Astérisque

M. FLEXOR
J. OESTERLÉ

Sur les points de torsion des courbes elliptiques

Astérisque, tome 183 (1990), p. 25-36
<http://www.numdam.org/item?id=AST_1990__183__25_0>

Société Mathématique de France
Astérisque 183 (1990)

Sur les points de torsion des courbes elliptiques

par M. Flexor et J. Oesterlé [1]

1. Énoncé des résultats

Soit K un corps de nombres. Une courbe elliptique définie sur K ne possède qu'un nombre fini de points de torsion rationnels sur K. On a la conjecture classique suivante (dont une démonstration, qui malheureusement semble incomplète, a été publiée dans [1]) :

CONJECTURE 1. - *Il existe une constante* A(K) *telle que, pour toute courbe elliptique* E *définie sur* K, *on ait*

(1) $\quad \mathrm{Card}(E(K)_{\mathrm{tors}}) \leq A(K).$

Lorsque K est égal à $\mathbb{Q}$, la conjecture 1 est une conséquence du résultat plus précis suivant de Mazur ([5], th.8) : si E est une courbe elliptique définie sur $\mathbb{Q}$, le groupe $E(\mathbb{Q})_{\mathrm{tors}}$ est isomorphe à l'un des groupes

$$\mathbb{Z}/n\mathbb{Z} \qquad \text{avec } 1 \leq n \leq 10 \text{ ou } n = 12,$$

$$\text{ou} \quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z} \quad \text{avec } 1 \leq n \leq 4\,,$$

et par suite est d'ordre au plus 16.

Revenons au cas où K est un corps de nombres quelconque. Manin ([4]) démontre en 1969 que si p est un nombre premier, la courbe modulaire $X_0(p^n)$ n'a , pour n assez grand, qu'un nombre fini de points rationnels sur K (un cas particulier de la conjecture de Mordell, démontrée par Faltings en 1983) ; il en déduit que l'ordre de la composante p-primaire de $E(K)_{\mathrm{tors}}$ est majoré par une constante ne dépendant que de p et de K.

---

[1] Le second auteur remercie le Tata Institute of Fundamental Research pour un séjour à Bombay durant lequel a été rédigé cet article.

Étant donnée une courbe elliptique E définie sur K, nous noterons Δ_E l'idéal discrimant minimal de E et N_E l'idéal conducteur de E ; lorsque E est semi-stable (i.e. a en toute place finie de K bonne réduction ou réduction de type multiplicatif), N_E est le produit des idéaux premiers de l'anneau des entiers de K qui divisent Δ_E. Posons

$$\beta_E = \frac{\log(N_{K/\mathbb{Q}}(\Delta_E))}{\log(N_{K/\mathbb{Q}}(N_E))} \tag{2}$$

(avec par convention $\beta_E = 1$ lorsque $N_{K/\mathbb{Q}}(N_E)$ est égal à 1, c'est-à-dire lorsque E a partout bonne réduction).

Szpiro formule en 1982 la conjecture suivante (cf. [7], conj. 1) :

CONJECTURE 2. - *Il existe une constante* B(K) *telle que, pour toute courbe elliptique semi-stable* E *définie sur* K, *on ait*

$$\beta_E \leq B(K). \tag{3}$$

(Une forme optimiste de la conjecture 2 affirme que pour tout $\varepsilon > 0$ il n'existe, à K-isomorphisme près, qu'un nombre fini de courbes elliptiques définies sur K, semi-stables ou non, pour lesquelles on a $\beta_E \geq 6 + \varepsilon$).

Frey ([2]), le premier, a remarqué que la conjecture 2 implique la conjecture 1. Dans cette direction, il convient de citer la majoration, obtenue par voie analytique par Hindry et Silverman ([3], th.7.1) :

$$\mathrm{Card}(E(K)_{\mathrm{tors}}) \leq (20\ \beta_E)^{8[K:\mathbb{Q}]}\ 10^{\beta_E}. \tag{4}$$

Dans cet article, nous établissons par voie algébrique, en suivant les idées de Frey, d'autres majorations de l'ordre de $E(K)_{\mathrm{tors}}$, qui montrent que la conjecture 2 implique la conjecture 1.

Lorsque la courbe elliptique E (définie sur K) n'est pas semi-stable, ou bien lorsqu'elle a partout bonne réduction, l'ordre de $E(K)_{\mathrm{tors}}$ est majoré par une constante qui ne dépend que de K, comme il résulte des trois théorèmes suivants :

THÉORÈME 1. - *Soit* E *une courbe elliptique définie sur* K, *qui a mauvaise réduction de type additif en au moins deux places finies de* K, *de caractéristiques résiduelles distinctes. On a*

$$\mathrm{Card}(E(K)_{\mathrm{tors}}) \leq 12. \tag{5}$$

Remarque 1. - L'inégalité (5) est optimale : ainsi par exemple la courbe elliptique E d'équation $y^2 - 2y = x^3$ a mauvaise réduction de type additif aux places de $K = \mathbb{Q}(\sqrt{-3})$ de caractéristiques résiduelles 2 et 3, et le groupe $E(K)_{tors}$ est d'ordre 12.

THÉORÈME 2. - *Soit* E *une courbe elliptique définie sur* K, *qui a mauvaise réduction de type additif en au moins une place finie de* K. *On a*

(6) $$\mathrm{Card}(E(K)_{tors}) \leq 48[K:\mathbb{Q}].$$

Remarque 2. - Soient p un nombre premier et L une extension finie de $\mathbb{Q}_p$. Nous démontrerons que si une courbe elliptique E définie sur L a mauvaise réduction de type additif, on a $\mathrm{Card}(E(L)_{tors}) \leq 48e$, où e est l'indice de ramification de L sur $\mathbb{Q}_p$. Le théorème 2 s'en déduit aussitôt en prenant pour L le complété de K en une place finie en laquelle la courbe elliptique a mauvaise réduction de type additif.

THÉORÈME 3. - *Soit* E *une courbe elliptique définie sur* K *qui a partout bonne réduction. On a*

(7) $$\mathrm{Card}(E(K)_{tors}) \leq 5.2^{[K:\mathbb{Q}]}.$$

Remarque 3. - Seule l'hypothèse que E a bonne réduction en une place de K de caractéristique résiduelle 2 est utilisée dans la démonstration de l'inégalité (7). Il serait intéressant de savoir si, sous les hypothèses du théorème 3, le cardinal de $E(K)_{tors}$ est majoré par une fonction polynomiale de $[K:\mathbb{Q}]$.

Si E est une courbe elliptique définie sur K, posons

(8) $$\beta'_E = \sup_F \beta_F ,$$

où F parcourt l'ensemble des courbes elliptiques K-isogènes à E. (À K-isomorphisme près, il n'y a qu'un nombre fini de telles courbes, d'après les résultats de Serre exposés dans [6]). La conjecture 2 de Szpiro entraîne la conjecture 1 d'après les théorèmes 1, 2, 3 précédents et le théorème suivant :

THÉORÈME 4 (Frey). - *Soit* E *une courbe elliptique semi-stable définie sur* K, *qui a mauvaise réduction en au moins une place finie de* K. *On a*

(9) $$\mathrm{Card}(E(K)_{\mathrm{tors}}) \leq \beta_E^2.$$

2. Points de torsion des groupes formels

Soit L un corps complet pour une valuation discrète v, que l'on suppose normée : on a $v(L^\times) = \mathbb{Z}$. Notons A l'anneau de valuation de v et $\mathfrak{m}$ l'idéal maximal de A. Supposons que L soit de caractéristique 0 et que le corps résiduel $A/\mathfrak{m}$ soit de caractéristique $p > 0$. Enfin soit $e = v(p)$ l'indice de ramification absolu de L.

Rappelons qu'une loi de groupe formel (commutative à un paramètre) sur A est une série formelle $G \in A[[X,Y]]$ telle que :

a) $G(X,0) = X$ et $G(0,Y) = Y$;

b) $G(X,Y) = G(Y,X)$;

c) $G(X,G(Y,Z)) = G(G(X,Y),Z)$.

Soit G une telle loi de groupe formel. Pour chaque entier $r \geq 1$, l'ensemble $\mathfrak{m}^r$ muni de la loi de composition $(x,y) \longmapsto G(x,y)$ est un groupe commutatif, que l'on note $G(\mathfrak{m}^r)$. La multiplication par un entier $n \geq 0$ dans ce groupe est donnée par $x \longmapsto [n]_G(x)$, où $[n]_G = nX+...$ est une série formelle dans $A[[X]]$ que l'on définit par récurrence par

$$[0]_G = 0 \qquad [n+1]_G = G(X,[n]_G).$$

PROPOSITION 1. - *Soit* G *une loi de groupe formel (commutative à un paramètre) sur* A. *Le sous-groupe de torsion de* $G(\mathfrak{m})$ *est un* p*-groupe fini d'ordre* $\leq \frac{p}{p-1} e$.

Pour tout entier $r \geq 1$, le groupe $G(\mathfrak{m}^r)/G(\mathfrak{m}^{r+1})$ est annulé par p. Par ailleurs, si r est assez grand, le logarithme et l'exponentielle du groupe formel induisent des isomorphismes de groupes réciproques l'un de l'autre entre $G(\mathfrak{m}^r)$ et le groupe additif $\mathfrak{m}^r$, de sorte que $G(\mathfrak{m}^r)$ est sans torsion. Il en résulte le sous-groupe de torsion $G(\mathfrak{m})_{\mathrm{tors}}$ de $G(\mathfrak{m})$ est annulé par une puissance de p.

Soit H un sous-groupe fini non nul de $G(\mathfrak{m})$. Notons n le plus petit entier naturel tel que p^n annule H, et H' le sous-groupe de H formé des éléments