ACTA ARITHMETICA
102.4 (2002)

Rang de courbes elliptiques liées à certaines extensions cycliques de degré 4 et 6

par

Odile Lecacheux (Paris)

1. Introduction. Dans un précédent article [4] nous avons considéré les deux familles de corps cycliques de degré 4 (resp. 6) notées K_4 (resp. K_6) engendrés par les racines des polynômes de $\mathbb{Z}[x]$

$$x^4 - tx^3 - 6x^2 + tx + 1, \quad \text{pour } K_4,$$
$$x^6 - tx^5 - 5\left(\frac{t+6}{2}\right) - 20x^3 + 5\left(\frac{t}{2}\right)x^2 + (t+6)x + 1, \quad \text{pour } K_6.$$

Nous avons montré comment le 5-rang pour K_4 et le 7-rang pour K_6 du groupe des classes d'idéaux était relié au rang sur $\mathbb{Q}$ des courbes elliptiques

$$E_n^5: \quad y^2 + (n-11)xy + (n-11)y = x^3 + \frac{1}{2}(3n-31)x^2 - x - \frac{n}{2} + \frac{13}{2},$$
$$E_n^7: \quad y^2 + (n+8)xy = x^3 - \frac{1}{4}(7n+47)x^2 + (5+n)x + 1$$

où $t = 2(n-11)$ pour K_4 et $t = 2(n+5)$ pour K_6.

Dans un premier article nous étudierons le rang sur $\mathbb{Q}$ de ces deux familles de courbes elliptiques et chercherons des sous-familles de rang > 1. Remarquons que ces deux familles de courbes elliptiques ont des points d'ordre infini, les points $(-3/4, 11/8)$ pour E_n^5 et $(0,1)$ pour E_n^7. Dans un deuxième article nous chercherons s'il existe une infinité de corps K_4 (resp. K_6) ayant un nombre de classes d'idéaux divisible par 5 (resp. 7) et construits par notre méthode.

Considérant n comme une variable nous noterons

$$E^N \to \mathbb{P}_n^1 \quad \text{avec} \quad N = 5 \text{ ou } 7$$

les surfaces elliptiques rationnelles de fibres génériques E_n^N ($N = 5$ ou 7) obtenues après résolution des singularités, où $\mathbb{P}_n^1$ désigne l'espace projectif avec un point générique n. Ces surfaces sont en fait des surfaces modulaires

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

de base les courbes modulaires de genre 0, $X_0(N)$. En effet, si on pose $n = N^{s/2}(\eta(N\tau)/\eta(\tau))^s$ avec $s(N-1)/24 = 1$, où η est la fonction éta de Dedekind, on obtient alors le développement habituel en $q = e^{2i\pi\tau}$ de l'invariant modulaire j.

Par spécialisation de $n \in \mathbb{Q}$ les extensions K_4 (resp. K_6) sont alors les corps engendrés par les points d'ordre 5 (resp. 7) de E_n^5 (resp. de E_n^7) stable par $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Ces surfaces figurent dans les tables de [6] où on peut lire les types de fibres singulières I_5, I_1, III, III pour E^5 et I_7, I_1, II, II pour E^7. Notons aussi que les équations des surfaces figurent dans la table (p. 339) de [3].

Dans cet article nous commençons par construire un revêtement de degré 2 de $\mathbb{P}_n^1$

$$\mathbb{P}_b^1 \to \mathbb{P}_n^1,$$

et par changement de base, pour la surface E^5 nous obtenons alors une surface elliptique dont la fibre générique a un rang 3 sur $\mathbb{Q}(b)$. La surface S ainsi obtenue est une surface $K3$. Nous pouvons alors améliorer le rang en considérant une autre fibration elliptique de la surface S dont la fibre générique a un point d'ordre infini. Considérant les multiples de ce point on construit un deuxième revêtement

$$\mathbb{P}_t^1 \to \mathbb{P}_b^1.$$

Par changement de base, on obtient alors une surface elliptique dont la fibre générique a alors un rang ≥ 4 sur $\mathbb{Q}(t)$.

Un autre exemple de surface elliptique de fibre générique rang 4 est aussi donné. Une construction analogue est faite pour E^7.

Enfin par spécialisation nous obtenons, pour certaines valeurs de n, des courbes E_n^5 et E_n^7 de rang sur $\mathbb{Q}$ supérieur ou égal à 5.

2. Rang sur $\mathbb{C}(n)$ des courbes E_n^5. Nous ne traiterons que le cas des courbes E_n^5. On trouvera l'énoncé des résultats dans [5] pour E_n^7 ; la démonstration est de même type.

Théorème 1. *Le rang sur $\mathbb{C}(n)$ de E_n^5 est égal à 2.*

Le groupe de Mordell–Weil $E_n^5(\mathbb{C}(n))$ est engendré par les points conjugués $R = (i, -1+i)$ et $R' = (-i, -1-i)$.

Le groupe de Mordell–Weil $E_n^5(\mathbb{Q}(n))$ est engendré par

$$P = (x = -(n-11)/2, y = -(n-9)/2).$$

Considérerons la surface rationnelle E^5. Les sections $n = \infty$ déterminent les points $(x = -3/4, y = 11/8)$, $(i, -1+i)$, $(-i, -1-i)$ de E_n^5.

La formule suivante donnée dans [8] permet de calculer le rang de $E_n^5(\mathbb{C}(n))$:

$$\mathrm{NS}(E^5) = 2 + \mathrm{rang}(E_n^5(\mathbb{C}(n))) + \sum_p (m_p - 1)$$

où $\mathrm{NS}(E^5)$ est le rang de Néron–Séveri de la surface E^5, m_p le nombre de composantes de multiplicité 1 dans la fibre au-dessus de p du modèle de Néron de $E_n^5(\mathbb{C}(n))$.

Le genre géométrique de la surface elliptique E^5 est 0, le rang du groupe de Néron–Séveri est donc majoré par 10. Le discriminant de E_n^5 est égal à $n(n^2 - 22n + 125)^3 = n(n - 11 + 2i)^3(n - 11 - 2i)^3$. Le type des fibres singulières donne alors les valeurs de m_p ; ainsi $m_p = 1$ sauf pour $p = (n - 11 \pm 2i)$ et $p = \infty$; dans les deux premiers cas $m_p = 2$ et dans le troisième cas $m_p = 5$. On utilise, par exemple, l'algorithme donné dans [11] pour calculer les hauteurs de R, R' et $R + R'$. On peut aussi calculer la matrice d'intersection des deux points R et R' de la courbe vue comme surface elliptique sur $\mathbb{Q}$ ([9], [1]). La matrice d'intersection est alors égale à $\left(\begin{smallmatrix} 3/10 & -1/5 \\ -1/5 & 3/10 \end{smallmatrix}\right)$ et son déterminant $d = 1/20$. Comme d est non nul, les deux points R et R' sont indépendants et donc $\mathrm{rang}(E_n^5(\mathbb{C}(n))) \geq 2$. On en déduit, grâce à la formule précédente, que le rang de $E_n^5(\mathbb{C}(n))$ est égal à 2.

D'autre part on a la relation donnée dans [1] :

$$T^2 k^2 \Big/ \prod m_p = d$$

où $T = 1$ est l'ordre du groupe de torsion de $E_n^5(\mathbb{C}(n))$ et k l'indice du groupe engendré par R et R' dans $E_n^5(\mathbb{C}(n))$. Il en résulte que R et R' engendrent le groupe $E_n^5(\mathbb{C}(n))$.

L'action de Galois permet de conclure. Enfin remarquons que $2P = (-3/4, 11/8)$.

3. Courbes elliptiques de rang 3 sur $\mathbb{Q}(b)$ ayant une 5-isogénie $\mathbb{Q}(b)$-rationnelle. Décrivons la méthode utilisée pour construire un polynôme $T(b)$ de degré 2 et à coefficients entiers tel que, si on considére le revêtement

$$\mathbb{P}_b^1 \to \mathbb{P}_n^1$$

défini par $n = T(b)$, la fibre générique de la surface elliptique obtenue par changement de base ait un rang sur $\mathbb{Q}(b) \geq 3$.

Ordonnons en n l'équation de E_n^5 ; on a

$$(y(x+1) + (1 - 3x^2)/2)n + y^2 - 11xy - 11y - x^3 + \frac{31}{2}x^2 + x - \frac{13}{2} = 0.$$

On constate que le coefficient de n est indépendant de y si $x = -1$. Dans ce cas l'ordonnée y du point d'abscisse -1 vérifie $n = y^2 + 9$. Posant alors

$n = T(b) = b^2 + 9$, on est donc amené à considérer la surface elliptique S de fibre générique la courbe elliptique, notée E_b, d'équation

$$y^2 + (b^2-2)(1+x)y = x^3 + \left(\frac{3}{2}b^2 - 2\right)x^2 - x - \frac{1}{2}b^2 + 2.$$

En outre les points $(1 \pm 2b, 4 \pm 3b)$ sont sur $E_b(\mathbb{Q}(b))$.

Spécialisant pour quelques valeurs de $b \in \mathbb{Q}$, on calcule la matrice des hauteurs des trois points $(1 \pm 2b, 4 \pm 3b)$ et $(-1, b)$ et l'on constate que ces points sont indépendants. Le rang sur $\mathbb{Q}(b)$ de E_b est donc ≥ 3. On peut aussi calculer la matrice d'intersection des trois points de la courbe vue comme surface elliptique sur $\mathbb{Q}$ ([9]). Le déterminant de cette matrice est égal à $2^4/5$.

On a alors le théorème

Théorème 2. *La courbe elliptique E_b sur $\mathbb{Q}(b)$*

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

d'invariant modulaire $j = -(b^4+8b^2-4)^3/(b^2+9)$, a un rang sur $\mathbb{Q}(b)$ supérieur ou égal à 3. Les points suivants sont $\mathbb{Q}(b)$-rationnels :

$$A = A_1 = (1 - b^2/2, -b^2/2), \quad 2A = (-3/4, 11/8),$$
$$A_2 = (-1, b),$$
$$A_3 = (1 + 2b, 4 + 3b),$$
$$\widetilde{A}_3 = (1 - 2b, 4 - 3b) = 2A - A_3,$$

et les points A_2, A_3 et $\widetilde{A}_3$ sont indépendants.

4. La surface $\widetilde{S}$. La surface projective d'équation

$$Y^2T^2 + (B^2 - 2T^2)(T+X)Y = X^3T + \left(\frac{3}{2}B^2 - 2T^2\right)X^2 - XT^3 - \frac{1}{2}B^2T^2 + 2T^4$$

possède les 6 points singuliers $(X=0, Y=1, B=0, T=0)$, $(0,0,1,0)$, $(i, -1+i, \sqrt{2-2i}, 1)$ et ses conjugués. La surface $\widetilde{S}$ est obtenue en éclatant ces 6 points et on voit facilement que se sont des points doubles ordinaires. Il résulte alors de [7] que $\widetilde{S}$ est une surface $K3$. La droite qui joint les deux points singuliers $(0,1,0,0)$, $(0,0,1,0)$ est contenue dans la surface projective. L'intersection des plans passant par cette droite et de la surface est formée de cette droite et d'une cubique. Ceci donne la fibration elliptique

$$S \to \mathbb{P}^1_x.$$

Théorème 3. *La surface S admet une autre fibration elliptique définie par*

$$(x, y, b) \mapsto x.$$

La fibre générique notée F_x a pour équation l'équation de Weierstrass

$$Y^2 = X^3 + (-4x^2 + 16x + 12)X^2 - 4(4x + 3)(x^2 + 1)^2 X.$$

Sur $\mathbb{Q}(x)$ la courbe F_x a un point d'ordre 2 et le point M d'ordre infini

$$M = (X = (x^2 + 1)^2, Y = (x^2 - 1)(x^2 + 1)^2).$$

L'équation de S est de degré 2 en y, on la transforme pour obtenir

$$w^2 = ab^4 + cb^2 + q^2$$

où a, c, q sont des polynômes en x. On utilise ensuite les transformations habituelles faisant passer de la forme quartique à la forme de Weierstrass. En résumé, le changement de variables

$$y = \frac{1}{2} \cdot \frac{3x^2 - 1}{1 + x} + \frac{(4x + 3)(x^2 + 1)^2}{(1 + x)X}, \qquad b = -\frac{1}{2} \cdot \frac{Y}{X(1 + x)}$$

d'inverse

$$X = 2\frac{(4x + 3)(x^2 + 1)^2}{-2(x + 1)y + 3x^2 - 1}, \qquad Y = \frac{-2bX}{1 + x}$$

transforme la surface S en la surface d'équation

$$Y^2 = X^3 + (-4x^2 + 16x + 12)X^2 - 4(4x + 3)(x^2 + 1)^2 X.$$

La fibre générique a pour discriminant

$$16384(x^2 - 2x + 3)(4x + 3)^2(x + 1)^3(x^2 + 1)^4.$$

Comme dans le paragraphe précédent, l'étude des fibres singulières permet de montrer que le rang du groupe de Néron–Séveri est supérieur à 19 ; il ne peut être égal à 20 car, dans ce cas, la monodromie serait finie [10].

5. Courbes de rang 4. Partant de la surface elliptique $S \to \mathbb{P}^1_b$ on construit, par changement de base, deux autres surfaces elliptiques

$$S_1 \to \mathbb{P}^1_t, \qquad S_2 \to \mathbb{P}^1_w$$

dont les fibres génériques sont de rang ≥ 4 sur $\mathbb{Q}(t)$ (resp. $\mathbb{Q}(w)$).

5.1. *Première famille*

Théorème 4. *La courbe elliptique E_t*

$$\begin{aligned} y^2 + \left(\frac{1}{4}\left(\frac{t^5 + t^4 - 8t^2 - 4}{(t^3 + t^2 + t + 2)t}\right)^2 - 2\right)(1 + x)y \\ = x^3 + \left(\frac{3}{8}\left(\frac{t^5 + t^4 - 8t^2 - 4}{(t^3 + t^2 + t + 2)t}\right)^2 - 2\right)x^2 - x \\ - \frac{1}{8} \cdot \frac{(t^5 - 3t^4 - 4t^3 - 12t^2 - 8t - 4)(t^5 + 5t^4 + 4t^3 - 4t^2 + 8t - 4)}{(t^3 + t^2 + t + 2)^2 t^2} \end{aligned}$$

possède quatre points $\mathbb{Q}(t)$-rationnels indépendants d'abscisses

$$-\frac{1}{8}\cdot\frac{t^{10}+2t^9-7t^8-32t^7-40t^6-56t^5+16t^4-32t^3+32t^2+16}{(t^3+t^2+t+2)^2t^2},$$
$$-1,$$
$$\frac{t^5+2t^4+t^3-7t^2+2t-4}{(t^3+t^2+t+2)t},$$
$$1+2t.$$

Reprenons la surface elliptique $S\to\mathbb{P}^1_x$ et considèrons sur la fibre F_x le point $2M$. Le point de S correspondant vérifie

$$b=\frac{x^5-3x^4+2x^3-62x^2+125x-191}{4(x-1)(x^3-x^2+3x+13)}.$$

Posons $x=1+2t$ pour simplifier les expressions, on obtient alors le théorème ; l'indépendance étant montrée en spécialisant avec $t=-1/2$, soit $b=191/52$, et en calculant la matrice des hauteurs.

Remarquons que pour cette valeur de t le signe de l'équation fonctionnelle est égal à -1, ce qui, conjecturalement, montre que le rang sur $\mathbb{Q}$ de la courbe elliptique $E_{t=-1/2}$ est ≥ 5.

On peut construire d'autres familles en considérant les points kM. Nous n'avons pas trouvé d'exemples plus simples que celui du théorème.

5.2. *Deuxième famille.* Soit E'_n la courbe quotient de E_n par le sous-groupe $\mathbb{Q}(n)$-rationnel d'ordre 5. Les résultats de [4] donnent

$$\begin{aligned}E'_n\colon\quad & y^2+(n-11)xy+(n-11)y\\ &=x^3+\left(\frac{3}{2}n-\frac{31}{2}\right)x^2+\left(-1+\frac{5}{2}(n^2-22n+125)(2n-26)\right)x\\ &\quad+\frac{13}{2}-\frac{1}{2}n+(n^2-22n+125)\left(\frac{1}{2}(n^2-22n+125)(2n-42)-5n+45\right).\end{aligned}$$

Considèrons le point de E'_n d'abscisse $x=-(n-11)/2$. Si $16n-375=5^2w^2$, ce point est dans $E'_n(\mathbb{Q}(w))$. Le point de E_n d'abscisse

$$-\frac{25w^8+1044w^6+25358w^4+258500w^2+890625}{(125+62w^2+5w^4)^2}$$

est alors $\mathbb{Q}(w)$-rationnel.

Si, de plus, on impose la condition $n=9+b^2$, alors b et w vérifient

$$16b^2-25w^2=231.$$

Paramétrisant la conique $16b^2-25w^2=231$ on obtient le théorème suivant.

THÉORÈME 5. *La courbe elliptique* $E_H = E_{n(H)}$ *où*

$$n(H) = \frac{1}{4} \cdot \frac{136H^4 - 260H^3 + 297H^2 - 260H + 136}{(H-1)^2(H+1)^2}$$

a un rang ≥ 4 *sur* $\mathbb{Q}(H)$. *Les points d'abscisse*

$$-(n-11)/2,$$
$$-1,$$
$$1 + 2b,$$
$$-\frac{25w^8 + 1044w^6 + 25358w^4 + 258500w^2 + 890625}{(125 + 62w^2 + 5w^4)^2}$$

sont indépendants, où

$$b = \frac{1}{2} \cdot \frac{10H^2 - 13H + 10}{(H-1)(H+1)} \quad \textit{et} \quad w = \frac{1}{5} \cdot \frac{13H^2 - 40H + 13}{(H-1)(H+1)}.$$

Remarques numériques. La construction des courbes E_t et E_H donne, par spécialisation avec t et $H \in \mathbb{Q}$ des courbes de rang ≥ 4 sur $\mathbb{Q}$, ayant une 5 isogénie rationnelle. Malheureusement les valeurs de n correspondantes ne sont pas entières en général. Quelques calculs numériques montrent que, pour des petites valeurs de b entières, les courbes E_b sont de rang ≥ 4, par exemple pour b pair compris entre 8 et 26, pour $b = 22$ le rang est 5. Utilisant le programme mwrank de J. Cremona [2], il est possible de construire explicitement un système générateur d'un sous-groupe d'indice fini du groupe de Mordell–Weil sur $\mathbb{Q}$. Certaines de ces courbes appartiennent à des familles infinies de courbes de rang 4. Par exemple, si on cherche une condition sur $b \in \mathbb{Q}$ pour que le point d'abscisse $x = 0$ de E_b soit rationnel on est amené à chercher des points rationnels sur une courbe elliptique sur $\mathbb{Q}$ de rang > 1 sur $\mathbb{Q}$. Il en est de même pour $x = -7/4$ et on trouve ainsi la valeur $b = 5$.

6. Courbes elliptiques de rang 3 sur $\mathbb{Q}(r)$ ayant une 7-isogénie $\mathbb{Q}(r)$-rationnelle. On considère la courbe E_n sous la forme $A(x,y)n + B(x,y)$. Il existe deux valeurs de x, à savoir $x_1, x_2 \in \mathbb{Q}$ telles que $B(x_1,y)$ et $B(x_2,y)$ soient les carrés d'un polynôme de degré 1 en y. La courbe d'équation $F(y,t) = A(x_1,y)B(x_2,t) - A(x_2,y)B(x_1,t) = 0$ est alors une cubique singulière. On peut alors paramétrer cette courbe ; il existe $y(r)$ et $t(r)$ deux fractions rationnelles telles que

$$n = \frac{-B(x_1,t(r))}{A(x_1,t(r))} = \frac{-B(x_2,y(r))}{A(x_2,y(r))}.$$

Les valeurs de x_1 et x_2 sont les racines du discriminant par rapport à la variable y du polynôme B soit -2 et $-1/4$. Il reste à vérifier par spécialisation que les points d'abscisse $-1, x_1, x_2$ ainsi obtenus sont indépendants. Après

calcul on obtient

$$n = \frac{-7}{4} \cdot \frac{(1+r^2)^2}{r(r^2-1)}.$$

On a alors le théorème suivant :

THÉORÈME 6. *La courbe elliptique* $E_r = E_{n(r)}$

$$y^2 - \frac{7r^4 - 32r^3 + 14r^2 + 32r + 7}{4r(r-1)(r+1)}xy = x^3 - \frac{49r^4 - 188r^3 + 98r^2 + 188r + 49}{16r(r-1)(r+1)}x^2 - \frac{-20r^3 + 20r + 7 + 14r^2 + 7r^4}{4r(r-1)(r+1)}x + 1$$

a un rang supérieur à 3 *sur* $\mathbb{Q}(r)$.

Les points $(0,1)$, $\left(-\frac{1}{4}, \frac{23r^2+16r+7}{16(1+r)r}\right)$, $\left(-2, \frac{9r^2-16r-7}{2(-1+r)r}\right)$ *sont indépendants.*

La démonstration du théorème est complète en spécialisant. Les valeurs suivantes de r donnent de plus le résultat suivant :

THÉORÈME 7. *Si* $r = -3$, *le rang de* E_{-3} *est supérieur à cinq.*
Les points d'abscisses $-2, 0, -1/4, -1/3, -20/3$ *sont indépendants.*

De même pour $r = 6$ et -6 le rang de E_r est supérieur à 5.

Références

[1] D. A. Cox and S. Zucker, *Intersection number of sections of elliptic surfaces*, Invent. Math. 53 (1979), 1–44.

[2] J. Cremona, http://www.maths.nottingham.ac.uk/personal/jec/ftp/progs/.

[3] S. Herfurtner, *Elliptic surfaces with four singular fibres*, Math. Ann. 291 (1991), 319–342.

[4] O. Lecacheux, *Courbes elliptiques et groupe des classes d'idéaux de corps quartiques*, C. R. Acad. Sci. Paris Sér. I Math. 316 (1993), 217–220.

[5] —, *Units in number fields and elliptic curves*, in: Advances in Number Theory (Kingston, ON, 1991), Oxford Univ. Press, 1993, 293–301.

[6] U. Persson, *Configuration of Kodaira fibers on rational elliptic surfaces*, Math. Z. 205 (1990), 1–47.

[7] C. Peters, J. Top and M. van der Vlugt, *The Hasse zeta function of a K*3 *surface related to the number of words of weight* 5 *in the Mela code*, J. Reine Angew. Math. 432 (1992), 151–176.

[8] T. Shioda, *On elliptic modular surfaces*, J. Math. Soc. Japan 24 (1972), 20–59.

[9] —, *On the Mordell–Weil lattices*, Comment. Math. Univ. St. Paul. 39 (1990), 211–240.

[10] T. Shioda and H. Inose, *On singular K*3 *surfaces*, in: Complex Analysis and Algebraic Geometry, W. L. Baily and T. Shioda (eds.), Iwanami Shoten and Cambridge Univ. Press, 1977, 119–136.

[11] J. H. Silvermann, *Computing height on elliptic curves*, Math. Comp. 51 (1988), 339–358.

Institut de Mathématiques
Université Paris 6
Boîte 247
4 Place Jussieu
75252 Paris Cedex 05, France
E-mail: lecacheu@math.jussieu.fr

Reçu le 26.1.2001
et révisé le 17.7.2001 (3959)