Journal de Théorie des Nombres
de Bordeaux **15** (2003), 231–247

Rang de courbes elliptiques avec groupe de torsion non trivial

par Odile LECACHEUX

Résumé. On construit des courbes elliptiques sur $\mathbb{Q}(T)$ de rang au moins 3, avec un sous-groupe de torsion non trivial. Par spécialisation, des courbes elliptiques de rang 5 et 6 sur $\mathbb{Q}$ sont obtenues.

Abstract. We construct elliptic curves on $\mathbb{Q}(T)$ with rank greater than 3 and non zero torsion group. After specialization, we obtain elliptic curves of rank 5 and 6 on $\mathbb{Q}$.

1. Introduction

Soit E une courbe elliptique sur $\mathbb{Q}$. Le théorème de Mordell-Weil donne la structure du groupe des points rationnels de E :

$$E(\mathbb{Q}) \simeq E(\mathbb{Q})_{tor} \times \mathbb{Z}^r$$

où r est appelé le rang sur $\mathbb{Q}$ de E et $E(\mathbb{Q})_{tor}$ désigne le sous-groupe de torsion de $E(\mathbb{Q})$. Lorsque E décrit l'ensemble des courbes elliptiques sur $\mathbb{Q}$, un théorème de Mazur montre qu'il n'y a qu'un nombre fini de groupes de torsion possibles; par contre on ignore si r est borné. Les exemples connus de courbes avec rang élevé correspondent à des courbes avec un groupe de torsion d'ordre 1 ou 2 (Voir [5] et [6], par exemple, et [2] pour une liste actualisée). Dans un précédent article [3], nous avons construit des courbes elliptiques sur $\mathbb{Q}(T)$ de rang ≥ 3 avec $E(\mathbb{Q}(T))_{tor} \simeq \mathbb{Z}/5\mathbb{Z}$. Nous poursuivons notre étude et montrons que les méthodes utilisées s'appliquent pour d'autres sous-groupes de torsion correspondants à toutes les surfaces modulaires rationnelles avec quatre fibres singulières de type I_c. Nous montrons les résultats suivants :

Théorème 1. *Il existe une courbe elliptique sur $\mathbb{Q}(T)$, d'invariant modulaire non constant, possédant trois points indépendants définis sur $\mathbb{Q}(T)$ et un sous-groupe de torsion, défini sur $\mathbb{Q}(T)$, isomorphe à l'un des groupes : $\mathbb{Z}/6\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/3\mathbb{Z} \times \mu_3$.*

Manuscrit reçu le 29 novembre 2001.

Nous étudions aussi le cas où $E(\mathbb{Q})_{tor} \simeq \mathbb{Z}/4\mathbb{Z} \subset C_8$, le groupe C_8 étant stable par le groupe de Galois de $\overline{\mathbb{Q}}/\mathbb{Q}$.

2. Méthode

2.1. Surfaces modulaires rationnelles.

On considère l'ensemble

$$\mathfrak{G} = \{\Gamma(3), \Gamma_1(4) \cap \Gamma(2), \Gamma_1(5), \Gamma_1(6), \Gamma_0(8) \cap \Gamma_1(4), \Gamma_0(9) \cap \Gamma_1(3)\}$$

où les sous-groupes $\Gamma(n), \Gamma_1(n)$ et $\Gamma_0(n)$ de $SL_2(\mathbb{Z})$ sont définis par

$$\Gamma(n) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}),\, b \equiv c \equiv 0 \text{ et } a \equiv 1 \ \ (n) \right\}$$

$$\Gamma_0(n) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}),\ c \equiv 0\,(n) \right\}$$

$$\Gamma_1(n) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}),\ c \equiv 0,\ a \equiv 1 \ \ (n) \right\}.$$

Si $\Gamma \in \mathfrak{G}$, le produit semi-direct de Γ par $\mathbb{Z}^2$ opère librement sur $\mathfrak{H} \times \mathbb{C}$ par

$$(\gamma, p, q)(\tau, z) = \left(\gamma.\tau, (c\tau + d)^{-1}(z + p\tau + q)\right).$$

On note E_Γ la surface quotient et $Y_\Gamma = \Gamma \backslash \mathfrak{H}$ la courbe quotient. La fibration elliptique

$$E_\Gamma^0 \longrightarrow Y_\Gamma$$

se prolonge en une fibration semi-stable

$$E_\Gamma \longrightarrow X_\Gamma$$

que l'on note surface elliptique modulaire.

Par ailleurs, si on considère les surfaces elliptiques semi-stables sur $\mathbb{P}^1$

$$f : X \longrightarrow \mathbb{P}^1$$

c'est à dire les surfaces dont les fibres singulières sont de type I_c, (où I_c est un polygone à c côtés formé de courbes rationnelles) on montre qu'elles admettent au moins quatre fibres singulières et sont rationnelles. Beauville [1] a donné une liste (finie) de telles surfaces et montré qu'elles correspondent aux surfaces elliptiques modulaires avec $\Gamma \in \mathfrak{G}$.

$\Gamma(3)$
$X^3+Y^3+Z^3+tXYZ=0$
$\Gamma_1(4)\cap\Gamma(2)$
$X\left(X^2+Z^2+2ZY\right)+tZ\left(X^2-Y^2\right)=0$
$\Gamma_1(5)$
$X(X-Z)(Y-Z)+tZY(X-Y)=0$
$\Gamma_1(6)$
$(X+Y)(Y+Z)(Z+X)+tXYZ=0$
$\Gamma_0(8)\cap\Gamma_1(4)$
$(X+Y)\left(XY-Z^2\right)+tXYZ=0$
$\Gamma_0(9)\cap\Gamma_1(3)$
$X^2Y+Y^2Z+Z^2X+tXYZ=0$

Rappelons que la courbe $Y_{\Gamma_1(N)}$ (resp. $Y_{\Gamma_0(N)}$) est définie sur $\mathbb{Q}$ et paramétrise les couples (E, A_N) où E est une courbe elliptique, ayant un point A_N d'ordre N, (resp. (E, C_N) où C_N est un groupe cyclique d'ordre N). Si E est une courbe elliptique définie sur $\mathbb{Q}$ et si A_N est définie sur $\mathbb{Q}$, il existe $t\in\mathbb{Q}$ telle que E soit isomorphe, sur $\mathbb{Q}$, à $E_{\Gamma_1(N)}$. Pour cela il suffit d'écrire une équation de Weierstrass de E de la forme

$$E_{b,c} : y^2+(1-b)\,xy-cy=x^3-cx^2 \tag{1}$$

en choisissant le point de N-torsion en $(0,0)$, ce qui donne une relation entre b et c. Nous expliciterons, dans le troisième paragraphe et pour chaque groupe de $\mathfrak{G}$ l'isomorphisme entre $E_{b,c}$ et la fibre en t de E_Γ. On utilisera une propriété analogue dans les cas où le groupe de torsion n'est pas cyclique.

2.2. Courbes de rang 2.

On considère le produit fibré associé à Γ

$$f^2=f\times f : E_\Gamma^2=E_\Gamma\times_{X_\Gamma}E_\Gamma\longrightarrow X_\Gamma.$$

En général E_Γ^2 a des singularités provenant des points critiques de l'application f. Cependant, comme f n'a que des fibres singulières semi-stables, les singularités de E_Γ^2 sont des points singuliers ordinaires.

On montre (cf. [7] et [8]) qu'on peut construire une résolution projective

$$\mathcal{X}\longrightarrow E_\Gamma\times_{X_\Gamma}E_\Gamma$$

telle que $\mathcal{X}$ soit une variété de dimension 3, de Calabi-Yau, c'est à dire une variété projective lisse telle que

- $H^1(\mathcal{X}, O_X)=H^2(\mathcal{X}, O_{\mathcal{X}})=0$
- le fibré canonique est trivial, i.e. $K_{\mathcal{X}}\simeq O_{\mathcal{X}}$.

De plus, la variété est rigide ($h^{1,2}(\mathcal{X}) = h^{2,1}(\mathcal{X}) = 0$), de sorte que le nombre de Betti $B_3(\mathcal{X}) = 2$.

Chercher des courbes elliptiques de rang 2 avec une structure de torsion correspondant à la liste $\mathfrak{G}$ revient à chercher des points rationnels sur le produit fibré et à montrer, en plus, que les points construits sur la courbe elliptique (fibre en t de E_Γ) sont indépendants.

2.3. Fibrations elliptiques.

Nous montrons que les produits fibrés des surfaces elliptiques modulaires E_Γ avec $\Gamma \in \mathfrak{G}$ admettent une fibration elliptique

$$\begin{array}{ccc} E_\Gamma \times_{X_\Gamma} E_\Gamma & \longrightarrow & \mathbb{P}^1 \times \mathbb{P}^1 \\ (\mathbf{X}, \mathbf{Y}, a, b) & \longmapsto & (a, b) \end{array}$$

Nous regroupons dans un tableau les résultats qui sont montrés dans [3] et dans les paragraphes suivants.

$\Gamma(3)$
$\mathbf{Y}^2 + (b-a)\left(b^2a^2 + 2a + 2b\right)\mathbf{XY} = \mathbf{X}\left(\mathbf{X} - a^4(b+1)^2\left(b^2 - b + 1\right)^2\right)\left(\mathbf{X} - b^4(a+1)^2\left(a^2 - a + 1\right)^2\right)$
$\Gamma_1(4) \cap \Gamma(2)$
$\mathbf{Y}^2 + 2(ba-1)(b-a)\mathbf{XY} = \mathbf{X}\left(\mathbf{X} - b^2\left(a^2-1\right)^2\right)\left(\mathbf{X} - a^2(b-1)^2\right)$
$\Gamma_1(5)$
$\mathbf{Y}^2 + (b-a)(ab-2)\mathbf{XY} = \mathbf{X}\left(\mathbf{X} + a^2(b-1)^3\right)\left(\mathbf{X} + b^2(a-1)^3\right)$
$\Gamma_1(6)$
$\mathbf{Y}^2 - (b-a)(ab-1)\mathbf{XY} = \mathbf{X}(\mathbf{X} - ba^2(b+1)^2)(\mathbf{X} - ab^2(a+1)^2).$
$\Gamma_0(8) \cap \Gamma_1(4)$
$\mathbf{Y}^2 - (ab+1)(b-a)\mathbf{XY} = \mathbf{X}(\mathbf{X} + a^2b^2)^2$
$\Gamma_0(9) \cap \Gamma_1(3)$
$\mathbf{Y}^2 + (b-a)\mathbf{XY} = \mathbf{X}\left(\mathbf{X} - a^2b^3\right)\left(\mathbf{X} - a^3b^2\right)$

Les fibres génériques possèdent toutes des points de $2-$torsion et des points $\mathbb{Q}(a,b)$-rationnels d'ordre infini.

$\Gamma(3)$
$S_1 = \left(a^4(b+1)^2\left(b^2-b+1\right)^2, 0\right)$, $S_2 = \left(pb^2a^2, pb^2a^2(a-b)(ab-1)(ba-b-a)\right)$ où $p = \left(a^2-a+1\right)\left(b^2-b+1\right)(b+1)^2$ $T = (0,0)$ d'ordre 2
$\Gamma_1(4) \cap \Gamma(2)$
$S = \left(b^2\left(a^2-1\right)^2, 0\right)$ Tous les points d'ordre 2
$\Gamma_1(5)$
$S_1 = \left(-a^2(b-1)^3, 0\right)$ $S_2 = \left(ab(a-1)(b-1), ab(a-1)(b-1)(a^2b-ab+b-a\right)$ $T = (0,0)$ de 2-torsion
$\Gamma_1(6)$
$S_1 = \left(ab^2(a+1)^2, 0\right)$ $S_2 = \left(a^2b^2(a+1)(b+1), a^2b^3(a+1)(b+1)(ab-1)\right)$ $T = (0,0)$ de 2-torsion
$\Gamma_0(8) \cap \Gamma_1(4)$
$S = \left(ba^3, b^4a^3(ax+1)\right)$ $T = \left(-a^2b^2, 0\right)$ d'ordre 4
$\Gamma_0(9) \cap \Gamma_1(3)$
$S = \left(a^3b^2, 0\right)$ $T = (0,0)$ de 2-torsion

2.4. Courbes de rang ≥ 3.

Soit $\Gamma \in \{\Gamma_1(4) \cap \Gamma(2), \Gamma_1(5), \Gamma_1(6), \Gamma_0(8) \cap \Gamma_1(4)\}$. Par combinaison de points S_i (ou S) et de torsion on construit comme pour $\Gamma_1(5)$ (cf. [3]) une courbe elliptique sur $\mathbb{Q}(a)$ de rang ≥ 3. Pour $\Gamma(3)$ et $\Gamma_0(9) \cap \Gamma_1(3)$ il est possible de faire une construction analogue mais il faut changer la base de la fibration précédente.

Des courbes de rang > 3 ont été construites par A. Dujella par spécialisation des familles de rang 2 et 3 issues des exemples donnés dans les paragraphes suivants. La méthode consiste d'abord à sélectionner des courbes avec de nombreux points modulo un nombre premier p.

Plus précisément, pour N un entier fixé, E une courbe elliptique et $a_p = p + 1 - |E(\mathbb{F}_p)|$, on définit

$$S_1(N) = S_1(N,E) = \sum_{\substack{p \leq N \\ p \text{ premier}}} \frac{-a_p + 2}{p + 1 - a_p} \log p,$$

$$S_2(N) = S_2(N,E) = \sum_{\substack{p \leq N \\ p \text{ premier}}} \frac{-a_p + 2}{p + 1 - a_p},$$

$$S_3(N) = S_3(N,E) = \sum_{\substack{p \leq N \\ p \text{ premier}}} -a_p \log p.$$

Il est alors expérimentalement connu qu'on peut espérer obtenir des courbes de grand rang si $S_{i=1,2,3}(N)$ est grand. Le rang est alors minoré par construction effective de points indépendants, utilisant les programmes MWRANK (J. Cremona) et RATPOINTS (M. Stoll). Le rang est majoré par la borne de Mazur pour les courbes ayant de la torsion [4]. Nous remercions A. Dujella pour les exemples de courbes de rang 5 et 6 que nous donnons ici. Une étude plus approfondie fera l'objet d'une autre publication.

3. Résultats

3.1. Surface $\Gamma_1(5)$. Complétons l'étude de ce cas, en donnant des exemples de courbes de rang 6 et 5.

3.1.1. *Exemples.* Le plus grand rang actuellement connu (Septembre 2002) [2] , a été obtenu avec l'exemple (2) de [3] pour $(a,b) = \left(\frac{3}{7}, \frac{7}{16}\right)$. Plus précisément la courbe

$$y^2 + (1-d)\,xy - dy = x^3 - dx^2$$

avec $d = \frac{-65151}{15785} = -\frac{3^3 19 \times 127}{5 \times 7 \times 11 \times 41}$est de rang 6. Les points suivants sont indépendants

$$\begin{array}{cc}
\left(\frac{-3^3 \times 19}{7 \times 11}, \frac{3^6 19}{7 \times 11 \times 41}\right) & \left(\frac{-3^3 19 \times 37}{2^2 5^2 7 \times 41}, \frac{-3^6 19 \times 37^2 79}{2^3 5^3 7^2 11 \times 41^2}\right) \\
\left(\frac{-3^3 19}{5 \times 41^2}, \frac{2 \times 3^6 19^2}{5^2 \times 7 \times 11 \times 41^3}\right) & \left(\frac{-2^5 3 \times 19 \times 127}{7^2 29^2}, \frac{3 \times 19^2 127^2}{7^3 29^3}\right) \\
\left(\frac{3^4 19 \times 127}{2^4 5 \times 41}, -\frac{3^8 19^2 127}{2^6 5^2 7 \times 41}\right) & \left(\frac{3^2 19 \times 127}{577^2}, \frac{2^2 3^2 19^2 127 \times 179}{5 \times 7 \times 11 \times 577^3}\right).
\end{array}$$

Si on choisit $(a,b) = \left(\frac{1}{3}, \frac{6}{7}\right)$, soit $d = 1292/12201 = \frac{2^2 17 \times 19}{3 \times 7^2 \times 83}$, les points d'abscisse

$$\begin{array}{ccc}
\frac{2^2 5 \times 17}{3^4}, & -\frac{2^2 17}{3^6}, & -\frac{2^3 5 \times 17 \times 19}{7^2 31^2}, \\
\frac{2^7 17 \times 19}{5^6 7^2}, & \frac{2^4 19 \times 31}{7^3 17^2}, &
\end{array}$$

sont rationnels et indépendants sur la courbe correspondante.

On obtient aussi deux courbes de rang 5 pour $(a,b) = (2, 5/7)$ (soit $d = -\frac{2^2 3^2 5^2}{7\times 43}$) et $(a,b) = (3/4, 7/5)$ $(d = \frac{3^2\times 7\times 11}{5\times 23\times 31})$.

3.2. Surface $\mathbf{E}_{\Gamma_1(6)}$. Dans ce cas la courbe $E_{b,c}$ a pour équation

$$y^2 + (1-c)\,xy - \left(c+c^2\right) y = x^3 - \left(c+c^2\right) x^2 \tag{2}$$

de discriminant $c^6\,(9c+1)\,(c+1)^3$.

Posant $x = \frac{c}{4}\,(Xc+2c+4)$, $y = \frac{1}{8}c^2\,(Yc+2Xc+4c+8)$ et $c = -1/d$, la courbe E_c est isomorphe à la courbe d'équation

$$Y\,(Y - 2\,(X+2)\,(d-1)) = (X-2)\,(X+2)\,(X+2-4d)$$

où le point $(2,0)$ est d'ordre 3, le point $(-2,0)$ d'ordre 2 et enfin $(-2+4d,0)$ d'ordre 6. Cette dernière forme de Weierstrass montre aussi que la surface elliptique est rationnelle.

Nous préférons toutefois utiliser le modèle

$$E_d : Y^2 - 2\,(d-1)\,(X+4d)\,Y = X\,(X+4d)\,(X-4+4d)$$

dans lequel les coordonnées des points obtenus dans le théorème suivant sont plus simples. L'équation E_d est obtenue à partir de la précédente en remplaçant X par $-2+4d+X$.

Le changement de variables

$$X = 2\left(1 - 2d + \frac{1-d}{U} + \frac{V+1}{U^2}\right), \quad Y = \frac{2}{U}X,$$

montre que la courbe E_d est birationnellement équivalente à la quartique

$$V^2 = U^4 + 2(-d+1)U^3 + (3-6d+d^2)U^2 + 2(-d+1)U + 1.$$

Enfin, posant

$$W = \frac{\left(-U^2 - 3U + dU - 1\right)}{2(U+1)} + \frac{V}{2\,(U+1)}$$

la courbe E_d est birationnellement équivalente à la courbe notée S_d d'équation (cf. [1] et [9])

$$S_d : (W+U+1)\,(WU+U+W) = dWU.$$

Remarque 2. Posant $d = t+1$, (cf. [1]) on obtient aussi l'équation de $E_{\Gamma_1(6)}$

$$(U+W)\,(W+1)\,(U+1) = tUW.$$

Si K désigne un corps et si M_1 et $M_2 \in E_d\,(K)$ sont deux points $\notin E_d\,(K)_{tor}$, on note (A,Z) et (B,T) les points correspondants sur S_d. Le point (A,Z,B,T) est un point $K-$rationnel du produit fibré $E_{\Gamma_1(6)} \times_{\Gamma_1(6)} E_{\Gamma_1(6)}$ d'équation

$$(A+Z+1)\,(AZ+A+Z)\,BT = (B+T+1)\,(BT+T+B)\,AZ.$$

Notons aussi

$$\begin{aligned} d &= d\,(A,Z) = \frac{(A+Z+1)\,(AZ+A+Z)}{AZ} \\ &= \frac{(B+T+1)\,(BT+B+T)}{BT}. \end{aligned}$$

On étudie la fibration elliptique

$$\begin{aligned} E_{\Gamma_1(6)} \times_{\Gamma_1(6)} E_{\Gamma_1(6)} &\longrightarrow \mathbb{P}^1 \times \mathbb{P}^1 \\ (A,Z,B,T) &\longmapsto (A,B)\,. \end{aligned}$$

Définition 3. On notera $C_{a,b}$ la courbe affine d'équation

$$(a+Z+1)\,(aZ+a+Z)\,bT = (b+T+1)\,(bT+T+b)\,aZ.$$

Proposition 4. *La cubique* $C_{a,b}$ *a un modèle de Weierstrass*

$$\mathbf{Y}^2 - (b-a)(ab-1)\mathbf{XY} = \mathbf{X}(\mathbf{X} - ba^2(b+1)^2)(\mathbf{X} - ab^2(a+1)^2).$$

Les points de coordonnées

$$\begin{aligned} S_1 &= \left(\mathbf{X} = ab^2\,(a+1)^2\,, \mathbf{Y} = 0\right) \\ S_2 &= \left(\mathbf{X} = a^2b^2\,(a+1)\,(b+1)\,, \mathbf{Y} = a^2b^3\,(a+1)\,(b+1)\,(ab-1)\right) \end{aligned}$$

sont indépendants et le point $(0,0)$ *est d'ordre* 2.

Posons

$$T = \frac{\mathbf{X}\left(\mathbf{X} - ba^2\,(b+1)^2\right)}{a(b+1)\mathbf{Y}}, Z = \frac{\mathbf{Y}}{b\,(a+1)\left(\mathbf{X} - ba^2\,(b+1)^2\right)}.$$

On définit ainsi une application birationnelle, définie sur $\mathbb{Q}\,(a,b)$, d'inverse

$$\begin{aligned} \mathbf{X} &= ab\,(b+1)\,(a+1)\,ZT \\ \mathbf{Y} &= ab^2\,(b+1)\,(a+1)\,Z\,(-\,(a+1)\,ZT + a\,(b+1)) \end{aligned}$$

entre la cubique $C_{a,b}\,(Z,T)$ et la courbe elliptique d'équation

$$\mathbf{Y}^2 - (b-a)(ab-1)\mathbf{XY} = \mathbf{X}(\mathbf{X} - ba^2(b+1)^2)(\mathbf{X} - ab^2(a+1)^2).$$

Le point $(Z=b, T=a)$ de $C_{a,b}$ a pour image S_2.

L'étape suivante consiste à construire une courbe elliptique sur $\mathbb{Q}\,(a,b)$ avec deux points $\mathbb{Q}\,(a,b)$ rationnels.

Au point $S = n_1S_1 + m_1S_1 + \varepsilon\,(0,0)$ où $(m_1,n_1,\varepsilon) \in \mathbb{Z}^2 \times \{0,1\}$ de $C_{a,b}$ correspond le point $(a, Z\,(a,b)\,, b, T\,(a,b))$ du produit fibré $E_{\Gamma_1(6)} \times_{\Gamma_1(6)} E_{\Gamma_1(6)}$. Les courbes elliptiques E_d avec $d = d\,(a, Z\,(a,b))$ définies sur $\mathbb{Q}\,(a,b)$ possèdent alors deux points $\mathbb{Q}\,(a,b)$-rationnels. Plus précisément, nous donnons quatre exemples de cette construction.

Exemple 1. A partir du point

$$S_1 + 2S_2 + (0,0) = \left(Z_1 = \frac{-\left(a^2-1\right)b}{(b+a)(b-1)}, T_1 \right)$$

de $C_{a,b}(Z,T)$ on considère la courbe E_{d_1} avec

$$d_1 = d(a, Z_1(a,b)) = \frac{\left(b-a^2\right)\left(a-b^2\right)(ab+1)}{ab(a+b)(a-1)(b-1)}.$$

Exemple 2. A partir du point

$$2S_1 - S_2 + (0,0) = \left(Z_2 = -\frac{(ba+b+a)a}{b(b+a+1)}, T_2 \right)$$

de $C_{a,b}(Z,T)$ on considère la courbe E_{d_2} avec

$$d_2 = d(a, Z_2(a,b)) = \frac{\left(a(a+1)(b+1)-b^2\right)\left(b(b+1)(a+1)-a^2\right)}{ab(ab+b+a)(b+a+1)}.$$

Exemple 3. A partir du point

$$3S_1 + (0,0) = \left(Z_3 = \frac{\left(a^2+a+1\right)b}{(b^2+b+1)(a+1)}, T_3 \right)$$

de $C_{a,b}(Z,T)$ on considère la courbe E_{d_3} avec

$$d_3 = \frac{\left(ba(ab+2(a+b)+1)+(b+a+1)^2\right)(ba(a+b+2)+a+b)}{ab(a^2+a+1)(b^2+b+1)}.$$

Exemple 4. A partir du point

$$2S_2 = \left(Z_4 = -\frac{\left(-b^2+a\right)a(a+1)}{(b+a)(a^2-b)}, T_4 \right)$$

de $C_{a,b}(Z,T)$ on considère la courbe E_{d_4} avec

$$d_4 = -\frac{(a-1)(b-1)(ab+2(a+b)+1)\left(b^2+a^2+ab\right)}{(a+b)(b-a^2)(a-b^2)}.$$

Dans tous ces exemples, les points de E_{d_i} qui vérifient $Y = 2X/a$ et $Y = 2X/b$ engendrent un groupe de rang 2 : dans chaque cas, l'indépendance des points est montrée par spécialisation.

Remarque 5. Nous avons choisi des points S qui donnent des fractions rationnelles $Z(a,b)$ de degré au plus 2 en a ou b.

3.2.1. *Courbes de rang* 3. On choisit x et y de sorte que $Z_1(a,x) = Z_2(a,y)$, soit

$$\frac{-\left(a^2-1\right)x}{(x+a)(x-1)} = -\frac{(ya+y+a)\,a}{y\,(y+a+1)} \tag{3}$$

et on considère la courbe E_d telle que

$$d = d\,(a, Z_1(a,x)) = d\,(a, Z_2(a,y))\,.$$

Les points de E_d qui vérifient $Y = 2X/a, Y = 2X/x$ ou bien $Y = 2X/y$ sont définis sur le corps $\mathbb{Q}(a,x,y)$.

L'égalité $Z_1(a,x) = Z_2(a,y)$ définit une courbe H_a. On se ramène alors à étudier les points de cette courbe sur $\mathbb{Q}(a)$. Les factorisations de (3) montrent que H_a est une courbe elliptique sur $\mathbb{Q}(a)$ qui possède des points rationnels sur ce corps. Plus précisément, on montre que cette courbe a deux points indépendants et un point d'ordre 2, définis sur $\mathbb{Q}(a)$. Par exemple le point $\left(x = \frac{a^3+a^2+a-1}{a^2+2a-1}, y = \frac{a^3(a+1)}{a^3+a^2+a-1}\right)$ est $\mathbb{Q}(a)$-rationnel sur H_a. La courbe E_d où $d = d_1(a, Z_1(a,x)) = d_2(a, Z_2(a,y))$ a alors trois points $\mathbb{Q}(a)$-rationnels. Par spécialisation en $a = 1/2$ on montre l'indépendance de ces points, ce qui prouve le théorème suivant :

Théorème 6. *La courbe* E_d

$$Y^2 - 2(d-1)(X+4d)\,Y = X\,(X+4d)\,(X-4+4d)$$

où

$$d = \frac{\left(a^2+a-1\right)\left(a^3+2a-1\right)\left(a^5+2a^4+a^3-a^2+2a-1\right)}{a^2(a+1)(2a-1)(a^3+a^2+a-1)(a^2+2a-1)}$$

a un rang ≥ 3 *sur* $\mathbb{Q}(a)$.

Les points $P_1 = (X_1, Y_1 = 2X_1/a)$, $P_2 = (X_2, Y_2 = 2X_2/x)$ *et* $P_3 = (X_3, Y_3 = 2X_3/y)$ *sont indépendants, où*

$$X_1 = -\frac{4(a-1)^2\left(a^2+a-1\right)\left(a^3+2a^2+a-1\right)\left(a^3+2a-1\right)}{a^3(2a-1)(a^2+2a-1)(a^3+a^2+a-1)},$$

$$X_2 = -\frac{4(a-1)\left(a^3+2a-1\right)\left(a^4+2a^3+a^2+a-1\right)}{a^2(a+1)(2a-1)(a^2+2a-1)} \times \frac{\left(a^5+2a^4+a^3-a^2+2a-1\right)}{(a^3+a^2+a-1)^2},$$

$$X_3 = -\frac{4(a-1)\left(a^4+2a^3+a^2+a-1\right)\left(a^5+2a^4+a^3-a^2+2a-1\right)}{a(a+1)^2(2a-1)(a^2+2a-1)(a^3+a^2+a-1)},$$

$$x = \frac{a^3+a^2+a-1}{a^2+2a-1} \qquad et \qquad y = \frac{a^3(a+1)}{a^3+a^2+a-1}.$$

Remarque 7. Les seuls facteurs premiers de $\mathbb{Z}[a]$ qui interviennent dans les coordonnées X_i et Y_i sont des diviseurs des numérateurs et dénominateurs de d et de $d-1$. D'autres courbes E_d peuvent être construites avec $Z_1(a,x) = Z_2(a,y)$; on obtient toutefois des fractions en a de degré plus élevé, par exemple

$$x = \frac{3a^3 + a^2 + a - 1}{(a-1)^2(a+1)}, \qquad y = -\frac{(a^2+1)(a^3+a^2+a-1)}{(a+1)(3a^3+a^2+a-1)}.$$

3.2.2. *Courbes de rang* > 3. Le plus grand rang obtenu pour une courbe elliptique E avec $E(\mathbb{Q})_{tor} \sim \mathbb{Z}/6\mathbb{Z}$ est, à ce jour, de 7. Utilisant la famille donnée par le théorème, on obtient pour $a = 5/8$ une courbe de rang 6, pour $a = 9$ une courbe de rang 5. Les valeurs $a = 2, 3, 4$ donnent des courbes de rang 4.

Les courbes de l'exemple (1) avec $(a,b) = (7,34)$ et $(2,39)$, de l'exemple (3) avec $(a,b) = (9,25)$ donnent des courbes de rang 6. L'exemple (2) fournit une courbe de rang 5 pour $(a,b)=(2,39)$.

3.3. Surface $\mathbf{E}_{\Gamma(2)\cap\Gamma_1(4)}$. La méthode et les définitions sont essentiellement les mêmes que dans le cas précédent, nous ne donnerons que les résultats.

La courbe elliptique $E_{b,c}$ d' équation

$$y^2 - 2cxy = x^3 + x^2 + c^2x$$

a un groupe de torsion isomorphe à $\mathbb{Z}/2 \times \mathbb{Z}/4$. Posant $c = 1/d, X = -dx$ et $Y = dy, Z = 1$ cette courbe est birationnellement équivalente à la courbe $E_{\Gamma(2)\cap\Gamma_1(4)}$ d'équation

$$X\left(X^2 + Z^2 + 2YZ\right) + d\left(X^2 - Y^2\right)Z = 0.$$

Le produit fibré a pour équation

$$E^2_{\Gamma(2)\cap\Gamma_1(4)} : A\left(A^2 + 1 + 2Z\right)\left(B^2 - T^2\right) - B\left(B^2 + 1 + 2T\right)\left(A^2 - Z^2\right) = 0.$$

Nous utiliserons la fibration elliptique de $E^2_{\Gamma(2)\cap\Gamma_1(4)}$

$$\begin{array}{ccc} E^2_{\Gamma(2)\cap\Gamma_1(4)} & \longrightarrow & \mathbb{P}^1 \times \mathbb{P}^1 \\ (a, Z, b, T) & \longmapsto & (a, b) \end{array}$$

et nous noterons $C_{a,b}$ la fibre générique

$$b\left(b^2 + 1 + 2T\right)\left(a - B^2\right) - a\left(a^2 + 1 + 2B\right)\left(b^2 - T^2\right) = 0.$$

Proposition 8. *La fibre générique $C_{a,b}$ a un modèle de Weierstrass*

$$\mathbf{Y}^2 + 2(ba-1)(b-a)\mathbf{XY} = \mathbf{X}^3 - \left(a^4b^2 + b^4a^2 - 4a^2b^2 + a^2 + b^2\right)\mathbf{X}^2 + a^2\left(a^2-1\right)^2\left(b^2-1\right)^2 b^2\mathbf{X}.$$

Les points d'abscisses 0, $ab\left(a+1\right)^2\left(b-1\right)^2$ $ab\left(a-1\right)^2\left(b+1\right)^2$ *sont d'ordre* 2. *Le point* $P_1=\left(b^2\left(a^2-1\right)^2,0\right)$ *est d'ordre infini.*

Le changement de variables

$$T=-\frac{1}{2}\left(b^2+1\right)+\frac{1}{2}\frac{\mathbf{X}\left(\mathbf{X}-a^2\left(b^2-1\right)^2\right)}{a\mathbf{Y}}$$
$$Z=\frac{1}{2}\frac{\mathbf{Y}-b\left(a^2+1\right)\mathbf{X}+ba^2\left(a^2+1\right)\left(b^2-1\right)^2}{b\left(\mathbf{X}-a^2\left(b^2-1\right)^2\right)}$$

d'inverse

$$\mathbf{X}=ba\left(a^2+1+2B\right)\left(b^2+1+2Y\right)$$
$$\mathbf{Y}=ba\left(a^2+1+2B\right)$$
$$\times\left(4bBY+2b\left(a^2+1\right)Y+2b\left(c^2+1\right)B-\left(b^3a-1\right)\left(b-a\right)+b\left(b+a\right)^2\right)$$

donne le résultat.

Exemple 1. Considérant le point $-S$ on obtient

$$Z_1\left(a,b\right)=-\frac{1}{2}\frac{a\left(a^2+1\right)\left(b^2+1\right)-b\left(a^4-6a^2+1\right)}{\left(a+b\right)\left(ab+1\right)}$$
$$T_1\left(a,b\right)=-\frac{1}{4}\frac{\left(ba-1\right)\left(b-a\right)}{a}$$

et

$$d_1=-8\frac{ab\left(a+b\right)\left(ab+1\right)}{\left(\left(ba-1\right)^2\left(b-a\right)^2-16b^2a^2\right)}.$$

Exemple 2. Considérant le point $2S$, on obtient

$$Z_2\left(a,b\right)=\frac{1}{4}\frac{\left(ba-1\right)\left(b-a\right)}{b}$$
$$T_2\left(a,b\right)=-\frac{1}{4}\frac{\left(ba-1\right)\left(b-a\right)}{a}$$

et la même valeur de d que dans l'exemple précédent.

3.3.1. *Courbes de rang* 3. Pour a fixé, chercher x et y tels que $Z_1\left(a,x\right)=Z_2\left(a,y\right)$ revient à chercher des points $\mathbb{Q}\left(a\right)$-rationnels sur la courbe elliptique

$$y_1^2-\frac{3a^2+1}{a}x_1y_1=x_1^3-17x_1^2+16x_1.$$

Cette courbe est de rang > 0 sur $\mathbb{Q}(a)$: le point $L = \left(x_1 = 1, y_1 = 3\frac{a^2+1}{a}\right)$ est d'ordre infini. Le point $-2L$ donne la solution

$$\begin{aligned} x &= \frac{a^2-4}{a\,(4a^2-1)} \\ y &= -5\frac{a}{a^2+1}. \end{aligned}$$

On obtient alors le théorème suivant :

Théorème 9. *La courbe elliptique*

$$Y^2 - \frac{2}{d}XY = X^3 + X^2 + \frac{X}{d^2}$$

avec

$$d = -40\frac{a\left(a^2+1\right)\left(a^2-4\right)\left(4a^2-1\right)}{36a^8+44a^6+641a^4+44a^2+36}$$

a un rang ≥ 3 *sur* $\mathbb{Q}(a)$; *les points d'abcsisses* $-\frac{a}{d}, -\frac{a^2-4}{a(4a^2-1)d}$, *et* $5\frac{a}{(a^2+1)d}$ *sont indépendants.*

En spécialisant pour $a = 1/3$ soit $d = -112/171$, on montre l'indépendance des trois points.

3.3.2. *Courbes de rang >3.* Le plus grand rang obtenu, à ce jour, pour une courbe elliptique sur $\mathbb{Q}$ dont le groupe de torsion est isomorphe à $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, est de 6. Choisissant $a = 1/12$, $a = 2/11$ dans le théorème, ou bien $(a, b) = (20, 64)$ dans l'exemple (1), permet de construire des courbes de rang 5.

3.4. Surface $\mathbf{E}_{\Gamma_0(8)\cap\Gamma_1(4)}$. La surface elliptique rationnelle

$$(X+Y)\left(XY - Z^2\right) - dXYZ = 0$$

correspondant au groupe de congruence $\Gamma_0(8) \cap \Gamma_1(4)$ a pour équation de Weierstrass

$$y^2 + dxy = x\,(x+1)^2\,.$$

Il suffit, pour cela, de poser $-x = XY$, $y = -(x+1)Y$ et $Z = 1$.

Le point $A = (x = -1, d)$ est d'ordre 4, et il existe un point A_1 d'ordre 8 tel que $2A_1 = A$. Le point A_1 est défini dans une extension galoisienne de $\mathbb{Q}(d)$.

Le produit fibré a pour équation

$$(B+T)\,(BT-1)\,AZ - (A+Z)\,(AZ-1)\,BT = 0.$$

Considérons la fibration elliptique

$$\begin{array}{ccc} E^2_{\Gamma_0(8)\cap\Gamma_1(4)} & \longrightarrow & \mathbb{P}^1 \times \mathbb{P}^1 \\ (A, Z, B, T) & \longmapsto & (A, B) \end{array}$$

de fibre générique $C_{a,b}$ d'équation

$$(b+T)\,(bT-1)\,aZ - bT\,(a+Z)\,(aZ-1) = 0.$$

Proposition 10. *$C_{a,b}$ est birationnellement équivalente à la courbe*

$$\mathbf{Y}^2 - (ab+1)\,(b-a)\,\mathbf{XY} = \mathbf{X}(\mathbf{X}+a^2b^2)^2$$

Le point $T = \left(-a^2b^2, 0\right)$ est d'ordre 4. Le point $S = \left(b^3a^3, b^4a^3\,(ab+1)\right)$ est d'ordre infini.

Le changement de variables

$$T = \frac{\mathbf{X}\left(\mathbf{X}+a^2b^2\right)}{ba\mathbf{Y}}$$
$$Z = \frac{\mathbf{Y}}{ba\,(b^2a^2+\mathbf{X})}$$

transforme $C_{a,b}$ en

$$\mathbf{Y}^2 - (ab+1)\,(b-a)\,\mathbf{XY} = \mathbf{X}\left(\mathbf{X}+a^2b^2\right)^2.$$

Exemple 1. Le point $2S$ correspond à

$$\left(T_1 = \frac{b\,(ab-1)\left(1+a^2\right)}{a\,(1+b^2)\,(b+a)}, Z_1 = \frac{a\left(1+b^2\right)(ab-1)}{b\,(b+a)\,(1+a^2)}\right)$$

$$d_1 = \frac{\left(b^3a^3 - a^2 - b^2 - 2a^2b^2 - ab\right)\left(a^3b + b^3a + b^2a^2 + 2ab - 1\right)}{ba\,(1+b^2)\,(1+a^2)\,(ab-1)\,(b+a)}.$$

Exemple 2. Le point $2S + 2T$ correspond à

$$\left(T_2 = -\frac{a\left(1+b^2\right)(b+a)}{b\,(ab-1)\,(1+a^2)}, Z_2 = -\frac{b\left(1+a^2\right)(b+a)}{a\,(1+b^2)\,(ab-1)}\right)$$

$$d_2 = \frac{\left(a^3 + 2ba^2 + b^3a^2 - b^2a + b\right)\left(b^3 + a^3b^2 + 2ab^2 - a^2b + a\right)}{ba\,(1+b^2)\,(1+a^2)\,(b+a)\,(ba-1)}.$$

3.4.1. *Courbes de rang* 3. Chercher des valeurs de x et z pour lesquelles

$$Z_1\,(a,x) = Z_2\,(a,y)$$

revient à étudier l'équation

$$y^2a^2x - ay^2 - x^2y - 2axy - ya^2 - ax^2 + x = 0$$

c'est à dire à chercher des points $\mathbb{Q}(a)$-rationnels sur une courbe elliptique. On montre que cette courbe est de rang 1 sur $\mathbb{Q}(a)$ et possède un point d'ordre 3 sur $\mathbb{Q}(a)$. On trouve par exemple

$$y = -\frac{2a^4 + 2a^2 + 1}{a^3\,(a^4 + 2a^2 + 2)}$$

$$x = -\frac{(a-1)\,(a+1)\,\left(a^2+1\right)}{(a^4 + 2a^2 + 2)\,a}$$

comme solution de $Z_1(a,x) = Z_2(a,y)$.

Théorème 11. *Soit*

$$d = \frac{\left(a^{16} + 4a^{14} + 7a^{12} + 12a^{10} + 24a^8 + 32a^6 + 28a^4 + 14a^2 + 3\right)}{(a^6 + a^4 + 2a^2 + 1)\,(a^6 + 2a^4 + a^2 + 1)}$$

$$\times\frac{\left(3a^{16} + 14a^{14} + 28a^{12} + 32a^{10} + 24a^8 + 12a^6 + 7a^4 + 4a^2 + 1\right)}{(a^4 + 3a^2 + 1)\,(a^4 + 2a^2 + 2)\,(2a^4 + 2a^2 + 1)\,a\,(a^2 - 1)\,(a^2+1)^2};$$

la courbe

$$Y^2 + dXY = X\,(X+1)^2$$

a trois points indépendants sur $\mathbb{Q}(a)$. *Plus précisément les points de cette courbe qui sont aussi sur l'une des courbes*

$$aY = X\,(X+1)\,, \quad xY = X\,(X+1) \ \ \textit{et}\ yY = X\,(X+1)$$

où

$$x = -\frac{(a-1)\,(a+1)\,\left(a^2+1\right)}{(a^4 + 2a^2 + 2)\,a}$$

$$y = -\frac{2a^4 + 2a^2 + 1}{a^3\,(a^4 + 2a^2 + 2)}$$

sont $\mathbb{Q}(a)$*-rationnels et engendrent un groupe de rang* 3.

En spécialisant pour $a = 1/2$ on obtient l'indépendance des points d'où le résultat du théorème.

3.5. Surface $E_{\Gamma_0(9)\cap\Gamma_1(3)}$. La courbe $X^2Z + Y^2X + Z^2Y - dXYZ = 0$ est isomorphe à la courbe

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

par l'application

$$(X,Y,Z) \longmapsto \left(x = -X/Z, y = XY/Z^2\right)$$

d'inverse

$$(x,y) \longmapsto \left(x^2, y, -x\right).$$

Le produit fibré a pour équation

$$\left(B^2+T^2B+T\right)AZ=\left(A^2+Z^2A+Z\right)BT.$$

Nous utiliserons la fibration elliptique

$$\begin{array}{ccc} E^2_{\Gamma_0(9)\cap\Gamma_1(3)} & \longrightarrow & \mathbb{P}^1\times\mathbb{P}^1 \\ (a,Z,b,T) & \longmapsto & (a,b)\,. \end{array}$$

Proposition 12. *La fibre générique $C_{a,b}$ est birationnellement équivalent à*

$$\mathbf{Y}^2+(b-a)\,\mathbf{XY}=\mathbf{X}\left(\mathbf{X}-a^2b^3\right)\left(\mathbf{X}-a^3b^2\right).$$

Cette courbe possède les points rationnels $T=(0,0)$ d'ordre 2 et $S=\left(a^3b^2,0\right)$ d'ordre infini.

Le résultat est obtenu par le changement de variables

$$T=\frac{\mathbf{X}\left(\mathbf{X}-a^2b^3\right)}{\mathbf{Y}}$$
$$Z=\frac{\mathbf{Y}}{ab\left(\mathbf{X}-a^2b^3\right)}.$$

En considérant les points $3S$ et $3S+T$ nous obtenons respectivement les points

$$\left(T_1=\frac{-\left(a^2b-1\right)b^2}{\left(ab^2-1\right)},Z_1=-\frac{a^2b-1}{a\left(ab^2-1\right)}\right)$$
$$\left(T_2=-\frac{ab^2-1}{b\left(a^2b-1\right)},Z_2=-\frac{a^2\left(ab^2-1\right)}{a^2b-1}\right).$$

Ce qui donne

$$d_1=d_2=-\frac{a^4b^4-b^2a^2\left(a+b\right)+a^2+b^2-ab}{\left(a^2b-1\right)\left(ab^2-1\right)}.$$

3.6. Courbes de rang 3. Cherchons des valeurs de x et y pour lesquelles

$$Z_1\left(a,x\right)=Z_2\left(a,y\right).$$

Si $a=r^2$, nous trouvons que l'équation $Z_1\left(a,x\right)=Z_2\left(a,y\right)$ définit une courbe elliptique de rang >0 sur $\mathbb{Q}(r)$. Par exemple, si $y=\frac{1}{8}\frac{5r^6+3}{r^4}$ et $x=\frac{7+5r^3}{r(3+5r^3)}$ alors $Z_1\left(r^2,x\right)=Z_2\left(r^2,y\right)$ et

$$d=-\frac{625r^{12}-5850r^6+21801}{40\left(5r^3+13\right)\left(5r^3-13\right)r^2}.$$

Théorème 13. *La courbe elliptique*

$$Y^2 + dYX + Y = X^3$$

où

$$d = -\frac{625r^{12} - 5850r^6 + 21801}{40\,(5r^3+13)\,(5r^3-13)\,r^2}$$

possède trois points indépendants sur $\mathbb{Q}(r)$ *d'abscisses* $-r^2$, $-\frac{1}{8}\frac{5r^6+3}{r^4}$ *et* $-\frac{7+5r^3}{r(3+5r^3)}$.

L'indépendance des points est montrée en spécialisant en $r = 3$.

Les courbes correspondant à $\Gamma(3)$ sont isogènes sur $\mathbb{Q}(d)$ aux courbes $y^2 + dxy + y = x^3$. Des résultats analogues sont donc obtenus par isogénie.

Bibliographie

[1] A. Beauville, *Les familles stables de courbes elliptiques sur* $\mathbb{P}^1$ *admettent quatre fibres singulières.* C.R. Acad. Sc. Paris, Série I **294** (1982), 657–660.

[2] A. Dujella, *High rank elliptic curves with prescribed torsion.* http://www.math.hr/~duje/tors/tors.html.

[3] O. Lecacheux, *Rang de courbes elliptiques sur* $\mathbb{Q}$ *avec un groupe de torsion isomorphe à* $\mathbb{Z}/5\mathbb{Z}$. C. R. Acad. Sci. Paris Sér. I Math. **332** (2001), 1–6.

[4] B. Mazur, *Rational points on abelian varieties with values in towers of number fields.* Invent. Math. **18** (1972), 183–266.

[5] J.-F. Mestre, *Construction de courbes elliptiques sur* $\mathbb{Q}$ *de rang* ≥ 12. C. R. Acad. Sci. Paris Ser. I **295** (1982), 643–644.

[6] K. Nagao, *An example of elliptic curve over* $\mathbb{Q}$ *with rank* ≥ 20. Proc. Japan Acad. Ser. A Math. Sci. **69** (1993), 291–293.

[7] C. Schoen, *On the fiber product of rational elliptic surfaces with section.* Math.Z. **197** (1988), 177–199.

[8] M.-H. Saito, N. Yui, *The modularity conjecture for rigid Calabi-Yau threefolds over* $\mathbb{Q}$. J. Math. Kyoto Univ. **41** (2001), 403–419.

[9] J. Strienstra, F. Beukers, *On the Picard-Fuchs Equation and the Formal Brauer Group of Certain Elliptic* $K3$*-surfaces.* Math. Ann. **271** (1985), 269–304.

Odile Lecacheux
Institut de Mathématiques
Université Paris-VI
case 247
175 rue du Chevaleret
75013 Paris
France
E-mail : `lecacheu@math.jussieu.fr`