ACTA ARITHMETICA
109.2 (2003)

Rang de familles de courbes elliptiques

par

ODILE LECACHEUX (Paris)

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 :

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

où r est appelé le rang sur $\mathbb{Q}$ de E. Un théorème de Mazur donne les seules structures de torsion possibles :

$$E(\mathbb{Q})_{\text{tors}} = \begin{cases} \mathbb{Z}/m\mathbb{Z}, & m = 1, 2, \ldots, 10, 12, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}, & m = 1, \ldots, 4. \end{cases}$$

On notera $\mathcal{E}_N$ (resp. $\mathcal{E}_{n,m}$) l'ensemble des courbes elliptiques sur $\mathbb{Q}$ telles que $E(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/N\mathbb{Z}$ (resp. $E(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$), et on définit

$$b(N) = \sup\{r\,;\, E \in \mathcal{E}_N\}, \qquad B(N) = \limsup\{r\,;\, E \in \mathcal{E}_N\},$$
$$b(n,m) = \sup\{r\,;\, E \in \mathcal{E}_{n,m}\}, \qquad B(n,m) = \limsup\{r\,;\, E \in \mathcal{E}_{n,m}\}.$$

On ignore si $b(n,m)$ et $b(N)$ sont finis. Sans entrer dans les détails il faut retenir les résultats suivants :

• $b(0) \geq 24$ et $B(0) \geq 14$,

• $B(N)$ et $B(n,m) \geq 1$ pour toutes les valeurs de N, n et m, par exemple $B(2) \geq 8, B(5) \geq 3$.

Citons les travaux de divers auteurs qu'on pourrait presque faire remonter à Fermat : Kretschmer, Nagao, Fermigier, Mestre, Martin–McMillen, Kihara, Kulesz, Atkin–Morain, Dujella ... et d'autres (voir [3]).

Dans cet article nous nous intéresserons à $B(N)$ pour $N = 7$. Pour cet entier des exemples ont été construits et donnent $B(7) \geq 1$ (Kulesz [4], Atkin–Morain [1]). Notons aussi que $b(7) \geq 5$ [3].

Nous obtenons les résultats suivants :

THÉORÈME 1. *L'entier* $B(7)$ *est supérieur ou égal à* 2.

2000 *Mathematics Subject Classification*: Primary 11G05, 14H52; Secondary 14H10, 14J27, 14J28.

Plus précisément, il existe des courbes elliptiques sur $\mathbb{Q}$, de rang au moins deux sur $\mathbb{Q}$, ayant un point d'ordre 7 rationnel, paramétrées par les points rationnels de plusieurs courbes elliptiques dont au moins deux ont un rang sur $\mathbb{Q}$ égal à 3. Parmi ces familles de courbes ainsi construites, ayant un point de 7-torsion $\mathbb{Q}$-rationnel, certaines ont un rang 3.

2. Notations et méthode. On désignera par N un entier ≥ 5 ; on note $Y_1(N)$ la courbe modulaire sur $\mathbb{Q}$ qui paramétrise les couples (E, A_N) où E est une courbe elliptique, ayant un point A_N d'ordre exactement N. Soit $X_1(N)$ la compactification de $Y_1(N)$.

Soit E_N la courbe elliptique universelle qui correspond à cette structure. Alors E_N est une surface elliptique définie sur $\mathbb{Q}$ avec un morphisme de projection

$$\pi : E_N \to Y_1(N)$$

et une section $s : Y_1(N) \to E_N$, tous deux définis sur $\mathbb{Q}$.

La courbe $X_1(7)$ est de genre 0 et on notera d un générateur de son corps de fonctions. Nous noterons E_d la fibre générique. Enfin nous noterons $\mathbb{P}^1_z$ l'espace projectif avec point générique z.

Pour $N = 7$, le modèle minimal non singulier de la surface E_7 est une surface $K3$ ([7, pp. 276–277]). Nous montrons que la surface E_7 est birationnellement équivalente à la surface S_7 d'équation

$$(uv - u - v)(dv - 1)(du - 1) = uv(u - 1)(v - 1)d(d - 1)$$

et nous construisons une autre fibration elliptique de la surface S_7,

$$\phi_v : S_7 \to \mathbb{P}^1_v,$$

avec une section définie sur $\mathbb{Q}$. Nous noterons H_v la fibre générique. Les sections de E_7 correspondant aux points d'ordre 7 de E_d donnent sur H_v un point d'ordre 4 ainsi qu'un point P d'ordre infini sur $\mathbb{Q}(v)$. On construit ainsi en considérant les multiples de P une infinité de revêtements de

$$\mathbb{P}^1_{v_n} \to \mathbb{P}^1_d$$

et les changements de base $E_d \times_{\mathbb{P}^1_d} \mathbb{P}^1_{v_n}$ correspondants, ce qui donne une courbe elliptique de rang au moins 1 sur $\mathbb{Q}(v_n)$ avec un point de 7-torsion.

Parmi ces revêtements nous avons étudié ceux de petit degré, en particulier de degré 2, correspondant aux fractions rationnelles d_0, d_1, d_4 et d_5.

En prenant le produit fibré de deux tels changements de base on obtient une famille de courbes elliptiques de rang au moins deux au-dessus d'une base de genre 1. Cette dernière courbe, dans les cas étudiés, est une courbe elliptique de rang au moins 1 sur $\mathbb{Q}$. On obtient ainsi une infinité de courbes de rang au moins 2 sur $\mathbb{Q}$ munies d'un point $\mathbb{Q}$-rationnel d'ordre 7. Certaines courbes correspondant à trois points rationnels de $\mathbb{P}^1_{v_{n_i}}$ pour $i = 1, 2, 3$

donnent des exemples de courbes de rang 3 munies d'un point $\mathbb{Q}$-rationnel d'ordre 7.

2.1. *La surface E_7 et ses automorphismes.* Soit E une courbe elliptique sur $\mathbb{Q}$ ayant un point rationnel de 7-torsion. Il existe un rationnel d tel que la courbe E soit $\mathbb{Q}$-isomorphe à la courbe E_d d'équation

$$(E_d): \quad y^2 + (1 + d - d^2)xy + (d^2 - d^3)y = x^3 + (d^2 - d^3)x^2$$

de discriminant $d^7(d-1)^7(d^3 - 8d^2 + 5d + 1)$ et où le point d'ordre 7 est le point $A = (0, 0)$. Si on considère d comme une indéterminée on notera E_7 la surface d'équation

$$y^2 + (1 + d - d^2)xy + (d^2 - d^3)y = x^3 + (d^2 - d^3)x^2.$$

La surface elliptique E_7 admet l'automorphisme d'ordre 6 noté σ défini par

$$\begin{aligned} x &\mapsto \frac{x - d^2(d-1)}{d^4}, & & & x &\mapsto \frac{x + d - d^2}{(d-1)^4}, \\ y &\mapsto \frac{-y - dx + d^3(d-1)}{d^6}, & &\text{d'inverse} & y &\mapsto \frac{-(x+y) + xd}{(d-1)^6}, \\ d &\mapsto \frac{d-1}{d}, & & & d &\mapsto \frac{-1}{d-1}, \end{aligned}$$

qui a l'interprétation modulaire suivante : au couple (E, A) on associe le couple (E, iA) avec $(i, 7) = 1$.

Si M est un point générique de la courbe E_d, l'automorphisme défini sur E_d par $M \mapsto A + M$ définit un automorphisme noté σ_7, d'ordre 7, de E_7.

2.2. *La surface S_7.* Faisons les changements de coordonnées

$$x = \frac{d(d-1)}{u + v - uv}, \qquad y = \frac{(d-1)^2 d^2 u}{(u + v - uv)^2}$$

d'inverse

$$u = \frac{y}{x^2}, \qquad v = \frac{(x+d)d(d-1) - (x+y)}{x^2}.$$

Les fonctions u et v sur E_d ont comme diviseur

$$\operatorname{div}(u) = -2(6A) + 5A + \infty, \qquad \operatorname{div}(v) = -2(A) + 2A + \infty.$$

La surface E_7 est birationnellement équivalente à la surface

$$S_7: \quad -d(d-1)uv + (uv - u - v)(1 + d(uv - u - v)) = 0. \tag{2.1}$$

Nous utiliserons aussi les deux factorisations suivantes de l'équation de S_7 :

$$\begin{aligned} (dv - 1)(uv - u - v)(du - 1) &= uv(u-1)(v-1)d(d-1), \\ u(u-1)d(v-1)^2 &= (dv - 1)(ud + vu - u - v), \end{aligned}$$

ainsi que celle obtenue en intervertissant u et v.

On remarque que l'involution qui échange u en v correspond à l'involution $P \mapsto -P$ sur la courbe elliptique E_d.

L'automorphisme σ est défini sur 2.1 par

$$(u,v,d) \mapsto \left(\frac{(dv-1)(uv-u-v)^2}{(d-1)^2uv^2}, \frac{(du-1)(uv-u-v)^2}{(d-1)^2vu^2}, \frac{d-1}{d}\right).$$

L'automorphisme σ_7 est défini sur 2.1 par

$$(u,v,d) \mapsto \left(\frac{(u-1)(uv-u-v)}{du^2(d-1)}, -\frac{1}{d(uv-u-v)}, d\right).$$

Proposition 2. *La fibration*

$$\phi : S_7 \to \mathbb{P}^1_v, \qquad (u,v,d) \mapsto v,$$

définit sur S_7 une structure de surface elliptique de fibre générique H_v. La torsion du groupe de Mordell–Weil $H_v(\mathbb{Q}(v))$ est cyclique d'ordre 4 et le rang de ce groupe est égal à 1.

On pose

$$u = \frac{dv-1+Y}{d(v-1)}, \quad \text{soit} \quad Y = 1 + d(uv-u-v).$$

On obtient alors une cubique en (Y,d) dépendant de v.

Les transformations habituelles pour obtenir une forme de Weierstrass sont

$$\begin{aligned} U &= v(v-1)(Y+dv-(v^2-v+1)),\\ u &= \frac{(U+v^2(v-1)^2)U}{Z(v-1)^2}. \end{aligned}$$

Le changement de variable

$$\begin{aligned} d &= \frac{Z}{vU},\\ x &= \frac{(v-1)Z^2(Uv-Z)}{v^2U^2(U^2+v^2(v-1)^2U-vZ(v-1))},\\ y &= \frac{Z^3(Uv-Z)^2(U+v^2(v-1)^2)}{v^4U^3(U^2+v^2(v-1)^2U-vZ(v-1))^2} \end{aligned}$$

donne un modèle de Weierstrass de la fibre H_v, soit

$$\begin{aligned} &Z^2 + v(2v-3)UZ + v^2(2v-1)(v-1)^3Z\\ &\qquad = U(U+v(v-1)(v^2-v+1))(U+v^2(v-1)^2). \end{aligned}$$

Les points d'ordre 7 de E_d correspondent aux sections $U = Z$ et $vU = Z$, ce qui donne les points de H_v

$$\begin{aligned} A_1 &= (U = -v^2(v-1)^2, Z = -v^2(v-1)^2),\\ A_2 &= (-(v+1)(v-1)^3, -(v+1)(v-1)^3), \end{aligned}$$

$$A_3 = (-v(v-1)^3, -v^2(v-1)^3),$$
$$A_4 = (-v^2(v-1)(v-2), -v^3(v-1)(v-2)),$$
$$A_5 = (0,0).$$

Le point A_3 est d'ordre 2 et $2A_1 = A_3$, donc A_1 est d'ordre 4. D'autre part on a les relations suivantes :

$$A_1 + A_5 = A_2,$$
$$2A_1 + A_5 = A_4,$$
$$3A_1 + A_5 = (-v(v-1)(v^2-v+1), v^2(v-1)(v-2)).$$

En utilisant un résultat de Shioda [5], on peut calculer le rang sur $\mathbb{C}(v)$ de H_v. Par calcul on déduit le type des fibres dégénérées : en $v=0$ et $v=\infty$ les fibres sont de type I_1^*, en $v=1$ de type I_8 et en $v = (31 \pm 3i\sqrt{7})/32$ de type I_1. Le nombre de composantes est respectivement $m_s = 6, 8$, et 1. De la relation fondamentale

$$\mathrm{Rang}(H_v(\mathbb{C}(v))) + 2 + \sum_s (m_s - 1) = \mathrm{Rang}\,\mathrm{NS}(E_7)$$

il résulte que le rang du groupe de Mordell–Weil de $H_v(\mathbb{C}(v))$ est inférieur ou égal à un, compte tenu de l'inégalité $\mathrm{Rang}\,\mathrm{NS}(E_7) \leq 20$. Par spécialisation, par exemple pour $v=5$ on montre que le point A_5 spécialisé n'est pas d'ordre $2, 8$ ou 4, il est donc d'ordre infini compte tenu du théorème de Mazur.

On construit alors une infinité de familles à un paramètre de courbes elliptiques ayant de la 7-torsion et un rang ≥ 1. Pour cela on considère les points $rA_1 + sA_5$ ($s \in \mathbb{Z}$, $0 \leq r \leq 3$) de coordonnées $(u_{r,s}(v), v, d_{r,s}(v))$ sur S_7. En utilisant le changement de coordonnées $(u,v) \mapsto (x,y)$ précédent on obtient la famille $(E_{d_{r,s}(v)}, P_{r,s}(v))$. Montrons que $P_{r,s}(v)$ est d'ordre infini si $s \neq 0$. Si $rA_1 + sA_5 \neq A_i$, $1 \leq i \leq 5$, le point $P_{r,s}(v)$ n'est pas un multiple de A. Il existe donc au moins une valeur de $v_0 \in \mathbb{Q}$ pour laquelle le point $P_{r,s}(v_0)$ n'est pas multiple de A. Utilisant le théorème de Mazur, le point $P_{r,s}(v_0)$ ne peut être de torsion car la courbe $E_{d_{r,s}(v_0)}$ aurait un point rationnel d'ordre $7m, m \neq 1$.

Si $d = P/Q$ où P et Q sont deux polynômes premiers entre eux, on pose $\mathrm{ht}(d) = \max(\deg(P), \deg(Q))$. Les familles correspondant aux points

$$-2A_5 + hA_1 \qquad \text{avec } 0 \leq h \leq 4,$$

vérifient $\mathrm{ht}(d) = 2$.

2.3. *Involutions.* L'équation définissant S_7 est quadratique par rapport à chaque variable ; la surface S_7 peut être considérée comme un revêtement double de $\mathbb{P}^1 \times \mathbb{P}^1$ de 3 façons différentes, ce qui définit trois involutions

$$\begin{aligned}
e_u : \quad & (u,v,d) \mapsto \left(\frac{v(dv-1)}{d(v-1)^2u}, v, d\right),\\
e_v : \quad & (u,v,d) \mapsto \left(u, \frac{u(du-1)}{d(u-1)^2v}, d\right),\\
e_d : \quad & (u,v,d) \mapsto \left(u, v, -\frac{(u-1)(v-1)(d-1)}{(dv-1)(du-1)}\right).
\end{aligned}$$

On remarque que $(e_u \circ e_v)^2 = \sigma_7$. Si $f = e_u \circ e_v$, $g = e_d \circ e_v$ et $f_1 = g \circ f \circ g^{-1}$ alors $\sigma^3 = f \circ f_1 \circ f \circ e_d$ et $\sigma^4 = (g^2 \circ f \circ f_1 \circ g^2)^2$. Un calcul montre que $e_d \circ e_u$ est d'ordre 4, ainsi que $e_d \circ e_v$.

La surface S_7 contient les droites suivantes :

$$\begin{aligned}
D_0 : \quad & u = 0,\ v = 0,\\
D_1 : \quad & d = 1,\ u = 1,\\
D_2 : \quad & d = 1,\ v = 1.
\end{aligned}$$

Le plan tangent à S_7 passant par D_1 a pour équation

$$u + d = 2.$$

La surface S_7 contient les courbes de genre 0 :

$$\begin{aligned}
C_1 : \quad & d = 0,\ uv - u - v = 0,\\
C_2 : \quad & d = 1,\ uv - u - v = 0,\\
C_3 : \quad & u = 0,\ dv = 1; \qquad \widetilde{C}_3 : \quad u = 1,\ dv = 1,\\
C_5 : \quad & v = 0,\ du = 1; \qquad \widetilde{C}_5 : \quad v = 1,\ du = 1,\\
C_6 : \quad & u + d = 2,\ d = -\frac{v-2}{v^2 - v + 1},\\
C_7 : \quad & v + d = 2,\ d = -\frac{u-2}{u^2 - u + 1}.
\end{aligned}$$

La conique C_7 (resp. C_6) est stable par e_u (resp. e_v).

Les points $-2A_5 + hA_1$ correspondent à $e_u \circ \sigma_7^2 \circ (e_d \circ e_u)^{h+1} \circ e_u(C_6)$, ce qui donne les quatre valeurs de d :

$$d_0 = \frac{v^2-1}{v(v-2)}, \quad d_1 = \frac{-(v-2)}{v^2-v+1}, \quad d_2 = \frac{2v-1}{v(v+1)}, \quad d_3 = \frac{v^2-v+1}{2v-1}.$$

Remarque 3. On remarque que si on note g l'automorphisme d'ordre 6 de la droite projective défini par

$$t \mapsto g(t) = \frac{t+1}{2-t}$$

alors $g^4(v) = (v-1)/v$ et on a les résultats suivants : l'application $d \mapsto (d-1)/d$ laisse invariant d_0, plus précisément $d_0 = -g(v)g^4(v)$ et $d_0(g^4(v)) = (d_0(v)-1)/d_0(v)$, et elle permute les autres d_i, plus précisément $d_2(v) = (d_1(g^4(v)) - 1)/d_1(g^4(v))$ et $d_3(v) = -1/(d_1(g(v)) - 1)$.

La famille E_d avec $d = d_1(z)$ a été donnée dans [4].

Nous obtenons ainsi

Théorème 4. *Les courbes elliptiques* E_{d_i} *avec* $i = 0, 1, 2, 3$ *sont de rang* ≥ 1 *sur* $\mathbb{Q}(v)$ *et* $\mathrm{ht}(d) = 2$.

Le point de coordonnées (x_{P_i}, y_{P_i}) donné dans le tableau 1 est d'ordre infini.

Tableau 1

	d	(x_{P_i}, y_{P_i})
d_0	$\frac{v^2-1}{v(v-2)}$	$\left(-\frac{(v-1)(2v-1)}{v^2(v-2)}, \frac{(v-1)^2(2v-1)^2}{v^3(v-2)^2}\right)$
d_1	$\frac{-(v-2)}{v^2-v+1}$	$\left(\frac{-v(v^2-1)(v-2)^2}{(v^2-v+1)^3}, \frac{(v^2-1)^2(v-2)^2}{(v^2-v+1)^4}\right)$
d_4	$-6\,\frac{z-1}{(z-2)(z-4)}$	$\left(-9\,\frac{(z-1)^2}{(z-2)^2(z-4)^2}, 81\,\frac{z(z-1)^2}{(z-4)^3(z-2)^4}\right)$
d_5	$\frac{1}{2}\,\frac{(z+1)(z-4)}{(2z+1)(z-2)}$	$\left(-\frac{3}{2}\,\frac{z(z-1)(z+1)^2(z-4)^2}{(z+2)^2(z-2)^3(1+2z)^2}, \frac{9}{8}\,\frac{z^2(z-1)(z+1)^2(z-4)^3}{(2+z)^3(z-2)^4(1+2z)^3}\right)$
d_6	$8\,\frac{w}{w^3-w^2-w+9}$	$\left(-2\,\frac{w^2-9}{w^3-w^2-w+9}, 4\,\frac{(w^2-9)^2(w^3+w^2-w-9)}{(w^3-w^2-w+9)^3}\right)$
d_7	$-\frac{(v^2-1)(v-2)}{2v-1}$	$\left(-\frac{(v(v-1)^2+1)(v+1)(v^2-v+1)(v^3-v^2-1)(v-2)^2}{(2v-1)^4}, -\frac{(v+1)(v^3-v^2-1)^2(v(v-1)^2+1)^2(v-2)^3}{(2v-1)^6}\right)$

3. Autres familles de rang 1

3.1. Exemple 1. On cherche s'il existe des courbes C rationnelles sur S_7 telles que si $M = (u, v, d) \in C$ alors $e_d(M) = (u, v, k/d), k \in \mathbb{Q}$. On obtient de telles courbes avec $k = 1$ et $k = 1/4$ en imposant à la projection de C sur le plan $u = 0$ d'être rationnelle. Si $k = 1$ on retrouve d_0. Considérant la courbe correspondant au cas $k = 1/4$ ainsi que les courbes $(e_d \circ e_v)^h(C)$ on obtient deux nouvelles valeurs de d, $d_i(z)$, $i = 4, 5$ avec $\mathrm{ht}(d_i) = 2$:

$$d_4(z) = -6\,\frac{z-1}{(z-2)(z-4)}, \qquad d_5(z) = \frac{1}{2}\,\frac{(z+1)(z-4)}{(2z+1)(z-2)}.$$

Les coordonnées d'un point d'ordre infini sur E_{d_4} et E_{d_5} figurent dans le tableau 1. La courbe E_{d_4} possède aussi un point rationnel vérifiant $x = -1/(4d^2)$ [2].

Remarque 5. Si G désigne le groupe engendré par les trois involutions on peut construire un sous groupe $\neq \mathrm{Id}$ laissant fixe globalement C, correspondant au cas $k = 1/4$. Si $\varepsilon \in G$ nous n'avons pas obtenu d'exemples de courbe $\varepsilon(C)$ avec $\mathrm{ht}(d) < 3$.

3.2. Exemple 2. Considérons la courbe

$$e_u(C_6): \quad \left(u_1(v), v_1(v) = \frac{v(2v-1)}{v^2-v+1}, d_1(v)\right).$$

La courbe $H_{v_1(v)}$ a un rang sur $\mathbb{Q}(v)$ supérieur ou égal à deux, les points A_5 et l'image de $e_u(C_6)$ sont indépendants. Par combinaison de ces deux points et du point A_1 d'ordre 4, on construit comme au paragraphe précédent d'autres familles avec $\mathrm{ht}(d) \geq 3$. Les exemples d_6 et d_7 du tableau 1 sont ainsi obtenus. On peut de même utiliser la courbe $(u_4(z), v_4(z) = -(z^2-4)/3, d_4(z))$ de S_7 et la courbe $H_{v_4(z)}$.

4. Courbes elliptiques de rang ≥ 2

4.1. *Première méthode.* Les égalités $d_i(v) = d_j(w)$, $(d_i(w)-1)/d_i(w) = d_j(v)$ et $-1/(d_i(w)-1) = d_j(v)$ définissent des courbes affines et pour chercher des courbes de rang 2 nous chercherons des points rationnels sur ces courbes. Pour i et $j \in \{0,1,2,3,4,5\}$ les courbes obtenues sont des courbes elliptiques sur $\mathbb{Q}$ dont nous allons préciser les équations et le rang sur $\mathbb{Q}$.

Lemme 6. *Soit K le corps engendré par les coefficients de la courbe Γ d'équation*

$$k(x-a)(x-b)(y^2-ry+t) = (y-a_1)(y-b_1)(x^2-sx+p). \tag{4.1}$$

Il existe un point Ω K-rationnel de Γ et une transformation birationnelle f définie sur K telle que $f(\Gamma)$ soit, en général, une courbe elliptique sur K d'élément neutre $f(\Omega)$. Cette courbe elliptique possède un point de torsion K-rationnel d'ordre 2 ainsi qu'un point K-rationnel. Si de plus les polynômes x^2-sx+p et y^2-ry+t se factorisent sous la forme $(x-c)(x-d)$ et $(y-c_1)(y-d_1)$ la courbe elliptique possède un autre point K'-rationnel où $K' = K(c,d,c_1,d_1)$. Enfin si les fractions rationnelles

$$h\,\frac{(x-a)(x-b)}{(x-c)(x-d)} - 1 \quad et \quad m\,\frac{(y-a_1)(y-b_1)}{(y-c_1)(y-d_1)} - 1$$

avec $h/m = k$ ont des numérateurs qui se factorisent sur K' en polynômes de degré 1 en x et en y alors ces courbes elliptiques ont trois points K'-rationnels généralement indépendants.

Par deux transformations homographiques en x et en y on se ramène à l'étude de

$$\frac{U}{U^2-sU+p} = k\,\frac{V}{V^2-rV+t}.$$

On pose $U = X(X-k^2p)/(kY)$, $V = Y/(X-k^2p)$, ce qui définit une application birationnelle d'inverse $X = UVk, Y = Vk(VU-kp)$. On obtient alors le modèle de Weierstrass

$$Y^2 + YX(-r+sk) = X(X-t)(X-k^2p).$$

Si le discriminant n'est pas nul on obtient une courbe elliptique ; le point $p_1 = (0,0)$ est de 2-torsion et le point $p_2 = (t,0)$ est en général d'ordre infini sur K. Le point $p_3 = (k^2p, 0)$ vérifie $p_1 + p_2 + p_3 = 0$. Si les dénominateurs $U^2 - sU + p$ et $V^2 - rV + t$ se factorisent en $(U-m)(U-n)$ et $(V-m_1)(V-n_1)$, la courbe en X, Y se factorise aussi sous la forme

$$(Y + X(mk - n_1))(Y + X(kn - m_1)) = X(X - kmm_1)(X - knn_1)$$

et possède les points K'-rationnels

$$\begin{aligned} q_2 &= (kmm_1, -mm_1k(km - n_1)), & -q_2 &= (kmm_1, -mm_1k(kn - m_1)),\\ q_3 &= (knn_1, -nn_1k(kn - m_1)), & -q_3 &= (knn_1, -nn_1k(km - n_1)). \end{aligned}$$

On remarque que q_3, q_2 et p_1 sont alignés, donc $p_1 + q_2 + q_3 = 0$.

S'il existe des factorisations de $h\frac{(x-a)(x-b)}{(x-c)(x-d)} - 1$ et $m\frac{(y-a_1)(y-b_1)}{(y-c_1)(y-d_1)} - 1$ alors on obtient 4 points supplémentaires, ce qui compte tenu des relations évidentes entre les points augmente le rang de 1 au maximum.

Nous regrouperons les résultats obtenus dans le tableau 2. Pour chaque courbe $d_i(x) = d_j(y)$ nous donnons au moins une valeur de $d = d_i(x_1) = d_j(y_1)$ telle que la courbe E_d soit de rang ≥ 2, en vérifiant que les points de E_d donnés par le tableau 1 sont indépendants.

Tableau 2

$d_0 = d_1$	$y^2 = x^3 + x^2 - 9x$ rang 1	$d = 15/7$ conducteur $2 \cdot 3 \cdot 5 \cdot 7 \cdot 41 \cdot 127$
$d_0 = d_4$	$y^2 = (x-5)(x^2 + 6x - 379)$ rang 2	$d = 24/35$ conducteur $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 251$
$d_0 = d_5$	$y^2 = (x-22)(x^2 + 23x - 1638)$ rang 3	$d = 25/168$ conducteur $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 29 \cdot 139 \cdot 1847$
$d_5 = \frac{d_5 - 1}{d_5}$	$y^2 + xy = x^3 - 550315x + 156674225$ rang 3	$d = -7/125$ conducteur $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 1356907$
$d_1 = \frac{-1}{d_4 - 1}$	$y^2 = (x+12)(x^2 - 11x + 48)$ rang 1 et 4-torsion	$d = 21/40$ et $80/7$ rang 3
$d_1 = \frac{d_5 - 1}{d_5}$	$y^2 = (x+17)(x^2 - 16x + 87)$ rang 2	$d = 21/2$ conducteur $2 \cdot 3 \cdot 7 \cdot 19 \cdot 2633$
$d_4 = \frac{-1}{d_5 - 1}$	$y^2 + xy + y = x^3 - 716x + 182$ rang 2	$d = -12/5$ conducteur $2 \cdot 3 \cdot 5 \cdot 17 \cdot 8863$

Théorème 7. *Il existe une infinité de courbes elliptiques sur $\mathbb{Q}$ avec un point rationnel d'ordre 7 et un rang sur $\mathbb{Q}$ supérieur ou égal à 2. Ces courbes sont paramétrées par les points rationnels de courbes elliptiques.*

Notons L le corps des fonctions sur $\mathbb{Q}$ d'une courbe définie par $d_i = d_j$. Les résultats du tableau 2 montrent que $E_d(L)$ est de rang ≥ 2 sur L. Il résulte d'un résultat de Silverman [6] que les courbes spécialisées E_d, $d = d_i(z) = d_j(v)$, $(z, v) \in \mathbb{Q}^2$, sont de rang 2 sur $\mathbb{Q}$, sauf peut-être pour un nombre fini de valeurs de d.

4.2. *Deuxième méthode.* Si nous partons d'une famille $E_{d_i(t)}$ de courbes de rang 1 sur $\mathbb{Q}(t)$ de générateur P_t, considérons les points $P_t + iA = (x_i, y_i)$ où $7A = 0$. Cherchons une condition pour que les points d'ordonnées y_i soient rationnels. Pour deux de nos familles d_i nous sommes ramenés à chercher des points rationnels sur une courbe elliptique $\mathfrak{C}$ sur $\mathbb{Q}$ de rang positif.

Pour $E_{d_0(v)}$, on considère les points de même ordonnée que $P + 4A$, $-P + A$. La courbe elliptique $\mathfrak{C}$ correspondante est la courbe $y^2 = x^3 - 12x + 20$ de rang 1 sur $\mathbb{Q}$. On construit ainsi la courbe $E_{35/11}$ de petit conducteur $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 251$, ainsi que $E_{13/48}$ de conducteur $2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 239 \cdot 827$.

Il en est de même pour la courbe $E_{d_5(z)}$ avec le point $P + 2A$. L'une des plus petites valeurs obtenue pour d est $11 \cdot 17/(2^4 13)$.

5. Courbes de rang ≥ 3. Divers exemples de courbes de rang 3 ont été trouvés et se répartissent en plusieurs classes.

1) Le premier cas correspond à un point sur les courbes $d_i(v) = d_j(w)$, $d_i(v) = d_k(t)$. Chaque égalité définissant une courbe elliptique, ces cas correspondent à des points rationnels sur des courbes de genre > 1. Par exemple, soit

$$d = \frac{72}{275} = d_0\left(\frac{-11}{7}\right) = d_5(-28) = \frac{d_5 - 1}{d_5}\left(\frac{32}{23}\right)$$

et la courbe E_d

$$y^2 + \frac{31 \cdot 41 \cdot 71}{5^4 11^2} xy + \frac{2^6 3^4 7 \cdot 29}{5^6 11^3} y = x^3 + \frac{2^6 3^4 7 \cdot 29}{5^6 11^3} x^2$$

de conducteur $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 29 \cdot 41 \cdot 421 \cdot 2143$. Les points suivants sont indépendants :

$$P_{d_0} = \left(-\frac{2^2 7 \cdot 29}{5^4 11}, \frac{2^2 7^2 13 \cdot 19 \cdot 29^2}{5^8 11^3}\right),$$

$$P_{d_5} = \left(\frac{2^6 3^4 7 \cdot 29}{5^5 11^2 13^2}, -\frac{2^{14} 3^8 7^2 29^2}{5^9 11^4 13^3}\right),$$

$$P'_{d_5} = \left(-\frac{2^3 3^4 7 \cdot 23}{5^5 11^3}, \frac{2^3 3^7 7^2}{5^7 11^4}\right).$$

2) La valeur $d = -45/11$ est obtenue en spécialisant en $w = -5/3$, $t = 0$, et $z = 10$ les trois fractions rationnelles construites avec les méthodes

précédemment données, $d_6(w), d_8(t) = -\frac{3(t+3)(2t+5)}{(t+1)(t^2+6t+11)}$ et $(d_5 - 1)/d_5(z)$. Les points

$$P_8 = \left(\frac{3(t+2)(2t+5)^2(t+4)}{(t^2+6t+11)^2(t+1)^2}, \frac{18(t+4)^2(t+2)(2t+5)^3}{(t^2+6t+11)^3(t+1)^4}\right),$$
$$P_5 = \left(\frac{6(z-1)z^2(2z+1)(z-2)}{(z-4)(z+1)^2(z+2)^2}, \frac{36z^4(z-1)(2z+1)^2(z-2)}{(z-4)^2(z+1)^3(z+2)^3}\right)$$

sont rationnels sur E_d. Le calcul du régulateur montre qu'ils sont indépendants, ce qui donne la courbe et les points suivants :

$$y^2 - \frac{2399}{11^2}\, xy + \frac{2^3 3^4 5^2 7}{11^3}\, y = x^3 + \frac{2^3 3^4 5^2 7}{11^3}\, x^2,$$
$$P_6 = \left(\frac{2\cdot 3\cdot 7}{11}, -\frac{2^2 3^2 7^2 31}{11^3}\right),$$
$$P_8 = \left(\frac{2^3 3\cdot 5^2}{11^2}, \frac{2^6 3^2 5^3}{11^3}\right),$$
$$P_5 = \left(\frac{2\cdot 3\cdot 5^2 7}{11^2}, \frac{2\cdot 3\cdot 5^4 7^2}{11^3}\right).$$

3) La courbe elliptique de rang 3 de plus petit conducteur est sans doute obtenue avec $d = 21/40$ (voir [2]) ; son équation est

$$y^2 + \frac{1999}{2^6 5^2}\, xy + \frac{3^2 7^2 19}{2^9 5^3}\, y = x^3 + \frac{3^2 7^2 19}{2^9 5^3}\, x^2$$

et son conducteur vaut $2\cdot 3\cdot 5\cdot 7\cdot 19\cdot 239\cdot 419$. Elle possède les points rationnels indépendants

$$P_1 = \left(-\frac{3^2 7\cdot 19}{2^6 5^3}, \frac{3^4 7^2 19}{2^9 5^5}\right),$$
$$P_2 = \left(-\frac{3\cdot 7^2}{2^3 5^3}, \frac{3\cdot 7^4}{2^8 5^4}\right),$$
$$P_3 = \left(-\frac{3^3 19}{2^7 5^2}, \frac{3^6 19}{2^{13} 5^3}\right).$$

Les deux premiers points correspondent à

$$\frac{21}{40} = d_4(-6) \quad \text{et} \quad \frac{21}{40} = \frac{d_1(1/8) - 1}{d_1(1/8)}.$$

Le troisième point ne provient pas d'une famille d_n rencontrée dans nos calculs.

Remarque 8. Les calculs de rang ont été faits avec Maple et Apecs, Pari et mwrank (J. Cremona).

Références

[1] A. O. L. Atkin and F. Morain, *Finding suitable curves for the elliptic curve method of factorization*, Math. Comput. 60 (1993), 399–405.
[2] J. Buddenhagen, communication personnelle.
[3] A. Dujella, http://www.math.hr/˜duje/tors/tors.html.
[4] L. Kulesz, *Arithmétique des courbes algébriques de genre au moins deux*, thèse de doctorat, Univ. Paris 7, 1998.
[5] T. Shioda, *On the Mordell–Weil lattices*, Comment. Math. Univ. St. Paul. 39 (1990), 211–240.
[6] J. Silverman, *Heights and specialization map for families of abelian varieties*, J. Reine Angew. Math. 342 (1983), 555–565.
[7] J. Stienstra and F. Beukers, *On the Picard–Fuchs equation and the formal Brauer group of certain elliptic K3-surfaces*, Math. Ann. 271 (1985), 269–304.

Institut de Mathématiques
Université Paris VI
175 rue du Chevaleret
Paris 75013, France
E-mail: lecacheu@math.jussieu.fr

Reçu le 16.5.2001
et révisé le 26.8.2002 (4031)