# Borne sur les points de torsion d'une courbe elliptique

Fabien Pazuki

Février 2005

Version beta

# Table des matières

# Introduction

Soient $K$ un corps de nombres de degré $d$, $E$ une courbe elliptique définie sur $K$. On sait alors par le théorème de Mordell-Weil que $E(K)$, l'ensemble des points rationnels sur $K$, forme un groupe de type fini. L'étude de ce groupe se ramène donc d'un côté à l'étude de son rang en tant que $\mathbb{Z}$-module (et de ses générateurs éventuels) et d'un autre à celle de son sous-groupe de torsion. On s'intéresse dans ce qui suit à la partie torsion.

On sait qu'il existe une constante $C_d$ indépendante de la courbe telle que $\mathsf{card}(E(K)_{tors}) \leq C_d$, résultat qui dans sa généralité au regard du corps $K$ est dû à L.Merel (voir [5]). Cette constante est exponentielle en $d$ et pas entièrement explicite.

On présente dans ce texte la méthode de M.Hindry et J.Silverman permettant d'obtenir une borne effective au nombre de points de torsion d'une courbe elliptique, polynômiale en $d$, ceci au prix d'une hypothèse supplémentaire sur les courbes. Cette méthode est basée sur la théorie des hauteurs et illustre plus particuliérement l'intérêt de la décomposition de la hauteur canonique en hauteurs locales. L'exposé qui suit reprend pour l'essentiel la référence [3] en y incluant des définitions et des remarques en dernière partie.

On se concentre sur la preuve du théorème suivant :

**Théorème 1.** *Soit $K$ un corps de nombres, on note $d = [K : \mathbb{Q}]$. Soit $E$ une courbe elliptique définie sur $K$ possédant bonne réduction partout. On a alors* $\mathsf{card}(E(K)_{tors}) \leq 1977408 d \log d$.

# 1 Hauteurs locales

Nous allons nous servir de la hauteur canonique $\hat{h} : E(K) \to \mathbb{R}$ définie par Néron et Tate. C'est une forme quadratique, définie positive sur $E(K) \otimes \mathbb{R}$, vérifiant $\hat{h}(P) = 0 \Leftrightarrow P \in E(K)_{tors}$. De plus elle peut être décomposée en une somme de hauteurs locales de la manière suivante (avec $v$ place de $K$) :

$$\forall P \in E(K) - \{0\},\ \hat{h}(P) = \frac{1}{[K : \mathbb{Q}]} \sum_v [K_v : \mathbb{Q}_v] \lambda_v(P).$$

Les hauteurs locales $\lambda_v$ sont définies ainsi :

– Si $v$ est une place finie et qu'on se donne un modèle entier de Weierstrass avec discriminant $\Delta$ de la courbe $E$ on peut alors définir pour un point $P$ de bonne réduction en $v$ :

$$\lambda_v(P) = \frac{1}{2}\max\{v(x(P)^{-1}), 0\} + \frac{1}{12}v(\Delta).$$

– Si $v$ est une place archimédienne on a un isomorphisme du type $E(\bar{K}_v) \simeq \mathbb{C}/(\mathbb{Z}+\tau\mathbb{Z})$ pour un certain $\tau$ tel que $Im(\tau) > 0$. Si on pose de plus $q = \exp(2i\pi\tau)$ et $u = \exp(2i\pi z)$ on peut définir :

$$\lambda : \frac{\mathbb{C}}{\mathbb{Z}+\tau\mathbb{Z}} \setminus \{0\} \longrightarrow \mathbb{R}$$

par la formule suivante, lorsque $z = \alpha + \beta\tau$ avec $0 \leq \beta < 1$ :

$$\lambda(z,\tau) = -\frac{1}{2}B_2(\beta)\log|q| - \log|1-u| - \sum_{n\geq 1}\log|(1-q^n u)(1-q^n u^{-1})|.$$

$B_2(T)$ est le deuxième polynôme de Bernoulli défini par :

$$B_2(T) = \begin{cases} T^2 - T + \frac{1}{6} \\ \text{périodique en } T\text{, de période } 1 \end{cases}$$

– Enfin si $v$ est une place finie de mauvaise réduction on utilise la courbe de Tate $E_q$ : pour un corps $K$ $p$-adique il existe un élélement $q \in K^*$ tel que $|q|_v < 1$ et un isomorphisme $\phi : K^*/q^{\mathbb{Z}} \to E_q(K)$. On pose de plus $v(.) := -\log|.|_v$. On définit alors la hauteur locale de la même manière que pour les places archimédiennes, i.e. :

$$\lambda o \phi : E_q(K)\setminus\{0\} \longrightarrow \mathbb{R}$$

avec :

$$\lambda(\phi(u)) = \frac{1}{2}B_2\left(\frac{v(u)}{v(q)}\right)v(q) + v(1-u) + \sum_{n\geq 1} v((1-q^n u)(1-q^n u^{-1})).$$

(On ne se servira pas de cette dernière définition car les courbes qu'on considère dans la suite ont bonne réduction partout.)

## 2 Lemmes

Voici à présent les lemmes dont nous aurons besoin pour prouver le théorème 1.

**Lemme 2.1.** *Soit $M \geq 1$ un entier, soient $a$ et $b$ tels que $0 \leq a, b \leq \frac{1}{M}$, et soit $j$ l'invariant modulaire de la courbe $E$. On a alors :*

$$\lambda(a + b\tau, \tau) \geq \left(1 - \frac{23}{M}\right) \frac{\max\{\log |j(\tau)|, 1\}}{12}.$$

*Preuve :* La preuve de ce lemme est faite dans les articles [2] et [3]. Elle repose ur une estimation numérique des termes mis en jeu.

**Lemme 2.2.** *Soit $v$ une place finie de bonne réduction et $\Delta$ le discriminant de la courbe $E$. On a alors : $\lambda_v(P) \geq \frac{v(\Delta)}{12}$. En particulier : $\lambda_v(P) \geq 0$.*

*Preuve :* Il suffit de regarder l'expression, donnée plus haut, de la hauteur locale en une place finie de bonne réduction en $P$.

**Lemme 2.3.** *Soient $P_0, ..., P_N$ des points disctincts de $E(\mathbb{C}) = \mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z})$. On a alors :*

$$\sum_{0 \leq j \neq k \leq N} \lambda(P_j - P_k) \geq -\frac{1}{2}(N+1)\log(N+1) - \frac{N+1}{12}\max\{\log |j(\tau)|, 0\} - \frac{11}{3}(N+1).$$

*Preuve :* On trouve dans [4]p.218 la preuve du théorème suivant, à l'origine dû à N.Elkies : *Soit $v$ une place archimédienne pour $E(\bar{K}_v) \simeq \mathbb{C}/(\mathbb{Z} + \tau_v\mathbb{Z})$, $\tau_v = a_v + ib_v$ et $\Lambda_v^* = (1 - i\frac{a_v}{b_v})\mathbb{Z} + (\frac{i}{b_v})\mathbb{Z}$. Soit $g_v(.,.)$ la fonction de Green associée à la place $v$. On a alors l'estimation :*

$$\sum_{1 \leq i \neq j \leq N} g_v(P_i, P_j) \leq \frac{N \log N}{2} + N\left(\frac{1}{\pi b_v} + \frac{2 + b_v}{\sqrt{\pi b_v}} + \frac{1}{2\pi b_v}\sum_{\gamma \in \Lambda_v^*} \frac{\exp(-|\gamma|^2)}{|\gamma|^2}\right).$$

Or on a que $g_v(P_i, P_j) = -\lambda_v(P_i - P_j)$ et dans notre situation il y a $N + 1$ points. Il reste donc à étudier la constante $C_v$ en facteur du $N$ dans l'énoncé précédent. On a le développement en série de la fonction $j(\tau) = \frac{1}{q} + 744 + 196884q + ... = \frac{1}{q} + \sum_{n \geq 1} c(n)q^n$. Or $|q| = \exp(-2\pi b_v)$, et les majorations de [4]p.220 permettent de dire que $C_v \leq \frac{\max(\log |j(\tau)|, 0)}{12} + \frac{11}{3}$, ce qui achève la preuve du lemme.

# 3 Preuve du théorème

Le principe de la preuve est le suivant. On considère un grand nombre $N_0$ de points de la courbe $E$. On utilise les lemmes pour montrer que parmi ce grand nombre de points l'un au moins est nécessairement de hauteur plus grande qu'une constante $C_d$. On en déduit alors que le nombre de points de hauteur plus petite que cette constante $C_d$ est plus petit que $N_0$.

Commençons par prendre $M$ et $N$ deux entiers non nuls et soit $\varepsilon$ un ensemble de $M^2(N+1)$ points distincts de $E(K)$.

On choisit $v_0$ une place archimédienne telle que $|j|_{v_0} = \max_{v|\infty} |j|_v$. Dans $E(\overline{K}_{v_0})$ on considère des boîtes de taille $\frac{1}{M}$. Il y en a $M^2$. Par le principe des tiroirs, parmi les points de $\varepsilon$ on peut en trouver $N+1$ dans au moins une boîte : $P_0, ..., P_N$.

On applique le lemme 2.1 : $\lambda_{v_0}(P_j - P_k) \geq \left(1 - \frac{23}{M}\right) \frac{\max\{\log |j|_{v_0}, 1\}}{12}$.

Nous allons à présent chercher à minorer la hauteur des points de l'ensemble $\varepsilon$. On remarque pour commencer que l'on a l'inégalité $\hat{h}(P_j - P_k) \leq 4 \max \hat{h}(P_j)$. C'est ainsi qu'on va pouvoir utiliser le lemme 2.3. On va de plus se ramener à la seule étude des places archimédiennes grâce au lemme 2.2. On a donc les inégalités successives dans lesquelles on pose $J = \max\{\log |j|_{v_0}, 1\}$ :

$$4N(N+1) \max \hat{h}(P_j) \geq \sum_{0 \leq j \neq k \leq N} \hat{h}(P_j - P_k),$$

par le lemme 2.2 on a :

$$\sum_{0 \leq j \neq k \leq N} \hat{h}(P_j - P_k) \geq \frac{1}{d} \sum_{j \neq k} \left\{ d_{v_0} \lambda_{v_0}(P_j - P_k) + \sum_{\substack{v|\infty \\ v \neq v_0}} d_v \lambda_v(P_j - P_k) \right\}$$

or par le lemme 2.1 et le fait que $d_v \geq 1$ il vient :

$$d_{v_0} \lambda_{v_0}(P_j - P_k) \geq \left(1 - \frac{23}{M}\right) \frac{J}{12}$$

et par le lemme 2.3 pour chaque place $v|\infty$, $v \neq v_0$ :

$$\sum_{0 \leq j \neq k \leq N} d_v \lambda_v(P_j - P_k) \geq -\frac{1}{2}(N+1)\log(N+1) - \frac{(N+1)}{12} J - \frac{11}{3}(N+1)$$

donc

$$\sum_{0\leq j\neq k\leq N} \hat{h}(P_j - P_k) \geq \frac{N(N+1)}{d}\left(1-\frac{23}{M}\right)\frac{J}{12} - \frac{1}{2}(N+1)\log(N+1) - \frac{(N+1)}{12}J - \frac{11}{3}(N+1)$$

donc

$$4N\max\hat{h}(P_j) \geq \frac{N}{d}\left(1-\frac{23}{M}\right)\frac{J}{12} - \frac{1}{2}\log(N+1) - \frac{1}{12}J - \frac{11}{3}.$$

On utilise à présent $J \geq 1$ et on pose de plus $M = 24$ pour obtenir :

$$\max\hat{h}(P_j) \geq \frac{1}{1152d} - \frac{1}{8N}\log(N+1) - \frac{45}{48N}.$$

On pose enfin $N = 3432d\log d$, on vérifie alors que l'on a :

$$\max\hat{h}(P_j) \geq \frac{1}{164736d}.$$

On a donc montré la chose suivante : parmi $M^2(N+1) < 1977408d\log d$ points de $E(K)$ il y a au moins un point de hauteur minorée par $(164736d)^{-1}$. Les points de torsion étant de hauteur nulle, il y a par conséquent moins de $1977408d\log d$ points de torsion sur $E(K)$ : ceci est indépendant de la courbe, pourvu qu'elle ait bonne réduction partout.

# 4 Séries

On propose ici un petit énoncé faisant directement suite au résultat précédent. On appellera famille totale d'extensions une famille $\hat{K} = (K_n)_{n\geq 2}$ de corps de nombres tels que pour tout $n \geq 2$ on a $[K_n : \mathbb{Q}] = n$.

**Proposition 4.1.** *Soit $\hat{K}$ une famille totale d'extensions et soit $E$ une courbe elliptique définie sur $\hat{K}$ ayant bonne réduction partout. Alors la série :*

$$\Phi(\hat{K}, E) := \sum_d \frac{1}{Card(E(K_d)_{tors})}$$

*est une série divergente.*

*Preuve :* Il suffit de minorer le terme général et d'appliquer le critère de Bertrand.

## Références


[1] M.Hindry et J.Silverman. Diophantine geometry : an introduction, *Springer* (2000).

[2] M.Hindry et J.Silverman. Sur le nombre de points rationnels sur une courbe elliptique, *C.R.Acad.Sci. Paris* **t.329, Série I** (1999) p.97-100.

[3] M.Hindry et J.Silverman. The canonical height and integral points on elliptic curves, *Inventiones Mathematicae* **93** (1988) p.419-450.

[4] P.Hriljac. Splitting fields of principal homogeneous spaces, *Number Theory Seminar, Lect.Notes in Math.* **1240** *Springer-Verlag* (1987) p.214-229.

[5] L.Merel. Borne pour la torsion des courbes elliptiques sur les corps de nombres, *Invent.Math.* **124**(1996) p.437-449.

[6] J.H.Silverman. Advanced topics in the arithmetic of elliptic curves, *Springer-Verlag* (1994).