit $X_{\text{ndép}}(p)$ de manière analogue, lorsque G est le normalisateur d'un sous-groupe de Cartan non déployé de $\mathrm{GL}_2(\mathbb{F}_p)$. Les courbes $X_{\text{dép}}(p)$ et $X_{\text{ndép}}(p)$ sont bien définies, à $\mathbb{Q}$-isomorphisme près, parce que les sous-groupes de Cartan déployés d'un côté et non déployés de l'autre côté forment dans $\mathrm{GL}_2(\mathbb{F}_p)$ des classes de conjugaison.

Il y a au moins deux raisons de s'intéresser aux courbes $X_{\text{dép}}(p)$ et $X_{\text{ndép}}(p)$. La première est que ces courbes peuvent posséder des points rationnels sur $\mathbb{Q}$ autres que les pointes, à savoir les points CM, c'est-à-dire provenant de courbes elliptiques sur $\mathbb{Q}$ ayant des multiplications complexes (sur $\bar{\mathbb{Q}}$, fermeture algébrique de $\mathbb{Q}$ dans $\mathbb{C}$). Plus précisément, soit E une courbe elliptique sur $\mathbb{Q}$ ayant des multiplications complexes par un ordre d'un corps quadratique imaginaire K. Si p est ramifié (resp. décomposé, resp. inerte) dans K, il correspond à E un point de la courbe modulaire $X_0(p)$ (resp. $X_{\text{dép}}(p)$, resp. $X_{\text{ndép}}(p)$) rationnel sur $\mathbb{Q}$. Voir dans [Serre 1989, appendices A.5 et A.6] des exemples d'utilisation de ces points CM. La seconde raison est la suivante : soient E une courbe elliptique sur $\mathbb{Q}$, $E_p(\bar{\mathbb{Q}})$ le groupe des points de p-torsion de E et

$$\rho : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{Aut}\left(E_p(\bar{\mathbb{Q}})\right) \simeq \mathrm{GL}_2(\mathbb{F}_p)$$

la représentation associée. Supposons ρ non surjective. Son image est alors contenue dans le normalisateur d'un sous-groupe de Cartan (déployé ou non) de $\mathrm{GL}_2(\mathbb{F}_p)$, sauf peut-être si $p \leq 19$ ou $p = 37$, 43, 67 ou 163 [Mazur 1978, théorème 3]. Si donc on savait que, pour tout nombre premier p assez grand, les courbes $X_{\text{dép}}(p)$ et $X_{\text{ndép}}(p)$ ne possèdent pas de points rationnels sur $\mathbb{Q}$, hormis les points CM et certaines des pointes, on en déduirait ceci : pour tout nombre premier p assez grand et toute courbe elliptique E sur $\mathbb{Q}$ sans multiplication complexe, la représentation de $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ dans les points de p-torsion de E est surjective. Tout ceci est pour l'instant conjectural.

Plus modestement, le but essentiel de cet article est le suivant : la courbe $X_{\text{ndép}}(11)$ est de genre 1. Ligozat [1977] a démontré que cette courbe est isomorphe (sur $\mathbb{Q}$) à la courbe elliptique $\mathscr{E}$ définie par l'équation de Weierstrass suivante :

$$y^2 + y = x^3 - x^2 - 7x + 10. \tag{1–1}$$

$\mathscr{E}$ est la courbe 121B1 des tables de [Cremona 1992] et le groupe de Mordell–Weil $\mathscr{E}(\mathbb{Q})$ est de rang 1. Nous explicitons en 3.3 un isomorphisme Θ de $X_{\text{ndép}}(11)$ sur $\mathscr{E}$, retrouvant ainsi le résultat de [Ligozat 1977]. Ceci nous permet surtout, dans la proposition du paragraphe 2.2, d'expliciter la fonction rationnelle J sur $\mathscr{E}$ induite, via Θ, par la fonction modulaire j sur $X_{\text{ndép}}(11)$. Nous en déduisons en 2.4 des exemples de couples (E, E') de courbes elliptiques sur $\mathbb{Q}$, non isogènes sur $\mathbb{Q}$, mais telles que les représentations de $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ dans les points de 11-torsion de E et E' respectivement soient symplectiquement isomorphes. A ce sujet, voir la question posée par Mazur [1978, p. 133], ainsi que l'introduction de [Halberstadt et Kraus 1996].

Lorsque p est égal à 5 ou 7, les courbes $X_{\text{dép}}(p)$ et $X_{\text{ndép}}(p)$ sont de genre 0, elles sont donc isomorphes à $\mathbb{P}^1(\mathbb{Q})$, ce qu'on peut voir en considérant leurs points CM. Comme pour $X_{\text{ndép}}(11)$, on obtient dans chaque cas une fonction rationnelle J sur $\mathbb{P}^1(\mathbb{Q})$. Les références à ce sujet étant éparses, nous explicitons en 2.3 (mais sans démonstration ultérieure, car les calculs sont beaucoup plus simples que pour $X_{\text{ndép}}(11)$) les quatre fractions rationnelles correspondantes.

D'après Momose [1984, théorème 0.1 et les commentaires qui le suivent], la courbe modulaire $X_{\text{dép}}(37)$ a au plus un point rationnel sur $\mathbb{Q}$, hormis la pointe ordinaire ∞ et les points CM. Dans le même travail (proposition 5.1), Momose précise ce résultat ainsi : l'hypothétique point rationnel supplémentaire existe si et seulement un certain polynôme à coefficients rationnels possède une racine rationnelle. Dans l'appendice, nous démontrons, en utilisant des calculs de [Mazur et Swinnerton-Dyer 1974] concernant la courbe modulaire $X_0(37)$, que ce n'est pas le cas. Ainsi la pointe ordinaire ∞ et les points CM sont les seuls points de $X_{\text{dép}}(37)$ rationnels sur $\mathbb{Q}$.

De nombreuses conversations avec A. Kraus sont à l'origine de cet article. C'est lui qui m'a signalé que la proposition ci-dessous (dont l'énoncé lui est dû) permettrait d'obtenir explicitement des exemples de couples (E, E') de courbes elliptiques sur $\mathbb{Q}$ non isogènes sur $\mathbb{Q}$ mais telles que les représentations de $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ dans les points de 11-torsion de E et E' respectivement soient symplectiquement isomorphes, ceci à condition d'avoir explicité la fonction J mentionnée ci-dessus.

Par ailleurs, précisons que tous les calculs (numériques ou formels) nécessaires ont été effectués à l'aide du logiciel Pari.

2. ENONCÉ DES RÉSULTATS

2.1. Un résultat préliminaire

Dans la suite, on suppose toujours $p \geq 5$; on notera C un sous-groupe de Cartan de $\text{GL}_2(\mathbb{F}_p)$ «standard» et G son normalisateur dans $\text{GL}_2(\mathbb{F}_p)$: dans le cas déployé, C est formé des matrices du type

$$\begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix}.$$

Dans le cas non déployé, α désignant un élément de $\mathbb{F}_p$ non carré fixé (on prendra toujours $\alpha = -1$ si $p \equiv 3$ modulo 4), C est formé des matrices du type

$$\begin{pmatrix} x & \alpha y \\ y & x \end{pmatrix},$$

(x, y) décrivant $\mathbb{F}_p^2 \setminus \{0\}$.

Proposition. *Soit E une courbe elliptique sur $\mathbb{Q}$, sans multiplication complexe sur $\bar{\mathbb{Q}}$. On suppose que l'image de* $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ *dans* $\text{Aut}(E_p(\bar{\mathbb{Q}}))$ *est contenue dans le normalisateur $\widetilde{N}$ d'un sous-groupe de Cartan $\widetilde{C}$ (déployé ou non) sans être contenue dans $\widetilde{C}$. Considérons le caractère quadratique correspondant*

$$\varepsilon : \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \widetilde{N}/\widetilde{C} \simeq \{-1, 1\},$$

et soit E' la courbe elliptique déduite de E par torsion par ε. Alors :

a) *E et E' ne sont pas isogènes sur $\mathbb{Q}$, mais les* $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$*-modules $E_p(\bar{\mathbb{Q}})$ et $E'_p(\bar{\mathbb{Q}})$ sont isomorphes. Il en est de même des* $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$*-modules $E_{2p}(\bar{\mathbb{Q}})$ et $E'_{2p}(\bar{\mathbb{Q}})$.*

b) *Si $\widetilde{C}$ est déployé et p est congru à 1 modulo 4, ou si $\widetilde{C}$ est non déployé et p est congru à 3 modulo 4, les* $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$*-modules $E_p(\bar{\mathbb{Q}})$ et $E'_p(\bar{\mathbb{Q}})$ sont symplectiquement isomorphes. Il en est de même des* $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$*-modules $E_{2p}(\bar{\mathbb{Q}})$ et $E'_{2p}(\bar{\mathbb{Q}})$.*

Admettons un instant la conjecture (peut-être optimiste) selon laquelle, pour tout nombre premier p assez grand, il n'existe pas de couple (E, E') de courbes elliptiques sur $\mathbb{Q}$, non isogènes sur $\mathbb{Q}$, mais telles que les représentations de $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ dans les points de p-torsion de E et E' respectivement soient isomorphes. La proposition précédente montre alors (cf. l'introduction) que, pour tout nombre premier p assez grand et toute courbe elliptique E sur $\mathbb{Q}$ sans multiplication complexe, la représentation de $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ dans les points de p-torsion de E est surjective. On répond ainsi à une question posée dans [Serre 1972, 4.3], ce qui montre la portée de la conjecture ci-dessus.

2.2. La fonction rationnelle J sur $X_{\text{ndép}}(11)$

Notons ici simplement X la courbe modulaire $X_{\text{ndép}}(11)$. Comme on l'a dit dans l'introduction, X est isomorphe à la courbe elliptique $\mathscr{E}$ définie par l'équation (1–1). Nous expliciterons en 3.3 un isomorphisme Θ de X sur $\mathscr{E}$. Considérons alors la composée

$$J : \mathscr{E}(\mathbb{C}) \xrightarrow{\Theta^{-1}} X(\mathbb{C}) \xrightarrow{\nu} X(1) \xrightarrow{j} \mathbb{P}^1(\mathbb{C}),$$

où ν est le morphisme canonique et, par exemple, $X(\mathbb{C})$ est l'ensemble des points (fermés) de X à valeurs dans $\mathbb{C}$, muni de sa structure naturelle de surface de Riemann. J provient, par extension des scalaires de $\mathbb{Q}$ à $\mathbb{C}$, d'une fonction rationnelle sur $\mathscr{E}$, notée encore J. L'expression de J en fonction de x, y (fonctions coordonnées de Weierstrass sur $\mathscr{E}$) est la suivante :

Proposition. *Avec les notations précédentes, on a* :

$$J = \frac{(f_1 f_2 f_3 f_4)^3}{f_5^2 f_6^{11}}, \tag{2–1}$$

les fonctions f_i étant définies ainsi :

$$\begin{aligned} f_1 &= x^2 + 3x - 6, \\ f_2 &= 11(x^2 - 5)y + (2x^4 + 23x^3 - 72x^2 - 28x + 127), \\ f_3 &= 6y + 11x - 19, \\ f_4 &= 22(x-2)y + (5x^3 + 17x^2 - 112x + 120), \\ f_5 &= 11y + (2x^2 + 17x - 34), \\ f_6 &= (x-4)y - (5x-9). \end{aligned} \tag{2–2}$$

2.3. Les cas $p = 5$ et $p = 7$

Lorsque p vaut 5 ou 7, les courbes $X_{\text{dép}}(p)$ et $X_{\text{ndép}}(p)$ sont isomorphes à $\mathbb{P}^1(\mathbb{Q})$, on l'a vu. Soit X l'une de ces courbes. Une fois explicité un isomorphisme Θ de X sur $\mathbb{P}^1(\mathbb{Q})$, on obtient comme précédemment une fonction rationnelle J sur $\mathbb{P}^1(\mathbb{Q})$, à partir de la composée

$$J : \mathbb{P}^1(\mathbb{C}) \xrightarrow{\Theta^{-1}} X(\mathbb{C}) \xrightarrow{\nu} X(1) \xrightarrow{j} \mathbb{P}^1(\mathbb{C}).$$

Nous nous contentons de donner ci-dessous les différentes fonctions J obtenues.

2.4. Exemples numériques

Lorsque $p = 11$ ou $p = 7$, nous donnons ici quelques exemples de couples (E, E') de courbes elliptiques sur $\mathbb{Q}$ non isogènes sur $\mathbb{Q}$ mais telles que les représentations de $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ dans les points de p-torsion de E et E' respectivement soient isomorphes. On obtient ces exemples en appliquant la proposition du 2.1 et en utilisant les fonctions J explicitées en 2.2 et 2.3.

Cas de $X_{\text{ndép}}(11)$. Le groupe de Mordell–Weil $\mathscr{E}(\mathbb{Q})$ est de rang 1, plus précisément il est engendré par le point $A = (4, 5)$. Cela étant, soient $j \in \mathbb{Q}$ et E une courbe elliptique sur $\mathbb{Q}$, d'invariant modulaire j. Pour que l'image de $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ dans $\mathrm{Aut}(E_{11}(\bar{\mathbb{Q}}))$ soit contenue dans le normalisateur d'un sous-groupe de Cartan non déployé (ici, à cause de la conjugaison complexe, ladite image ne peut pas être contenue dans le sous-groupe de Cartan lui-même), il faut et il suffit que l'on ait

$$j = J(nA)$$

pour un certain entier n (cf. 3.1). Les premières valeurs de n correspondent à des points CM de $X(\mathbb{Q})$ et ne nous intéressent donc pas directement. Voici,

courbe	$J(x)$
$X_{\text{dép}}(5)$	$\dfrac{\left((x+5)(x^2+15)(x^2-10x+5)\right)^3}{\left(2(x^2-5)\right)^5}$
$X_{\text{ndép}}(5)$	$\dfrac{(x+1)\left(5(2x+1)(2x^2-3x+3)\right)^3}{\left((x^2+x-1)\right)^5}$
$X_{\text{dép}}(7)$	$\dfrac{(1-x)\left((x-2)(x^2+3x+4)(x^2+3x-3)(x^4+x^3-x^2+2x+4)\right)^3}{\left((x^3+x^2-2x-1)\right)^7}$
$X_{\text{ndép}}(7)$	$\dfrac{\left((3x+1)(x^2+10x+4)(x^2+3x+4)(4x^2+5x+2)\right)^3}{\left((x^3+x^2-2x-1)\right)^7}$

TABLEAU 1. Fractions rationnelles J pour $X_{\text{dép}}(5)$, $X_{\text{ndép}}(5)$, $X_{\text{dép}}(7)$ et $X_{\text{ndép}}(7)$.

pour chacune de ces valeurs de n, les coordonnées de nA ainsi que la valeur de $j = J(nA)$ correspondante.

n	nA	$J(nA)$
-2	$(2,-1)$	$-2^{15}.3.5^3$
-1	$(4,-6)$	$(2.3.11)^3$
0	0	$2^4.3^3.5^3$
1	$(4,5)$	$-(2^5.3.5.11)^3$
2	$(2,0)$	1728
3	$(\frac{5}{4},\frac{7}{8})$	0
4	$(-2,3)$	$-(2^6.3.5.23.29)^3$

Passons à des entiers n ne correspondant pas à des points CM.

n = −3. On a $-3A = \left(\frac{5}{4}, -\frac{15}{8}\right)$ et

$$J(-3A) = \frac{2^8.3^3.5^6.11^3.53^3}{23^{11}} = j\,.$$

Parmi les courbes elliptiques sur $\mathbb{Q}$ d'invariant j, la courbe E donnée par l'équation de Weierstrass minimale ci-dessous a un conducteur et un discriminant minimaux :

$$y^2 = x^3 + 2\,929\,575\,x - 16\,817\,998\,099\,.$$

Les invariants standard N, Δ, c_4 de E (voir par exemple [Silverman 1986, p. 303]) sont :

$$\begin{aligned} N &= 2^2.3^2.23.67^2,\\ \Delta &= -2^4.3^3.23^{11}.67^3,\\ c_4 &= -2^4.3^2.5^2.11.53.67\,. \end{aligned}$$

Le corps quadratique K associé à ρ_{11}, c'est-à-dire tel que, avec les notations du paragraphe 2.1, le noyau de ε soit égal à $\mathrm{Gal}(\bar{\mathbb{Q}}/K)$, est $\mathbb{Q}\left(\sqrt{-67}\right)$. En effet, d'une part K est non ramifié en dehors de $\{2,3,23,67\}$ (critère de Néron–Ogg–Shafarevitch), d'autre part, pour tout nombre premier $l \neq 11$ inerte dans K, le coefficient $a_l(E)$ de la fonction L de Hasse–Weil de E est multiple de 11. Il suffit alors de tester quelques a_l pour déterminer K. La tordue E' de E par ε a pour équation :

$$y^2 = x^3 + 13\,150\,862\,175\,x + 5\,058\,231\,562\,249\,537\,.$$

En vertu de la proposition du 2.1, le couple (E, E') a la propriété suivante : E et E' ne sont pas isogènes sur $\mathbb{Q}$ mais les représentations de $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ dans les points de 11-torsion (resp. de 22-torsion) de E et E' sont symplectiquement isomorphes.

n = −4. On a $-4A = (-2,-4)$ et

$$J(-4A) = -\frac{2^9.3^3.5^3.13.71^3.181^3}{43^{11}} = j\,.$$

Parmi les courbes elliptiques sur $\mathbb{Q}$ d'invariant j, la courbe E donnée par l'équation de Weierstrass minimale ci-dessous a un conducteur et un discriminant minimaux :

$$y^2 = x^3 - 6\,682\,520\,x + 39\,157\,150\,032\,.$$

Les invariants standard N, Δ, c_4 de E sont :

$$\begin{aligned} N &= 2^5.13^2.43 = 232\,544\,,\\ \Delta &= -2^{12}.13^2.43^{11},\\ c_4 &= 2^7.3.5.13.71.181\,. \end{aligned}$$

Le corps quadratique K associé à ρ_{11} est ici $\mathbb{Q}(i)$, on le vérifie comme précédemment. La tordue E' de E par ε a pour équation :

$$y^2 = x^3 - 6\,682\,520\,x - 39\,157\,150\,032\,.$$

Le couple (E, E') a les mêmes propriétés que dans l'exemple précédent. Les valeurs suivantes de n paraissent donner des courbes ayant des conducteurs plus gros.

Cas de $X_{\text{dép}}(7)$. Considérons la fraction rationnelle J donnée dans le tableau 1 pour $X_{\text{dép}}(7)$. Pour $x = -\frac{3}{2}$, on obtient le couple (E, E') de courbes elliptiques signalé à la fin de [Halberstadt et Kraus 1996]. Donnons un autre exemple : pour $x = -5$, on obtient la courbe E d'équation

$$y^2 = x^3 - 68\,943\,x - 5\,181\,946\,.$$

Les invariants standard N, Δ, c_4, j de E sont :

$$N = 2^2 . 3^3 . 7^2 . 13 = 68\,796\,,$$
$$\Delta = 2^8 . 3^5 . 7^4 . 13^7,$$
$$c_4 = 2^4 . 3^2 . 7^3 . 67\,,$$
$$j = 2^4 . 3 . 7^5 . 67^3 / 13^7\,.$$

Le corps quadratique associé (via la proposition du paragraphe 2.1) est $\mathbb{Q}(\sqrt{21})$, et la tordue E' de E par ε a pour équation

$$y^2 = x^3 - 30\,403\,863\,x - 47\,990\,001\,906\,.$$

Les courbes E et E' ne sont pas isogènes sur $\mathbb{Q}$ mais les représentations de $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ dans les points de 7-torsion (resp. de 14-torsion) de E et E' sont isomorphes.

Cas de $X_{\text{ndép}}(7)$. Considérons ici la fraction rationnelle J donnée dans le tableau 1 pour $X_{\text{ndép}}(7)$. Pour $x = -\frac{3}{2}$, on obtient la courbe E d'équation

$$y^2 = x^3 - x^2 - 6\,288\,x + 194\,020\,,$$

dont les invariants standard sont

$$N = 2^5 . 7^2 . 11^2 = 189\,728\,,$$
$$\Delta = 2^9 . 7^4 . 11^3\,,$$
$$c_4 = 2^4 . 5 . 7^3 . 11\,,$$
$$j = 2^3 . 5^3 . 7^5\,.$$

Le corps quadratique associé est $\mathbb{Q}(\sqrt{-77})$, et la tordue E' de E par ε a pour équation

$$y^2 = x^3 - x^2 - 37\,283\,528\,x - 87\,607\,177\,832\,.$$

Les représentations de $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ dans les points de 7-torsion (resp. de 14-torsion) de E et E' sont ici symplectiquement isomorphes.

3. PARAMÉTRISATION DE $X_{\text{ndép}}(11)$

Dans ce paragraphe, G désigne le normalisateur du sous-groupe de Cartan non déployé standard de $\mathrm{GL}_2(\mathbb{F}_{11})$. La courbe modulaire $X_{\text{ndép}}(11)$ associée est notée simplement X. Par ailleurs on pose :

$$\zeta = e^{2i\pi/11} \quad \text{et} \quad \omega = \tfrac{1}{2}(\zeta + \zeta^{-1}).$$

3.1. Rappels sur $X_{\text{ndép}}(11)$

La référence principale est ici [Ligozat 1977]. Le demi-plan de Poincaré est noté $\mathfrak{H}$, et l'on pose $\mathfrak{H}^* = \mathfrak{H} \cup \mathbb{P}^1(\mathbb{Q})$. Pour tout entier $N > 0$, $\Gamma(N)$ est le noyau du morphisme de réduction modulo N :

$$\mathrm{SL}_2(\mathbb{Z}) \longrightarrow \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}),$$

et $X(N)$ est la surface de Riemann compacte

$$\Gamma(N)\backslash\mathfrak{H}^*.$$

Soit $\Pi = \Gamma(11)\backslash\mathbb{P}^1(\mathbb{Q})$ l'ensemble des pointes de $X(11)$. Il s'identifie naturellement au quotient de $\mathbb{F}_{11}^2\backslash\{0\}$ par $\{\pm 1\}$: si a, b sont deux entiers non tous deux multiples de 11 et u, v leurs classes modulo 11, la classe de $\binom{u}{v} \in \mathbb{F}_{11}^2\backslash\{0\}$ correspond à l'orbite sous $\Gamma(11)$ de $[a, b] \in \mathbb{P}^1(\mathbb{Q})$.

Cela étant, soient H l'intersection de G avec $\mathrm{SL}_2(\mathbb{F}_{11})$, Γ son image réciproque par le morphisme de réduction modulo 11 dans $\mathrm{SL}_2(\mathbb{Z})$. On peut identifier $X(\mathbb{C})$ à la surface de Riemann compacte $\Gamma\backslash\mathfrak{H}^*$, qui est de genre 1. Alors $\Gamma\backslash\mathfrak{H}$ correspond à $Y(\mathbb{C})$, ensemble des points à valeurs complexes d'un certain ouvert Y de X ; son complémentaire $\Gamma\backslash P$, ensemble des pointes de $X(\mathbb{C})$, peut être identifié à $H\backslash\Pi$; il est de cardinal cinq. Plus précisément, soit $i \in \mathbb{F}_{11}^*$. Les $\binom{u}{v}$ pour lesquels $u^2 + v^2 = i$ représentent tous une même pointe $P_i \in H\backslash\Pi$; en outre $P_i = P_{-i}$ pour tout i. L'action de $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ sur ces pointes est la suivante : soit $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ tel que $\sigma(\zeta) = \zeta^h$, pour $h \in \mathbb{F}_{11}^*$, et soit $i \in \mathbb{F}_{11}^*$. Alors

$$\sigma \cdot P_i = P_{ih^{-1}}\,. \tag{3–1}$$

En particulier ces 5 pointes sont conjuguées sur $\mathbb{Q}$ et ont pour corps de rationalité le corps cyclotomique réel $L = \mathbb{Q}(\omega)$.

L'inclusion de Γ dans $\mathrm{SL}_2(\mathbb{Z})$ induit un morphisme canonique

$$\nu : X(\mathbb{C}) \longrightarrow X(1) = \mathrm{SL}_2(\mathbb{Z})\backslash\mathfrak{H}^*\,,$$

qui est de degré 55. La composée

$$j \circ \nu : X(\mathbb{C}) \longrightarrow \mathbb{P}^1(\mathbb{C})$$

provient, par passage aux points complexes, d'un morphisme de X dans $\mathbb{P}^1(\mathbb{Q})$. La fonction $j \circ \nu$ a 5 pôles, à savoir les pointes P_i, d'ordre 11 chacun. Ses zéros sont les points de la fibre $\nu^{-1}(\mathrm{cl}(\rho))$, où $\rho = e^{2i\pi/3}$. Comme $X(\mathbb{C})$ possède un seul point elliptique d'ordre 3 [Ligozat 1977, p. 192], $j \circ \nu$ a un zéro simple, rationnel sur $\mathbb{Q}$, et 18 zéros triples.

L'interprétation modulaire de Y est la suivante. Soient par exemple K un sous-corps de $\mathbb{C}$ et $\bar{K}$ sa fermeture algébrique dans $\mathbb{C}$. Considérons les couples $\left(E, \binom{P}{Q}\right)$, où E est une courbe elliptique sur K, (P, Q) est une base de $E_{11}(\bar{K})$ sur $\mathbb{F}_{11}$ dans laquelle l'action de $\mathrm{Gal}(\bar{K}/K)$ sur $E_{11}(\bar{K})$ se factorise par G. Deux tels couples $\left(E, \binom{P}{Q}\right)$ et $\left(E', \binom{P'}{Q'}\right)$ seront identifiés s'il existe un $\bar{K}-$isomorphisme de E sur E' appliquant $G \cdot \binom{P}{Q}$ sur $G \cdot \binom{P'}{Q'}$. L'ensemble quotient obtenu sera noté $\mathscr{M}(K)$. On a alors une bijection, fonctorielle en K :

$$\beta_K : Y(K) \xrightarrow{\approx} \mathscr{M}(K)\,.$$

Supposons par exemple que $K = \mathbb{Q}$ et soit μ un élément de $\mathscr{M}(\mathbb{Q})$. On peut le représenter par un couple $\left(E, \binom{P}{Q}\right)$ comme ci-dessus, avec en outre $\langle P, Q\rangle = \zeta$, en notant $\langle\,,\rangle$ l'accouplement de Weil. Soit (ω_1, ω_2) une base du réseau des périodes de E telle que ω_2 soit réelle et que

$$\tau = \frac{\omega_1}{\omega_2}$$

appartienne à $\mathfrak{H}$. Alors la classe de τ dans $Y(\mathbb{C})$ appartient en fait à $Y(\mathbb{Q})$, et son image par $\beta_{\mathbb{Q}}$ est μ.

Soit enfin E une courbe elliptique sur $\mathbb{Q}$ ayant des multiplications complexes par un ordre de k, corps quadratique imaginaire. Si 11 est inerte dans k, on sait que l'image du groupe $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ dans $\mathrm{Aut}(E_{11}(\bar{\mathbb{Q}}))$ est contenue dans le normalisateur d'un sous-groupe de Cartan non déployé. On obtient ainsi les points CM de $X(\mathbb{Q})$.

3.2. Formes de Klein

Les références sont ici [Kubert et Lang 1975; Lang 1987; Ligozat 1977]. Soit $l = (r, s)$ un élément de $\mathbb{Z}^2 \setminus 11\mathbb{Z}^2$. On lui associe une fonction $\mathfrak{k}_l$ sur $\mathfrak{H}$ comme suit : si $\tau \in \mathfrak{H}$,

$$\mathfrak{k}_l(\tau) = \exp\left(-\frac{\eta(z;\Lambda_\tau)z}{2}\right)\sigma(z;\Lambda_\tau)\,,$$

où $z = (r\tau + s)/11$, Λ_τ est le réseau $\mathbb{Z}\tau + \mathbb{Z}$, et σ et η sont les fonctions de Weierstrass associées à Λ_τ. La fonction $\mathfrak{k}_l$ admet en ∞ un développement en produit eulérien [Kubert et Lang 1975, p. 178], qui montre qu'elle est holomorphe et ne s'annule pas sur $\mathfrak{H}$. C'est une fonction modulaire de poids -1 pour $\Gamma(2.\,11^2)$, appelée forme de Klein.

Soit maintenant Π le quotient de $\mathbb{F}_{11}^2 \setminus \{0\}$ par $\{\pm 1\}$, les vecteurs de $\mathbb{F}_{11}^2$ étant ici des vecteurs lignes. Le groupe $\mathrm{GL}_2(\mathbb{F}_{11})$ opère naturellement à droite sur Π. Pour tout $i \in \mathbb{F}_{11}^*$ soit ϖ_i l'ensemble des classes dans Π des vecteurs (u, v) tels que $u^2 + v^2 = \pm i$. Par transposition, on voit que les ϖ_i, pour $i \in \mathbb{F}_{11}^*$, sont les 5 orbites (de cardinal 12 chacune) de Π sous H (on a $\varpi_i = \varpi_{-i}$ pour tout i). Choisissons pour tout i un système de représentants R_i de ϖ_i dans $\mathbb{Z}^2 \setminus 11\mathbb{Z}^2$. On définit une fonction F_i sur $\mathfrak{H}$ par la formule suivante :

$$F_i = K_i \prod_{l \in R_i} \mathfrak{k}_l\,,$$

K_i étant une constante choisie de sorte que le développement de F_i à l'infini soit unitaire (le coefficient de la plus petite puissance de $q = e^{2\pi i\tau}$ soit 1). La fonction F_i ne dépend pas, en fait, du choix de R_i, c'est une fonction modulaire de poids -12 pour Γ, holomorphe et ne s'annulant pas sur $Y(\mathbb{C})$.

3.3. L'isomorphisme Θ

Considérons sur $X(\mathbb{C})$ les deux fonctions méromorphes suivantes :

$$\psi = \frac{F_3}{F_2} \qquad \text{et} \qquad \varphi = (2\pi)^{-12}(\Delta \circ \nu)\,F_3\,,$$

où Δ est la fonction discriminant. Les calculs de [Ligozat 1977, pp. 209–210] montrent que l'on a

$$\begin{aligned}\mathrm{div}(\varphi) &= (P_2) + (P_3) - 2\,(P_1)\\ \mathrm{div}(\psi) &= (P_2) + 2\,(P_4) - 3\,(P_1)\,.\end{aligned}$$

De plus les développements à l'infini de φ et ψ sont unitaires, vu la définition des F_i et la formule de Jacobi pour Δ. Le théorème de Riemann–Roch montre alors que ces deux fonctions vérifient une égalité de la forme

$$f(\varphi,\psi)=0, \tag{3–2}$$

où, les a_i étant *a priori* des nombres complexes, on a posé

$$f(x',y') \\ =(y'^2+a_1x'y'+a_3y')-(x'^3+a_2x'^2+a_4x'+a_6)\,.$$

En fait les coefficients des développements de φ et ψ aux différentes pointes appartiennent à L, donc les a_i appartiennent à L. En comparant les premiers termes des développements à l'infini des deux membres de (3–2), on obtient les valeurs suivantes :

$$\begin{aligned}
a_1 &= -2\omega\\
a_2 &= 2\omega^4+2\omega^3-6\omega^2-6\omega\\
a_3 &= -\omega^4-2\omega^3+2\omega^2+6\omega+2\\
a_4 &= -2\omega^4-4\omega^3+5\omega^2+11\omega+3\\
a_6 &= 0\,.
\end{aligned}$$

Ainsi φ et ψ donnent un isomorphisme, défini sur L, de $X_{(L)}$ (courbe obtenue par extension des scalaires de $\mathbb{Q}$ à L) sur la cubique plane non-singulière $\mathscr{E}'$ donnée par l'équation de Weierstrass $f(x',y')=0$. Un petit calcul formel permet ensuite d'obtenir un isomorphisme $(x',y')\longmapsto(x,y)$ de $\mathscr{E}'$ sur $\mathscr{E}_{(L)}$, par les formules habituelles

$$\begin{aligned}
x &= u^2x'+r\,,\\
y &= u^3y'+u^2sx'+t\,,
\end{aligned}$$

les valeurs de u,r,s,t étant les suivantes :

$$\begin{aligned}
u &= \omega^4-5\omega^2+4\\
r &= 2\omega^4+2\omega^3-7\omega^2-5\omega+5\\
s &= \omega^4+\omega^3-3\omega^2-\omega+1\\
t &= 2\omega^4+\omega^3-10\omega^2-3\omega+11\,.
\end{aligned}$$

On a donc un isomorphisme θ de $X(\mathbb{C})$ sur $\mathscr{E}(\mathbb{C})$, défini sur L, et donné par les formules

$$\theta(P_1)=O$$

et

$$\theta(\xi)=\bigl(u^2\varphi(\xi)+r,u^3\psi(\xi)+u^2s\varphi(\xi)+t\bigr)$$

si $\xi\neq P_1$.

Posons enfin $P=(r,t)\in\mathscr{E}(L)$. Le calcul montre que le point P est d'ordre 11, il engendre un sous-groupe d'ordre 11 de $\mathscr{E}_{11}(\bar{\mathbb{Q}})$ stable par $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. Ceci peut se voir aussi en calculant les diviseurs des fonctions analogues à φ et ψ, à savoir les F_{3h}/F_{2h} et $(2\pi)^{-12}(\Delta\circ\nu)\,F_{3h}$, où h décrit $\mathbb{F}_{11}^*$. Ce calcul donne les images des pointes par θ :

$$\begin{aligned}
\theta(P_1) &= O\,,\\
\theta(P_2) &= P\,,\\
\theta(P_3) &= -P\,,\\
\theta(P_4) &= 5P\,,\\
\theta(P_5) &= -3P\,.
\end{aligned}$$

Pour tout point M de $\mathscr{E}(\mathbb{C})$, notons τ_M la translation de vecteur M. Posons

$$\Theta=\tau_{4P}\circ\theta\,.$$

On a un nouvel isomorphisme Θ de $X(\mathbb{C})$ sur $\mathscr{E}(\mathbb{C})$, défini sur L, les images des pointes étant données par la formule

$$\Theta(P_i)=(2i)^2P,\quad \text{pour } i\in\mathbb{F}_{11}^*\,.$$

Si $\sigma\in\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ est tel que $\sigma(\zeta)=\zeta^h$, avec $h\in\mathbb{F}_{11}^*$, on voit que $\sigma\cdot P=h^{-2}P$. Grâce à la formule (3–1), on en déduit que Θ est défini sur $\mathbb{Q}$: c'est l'isomorphisme de X sur $\mathscr{E}$ cherché.

3.4. Détermination de la fonction J

On va déterminer le diviseur de J. On connaît déjà les pôles (d'ordre 11) de J : ce sont les points hP, où $h\in\mathbb{F}_{11}^*$ est un carré. Un petit calcul donne :

$$\Bigl(\sum_{k=1}^{5}(k^2P)\Bigr)-5\,(O)=\mathrm{div}(f_6)\,,$$

où f_6 est défini en (2–2). D'autre part on a vu que les zéros de J sont les images par Θ des points de la fibre

$$\Phi = \nu^{-1}(\mathrm{cl}(\rho)) = (j \circ \nu)^{-1}(0)\,.$$

Il faut donc expliciter Φ et son image par Θ. Indiquons brièvement le principe de ce calcul. Partons de la courbe elliptique E donnée par l'équation de Weierstrass

$$y^2 = x^3 + 1\,.$$

Le réseau des périodes de E a une base (ω_1, ω_2) telle que ω_2 soit réelle et que $\tau_0 = \omega_1/\omega_2$ soit égal à $\gamma_0{\cdot}\rho$, où $\gamma_0 = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 2 \end{smallmatrix}\right)$.

Détermination de Φ. Considérons un système de représentants W des doubles classes de

$$\Gamma\backslash \mathrm{SL}_2(\mathbb{Z})/\mathrm{SL}_2(\mathbb{Z})_{\tau_0}.$$

L'application $g \longmapsto \mathrm{cl}(g{\cdot}\tau_0)$ est une bijection de W sur Φ. Les 19 matrices $g_1, g_2, \dots, g_{19}$ ci-dessous forment un tel système W :

$$\left(\begin{smallmatrix} 1 & -5 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 3 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & -2 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 2 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 2 & 1 \\ 11 & 6 \end{smallmatrix}\right),$$
$$\left(\begin{smallmatrix} -8 & 5 \\ 11 & -7 \end{smallmatrix}\right), \left(\begin{smallmatrix} -8 & -3 \\ 11 & 4 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} -9 & 4 \\ 11 & -5 \end{smallmatrix}\right),$$
$$\left(\begin{smallmatrix} -20 & 9 \\ 11 & -5 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 5 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & -4 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 3 & -4 \\ -11 & 15 \end{smallmatrix}\right), \left(\begin{smallmatrix} -7 & 2 \\ -11 & 3 \end{smallmatrix}\right),$$
$$\left(\begin{smallmatrix} -9 & 5 \\ -11 & 6 \end{smallmatrix}\right), \left(\begin{smallmatrix} -9 & -5 \\ 11 & 6 \end{smallmatrix}\right), \left(\begin{smallmatrix} 9 & 4 \\ 11 & 5 \end{smallmatrix}\right), \left(\begin{smallmatrix} 2 & -3 \\ -11 & -5 \end{smallmatrix}\right).$$

Pour tout k, posons $\xi_k = \mathrm{cl}(g_k{\cdot}\tau_0)$. A l'aide de l'interprétation modulaire de Y, on voit que les orbites de Φ sous $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ sont $\{\xi_1\}$, $\{\xi_2, \xi_3\}$, $\{\xi_4, \xi_5, \xi_6, \xi_7\}$, $\{\xi_8, \xi_9, \xi_{10}, \xi_{11}\}$, $\{\xi_{12}, \xi_{13}, \xi_{14}, \xi_{15}\}$ et $\{\xi_{16}, \xi_{17}, \xi_{18}, \xi_{19}\}$. Ainsi, par exemple, ξ_1 appartient à $Y(\mathbb{Q})$, et donc $\Theta(\xi_1)$ appartient à $\mathscr{E}(\mathbb{Q})$.

Calcul approché des valeurs de Θ sur Φ. Les coordonnées des points $\Theta(\xi_k)$ peuvent être calculées de façon approchée grâce au développement en produit de la fonction σ. A l'aide de la formule classique

$$\mathfrak{p}(z) - \mathfrak{p}(a) = -\frac{\sigma(z+a)\,\sigma(z-a)}{\sigma^2(z)\,\sigma^2(a)}$$

(voir [Lang 1987, théorème 2, p. 243] par exemple) reliant les fonctions $\mathfrak{p}$ et σ de Weierstrass, on peut accélérer ce calcul en exprimant $\varphi(\xi_k)$ et $\psi(\xi_k)$ en fonction des coordonnées des points de 11-torsion de E. On obtient ainsi par exemple, avec une bonne approximation, les égalités

$$\begin{cases} \Theta(\xi_1) = \left(\dfrac{5}{4}, \dfrac{7}{8}\right), \\[2ex] \Theta(\xi_2) = \left(\dfrac{14 + i\sqrt{11}}{9}, \dfrac{17 - 11i\sqrt{11}}{54}\right), \\[2ex] \Theta(\xi_3) = \left(\dfrac{14 - i\sqrt{11}}{9}, \dfrac{17 + 11i\sqrt{11}}{54}\right). \end{cases} \tag{3–3}$$

Calcul exact des valeurs de Θ sur Φ. L'idée essentielle est la suivante : on montre que la fonction ψ est un élément entier sur $\mathbb{Z}[j]$ (la fonction φ aussi, à cause de la relation (3–2)) ; cela se voit sur les coefficients des développements en produit de ψ aux différentes pointes [Cassou-Noguès et Taylor 1987, prop. 3.2, page 94]. En fait ψ est une *unité modulaire* [Kubert et Lang 1975]. Soit alors Ω une orbite de Φ sous $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. Considérons le polynôme

$$Q = \prod_{\xi \in \Omega} \left(T - x(\Theta(\xi))\right).$$

A priori, Q est à coefficients rationnels, mais ce qui précède permet de trouver facilement un entier $d > 0$ tel que dQ soit à coefficients dans $\mathbb{Z}$. Une fois d connu, il est clair que des valeurs approchées assez précises des $\Theta(\xi)$, pour $\xi \in \Omega$, suffisent pour avoir les valeurs exactes correspondantes. On voit ainsi par exemple que les formules (3–3) sont exactes.

Conclusion. La restriction de Θ à Φ étant déterminée, on a déjà le diviseur de J. Un calcul un peu long mais trivial permet d'en déduire J elle-même, à une constante multiplicative près. Comme ci-dessus, on voit que

$$\Theta(\mathrm{cl}(i)) = 2\,A = (2, 0)\,,$$

ce qui montre que $J(2\,A) = 1728$; dès lors la constante en question est connue, et la formule (2–1) est établie.

4. DÉMONSTRATION DE LA PROPOSITION DU § 2.1

On considère donc, comme dans l'énoncé de la proposition en question, les courbes elliptiques E, E' et le caractère quadratique ε. D'abord E et E' ne sont pas isogènes sur $\mathbb{Q}$. En effet elles sont isomorphes sur $\bar{\mathbb{Q}}$, mais pas sur $\mathbb{Q}$. Une isogénie de E sur E' définie sur $\mathbb{Q}$ fournirait donc un endomorphisme de E défini sur $\bar{\mathbb{Q}}$, mais pas sur $\mathbb{Q}$, et E serait à multiplication complexe, contrairement à l'hypothèse.

Considérons les représentations de Galois

$$\rho_p : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{Aut}(E_p(\bar{\mathbb{Q}}))\,,$$
$$\rho'_p : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{Aut}(E'_p(\bar{\mathbb{Q}}))\,.$$

Par hypothèse, il existe une base de $E_p(\bar{\mathbb{Q}})$ sur $\mathbb{F}_p$ dans laquelle, pour tout élément σ de $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, $\rho_p(\sigma)$ soit représenté par une matrice A_σ appartenant à G. Dans une base de $E'_p(\bar{\mathbb{Q}})$ sur $\mathbb{F}_p$ convenable, chaque $\rho'_p(\sigma)$ est alors représenté par la matrice

$$A'_\sigma = \varepsilon(\sigma)\, A_\sigma\,.$$

Pour voir que ρ_p et ρ'_p sont isomorphes, il suffit, puisque C est abélien, de trouver une matrice $M \in C$ vérifiant la condition suivante :

$$MAM^{-1} = -A \quad \text{pour toute matrice } A \in G \setminus C\,.$$

C étant d'indice 2 dans G, il suffit que l'égalité ci-dessus soit vraie pour *une* matrice $A \in G\setminus C$. Dans le cas déployé, on peut prendre

$$M = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix};$$

dans le cas non déployé, on peut prendre

$$M = \begin{pmatrix} 0 & \alpha \\ 1 & 0 \end{pmatrix}, \quad A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Par ailleurs les $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-modules $E_2(\bar{\mathbb{Q}})$ et $E'_2(\bar{\mathbb{Q}})$ étant évidemment isomorphes, il en est de même des $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-modules $E_{2p}(\bar{\mathbb{Q}})$ et $E'_{2p}(\bar{\mathbb{Q}})$, ce qui établit le a).

Pour le b), notons $\langle\,,\rangle$ les accouplements de Weil. On déduit de ce qui précède un isomorphisme de $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-modules

$$\theta : E_p(\bar{\mathbb{Q}}) \xrightarrow{\approx} E'_p(\bar{\mathbb{Q}})$$

tel que, pour tous points $P, Q \in E_p(\bar{\mathbb{Q}})$, on ait

$$\langle \theta(P), \theta(Q) \rangle = \langle P, Q \rangle^{\det(M^{-1})}\,.$$

Vu les hypothèses faites en b), $\det(M)$ est un carré. Ainsi, en remplaçant M par λM, où $\lambda \in \mathbb{F}_p^*$ est bien choisi, θ devient un isomorphisme symplectique. La dernière assertion de b) est laissée au lecteur.

APPENDICE: INEXISTENCE DE POINTS RATIONNELS SUPPLÉMENTAIRES DE $X_{\text{dép}}(37)$

Comme on l'a dit dans l'introduction, la courbe modulaire $X_{\text{dép}}(37)$ a au plus un point rationnel sur $\mathbb{Q}$, hormis la pointe ordinaire ∞ et les points CM, et ce point hypothétique existe si et seulement si un certain polynôme Q, à coefficients rationnels, possède une racine rationnelle. Rappelons brièvement d'où vient le polynôme Q. La courbe modulaire $X_0(37)$ est de genre 2 ; l'équation ci-dessous en définit un modèle (singulier) $\mathscr{C}$:

$$y^2 = -x^6 - 9\,x^4 - 11\,x^2 + 37$$

[Mazur et Swinnerton-Dyer 1974, p. 22]. Dans ce modèle, la fonction j induit, de la même manière qu'au § 2.2, une fonction rationnelle J sur $\mathscr{C}$. Momose [1984, p. 130] montre que J a la forme

$$J = \frac{P(x) + yQ(x)}{(x-1)(x+1)^{37}}\,,$$

où P et Q sont deux polynômes à coefficients rationnels. Le polynôme Q est celui qui nous intéresse. En fait, on trouve dans [Mazur et Swinnerton-Dyer 1974, p. 23 à 26], toutes les étapes nécessaires pour évaluer J. En suivant ces étapes, un calcul formel permet d'expliciter P et Q. Commençons par Q. La décomposition de Q en produit de facteurs irréductibles sur $\mathbb{Q}$ est :

$$Q = 2^3\,(x^2-5)(9x^2-13)(3x^4+6x^2-25)\,Q_1 Q_2\,,$$

où les polynômes Q_1 et Q_2 sont donnés par

$$\begin{aligned} Q_1 = 77x^{14} - 148x^{13} - 619x^{12} + 5\,920x^{11} - \\ - 1\,5591x^{10} + 12\,876x^9 + 34\,625x^8 - \\ - 183\,520x^7 + 11\,735x^6 - 189\,884x^5 - \\ - 1\,038\,865x^4 + 774\,336x^3 + 2\,028\,163x^2 - \\ - 419\,580x - 1\,035\,909\,, \end{aligned}$$

$$\begin{aligned} Q_2 = 99x^{12} + 666x^{11} + 3\,975x^{10} + 15\,984x^9 + \\ + 48\,694x^8 + 126\,540x^7 + 247\,318x^6 + \\ + 359\,640x^5 + 387\,463x^4 + 112\,554x^3 - \\ - 446\,493x^2 - 615\,384x - 242\,080\,. \end{aligned}$$

Le polynôme Q n'a donc effectivement pas de racine rationnelle. Le polynôme P, lui, est irréductible et de degré 38 :

$$P = 2^3 \sum_{k=0}^{38} a_k x^k\,,$$

les coefficients a_k étant donnés par le tableau ci-après.

k	a_k	k	a_k
38	35 937	18	147 227 101 014 214
37	58 806	17	388 119 677 172 568
36	681 318	16	471 139 427 087 208
35	−461 538	15	86 501 040 355 720
34	4 485 177	14	−890 036 230 898 388
33	20 619 360	13	−3 043 349 732 012 896
32	45 163 088	12	−4 315 965 766 567 824
31	802 394 136	11	−608 251 175 518 816
30	2 016 349 484	10	5 963 719 239 019 164
29	7 274 245 584	9	12 187 169 363 559 560
28	25 317 502 784	8	13 665 520 831 967 704
27	24 219 438 096	7	−5 006 586 672 831 416
26	28 205 163 196	6	−31 305 822 456 742 271
25	−161 659 095 528	5	−19 562 454 283 353 586
24	−1 338 373 543 928	4	17 853 777 511 718 158
23	−3 415 577 348 840	3	22 848 066 502 482 966
22	−8 606 145 613 626	2	904 218 550 326 185
21	−16 231 037 035 828	1	−7 305 168 148 435 800
20	−5 144 969 449 764	0	−2 478 761 487 567 000
19	35 729 385 767 452		

Il résulte de [Mazur et Swinnerton-Dyer 1974, § 5] ou de [Momose 1984, p. 131] que la courbe modulaire $X_0(37)$ a quatre points rationnels sur $\mathbb{Q}$; dans le modèle $\mathscr{C}$, ce sont les points

$$(1,4), \quad (-1,4), \quad (1,-4), \quad (-1,-4).$$

Les deux premiers points correspondent aux deux pointes de $X_0(37)$. Les points $(1,-4)$ et $(-1,-4)$ correspondent aux deux courbes elliptiques sur $\mathbb{Q}$ possédant un sous-groupe d'ordre 37 stable sous $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ (à $\bar{\mathbb{Q}}$-isomorphisme près). On trouve aisément deux courbes elliptiques sur $\mathbb{Q}$, d'invariants modulaires respectifs

$$J(1,-4) = -7.\,11^3\,,$$
$$J(-1,-4) = -7.\,137^3.\,2\,083^3\,,$$

et ayant des conducteurs et discriminants minimaux, à savoir les courbes

$$E_1 :\ y^2 + xy + y = x^3 + x^2 - 8x + 6\,,$$
$$E_2 :\ y^2 + xy + y = x^3 + x^2 - 208083x - 36\,621\,194\,.$$

L'invariant modulaire de E_1 est $j = -7.\,11^3$, celui de E_2 est $-7.\,137^3.\,2\,083^3$. Ces deux courbes ont même conducteur $5^2.\,7^2 = 1225$ et même discriminant minimal $-5^3.\,7^2$. Elles possèdent chacune un sous-groupe d'ordre 37 stable sous $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, et elles sont liées par une isogénie de degré 37, définie sur $\mathbb{Q}$. La courbe E_1 est donnée en [Mazur et Swinnerton-Dyer 1974, p. 30] ; on peut si l'on veut en déduire E_2 par l'algorithme de [Vélu 1971].

Signalons pour terminer une petite erreur qui s'est glissée dans l'une des formules de [Mazur et Swinnerton-Dyer 1974, page 22] : la formule exacte donnant Z en fonction de X et f_4 est, avec leurs notations,

$$Z = \tfrac{1}{2}\bigl(X(f_4^2-1)^2 + f_4^4 + 6f_4^2 - 15\bigr)\,.$$

BIBLIOGRAPHIE

[Cassou-Noguès et Taylor 1987] P. Cassou-Noguès et M. J. Taylor, *Elliptic functions and rings of integers*, Progress in Mathematics **66**, Birkhäuser, Boston, Mass., 1987.

[Cremona 1992] J. E. Cremona, *Algorithms for modular elliptic curves*, Cambridge University Press, Cambridge, 1992.

[Deligne et Rapoport 1973] P. Deligne et M. Rapoport, "Les schémas de modules de courbes elliptiques", pp. 143–316 dans *Modular functions of one variable* (Antwerp, 1972), vol. II, édité par P. Deligne et W. Kuyk, Lecture Notes in Math. **349**, Springer, Berlin, 1973.

[Halberstadt et Kraus 1996] E. Halberstadt et A. Kraus, "Sur la comparaison galoisienne des points de torsion des courbes elliptiques", *C. R. Acad. Sci. Paris Sér. I Math.* **322**:4 (1996), 313–316.

[Kubert et Lang 1975] D. Kubert et S. Lang, "Units in the modular function field, II: A full set of units", *Math. Ann.* **218**:2 (1975), 175–189.

[Lang 1987] S. Lang, *Elliptic functions*, 2e éd., Graduate Texts in Mathematics **112**, Springer, New York, 1987.

[Ligozat 1977] G. Ligozat, "Courbes modulaires de niveau 11", pp. 149–237 dans *Modular functions of one variable, V* (Bonn, 1976), édité par J.-P. Serre et D. B. Zagier, Lecture Notes in Math. **601**, Springer, Berlin, 1977.

[Mazur 1978] B. Mazur, "Rational isogenies of prime degree", *Invent. Math.* **44**:2 (1978), 129–162.

[Mazur et Swinnerton-Dyer 1974] B. Mazur et P. Swinnerton-Dyer, "Arithmetic of Weil curves", *Invent. Math.* **25** (1974), 1–61.

[Momose 1984] F. Momose, "Rational points on the modular curves $X_{\text{split}}(p)$", *Compositio Math.* **52**:1 (1984), 115–137.

[Serre 1972] J.-P. Serre, "Propriétés galoisiennes des points d'ordre fini des courbes elliptiques", *Invent. Math.* **15**:4 (1972), 259–331.

[Serre 1989] J.-P. Serre, *Lectures on the Mordell-Weil theorem*, Aspects of Mathematics **E15**, Friedr. Vieweg & Sohn, Braunschweig, 1989.

[Shimura 1971] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Publications of the Mathematical Society of Japan **11**, Princeton University Press et Iwanami Shoten, Tokyo, 1971.

[Silverman 1986] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics **106**, Springer, New York, 1986.

[Vélu 1971] J. Vélu, "Isogénies entre courbes elliptiques", *C. R. Acad. Sci. Paris Sér. A-B* **273** (1971), A238–A241.

Emmanuel Halberstadt, Université Paris VI, Laboratoire de Mathématiques fondamentales, UFR 921
4, place Jussieu 75252 Paris Cedex 05, France (halberst@math.jussieu.fr)

Received July 3, 1997; accepted August 11, 1997