Une tordue de rang 4 d'une courbe elliptique de conducteur 15

By Emmanuel HALBERSTADT*) and Alain KRAUS**)

(Communicated by Shokichi IYANAGA, M. J. A., Feb. 12, 1998)

Abstract: For every elliptic curve over $\mathbf{Q}$ having conductor 15, the Mordell-Weil group over $\mathbf{Q}$ is finite. In this paper, for one of these curves, we exhibit a quadratic twist whose Mordell-Weil group has rank 4, as well as a basis of this group modulo torsion.

Introduction. Soit E une courbe elliptique sur $\mathbf{Q}$. Pour tout entier d libre de carrés, notons E_d la tordue de E par $\sqrt{d}$. Lorsque E est fixée et d varie, que peut-on dire du rang de E_d? D'après une conjecture de Honda (cf. [3]), le rang de E_d serait borné, i.e. majoré par une constante, dépendant de E mais pas de d. Par ailleurs on sait qu'il y a une infinité de d pour lesquels E_d est de rang 0. Considérons un tel d. Si le rang de E est grand, on a une variation importante du rang entre E et E_d, mais le conducteur de E_d est en général beaucoup plus gros que celui de E. Il est moins facile d'obtenir une variation du rang *dans le bon sens*. Plus précisément, supposons que le conducteur $N(E)$ de E soit minimum parmi les conducteurs des courbes elliptiques sur $\mathbf{Q}$ qui sont $\bar{\mathbf{Q}}$-isomorphes à E. On désire trouver des d pour lesquels, lorsqu'on passe de E à E_d, l'augmentation du rang soit aussi grande que possible.

Dans cet article, nous donnons, en partant d'une construction indiquée dans [6] (cf. ci-dessous), un exemple dans lequel E est de rang 0 et de conducteur 15, alors que E_d est de rang 4 et de conducteur: $N(E_d) = 7344061935$. On obtient aisément quatre points de $E_d(\mathbf{Q})$ indépendants (modulo la torsion), et une 2-descente montre que le rang de E_d est bien 4. Nous montrons en fait que les quatre points obtenus forment une base de $E_d(\mathbf{Q})$ modulo la torsion. A cet effet, vu la taille de $N(E_d)$, on ne peut pas utiliser directement les résultats de [5], mais on exploite le lien entre $E_d(\mathbf{Q})$ et $E(K)$, où $K = \mathbf{Q}(\sqrt{d})$.

Partons de la courbe elliptique E définie par l'équation minimale suivante:

(1) $y^2 + xy + y = x^3 + x^2 - 10x - 10.$

La courbe E est notée 15A1 dans les tables de [2]. Par ailleurs on sait que E est un modèle de la courbe modulaire $X_0(15)$ (cf. [4]), en particulier E est une courbe de Weil. Posons:

$$d = -22127 = -7 \times 29 \times 109.$$

Voici un modèle minimal de E_d:

(2) $y^2 + xy + y = x^3 + x^2 - 4906241376x + 61174463688624.$

Considérons les quatre points de $E_d(\mathbf{Q})$ suivants:

$$\begin{cases} P_1 = (2799, 6888000), \\ P_2 = (7566, 4944653), \\ P_3 = (-37269, 13884458), \\ P_4 = (-40076, 13928075). \end{cases}$$

Le résultat que nous avons en vue est alors le suivant:

Théorème 1. *Avec les notations ci-dessus, le groupe de Mordell-Weil $E_d(\mathbf{Q})$ est de rang 4. Plus précisément, les points P_1, P_2, P_3, P_4 forment une base de $E_d(\mathbf{Q})$ modulo la torsion.*

Principe de la démonstration. Expliquons d'abord l'origine de la courbe E. Soient b un rationnel distinct de 0, 1, -1 et $a = \left(\frac{b^2+1}{2b}\right)^2$. Considérons, comme dans [6], la courbe elliptique E d'équation

$$y^2 = x(x-1)(x-a),$$

et la tordue E_D de E par $\sqrt{D}$, où D est un certain élément de $\mathbf{Q}(T)$, dépendant de b (cf. [6, Th. 6, p. 960] pour la valeur de D). On dispose donc de trois points P_1, P_2, P_3 de $E_D(\mathbf{Q}(T))$ indépendants modulo la torsion (cf. *loc. cit.*). Pour presque tout rationnel t, lorsqu'on spécialise T en t, on obtient une courbe elliptique $E(t)$ sur $\mathbf{Q}$, sa tordue par $\sqrt{D(t)}$ et trois points $P_1(t)$, $P_2(t)$, $P_3(t)$ de cette tordue, rationnels sur $\mathbf{Q}$ et indépendants modulo la torsion [6, Lemme 1]. Supposons en outre que $E(t)$ soit de Weil et que le

*) Université Paris VI, Laboratoire de Mathématiques Fondamentales.

**) Université Paris VI, Institut de Mathématiques.

signe de l'équation fonctionnelle de sa fonction L de Hasse-Weil soit 1. Si l'on admet BSD (conjecture de Birch-Swinnerton-Dyer), la tordue en question sera de rang 4 au moins. Prenons la valeur de b la plus simple: $b = 2$, et soit $t = 25/9$. L'équation (1) est une équation minimale de la tordue de $E(t)$ par $\sqrt{-1}$, et le corps $K = \mathbf{Q}(\sqrt{d})$ est égal à $\mathbf{Q}(\sqrt{-D(t)})$. Ainsi l'équation (2) est une équation minimale de la tordue de $E(t)$ par $\sqrt{D(t)}$.

Le groupe $E(\mathbf{Q})$ est d'ordre 8, il est engendré par les points $B_1 = (-2, 3)$ et $B_2 = (-1, 0)$, d'ordre 4 et 2 respectivement, et $2B_1 = B_3 = (3, -2)$. En fait on a:

$$E_{\text{tors}}(K) = E(\mathbf{Q}) = < B_1, B_2 > \approx (\mathbf{Z}/4\mathbf{Z}) \times (\mathbf{Z}/2\mathbf{Z}).$$

Soit θ un isomorphisme de E_d sur E; θ est déterminé au signe près, et il est défini sur K Notons Q_i l'image de P_i par θ $(i = 1, \ldots, 4)$ et A_h l'image réciproque de B_h par θ $(h = 1, 2, 3)$. On a:

$$(E_d)_{\text{tors}}(\mathbf{Q}) = < A_2, A_3 > \approx (\mathbf{Z}/2\mathbf{Z})^2.$$

En effectuant une 2-descente, on obtient le Lemme ci-dessous:

Lemme 1. *Le groupe $E_d(\mathbf{Q})$ est de rang 4. Plus précisément, les classes de P_1, P_2, P_3, P_4, A_2 et A_3 forment une base de $E_d(\mathbf{Q})/2E_d(\mathbf{Q})$*

Pour démontrer le Théorème 1, appliquons un Lemme de Zagier [5, Prop. 7.2]. Considérons la hauteur de Néron-Tate $\hat{h}$ sur E_d et la hauteur naïve h sur $\mathbf{P}^1(\bar{\mathbf{Q}})$. Lorsque P décrit l'ensemble des combinaisons linéaires, à coefficients 0 ou 1, des six points figurant dans l'énoncé du Lemme 1, la valeur maximum de $\hat{h}(P)$ est $\hat{h}(P_2 - P_3) < 6.53421 = C_1$. Ainsi $E_d(\mathbf{Q})$ est engendré par l'ensemble des points P de $E_d(\mathbf{Q})$ tels que $\hat{h}(P) < C_1$. Appliquons ensuite le Th. 1.1 de [5], permettant de comparer $\hat{h}(P)$ et $h(x(P))$. Ce Théorème montre que $E_d(\mathbf{Q})$ est engendré par l'ensemble S_1 des points P de $E_d(\mathbf{Q})$ tels que $h(x(P)) < 30.345 = M_1$. Il suffit ainsi de vérifier que tout point P de S_1 appartient au sous-groupe de $E_d(\mathbf{Q})$ engendré par les six points ci-dessus. Le nombre de tests à effectuer est de l'ordre de: $2\exp(3M_1/2) \# 1.17 \times 10^{20}$. C'est évidemment impraticable.

L'idée est alors d'appliquer le Th. 1.1 de [5] non à E_d mais à E elle-même (sur le corps K), dont la hauteur est beaucoup plus petite. On a d'abord besoin d'un Lemme:

Lemme 2. a) *La restriction de θ à $E_d(\mathbf{Q})$ est un isomorphisme de $E_d(\mathbf{Q})$ sur un sous-groupe d'indice 2 de $E(K)$, ne contenant pas B_1.*

b) *Le groupe $E(K)$ est de rang 4. Plus précisément, les classes de Q_1, Q_2, Q_3, Q_4, B_1 et B_2 forment une base de $E(K)/2E(K)$.*

On démontre simultanément a) et b), en considérant l'application norme ν de $E(K)$ dans $E(\mathbf{Q})$: $P \mapsto P + P^\sigma$, où σ est l'automorphisme non trivial de K. On vérifie que ν a pour noyau $\theta(E_d(\mathbf{Q}))$ et pour image le sous-groupe engendré par B_3; le Lemme 2 en résulte. Revenant au Théorème, il suffit ensuite de montrer que le sous-groupe de $E(K)$ engendré par Q_1, Q_2, Q_3, Q_4, B_1 et B_2 est $E(K)$ lui-même. On applique cette fois les résultats de [5] à $E(K)$, et le nombre de tests à effectuer est de l'ordre de: 6.36×10^{13}. C'est encore peu praticable !

Considérons maintenant l'espace vectoriel $V = E(K) \otimes_{\mathbf{Z}} \mathbf{R}$, mumi du produit scalaire induit par la hauteur de Néron-Tate de E. On peut identifier $E(K)/E_{\text{tors}}(K)$ à un réseau Λ de V; les images de Q_1, Q_2, Q_3, Q_4 engendrent un sous-réseau Λ' de Λ. D'après le Lemme 2, l'indice m de Λ' dans Λ est (fini et) impair. Il s'agit de montrer que $\Lambda' = \Lambda$. Raisonnons par l'absurde, en supposant $m > 1$. On vérifie d'abord que m est distinct de 3 et 5, en considérant la réduction de E_d modulo des nombres premiers convenablement choisis. Ainsi $m \geq 7$. En suivant une suggestion de D. Bernardi, on applique alors le Lemme de Minkowski pour montrer que Λ contient un vecteur non nul appartenant à une boule de centre 0 et de rayon r bien choisi en fonction de m. Pour abréger, disons qu'on choisit r proportionnel (essentiellement) à $m^{-1/4}$, et c'est ce choix qui explique le fait qu'une nouvelle application des résultats de [5] donne la contradiction voulue, le nombre de tests à effectuer étant ici de l'ordre de : 2.05×10^7. Cette fois, la vérification devient possible, nous l'avons faite à l'aide du logiciel Pari. Bien entendu, il aurait été possible de vérifier par exemple l'inégalité $m \geq 11$, et de réduire ainsi encore le nombre de tests à effectuer. En réalité le gain eût été illusoire, à cause des calculs supplémentaires nécessaires pour montrer que m était distinct de 7. Par ailleurs on peut aussi utiliser l'algorithme LLL (cf.[1, Th. 2.6.2]) pour trouver dans Λ' un vecteur non nul de norme aussi petite que possible (ce vecteur cor-

respond au point Q_4).

Terminons par deux remarques.

1) Puisque nous disposons, grâce au Théorème 1, d'une base de $E_d(\mathbf{Q})$ modulo la torsion, on peut, si l'on admet BSD, et en particulier la finitude du groupe de Tate-Shafarevitch $Ш = Ш(E_d(\mathbf{Q}))$, en déduire l'ordre de $Ш$. On doit notamment calculer une valeur (approchée) de la dérivée quatrième de la fonction L de E_d au point 1 (cf. [2, pp. 30-32]). Nous avons obtenu, toujours a l'aide de Pari, la valeur suivante:

$$L^{(4)}(1) \sim 3549.821272687.$$

On trouve ainsi, pour l'ordre de $Ш$, la valeur 1, à 10^{-12} près. On voit directement, en tous cas, que le groupe $Ш[2]$ est trivial.

2) Dans la construction indiquée dans [6], le choix des paramètres b et t fait ici semble avoir été assez heureux. En effet, nous n'avons pas trouvé d'autre couple (b, t) conduisant à une tordue de rang 4, dont on puisse déterminer complètement le groupe de Mordell-Weil avec un temps de calcul comparable à celui qu'il nous a fallu ici.

References

[1] H. Cohen: A course in computational algebraic number theory. Springer-Verlag Berlin, p. 84 (1993).

[2] J. E. Cremona: Algorithms for modular elliptic curves. Cambridge Univ. Press Cambridge, Table 1 (1992).

[3] T. Honda: Isogenies, rational points and section points of group varieties. Jap. J. Math., **30**, 84–101 (1960).

[4] G. Ligozat: Courbes modulaires de genre 1. Mém. 43, Suppl. au Bull., **103**, no. 3, (1975).

[5] J. H. Silverman: The difference between the Weil height and the canonical height on elliptic curves. Math. of Comput., **55**, no. 192, 723–743 (1990).

[6] C. L. Stewart and J. Top: On ranks of twists of elliptic curves and power-free values of binary forms. J. of the A. M. S., **8**, no. 4, 943–973 (1995).