

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, 1990, tous droits réservés.

L'accès aux archives de la collection « Astérisque » (<http://smf4.emath.fr/Publications/Asterisque/>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques

<http://www.numdam.org/>

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*

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

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 $E(\mathbb{Q})_{\text{tors}}$ est isomorphe à l'un des groupes

$$\begin{aligned} & \mathbb{Z}/n\mathbb{Z} \quad \text{avec } 1 \leq n \leq 10 \text{ ou } n = 12, \\ \text{ou } & \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z} \quad \text{avec } 1 \leq n \leq 4, \end{aligned}$$

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 $E(K)_{\text{tors}}$ 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 discriminant 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

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

(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*

$$(3) \quad \beta_E \leq B(K).$$

(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) :

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

Dans cet article, nous établissons par voie algébrique, en suivant les idées de Frey, d'autres majorations de l'ordre de $E(K)_{\text{tors}}$, 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 $E(K)_{\text{tors}}$ 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*

$$(5) \quad \text{Card}(E(K)_{\text{tors}}) \leq 12.$$

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 $E(K)_{\text{tors}}$ 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*

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

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 $\text{Card}(E(L)_{\text{tors}}) \leq 48e$, 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*

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

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 $E(K)_{\text{tors}}$ est majoré par une fonction polynomiale de $[K:\mathbb{Q}]$.

Si E est une courbe elliptique définie sur K , posons

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

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*

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

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 :

$$a) \quad G(X, 0) = X \text{ et } G(0, Y) = Y ;$$

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

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

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 $(x, y) \mapsto G(x, y)$ 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 $x \mapsto [n]_G(x)$, où $[n]_G = nX + \dots$ est une série formelle dans $A[[X]]$ que l'on définit par récurrence par

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

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 annihilé 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 $G(\mathfrak{m})_{\text{tors}}$ de $G(\mathfrak{m})$ est annihilé 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

annulés par p^{n-1} . Le groupe H' est distinct de H ; son ordre est donc majoré par $\text{Card}(H)/p$. La série formelle $[p]_G$ s'écrit $Xu(X)$, où $u \in A[[X]]$ est une série formelle telle que $u(0) = p$. Posons $w = u \circ [p^{n-1}]_G$. On a $w(0) = p$ et

$$(10) \quad [p^n]_G = [p]_G \circ [p^{n-1}]_G = [p^{n-1}]_G w .$$

LEMME 1. - Soient $f \in A[[X]]$ une série formelle et α un élément de m tel que $f(\alpha) = 0$. Il existe une série formelle $g \in A[[X]]$ telle que $f(X) = (X-\alpha)g(X)$.

Ecrivons $f = \sum_{i=0}^{\infty} a_i X^i$. La série $\sum_{i=1}^{\infty} a_i (X^{i-1} + \alpha X^{i-2} + \dots + \alpha^{i-2} X + \alpha^{i-1})$ converge alors dans l'anneau $A[[X]]$, muni de la topologie J -adique, où J est l'idéal engendré par X et m . Soit g sa somme. On a $(X-\alpha)g(X) = \sum_{i=1}^{\infty} a_i (X^i - \alpha^i) = f(X) - f(\alpha) = f(X)$, d'où le lemme.

Pour tout $x \in H-H'$, on a $[p^n]_G(x) = 0$ et $[p^{n-1}]_G(x) \neq 0$, d'où $w(x) = 0$ en vertu de la formule (10). On déduit alors du lemme 1 que la série formelle w est multiple de $\prod_{x \in H-H'} (X-x)$ dans $A[[X]]$. En particulier le terme constant $w(0) = p$ est multiple de $\prod_{x \in H-H'} x$ dans A , et l'on a $e = v(p) \geq \text{Card}(H-H')$
 $\geq (1 - \frac{1}{p}) \text{Card}(H)$. Nous avons ainsi prouvé que l'on a $\text{Card}(H) \leq \frac{p}{p-1} e$ pour tout sous-groupe fini H de $G(m)$. La proposition 1 en résulte, puisque $G(m)_{\text{tors}}$ est réunion filtrante de tels sous-groupes.

3. Points de torsion d'une courbe elliptique définie sur un corps local

Soient L, A, v, m, p et e comme au n°2. Notons \tilde{L} le corps résiduel A/m et supposons-le parfait.

Soit E une courbe elliptique définie sur L . Notons \tilde{E} la fibre spéciale du modèle de Néron de E sur A , et \tilde{E}° la composante neutre de \tilde{E} . On dispose d'un homomorphisme de réduction $E(L) \rightarrow \tilde{E}(\tilde{L})$. Il est surjectif parce que le modèle Néron de E est lisse sur A et que l'anneau A est complet par hypothèse. Notons $E_1(L)$ le noyau de l'homomorphisme de réduction et $E_0(L)$ le groupe

des points de $E(L)$ dont la réduction appartient à $\tilde{E}^\circ(\tilde{L})$. On a ainsi une filtration $0 \subset E_1(L) \subset E_0(L) \subset E(L)$ de $E(L)$ et le groupe quotient $E_0(L)/E_1(L)$ est isomorphe à $\tilde{E}^\circ(\tilde{L})$.

PROPOSITION 2. - a) *Le sous-groupe de torsion de $E_1(L)$ est un p -groupe fini d'ordre $\leq \frac{p}{p-1} e$.*

b) *Lorsque E a mauvaise réduction de type additif, l'indice $[E(L) : E_0(L)]$ est majoré par 4.*

De la loi de groupe sur le modèle de Néron de E , on déduit par complétion formelle le long de la section nulle une loi de groupe formel G (commutative à un paramètre) sur A , et le groupe $E_1(L)$ est canoniquement isomorphe au groupe $G(m)$. L'assertion a) résulte ainsi de la proposition 1. L'indice $[E(L) : E_0(L)]$ est majoré par le nombre de composantes connexes géométriques de \tilde{E} , et, d'après la classification de Néron, ce nombre est au plus 4 lorsque E a mauvaise réduction de type additif. Cela prouve b).

COROLLAIRE. - *Supposons que le corps \tilde{L} soit fini et soit q son cardinal. Si la courbe elliptique E a bonne réduction, on a*

$$\text{Card}(E(L)_{\text{tors}}) \leq \frac{p}{p-1} e (q+1+[2\sqrt{q}]).$$

Si E a bonne réduction, \tilde{E} est une courbe elliptique sur \tilde{L} . On a alors

$$[E(L) : E_1(L)] = \text{Card}(\tilde{E}(\tilde{L})) \leq q + 1 + [2\sqrt{q}]$$

d'après les majorations de Hasse. Par ailleurs le groupe $E_1(L)_{\text{tors}}$ est d'ordre inférieur à $\frac{p}{p-1} e$ d'après la proposition 2, a), d'où le corollaire.

PROPOSITION 3. - *Supposons que la courbe elliptique E ait mauvaise réduction de type additif. Le groupe $E(L)_{\text{tors}}$ est alors fini. Son ordre est de la forme $p^n m$ avec $n \geq 0$ et $m \leq 4$. Il est majoré par $48e$.*

Quitte à remplacer L par la complétion d'une de ses extensions algébriques non ramifiées maximales, on se ramène au cas où le corps \tilde{L} est algébriquement clos. Il existe alors une plus petite extension finie L' de L sur laquelle E acquiert réduction semi-stable ([6], 5.6). C'est une extension galoisienne de L ; notons Φ son groupe de Galois. Soient A' la fermeture intégrale de A dans L' . Notons E' la courbe elliptique sur L' déduite de E par extension des scalaires, \underline{E} et \underline{E}' les modèles de Néron de E et de E' sur A et A' respectivement, \tilde{E} et \tilde{E}' leurs fibres spéciales. Remarquons que le corps résiduel \tilde{L} de A s'identifie canoniquement à celui de A' . En vertu de la propriété universelle des modèles de Néron, il existe un unique A' -morphisme $u : \underline{E} \otimes_A A' \rightarrow \underline{E}'$ qui induit l'identité $E \otimes_K K' \rightarrow E'$ sur les fibres génériques. Soit $\tilde{u} : \tilde{E} \rightarrow \tilde{E}'$ le morphisme déduit de u par passage aux fibres spéciales. La restriction de \tilde{u} à la composante neutre \tilde{E}° de \tilde{E} est nulle, car le groupe algébrique \tilde{E}° est isomorphe au groupe additif, alors que \tilde{E}'° est isomorphe au groupe multiplicatif ou est une courbe elliptique. Il en résulte que $E_0(L)$ est contenu dans $E'_1(L')$. D'après la prop. 2, a), $E'_1(L')_{\text{tors}}$ est un p -groupe fini et l'on a

$$(11) \quad \text{Card}(E'_1(L')_{\text{tors}}) \leq \frac{p}{p-1} e \text{Card}(\Phi).$$

(Noter que l'indice de ramification absolu de L' est $e\text{Card}(\Phi)$.) Grâce à la prop. 2, b), on en déduit que le groupe $E(L)_{\text{tors}}$ est fini, que son ordre s'écrit $p^n m$ avec $n \geq 0$, $m \leq 4$, et que l'on a

$$(12) \quad \text{Card}(E(L)_{\text{tors}}) \leq \frac{4p}{p-1} e \text{Card}(\Phi) \leq 8e\text{Card}(\Phi).$$

Lorsque l'ordre de Φ est majoré par 6, cela achève la démonstration.

Avant de traiter les autres cas, remarquons que Φ opère par transport de structure sur le schéma \underline{E}' ; cette opération n'est pas A' -linéaire, mais seulement semi-linéaire relativement à l'opération de Φ sur A' . On en déduit, parce que Φ opère trivialement sur le corps résiduel de A' , une opération de Φ sur le \tilde{L} -schéma \tilde{E}' , c'est-à-dire un homomorphisme $\Phi \rightarrow \text{Aut}_{\tilde{L}}(\tilde{E}')$. Cet homomorphisme est injectif ([6], 5.6). Supposons maintenant que l'ordre de Φ

soit strictement supérieur à 6 ; il en est alors de même de celui de $\text{Aut}_{\tilde{\mathcal{L}}}(\tilde{E}')$, et l'on est dans l'un des deux cas suivants (*loc. cit.*) :

a) On a $p = 2$, E' a bonne réduction, l'invariant modulaire de la courbe elliptique \tilde{E}' est 0, le groupe $\text{Aut}_{\tilde{\mathcal{L}}}(\tilde{E}')$ est d'ordre 24 et le groupe Φ est d'ordre 8 ou 24. Dans ce cas \tilde{E}' est isomorphe à la courbe elliptique d'équation $y^2 - y = x^3$ et l'image de Φ dans $\text{Aut}_{\tilde{\mathcal{L}}}(\tilde{E}')$ contient l'automorphisme

$$(x, y) \mapsto (x, y+1) \text{ de } \tilde{E}'.$$

b) On a $p = 3$, E' a bonne réduction, l'invariant modulaire de la courbe elliptique \tilde{E}' est 0, le groupe $\text{Aut}_{\tilde{\mathcal{L}}}(\tilde{E}')$ est d'ordre 12 et le groupe Φ également. Dans ce cas \tilde{E}' est isomorphe à la courbe elliptique d'équation $y^2 = x^3 - x$, l'homomorphisme $\Phi \rightarrow \text{Aut}_{\tilde{\mathcal{L}}}(\tilde{E}')$ est bijectif et $(x, y) \mapsto (x+1, y)$ est un automorphisme de \tilde{E}' .

Dans chacun des deux cas ci-dessus, on constate que le seul point de $\tilde{E}'(\tilde{\mathcal{L}})$ fixé par Φ est 0. Comme on a $\sigma \circ \tilde{u} = \tilde{u}$ pour tout $\sigma \in \Phi$, le morphisme $\tilde{u} : \tilde{E} \rightarrow \tilde{E}'$ est nul et le groupe $E(L)$ est contenu dans $E'_1(L)$. De (11), on déduit alors

$$\text{Card}(E(L)_{\text{tors}}) \leq \frac{p}{p-1} e \quad \text{Card}(\Phi) \leq 48e.$$

Cela termine la démonstration de la prop. 3.

PROPOSITION 4. - *Supposons que E ait mauvaise réduction de type multiplicatif. Soit P un point de torsion de $E(L)$. Notons n son ordre et m le plus petit entier ≥ 1 tel que mP appartienne à $E_0(L)$. Soit E' la courbe elliptique quotient de E par le sous-groupe engendré par P . Notons Δ et Δ' les discriminants de modèles minimaux de E et E' respectivement. Alors m divise $v(\Delta)$ et l'on a $v(\Delta') = nv(\Delta)/m^2$.*

Quitte à effectuer une extension finie non ramifiée du corps de base, on se ramène au cas où E' est une courbe de Tate $\mathbb{G}_m/q^{\mathbb{Z}}$, avec $q \in m$. On a

$v(\Delta) = v(q)$, $E(L) = L^\times/q\mathbb{Z}$ et $E_0(L) = A^\times q\mathbb{Z}/q\mathbb{Z}$. Soit x un élément de L^\times dont la classe modulo $q\mathbb{Z}$ soit le point P . Par définition, m est le plus petit entier ≥ 1 tel que x^m appartienne à $A^\times q\mathbb{Z}$, c'est-à-dire tel que $mv(x)$ soit multiple de $v(q) = v(\Delta)$. L'entier m divise n et $v(\Delta)$, et l'on a $x^m = \zeta q^r$, avec $\zeta \in A^\times$ et r un entier premier à m . Par définition de n , ζ est une racine primitive (n/m) -ième de l'unité. Choisissons des entiers a et b tels que $ar + bm = 1$ et posons $q' = (x^a q^b)^{n/m}$. On a les relations

$$(13) \quad q'^m = (\zeta^a q^{ar} q^{bm})^{n/m} = q^{n/m}$$

$$(14) \quad q'^r = (x^{ar} \zeta^{-b} x^{bm})^{n/m} = x^{n/m}.$$

Les morphismes $\lambda \mapsto \lambda^{n/m}$ et $\lambda \mapsto \lambda$ de \mathbb{G}_m dans \mathbb{G}_m définissent des isogénies

$$u : \mathbb{G}_m/q\mathbb{Z} \rightarrow \mathbb{G}_m/q^{(n/m)}\mathbb{Z} = \mathbb{G}_m/q'^m\mathbb{Z}$$

et $v : \mathbb{G}_m/q'^m\mathbb{Z} \rightarrow \mathbb{G}_m/q\mathbb{Z}$

de degrés n/m et m respectivement. L'isogénie $v \circ u$ est de degré n . On a $u(P) = u(xq\mathbb{Z}) = x^{n/m} q'^m\mathbb{Z} = q'^r q'^m\mathbb{Z}$ d'après (14), d'où $(v \circ u)(P) = 0$. Le noyau de $v \circ u$ est donc le sous-groupe cyclique d'ordre n de E engendré par P , et la courbe elliptique E' est isomorphe à la courbe de Tate $\mathbb{G}_m/q'\mathbb{Z}$. On a alors

$$v(\Delta') = v(q') = nv(q)/m^2 = nv(\Delta)/m^2$$

d'après (13), d'où la proposition.

COROLLAIRE. - *Supposons que E ait mauvaise réduction de type multiplicatif et soit H un sous-groupe fini de $E(L)$. Il existe des entiers naturels a et b tels que b divise a et que H soit isomorphe au groupe*

$\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$. Notons E' la courbe elliptique E/bH , et Δ et Δ' les discriminants de modèles minimaux de E et E' . On a

$$(15) \quad v(\Delta) + v(\Delta') \geq 2 \sqrt{\text{Card}(H)}.$$

Le groupe des points de torsion de $E(\bar{L})$, où \bar{L} est une clôture algébrique de L , est isomorphe à $(\mathbb{Q}/\mathbb{Z})^2$. D'après le théorème des diviseurs élémentaires, tout sous-groupe de $(\mathbb{Q}/\mathbb{Z})^2$ est isomorphe à un groupe de la forme

$\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$, où a, b sont des entiers naturels tels que b divise a . Cela prouve la première assertion. Pour démontrer la seconde, on se ramène, comme dans la démonstration de la prop. 4, au cas où E est une courbe de Tate $\mathbb{G}_m/q^{\mathbb{Z}}$.

Tous les points d'ordre b de $E(\bar{L})$ appartiennent à H , donc sont rationnels sur L . Il en résulte que q est une puissance b -ième dans L ; sa valuation $v(q) = v(\Delta)$ est multiple de b . Soit Q un point d'ordre a de H . Le groupe bH est le groupe cyclique d'ordre a/b engendré par le point $P = bQ$. Soit m le plus petit entier ≥ 1 tel que mP appartienne à $E_0(L)$. Comme $E_0(L)$ est d'indice $v(\Delta)$ dans $E(L)$, le point $(v(\Delta)/b)P = v(\Delta)Q$ appartient à $E_0(L)$, et m divise $v(\Delta)/b$. D'après la prop.4, on a $v(\Delta') = av(\Delta)/bm^2$, d'où

$$v(\Delta)+v(\Delta') = \frac{v(\Delta)}{bm} \left(bm + \frac{a}{m} \right) \geq bm + \frac{a}{m} \geq 2\sqrt{ab}.$$

Cela démontre le corollaire.

4. Démonstration des théorèmes 1 à 4

Dans ce numéro, K désigne un corps de nombres et E une courbe elliptique définie sur K .

a) Démonstration du théorème 1

Supposons que E ait mauvaise réduction de type additif en au moins deux places finies de K de caractéristiques résiduelles p et p' distinctes. Soient n et n' les plus grands diviseurs de l'ordre de $E(K)_{\text{tors}}$ premiers à p et à p' respectivement. Les entiers n et n' sont majorés par 4 d'après la prop.3 du n°3. Comme l'ordre de $E(K)_{\text{tors}}$ divise $\text{ppcm}(n, n')$, il divise 12. Cela démontre le théorème 1.

Remarque 4. - Si l'on a $p \geq 5$ ou $p' \geq 5$, il résulte de la démonstration précédente que l'on a $\text{Card}(E(K)_{\text{tors}}) \leq 4$.

b) Démonstration du théorème 2

D'après la remarque 2 du n°1, le théorème 2 résulte de la prop.3 du n°3.

c) *Démonstration du théorème 3*

Supposons que la courbe elliptique E ait bonne réduction en une place finie v de K de caractéristique résiduelle 2. Notons e l'indice de ramification et f le degré résiduel de cette place. On a $ef \leq [K:\mathbb{Q}]$, et d'après le corollaire de la prop.2 du n°3, appliqué en prenant pour L le complété de K en v , on a

$$\text{Card}(E(K)_{\text{tors}}) \leq 2e(2^{f+1} + [2^{1+(f/2)}]).$$

On a $1 \leq 2^{f-1}$ et $[2^{1+(f/2)}] \leq 2^f$, d'où

$$\text{Card}(E(K)_{\text{tors}}) \leq 5e2^f \leq 5[K:\mathbb{Q}]2^f/f.$$

Comme la suite $(2^n/n)_{n \geq 1}$ est croissante, $2^f/f$ est majoré par $2^{[K:\mathbb{Q}]}/[K:\mathbb{Q}]$ et $\text{Card}(E(K)_{\text{tors}})$ par $5 \cdot 2^{[K:\mathbb{Q}]}$, d'où le théorème 3.

d) *Démonstration du théorème 4*

Supposons que la courbe elliptique E soit semi-stable et n'ait pas partout bonne réduction. On voit comme dans la preuve du cor. de la prop.4 que le groupe fini $E(K)_{\text{tors}}$ est isomorphe à un groupe de la forme $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$, où a, b sont des entiers naturels tels que b divise a . Notons E' la courbe elliptique quotient de E par le sous-groupe fini $bE(K)_{\text{tors}}$. Elle est K -isogène à E , donc a même conducteur N_E que E . Par définition de la constante β_E^i (cf. formules (2) et (8) du n°1), on a

$$\log(N_{K/\mathbb{Q}}(\Delta_E)) \leq \beta_E^i \log(N_{K/\mathbb{Q}}(N_E))$$

$$\log(N_{K/\mathbb{Q}}(\Delta_{E'})) \leq \beta_E^i \log(N_{K/\mathbb{Q}}(N_E)).$$

Notons q_v le cardinal du corps résiduel d'une place finie v de K . En sommant les deux inégalités précédentes, on obtient

$$(16) \quad \sum_v (v(\Delta_E) + v(\Delta_{E'})) \log q_v \leq 2 \beta_E^i \sum_v \log q_v,$$

où les sommes sont étendues à l'ensemble des places finies de K en lesquelles E a mauvaise réduction. Pour une telle place, on a

$v(\Delta_E) + v(\Delta_{E'}) \geq 2\sqrt{\text{Card}(E(K)_{\text{tors}})}$ d'après le corollaire de la prop.4 du n°3.
La somme $\sum_v \log q_v$ étant non nulle par hypothèse, on déduit de (16) que l'on a
 $\sqrt{\text{Card}(E(K)_{\text{tors}})} \leq \beta_E$, d'où le théorème 4.

BIBLIOGRAPHIE

- [1] V.A. DEMIANENKO, *Sur la torsion des courbes elliptiques*, Izv. Akad. N. CCCP 35 (1971), 280-307.
- [2] G. FREY, *Links between elliptic curves and solutions of $A-B=C$* , Proceedings of the Journées Arithmétiques ULM, 1987.
- [3] M.HINDRY et J.H. SILVERMAN, *The canonical height and integral points on elliptic curves*, Invent. Math. 93 (1988), 419-450.
- [4] Ju. I. MANIN, *The p-torsion of elliptic curves is uniformly bounded*, Math. USSR Izvestija, vol.3 (1969).
- [5] B. MAZUR, *Modular curves and the Eisenstein ideal*, Publ. math. IHES 47 (1977), 33-186.
- [6] J.-P. SERRE, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. 15 (1972), 259-331.
- [7] L. SZPIRO, *Discriminant et conducteur des courbes elliptiques*, dans ce volume.

M. FLEXOR
Département de mathématiques
Bâtiment 425
Université de Paris Sud
91405 Orsay

J. OESTERLÉ
Université de Paris VI
Tour 45-46, 5ème étage
4, Place Jussieu
75005 Paris 5ème