# Théorème de Dobrowolski-Laurent pour les extensions abéliennes sur une courbe elliptique à multiplication complexe

Nicolas Ratazzi

**Abstract :** Let $E/K$ be an elliptic curve with complex multiplication and let $K^{\mathrm{ab}}$ be the Abelian closure of $K$. We prove in this article that there exists a constant $c(E/K)$ such that : for all point $P \in E(\overline{K})\backslash E_{\mathrm{tors}}$, we have

$$\widehat{h}(P) \geq \frac{c(E/K)}{D}\left(\frac{\log\log 5D}{\log 2D}\right)^{13},$$

where $D = [K^{\mathrm{ab}}(P) : K^{\mathrm{ab}}]$. This result extends to the case of elliptic curves with complex multiplication the previous result of Amoroso-Zannier [2] on the analogous problem on the multiplicative group $\mathbb{G}_m$, and generalizes to the case of extensions of degree D the result of Baker [3] on the lower bound of the Néron-Tate height of the points defined over an Abelian extension of an elliptic curve with complex multiplication. This result also enables us to simplify the proof of a theorem of Viada [18].

Keywords : elliptic curves, normalised height, Lehmer's problem, Abelian extensions
2000 Mathematics Subject Classification : 11G50, 14G40, 14K22

## 1 Introduction

Soit $K$ un corps de nombres. En notant $\widehat{h}$ la hauteur de Néron-Tate sur une courbe elliptique $E/K$ et en notant $K^{\mathrm{ab}}$ la clôture abélienne de $K$, on montre dans cet article les deux résultats suivants :

**Théorème 1.1** *Si $E/K$ est une courbe elliptique à multiplication complexe, il existe une constante $c(E/K)$ strictement positive, telle que*

$$\forall P \in E(\overline{K})\backslash E_{\mathrm{tors}}, \quad \widehat{h}(P) \geq \frac{c(E/K)}{D}\left(\frac{\log\log 5D}{\log 2D}\right)^{13},$$

*Email address :* ratazzi@math.jussieu.fr

*où* $D = [K^{\mathrm{ab}}(P) : K^{\mathrm{ab}}]$.

**Théorème 1.2** *Soient* $c_0 > 0$ *et* $E/K$ *une courbe elliptique à multiplication complexe. Il existe une constante strictement positive* $c(E/K, c_0)$*, telle que : pour toute extension abélienne* $F/K$ *et pour tout point* $P \in E(\overline{K})\backslash E_{\mathrm{tors}}$ *vérifiant* $D = [F(P) : F]$*, si le nombre de nombres premiers qui se ramifient dans* $F$ *est borné par* $c_0 \left(\frac{\log 2D}{\log\log 5D}\right)^2$*, alors on a l'inégalité*

$$\widehat{h}(P) \geq \frac{c(E/K, c_0)}{D} \left(\frac{\log\log 5D}{\log 2D}\right)^3.$$

On voit qu'en imposant une contrainte sur l'étendue de la ramification dans l'extension abélienne (théorème 1.2), on obtient une généralisation d'un précédent résultat de Laurent [11] (cf. le théorème 1.4 plus loin). Dans le cas général (théorème 1.1), sans imposer aucune condition, on obtient une minoration optimale aux puissances de log près, avec un exposant légerement dégradé par rapport au cas classique : on a comme puissance de log un exposant 13 au lieu d'un exposant 3 ; toutefois cet exposant 13 est le même que dans le cas multiplicatif dû à Amoroso-Zannier [2] (cf. théorème 1.5 plus loin). Ce théorème 1.1, dans le cas des courbes elliptiques à multiplication complexe, généralise au cas $D$ quelconque un précédent résultat de Baker [3] (cf. théorème 1.6 plus loin). Nous donnons à la fin de l'introduction une application de notre théorème 1.1.

Ce type de problème remonte aux travaux de Lehmer dans les années 1930 : soit $x \in \mathbb{G}_m(\overline{\mathbb{Q}})\backslash\mu_\infty$ un nombre algébrique qui n'est pas une racine de l'unité. On sait par un théorème de Kronecker que sa hauteur logarithmique absolue $h(x)$ est strictement positive. En 1933 Lehmer énonce la célèbre conjecture

**Conjecture 1.1 (Problème de Lehmer)** *Il existe une constante* $c > 0$ *telle que*

$$\forall x \in \mathbb{G}_m(\overline{\mathbb{Q}})\backslash\mu_\infty, \quad h(x) \geq \frac{c}{D},$$

*où* $D = [\mathbb{Q}(x) : \mathbb{Q}]$.

Plus exactement, Lehmer se pose plutôt la question inverse : est-il possible de contredire cet énoncé ?

C'est en 1979 , avec le théorème de Dobrowolski [9], qu'est obtenu un résultat optimal à des puissances de log près, en direction de cette conjecture :

**Théorème 1.3 (Dobrowolski)** *Il existe une constante* $c > 0$ *telle que*

$$\forall x \in \mathbb{G}_m(\overline{\mathbb{Q}})\backslash\mu_\infty, \quad h(x) \geq \frac{c}{D} \left(\frac{\log\log 3D}{\log 2D}\right)^3,$$

*où* $D = [\mathbb{Q}(x) : \mathbb{Q}]$.

Peu de temps après, Laurent a étendu, dans son article [11], la conjecture de Lehmer aux courbes elliptiques sur un corps de nombres, en remplaçant la hauteur sur $\mathbb{G}_m$ par la hauteur de Néron-Tate et il a étendu le résultat de Dobrowolski au cas des courbes elliptiques $E/K$ à multiplication complexe.

**Théorème 1.4 (Laurent)** *Soit $E/K$ une courbe elliptique à multiplication complexe. Il existe une constante strictement positive $c(E/K)$ telle que*

$$\forall P \in E(\overline{K})\backslash E_{\text{tors}}, \quad \widehat{h}(P) \geq \frac{c(E/K)}{D}\left(\frac{\log\log 3D}{\log 2D}\right)^3,$$

*où $D = [K(P) : K]$.*

Dans les articles [1] et [2], Amoroso-Dvornicich et Amoroso-Zannier ont étendu le problème de Lehmer sur $\mathbb{G}_m$ au cas des extensions abéliennes relatives. Précisément, ils énoncent la conjecture et démontrent le théorème suivant :

**Conjecture 1.2 (Amoroso-Zannier)** *Soit $K$ un corps de nombres. Il existe une constante strictement positive $c(K)$, telle que*

$$\forall x \in \mathbb{G}_m(\overline{K})\backslash\mu_\infty, \quad h(x) \geq \frac{c(K)}{D},$$

*où $D = [K^{\text{ab}}(x) : K^{\text{ab}}]$.*

**Théorème 1.5 (Amoroso-Zannier)** *Soit $K$ un corps de nombres. Il existe une constante $c(K)$ strictement positive, telle que*

$$\forall x \in \mathbb{G}_m(\overline{K})\backslash\mu_\infty, \quad h(x) \geq \frac{c(K)}{D}\left(\frac{\log\log 5D}{\log 2D}\right)^{13},$$

*où $D = [K^{\text{ab}}(x) : K^{\text{ab}}]$.*

Ce théorème étend le résultat de Amoroso-Dvornicich qui traitait le cas où $x$ appartenait à une extension abélienne de $K$, *i.e.*, le cas $D = 1$. C'est précisément ce théorème, dans le cas $D = 1$, qui a été étendu aux courbes elliptiques à multiplication complexe, ou ayant un $j$-invariant non-entier, par Baker dans [3], puis par Silverman [15] dans le cas des courbes elliptiques sans multiplication complexe. Ainsi pour les courbes elliptiques, on a

**Théorème 1.6 (Baker-Silverman)** *Soit $E/K$ une courbe elliptique. Il existe une constante strictement positive $c(E/K)$ telle que*

$$\forall P \in E(K^{\text{ab}})\backslash E_{\text{tors}}, \quad \widehat{h}(P) \geq c(E/K).$$

Notons que Baker et Silverman ont récemment étendu ce résultat au cas des variétés abéliennes dans leur article [4].

L'objectif du présent article est d'étendre le résultat d'Amoroso-Zannier au cas des courbes elliptiques à multiplication complexe, généralisant ainsi le résultat de Baker au cas $D$ quelconque. Notons que le théorème 1.1 répond à une conjecture de David dans le cas des courbes elliptiques à multiplication complexe :

**Conjecture 1.3 (David)** *Soient $A/K$ une variété abélienne sur un corps de nombres et $\mathcal{L}$ un fibré en droites ample et symétrique sur $A$. Pour tout $\varepsilon > 0$, il existe une constante strictement positive $c(A/K, \mathcal{L})$ telle que pour tout point $P \in A(\overline{K})$ qui n'est pas de* $\mathrm{End}(A(\overline{K}))$*-torsion, on a*

$$\widehat{h}_{\mathcal{L}}(P) \geq \frac{c(A/K, \mathcal{L}, \varepsilon)}{D_{\mathrm{tors}}^{\frac{1}{g}+\varepsilon}},$$

*où $D_{\mathrm{tors}} = [K(A_{\mathrm{tors}}, P) : K(A_{\mathrm{tors}})]$.*

En effet, le théorème 1.1 étant vrai pour $D = [K^{\mathrm{ab}}(P) : K^{\mathrm{ab}}]$, il l'est en particulier pour $D = [F(P) : F]$ pour toute extension abélienne $F/K$. De plus, quitte à remplacer $K$ par une extension de degré borné en fonction de $E$, le résultat reste toujours vrai (on ne change que la constante $c(E/K)$). L'extension $H(E_{\mathrm{tors}})/H$ est abélienne pour $H = K(j)$ corps de classes de Hilbert de $E$, ce qui conclut.

Le théorème 1.1 rend naturel de généraliser la conjecture 1.2 aux courbes elliptiques :

**Conjecture 1.4** *Soit $E/K$ une courbe elliptique. Il existe une constante strictement positive $c(E/K)$, telle que*

$$\forall P \in E(\overline{K}) \backslash E_{\mathrm{tors}}, \quad \widehat{h}(P) \geq \frac{c(E/K)}{D},$$

*où $D = [K^{\mathrm{ab}}(P) : K^{\mathrm{ab}}]$.*

Le théorème 1.1 est une première étape en direction de cette conjecture 1.3, au moins dans le cas de multiplication complexe. On peut indiquer brièvement un des intérêts d'un tel résultat. Pour expliquer cela, on introduit quelques notations : on dit qu'une courbe (intègre) sur une variété abélienne $A$ est *transverse* si elle n'est contenue dans aucun translaté de sous-variété abélienne de $A$ différente de $A$. Si $X$ est un sous-schéma fermé intègre de $A$ et $r$ un entier, alors $Z_{x,0}^{(r)} \subset X(\overline{K})$ est l'ensemble des points pour lesquels il existe un sous-schéma en groupes $G$ de $A$ avec

$$\dim_P X \cap G \geq \max\{1, r - \mathrm{codim}\ G\}.$$

On dit qu'une variété abélienne simple $A$ est de *type* $(g, \delta)$, si elle est de dimension $g$ et si le rang de $\mathrm{End}(A) = 2g/\delta$. Enfin, on note

$$A^{[r]} = \bigcup_{\mathrm{codim}\, G \geq r} G(\overline{K}),$$

où $G$ est un sous-schéma en groupe de codimension indiquée. Dans son article [12], Rémond prouve :

**Théorème 1.7 (Rémond)** *Soit $A$ une variété abélienne sur $\overline{K}$. Nous choisissons une isogénie entre $A$ et un produit $A_1^{n_1} \times \cdots \times A_m^{n_m}$ où $m$ est un entier naturel et pour chaque indice $i$ avec $1 \leq i \leq m$ la variété abélienne $A_i$ est simple de type $(g_i, \delta_i)$ et $n_i \in \mathbb{N}^*$. Soient $X$ un sous-schéma fermé intègre de $A$ et $r, r'$ deux entiers tels que $0 \leq r \leq r' \leq \dim A$. Nous supposons que l'une des conditions suivantes est vérifiée.*
*$(C_1)$ La conjecture (1.3) est vraie.*
*$(C_2)$ La variété abélienne $A$ est à multiplication complexe et $r' > (1 + \sum_{i=1}^m g_i)(r-1)$.*
*$(C_3)$ On a l'inégalité*

$$r' > \sum_{i=1}^{m} g_i(n_i + \delta_i)\frac{r-1}{r}.$$

*Alors, pour toute hauteur $h$ associée à un fibré ample $\mathcal{L}$ sur $A$ et tout réel $H$, l'ensemble*

$$\left\{ P \in \left( X(\overline{K}) \backslash Z_{X,0}^{(r)} \right) \cap A^{[r']} \ / \ h(P) \leq H \right\}$$

*est fini. Si de plus $X$ est une courbe transverse et $r \geq 2$, alors $X(\overline{K}) \cap A^{[r']}$ est fini.*

Notons que notre théorème 1.1 permet déjà de simplifier la preuve du theorem 2. de Viada [18] suivant :

**Théorème 1.8 (Viada)** *Soient $E/K$ une courbe elliptique à multiplication complexe, $n$ un entier non nul et $C/K$ une courbe transverse dans $E^n$. Pour $r \geq 0$ on considère les ensembles*

$$S_r(C) := \bigcup_{\mathrm{codim}\, G \geq r} G \cap C(\overline{K})$$

*où l'union porte sur les sous-groupes algébriques $G$ de $E^n$ de codimension au moins $r$. Alors l'ensemble $S_2(C)$ est fini.*

La preuve de Viada est calquée sur celle de Bombieri, Masser et Zannier [5] dans le cas de $\mathbb{G}_m^n$. Elle utilise le fait que la hauteur des points de $S_1(C)$ est bornée. Il s'agit du Theorem 1. du même article de Viada qui résulte simplement des propriétés fonctorielles des hauteurs et du théorème du cube pour les variétés abéliennes. Ceci étant acquis on constate, en appliquant le théorème de Northcott, qu'il suffit alors de montrer que le degré des points

de $S_2(C)$ est borné. C'est la partie difficile de la preuve. Viada montre ceci en deux étapes : la première consiste à montrer la finitude de l'ensemble $S_3(C)$. La seconde étape consiste à montrer la finitude de $S_2(C)$ en utilisant un subtil argument cohomologique. Nous montrons ici comment éviter cet argument cohomologique en appliquant notre théorème 1.1. En fait l'utilisation de ce théorème 1.1 permet de ramener la seconde étape à la première. Nous expliquons ceci dans la dernière partie de cet article.

Dans la suite (dernière partie exceptée) on s'attache à prouver le théorème 1.1. On explique à la fin comment le théorème 1.2 s'obtient de la même façon. La preuve est une preuve classique de transcendance à deux exceptions près : on utilise un lemme de Siegel absolu et il y a en fait deux extrapolations selon que l'on est dans une situation avec beaucoup de ramification ou non. Ceci étant dit, dans le cas non-ramifié, la preuve suit le schéma initié par Dobrowolski, à savoir une extrapolation sur les transformés par le morphisme de Frobenius. Dans le cas ramifié, on suit la preuve du cas multiplicatif de [2] en utilisant encore des transformés par Frobenius. On utilise l'astuce de Laurent [11] consistant à dédoubler les variables pour permettre une plus grande liberté dans le choix des paramètres auxiliaires. La partie 2 consiste en des rappels sur la hauteur de Néron-Tate et sur les propriétés dont nous aurons besoin concernant les courbes elliptiques à multiplication complexe. La partie 3 consiste en une série de réductions en vue de prouver les théorèmes 1.1 et 1.2. La preuve proprement dite se trouve dans les parties 5, 6 et 7.

Dans la preuve on se ramène à travailler avec une extension abélienne $F/K$ finie et avec $D = [F(P) : F]$. Notons que l'hypothèse "$F/K$ est abélienne" sert de manière cruciale dans les deux étapes d'extrapolation : dans l'étape où il y a peu de premiers ayant un grand indice de ramification dans $F$, *i.e.* l'étape "quasi-classique", l'extrapolation se fait grâce au lemme 4.3 qui utilise de manière fondamentale l'hypothèse d'abélianité. Dans l'autre extrapolation, *i.e.* le cas complémentaire où beaucoup de premiers ont un grand indice de ramification dans $F$, l'hypothèse sert à fabriquer le groupe $H_p$ du lemme 4.2 : on utilise pour cela le théorème de Kronecker-Weber.

# 2 Hauteur et multiplication complexe

## 2.1 Hauteur

Soient $K$ un corps de nombres de degré d, $M_K$ l'ensemble des valeurs absolues (deux à deux non équivalentes) sur $K$, $M_K^0$ les valeurs absolues ultramétriques de $M_K$ normalisées par $|p|_v = p^{-1}$ pour toute place finie $v$ au-dessus du nombre premier $p$ et $M_K^\infty$ les valeurs absolues archimédiennes de $M_K$. On note $d_v = [K_v : \mathbb{Q}_p]$ le degré local et on définit la *hauteur (logarithmique absolue)* sur $\mathbb{P}^n(\overline{\mathbb{Q}})$ par

$$h(x_0 : \ldots : x_n) = \frac{1}{d} \sum_{v \in M_K} d_v \log \max_{0 \leq i \leq n} |x_i|_v.$$

Dans cette définition, la renormalisation par $\frac{1}{d}$ sert juste à faire en sorte que $h(x)$ soit indépendante du choix du corps $K$ contenant $x$. De plus par la formule du produit, la hauteur est aussi indépendante du choix d'un système de coordonnées projectives.

En plongeant $\mathbb{G}_m^n$ dans $\mathbb{P}^n$ par $(x_1, \ldots, x_n) \mapsto (1 : x_1, \ldots : x_n)$ ceci défini également la hauteur sur $\mathbb{G}_m^n$.

Dans la suite on utilisera également la hauteur $h_2$ définie sur $\mathbb{G}_m^n(\overline{\mathbb{Q}})$ par

$$h_2(x_1, \ldots, x_n) = \frac{1}{d}\left(\sum_{v \in M_K^0} d_v \log \max_{1 \leq i \leq n} |x_i|_v + \sum_{v \in M_K^\infty} d_v \log \sqrt{\sum_{1 \leq i \leq n} |x_i|_v^2}\right).$$

Soit $N$ un entier. On définit comme le fait Schmidt (voir [14]) la hauteur $h_2$ d'un sous-$\overline{\mathbb{Q}}$-espace vectoriel $S$ algébrique de dimension $d$ de $\overline{\mathbb{Q}}^{N+1}$ par :

$$h_2(S) = h_2(\mathbf{x}_1 \wedge \ldots \wedge \mathbf{x}_d),$$

où $\mathbf{x}_1, \ldots, \mathbf{x}_d$ est une base de $S$ sur un corps de nombres quelconque sur lequel $S$ est défini.

## 2.2 Hauteur de Néron-Tate

**Définition 2.1.** Si $E/K$ est une courbe elliptique donnée par une équation de Weierstrass, on définit la *hauteur* $h : E(\overline{K}) \to \mathbb{R}^+$ par $h(P) := h(x(P) : 1)$, où $h(x : y)$ est la hauteur logarithmique absolue sur $\mathbb{P}^1(\overline{K})$ définie précédemment.

Cette hauteur vérifie un certain nombre de propriétés. Nous indiquons les plus essentielles, qui nous serviront dans la suite. On renvoie par exemple au livre [10] Part B pour tout ce qui concerne les hauteurs.

**Proposition 2.1** *Sur une courbe elliptique $E/K$, la hauteur $h$ vérifie :*
*(i)* $\forall P \in E(\overline{K})$ $\quad h([m]P) = m^2 h(P) + O(1)$.
*(ii)* $\forall P, Q \in E(\overline{K})$ $\quad h(P+Q) + h(P-Q) = 2h(P) + 2h(Q) + O(1)$.
*(iii)* $\forall h > 0$ $\quad$ l'ensemble $\{P \in E(\overline{K})/\ h(P) \leq h\}$ est fini.
*Dans les affirmations précédentes, la constante $O(1)$ dépend de $E$ et $m$, mais pas des points $P$ et $Q$.*

À partir de cette hauteur, on peut en construire une plus jolie : la *hauteur de Néron-Tate*, notée $\widehat{h}$. La définition est la suivante :

$$\widehat{h}(P) = \lim_{n \to +\infty} \frac{h([2^n]P)}{4^n}.$$

Les propriétés classiques de cette hauteur sont résumées dans le théorème suivant.

**Théorème 2.1** *La hauteur canonique est une forme quadratique positive semi-définie sur $E(\overline{K})$, telle que*

$$\textit{d'une part } \forall P \in E(\overline{K})\ \widehat{h}(P) = h(P) + O(1),\ \textit{ et d'autre part, }\ \widehat{h}(P) = 0 \iff P \in E_{\text{tors}}.$$

## 2.3 Multiplication complexe

Soient $K$ un corps de nombres et $E/K$ une courbe elliptique à multiplication complexe par l'ordre d'un corps quadratique imaginaire $k$. On note $\mathcal{O}_K$ l'anneau d'entiers de $K$ et pour toute place finie $v$ de $K$ on note $k_v$ le corps résiduel associé à $v$. Quitte à faire une extension de corps ne dépendant que de $E/K$ et quitte à prendre une courbe elliptique isogène à la courbe de départ, on peut supposer que $K$ contient $k$ et que l'anneau des endomorphismes de $E/K$ est exactement $\mathcal{O}_k$, l'anneau des entiers de $k$. De plus, la courbe est à multiplication complexe, donc elle a bonne réduction potentielle. Ainsi, quitte à remplacer $K$ par une extension de degré borné (en fonction de $E/K$), on peut également supposer que $E/K$ a bonne réduction en toute place de $K$. On fait toutes ces hypothèses dans la suite.

On fixe un point $P \in E(\overline{K})\backslash E_{\text{tors}}$ et on note $D = [K^{\text{ab}}(P) : K^{\text{ab}}]$. On choisit alors une extension $F/K$ abélienne finie, telle que $D = [F(P) : F]$, ceci étant possible car $K^{\text{ab}}$ est le compositum des extensions abéliennes sur $K$.

Dans la suite, on fixe un modèle de Weierstrass de $E$ de la forme

$$Y^2 = X^3 + a_4X + a_6,$$

où $a_4$ et $a_6$ sont des éléments de $K$. Si $\wp$ est la fonction de Weierstrass associée, la courbe complexe $E(\mathbb{C})$ est paramétrée par $X = \wp(z)$ et $Y = \wp'(z)$. On rappelle que les points complexes d'une courbe elliptique sont paramétrés par l'isomorphisme de groupes de Lie complexes

$$\mathbb{C}/\Lambda \to E(\mathbb{C})\ :\ y^2 = x^3 + a_4x + a_6, \quad z \mapsto (\wp(z), \wp'(z))\,,$$

où $\wp(z)$ est la fonction de Weierstrass définie par la formule

$$\forall z \in \mathbb{C},\ \ \wp(z) = \frac{1}{z^2} + \sum_{\omega \in \Lambda^*} \left( \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right).$$

Soient $p$ un nombre premier et $v$ une place de $K$ au-dessus de $p$. On rappelle le théorème fondamental, dû à Deuring [8], concernant la multiplication complexe que l'on va utiliser ici. On renvoie par exemple à [16] Chapter II pour les démonstrations.

**Proposition 2.2** *Soit $E/\mathbb{C}$ une courbe elliptique à multiplication complexe par $\mathcal{O}_k$, anneau d'entiers d'un corps de nombres quadratique imaginaire. Il existe un unique isomorphisme*

$$[\cdot]\ :\ \mathcal{O}_k \to \text{End}(E)$$

*tel que pour toute différentielle invariante de $E$, $\omega \in \Omega_E$ et pour tout $\alpha \in \mathcal{O}_k$, on a*

$$[\alpha]^*\omega = \alpha\omega.$$

*De plus le degré de $[\alpha]$ est égal à $N_{\mathbb{Q}}^k(\alpha)$.*

**Théorème 2.2 (Deuring)** *Soit $E/K$ une courbe définie sur le corps de nombres $K$, à multiplication complexe par le corps quadratique imaginaire $k$. Soient $p$ un nombre premier et $v$ une place de $K$ au-dessus de $p$ telle que $E$ a bonne réduction en $v$. Alors il existe un unique $\alpha_v \in \mathcal{O}_k$ tel que $\widetilde{[\alpha_v]} = \mathrm{Frob}_{E_v}$ où $E_v$ est la réduction de $E$ sur $\mathbb{F}_v$ et où $\widetilde{[\alpha_v]}$ dénote la réduction de l'endomorphisme $[\alpha_v]$.*

De plus au cours de la preuve de ce théorème on montre que $q := N_{\mathbb{Q}}^K(v) = N_{\mathbb{Q}}^K(\alpha)$. Dans les deux lemmes qui suivent, conséquences du théorème précédent, on note $\pi$ une uniformisante dans $k$ de l'idéal maximal $\mathfrak{M}$ correspondant à la place $v$.

**Lemme 2.1** *Pour tout élément $\alpha \in \mathcal{O}_k$, il existe deux polynômes $R_\alpha$ et $S_\alpha$ premiers entre eux, à coefficients dans $\mathcal{O}_k$ tels que*

$$\wp(\alpha z) = \frac{R_\alpha(\wp(z))}{S_\alpha(\wp(z))}, \text{ et } \widetilde{S_\alpha} \neq 0.$$

*Ces deux polynômes sont définis à multiplication par une même unité de $\mathcal{O}_k$ près. Notamment quand $\alpha = \alpha_v$, on a*

$$R_\alpha(X) = uX^q + \pi V(X), \text{ et } S_\alpha(X) = u + \pi W(X),$$

*où $u$ est une unité $v$-adique de $\mathcal{O}_k$ et $V$ et $W$ sont deux polynômes à coefficients dans $\mathcal{O}_k$.*

**Lemme 2.2** *Pour tout $\alpha \in \mathcal{O}_k$, les polynômes $\widetilde{R_\alpha}$ et $\widetilde{S_\alpha}$ sont premiers entre eux.*

*Démonstration* : On trouvera par exemple une preuve de ces deux lemmes dans [11] lemmes 3.1 et 3.2 respectivement. □

Nous aurons également besoin d'un lemme sur les endomorphismes du groupe formel associé à la courbe elliptique $E$. Si $P$ est un point de la courbe de coordonnées affines $(X, Y)$, on note $t = -\frac{X}{Y}$ et on note $[\alpha_v]$ l'opérateur du groupe formel associé à l'endomorphisme $\alpha_v$.

**Lemme 2.3** *Il existe une série entière $\psi$, à coefficients dans $\mathcal{O}_{K_v}$ telle que*

$$[\alpha_v](t) = t^p + \pi_p\psi(t).$$

*Démonstration* : C'est le lemme 3.3 de [11]. □

# 3 Réductions

On fait maintenant les mêmes réductions que dans le cas multiplicatif dû à Amoroso-Zannier. On note $\mathcal{P}$ l'ensemble des nombres premiers qui se décomposent totalement dans $K$. Pour chacune des places $v$ de $K$ au-dessus d'un tel premier $p$, la complétion $v$-adique de $K$ est $K_v = \mathbb{Q}_p$. Pour $p \in \mathcal{P}$, on notera donc $K_p$ cette complétion dans la suite. Soient $p \in \mathcal{P}$ et $F/K$ une extension abélienne finie, on note $e_p(F)$ l'indice de ramification de $p$ dans $F$ et $F_v$ la complétion $v$-adique de $F$ en $v$. On a $K_p = \mathbb{Q}_p$, donc $F_v$ est une extension abélienne de $\mathbb{Q}_p$. Par le théorème de Kronecker-Weber local, elle est donc contenue dans une extension cyclotomique de $\mathbb{Q}_p$ que l'on notera $\mathbb{Q}_p(\zeta_m)$. On pose $m = m_p(F)$ le plus petit entier ayant cette propriété et on définit $\mathfrak{f}_p(F)$ le *conducteur local de $F$ en $p$* comme étant la plus grande puissance de $p$ divisant $m$ (il s'agit bien du conducteur local au sens de la théorie du corps de classes local). On pose

$$\mathfrak{f}(F) = \prod_{p \in \mathcal{P}} \mathfrak{f}_p(F),$$

le *conducteur de $F$* et on note que si $F' \subset F$ alors $\mathfrak{f}(F') \leq \mathfrak{f}(F)$.

Soit maintenant $P$ un point de $E(\overline{K})\backslash E_{\text{tors}}$ contredisant le théorème 1.1, de degré minimal, *i.e.*, tel que pour tout point $P' \in E(\overline{K})\backslash E_{\text{tors}}$ de degré $D' < D$ sur $K^{\text{ab}}$, on a

$$\widehat{h}(P') \geq \frac{c(E/K)}{D'} \left( \frac{\log\log 5D'}{\log 2D'} \right)^{13}.$$

**Lemme 3.1** *Pour démontrer le théorème 1.1, on peut supposer que pour tout point de torsion $T \in E_{\text{tors}}$ on a $[K^{\text{ab}}(P+T) : K^{\text{ab}}] \geq D$.*

*Démonstration* : La hauteur de Néron-Tate est invariante par translation par un point de torsion. Le résultat découle donc immédiatement de la définition du point $P$ et de la décroissance pour $t \geq 1$ de la fonction $t \mapsto \frac{c(E/K)}{t} \left( \frac{\log\log 5t}{\log 2t} \right)^{13}$. □

Soit $\mathcal{A}$ l'ensemble des extensions abéliennes finies $F/K$ telles qu'il existe un point de torsion $T \in E_{\text{tors}}$ tel que $[F(P+T) : F] \leq D$, *i.e.*, tel que $[F(P+T) : F] = D$ par le lemme précédent. Cet ensemble est non vide, puisque par définition de $K^{\text{ab}}$, on sait qu'il existe une extension abélienne finie $F/K$ telle que $[F(P) : F] = [K^{\text{ab}}(P) : K^{\text{ab}}] = D$. L'extension $F$ et le point $T = 0$ montrent donc que $\mathcal{A}$ est non vide. On définit alors l'entier

$$\mathfrak{f} = \min_{F \in \mathcal{A}} \mathfrak{f}(F).$$

**Lemme 3.2** *Avec les notations précédentes, pour démontrer le théorème 1.1, on peut supposer que*

$$D = [F(P) : F] \text{ où } F/K \text{ est une extension appartenant à } \mathcal{A}, \text{ contenue dans } K(P). \quad (1)$$

*On peut également supposer que*

$$\mathfrak{f}(F) = \mathfrak{f}. \quad (2)$$

*Enfin, on peut aussi supposer que*

$$\forall T \in E_{\text{tors}} \text{ tel que } K(P+T) \subset K(P), \text{ on a } K(P+T) = K(P). \quad (3)$$

*Démonstration* : Par définition de $K^{\text{ab}}$, il existe une extension abélienne finie $F/K$ telle que $D = [F(P) : F]$, donc appartenant à $\mathcal{A}$. On prend dans $\mathcal{A}$ une extension $F/K$ réalisant le min des $\mathfrak{f}(F)$, *i.e.*, réalisant $\mathfrak{f}$. Montrons qu'on peut supposer (3). Soit $T \in E_{\text{tors}}$ tel que $K(P+T) \subset K(P)$, alors, le point $T$ est défini sur le corps de nombres $K(P)$ car $P + T - P = T$. Si pour tous ces $T$, on a l'égalité $K(P+T) = K(P)$, il n'y a alors rien à montrer. Sinon, on note $\mathcal{T}$ l'ensemble fini des points de torsion tels que $K(P+T) \subsetneq K(P)$. Soient $T \in \mathcal{T}$ et $P_1 = P + T$. L'extension $K(P_1)$ est une sous-extension stricte de $K(P)$. On note $\mathcal{T}_1$ l'ensemble fini des points de torsion tels que $K(P_1+T) \subsetneq K(P_1)$. Si $\mathcal{T}_1$ est non vide, on choisit $T_1 \in \mathcal{T}_1$ et on pose $P_2 = P_1 + T_1$. L'extension $K(P_2)$ est une sous-extension stricte de $K(P_1)$. On construit ainsi une chaîne

$$K(P_n) \subsetneq \ldots \subsetneq K(P_1) \subsetneq K(P).$$

Donc pour $n$ assez grand, on sait que $K(P_{n+1}) = K(P_n)$, autrement dit que l'ensemble $\mathcal{T}_{n+1}$ correspondant est vide, c'est-à-dire que

$$\forall T \in E_{\text{tors}} \text{ tel que } K(P_n+T) \subset K(P_n), \text{ on a } K(P_n+T) = K(P_n).$$

Or par construction, on a $P_n = P + T_n$ où $T_n$ est un point de torsion de $E$, donc le lemme 3.1 précédent assure que $[F(P_n) : F] \geq D_n \geq D$. De plus on a

$$D_n = [K^{\text{ab}}(P_n) : K^{\text{ab}}] \leq [F(P_n) : F] \leq [F(P) : F] = D$$

car $K(P_n) \subset K(P)$, donc $D_n = D$. La hauteur de Néron-Tate étant invariante par translation par un point de torsion, on a également $\widehat{h}(P_n) = \widehat{h}(P)$. Enfin, quitte à remplacer $F$ par $F_1 = F \cap K(P_n)$, on voit que l'on peut aussi supposer l'hypothèse (1) vraie. La fonction $\mathfrak{f}(\cdot)$ étant croissante, l'hypothèse (2) est elle aussi vérifiée, ce qui conclut. □

Dans toute la suite on supposera désormais vraies les hypothèses (1), (2) et (3).

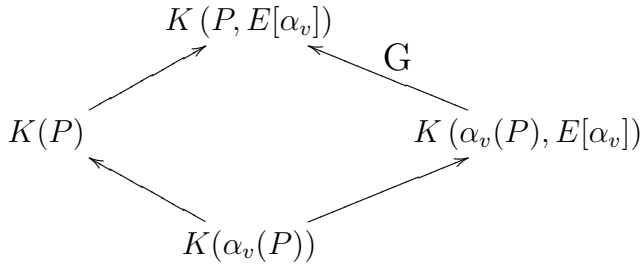
**Remarque 3.1** On note que, comme $K \subset F \subset K(P)$, on a aussi, $F(P) = K(P)$.

On peut maintenant énoncer les deux lemmes de réduction qui nous serviront dans la suite. Le premier est inspiré du Lemma 2.1. (ii) de [2], le second est plus classique dans le cadre du probème de Lehmer.

**Lemme 3.3** *Soient $p \in \mathcal{P}$ et $v$ une place de $K$ au-dessus de $p$, alors, pour démontrer le théorème 1.1, on peut supposer que*

$$\textit{soit } K(\alpha_v(P)) = K(P), \ \textit{ soit } [K(P) : K(\alpha_v(P))] = p.$$

*Démonstration* : On considère le diagramme




L'extension $K(P, E[\alpha_v])/K(\alpha_v(P), E[\alpha_v])$ est galoisienne d'ordre 1 ou $p$. En effet on a une injection naturelle $\mathrm{Gal}(\overline{K}/K(\alpha_v(P), E[\alpha_v])) \hookrightarrow E[\alpha_v]$ : les conjugués de $P$ par l'action de $\mathrm{Gal}(\overline{K}/K(\alpha_v(P), E[\alpha_v]))$ sont parmi les $P+T$, où $T \in E[\alpha_v]$ et $\alpha_v$ est une isogénie cyclique d'ordre $p$.

Si le groupe de Galois correspondant G est d'ordre $p$, alors l'extension $K(P)/K(\alpha_v(P))$ est également d'ordre $p$.

Si G est d'ordre 1, on va montrer qu'il existe $T \in E[\alpha_v]$ tel que $K(P+T) \subset K(\alpha_v(P))$. On regarde l'action de $\mathrm{Gal}(\overline{K}/K(\alpha_v(P))$ sur l'ensemble $\{P + T \ / \ T \in \ker[\alpha_v]\}$. Soit il y a une seule orbite, auquel cas $[K(\alpha_v(P)) : K(P)] = p$ ; soit l'orbite $\omega_P$, contenant $P$ est de cardinal $m$ strictement inférieur à $p$, donc premier à $p$. Dans ce cas, il existe $T' \in E[\alpha_v]$, tel que

$$\sum_{T \in \omega_P} (P + T) = mP + T'$$

est stable sous l'action de $\mathrm{Gal}(\overline{K}/K(\alpha_v(P))$. Par le théorème de Bézout, il existe deux entiers, $\lambda$ et $\mu$ tels que $\lambda m + \mu p = 1$. Par ailleurs, en notant $\alpha_v^\vee$ l'isogénie duale de $\alpha_v$, on a

$$K\,([p]P) = K\,(\alpha_v^\vee(\alpha_v(P))) \subset K(\alpha_v(P)).$$

Ainsi, on a les inclusions

$$K\,([\lambda]([m]P + T') + [\mu p]P)) = K\,(P + [\lambda]T') \subset K(\alpha_v(P)).$$

On a donc l'inclusion $K(P + [\lambda]T') \subset K(P)$. Par l'hypothèse (3) ceci entraîne que

$$K(P) = K(P + [\lambda]T') \subset K(\alpha_v(P)).$$

On en déduit que $K(P) = K(\alpha_v(P))$. □

**Lemme 3.4** *Pour tout $p \in \mathcal{P}$ sauf pour au plus $\frac{1}{2}\log D$ d'entre eux et pour toute place $v$ de $K$ au-dessus de $p$, on a*

$$F(P) = F(\alpha_v(P)).$$

*Démonstration* : C'est le lemme combinatoire classique de Dobrowolski [9] (dû à Laurent [11] lemme 4.2 dans le cas des courbes elliptiques). □

Notons que l'on pourrait éviter de recourir à ce lemme combinatoire, en faisant un raisonnement du même type que dans le lemme précédent, comme il est fait dans l'article d'Amoroso-Zannier [2]. Dans la suite on notera $\mathcal{P}^\star$ le sous-ensemble de $\mathcal{P}$ formé des premiers vérifiant le lemme 3.4 précédent.

# 4 Lemmes d'extrapolation

Dans la partie 6 on va faire deux extrapolations différentes, selon qu'il y a beaucoup de places de $F$ au-dessus de $\mathcal{P}^\star$ ayant un gros indice de ramification, ou non, tout ceci étant bien évidemment quantifié. On commence par les lemmes qui nous permettront d'extrapoler dans le cas où il y a beaucoup de ramification.

## 4.1 Lemme ramifié

**Lemme 4.1** *Soient $E/K$ une courbe elliptique à multiplication complexe, $v$ une place de bonne réduction ordinaire et $I_v$ le groupe d'inertie de* $\mathrm{Gal}(\overline{K_v}/K_v)$*. Alors, pour tout entier $n \geq 1$, on a l'isomorphisme de $I_v$-module $E[\alpha_v^n] \simeq \mu_{p^n}$.*

*Démonstration* : C'est le lemme 3.2 de [3]. □

Le lemme suivant est inspiré du lemme 3.2. de [2].

**Lemme 4.2** *Soient $p \in \mathcal{P}^\star$ et $e_p$ son indice de ramification dans $F$. Il existe un sous-groupe $H_p$ de* $\mathrm{Gal}(F/K)$ *d'ordre*

$$\mid H_p \mid \geq \min\{e_p, p\},$$

*tel que*

$$\mid x^p - \sigma x^p \mid_w \leq \frac{1}{p},$$

*pour tout $x \in \mathcal{O}_F$, tout $\sigma \in H_p$ et toute place $w$ de $F$ au-dessus de $p$. De plus, pour toute place $v$ de $K$ au-dessus de $p$ et pour toute extension $\tau \in \mathrm{Gal}(\overline{K}/K)$ de $\sigma \in H_p - \{\mathrm{Id}\}$, on a*

$$\tau(\alpha_v(P)) \neq \alpha_v(P).$$

*Démonstration* : La fabrication de $H_p$ et l'estimation de son cardinal se fait comme dans l'article de Amoroso-Zannier : soient $v$ une place de $F$ étendant $p$ et $F_v$ le complété $v$-adique de $F$. On pose $m := m_p(F)$ le plus petit entier $m$ tel que $F_v \subset \mathbb{Q}_p(\zeta_m)$. On décompose $m$ sous la forme $m = \mathfrak{f}_p \cdot n$ où $n$ est premier à $p$ et $\mathfrak{f}_p$ est le conducteur local de $F$ en $p$.

Si $p$ ne se ramifie pas dans $F$, alors $e_p = 1$ et $H_p = \{\mathrm{Id}\}$ convient. On peut donc supposer que $p$ se ramifie dans $F$, donc *a fortiori* dans $\mathbb{Q}(\zeta_m)$. Ainsi $p$ divise le conducteur

local $\mathfrak{f}_p$. On pose $\Sigma_p$ le groupe de Galois de l'extension $\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p(\zeta_{m/p})$. C'est un groupe cyclique d'ordre $p$ ou $p-1$ selon que $p^2$ divise $\mathfrak{f}_p$ ou non. Par la propriété de minimalité de $m$, $\Sigma_p$ ne fixe pas $F_v$, donc induit par restriction un sous-groupe non-trivial $H_v^*$ de $\mathrm{Gal}(F_v/K_p)$. On note que si $p^2$ ne divise pas $\mathfrak{f}_p$, alors l'ordre de $H_v^*$ est au moins $e_p$ car l'extension $\mathbb{Q}_p(\zeta_{m/p})/\mathbb{Q}_p$ est non-ramifiée ; alors que si $p^2$ divise $\mathfrak{f}_p$, nécessairement $H_v^*$ est d'ordre $p$. On définit $H_v$ comme étant l'image isomorphe de $H_v^*$ dans $\mathrm{Gal}(F/K)$. On peut voir que $H_v^*$ ne dépend pas de $v$, mais seulement de $p$. Il en est de même de $H_v$ que l'on note désormais $H_p$. On a déja obtenu l'estimation de son cardinal.

Montrons la propriété de congruence : soit $\mathcal{O}$ l'anneau des entiers de $\mathbb{Q}_p(\zeta_m)$. On a

$$\forall x \in \mathcal{O},\ \forall \sigma \in \Sigma_p \quad x^p \equiv \sigma x^p \mod p\mathcal{O}, \tag{4}$$

(cf. par exemple [2] p. 717). Ainsi pour tout $x \in \mathcal{O}_F$ et pour tout $\sigma \in H_p$, l'entier $x^p - \sigma x^p \in F$ est d'ordre supérieur à $e_p$ en $v$.

Montrons maintenant la dernière propriété. Soient $\sigma \in H_p - \{\mathrm{Id}\}$ et $\tau \in \mathrm{Gal}(\overline{K}/K)$ une extension de $\sigma$. Supposons par l'absurde que $\tau(\alpha_v(P)) = \alpha_v(P)$. Soit $\mathbb{E}$ le sous-corps de $F$ fixe par $\sigma$. On a $[\mathbb{E}(\alpha_v(P)) : \mathbb{E}] = [F(\alpha_v(P)) : F]$. De plus, par le lemme 3.4, le point $P$ est défini sur la même extension de $F$ que $\alpha_v(P)$. Donc,

$$[\mathbb{E}(\alpha_v(P)) : \mathbb{E}] = [F(\alpha_v(P)) : F] = [F(P) : F] = D. \tag{5}$$

On va maintenant montrer que $\mid \Sigma_p \mid = p$ : tout d'abord, comme $\mathbb{E}$ est strictement inclus dans $F$, on a $[F(P) : \mathbb{E}] > [F(P) : F]$ et donc, d'après (5),

$$[F(P) : \mathbb{E}(\alpha_v(P))] = \frac{[F(P) : \mathbb{E}]}{[\mathbb{E}(\alpha_v(P)) : \mathbb{E}]} = \frac{[F(P) : \mathbb{E}]}{[F(P) : F]} > 1. \tag{6}$$

Par ailleurs, d'après la remarque 3.1, on a $K(P) = F(P)$ et $K \subset \mathbb{E}(\alpha_v(P)) \subset F(P)$. Ainsi, $[F(P) : \mathbb{E}(\alpha_v(P))]$ divise $[K(P) : K(\alpha_v(P))]$. Si $K(P) = K(\alpha_v(P))$, alors $\tau$ fixe $K(P) = F(P)$ donc fixe $F$ ce qui contredit le choix de $\sigma \neq \mathrm{Id}$. Ainsi, par le lemme 3.3, l'extension $K(P)/K(\alpha_v(P))$ est de degré $p$. On en déduit que l'extension $F(P)/\mathbb{E}(\alpha_v(P))$ qui est non triviale par (6), est de degré $p$. On a ainsi

$$[F(\alpha_v(P) : \mathbb{E}(\alpha_v(P))] = \frac{[F(P) : \mathbb{E}(\alpha_v(P))]}{[F(P) : F(\alpha_v(P))]} = [F(P) : \mathbb{E}(\alpha_v(P))] = p \text{ par le lemme 3.4.}$$

L'extension $F/\mathbb{E}$ étant galoisienne, on en déduit que $\mid H_p \mid = [F : \mathbb{E}] = p$, donc par construction de $H_p$ on obtient $\mid \Sigma_p \mid = p$.

On sait que sur une courbe elliptique à multiplication complexe, on a bonne réduction ordinaire en toutes les places $v$ au-dessus d'un premier $p \in \mathcal{P}$. On peut donc appliquer le lemme 4.1 dans notre situation. Par ce lemme on sait que les points de $\alpha_v^k$-torsion sont définis sur $\mathbb{Q}_p(\zeta_{p^k}) \subset \mathbb{Q}_p(\zeta_m)$. Ainsi $F_v(E[\alpha_v^k]) \subset \mathbb{Q}(\zeta_m)$, donc le groupe de Galois $\Sigma_p$ induit par restriction un sous-groupe non-trivial de $\mathrm{Gal}(F(E[\alpha_v^k])/K)$ qui est cyclique d'ordre $p$ par le paragraphe précédent. Soit donc $\mathbb{F} \subset F(E[\alpha_v^k])$ son sous-corps fixe. Soient $x \in \mathbb{E}$

et $\rho \in G_1 = \mathrm{Gal}(F(E[\alpha_v^k])/\mathbb{F}) - \{\mathrm{Id}\}$. Puisque $[F : \mathbb{E}] = p$, le morphisme $\sigma$ engendre le groupe $\mathrm{Gal}(F/\mathbb{E})$, donc il existe un entier $u$ tel que $\rho_F = \sigma^u$. Notamment, on en déduit que $\rho(x) = x$, c'est-à-dire que

$$\mathbb{E} \subset \mathbb{F}. \tag{7}$$

On va maintenant montrer qu'il existe un point de $\alpha_v^k$-torsion $T$ tel qu'on ait l'inclusion $\mathbb{F}(P+T) \subset \mathbb{F}(\alpha_v(P))$. Si $\mathbb{F}(P) \subset \mathbb{F}(\alpha_v(P))$, il n'y a rien à montrer. Sinon, on a *a fortiori* l'inclusion stricte

$$\mathbb{F}(\alpha_v(P)) \subsetneq F\left(E[\alpha_v^k], P\right).$$

Les extensions étant galoisiennes, $[F(E[\alpha_v^k], \alpha_v(P)) : \mathbb{F}(\alpha_v(P))]$ divise $[F(E[\alpha_v^k]) : \mathbb{F}] = p$. De plus, par le lemme 3.4, $F(E[\alpha_v^k], P) = F(E[\alpha_v^k], \alpha_v(P))$, donc on a l'égalité

$$\left[F\left(E[\alpha_v^k], P\right) : \mathbb{F}\left(\alpha_v(P)\right)\right] = p.$$

Ainsi, le morphisme de restriction

$$\mathrm{res} : \mathrm{Gal}\left(F(E[\alpha_v^k], P)/\mathbb{F}(\alpha_v(P))\right) \to \mathrm{Gal}\left(F(E[\alpha_v^k])/\mathbb{F}\right),$$

entre groupes de même cardinaux est un isomorphisme. Soit $\widetilde{\rho}$ un générateur du groupe cyclique $\mathrm{Gal}\left(F(E[\alpha_v^k], P)/\mathbb{F}(\alpha_v(P))\right)$. Il existe un point de $\alpha_v$-torsion $T_1$ tel que

$$\widetilde{\rho}(P) = P + T_1.$$

De plus, par le lemme 4.1, on a l'isomorphisme de $I_v$-modules, $E[\alpha_v^k] \simeq \mu_{p^k}$, donc si $T_2$ est un point de $E[\alpha_v^k] \backslash E[\alpha_v^{k-1}]$, alors le point $T_3 = \rho(T_2) - T_2$ est d'ordre $p$. Finalement, il existe un entier $v$ tel que

$$T_1 = vT_3.$$

On pose $T = -rT_2$. On a alors

$$\rho(P+T) = P + T_1 - v\rho(T_2) = P + vT_3 - vT_3 - vT_2 = P + T.$$

Ceci nous donne bien l'inclusion $\mathbb{F}(P+T) \subset \mathbb{F}(\alpha_v(P))$.

En utilisant (5) et (7), on obtient

$$[\mathbb{F}(P+T) : \mathbb{F}] \leq [\mathbb{F}(\alpha_v(P) : \mathbb{F}] \leq [\mathbb{E}(\alpha_v(P) : \mathbb{E}] = D.$$

Or par construction, $\mathbb{F}_v \subset \mathbb{Q}_p(\zeta_{m/p})$ et $\mathbb{F} \subset F(E[\alpha_v^k])$, donc

$$\mathfrak{f}_p(\mathbb{F}) \leq \frac{p^k}{p} < \mathfrak{f}_p(F), \text{ et, si } l \neq p, \mathfrak{f}_l(\mathbb{F}) \leq \mathfrak{f}_l(F).$$

On en conclut, que

$$[\mathbb{F}(P+T) : \mathbb{F}] \leq D \text{ et, } \mathfrak{f}(\mathbb{F}) < \mathfrak{f}(F) = \mathfrak{f},$$

ce qui contredit la définition de $\mathfrak{f}$. Ceci conclut la preuve par l'absurde. □

## 4.2 Lemme non-ramifié

On passe maintenant au lemme qui va nous permettre de faire l'extrapolation dans le cas où il n'y a pas beaucoup de ramification. Il s'agit du même lemme que dans le cas multiplicatif.

**Lemme 4.3** *Soit $p \in \mathcal{P}^\star$, il existe $\Phi_p \in \mathrm{Gal}(F/K)$ tel que*

$$| \, x^p - \Phi_p x \, |_v \leq p^{-\frac{1}{e_p}},$$

*où $x \in \mathcal{O}_F$ et $v$ est une valuation sur $\overline{\mathbb{Q}}$ étendant $p$.*

*Démonstration* : C'est le lemme 3.1. de [2]. □

# 5 Lemme de Siegel

Dans la suite, on considère un point $P_1$ qui sera soit $P$ soit $\alpha_v(P)$. On note $\wp(u)$ la coordonnée $x$ de $P_1$ et on note $\wp(u_1), \ldots, \wp(u_D)$ les différents conjugués de $\wp(u)$ sur $F$. On dit que les $u_i$ sont *les conjugués de $u$*.

Soient $L$ et $T$ deux entiers strictement positifs et $N \in ]\sqrt{L}, 2\sqrt{L}[$ un nombre premier (qui existe par le "postulat de Bertrand"). On va construire une fonction

$$\varphi(z) = \sum_{\lambda_1=0}^{L} \sum_{\lambda_2=0}^{L} p(\lambda_1, \lambda_2) \wp(z)^{\lambda_1} \wp(Nz)^{\lambda_2}$$

avec $p(\lambda_1, \lambda_2) \in \overline{\mathbb{Z}}$ non tous nuls, telle que : $\varphi$ n'est pas constamment nulle sur $E(\mathbb{C})$, $\varphi$ est nulle en les conjugués $u_i$ de $u$ avec multiplicité $T$ et les coefficients $p(\cdot, \cdot)$ sont bien controlés. Le premier point est assuré par le choix de $N$ et le fait que les $p(\cdot, \cdot)$ ne sont pas tous nuls, le second découle d'un lemme de Siegel absolu.

**Lemme 5.1** *Soient $n$ un entier et $S$ un sous $\overline{\mathbb{Q}}$-espace vectoriel de dimension $d$ de $\overline{\mathbb{Q}}^n$. Pour tout $\varepsilon > 0$, il existe un vecteur $\boldsymbol{x} \in S$ tel que*

$$h_2(\boldsymbol{x}) \leq \frac{h_2(S)}{d} + \frac{\log d}{2} + \varepsilon.$$

*Démonstration* : cf. [7] lemme 4.7 et la remarque qui suit. □

**Proposition 5.1** *Soient $L$, $T$ et $k$ trois entiers positifs tels que $L^2 \geq kT$ et $k^{c_2} > (L + T)^2$ pour une certaine constante absolue $c_2 > 0$. Avec les notations précédentes, on peut*

*construire la fonction $\varphi$, s'annulant en des points $v_1, \dots, v_k$ avec multiplicité supérieure à $T$, telle que*

$$h(\varphi) \leq \frac{ckT}{(L+1)^2 - kT} \left( LN^2 \widehat{h}(P_1) + T \log(T+L) + T \log N + L \right) + \log L,$$

*où $c$ est une constante ne dépendant que de $E/K$.*

*Démonstration* : Par récurrence sur $t \leq T$, on montre qu'il existe un polynôme $Q_{\lambda_1,\lambda_2,t}$ dans $\mathcal{O}_k[X_1, \dots, X_4]$ de degré partiel en chaque variable majoré par $L + 2t$, à coefficients de valeur absolue majorée par $c_1 k^{c_2 t}$ et tel que

$$\frac{d^t}{dz^t} \left( \wp(z)^{\lambda_1} \wp(Nz)^{\lambda_2} \right) = Q_{\lambda_1,\lambda_2,t} \left( \wp(z), \wp'(z), \wp(Nz), \wp'(Nz) \right).$$

Au rang $t = 0$, le polynôme $Q = X_1^{\lambda_1} X_3^{\lambda_2}$ convient.
Supposons la propriété vraie au rang $t$ et montrons-la au rang $t+1$ : en notant abusivement $Q_t$ le polynôme $Q_{\lambda_1,\lambda_2,t}$, on a

$$\begin{aligned} \frac{d^{t+1}}{dz^{t+1}} \left( \wp(z)^{\lambda_1} \wp(Nz)^{\lambda_2} \right) &= \frac{d}{dz} \frac{d^t}{dz^t} \left( \wp(z)^{\lambda_1} \wp(Nz)^{\lambda_2} \right) \\ &= \frac{d}{dz} Q_t \left( \wp(z), \wp'(z), \wp(Nz), \wp'(Nz) \right) \\ &= \frac{\partial Q_t}{\partial X_1} (\cdot) \, \wp'(z) + \ldots + N \frac{\partial Q}{\partial X_4} (\cdot) \, \wp''(Nz). \end{aligned}$$

En utilisant la relation $\wp''(Nz) = 6\wp(Nz)^2 + 2a_4$, on pose donc

$$Q_{t+1} = X_2 \frac{\partial Q_t}{\partial X_1} + \ldots + N(6X_3^2 + 2a_4) \frac{\partial Q_t}{\partial X_4}.$$

On a clairement $\deg_{X_i} Q_{t+1} \leq L + 2(t+1)$. De plus, en notant $q_{i,t}$ les coefficients de $Q_t$, on a

$$|q_{i,t+1}| \leq 6c_1 N(L+2t) k^{c_2 t} \leq 12 c_1 \sqrt{L}(L+2T) k^{c_2 t} \leq c_1 k^{c_2(t+1)}.$$

Finalement, le système $\forall t \leq T-1$, $\forall i \in [\![1, k]\!]$, $\varphi^{(t)}(v_i) = 0$ s'écrit :

$$\forall t \leq T-1, \quad \forall i \in [\![1,k]\!], \quad \sum_{\lambda_1=0}^{L} \sum_{\lambda_2=0}^{L} p(\lambda_1, \lambda_2) Q_{\lambda_1,\lambda_2,t} \left( \wp(v_i), \wp'(v_i), \wp(Nv_i), \wp'(Nv_i) \right) = 0.$$

Pour tout $0 \leq i \leq k$, posons

$$\forall 0 \leq t \leq T-1, \ \forall 0 \leq \lambda_1, \lambda_2 \leq L, \quad \alpha^{(i)}_{(\lambda_1,\lambda_2),t} = Q_{\lambda_1,\lambda_2,t} \left( \wp(v_i), \wp'(v_i), \wp(Nv_i), \wp'(Nv_i) \right).$$

On considère les vecteurs

$$\mathbf{y}_{i,t} = \left( \alpha^{(i)}_{(0,0),t}, \ldots, \alpha^{(i)}_{(L,0),t}, \ldots, \alpha^{(i)}_{(L,L),t} \right) \in \overline{\mathbb{Q}}^{(L+1)^2}.$$

Comme dans [6] p.42 inégalité (18) et suivante, on vérifie que les coefficients du système

$$\mathbf{y}_{i,t} \cdot \mathbf{x} = 0, \quad 0 \leq i \leq k, \quad 0 \leq t \leq T-1$$

avec $\mathbf{x} \in \overline{\mathbb{Q}}^{(L+1)^2}$ sont tous de hauteur au plus

$$c_3 \left( LN^2 \widehat{h}(P_1) + T \log(T+L) + T \log N + L \right).$$

Par ailleurs, le $\overline{\mathbb{Q}}$-espace vectoriel

$$S = \left\{ \mathbf{x} \in \overline{\mathbb{Q}}^{(L+1)^2} \ / \ \mathbf{y}_{i,t} \cdot \mathbf{x} = 0, \quad 0 \leq i \leq k, \quad 0 \leq t \leq T-1 \right\}$$

est de dimension $(L+1)^2 - kT$ et les vecteurs $\mathbf{y}_{i,t}$ forment une base de l'orthogonal $S^{\perp}$. De plus, le Lemma IV p.10 de [14], nous indique que

$$h_2(S) = h_2\left(S^{\perp}\right) \leq \sum_{i,t} h_2(\mathbf{y}_{i,t}) \leq c_3 kT \left( LN^2 \widehat{h}(P_1) + T \log(T+L) + T \log N + L \right).$$

On applique le lemme 5.1 avec $\varepsilon = \frac{1}{2} \log \frac{(L+1)^2}{(L+1)^2 - kT}$. On a ainsi obtenu la fonction voulue, avec des coefficients dans $\overline{\mathbb{Q}}$ et avec la hauteur projective $h_2$. En fait, en appliquant une remarque de Roy et Thunder [13], on peut également trouver une solution à coefficients entiers algébriques et avec la hauteur $h$. La remarque consiste à dire que si $x \in \overline{\mathbb{Q}}^n$, il existe $a \in \overline{\mathbb{Q}}$ tel que $ax$ est à coefficients entiers algébriques et tel que $h(ax) = h_2(ax) = h_2(x)$. □

# 6 Extrapolation

Il y a deux cas, selon que l'on a "beaucoup" de premiers ayant "beaucoup" de ramification ou non (ceci étant quantifié). On commence par le cas qui sera utilisé quand il n'y a pas beaucoup de grande ramification.

**Proposition 6.1** *Soient $L_1$ et $T_1$ deux entiers strictement positifs d'ordre de grandeur polynomial en $D$, tels que $L_1^2 \geq DT_1$. On pose $P_1 = P$ et on considère la fonction $\varphi$ obtenue dans la proposition 5.1 avec $L = L_1$, $T = T_1$ et $k = D$. Soient $p \in \mathcal{P}^{\star}$ et $v$ une place étendant $p$ sur $\overline{K}$. Pour tout $t \leq \min\{L_1, \frac{T_1}{2}\}$ et pour tout $\tau \in \mathrm{Gal}(\overline{K}/K)$ étendant le morphisme $\Phi_p$ du lemme 4.3, on a*

$$\log \mid \tau(\varphi)^{(t)}(\alpha_p u) \mid_v \leq -\frac{T_1}{2e_p} \log p + 8L_1 \log \max\{1, \mid \wp(N\alpha_v u) \mid_v\}.$$

*Démonstration* : Il s'agit essentiellement du deuxième pas de [11] à la différence que l'on utilise un lemme de Siegel absolu, ce qui conduit à supposer l'annulation en un point et en tous ses conjugués, ainsi qu'à faire intervenir l'indice de ramification $e_p$ de $p$ dans $F$. On étend $v$ au corps $\overline{K}(X)$ en posant $\mid X \mid_v = 1$.

Il y a deux cas : soit $\wp(u)$ est un $v$-entier, soit non.

Cas 1 : on vérifie simplement que l'on peut écrire $\varphi^{(t)}$ comme un polynôme en les variables $\wp(z)$, $\wp(Nz)$, $\frac{\wp'(Nz)}{\wp'(z)}$ de degré partiels en $\wp(Nz)$ et $\frac{\wp'(Nz)}{\wp'(z)}$ respectivement majorés par $3(L_1+t) \leq 6L_1$ et par 1. On en déduit l'existence d'une fraction rationnelle $G$, telle que $S_N(X)^{8L_1}G(X)$ soit un polynôme à coefficients dans $\mathcal{O}_{\overline{K}}$ et vérifiant

$$G(\wp(z)) = \varphi^{(t)}(z)^2.$$

La fraction rationnelle $G(X)$ admet donc un zéro d'ordre supérieur à $T_1$ aux points $X = \wp(u_1), \ldots, X = \wp(u_D)$. Notons $\Delta = \sum a_i X^i$ le polynôme minimal unitaire sur $F$ de $\wp(u)$. Par hypothèse sur $\wp(u)$, il est à coefficients entiers algébriques. Ainsi, il existe un polynôme $H$ à coefficients $v$-entiers, tel que

$$S_N(X)^{8L_1}G(X) = \Delta(X)^{T_1}H(X). \tag{8}$$

Si $\pi_p$ est une uniformisante au-dessus de $p$ dans $K$ et $\pi_{p,F}$ une uniformisante de $p$ dans $F$, par le petit théorème de Fermat et le lemme 4.3, on obtient donc

$$\tau(\Delta)(\wp(\alpha_v u)) = \tau(\Delta)(\wp(u)^p) = (\Delta(\wp(u)))^p = 0 \mod \pi_{p,F},$$

et ce, pour tout $\pi_{p,F}$ au-dessus de $\pi_p$. En substituant $\wp(\alpha_v u)$ à $X$ dans (8) et en appliquant $\tau$ aux coefficients des polynômes $S$, $G$, $H$ et $\Delta$, on en déduit que le membre de droite de cette égalité transformée par $\tau$ est d'ordre en $\pi_p$ supérieur à $\frac{T_1}{e_p}$. Il reste maintenant à majorer l'ordre en $\pi_p$ de $\tau(S_N)(\wp(\alpha_v u)$. Or $S_N$ est à coefficients dans $K$, donc est, de même que $R_N$, invariant par $\tau$. De plus,

$$\wp(N\alpha_v u) = \frac{R_N(\wp(\alpha_v u))}{S_N(\wp(\alpha_v u))}.$$

D'après le lemme 2.2, les polynômes $R_N$ et $S_N$ réduits mod $\pi_p$ sont premiers entre eux. Autrement dit, l'un des deux nombres $R_N(\wp(\alpha_v u))$, $S_N(\wp(\alpha_v u))$ est une unité de $\mathcal{O}_{\overline{K_v}}$. Si c'est $S_N(\wp(\alpha_v u))$, on a fini, sinon, c'est $R_N(\wp(\alpha_v u))$ et donc

$$\mathrm{ord}_{\pi_p}(S_N(\wp(\alpha_v u)) = -\mathrm{ord}_{\pi_p}\wp(N\alpha_v u).$$

Cas 2 : Si $\wp(u)$ n'est pas un $v$-entier, on fait un changement de carte comme dans le b) du deuxième pas de Laurent [11] : on effectue le changement de variable projectif

$$t = -\frac{X}{Y} \quad \text{et,} \quad s = -\frac{1}{Y}.$$

Alors $s$ s'exprime en fonction du paramètre local $t$ par une série entière $s(t)$ à coefficients $v$-entiers. On considère cette fois la fonction

$$(\wp'(z)\wp'(Nz))^{-(L_1+t)}\,\varphi^{(t)}(z), \text{ à la place de } \varphi^{(t)}(z)^2.$$

Elle s'écrit comme un polynôme en les variables $-\frac{\wp(z)}{\wp'(z)}$, $-\frac{1}{\wp(z)}$, $-\frac{\wp(Nz)}{\wp'(Nz)}$ et $-\frac{1}{\wp'(Nz)}$. Il existe donc une série entière $G$, à coefficients $v$-entiers, telle que

$$G(t) = (\wp'(z)\wp'(Nz))^{-(L_1+t)}\,\varphi^{(t)}(z). \tag{9}$$

Soient $\xi = -\frac{\wp(u)}{\wp'(u)}$ le paramètre local associé au point $P$ et $\Delta$ le polynôme minimal unitaire de $\xi$ sur $F_v$. D'après l'hypothèse, le nombre $\xi$ est dans l'idéal maximal $\overline{\mathfrak{m}_v}$, donc tous les coefficients de $\Delta$, sauf le coefficient dominant, sont divisibles par $\pi_p$. Le théorème de préparation de Weierstrass montre qu'il existe une série entière $H$, à coefficients $v$-entiers, telle que

$$G(t) = \Delta(t)^{(T_1-t)}H(t).$$

Dans cette identité on substitue $t = [\alpha_v](\xi) = \xi^p + \pi_p\psi(\xi)$ par le lemme 2.3. On conclut alors comme dans le premier cas $\big($il faut savoir majorer

$$\mathrm{ord}_{\pi_p}(\wp'(\alpha_v u)\wp'(N\alpha_v u)) = \mathrm{ord}_{\pi_p}s([\alpha_v](\xi)) + \mathrm{ord}_{\pi_p}s([N\alpha_v](\xi)).$$

Puisque $N$ est premier à $p$, ces dernières quantités sont toutes deux égales à

$$-\frac{3}{2}\mathrm{ord}_{\pi_p}\wp(N\alpha_v u) \text{ (cf. paragraphes 3 et 6 de [17]).}$$

Remplaçant dans (9), $z$ par $\alpha_v u$ et $t$ par $[\alpha_v](\xi)$ on peut alors conclure$\big)$. □

On passe maintenant à la proposition qui nous servira quand il y a beaucoup de grande ramification.

**Proposition 6.2** *Soient $L_2$ et $T_2$ deux entiers d'ordre de grandeur polynomial en $D$ et $\Lambda_2$ un entier strictement positif, tels que $L_2^2 \geq DT_2\Lambda_2$. On considère la fonction $\varphi$ obtenue dans la proposition 5.1 avec $L = L_2$, $T = T_2$, $k = D\Lambda_2$ et avec*

$$\{u_1, \ldots, u_k\} := \{\alpha_v u_i \ / i \in \{1, \ldots, D\} \text{ et } v \text{ décrivant un ensemble } \mathcal{P}_2^\star \text{ de cardinal } \Lambda_2\}.$$

*Pour tout $t \leq \min\{L_2, \frac{T_2}{2}\}$, pour tout $v$ dans l'ensemble $\mathcal{P}_2^\star$ et pour tout $\tau \in \mathrm{Gal}(\overline{K}/K)$ tel que $\tau_F \in H_p$, $p/v \in \mathcal{P}_2^\star$, on a*

$$\log \mid \tau(\varphi^{(t)})(\alpha_p u) \mid_v \leq -\frac{T_2}{2}\log p + 8L_2 \log\max\{1, \mid \wp(N\alpha_v u) \mid_v\}.$$

*Démonstration* : Là encore il y a deux cas selon que $\wp(u)$ est un $v$-entier ou non. On commence par le cas où c'est un $v$-entier. On étend $v$ au corps $\overline{K}(X)$ en posant $\mid X \mid_v = 1$ et on fait la même preuve que précédemment, en montrant cette fois-ci que

$$\tau\left(\Delta_{\alpha_v}\right)\left(\wp(\alpha_v u)\right) = 0 \mod \pi_p,$$

où $\Delta_{\alpha_v}$ est le polynôme minimal de $\wp(\alpha_v u)$. Pour montrer ceci, on note $\Delta^{(p)}$ le polynôme minimal de $\wp(u)$ où l'on a élevé les coefficients à la puissance $p$. On a alors

$$\begin{aligned}
\tau\left(\Delta_{\alpha_v}\right)\left(\wp(\alpha_v u)\right) &= \tau\left(\Delta^{(p)}\right)\left(\wp(\alpha_v u)\right) \mod \pi_p \text{ par le petit théorème de Fermat,} \\
&= \Delta^{(p)}(\wp(\alpha_v u)) \mod \pi_p \text{ par le lemme 4.2,} \\
&= \Delta^{(p)}(\wp(u)^p) \mod \pi_p, \\
&= (\Delta(\wp(u)))^p \mod \pi_p, \\
&= 0.
\end{aligned}$$

Si $\wp(u)$ n'est pas un $v$-entier, on utilise le même argument que dans le cas 2 de la proposition 6.1 précédente pour conclure de la même façon. □

# 7 Conclusion

## 7.1 Le cas du théorème 1.1

En notant $[\cdot]$ la partie entière, on pose $C$ une constante assez grande (de sorte que les inégalités soient vérifiées) ne dépendant que de $E/K$ et on pose

$$N_1 = \left[C^4 \frac{(\log 2D)^6}{(\log\log 5D)^5}\right] \text{ et } E = \left[C\left(\frac{\log 2D}{\log\log 5D}\right)^2\right].$$

Pour $p$ entre $N_1/2$ et $N_1$, le théorème de Chebotarev nous indique qu'il y a plus de $\Lambda = \left[\frac{C^4}{2}\left(\frac{\log 2D}{\log\log 5D}\right)^6\right]$ tels $p$. En notant $e_v$ l'indice de ramification de $v$ dans $F$, on a : soit il y a plus de $\Lambda_1 = \Lambda/2$ nombres premiers $p$ ayant une place $v$ avec un $e_v \leq E$, soit il y a plus de $\Lambda_2 = \Lambda/2$ nombres premiers $p$ ayant toutes les places $v$ avec un $e_v > E$. On va traiter chaque cas séparément et conclure dans chacun de ces deux cas.

Cas 1 : il y a plein de $v$ ayant peu de ramification, *i.e.*, il y a plus de $\Lambda_1 = \Lambda/2$ nombres premiers $p$ ayant une place $v$ avec un $e_v \leq E$.

Dans ce cas, on note $\mathcal{P}_1^\star$ le sous-ensemble de $\mathcal{P}^\star$ correspondant à $\Lambda_1$ et on introduit les paramètres suivants :

$$L_1 = \left[C^3 D \frac{(\log 2D)^5}{(\log\log 5D)^6}\right],\ T_1 = \left[C^{\frac{9}{2}} D \frac{(\log 2D)^7}{(\log\log 5D)^9}\right],\ \text{et, } T_1' = \left[C^3 D \frac{(\log 2D)^4}{(\log\log 5D)^6}\right],$$

et $N$ est un nombre premier tel que $\frac{1}{2}\sqrt{L_1} \leq N \leq \sqrt{L_1}$.

**Proposition 7.1** *Pour tout $p \in \mathcal{P}_1^\star$, pour tout $\tau$ étendant $\Phi_p^{-1}$ et pour tout $t \leq T_1'$, la fonction $\tau^{-1}\left(\varphi^{(t)}\right)$ de la proposition 6.1 s'annule en $\alpha_v u$.*

*Démonstration* : En notant

$$\zeta = \mathrm{N}_{F(P)/F}\left(\tau\left(\varphi^{(t)}\right)(\alpha_v u)\right),$$

on a grâce à la proposition 6.1,

$$\log \mid \zeta \mid_v \leq -\frac{DT_1 \log p}{2e_v} + 8L_1 \sum_{w/v} D_w \log \max\left(1, \mid \wp(N\alpha_v u \mid_w\right).$$

On en déduit

$$\log \mid \zeta \mid_v \leq -c_{12}\frac{DT_1 \log p}{2E} + DL_1\left(c_{10} + N^2 p\widehat{h}(P)\right).$$

Or par hypothèse sur $\widehat{h}(P)$, on a $N^2 p\widehat{h}(P) \leq N^2 N_1 \widehat{h}(P) \leq c_{11}$. En remplaçant les paramètres par leur valeur, on obtient donc

$$\log \mid \zeta \mid_v \leq -C^{\frac{7}{2}} D^2 \frac{(\log 2D)^5}{(\log\log 5D)^6}.$$

Ainsi, si $\zeta$ est non nul,

$$h(\zeta) = h(\zeta)^{-1} \geq \frac{d_v}{d} \log \max\{1, \mid \zeta^{-1} \mid_v\} \geq C^{\frac{7}{2}} D^2 \frac{(\log 2D)^5}{(\log\log 5D)^6}. \tag{10}$$

Par ailleurs, un calcul classique (cf. par exemple [6] p.50) permet d'écrire

$$h(\zeta) \leq c_{15} DT_1' \log(T_1' + L_1) + c_{16} DL_1 N^2 p\widehat{h}(P) + c_{17} Dh(\varphi)$$

où $h(\varphi)$ est donnée par la proposition (5.1) :

$$h(\varphi) \leq \frac{cDT_1}{(L_1+1)^2 - DT_1}\left(L_1 N^2 \widehat{h}(P) + T_1 \log(T_1 + L_1) + T_1 \log N + L_1\right) + \log L_1.$$

en remplaçant les paramètres par leur valeur, on obtient :

$$h(\zeta) \leq c_{15} C^3 D^2 \frac{(\log 2D)^5}{(\log\log 5D)^6} + c_{16} C^3 D^2 \frac{(\log 2D)^5}{(\log\log 5D)^6} + c_{17} C^3 D^2 \frac{(\log 2D)^5}{(\log\log 5D)^6},$$

Soit

$$h(\zeta) \leq c_{18} C^3 D^2 \frac{(\log 2D)^5}{(\log\log 5D)^6}. \tag{11}$$

En comparant les inégalités (10) et (11), on obtient une contradiction pour $C$ suffisamment grand, ce qui conclut. □

Puisque l'on travaille avec des $p \in \mathcal{P}^\star \subset \mathcal{P}$, on a $[F(\alpha_v(P)) : F] = D$. Donc, on obtient ainsi, en comptant les multiplicités, au moins

$$DT_1'\Lambda_1 \geq \frac{1}{2} C^7 D^2 \frac{(\log 2D)^{10}}{(\log\log 5D)^{12}} \tag{12}$$

racines. Or en utilisant la relation

$$\wp(Nz) = \frac{R_N(\wp(z))}{S_N(\wp(z))},$$

on peut écrire $\varphi$ sous la forme

$$\varphi(z) = F(\wp(z)),$$

où $F$ est une fraction rationnelle de degré majoré par

$$(N^2+1)L_1 \leq 2L_1^2 \leq 2C^6D^2\frac{(\log 2D)^{10}}{(\log\log 5D)^{12}}. \tag{13}$$

En comparant (12) et (13), on en déduit que la fraction $F$ est identiquement nulle. Donc il en est de même pour $\varphi$, ce qui est absurde par le choix de $N$. Le théorème est donc démontré dans ce cas.

Cas 2 : il y a plein de $v$ ayant beaucoup de ramification, *i.e.*, il y a plus de $\Lambda_2 = \Lambda/2$ nombres premiers $p$ ayant toutes les places $v$ avec un $e_v > E$.

Dans ce cas, on note $\mathcal{P}_2^\star$ le sous-ensemble de $\mathcal{P}^\star$ correspondant à $\Lambda_2$ et on introduit les paramètres suivants :

$$L_2 = \left[C^{\frac{35}{8}}D\frac{(\log 2D)^7}{(\log\log 5D)^8}\right],\ T_2 = \left[C^{\frac{9}{2}}D\frac{(\log 2D)^7}{(\log\log 5D)^9}\right] \text{ et, } T_2' = \left[C^4D\frac{(\log 2D)^6}{(\log\log 5D)^8}\right],$$

et $N$ est un nombre premier tel que $\frac{1}{2}\sqrt{L_2} \leq N \leq \sqrt{L_2}$.

**Proposition 7.2** *Pour tout $p \in \mathcal{P}_2^\star$, pour tout $\tau$ tel que $\tau_F \in H_p$ et pour tout $t \leq T_2'$, la fonction $\tau^{-1}\left(\varphi^{(t)}\right)$ de la proposition 6.2 s'annule en $\alpha_v u$.*

*Démonstration* : En notant

$$\zeta = \mathrm{N}_{F(P)/F}\left(\tau\left(\varphi^{(t)}\right)(\alpha_v u)\right),$$

on a grâce à la proposition 6.2,

$$\log \mid \zeta \mid_v \leq -\frac{DT_2\log p}{2} + 8L_2\sum_{w/v} D_w \log\max\left(1, \mid \wp(N\alpha_v u \mid_w\right).$$

On en déduit

$$\log \mid \zeta \mid_v \leq -c_{12}\frac{DT_2\log p}{2} + DL_2\left(c_{10} + N^2p\widehat{h}(P)\right).$$

Or par hypothèse sur $\widehat{h}(P)$, on a $N^2p\widehat{h}(P) \leq N^2N_1\widehat{h}(P) \leq c_{11}$. En remplaçant les paramètres par leur valeur, on obtient donc

$$\log \mid \zeta \mid_v \leq -c_{13}C^{\frac{9}{2}}D^2\frac{(\log 2D)^7}{(\log\log 5D)^8}.$$

Ainsi, si $\zeta$ est non nul, on a

$$h(\zeta) = h(\zeta^{-1}) \geq \frac{d_v}{d} \log \max\{1, \mid \zeta^{-1} \mid_v\} \geq c_{14} C^{\frac{9}{2}} D^2 \frac{(\log 2D)^7}{(\log\log 5D)^8}. \tag{14}$$

Par ailleurs, le même calcul que précédemment permet d'écrire

$$h(\zeta) \leq c_{15} D T_2' \log(T_2' + L_2) + c_{16} D L_2 N^2 p\widehat{h}(P) + c_{17} D h(\varphi)$$

où $h(\varphi)$ est donnée par la proposition (5.1) :

$$h(\varphi) \leq \frac{cD\Lambda_2 T_2}{(L_2+1)^2 - D\Lambda_2 T_2} \Big( L_2 N^2 \widehat{h}(P) + T_2 \log(T_2 + L_2) + T_2 \log N + L_2 \Big) + \log L_2.$$

en remplaçant les paramètres par leur valeur, on obtient :

$$h(\zeta) \leq \left( c_{15} C^4 + c_{16} C^{\frac{35}{8}} + c_{17} C^{\frac{17}{4}} \right) D^2 \frac{(\log 2D)^7}{(\log\log 5D)^8},$$

soit,

$$h(\zeta) \leq c_{18} C^{\frac{17}{4}} D^2 \frac{(\log 2D)^7}{(\log\log 5D)^8}. \tag{15}$$

En comparant les inégalités (14) et (15), on obtient une contradiction, ce qui conclut. □

Puisque l'on travaille avec des $p \in \mathcal{P}^\star \subset \mathcal{P}$, on a $[F(\alpha_v(P)) : F] = D$. Donc, on obtient ainsi, en comptant les multiplicités, au moins

$$EDT_2'\Lambda_2 \geq \frac{1}{2} C^9 D^2 \frac{(\log 2D)^{14}}{(\log\log 5D)^{16}} \tag{16}$$

racines. Or en utilisant la relation

$$\wp(Nz) = \frac{R_N(\wp(z))}{S_N(\wp(z))},$$

on peut écrire $\varphi$ sous la forme

$$\varphi(z) = F(\wp(z)),$$

où $F$ est une fraction rationnelle de degré majoré par

$$(N^2+1)L_2 \leq 2L_2^2 \leq 2C^{\frac{35}{4}} D^2 \frac{(\log 2D)^{14}}{(\log\log 5D)^{16}}. \tag{17}$$

En comparant (16) et (17), on en déduit que la fraction $F$ est identiquement nulle. Donc il en est de même pour $\varphi$, ce qui est absurde par le choix de $N$. Le théorème est donc démontré dans ce cas. Il est donc démontré dans tous les cas. □

## 7.2 Le cas du théorème 1.2

Pour prouver le théorème 1.2, on fait essentiellement la même preuve que pour le théorème 1.1 : on peut faire les mêmes réductions et on a uniquement besoin de la partie non-ramifiée de la preuve précédente. La seule chose qui change est le choix des paramètres permettant de conclure.

En notant $[\cdot]$ la partie entière et $C$ une constante assez grande (de sorte que les inégalités soient vérifiées) ne dépendant que de $E/K$ et de $c_0$, on pose $E = 1$ et

$$N_1 = \left[3C^2 \frac{(\log 2D)^2}{\log\log 5D}\right].$$

Pour $p$ entre $N_1/2$ et $N_1$, le théorème de Chebotarev nous indique qu'il y a plus de $\Lambda = \left[\frac{C^2}{2}\left(\frac{\log 2D}{\log\log 5D}\right)^2\right]$ tels $p$. On note $\mathcal{P}_1^\star$ le sous-ensemble de $\mathcal{P}$ correspondant à $\Lambda$ et on introduit les paramètres suivants :

$$L_1 = \left[C^2 D \frac{\log 2D}{\log\log 5D}\right],\ T_1 = \left[2CD\frac{\log 2D}{\log\log 5D}\right],\ \text{et, } T_1' = \left[\frac{C^2}{2}D\right],$$

et $N$ est un nombre premier tel que $\frac{1}{2}\sqrt{L_2} \leq N \leq \sqrt{L_2}$.

Le même argument qu'au cas 1 du paragraphe précédent nous permet alors de conclure.

**Remarque 7.1** Notons que bien que la preuve de ce théorème 1.2 soit moralement la même que celle du théorème de [11], le fait d'utiliser un lemme de Siegel absolu conduit à un choix différent des paramètres pour faire fonctionner l'étape d'extrapolation.

# 8 Application du théorème 1.1

En fait une version affaiblie du théorème 1.1 suffit déjà. Précisément, on utilisera le corollaire suivant :

**Corollaire 8.1** *Soient $E/K$ une courbe elliptique à multiplication complexe et $\varepsilon$ un réel strictement positif. On note $K^{\mathrm{ab}}$ la clôture abélienne de $K$. Il existe une constante strictement positive $c(E/K, \varepsilon)$ telle que*

$$\forall P \in E(\overline{K})\backslash E_{\mathrm{tors}},\quad \widehat{h}(P) \geq \frac{c(E/K,\varepsilon)}{D^{1+\varepsilon}},$$

*où $D = [K^{\mathrm{ab}}(P) : K^{\mathrm{ab}}]$.*

On reprend les notations de l'article [18], et on va montrer comment éviter la seconde partie de la preuve (parties 4.3 et 4.4 et 6 de l'article [18]).

Soient $n \geq r \geq 0$ et $P \in S_{n-r}(C)$. On note $K(P)$ le corps de définition de $P$. On note $x_i : C \to E$ les applications coordonnées définies par la composition de l'immersion fermée $C \hookrightarrow E^n$ et de la $i$-ème projection $E^n \to E$. Comme $E$ est à multiplication complexe, on sait que son anneau d'endomorphismes est un ordre $\mathcal{O} = \mathbb{Z}+\tau\mathbb{Z}$ dans un corps quadratique imaginaire. On définit alors $n$ morphismes supplémentaires : $\forall 1 \leq i \leq n$, $x_{n+i} = \tau x_i$. On note

$$\Gamma = \langle x_1, \ldots, x_n \rangle_{\mathrm{End}(E)}$$

le *coordinate module* (définition de [18] p.51) : c'est le $\mathbb{Z}$-module engendré par les $x_i$ avec $1 \leq i \leq 2n$. On considère par ailleurs le $\mathbb{Z}$-module (qui est de rang $2r$ comme il suit du lemma 2. de [18])

$$\Gamma_P := \langle x_1(P), \ldots, x_{2n}(P) \rangle_{\mathrm{End}(E)} .$$

Dans sa proposition 2. de [18], Viada montre que $K\left((\Gamma_P)_{\mathrm{tors}}\right) \subset K(P)$ et elle montre également qu'il existe des éléments $\mathbb{Z}$-linéairement indépendants $g_1, \ldots, g_{2r}$ de $\Gamma_P$, définis sur $K(P)$ et engendrant la partie libre de $\Gamma_P$. Ainsi on peut écrire pour tout $1 \leq i \leq 2n$,

$$x_i(P) = \sum_{j=1}^{2r} a_{ij} g_j + T_i$$

où $T_i$ est un point de torsion. On pose $\nu_j = (a_{1j}, \ldots, a_{nj})$ et on pose $\mid \nu_j \mid = \max_i \mid a_{ij} \mid$. Avec ces notations on a l'inégalité (19) de [18] :

$$\prod_{i=1}^{2r} \widehat{h}(g_i) \ll \prod_{i=1}^{2r} \mid \nu_i \mid^{-2} . \tag{18}$$

Dans son corollary 1. Viada obtient alors l'inégalité

$$d \ll \left( NR \prod_{i=1}^{2r} \mid \nu_i \mid \right)^{\frac{1}{n-r}} \tag{19}$$

où $d = [K(P) : K]$ et $N$ et $R$ sont deux entiers tels que $(\Gamma_P)_{\mathrm{tors}} \simeq \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/R\mathbb{Z}$. (Ces entiers existent par la proposition 2. de [18].)

Dans son corollary 2. Viada obtient enfin les inégalités

$$(NR)^{1-\varepsilon} \ll d \ll (NR)^{\frac{1}{n-r-1-\varepsilon}}.$$

Ainsi $d$ est borné en fonction de $N$ et si $n - r \geq 3$ on obtient l'inégalité

$$(NR)^{1-\varepsilon} \ll (NR)^{\frac{1}{2-\varepsilon}}$$

Ce qui permet de borner $N$ et donc de conclure. Dans le cas où $n - r = 2$, autrement dit le cas qui nous intéresse réellement, on obtient juste

$$(NR)^{1-\varepsilon} \ll (NR)^{\frac{1}{1-\varepsilon}}$$

ce qui ne permet malheureusement pas de conclure, d'où la nécessité d'une seconde étape assez technique dans l'article [18]. On montre maintenant, et c'est là la nouveauté, comment conclure dans le cas général en utilisant notre corollaire 8.1 et en réutilisant ce qui a été fait jusqu'à présent. On se place désormais dans le cas où $n - r = 2$. On note $K_N = K\left((\Gamma_P)_{\text{tors}}\right)$. On peut toujours supposer que $K = K(j(E))$, donc $K_N/K$ est une sous-extension abélienne de l'extension abélienne $K\left(E[N]\right)/K$. On pose $D = [K(P) : K_N]$. On a, en utilisant toujours le corollary 2. de [18],

$$D = \frac{d}{[K_N : K]} \ll (NR)^{\frac{1}{1-\varepsilon}} (NR)^{-(1-\varepsilon)} \leq (NR)^{3\varepsilon} \tag{20}$$

si $\varepsilon$ est suffisament petit. Par ailleurs, les points $g_1$,..., $g_{2r}$ sont des points d'ordre infini de $E(K(P))$. En appliquant le corollaire 8.1 puis l'inégalité (20), on obtient

$$\prod_{i=1}^{2r} \widehat{h}(g_i) \gg D^{-2r-2r\varepsilon} \gg (NR)^{-6r\varepsilon(1+\varepsilon)} \gg (NR)^{-12n\varepsilon}. \tag{21}$$

On a ainsi

$$\begin{aligned}
(NR)^{1-\varepsilon} \ll d &\ll \left( NR \prod_{i=1}^{2r} \mid \nu_i \mid \right)^{\frac{1}{2}} \text{ par l'inégalité (19)} \\
&\ll (NR)^{\frac{1}{2}} \prod_{i=1}^{2r} \widehat{h}(g_i)^{-\frac{1}{4}} \text{ par l'inégalité (18)} \\
&\ll (NR)^{\frac{1}{2}+3n\varepsilon} \text{ par l'inégalité (21)}
\end{aligned}$$

Ceci permet de conclure la preuve du théorème en prenant $\varepsilon$ assez petit.

# Références


[1] F. Amoroso et R. Dvornicich. A Lower Bound for the height in Abelian Extensions. In *J. Number Theory*, volume 80, pages 260–272, 2000.

[2] F. Amoroso et U. Zannier. A Relative Dobrowolski Lower Bound over Abelian Extensions. In *Ann. Scuola Norm. Pisa Cl. Sci. (4)*, volume XXIX, pages 711–727, 2000.

[3] M. Baker. Canonical heights on elliptic curves over abelian extensions. In *Internat. Math. Res. Notices*, volume 29, pages 1571–1589, 2003.

[4] M. Baker et J. Silverman. A lower bound for the canonical height on abelian varieties over abelian extensions. To appear in *Math. Rev. Letters*, arXiv :mathNT/0312393.

[5] E. Bombieri, D. Masser, et U. Zannier. Intersecting a Curve with Algebraic Subgroups of Multiplicative Groups. In *Internat. Math. Res. Notices*, volume 20, pages 1119–1139, 1999.

[6] S. David et M. Hindry. Minoration de la hauteur de Néron-Tate sur les variétés abéliennes de type C. M. In *J. Reine Angew. Math.*, volume 529, pages 1–74, 2000.

[7] S. David et P. Philippon. Minoration des hauteurs normalisées des sous-variétés des tores. In *Ann. Scuola Norm. Pisa Cl. Sci. (4)*, volume 28, pages 489–543, 1999.

[8] M. Deuring. Die Zetafunktion einer algebräischen Kurve vom Geschlechte Eins. In *Nachrichten Alad. Wiss.* Göttingen, pages 85–94 (1953), 13–42 (1955), 37–76 (1956), 55–80, (1957).

[9] E. Dobrowolski. On a question of Lehmer and the number of irreductible factors of a polynomial. In *Acta Arith.*, volume 34, pages 391–401, 1979.

[10] M. Hindry et J. Silverman. *Diophantine Geometry An Introduction*, volume 201 of *Graduate Texts in Mathematics*. Springer-Verlag, 2000.

[11] M. Laurent. Minoration de la hauteur de Néron-Tate. In M.-J. Bertin, editor, *Séminaire de théorie des nombrs de* P*aris, 1981-1982*, volume 38, pages 137–152. Progr. Math., 1983.

[12] G. Rémond. Intersection de sous-groupes et de sous-variétés I. Prépublication de l'Institut Fourier no. 626, octobre 2003.

[13] D. Roy et J.-L. Thunder An absolute Siegel's lemma. In *J. Reine Angew. Math.*, volume 476, pages 1–26, 1996.

[14] W. Schmidt. *Diophantine approximations and Diophantine equations*, volume 1467 of *Lecture Notes in Matematics*. Springer-Verlag, 1991.

[15] J. Silverman. A Lower Bound for the Canonical Height on Elliptic Curves over Abelian Extensions. In *J. Number Theory*, volume 104, pages 353–372, 2004.

[16] J. H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*, volume 156. Springer, 1999.

[17] J. Tate. The arithmetic of elliptic curves. In *Invent. Math.*, volume 23, pages 179–206, 1974.

[18] E. Viada. The intersection of a curve with algebraic subgroups in a product of elliptic curves. In *Ann. Scuola Norm. Pisa Cl. Sci.* Série *(V)*, volume 2, pages 47–75, 2003.

**Adress :** RATAZZI Nicolas
Université Paris 6 Institut de Mathématiques
Projet Théorie des nombres
Case 247
4, place Jussieu
75252 Paris Cedex 05
FRANCE
email : ratazzi@math.jussieu.fr