ACTA ARITHMETICA
Online First version

Problème de Lehmer sur les courbes elliptiques à multiplications complexes

par

Bruno Winckler (Lyon)

Table des matières

1. Introduction

1.1. Problème de Lehmer et théorème principal. Soit E/K une courbe elliptique, où K est un corps de nombres dont l'anneau des entiers est noté $\mathcal{O}_K$, et dont on fixe une clôture algébrique $\bar{K}$; posons $B = \mathrm{Spec}(\mathcal{O}_K)$, et soit $\mathcal{E} \to B$ le modèle minimal régulier de E, dont la section neutre est notée O. On cherche à minorer la hauteur de Néron–Tate d'un point algébrique P de E/K qui n'est pas de torsion, et qui s'étend en une section $\mathcal{P} : \mathrm{Spec}(\mathcal{O}_{K(P)}) \to \mathcal{E}$ telle que $\mathcal{P}(0) = P$.

2010 *Mathematics Subject Classification*: Primary 11G50, 14G40 ; Secondary 11M06.
Key words and phrases: Lehmer problem, Néron–Tate, canonical height, elliptic curves, complex multiplication, Arakelov geometry, arithmetic intersection, Dirichlet L-functions, Faltings height.
Received 4 April 2017.
Published online *.

Cette hauteur $\hat{h} : E(\bar{K}) \to \mathbb{R}$ a pour propriétés d'être positive et d'avoir précisément, comme lieu d'annulation, le sous-groupe de torsion de la courbe elliptique. Une problématique récurrente en géométrie diophantienne est la minoration uniforme de cette fonction sur une famille de courbes elliptiques (en dehors des sous-groupes de torsion) ; énonçons par exemple la conjecture de Lang (voir [Lan78]), qui s'attend à ce que pour tout corps de nombres K, il existe une minoration uniforme pour toute courbe elliptique définie sur K, de la forme

$$\hat{h}(P) \geq c(K) \max\big(\ln(\mathrm{N}_{K/\mathbb{Q}}(\Delta(E/K))), h(j_E)\big),$$

pour tout point $P \in E(K)$ d'ordre infini, où $c(K)$ est une constante ne dépendant que de K, $\Delta(E/K)$ le discriminant minimal de E/K, et $h(j_E)$ la hauteur naïve de l'invariant modulaire j_E de la courbe E.

Une autre question se pose si, cette fois, on fixe la courbe elliptique E/K, et qu'on laisse toute liberté au corps de rationalité du point P d'ordre infini dont on estime la hauteur. On pense qu'il existe une constante $c(E/K)$ strictement positive telle que pour tout $P \in E(\bar{K})$ qui n'est pas de torsion, on ait

$$\hat{h}(P) \geq \frac{c(E/K)}{D},$$

où on a posé $D = [K(P) : K]$; il s'agit de la conjecture de Lehmer pour les courbes elliptiques. Notons que la formulation équivalente pour la hauteur des nombres algébriques est encore conjecturale à ce jour.

Le meilleur résultat général actuellement connu est dû à Masser, suivant une méthode de comptage qui a ensuite été reprise plusieurs fois dans des estimations de hauteurs (voir [Pet06], ou [GM17] par exemple).

Théorème (Masser [Mas89]). *Soit E/K une courbe elliptique. Il existe une constante $c(E/K) > 0$ telle que pour tout point $P \in E(\bar{K})$ d'ordre infini, de degré $D = [K(P) : K]$, on ait*

$$\hat{h}(P) \geq \frac{c(E/K)}{D^3(\ln(2D))^2}.$$

Hindry et Silverman montrent même dans [HS99] que si E/K a bonne réduction partout, alors $\hat{h}(P) \geq (10^{18} D'^3(\ln(2D'))^2)^{-1}$ où $D' = [\mathbb{Q}(P) : \mathbb{Q}]$. Il est intéressant de remarquer que la minoration ne dépend pas de E.

Si E/K admet des places de mauvaise réduction multiplicative, alors on peut améliorer cette inégalité :

Théorème (David [Dav97]). *Soit E/K une courbe elliptique dont le j-invariant n'est pas un entier algébrique. Il existe une constante $c(E/K) > 0$ telle que pour tout point $P \in E(\bar{K})$ d'ordre infini, de degré $D = [K(P) : K]$, on ait*

$$\hat{h}(P) \geq \frac{c(E/K)}{D^{15/8}(\ln(2D))^2}.$$

Enfin, notons que la conjecture de Lehmer a récemment été démontrée pour les points qui engendrent une extension galoisienne de K.

Théorème (Galateau et Mahé [GM17]). *Soit E/K une courbe elliptique. Il existe une constante $c(E/K) > 0$ telle que pour tout point $P \in E(\bar{K})$ d'ordre infini tel que $K(P)/K$ soit une extension galoisienne, on ait*

$$\hat{h}(P) \geq \frac{c(E/K)}{[K(P) : K]}.$$

Cette publication propose d'autres résultats analogues si le groupe de Galois de la clôture galoisienne n'est pas trop « gros ».

Autrement, le résultat le plus proche de celui espéré est, pour le moment, sur les courbes elliptiques à *multiplications complexes*, c'est-à-dire celles dont l'anneau d'endomorphismes contient strictement les multiplications par des entiers relatifs. Laurent [Lau83] démontre que pour tout point P d'ordre infini

$$\hat{h}(P) \geq \frac{c(E/K)}{D}\left(\frac{\ln(\ln(3D))}{\ln(2D)}\right)^3, \tag{1}$$

où $c(E/K)$ est une constante théoriquement effective, dépendant d'une version explicite du théorème de densité de Chebotarev. En particulier, pour tout $\varepsilon > 0$, on a $\hat{h}(P) \geq c(E/K, \varepsilon)/D^{1+\varepsilon}$, pour une constante appropriée $c(E/K, \varepsilon)$ théoriquement effective.

On se propose de démontrer une inégalité de cette nature en interprétant la hauteur de Néron–Tate en termes d'intersection sur les surfaces arithmétiques, grâce au théorème 2.5 ; selon les affinités du lecteur, ce théorème peut même faire office de définition de la hauteur de Néron–Tate. Notre approche a l'avantage d'être géométriquement intrinsèque – il n'y a notamment pas de recours à la hauteur naïve ni de choix de coordonnées projectives à faire – et de fournir une constante explicite éclaircissant la dépendance en la courbe elliptique. Appelons « HRG » l'hypothèse de Riemann généralisée. L'énoncé du théorème principal est le suivant :

Théorème 1.1. *Soit E/K une courbe elliptique à multiplications complexes, sur un corps de nombres K de degré n_K sur $\mathbb{Q}$. Pour tout point $P \in E(\bar{K})$ d'ordre infini, de degré $D = [K(P) : K]$, on a*

$$\hat{h}(P) \geq \frac{c(E/K)}{6D}\left(\frac{\ln(\ln(24D))}{\ln(24D)}\right)^3, \tag{2}$$

où on peut prendre

$$c(E/K)^{-1} = 10^{-30} e^{e^{1{,}3\cdot 10^7 n_K^2 (h_{F^+}(E/K)+1)}}\left(1 + 10^{-4754} e^{e^{1{,}3\cdot 10^7 n_K^2 (h_{F^+}(E/K)+1)}}\right)$$

avec $h_{F^+}(E/K)$ la hauteur de Faltings définie en (9)*. Si HRG est supposée*

vraie, alors on peut même prendre

$$c(E/K)^{-1} = c(K)^{-1} = 2{,}4 \cdot 10^{32} n_K^{13,5} (\ln(n_K e^{109}))^{10}.$$

En vérité, la minoration peut ne dépendre que de n_K même sans supposer que HRG est vraie, mais elle n'est plus effective : voir la remarque 2.19 à ce propos.

L'essence de la démonstration réside dans la comparaison entre la hauteur de Néron–Tate et l'intersection arithmétique sur le modèle minimal régulier de la courbe elliptique, permise par le théorème 2.5 (dû à Faltings et Hriljac) et le corollaire 2.7 ; une conséquence particulière de ces résultats est la négativité de l'auto-intersection d'un diviseur de la courbe elliptique. Une combinaison linéaire convenable de diviseurs liés au point dont on veut estimer la hauteur permet donc, en utilisant ce fait, de comparer cette hauteur à des calculs d'intersections locales impliquant le point en question et des images de ce point par des Frobenius de la courbe elliptique. Ces endomorphismes sont d'un intérêt tout particulier, parce qu'on connaît précisément les points qui coupent leur image par un Frobenius au-dessus de son idéal maximal associé, grâce au petit théorème de Fermat. Les intersections locales aux places archimédiennes sont évaluées à l'aide d'une version affinée du lemme d'Elkies.

Afin de ne pas obscurcir plus que de raison la démonstration du théorème 1.1, nous supposons que l'hypothèse de Riemann généralisée est vraie dans la troisième section. Nous verrons comment obtenir une borne un peu moins heureuse en toute généralité.

1.2. Stratégie de démonstration. Nous estimons la hauteur de Néron–Tate d'un point par des estimations locales en chaque place v de K ; à cet égard, notre approche rappelle celle de Hindry et Silverman [HS99], par exemple, même si le vocabulaire n'est pas le même. En effet, la hauteur de Néron–Tate $\hat{h}(P)$ peut s'exprimer comme somme de termes locaux notés $\lambda_v(P)$, qui mesurent en quelque sorte la distance v-adique de P au point O. Hindry et Silverman passent par la minoration de sommes de la forme

$$\sum_{\sigma \neq \tau} \lambda_v(P^\sigma - P^\tau)$$

où les $\sigma, \tau : K(P) \hookrightarrow \bar{K}$ sont certains plongements. Le cas ultramétrique est directement réglé, tandis que le cas archimédien s'obtient par un lemme dû à Elkies, qu'on peut interpréter comme un résultat explicite d'équirépartition. En sommant toutes les contributions, ils obtiennent leur minoration de l'ordre de $D^{-3}(\ln(2D))^{-2}$.

Pour améliorer l'inégalité qu'ils ont produite, on utilise ici une propriété propre aux courbes elliptiques à multiplications complexes, afin d'ob-

tenir une estimation plus fine aux places finies : l'existence des relèvements de Frobenius. En termes d'intersection arithmétique, on considérera l'auto-intersection du diviseur $\mathcal{L}$ défini par

$$\mathcal{L} = \sum_{i=0}^{r} m_i\big((\mathrm{F}_{p_i}(\mathcal{P})) - D\cdot(\mathcal{O})\big),$$

où les F_{p_i} sont différents relèvements de Frobenius relatifs à des nombres premiers rationnels p_i, et m_i des entiers convenablement choisis en fin de démonstration (le diviseur $\mathcal{L}$ apparaît implicitement dans la démonstration de l'inégalité (1) dans [Lau83], bien que l'approche soit conceptuellement très différente). Ce qu'il importe provisoirement de savoir est qu'un théorème dû à Faltings et Hriljac nous donne une inégalité non triviale, liant la fonction de hauteur de Néron–Tate aux intersections d'itérés du point P :

$$2D^2 n_{K'}\Big(\sum_{i=0}^{r} m_i\Big)\Big(\sum_{j=0}^{r} m_j p_j\Big)\hat{h}(P) \geq \sum_{0\leq i,j\leq r} m_i m_j \langle \mathrm{F}_{p_i}(\mathcal{P}), \mathrm{F}_{p_j}(\mathcal{P})\rangle. \tag{3}$$

La façon de traiter les intersections aux places archimédiennes est classique, et passe par le lemme d'Elkies ; seulement, il faut ici en obtenir une version plus générale, entre autres pour englober le cas de points algébriques : c'est l'objet du lemme 3.4. La réelle nouveauté réside dans l'estimation des intersections aux places ultramétriques, explicitée dans le lemme 3.3, et qui fait intervenir une nouvelle somme indexée par des nombres premiers bien choisis, qu'on minore avec soin grâce à une version explicite du théorème de densité de Chebotarev [Win15, théorèmes 1.7 et 1.8]). On conclut grâce à un bon choix de paramètres m_i, qui cherche à maximiser la minoration de la hauteur obtenue.

Toutes ces estimations font apparaître trois types de quantités dans la minoration finale de la hauteur : celles liées à la réduction au cas d'une courbe elliptique E'/K' avec bonne réduction partout et $\mathrm{End}_{\bar{K}'}(E') = \mathrm{End}_{K'}(E')$ (d'où les quantités $\ln(-d)$, f et N_E, où $-df^2$ est le discriminant de $\mathrm{End}(E)$ et N_E la norme du conducteur de E), celles liées aux sommes indexées par des nombres premiers rationnels particuliers (d'où les quantités provenant du terme d'erreur dans le théorème de Chebotarev : n_K et $\ln(d_K)$), et enfin celles liées à la contribution négative des places archimédiennes, par le lemme d'Elkies (d'où la dépendance en $h(j_E)$ et D). Nous allons montrer qu'en vérité, pouvant comparer toutes ces quantités à n_K (sauf D, bien entendu), il est possible d'obtenir une minoration de la hauteur ne dépendant que de n_K et D, du moins si on suppose que l'hypothèse de Riemann généralisée est vraie. Ceci achèvera la démonstration du théorème 1.1.

Pour résumer, et pour justifier la structure de cet article :

— À isogénie près, on peut se ramener au cas d'une courbe elliptique à bonne réduction partout dont l'anneau d'endomorphismes est l'anneau

des entiers d'un corps quadratique, et dont les relèvements de Frobenius sont définis sur le corps de définition de la courbe ; toutes les propriétés nécessaires des courbes elliptiques à multiplications complexes, qui justifient cette réduction, sont exposées dans la sous-section 2.2.

— Des propriétés de l'intersection arithmétique, et son lien à la hauteur de Néron–Tate, permettent d'obtenir l'inégalité non triviale (3), où il suffit ensuite de minorer les intersections locales entre les images de P par des relèvements de Frobenius, pour obtenir une minoration de la hauteur de Néron–Tate de P ; on rappelle ces propriétés et ce lien dans la sous-section 2.1.

— La démonstration esquissée ci-dessus est pleinement développée dans la section 3.

— Certaines estimations font appel à des résultats sophistiqués de la théorie analytique des nombres : en particulier celles des sommes indexées par des nombres premiers (lemmes 3.5 et 3.9), et de la hauteur du j-invariant dans la sous-section 2.2 ; les estimations analytiques étant longues et écartées de notre préoccupation principale, elles sont reportées à la section 4.

Le lecteur rompu aux techniques de géométrie invoquées, et ne s'intéressant qu'à la démonstration du théorème principal, peut donc se contenter de la section 3. Il nous semble cependant que la proposition 2.16 et le corollaire 2.18 sont pourvus d'intérêt en soi, la premiere parce qu'elle explicite le rapport entre la hauteur de Faltings d'une courbe elliptique et le logarithme du discriminant de son anneau d'endomorphismes, et le deuxième parce qu'il compare toutes les quantités naturellement liées à une courbe elliptique à des fonctions ne dépendant que du degré de son corps de définition, pourvu que la courbe ait des multiplications complexes.

2. Définitions, résultats préliminaires

2.1. Hauteur et intersection arithmétique. Si K est un corps de nombres de degré n_K, on note M_K l'ensemble de ses places ($M_K^0 \subseteq M_K$ se restreint aux places ultramétriques, et M_K^∞ aux places archimédiennes), et pour tout $v \in M_K$ la valeur absolue associée à v est notée $|\cdot|_v$ (normalisée par $|p|_v = 1/p$ si v divise p, et prolongeant la valeur absolue usuelle de $\mathbb{Q}$ si v divise ∞). Alors, pour tout point $P = (x_0 : \cdots : x_n)$ de l'espace projectif $\mathbb{P}^n(K)$, la *hauteur naïve* de P est définie par

$$h(P) = \frac{1}{n_K} \sum_{v \in M_K} n_v \ln\Big(\max_{0 \leq i \leq n} (|x_i|_v)\Big),$$

où $n_v = [K_v : \mathbb{Q}_v]$. On vérifie que $h(P)$ ne dépend ni du choix des coordonnées projectives de P, ni du choix du corps de rationalité K. Si x est un nombre algébrique, on pose $h(x) = h([x : 1])$. Si, à présent, on considère

une courbe elliptique E, plongée dans $\mathbb{P}^2$ par le choix d'un modèle de Weierstrass défini sur K, alors on définit la *hauteur de Néron–Tate* d'un point P de $E(\bar{K})$ par la formule

$$\hat{h}(P) = \lim_{n\to\infty} \frac{h([2^n]P)}{4^n},$$

où $[2^n] : E \to E$ représente la multiplication. On résume, dans la proposition suivante, les propriétés de $\hat{h}$ qui nous serviront pour notre théorème principal.

Proposition 2.1 ([HS00, théorèmes B.4.1 et B.5.6]). *La hauteur de Néron–Tate $\hat{h} : E(\bar{K}) \to \mathbb{R}$ vérifie les propriétés suivantes :*

- *la valeur de $\hat{h}(P)$, pour $P \in E(\bar{K})$, ne dépend pas du corps de rationalité de P considéré ;*
- *elle est invariante par conjugaison : si $P \in E(\bar{K})$ et $\sigma : K(P) \hookrightarrow \bar{K}$ est un plongement, alors $\hat{h}(P) = \hat{h}(P^\sigma)$;*
- *elle induit une forme quadratique définie positive sur $E(\bar{K}) \otimes \mathbb{Q}$, donc également un produit scalaire $(\cdot|\cdot)$ défini par la formule*

$$(P|Q) = \tfrac{1}{2}(\hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q));$$

- *pour tout endomorphisme non nul ϕ de la courbe elliptique E et tout point $P \in E(\bar{K})$, on a $\hat{h}(\phi(P)) = \deg(\phi)\hat{h}(P)$.*

On se permettra, par la suite, d'amalgamer l'accouplement bilinéaire défini ci-dessus sur $E(\bar{K})$ et celui défini sur $\mathrm{Div}^0(E)$ par $((P)-(O)|(Q)-(O)) = (P|Q)$ puis étendu par linéarité. Cet accouplement a également une interprétation géométrique arakélovienne, comme on le verra bientôt. Le nombre d'intersection au sens d'Arakelov est obtenu par calcul d'intersection dans les fibres de chaque place finie avec, en plus, une contribution aux « fibres à l'infini ». Par commodité, on note dorénavant $\sigma : L \hookrightarrow \bar{K}$ les morphismes de corps $\sigma : L \to \bar{K}$ qui fixent K (ce dernier aspect est donc désormais implicite).

Sans donner en détail toutes les définitions nécessaires à l'introduction de l'intersection sur les surfaces arithmétiques, mentionnons au moins les formules dont on aura besoin. Les intersections locales aux places finies de deux points mesurent, en un certain sens, la proximité $\mathfrak{p}$-adique des coordonnées de ces points. En particulier, l'intersection en $\mathfrak{p}$ de deux points sera strictement positive si et seulement si ces points se coupent dans la fibre au-dessus de $\mathfrak{p}$.

Définition 2.2 (Intersection en une place finie). Soient $\mathcal{D}_1, \mathcal{D}_2$ deux diviseurs horizontaux de $\mathcal{E}$. Notons v une place finie, et $\mathfrak{p}$ l'idéal maximal associé. Pour chaque point x dont le corps résiduel $k(x)$ est une extension finie de $\mathcal{O}_K/\mathfrak{p}$, soient f et g des équations locales (autour de x) pour $\mathcal{D}_1$ et $\mathcal{D}_2$ respectivement. On définit le *nombre d'intersection* de $\mathcal{D}_1$ et $\mathcal{D}_2$ en x, noté

$i_x(\mathcal{D}_1, \mathcal{D}_2)$, comme étant la longueur de $\mathscr{O}_x/(f,g)$ vu comme $\mathscr{O}_x$-module. Alors,

$$\langle \mathcal{D}_1, \mathcal{D}_2 \rangle_v = \langle \mathcal{D}_1, \mathcal{D}_2 \rangle_{\mathfrak{p}} = \sum_{x|v} i_x(\mathcal{D}_1, \mathcal{D}_2) \ln(|k(x)|).$$

Voici comment traduire, plus concrètement, cette définition. D'après [Lan88, propriété « INT 3 », p. 73], la somme des intersections en toutes les places finies de deux diviseurs horizontaux donnés par $\mathcal{P}_1, \mathcal{P}_2 : \mathrm{Spec}(\mathcal{O}_L) \to \mathcal{E}$ égale

$$\sum_{\mathfrak{p}} \langle \mathcal{P}_1, \mathcal{P}_2 \rangle_{\mathfrak{p}} = \sum_{\sigma : L \hookrightarrow \bar{K}} \mathrm{ord}_{P_1^\sigma}(\mathcal{P}_2) \ln(|k(P_1^\sigma)|), \tag{4}$$

où ord_P est la valuation définie sur le germe en P (qui est un anneau de valuation discrète). Autrement dit, comme $\mathcal{P}_2 \otimes \bar{K}_{\mathfrak{p}}$ se décompose en somme de conjugués P_2^τ, la quantité $\mathrm{ord}_{P_1^\sigma}(\mathcal{P}_2)$ est strictement positive si, et seulement si, un des conjugués P_2^τ coïncide avec P_1^σ modulo un idéal maximal.

Notons au passage que si on considère une extension L de K, v une place de K et $w \,|\, v$ une place de L, alors $\langle \cdot, \cdot \rangle_w = [L_w : K_v] \langle \cdot, \cdot \rangle_v$. Donc l'intersection en v est strictement positive si et seulement si celle en w l'est.

L'intersection à une place infinie passe par la définition des fonctions de Néron (ou de Green–Arakelov), qu'on normalise comme dans [Lan88].

Définition 2.3 (Fonction de Néron). Fixons un isomorphisme entre $E(\bar{K}_v)$ et $\mathbb{C}/(\mathbb{Z} + \tau_v \mathbb{Z})$, où $\tau_v \in \mathbb{C}$ vérifie $\mathrm{Im}(\tau_v) > 0$. La fonction $\lambda_v : \mathbb{C}/(\mathbb{Z} + \tau_v \mathbb{Z}) \setminus \{0\} \to \mathbb{R}$ est définie par

$$\lambda_v(z) = -\frac{1}{2} B_2\left(\frac{\ln(|u|)}{\ln(|q|)}\right) \ln(|q|) - \ln(|1-u|) - \sum_{n=1}^{\infty} \ln\left(\left|(1-q^n u)\left(1 - \frac{q^n}{u}\right)\right|\right),$$

où $u = e^{2i\pi z}$, $q = e^{2i\pi\tau_v}$, tandis que $B_2 = X^2 - X + 1/6$ est le deuxième polynôme de Bernoulli.

On peut montrer que λ_v est continue sur son domaine de définition, et a une singularité logarithmique en 0. Encore une fois, donc, l'intersection en une place v de deux points (qui sera, essentiellement, définie à l'aide de λ_v) mesure la proximité v-adique entre ces deux points sur le tore $E(\bar{K}_v)$.

Suivant la définition donnée dans [Lan88, p. 74], l'intersection de deux diviseurs horizontaux irréductibles $\mathcal{P}_1$ et $\mathcal{P}_2$ en une place archimédienne v est donnée par

$$\langle \mathcal{P}_1, \mathcal{P}_2 \rangle_v = n_v \sum_{\sigma,\tau} \lambda_v(P_1^\sigma - P_2^\tau),$$

où, donc, $\mathcal{P}_1 \otimes_{v,B} \mathbb{C} = \sum_\sigma (P_1^\sigma)$ et de même pour $\mathcal{P}_2$. On peut la définir pour des diviseurs quelconques sans composante commune, mais cela ne sera pas nécessaire dans notre étude.

En sommant l'ensemble des intersections locales, on obtient une intersection globale qui s'étend, en vérité, à l'ensemble des diviseurs d'Arakelov. Dans le théorème suivant, $\widehat{\mathrm{Div}(\mathcal{E})}$ et $\widehat{\mathrm{Cl}(\mathcal{E})}$ désignent respectivement le groupe des diviseurs d'Arakelov et le groupe des diviseurs d'Arakelov modulo la relation d'équivalence linéaire.

Théorème 2.4 (Intersection globale). *Il existe un accouplement bilinéaire symétrique* $\langle\cdot,\cdot\rangle_K : \widehat{\mathrm{Div}(\mathcal{E})} \times \widehat{\mathrm{Div}(\mathcal{E})} \to \mathbb{R}$*, dit nombre d'intersection. Il se factorise à travers la relation d'équivalence linéaire, et définit donc un nombre d'intersection* $\widehat{\mathrm{Cl}(\mathcal{E})} \times \widehat{\mathrm{Cl}(\mathcal{E})} \to \mathbb{R}$*. Si* $\mathcal{D}_1$ *et* $\mathcal{D}_2$ *sont deux sections distinctes, on a* $\langle \mathcal{D}_1, \mathcal{D}_2\rangle_K = \sum_{v\in M_K} \langle \mathcal{D}_1, \mathcal{D}_2\rangle_v$.

Toutes les propriétés de base de l'intersection au sens d'Arakelov sont, par exemple, présentées dans [Lan83] ou [Lan88] ; notons-en une en particulier : si L/K est une extension de corps finie et $\mathcal{E}'$ le modèle minimal régulier de $E \otimes_K \mathrm{Spec}(L)$, alors notant g le morphisme canonique $\mathcal{E}' \to \mathcal{E}$, on a

$$\langle g^*(\mathcal{D}_1), g^*(\mathcal{D}_2)\rangle_L = [L : K]\langle \mathcal{D}_1, \mathcal{D}_2\rangle_K. \tag{5}$$

Pour un diviseur $\mathcal{D} \in \mathrm{Div}(\mathcal{E})$ de degré nul, il existe un diviseur vertical $[\mathcal{D}] \in \mathrm{Div}(\mathcal{E}) \otimes \mathbb{Q}$, unique modulo les fibres, tel que l'intersection de $\mathcal{D} + [\mathcal{D}]$ avec tout diviseur vertical soit nul. Le point de départ de la démonstration du théorème principal est alors le théorème suivant :

Théorème 2.5 (Faltings [Fal84], Hriljac [Hri85]). *Soit E une courbe elliptique définie sur un corps de nombres K, et $\mathcal{E} \to B$ son modèle minimal régulier. Notons $(\cdot|\cdot)$ l'accouplement bilinéaire associé à la hauteur de Néron–Tate de E. Alors, pour tous diviseurs $D_1, D_2 \in \mathrm{Div}(E)(L)$ de degré nul, dont on note $\mathcal{D}_1$ et $\mathcal{D}_2$ l'adhérence dans $\mathcal{E}$, on a*

$$\langle \mathcal{D}_1 + [\mathcal{D}_1], \mathcal{D}_2 + [\mathcal{D}_2]\rangle_K = -2[L : \mathbb{Q}](D_1|D_2).$$

Si $\mathcal{E} \to B$ est lisse, alors $[\mathcal{D}] = 0$ pour tout diviseur $\mathcal{D} \in \mathrm{Div}(\mathcal{E})$ de degré nul. En effet, il suffit dans ce cas de le vérifier pour chaque fibre, laquelle est un diviseur principal (celui d'une uniformisante), donc son intersection avec $\mathcal{D}$ est nulle.

On a donc fait le lien entre la hauteur de Néron–Tate sur une courbe elliptique et l'intersection arithmétique. Si $\mathcal{D}_1 = \mathcal{D}_2$, on se retrouve avec une auto-intersection. Mentionnons le résultat suivant, qui est très pratique pour calculer les auto-intersections :

Théorème 2.6 (Formule d'adjonction). *Soit E une courbe elliptique définie sur un corps de nombres K, soit $\mathcal{E} \to B$ son modèle minimal régulier et $\mathcal{Q} : \mathrm{Spec}(\mathcal{O}_L) \to \mathcal{E}$ un diviseur horizontal. Notant $\mathrm{K}_{E/K}$ le diviseur canonique (d'Arakelov) de E/K, on a*

$$\langle \mathcal{Q}, \mathrm{K}_{E/K}\rangle_K + \langle \mathcal{Q}, \mathcal{Q}\rangle_K = \mathrm{d}_{\mathcal{Q}/L} + \sum_{v\in M_K^\infty} n_v \sum_{\substack{\sigma,\tau: L\hookrightarrow \bar{K}\\ \sigma\neq\tau}} \lambda_v(Q^\sigma - Q^\tau), \tag{6}$$

où $\mathrm{d}_{\mathcal{Q}/L} \geq 0$ *est le logarithme du discriminant de* $\mathcal{Q}/L$ (*voir* [Lan88, p. 97] *pour une définition*). *En particulier, si* $L = K$, *le membre de droite est nul et* $\langle \mathcal{Q}, \mathcal{Q}\rangle_K = -\langle \mathcal{Q}, \mathrm{K}_{E/K}\rangle_K$.

Les théorèmes 2.5 et 2.6 permettent d'écrire une autre relation entre hauteur canonique et intersection.

Corollaire 2.7. *Soit* E *une courbe elliptique définie sur un corps de nombres* K *ayant bonne réduction partout, et* $\mathcal{E} \to B$ *son modèle minimal régulier, de section neutre* O. *Alors, pour tout point* $Q \in E(\bar{K})$ *qui induit* $\mathcal{Q} : \mathrm{Spec}(\mathcal{O}_{K(Q)}) \to \mathcal{E}$, *on a*

$$\hat{h}(Q) = \frac{\langle \mathcal{Q}, O\rangle_K}{[K(Q):\mathbb{Q}]}. \tag{7}$$

Démonstration. Notons $L = K(Q)$. On se ramène par changement de base au cas où $\mathcal{Q}$ est une section d'un modèle minimal régulier $\mathcal{E}'/\mathcal{O}_L$; ceci n'affecte pas le calcul de $\hat{h}(Q)$, car la hauteur est invariante par extension de corps. Donc $\langle \mathcal{Q}, \mathcal{Q}\rangle_L = -\langle \mathcal{Q}, \mathrm{K}_{\mathcal{E}'/\mathcal{O}_L}\rangle_L$ par la formule d'adjonction énoncée dans le théorème 2.6, et il est démontré dans [Szp90, théorème 2] que si E a réduction semi-stable, alors

$$\langle \mathcal{Q}, \mathrm{K}_{\mathcal{E}'/\mathcal{O}_L}\rangle_L = \tfrac{1}{12}\ln(|\mathrm{N}_{L/\mathbb{Q}}(\Delta(E/L))|). \tag{8}$$

Ici, $\Delta(E/L) = \mathcal{O}_L$, donc finalement l'auto-intersection de toute section de $\mathcal{E}' \to \mathrm{Spec}(\mathcal{O}_L)$ est nulle. De fait, en appliquant le théorème 2.5 aux diviseurs $D_1 = D_2 = (Q) - (\mathcal{O}')$ (on a noté $\mathcal{O}'$ la section neutre de $\mathcal{E}' \to \mathrm{Spec}(\mathcal{O}_L)$), on obtient

$$\begin{aligned} 2[L:\mathbb{Q}]\hat{h}(Q) &= -\langle \mathcal{Q} - \mathcal{O}', \mathcal{Q} - \mathcal{O}'\rangle_L = -\langle \mathcal{Q}, \mathcal{Q}\rangle_L - \langle \mathcal{O}', \mathcal{O}'\rangle_L + 2\langle \mathcal{Q}, \mathcal{O}'\rangle_L \\ &= 2\langle \mathcal{Q}, \mathcal{O}'\rangle_L. \end{aligned}$$

On a le résultat voulu grâce à la formule (5) du changement de base. En effet, comme la hauteur canonique est invariante par conjugaison,

$$\begin{aligned} 2[L:\mathbb{Q}]\hat{h}(Q) &= 2[K:\mathbb{Q}] \sum_{\sigma: L\hookrightarrow\bar{K}} \hat{h}(Q^\sigma) = \frac{2}{[L:K]} \sum_{\sigma: L\hookrightarrow\bar{K}} \langle \mathcal{Q}^\sigma, \mathcal{O}'\rangle_L \\ &= \frac{2}{[L:K]}\langle r^*(\mathcal{Q}), r^*(\mathcal{O})\rangle_L = 2\langle \mathcal{Q}, \mathcal{O}\rangle_K. \ \blacksquare \end{aligned}$$

2.2. Courbes elliptiques à multiplications complexes

2.2.1. *Endomorphismes*

Définition 2.8 (Multiplications complexes). Soit E/K une courbe elliptique définie sur un corps de nombres. On dit que E admet des *multiplications*

complexes si $\mathbb{Z} \subsetneq \mathrm{End}(E)$, c'est-à-dire s'il existe d'autres endomorphismes que les multiplications par des entiers.

Si E/K est une courbe elliptique, on sait [Sil09, VI.5.5] que $\mathrm{End}(E) \otimes \mathbb{Q}$ est isomorphe soit à $\mathbb{Q}$ (si $\mathrm{End}(E)$ ne contient que les multiplications $[n]$ par des entiers), soit à un corps quadratique imaginaire de discriminant d, et dans ce cas $\mathrm{End}(E)$ est un ordre de ce corps : il existe un unique entier $f \geq 1$, appelé le *conducteur* de $\mathrm{End}(E)$ (à ne pas confondre avec le conducteur de E), tel que

$$\mathrm{End}(E) \simeq \mathbb{Z} + f\mathcal{O}_{\mathbb{Q}(\sqrt{d})}.$$

On dit alors que E/K admet des *multiplications complexes* par le corps $\mathbb{Q}(\sqrt{d})$, ou par l'anneau $\mathbb{Z} + f\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ si cette précision est nécessaire. Il est important de ne pas perdre de vue que dans cet article, d désignera toujours le discriminant du corps de nombres $\mathrm{End}(E) \otimes \mathbb{Q}$ (il n'est donc *a priori* pas sans facteur carré, contrairement à l'usage quand on manipule $\mathbb{Q}(\sqrt{d})$).

Il existe toujours une courbe elliptique définie sur K et isogène à E/K, telle que son anneau d'endomorphismes soit exactement $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$: si f est le conducteur de $\mathrm{End}(E) \simeq \mathbb{Z}+f\mathbb{Z}[x]$, il suffit de prendre l'image du morphisme $E \to E^2$ défini par $P \mapsto ([f]P, [fx]P)$, où $[\cdot]$ est l'application de multiplication normalisée pour que $[\alpha]^*$ soit la multiplication par $\alpha \in \mathbb{Z}+f\mathbb{Z}[x]$ sur Ω_E, et l'isogénie obtenue est de degré f. Cette stratégie nous a été indiquée par Rémond [Rém17]. On en sait même davantage :

Proposition 2.9 ([GR14, proposition 10.1], [Rém17, théorème 1.1]). *Soit E/K une courbe elliptique à multiplications complexes par $\mathbb{Q}(\sqrt{d})$. Il existe une extension K' de K contenant $\mathbb{Q}(\sqrt{d})$, une courbe elliptique E'/K' à multiplications complexes par $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$, et une isogénie $\phi : E \to E'$ définie sur K' telles que*

$$\deg(\phi) \leq 30 n_K \max(1, h_F(E/K) + \ln(n_K)/2)$$

où $h_F(E/K)$ est la hauteur de Faltings de E/K (voir définition en (9) et (10)), et $[K' : K] \leq 2$.

De plus, une lecture attentive de sa démonstration permet de montrer

Proposition 2.10. *Soit E/K une courbe elliptique à multiplications complexes par un ordre de discriminant $-df^2$. Alors*

$$\sqrt{-d}\, f \leq 8\sqrt{167}\, n_K \max\bigl(1, h_F(E/K) + \ln(n_K)/2\bigr).$$

Démonstration. Dans la démonstration de [GR14, proposition 10.1], on compare le volume de $\mathrm{End}(E)$ avec le degré d'une certaine isogénie ψ : on a $\mathrm{vol}(\mathrm{End}(E)) \leq 2\sqrt{\deg(\psi)}$. Or, il est démontré dans cette même proposition que

$$\deg(\psi) \leq 668\bigl[n_K \max\bigl(1, h_F(E/K) + \ln(n_K)/2\bigr)\bigr]^2,$$

et on sait que le volume de $\mathrm{End}(E)$ égale $\sqrt{-d}\, f/2$. ∎

On peut donc supposer, dans beaucoup de situations, que $\mathrm{End}(E) = \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$.

On a énoncé qu'une courbe elliptique à multiplications complexes a d'autres endomorphismes que les multiplications par des entiers ; parmi ces multiplications complexes, certaines vont ici être privilégiées : les endomorphismes de Frobenius.

Théorème 2.11 (Relèvement du Frobenius [ST61, III.13, théorème 1]). *Soit E une courbe elliptique à multiplications complexes par $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$, définie sur un corps de nombres K. Supposons que K contient $\mathbb{Q}(\sqrt{d})$. Pour tout idéal premier $\mathfrak{p}$ de K de bonne réduction, il existe une unique isogénie $\mathrm{F}_\mathfrak{p} : E \to E$ définie sur K qui induit, modulo $\mathfrak{p}$, l'exponentiation à la puissance $\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p})$ sur la réduction de la courbe elliptique. On l'appelle* endomorphisme de Frobenius *de E associé à $\mathfrak{p}$, et il est de degré $\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p})$.*

En d'autres termes, il est possible de relever le Frobenius modulo $\mathfrak{p}$ sur une courbe elliptique à multiplications complexes.

2.2.2. *Le j-invariant.* La classe d'isomorphisme sur $\bar{K}$ d'une courbe elliptique E/K est caractérisée par une fraction rationnelle en les coefficients d'une équation intégrale de E, qu'on appelle le *j-invariant* et qu'on note j_E. Nous n'aurons pas besoin de définition plus précise dans notre exposé ; le lecteur intéressé peut se tourner vers [Sil09] par exemple.

En particulier, si E/K est une courbe elliptique à multiplications complexes, et de j-invariant j_E, il existe une courbe elliptique $E'/\mathbb{Q}(j_E)$ à multiplications complexes par le même corps quadratique, de même j-invariant, telle que E et E' soient isomorphes sur $\bar{K}$. Comme $j_E \in K$, on voit que $[\mathbb{Q}(j_E) : \mathbb{Q}] \leq n_K$. Les propriétés galoisiennes de cette extension sont de grande importance en théorie du corps de classe. On a en effet :

Théorème 2.12 ([Sil94, théorème 4.1]). *Soit E/K une courbe elliptique à multiplications complexes par $\mathbb{Q}(\sqrt{d})$, de j-invariant j_E. Alors l'extension $\mathbb{Q}(j_E, \sqrt{d})/\mathbb{Q}(\sqrt{d})$ est abélienne et non ramifiée.*

Dans le cas des courbes elliptiques, il est bien commode de pouvoir estimer des quantités liées à la courbe elliptique en fonction de la hauteur de son j-invariant. Selon les situations et les auteurs, une autre hauteur apparaît avec pertinence : il s'agit de la *hauteur de Faltings* h_{F^+}, qui est notamment d'une importance centrale dans la démonstration de la conjecture de Mordell, et qu'on peut définir pour une courbe elliptique par la formule

$$h_{F^+}(E/K) = \frac{1}{12n_K}\Big(\ln\big(\mathrm{N}_{K/\mathbb{Q}}(\Delta(E/K))\big) - \sum_{v\in M_K^\infty} n_v \ln\big(|\Delta(\tau_v)|(\mathrm{Im}(\tau_v))^6\big)\Big), \tag{9}$$

où $\Delta = q\prod_{n=1}^{\infty}(1-q^n)^{24}$ est le discriminant modulaire, et τ_v un nombre complexe du demi-plan supérieur tel que $E(\bar{K}_v) \simeq \mathbb{C}/(\mathbb{Z}+\tau_v\mathbb{Z})$; cette formule est donnée dans [CS86, proposition X.1.1] (où l'exposant de 2π doit être corrigé : voir par exemple [Fal84, théorème 7]). Quand on veut adopter un point de vue arakélovien, on peut préférer la normalisation originale de la hauteur de Faltings, notée $h_F(E/K)$, qui est définie comme le degré d'Arakelov normalisé du faisceau inversible $s^*\Omega_{\mathcal{E}/\mathcal{O}_K}$ sur $\mathcal{O}_K$ muni d'une structure de fibré en droites hermitien, où $s : \mathrm{Spec}(\mathcal{O}_K) \to \mathcal{E}$ est la section nulle du modèle minimal régulier de la courbe elliptique. Ce point de vue ne sera pas utilisé ici ; sachons néanmoins que ces deux hauteurs de Faltings ne diffèrent que d'une constante :

$$h_F(E/K) = h_{F^+}(E/K) + \ln(\pi)/2. \tag{10}$$

Ceci étant dit, nous voulons simplement en profiter pour montrer au lecteur que même si nous allons recourir à la hauteur du j-invariant dans l'inégalité de notre théorème principal, il peut se ramener sans difficulté à la hauteur de Faltings de la courbe elliptique, grâce à la proposition suivante.

Proposition 2.13. *Soit E/K une courbe elliptique. On peut écrire son j-invariant j_E comme le quotient de deux idéaux premiers entre eux, $(j_E) = \mathfrak{A}\mathfrak{D}^{-1}$, où $\mathfrak{D}$ est un diviseur de l'idéal $\Delta(E/K)$ (il y a même égalité dans le cas d'une courbe elliptique semi-stable). Posons $\mathfrak{Y}(E/K) = \Delta(E/K)\mathfrak{D}^{-1}$. La hauteur de son j-invariant et sa hauteur de Faltings sont alors reliées par les inégalités*

$$-6\ln(1+h(j_E)) - 4{,}22 \leq 12h_{F^+}(E/K) - h(j_E) \leq \frac{1}{n_K}\ln(\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{Y})) + 6{,}97.$$

Démonstration. Soit v une place archimédienne de K. Par uniformisation complexe, il existe un nombre τ_v tel que $|\mathrm{Re}(\tau_v)| \leq 1/2$, $\mathrm{Im}(\tau_v) \geq \sqrt{3}/2$ et $E(\bar{K}_v) \simeq \mathbb{C}/(\mathbb{Z}+\tau_v\mathbb{Z})$. On sait alors montrer d'une part, en recourant par exemple à [HS88, lemme 2.2] et à [BP05, lemme 24], que

$$-6 \leq \ln(\max(|j_E|_v, 1)) - 2\pi\,\mathrm{Im}(\tau_v) \leq 2{,}304,$$

et d'autre part, assez simplement, comme $\mathrm{Im}(\tau_v) \geq \sqrt{3}/2$,

$$|-2\pi\,\mathrm{Im}(\tau_v) - \ln(|\Delta(\tau_v)|)| \leq -24\sum_{n=1}^{\infty}\ln(1-e^{-\sqrt{3}\,\pi n}) \leq 0{,}105. \tag{11}$$

Partant de la formule (9), on obtient

$$\frac{1}{n_K}\ln(\mathrm{N}_{K/\mathbb{Q}}(\Delta(E/K))) + h_\infty(j_E) \\ - \frac{6}{n_K}\sum_{v\in M_K^\infty} n_v \ln(\ln(\max(|j_E|_v, e))) - 4{,}22 \leq 12h_{F^+}(E/K),$$

où l'on note $h_\infty(j_E) = n_K^{-1}\sum_{v\in M_K^\infty} n_v \max(\ln(|j_E|_v),0)$ par commodité, et

$$12h_{F^+}(E/K) \leq \frac{1}{n_K}\ln(\mathrm{N}_{K/\mathbb{Q}}(\Delta(E/K))) + h_\infty(j_E) + 6{,}97.$$

Il est facile de montrer que $n_K^{-1}\ln(\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{D})) + h_\infty(j_E) = h(j_E)$, et que

$$\begin{aligned}\sum_{v\in M_K^\infty} n_v \ln(\ln(\max(|j_E|_v,e))) &= \ln\Big(\prod_{v\in M_K^\infty}(\ln(\max(|j_E|_v,e)))^{n_v}\Big)\\ &\leq \ln\bigg(\sum_{v\in M_K^\infty} n_v \frac{\ln(\max(|j_E|_v,e))}{n_K}\bigg)^{n_K}\\ &\leq n_K\ln\bigg(1+\frac{1}{n_K}\sum_{v\in M_K^\infty} n_v\ln(\max(|j_E|_v,1))\bigg)\\ &\leq n_K\ln(1+h(j_E)),\end{aligned}$$

grâce à l'inégalité arithmético-géométrique, et on en déduit finalement les inégalités désirées. ∎

Corollaire 2.14. *Soit E/K une courbe elliptique de j-invariant j_E. On a*

$$h(j_E) \leq 12h_{F^+}(E/K) + 6\ln(0{,}76h_{F^+}(E/K)+1) + 24{,}85.$$

Démonstration. C'est une conséquence immédiate de la proposition précédente et du corollaire 4.18, puisque l'inégalité $h(j_E) - 6\ln(1+h(j_E)) \leq 12h_{F^+}(E/K) + 4{,}22$ équivaut à

$$\mathfrak{m}(-(h(j_E)+1)/6) \leq -\tfrac{1}{6}e^{-2h_{F^+}(E/K)-5{,}22/6}$$

(pour l'étude de $\mathfrak{m}$ et de ses fonctions réciproques $\mathrm{w}_{\pm1}$, voir la sous-section 4.2). Alors

$$\begin{aligned}h(j_E) &\leq 12h_{F^+}(E/K) + 8{,}22\\ &\quad + 6\Big(\ln(6) + \ln\big(\ln(6) + 5{,}22/6 + 2h_{F^+}(E/K)\big)\Big),\end{aligned}$$

d'où le résultat annoncé, après quelques simplifications menues. ∎

Nous disions qu'il est commode de relier la hauteur du j-invariant d'une courbe elliptique à des quantités qui lui sont naturellement associées. En particulier, remarquons qu'on peut relier le conducteur de E et le discriminant de $\mathrm{End}(E)$ à $h(j_E)$ (ou $h_{F^+}(E/K)$, ce qui revient au même d'après la proposition précédente).

Proposition 2.15. *Soit E/K une courbe elliptique de conducteur $\mathfrak{f}(E/K)$. On a*

$$\frac{1}{12n_K}\ln(\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{f}(E/K))) \leq h_{F^+}(E/K).$$

Démonstration. L'inégalité s'obtient directement partant de (9) et (11) ; on a $\ln(\mathrm{N}_{K/\mathbb{Q}}(\Delta(E/K))) \geq \ln(\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{f}(E/K)))$. ∎

Comparer $h_{F^+}(E/K)$ et $-df^2$ est plus délicat : une minoration de la hauteur par une quantité dépendant de $-df^2$ procède de la proposition 2.10, mais on peut aussi majorer en fonction de $-df^2$. Pour cela, notant $\mathrm{L}(\cdot,\chi)$ la fonction L de Dirichlet associée au caractère quadratique $\chi = \left(\frac{d}{\cdot}\right)$, et γ la constante d'Euler, on a l'égalité suivante (voir [Hab10, lemme 4.1] :

$$2h_F(E/K) = \tfrac{1}{2}\ln(-df^2) + \frac{\mathrm{L}'}{\mathrm{L}}(1,\chi) - \sum_{p|f} e_f(p)\ln(p) - \gamma - \ln(2\pi) \tag{12}$$

où

$$e_f(p) = \frac{1-\chi(p)}{p-\chi(p)}\,\frac{1-p^{-v_p(f)}}{1-p^{-1}}.$$

Habegger [Hab10] démontre que la somme portant sur les diviseurs premiers de f est dominée par $\ln(\ln(f))$, et on sait depuis longtemps que HRG implique $\frac{\mathrm{L}'}{\mathrm{L}}(1,\chi) \ll \ln(\ln(-d))$ (voir [GS00, p. 514]). On en déduit, sous réserve de la justesse de HRG, que

$$h_F(E/K) = \tfrac{1}{4}\ln(-df^2) + O(\ln(\ln(-df^2))).$$

Grâce à une version explicite du théorème de densité de Dirichlet pour les caractères réels, obtenue dans la section 4, nous pouvons obtenir une majoration plus précise.

Proposition 2.16. *Soit E/K une courbe elliptique à multiplications complexes par un ordre de discriminant $-df^2$. On a*

$$h_F(E/K) \leq 3{,}5\sqrt{-df^2}\,(\ln(-3df^2))^2 + 3{,}2\cdot 10^5.$$

Si HRG est supposée vraie, alors

$$h_F(E/K) \leq \tfrac{1}{4}\ln(-df^2) + 2{,}1\ln(\ln(-df^2)) + 102{,}2.$$

Démonstration. Comme $e_f(p) \geq 0$, tous les termes du membre de droite de (12) se majorent trivialement, sauf $\frac{\mathrm{L}'}{\mathrm{L}}(1,\chi)$. Si ψ_χ et ψ désignent respectivement les fonctions sommatoires de von Mangoldt associées à χ et 1 (voir section 4), alors d'après [RS62, formule (3.35)] on a

$$\psi(x)/x \leq 1{,}03883$$

pour tout $x > 0$, et le théorème 4.1 montre que, si on suppose HRG, alors

$$\psi_\chi(x) \leq \sqrt{x}\ln(x)\left[\frac{1}{2\pi}\ln(x) + \left(\frac{1}{\pi} + 2{,}88\right)\ln\left(\frac{-d}{2\pi}\right) + 57{,}76\right]$$

pour tout $x \geq 3$. On en déduit une majoration de la dérivée logarithmique de $\mathrm{L}(1,\chi)$:

$$\begin{aligned}\left|\frac{\mathrm{L}'}{\mathrm{L}}(1,\chi)\right| &= \left|-\sum_p\sum_{m=1}^{\infty}\frac{\chi(p^m)}{p^m}\ln(p)\right| \\ &\le \frac{\psi(\ln(-d)^4)}{(\ln(-d))^4} + \int_1^{(\ln(-d))^4}\frac{\psi(t)}{t^2}\,dt + \int_{(\ln(-d))^4}^{\infty}\frac{|\psi_\chi(t)|}{t^2}\,dt \\ &\le 4{,}15532\ln(\ln(-d)) + 204{,}231,\end{aligned}$$

toujours en supposant HRG. Si cette hypothèse n'est plus supposée vraie, alors toujours d'après le théorème 4.1, pour tout $x \ge \exp(6{,}5(\ln(-3d))^2)$,

$$|\psi_\chi(x)| \le \frac{x^{\beta_0}}{\beta_0} + 2200x\exp\left(-\frac{\sqrt{\ln(x)}}{10,2}\right),$$

où β_0 est l'éventuel zéro de Siegel de $\mathrm{L}(\cdot,\chi)$ (voir le théorème 4.14 pour une définition). Alors, reprenant le calcul précédent,

$$\begin{aligned}\left|\frac{\mathrm{L}'}{\mathrm{L}}(1,\chi)\right| &\le 1{,}03883\big(1+6{,}5(\ln(-3d))^2\big) \\ &\quad + \int_{\exp(6{,}5(\ln(-3d))^2)}^{\infty}\left(\frac{t^{\beta_0-1}}{\beta_0} + 2200\exp\left(-\frac{\sqrt{\ln(t)}}{10{,}2}\right)\right)\frac{dt}{t} \\ &\le 6{,}8(\ln(-3d))^2 + \frac{\exp\big(-6{,}5(1-\beta_0)(\ln(-3d))^2\big)}{\beta_0(1-\beta_0)} \\ &\quad + 4{,}58\cdot 10^5\frac{0{,}25\ln(-3d)+1}{\exp(0,25\ln(-3d))} \\ &\le 6{,}8(\ln(-3d))^2 + 3{,}3\sqrt{-d}\,(\ln(-ed))^2 + 4{,}6\cdot 10^5,\end{aligned}$$

où l'on a minoré $1-\beta_0$ grâce à la proposition 4.16, et on en déduit l'inégalité désirée pour $h_F(E/K)$, d'où le résultat inconditionnel. ∎

Remarque 2.17. Si $\frac{\mathrm{L}'}{\mathrm{L}}(1,\chi)$ est négatif, alors on peut améliorer la majoration (conditionnelle ou non), puisqu'on a simplement dans ce cas $h_F(E/K) \le \frac{1}{4}\ln(-df^2)$. C'est par exemple le cas si $\chi = \left(\frac{-4}{\cdot}\right)$. Mais il semble que « en moyenne », les fonctions L de Dirichlet aient une dérivée logarithmique positive en 1 : voir [IMS09, (1.2.2)], qui étudie asymptotiquement leur valeur moyenne (sur l'ensemble de tous les caractères modulo m, non nécessairement primitifs ni réels).

Corollaire 2.18. *Soit E/K une courbe elliptique à multiplications complexes par un ordre de discriminant $-df^2$, de conducteur $\mathfrak{f}(E/K)$, et soit $N_E = \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{f}(E/K))$. Si on suppose HRG, alors*

$$h_F(E/K), h(j_E), N_E, -df^2 \ll_{n_K} 1,$$

et plus précisément

$$h_F(E/K) \le 2{,}73\ln(n_K e^{109}), \qquad h(j_E) \le 33{,}3\ln(n_K e^{109}),$$
$$\ln(N_E) \le 32{,}7 n_K \ln(n_K e^{109}), \qquad -df^2 \le 1{,}2\cdot 10^5 n_K^2 (\ln(n_K e^{109}))^2.$$

Démonstration. Les propositions 2.10 et 2.16 montrent que, si HRG est supposée, alors

$$h_F(E/K) \ll \ln(-df^2) \ll_{n_K} \ln(h_F(E/K)),$$

ce qui n'est possible que si $h_F(E/K) \ll_{n_K} 1$. Ceci implique immédiatement la même domination pour $h(j_E)$, N_E et $-df^2$, notamment grâce à la proposition 2.15.

Plus précisément, supposons $h_F(E/K)+\ln(n_K)/2 > 1$. Si HRG est vraie, alors, toujours grâce aux mêmes propositions,

$$h_F(E/K) - 2{,}6\ln(h_F(E/K)+\ln(n_K)/2) \le 2{,}6\ln(32\sqrt{167}\,n_K) + 102{,}2 - 2{,}1\ln(e/2)$$

en utilisant l'inégalité $\ln(2\ln(x)) \le \ln(2x/e)$ valable pour $x > 1$. Par conséquent,

$$\mathfrak{m}\left(-\frac{h_F(E/K)}{2{,}6} - \frac{\ln(n_K)}{5{,}2}\right) \le -\frac{a}{n_K^{1+1/5{,}2}} \quad \text{où} \quad a = \frac{(e/2)^{2{,}1/2{,}6}}{2{,}6\cdot 32\sqrt{167}\,e^{102{,}2}}$$

(pour l'étude de $\mathfrak{m}$ et $\mathrm{w}_{\pm1}$, voir la sous-section 4.2). Ensuite, d'après le corollaire 4.18,

$$\frac{h_F(E/K)}{2{,}6} \le -\frac{\ln(n_K)}{5{,}2} - \mathrm{w}_{-1}\left(-\frac{a}{n_K^{6{,}2/5{,}2}}\right) \le \ln\left(\frac{n_K}{a}\ln\left(\frac{n_K^{6{,}2/5{,}2}}{a}\right)\right) + \frac{1}{2}.$$

Cette inégalité reste vraie si $h_F(E/K) + \ln(n_K)/2 \le 1$. Les dernières inégalités sont conséquences immédiates de l'inégalité vérifiée par $h_F(E/K)$, et des propositions 2.10, 2.15 et 2.16. ∎

Remarque 2.19. L'inégalité inconditionnelle de la proposition 2.16 ne permet pas d'obtenir une majoration ne dépendant que de n_K dans le corollaire ; il faudrait, pour y remédier *mutatis mutandis*, obtenir une meilleure majoration de l'éventuel zéro de Siegel (ou démontrer son inexistence). Si l'on suit notre schéma de démonstration, ceci dépend d'une meilleure majoration dans (33), où $\sqrt{|q|}$ devrait être remplacé par $q^{1/2-\varepsilon}$, ce qui nous semble inaccessible *a priori*. Toutefois, il reste possible de montrer que $h_F(E/K) \ll_{n_K} 1$ sans supposer la justesse de HRG, mais l'énoncé n'est plus effectif ; on sait montrer que $h_F(E/K) \ll_\varepsilon (-df^2)^\varepsilon$ pour tout $\varepsilon > 0$ (voir [Col98, p. 365, remarque (i)]).

3. Démonstration du théorème principal

3.1. Premières réductions. Soit E/K une courbe elliptique à multiplications complexes par $\mathbb{Q}(\sqrt{d})$, de j-invariant j_E, où K est un corps de

nombres de dimension n_K sur $\mathbb{Q}$. Alors E/K est isomorphe sur $\bar{K}$ (et même sur une extension de degré 6 sur K) à une courbe elliptique définie sur $\mathbb{Q}(j_E)$. Comme le théorème 1.1 concerne les $\bar{K}$-points, nous pouvons supposer sans perte de généralité que E est définie sur $K = \mathbb{Q}(j_E)$, d'après la remarque qui précède le théorème 2.12.

Supposons, de plus, que E/K est à multiplications complexes par $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$; toute courbe elliptique à multiplications complexes par $\mathbb{Q}(\sqrt{d})$ est isogène à une telle courbe, *via* une isogénie de degré contrôlé par la proposition 2.9. Ainsi, pour obtenir le théorème principal pour toute courbe elliptique à multiplications complexes, il conviendra de reprendre l'inégalité obtenue dans le cas d'un ordre maximal d'endomorphismes, et de diviser le minorant par le degré de cette isogénie, en vertu du dernier point de la proposition 2.1.

À présent, on effectue un changement de base adéquat $\mathrm{Spec}(\mathcal{O}_{K'}) \to B$, de sorte que :

— K' contient $\mathrm{End}(E) \otimes \mathbb{Q}$ (toutes les isogénies de E sont alors définies sur K') ;
— E a bonne réduction en toute place de K' ;
— K' est une extension normale de $\mathbb{Q}$.

On prend pour cela le corps composé de K, $\mathbb{Q}(\sqrt{d})$, et $K(E[12])$ (voir [Sil94, proposition IV.10.3]), qui reste galoisien sur $\mathbb{Q}$ si K l'est. Notons que ce changement de base n'affecte pas le calcul de la hauteur de Néron–Tate, qui ne dépend pas du corps de rationalité du point considéré. Dans cette section, on n'utilisera l'accouplement d'intersection que sur $\mathcal{E} \to \mathrm{Spec}(\mathcal{O}_{K'})$, on peut donc poser $\langle \cdot, \cdot \rangle = \langle \cdot, \cdot \rangle_{K'}$ sans risque de confusion. Soient $L = K'(P)$ et $D = [L : K']$.

Soient $s \geq 3$ un réel dont on fixera la valeur ultérieurement, et $\Pi_s = \{p_1, \ldots, p_r\}$ l'ensemble des nombres premiers rationnels inférieurs à s qui se décomposent complètement dans K'. À tout $p \in \Pi_s$ on associe un idéal premier $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_K)$ divisant p, puis une isogénie $\mathrm{F}_p : E \to E$ qui induit, modulo $\mathfrak{p}$, l'exponentiation à la puissance p sur la réduction de la courbe elliptique, dont l'existence est assurée par le fait que E est à multiplications complexes d'après le théorème 2.11. On sait, en particulier, que F_p est de degré p.

Montrons d'abord qu'on peut se ramener au cas où tous les conjugués de $\mathrm{F}_p(P)$ par les K'-plongements de L dans $\bar{K}$ sont distincts. Ceci permet de faire l'économie du lemme combinatoire 4.2 de [Lau83] sur le nombre de conjugués qui coïncident.

Lemme 3.1. *Nous pouvons supposer $K'(\mathrm{F}_p(P)) = L$ pour tout $p \in \Pi_s$. En particulier, on a toujours $\mathrm{F}_p(P)^\sigma \neq \mathrm{F}_p(P)^\tau$ pour $\sigma, \tau \in \mathrm{Hom}_{K'}(L, \bar{K})$ distincts.*

Démonstration. Les lemmes 3.2 et 3.3 de [Rat04] s'adaptent à notre situation, et montrent qu'on peut supposer que soit $K'(\mathrm{F}_p(P)) = L$, soit $[L : K'(\mathrm{F}_p(P))] = p$ pour tout $p \in \Pi_s$. Démontrons qu'on peut même s'affranchir du second cas pour démontrer l'inégalité (2) pour tout point d'ordre infini de degré D, à l'aide d'une récurrence sur D ; notons que si $L = K'$, alors il n'y a rien à dire.

S'il existe $p \in \Pi_s$ tel que $[L : K'(\mathrm{F}_p(P))] = p$, alors l'hypothèse de récurrence assure que (2) est vérifiée pour $\mathrm{F}_p(P)$, et on a

$$\begin{aligned}\hat{h}(P) = \frac{1}{p}\hat{h}(\mathrm{F}_p(P)) &\geq \frac{1}{p[K'(\mathrm{F}_p(P)) : K']} f([K'(\mathrm{F}_p(P)) : K']) \\ &= \frac{1}{D} f([K'(\mathrm{F}_p(P)) : K']),\end{aligned}$$

où $f(x) = \frac{c(E/K)}{6x}\left(\frac{\ln(\ln(24x))}{\ln(24x)}\right)^3$ définit une application décroissante pour $x \geq 1$, d'où l'inégalité (2) pour P. ∎

Il était déjà démontré, dans [Lau83, lemme 4.2], que les « orbites » par $\mathrm{Hom}_{K'}(L, \bar{K})$ des différents $\mathrm{F}_p(P)$ ne se recoupent pas (et même des différents $\phi(P)$, pour $\phi \in \mathrm{End}(E)$). Conjointement au lemme 3.1, on en déduit :

Corollaire 3.2. *Nous pouvons supposer que pour tous $p, p' \in \Pi_s$ et $\sigma, \tau \in \mathrm{Hom}_{K'}(L, \bar{K})$ tels que $(\sigma, p) \neq (\tau, p')$, on a $\mathrm{F}_p(P)^\sigma \neq \mathrm{F}_{p'}(P)^\tau$.*

Si P est un point de torsion, ce corollaire n'est plus nécessairement valable. C'est le seul endroit où l'on utilise le fait que P soit d'ordre infini.

3.2. Contribution positive des places finies. Soient $m_1, \ldots, m_r$ des entiers naturels ; on étend les morphismes F_p en des morphismes de $\mathcal{E}$ dans $\mathcal{E}$, et on considère le diviseur de Weil de $\mathcal{E}$ suivant :

$$\mathcal{L} = \sum_{i=0}^{r} m_i((\mathrm{F}_{p_i}(\mathcal{P})) - D \cdot (\mathcal{O})),$$

où, pour uniformiser les notations, on a posé $p_0 = 1$ et $\mathrm{F}_1 = \mathrm{Id}$. C'est par l'intermédiaire de ce diviseur qu'on compte calculer la hauteur de P. Le point de départ est le théorème 2.5 : comme $\mathcal{L}$ est de degré nul, on a

$$\begin{aligned}0 &\geq \langle \mathcal{L}, \mathcal{L} \rangle \\ &= \sum_{0 \leq i,j \leq r} m_i m_j (\langle \mathrm{F}_{p_i}(\mathcal{P}), \mathrm{F}_{p_j}(\mathcal{P}) \rangle + D^2 \langle \mathcal{O}, \mathcal{O} \rangle - D \langle (\mathrm{F}_{p_i} + \mathrm{F}_{p_j})(\mathcal{P}), \mathcal{O} \rangle).\end{aligned}$$

En vertu du corollaire 2.7 et de la proposition 2.1, on a

$$\langle (\mathrm{F}_{p_i} + \mathrm{F}_{p_j})(\mathcal{P}), \mathcal{O} \rangle = D n_{K'}(p_i + p_j)\hat{h}(P), \quad \text{et} \quad \langle \mathcal{O}, \mathcal{O} \rangle = 0,$$

donc

$$2D^2 n_{K'}\Big(\sum_{i=0}^{r} m_i\Big)\Big(\sum_{j=0}^{r} m_j p_j\Big)\hat{h}(P) \geq \sum_{0\leq i,j\leq r} m_i m_j \langle \mathrm{F}_{p_i}(\mathcal{P}), \mathrm{F}_{p_j}(\mathcal{P})\rangle.$$

Il nous reste à estimer les termes de la forme $\langle \mathrm{F}_{p_i}(\mathcal{P}), \mathrm{F}_{p_j}(\mathcal{P})\rangle$. Si $i = j$, alors la formule d'adjonction (6) et l'identité (8) montrent que la contribution des auto-intersections provient des places archimédiennes :

$$\langle \mathrm{F}_{p_i}(\mathcal{P}), \mathrm{F}_{p_i}(\mathcal{P})\rangle \geq \sum_{v\in M_{K'}^{\infty}} \sum_{\substack{\sigma,\tau: L\hookrightarrow \bar{K}\\ \sigma,\tau|v\\ \sigma\neq\tau}} n_v \lambda_v(\mathrm{F}_{p_i}(\mathcal{P})^{\sigma} - \mathrm{F}_{p_i}(\mathcal{P})^{\tau}). \tag{13}$$

Ainsi, en écrivant la décomposition locale du nombre d'intersection pour $i \neq j$ et en utilisant (13) ci-dessus pour $i = j$, on a

$$\begin{aligned} 2D^2 n_{K'}\Big(\sum_{i=0}^{r} m_i\Big)\Big(\sum_{j=0}^{r} m_j p_j\Big)\hat{h}(P) &\geq \sum_{v\in M_{K'}^{0}} \sum_{1\leq i\neq j\leq r} m_i m_j \langle \mathrm{F}_{p_i}(\mathcal{P}), \mathrm{F}_{p_j}(\mathcal{P})\rangle_v \\ &\quad + \sum_{v\in M_{K'}^{\infty}} \sum_{\substack{1\leq i,j\leq r\\ \sigma,\tau: L\hookrightarrow \bar{K}\\ \sigma,\tau|v\\ (i,\sigma)\neq(j,\tau)}} n_v m_i m_j \lambda_v(\mathrm{F}_{p_i}(\mathcal{P})^{\sigma} - \mathrm{F}_{p_j}(\mathcal{P})^{\tau}) \end{aligned} \tag{14}$$

Avant de poursuivre, notons que l'expression ci-dessus est homogène en les m_i, si bien qu'on peut les supposer rationnels en toute généralité. Par densité et continuité, on peut même supposer dorénavant que $m_i \in \mathbb{R}_+$.

Il reste à estimer chacune des sommes du membre de droite. On commence par celle indexée par les places finies, où on tire profit de la propriété des relèvements du Frobenius.

Lemme 3.3. *On a, en conservant les notations précédentes,*

$$\sum_{\substack{0\leq i,j\leq r\\ i\neq j}} \sum_{v\in M_{K'}^{0}} m_i m_j \langle \mathrm{F}_{p_i}(\mathcal{P}), \mathrm{F}_{p_j}(\mathcal{P})\rangle_v \geq [L:\mathbb{Q}] m_0 \sum_{i=1}^{r} m_i \ln(p_i).$$

Démonstration. Intéressons-nous d'abord aux intersections avec $\mathcal{P}$: démontrons que pour tout $\sigma : L \hookrightarrow \bar{K}$, tout $p \in \Pi_s$ et tout idéal premier $\mathfrak{p}$ au-dessus de p, il existe $\tau : L \hookrightarrow \bar{K}$ tel que $\mathrm{F}_p(\mathcal{P})^{\sigma} \equiv \mathcal{P}^{\tau} \bmod \mathfrak{p}$. Il suffit pour cela de montrer que pour $x \in \mathcal{O}_{L,\mathfrak{P}}$ (où $\mathfrak{P} \,|\, \mathfrak{p}$),

$$\mathfrak{p} \text{ divise } \prod_{\tau: L\hookrightarrow \bar{K}} ((x^p)^{\sigma} - x^{\tau}) \in K',$$

puisque F_p induit l'endomorphisme de Frobenius modulo $\mathfrak{p}$ sur les coordonnées de $\mathcal{P}$ (si $\mathcal{P}$ se réduit en O, alors le résultat est trivial).

Or, si $x \in \mathcal{O}_{L,\mathfrak{P}}$ et

$$\mu(X) = \prod_{\tau : L \hookrightarrow \bar{K}} (X - x^\tau),$$

alors $\mu(X) \in K'[X]$: il s'agit du polynôme minimal de x (sur K') à la puissance $[L : K'(x)]$. Ses coefficients sont donc fixés par σ, et

$$\mu(\sigma(X^p)) \equiv \sigma(\mu(X)^p) \bmod \mathfrak{p},$$

puis, après évaluation en x, $\mu(\sigma(x^p)) \equiv 0 \bmod \mathfrak{p}$, démontrant le résultat désiré. On obtient donc, partant de l'égalité (4),

$$\sum_{p \in \Pi_s} \sum_{v \in M^0_{K'}} \langle \mathrm{F}_p(\mathcal{P}), \mathcal{P} \rangle_v \geq \sum_{p \in \Pi_s} \sum_{\mathfrak{p} \mid p} \sum_{\sigma} \ln(\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p})) = [L : \mathbb{Q}] \sum_{p \in \Pi_s} \ln(p).$$

On minore trivialement les intersections locales restantes, qui sont positives. ∎

On doit dorénavant estimer les intersections locales aux places archimédiennes.

Lemme 3.4 (Lemme d'Elkies pondéré). *Soit v une place archimédienne, et soient $P_1, \dots, P_N$ des points distincts de $E(L)$ tels que $P_i^\sigma \neq P_j^\tau$ pour tous $(i,\sigma) \neq (j,\tau)$. Soient $m_1, \dots, m_N$ des réels strictement positifs qui vérifient $3\sum_{i=1}^N m_i^2 < 2D(\sum_{i=1}^N m_i)^2$. Alors*

$$\sum_{\substack{1 \leq i,j \leq N \\ (i,\sigma) \neq (j,\tau)}} m_i m_j \lambda_v(P_i^\sigma - P_j^\tau) \geq -D \sum_{i=1}^N m_i^2 \cdot \left(\frac{1}{2} \ln\left(2D \frac{(\sum_{i=1}^N m_i)^2}{\sum_{i=1}^N m_i^2} - 2 \right) + \frac{1}{12} J_v + \frac{27}{10} \right),$$

où l'on note $J_v = \max(\ln(|j_E|_v), 0)$.

Démonstration. Le lemme d'Elkies est démontré dans [BP05] dans le cas où $L = K'$ et $m_i = 1$ pour tout i. La démonstration s'adapte presque trivialement à notre situation.

La preuve nécessite quelques notations issues de la théorie de Fourier : on note Γ_E le groupe des caractères de $E(\mathbb{C})$, c'est-à-dire l'ensemble des morphismes de groupes de $E(\mathbb{C})$ dans le groupe des nombres complexes de module 1. On définit la transformée de Fourier, définie sur Γ_E, d'une application intégrable $f : E(\mathbb{C}) \to \mathbb{C}$ par la formule

$$\hat{f}(\chi) = \int_{E(\mathbb{C})} f(P) \bar{\chi}(P)\, dP.$$

Les autres définitions familières se transposent : on a des produits scalaires

$$\langle f, g\rangle_{E(\mathbb{C})} = \int\limits_{E(\mathbb{C})} f(P)\bar{g}(P)\,dP, \qquad \langle \hat{f}, \hat{g}\rangle_{\Gamma_E} = \sum_{\chi\in\Gamma_E} \hat{f}(\chi)\bar{\hat{g}}(\chi),$$

qui sont en vérité égaux quand les deux quantités sont définies (c'est la formule de Parseval), et un produit de convolution

$$f * g(P) = \int\limits_{E(\mathbb{C})} f(Q)g(P-Q)\,dQ.$$

Sous de bonnes hypothèses, une telle fonction f est caractérisée par sa transformée de Fourier, puisqu'on peut écrire la formule d'inversion $f(P) = \sum_{\chi\in\Gamma_E} \hat{f}(\chi)\chi(P)$.

Partant de [BP05, preuve de la proposition 2.4], les mêmes calculs aboutissent à

$$\begin{aligned}(15)\qquad \sum_{\substack{1\le i,j\le N\\(i,\sigma)\neq(j,\tau)}} m_i m_j \lambda_v(P_i^\sigma - P_j^\tau) &\\ \ge \sum_{\substack{1\le i,j\le N\\ \sigma,\tau: L\hookrightarrow\bar{K}}} m_i m_j \lambda_t(P_i^\sigma - P_j^\tau) &- D\sum_{i=1}^N m_i^2\lambda_t(O)\\ - \Big[D^2\Big(\sum_{i=1}^N m_i\Big)^2 - D\sum_{i=1}^N m_i^2\Big]t,&\end{aligned}$$

où $t > 0$ est un paramètre quelconque, et λ_t est le produit de convolution de λ_v avec le noyau de la chaleur $g_t(P) = \sum_{\chi\in\Gamma_E} \exp(-t/\widehat{\lambda_v}(\chi))\chi(P)$; remarquons que la transformée de Fourier de g_t se lit dans sa définition : on a $\widehat{g_t}(\chi) = \exp(-t/\widehat{\lambda_v}(\chi))$.

Posons $m = D\sum_{i=1}^N m_i$. Une observation cruciale concerne la première somme du membre de droite de (15) : si on note δ la mesure de probabilité qui donne la masse m_i/m à P_i^σ pour tout $\sigma : L \hookrightarrow \bar{K}$, alors

$$\begin{aligned}\frac{1}{m^2}\sum_{\substack{1\le i,j\le N\\ \sigma,\tau: L\hookrightarrow\bar{K}}} m_i m_j \lambda_t(P_i^\sigma - P_j^\tau) &= \iint\limits_{E(\mathbb{C})\times E(\mathbb{C})} \lambda_t(P-Q)\delta(P)\delta(Q)\,dP\,dQ\\ &= \langle \lambda_t * \delta, \delta\rangle_{E(\mathbb{C})},\end{aligned}$$

et donc, par la formule de Parseval,

$$\begin{aligned}\frac{1}{m^2}\sum_{\substack{1\le i,j\le N\\ \sigma,\tau: L\hookrightarrow\bar{K}}} m_i m_j \lambda_t(P_i^\sigma - P_j^\tau) &= \sum_{\chi\in\Gamma_E} \widehat{\lambda_t * \delta}(\chi)\bar{\hat{\delta}}(\chi) = \sum_{\chi\in\Gamma_E} \widehat{\lambda_t}(\chi)|\hat{\delta}(\chi)|^2\\ &= \sum_{\chi\in\Gamma_E} \widehat{\lambda_v}(\chi)\widehat{g_t}(\chi)|\hat{\delta}(\chi)|^2.\end{aligned}$$

Le terme principal de la somme est positif ; seule la positivité de $\widehat{\lambda_v}(\chi)$ est non triviale, et provient du fait qu'il s'agit de l'inverse d'une valeur propre du laplacien sur $E(\mathbb{C})$ (voir [BP05, proposition 2.2]). Alors, la première somme du membre de droite de (15) est positive. En utilisant [BP05, lemme A.6] pour majorer $\lambda_t(O)$ (pour $t<1$), on a

$$\begin{aligned}\frac{1}{D}\sum_{\substack{1\le i,j\le N\\(i,\sigma)\neq(j,\tau)}} m_i m_j \lambda_v(P_i^\sigma - P_j^\tau) &\\ \ge -\Big(\sum_{i=1}^N m_i^2\Big)\big(\tfrac12\ln(1/t)+\tfrac{1}{12}\max(\ln(|j_E|_v),0)+\tfrac{11}{5}\big)&\\ -\Big[D\Big(\sum_{i=1}^N m_i\Big)^2-\sum_{i=1}^N m_i^2\Big]t,&\end{aligned}$$

d'où le résultat en posant

$$t=\frac{\sum_{i=1}^N m_i^2}{2[D(\sum_{i=1}^N m_i)^2-\sum_{i=1}^N m_i^2]}<1,$$

qui est le réel maximisant le terme de droite. ∎

À présent, pour $i\ge 1$, posons $m_i=1$, et si $D=1$ choisissons $m_0<2r+\sqrt{4r^2+r(2r-3)}$; cette inégalité est équivalente à la condition d'application du lemme d'Elkies pondéré (pour $D\ge 2$, elle est trivialement toujours vérifiée). On a alors, en injectant dans (14) les résultats des lemmes 3.3 (pour les places finies) et 3.4 (pour les places infinies),

(16)
$$\hat h(P)\ge\frac{1}{D}\,\frac{m_0\sum_{i=1}^r\ln(p_i)-(m_0^2+r)\big(\frac12\ln\big(2D\frac{(m_0+r)^2}{m_0^2+r}-2\big)+\frac{1}{12}h(j_E)+\frac{27}{10}\big)}{2(m_0+\sum_{i=1}^r p_i)(m_0+r)}.$$

Il est temps de simplifier la minoration en estimant les sommes indexées par les nombres premiers. On suppose dans un premier temps que HRG est vraie, pour simplifier les calculs. La version inconditionnelle est démontrée dans la dernière section.

Lemme 3.5. *Soit $K/\mathbb{Q}$ une extension galoisienne. On a, en admettant HRG, pour tout $s\ge 10^5$,*

$$\Big|\mathrm{card}(\Pi_s)-\frac{1}{n_K}\,\mathrm{Li}(s)\Big|\le\frac{\alpha_K}{n_K}\sqrt{s}\ln(s),$$
$$\Big|\sum_{p\in\Pi_s}\ln(p)-\frac{s}{n_K}\Big|\le\frac{\beta_K}{n_K}\sqrt{s}\,(\ln(s))^2,$$

$$\sum_{p\in\Pi_s} p \leq \frac{1}{2n_K}\left[1+\frac{3}{\ln(s)}\right]\frac{s^2}{\ln(s)} + \frac{5}{3}\,\frac{\alpha_K}{n_K}s^{3/2}\ln(s),$$

où, pour $s \geq 10^5$,

$$\frac{s}{\ln(s)} \leq \mathrm{Li}(s) \leq \left[1+\frac{1{,}3}{\ln(s)}\right]\frac{s}{\ln(s)},$$

et

$$\alpha_K = 59{,}07 + 1{,}44\ln(|d_K|) + 4{,}35n_K,$$
$$\beta_K = 8{,}72 + 0{,}47\ln(|d_K|) + 3{,}30n_K.$$

Démonstration. L'inégalité (2.40) et le théorème 1.8 de [Win15] donnent exactement les deux premières inégalités. La dernière s'obtient facilement en partant d'une transformation d'Abel :

$$\sum_{p\in\Pi_s} p = \int_1^s t\,d\pi(t) = s\pi(s) - \int_2^s \pi(t)\,dt,$$

où $\pi(s) = \mathrm{card}(\Pi_s)$, qu'on vient d'estimer. Le calcul de la dernière intégrale provient donc essentiellement des estimations de $\int_2^s \frac{t^a}{(\ln(t))^b}\,dt$ pour $b > 0$ et $a > -1$, affinées avec une intégration par parties et une relation de Chasles (en scindant l'intégrale en $\sqrt{s}$). ∎

On peut simplifier les inégalités.

Lemme 3.6. *Conservons les notations du lemme précédent, et soit* $\varepsilon \in]0,1[$. *Alors, sous réserve de la justesse de HRG,*

— *si* $\ln(s) \geq 4\ln(4\sqrt{\beta_K e/\varepsilon}\ln(4\sqrt{\beta_K/\varepsilon}))$, *on a* $\sum_{p\in\Pi_s}\ln(p) \geq (1-\varepsilon)s/n_K$;

— *si* $\ln(s) \geq 4\ln(4\sqrt{\alpha_K e/\varepsilon}\ln(4\sqrt{\alpha_K/\varepsilon}))$, *on a* $\mathrm{card}(\Pi_s) \geq (1-\varepsilon)\mathrm{Li}(s) \geq \frac{1-\varepsilon}{n_K}\frac{s}{\ln(s)}$.

En particulier, si $s \geq 2^{16}(\alpha_K/\varepsilon)^4$, *ces deux inégalités sont vérifiées.*

Démonstration. Il suffit de résoudre l'inégalité

$$s/n_K - (\beta_K/n_K)\sqrt{s}(\ln(s))^2 \geq (1-\varepsilon)s/n_K,$$

et donc d'utiliser le corollaire 4.19(2) (avec $\alpha = 1/4$ et $b = \sqrt{\beta_K/\varepsilon}$), pour obtenir la première inégalité voulue ; on procède de même pour la deuxième inégalité. ∎

Remarque 3.7. Sous la même condition, on a également

$$\mathrm{card}(\Pi_s) \leq \frac{1+\varepsilon}{n_K}\mathrm{Li}(s), \qquad \sum_{p\in\Pi_s} p \leq \frac{1}{n_K}\left(\frac{1}{2}+\frac{5\varepsilon}{3}+\frac{3}{\ln(s)}\right)\frac{s^2}{\ln(s)}.$$

Soit $m_0 = \sqrt{r}$. On suppose désormais avoir choisi $s \geq 10^5$ tel que

$$\sqrt{s\ln(s)} \geq 8\sqrt{\frac{3n_{K'}}{2}\left(1+\frac{1{,}3}{5\ln(10)}\right)}\left(\tfrac{1}{2}\ln(4Ds)+\tfrac{1}{12}h(j_E)+2\right).$$

Ceci est vérifié pour, par exemple (voir corollaire 4.19),

$$s \geq \max\left(\frac{36n_{K'}(\ln(4De^{4+h(j_E)/6}))^2}{\ln\left(36n_{K'}(\ln(4De^{4+h(j_E)/6}))^2\right)}\sqrt{e}, 36n_{K'}\sqrt{e}\ln(36n_{K'})\right).$$

Prenons donc $s = 2^{20}\alpha_{K'}^4[\ln(4De^{4+h(j_E)/6})]^2\cdot[\ln(\ln(4De^{4+h(j_E)/6}))]^{-1}$. L'inégalité dessus, ainsi que les estimations données par le lemme 3.6 pour $\varepsilon = 1/2$, amènent à la minoration suivante :

$$\begin{aligned}\hat{h}(P) &\geq \frac{1}{4Dn_{K'}}\,\frac{s}{\frac{1}{\sqrt{n_{K'}}}\,\frac{s^2}{\ln(s)}\left(\frac{8}{5\sqrt{n_{K'}}}+\frac{4}{3\sqrt{3e}}\right)\left(\frac{1}{\sqrt{e}}+\frac{4}{3\sqrt{n_{K'}}}\right)\sqrt{\frac{s}{\ln(s)}}}\\ &\geq \frac{1}{20\sqrt{n_{K'}}\,D}\left(\frac{\ln(s)}{s}\right)^{3/2},\end{aligned}$$

d'où le résultat proche de celui annoncé dans le théorème 1.1, avec toutefois une dépendance en $n_{K'}$ et $\ln(|d_{K'}|)$ au lieu de n_K. Il est important de noter que $D \leq [K(P):K]$, et que l'application

$$x \mapsto \frac{1}{x}\left(\frac{\ln(4xe^{4+h(j_E)/6})}{\ln(\ln(4xe^{4+h(j_E)/6}))}\right)^3$$

est décroissante pour $x \geq 1$, on peut donc bien substituer D par $[K(P):K]$ dans l'inégalité ci-dessus ; on utilise le fait que $\frac{\ln(4xa)}{\ln(\ln(4xa))} \leq \left(1+\frac{\ln(a)}{\ln(4)}\right)\frac{\ln(4x)}{\ln(\ln(4x))}$ pour tous $a > 1$ et $x \geq 1$, afin d'obtenir une expression plus compacte. Concluons avec les majorations du lemme suivant.

Lemme 3.8. *On a*

$$n_{K'} \leq 192n_K \quad \textit{et} \quad \ln(|d_{K'}|) \leq 12520n_K^2\ln(n_Ke^{109}).$$

Démonstration. Concernant la première inégalité, on a bien entendu

$$n_{K'} \leq 2[K(\sqrt{d},E[12]):K(\sqrt{d})]n_K,$$

et l'action de $\mathrm{Gal}(K(\sqrt{d},E[12])/K(\sqrt{d}))$ sur $E[12]$ commute avec les éléments de $\mathrm{End}(E) = \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$, donc induit une injection

$$\mathrm{Gal}(K(\sqrt{d},E[12])/K(\sqrt{d})) \hookrightarrow \mathrm{Aut}_{\mathcal{O}_{\mathbb{Q}(\sqrt{d})}/12\mathcal{O}_{\mathbb{Q}(\sqrt{d})}}(E[12]) \simeq \left(\frac{\mathcal{O}_{\mathbb{Q}(\sqrt{d})}}{12\mathcal{O}_{\mathbb{Q}(\sqrt{d})}}\right)^{\times}.$$

Donc $[K(\sqrt{d},E[12]):K(\sqrt{d})] \leq 96$, le pire cas étant celui où 2 et 3 sont tous les deux inertes dans $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$.

La deuxième inégalité provient des relations de divisibilité entre des discriminants de corps de nombres et celui de leur extension composée, décrites dans [Tôy55]. Puisque K' s'obtient en composant $K(\sqrt{d})$ et $K(E[12])$, on a

$$\ln(|d_{K'}|) \leq \frac{n_{K'}}{n_K}\ln(|d_{K(\sqrt{d})}|) + \frac{n_{K'}}{[K(E[12]):\mathbb{Q}]}\big([K(E[12]):K]\ln(d_K) + \ln(\mathrm{N}_{K/\mathbb{Q}}(\Delta_{K(E[12])/K}))\big),$$

où $d_{K(\sqrt{d})}$ est le discriminant absolu de $K(\sqrt{d})$, et $\Delta_{K(E[12])/K}$ le discriminant relatif de l'extension $K(E[12])/K$. Or, [HS00, proposition C.1.5] démontre que l'extension $K(E[12])/K$ ne se ramifie au plus qu'en les places de mauvaise réduction et celles de caractéristiques résiduelles 2 et 3. Puis, [Ser81, proposition 5] établit l'inégalité

$$\ln(\mathrm{N}_{K/\mathbb{Q}}(\Delta_{K(E[12])/K})) \leq [K(E[12]):\mathbb{Q}]\left(1-\frac{1}{192}\right)\sum_{\substack{\mathfrak{p}|p\\ \mathfrak{p}\,\mathrm{ram.}}}\ln(p) + [K(E[12]):\mathbb{Q}]\ln(192),$$

parce que $[K(E[12]):K] \leq 192$. On en déduit que

$$\ln(\mathrm{N}_{K/\mathbb{Q}}(\Delta_{K(E[12])/K})) \leq 191 n_K \ln(6N_E) + 192 n_K \ln(192),$$

où N_E est la norme du conducteur de E. Enfin, l'extension $K(\sqrt{d})/\mathbb{Q}(\sqrt{d})$ étant non ramifiée, on a $\ln(d_{K(\sqrt{d})}) \leq n_K \ln(-d)$; il y a même égalité. Pour conclure, on observe que

(17)
$$\ln(|d_{K'}|) \leq n_K\ln(-d) + 2\big(n_K\ln(-d) + 191 n_K\ln(6N_E) + 192 n_K\ln(192)\big),$$

et on utilise le corollaire 2.18 pour obtenir une majoration ne dépendant que de n_K. ∎

Ceci démontre le théorème principal conditionnel complètement, conjointement aux remarques du début de section.

3.3. Démonstration du théorème principal inconditionnel. Pour s'affranchir de l'hypothèse de Riemann généralisée, peu de choses sont à modifier : le fil de la démonstration reste le même. Seules les estimations des lemmes 3.5, 3.6 et 3.8 sont à adapter (et, de fait, le choix de s en bout de course).

Lemme 3.9. *Soit $K/\mathbb{Q}$ une extension galoisienne, et soit β_0 l'éventuel zéro de Siegel de ζ_K. Notons $M_K = \exp(110000 n_K(\ln(9d_K^8))^2)$. Pour tout $s \geq M_K$, on a*

$$\left|\mathrm{card}(\Pi_s) - \frac{1}{n_K}\left(\mathrm{Li}(s) - \frac{s^{\beta_0}}{\ln(s^{\beta_0})}\right)\right| \leq \frac{3{,}37\cdot 10^{13}}{n_K} s\exp\left(-\frac{1}{12}\sqrt{\frac{\ln(s)}{n_K}}\right),$$

$$\left|\sum_{p\in\Pi_s}\ln(p) - \frac{s}{n_K}\left(1-\frac{s^{\beta_0-1}}{\beta_0}\right)\right| \leq \frac{3{,}5\cdot 10^{12}}{n_K} s\exp\left(-\frac{1}{8}\sqrt{\frac{\ln(s)}{n_K}}\right)$$

et

$$\sum_{p\in\Pi_s} p \le \frac{s^2}{2n_K\ln(s)}\biggl[1+\frac{1{,}00001}{\ln(s)}+4{,}24\cdot 10^{13}\exp\Bigl(-\frac{1}{8}\sqrt{\frac{\ln(s)}{n_K}}\Bigr) + \frac{8}{\beta_0(\beta_0+1)}\,\frac{1}{s^{1-\beta_0}}\biggr],$$

où, pour $s \ge M_K$,

$$\frac{s}{\ln(s)} \le \mathrm{Li}(s) \le \biggl[1+\frac{1{,}00001}{\ln(s)}\biggr]\frac{s}{\ln(s)}.$$

Les termes contenant β_0 *peuvent être supprimés en l'absence de zéro de Siegel.*

Démonstration. Les deux premières inégalités proviennent de [Win15, théorème 1.7 et inégalité (2.41)] ; la deuxième inégalité est même valable pour $s \ge \sqrt{M_K}$. La troisième inégalité se calcule par une autre transformation d'Abel, puisqu'on a

$$\sum_{p\in\Pi_s} p \le \frac{s\theta(s)}{\ln(s)} - \int_2^s \theta(x)\biggl(\frac{1}{\ln(x)}-\frac{1}{(\ln(x))^2}\biggr)\,dx,$$

où $\theta(s)=\sum_{p\in\Pi_s}\ln(p)$. On suppose à présent $s \ge M_K$, en minorant trivialement par zéro l'intégrande sur l'intervalle $[2,\sqrt{s}]$. La seule difficulté inédite réside dans l'estimation suivante, nécessaire à cause de l'intégration du terme d'erreur du théorème de Chebotarev inconditionnel, et qu'on obtient par intégration par parties :

$$\int_{\sqrt{s}}^{s} x\exp\Bigl(-\frac{1}{8}\sqrt{\frac{\ln(x)}{n_K}}\Bigr)\,dx \le \Bigl(1+\frac{1}{8\sqrt{n_K\ln(s)}}\Bigr)\frac{s^2}{2}\exp\Bigl(-\frac{1}{8}\sqrt{\frac{\ln(s)}{n_K}}\Bigr).\ \blacksquare$$

Remarque 3.10. Utilisant [Win15, lemme 2.17 et corollaire 2.26], on peut fournir une majoration de la somme des nombres premiers de Π_s qui ne dépend pas de β_0, toujours pour $s \ge M_K$:

$$\sum_{p\in\Pi_s} p \le \frac{s^2}{2n_K\ln(s)}\biggl[1{,}00001+6{,}37\exp\Bigl(\frac{12|d_K|^{2709}e^{387(26n_K+32)}}{n_K}-\frac{1}{8}\sqrt{\frac{\ln(s)}{n_K}}\Bigr)\biggr].$$

On a utilisé la majoration $s^{\beta_0-1} \le \exp\bigl(\frac{1}{16^2(1-\beta_0)n_K}\bigr)\exp\bigl(-\frac{1}{8}\sqrt{\frac{\ln(s)}{n_K}}\bigr)$ (si β_0 n'existe pas, l'inégalité ci-dessus reste évidemment valable).

Lemme 3.11. *Conservons les notations du lemme précédent, et soit* $\varepsilon \in]0,1[$. *De plus, posons* $B_K = 3072|d_K|^{2709}e^{387(26n_K+32)}$. *Alors*

— *si* $s \geq (2{,}2/\varepsilon)^{B_K} \exp(64 n_K (\ln(7 \cdot 10^{12}/\varepsilon))^2)$, *on a*

$$\sum_{p \in \Pi_s} \ln(p) \geq (1-\varepsilon) s/n_K.$$

— *si* $s \geq (2/\varepsilon)^{B_K} \exp\big(\frac{\varepsilon}{1{,}685 \cdot 10^{13}}\big)$, *on a* $\operatorname{card}(\Pi_s) \geq \frac{1-\varepsilon}{n_K} \frac{s}{\ln(s)}$.

Démonstration. Supposons d'abord que le zéro de Siegel β_0 existe pour ζ_K. Alors, l'inégalité $\sum_{p \in \Pi_s} \ln(p) \geq (1-\varepsilon) s/n_K$ est vraie sous l'hypothèse suffisante que

$$\varepsilon \geq \frac{1}{\beta_0 s^{1-\beta_0}} + 3{,}5 \cdot 10^{12} \exp\left(-\frac{1}{8}\sqrt{\frac{\ln(s)}{n_K}}\right).$$

Dans ce cas, cette inégalité est vérifiée si

$$s \geq \max\left[\left(\frac{2}{\beta_0 \varepsilon}\right)^{1/(1-\beta_0)}, \exp\left(64 n_K \left(\ln\left(\frac{7 \cdot 10^{12}}{\varepsilon}\right)\right)^2\right)\right].$$

Le corollaire 2.16 de [Win15] permet de majorer β_0, d'où l'inégalité requise. Si β_0 n'existe pas, il suffit de prendre $s \geq \exp(64 n_K (\ln(3{,}5 \cdot 10^{12}/\varepsilon))^2)$, donc la borne du premier cas convient encore. On procède de même pour la deuxième estimation. ∎

Reprenons la démonstration esquissée dans la sous-section 3.2, jusqu'à l'inégalité (16), avec encore une fois le choix $m_0 = \sqrt{r}$ (rappelons que $r = \operatorname{card}(\Pi_s)$). Notons que $X \mapsto X/\exp\big(\frac{1}{12}\sqrt{X/n_{K'}}\big)$ décroît à partir de $X \geq 576 n_{K'}$, donc en particulier

$$\frac{\ln(s)}{\exp\big(\frac{1}{12}\sqrt{\frac{\ln(s)}{n_{K'}}}\big)} \leq \frac{\ln(M_{K'})}{\exp\big(\frac{1}{12}\sqrt{\frac{\ln(M_{K'})}{n_{K'}}}\big)} \leq \frac{\ln(M_{K'})}{\exp\big(40\sqrt{\ln(|d_{K'}|)}\big)} \leq 298.$$

On suppose avoir choisi

$$s \geq \max\left[M_{K'}, \left(\frac{2{,}2}{\varepsilon}\right)^{B_{K'}} \exp\left(64 n_{K'} \left(\ln\left(\frac{7 \cdot 10^{12}}{\varepsilon}\right)\right)^2\right)\right]$$

tel que

$$\sqrt{s \ln(s)} \geq 8\sqrt{300 n_{K'}}\big(\tfrac{1}{2}\ln(4Ds) + \tfrac{1}{12}h(j_E) - 13\big).$$

Ceci est vérifié pour

$$s \geq \max\left(\frac{19200 n_{K'} (\ln(4De^{2h(j_E)-26}))^2}{\ln\big(19200 n_{K'} (\ln(4De^{2h(j_E)-26}))^2\big)}\sqrt{e}, 19200 n_{K'}\sqrt{e}\ln(19200 n_{K'})\right).$$

On remplace l'emploi du lemme 3.6, que nous avions appliqué avec $\varepsilon = 1/2$, par l'application du lemme 3.11 que nous venons de démontrer. Alors, prenant

$$s = [\ln(4De^{4+2h(j_E)})]^2 [\ln(\ln(4De^{4+2h(j_E)}))]^{-1} \exp(1{,}5 B_{K'}),$$

l'inégalité (16) amène à la minoration suivante :

$$\hat{h}(P) \geq \frac{1}{4\sqrt{n_{K'}}\,D}\,\frac{1}{13(13,14+6,37\cdot 10^{-4754}\exp(B_{K'}))}\left(\frac{\ln(s)}{s}\right)^{3/2},$$

d'où le résultat annoncé dans le théorème 1.1, avec $n_{K'}$ et $\ln(|d_{K'}|)$ au lieu de n_K et $\ln(|d_K|)$; là encore, on peut bien substituer D par $[K(P):K]$ dans l'inégalité ci-dessus. On adapte le lemme 3.8 pour conclure :

Lemme 3.12. *On a*

$$n_{K'} \leq 192 n_K \quad \textit{et} \quad \ln(|d_{K'}|) \leq 64 n_K^2 (72 h_{F+}(E/K) + 43).$$

Démonstration. L'inégalité vérifiée par n'_K est déjà démontrée dans le lemme 3.8. La majoration de $|d_{K'}|$ se déduit de (17), en recourant aux propositions 2.10 et 2.15 et au corollaire 2.14 pour tout exprimer à l'aide de $h_{F^+}(E/K)$ et n_K. ∎

Ceci démontre le théorème principal sous sa forme inconditionnelle.

4. Résultats analytiques

4.1. Majoration de la fonction de von Mangoldt. Nous démontrons, dans cette sous-section, une version explicite du théorème de la progression arithmétique de Dirichlet (en quelque sorte), nécessaire pour achever la démonstration de la proposition 2.16. La stratégie est classique, exposée par exemple dans [Dav67, chapitres 19 et 20] ; nous nous efforçons simplement de rendre explicite chaque étape du calcul, suivant de près la démonstration du théorème de densité de Chebotarev que nous avons produite dans [Win15, chapitre 2], tout en profitant des résultats supplémentaires connus dans le cas particulier des fonctions L de Dirichlet.

Soit χ un caractère réel primitif (par exemple $\chi = \left(\frac{d}{\cdot}\right)$, où $d < 0$ est un entier sans facteur carré), et soit $\mathrm{L}(\cdot,\chi)$ la fonction L de Dirichlet associée, définie pour $\mathrm{Re}(s) > 0$ par la formule

$$\mathrm{L}(s,\chi) = \sum_{n=0}^{\infty} \frac{\chi(n)}{n^s}.$$

La convergence est absolue pour $\mathrm{Re}(s) > 1$, et dans ce cas

$$-\frac{\mathrm{L}'}{\mathrm{L}}(s,\chi) = -\sum_p \frac{-\chi(p)\ln(p)}{p^s(1-\chi(p)/p^s)} = \sum_p \sum_{m=1}^{\infty} \frac{\chi(p^m)\ln(p)}{p^{ms}} = \sum_{n=1}^{\infty} \frac{\Lambda_\chi(n)}{n^s},$$

où

$$\Lambda_\chi(n) = \begin{cases} \chi(p^m)\ln(p) & \text{si } n = p^m,\ p \text{ premier},\ m \geq 1, \\ 0 & \text{sinon.} \end{cases}$$

L'étude de ces fonctions de Dirichlet donne donc des estimations de sommes indexées par les nombres premiers, et peut y trouver sa motiva-

tion : partant de la transformée de Mellin, il est possible de lier la fonction sommatoire de von Mangoldt $\psi_\chi(x) = \sum_{n\leq x} \Lambda_\chi(n)$ aux zéros de la fonction $\mathrm{L}(\cdot,\chi)$. Nous allons démontrer le théorème suivant :

THÉORÈME 4.1. *Soit χ un caractère réel primitif modulo q. Si $\mathrm{L}(\cdot,\chi)$ vérifie HRG, alors pour tout $x \geq 3$,*

$$|\psi_\chi(x)| \leq \sqrt{x}\ln(x)\left[\frac{1}{2\pi}\ln(x) + \frac{1}{\pi}\ln\left(\frac{q}{2\pi}\right) + 9{,}68 + \varepsilon_q(x)\right],$$

où

$$\varepsilon_q(x) = \frac{1{,}91\ln(q) + 34{,}16}{\ln(x)} + \frac{2{,}03}{(\ln(x))^2} + \frac{0{,}38}{(\ln(x))^3} + \frac{7{,}84}{\sqrt{x}} + \frac{1{,}64\ln(q) + 12{,}43}{\sqrt{x}\ln(x)} + \frac{0{,}58\ln(q) + 9{,}19}{\sqrt{x}(\ln(x))^2}.$$

Inconditionnellement, pour tout $x \geq \exp(6{,}5(\ln(3q))^2)$, on a

$$\left|\psi_\chi(x) + \frac{x^{\beta_0}}{\beta_0}\right| \leq 2200x\exp\left(-\frac{\sqrt{\ln(x)}}{10{,}2}\right),$$

où β_0 est l'éventuel zéro de Siegel de $\mathrm{L}(\cdot,\chi)$; le terme x^{β_0} peut être supprimé si β_0 n'existe pas.

Pour cela, commençons par écrire plus rigoureusement le lien entre ψ_χ et $\mathrm{L}(\cdot,\chi)$. On a le lemme suivant, qui permet d'utiliser une transformée de Mellin tronquée :

LEMME 4.2 ([Ram07, lemme 7.1]). *Si $y > 0$, $\sigma > 0$ et $T > 0$, alors*

$$\left|\frac{1}{2\pi i}\int_{\sigma-iT}^{\sigma+iT}\frac{y^s}{s}\,ds - 1\right| \leq \frac{y^\sigma}{\pi}\min(7/2, T^{-1}|\ln(y)|^{-1}) \quad \text{si } y > 1,$$

$$\left|\frac{1}{2\pi i}\int_{\sigma-iT}^{\sigma+iT}\frac{y^s}{s}\,ds - \frac{1}{2}\right| \leq \sigma T^{-1} \quad \text{si } y = 1,$$

$$\left|\frac{1}{2\pi i}\int_{\sigma-iT}^{\sigma+iT}\frac{y^s}{s}\,ds\right| \leq \frac{y^\sigma}{\pi}\min(7/2, T^{-1}|\ln(y)|^{-1}) \quad \text{si } 0 < y < 1.$$

Le cas où $y = 1$ n'est pas démontré dans [Ram07], mais on peut calculer directement l'intégrale en jeu très facilement, et de toute façon nous ne nous servirons pas de ce cas.

Grâce à ce lemme, nous pouvons déduire aisément que pour $x \geq 3$ différent d'une puissance d'un nombre premier, on a

$$\left|-\frac{1}{2\pi i}\int_{\sigma_0-iT}^{\sigma_0+iT}\frac{\mathrm{L}'}{\mathrm{L}}(s,\chi)\frac{x^s}{s}\,ds-\psi_\chi(x)\right| \leq R(x,T) := ex\sum_{n\neq x}\frac{\Lambda(n)}{\pi n^{\sigma_0}}\min(7/2, T^{-1}|\ln(x/n)|^{-1})$$

pour tout $\mathrm{Re}(s)>1$, où $\sigma_0 = 1+1/\ln(x)$ (de sorte que $x^{\sigma_0}=ex$) et $\Lambda(n)$ est la fonction de von Mangoldt traditionnelle, correspondant à $\chi=1$. Si x est une puissance d'un nombre premier, il suffit d'écrire, par continuité, que

$$\left|-\frac{1}{2\pi i}\int_{\sigma_0-iT}^{\sigma_0+iT}\frac{\mathrm{L}'}{\mathrm{L}}(s,\chi)\frac{x^s}{s}\,ds-\psi_\chi(x)\right| \leq R(x,T)+\ln(x), \tag{18}$$

et cette inégalité reste valable pour tout $x\geq 3$.

Pour majorer $R(x,T)$, on procède par disjonction de cas, selon que l'on considère des puissances de nombres premiers proches de x ou non. La démarche ressemble de près aux calculs entrepris dans [Win15, chapitre 2], et on la reproduit ici pour obtenir

$$R(x,T)\leq \frac{4^{1-1/\ln(3)}e^2}{T}x(\ln(x))^2+\frac{\ln(x)}{T\pi\ln(5/4)} + \frac{7}{\pi}\left(\frac{3}{2}\right)^{1+1/\ln(3)}\ln(x+1)+\ln(x) \tag{19}$$

pour tous $x\geq 3$ et $T\geq 2$. On a contrôlé explicitement l'écart entre ψ_χ et l'intégrale $\frac{1}{2\pi i}\int_{\sigma_0-iT}^{\sigma_0+iT}\frac{\mathrm{L}'}{\mathrm{L}}(s,\chi)\frac{x^s}{s}\,ds$. Il s'agit de voir, à présent, que cette intégrale est relativement proche de l'intégrale de la même fonction, mais sur un contour, afin de la relier aux zéros et pôles de son intégrande (et donc aux zéros de $\mathrm{L}(\cdot,\chi)$).

4.1.1. *Inégalités préliminaires.* Si on pose

$$\xi(s,\chi)=\left(\frac{q}{\pi}\right)^{(a+s)/2}\Gamma\left(\frac{s+a}{2}\right)\mathrm{L}(s,\chi), \tag{20}$$

avec $a=(1-\chi(-1))/2$ et Γ la fonction Gamma d'Euler, alors on a l'équation fonctionnelle

$$\xi(1-s,\bar{\chi})=W(\chi)\xi(s,\chi),$$

où $W(\chi)$ est une constante de module 1. De plus, $\xi(\cdot,\chi)$ est une fonction entière d'ordre 1 qui ne s'annule pas en 0, donc

$$\xi(s,\chi)=e^{B_1(\chi)+B(\chi)s}\prod_\rho\left(1-\frac{s}{\rho}\right)e^{s/\rho} \tag{21}$$

pour des constantes $B_1(\chi)$ et $B(\chi)$, où $\rho = \beta + i\gamma$ parcourt l'ensemble des zéros (non triviaux) de $\mathrm{L}(\cdot,\chi)$ tels que $0 < \beta < 1$ (la lettre ρ désignera toujours ces zéros) ; tous ces résultats sont exposés dans [Dav67, chapitre 12].

En dérivant logarithmiquement (20) et (21), on obtient la relation importante

$$\frac{\mathrm{L}'}{\mathrm{L}}(s,\chi) = B(\chi) + \sum_{\rho}\left(\frac{1}{s-\rho}+\frac{1}{\rho}\right) - \frac{1}{2}\ln\left(\frac{q}{\pi}\right) - \frac{1}{2}\frac{\Gamma'}{\Gamma}\left(\frac{s+a}{2}\right), \tag{22}$$

valable pour tout nombre complexe s où ces quantités sont définies.

Pour estimer les intégrales dépendant de L'/L, il est nécessaire de savoir majorer les sommes portant sur ses zéros, ainsi que la dérivée logarithmique de la fonction Γ. Pour ce faire, on établit quelques résultats préliminaires.

Lemme 4.3. *Si* $\mathrm{Re}(s) > 1$, *alors*

$$\left|\frac{\mathrm{L}'}{\mathrm{L}}(s,\chi)\right| \leq \frac{1}{\mathrm{Re}(s)-1}.$$

Démonstration. On adapte la démonstration de [Win15, lemme 2.6]. ∎

Lemme 4.4. *Soit z un nombre complexe.*

(1) *Si* $\mathrm{Re}(z) > 0$, *alors*

$$\left|\frac{\Gamma'}{\Gamma}(z)\right| \leq \ln(|z|) + \frac{\pi}{2} + \frac{1}{\mathrm{Re}(z)}.$$

(2) *Si* $|\mathrm{Im}(z)| > 0$, *alors*

$$\left|\frac{\Gamma'}{\Gamma}(z)\right| \leq \ln(|z|) + \pi\left(1 + \frac{1}{2|\mathrm{Im}(z)|}\right) + \frac{1}{2|\mathrm{Im}(z)|}.$$

(3) *Si* $\mathrm{Re}(z) \leq 0$, *alors*

$$\left|\frac{\Gamma'}{\Gamma}(z)\right| \leq \ln((1+|\mathrm{Im}(z)|)(1+|\mathrm{Re}(z)|)) + \frac{\pi}{2} + 2 + \frac{1}{|z+[-\mathrm{Re}(z)+1/2]|}.$$

Démonstration. Les deux premières inégalités sont démontrées dans [Win15, lemme 2.7] sous cette forme. Montrons la troisième inégalité : si $\mathrm{Re}(z) \leq 0$, l'équation fonctionnelle vérifiée par Γ permet de montrer que

$$\frac{\Gamma'}{\Gamma}(z) = \frac{\Gamma'}{\Gamma}(z+m) - \sum_{j=0}^{m-1}\frac{1}{z+j}$$

pour tout entier $m > 0$. On pose $m = [-\mathrm{Re}(z)+1]$, de sorte que $\mathrm{Re}(z+m) > 0$ (c'est le plus petit entier naturel à vérifier cette inégalité), ce qui permet de borner $\frac{\Gamma'}{\Gamma}(z+m)$:

$$\left|\frac{\Gamma'}{\Gamma}(z+m)\right| \leq \ln\bigl(\sqrt{1+(\mathrm{Im}(z))^2}\bigr) + \pi/2 + 1.$$

On vérifie aisément que $|z+j|$ est minimisé par $j_0 = [-\mathrm{Re}(z)+1/2]$. Comme $\mathrm{Re}(z) \le 1-m$, on a

$$\Big|\sum_{j=0}^{m-1} \frac{1}{z+j}\Big| \le \frac{1}{|z+j_0|} + \sum_{j=0}^{m-2} \frac{1}{-1+(m-j)} = \frac{1}{|z+j_0|} + \sum_{k=1}^{m-1} \frac{1}{k}$$
$$\le 1 + \frac{1}{|z+j_0|} + \ln(|\mathrm{Re}(z)|+1),$$

ce raisonnement valant du moins si $m > 2$ (si $m \le 2$, l'inégalité vaut même sans le terme logarithmique), pour finalement donner l'inégalité

$$\left|\frac{\Gamma'}{\Gamma}(z)\right| \le \ln(|\mathrm{Re}(z)|+1) + \ln\big(\sqrt{1+(\mathrm{Im}(z))^2}\big) + \frac{\pi}{2} + 2 + \frac{1}{|z+j_0|}. \ \blacksquare$$

Remarque 4.5. La troisième inégalité prévaut sur la deuxième lorsqu'on doit mesurer l'écart aux pôles dus aux facteurs Γ.

Enfin, le lemme suivant est très précieux pour les sommes indexées par les zéros de $\mathrm{L}(\cdot,\chi)$.

Lemme 4.6 ([Tru15, théorème 1]). *Soient $T > 0$ et χ un caractère primitif (non principal) modulo q. Soit $n_\chi(T)$ le nombre de zéros $\rho = \beta + i\gamma$ de $\mathrm{L}(\cdot,\chi)$ avec $0 < \beta < 1$ et $|\gamma| \le T$. On a*

$$\left|n_\chi(T) - \frac{T}{\pi}\ln\left(\frac{qT}{2\pi e}\right)\right| \le 0{,}317\ln(qT) + 6{,}401.$$

4.1.2. *L'intégrale sur un contour.* Maintenant, on évalue

$$I_\chi(x,T) = \frac{1}{2\pi i}\int_{\sigma_0-iT}^{\sigma_0+iT} \frac{x^s}{s}\frac{\mathrm{L}'}{\mathrm{L}}(s,\chi)\,ds.$$

On prend T différent de $\mathrm{Im}(\rho)$ pour tout zéro non trivial ρ, et on introduit un nouveau paramètre $U = 2k+1-a$ pour un certain entier naturel k (plus tard, on fera $U,k \to \infty$), et on définit

$$I_\chi(x,T,U) = \frac{1}{2\pi i}\int_{B_{T,U}} \frac{x^s}{s}\frac{\mathrm{L}'}{\mathrm{L}}(s,\chi)\,ds, \tag{23}$$

où $B_{T,U}$ est le rectangle (orienté dans le sens trigonométrique) dont les sommets sont $\sigma_0 - iT$, $\sigma_0 + iT$, $-U+iT$ et $-U-iT$; avec le choix de T que nous avons fait, aucun pôle de l'intégrande n'est sur le contour. Cette intégrale s'exprime simplement à l'aide des singularités de l'intégrande, mais ceci attendra encore un peu. L'objectif est de montrer que $R_\chi(x,T,U) = I_\chi(x,T,U) - I_\chi(x,T)$ est petit.

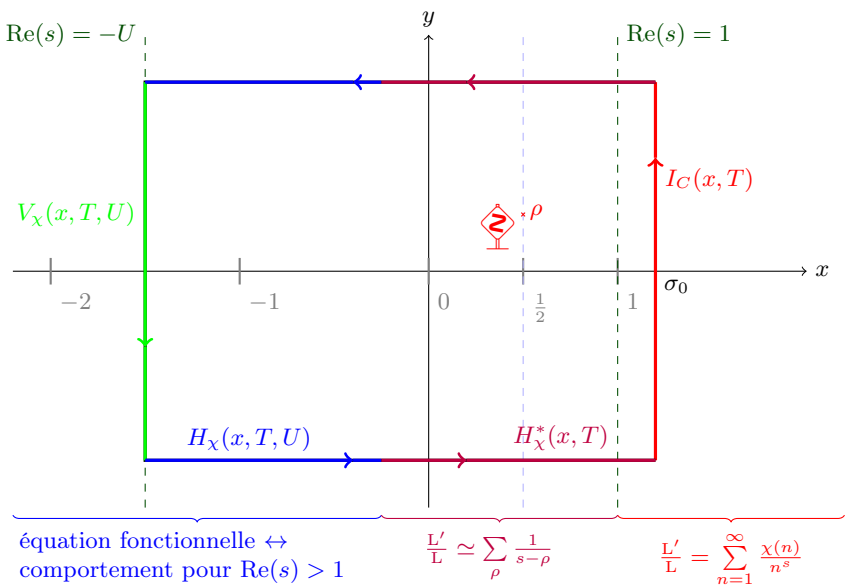

Fig. 1. Comportement des fonctions L de Dirichlet le long du contour d'intégration

On divise $R_\chi(x,T,U)$ en trois intégrales, celle verticale

$$V_\chi(x,T,U) = \frac{1}{2\pi}\int_T^{-T} \frac{x^{-U+it}}{-U+it}\,\frac{\mathrm{L}'}{\mathrm{L}}(-U+it,\chi)\,dt,$$

et les deux intégrales horizontales

$$H_\chi(x,T,U) = \frac{1}{\pi}\,\mathrm{Im}\left(\int_{-U}^{-1/4} \frac{x^{\sigma-iT}}{\sigma-iT}\,\frac{\mathrm{L}'}{\mathrm{L}}(\sigma-iT,\chi)\,d\sigma\right),$$
$$H^*_\chi(x,T) = \frac{1}{\pi}\,\mathrm{Im}\left(\int_{-1/4}^{\sigma_0} \frac{x^{\sigma-iT}}{\sigma-iT}\,\frac{\mathrm{L}'}{\mathrm{L}}(\sigma-iT,\chi)\,d\sigma\right).$$

Pour estimer $V_\chi(x,T,U)$, remarquons qu'on peut relier $\frac{\mathrm{L}'}{\mathrm{L}}(s,\chi)$ à $\frac{\mathrm{L}'}{\mathrm{L}}(1-s,\chi)$ grâce à l'équation fonctionnelle, et donc se ramener au comportement dans la région mieux connue $\mathrm{Re}(s)\geq 1$; si $s=-U+it=-(2k+1-a)+it$, avec $k\geq 1$, on a

$$\left|\frac{\mathrm{L}'}{\mathrm{L}}(s,\chi)\right| \leq \frac{2}{U} + \left|\ln\left(\frac{q}{\pi}\right)\right| + \ln\left(k+2+\frac{|t|}{2}\right) + \frac{1}{2}\ln(1+|t|) + \frac{1}{\sqrt{1+t^2}} + \frac{61}{14}$$

grâce aux première et dernière inégalités du lemme 4.4. On voit donc, pour

$x \geq 3$, $T \geq 2$ et $U \geq 2$, que

$$
\begin{aligned}
(24) \qquad |V_\chi(x,T,U)| &\leq \frac{x^{-U}}{2\pi U} \int_{-T}^{T} \left|\frac{\mathrm{L}'}{\mathrm{L}}(-U+it,\chi)\right| dt \\
&\leq \frac{x^{-U}}{\pi U}\left(\left(\frac{2}{U} + \left|\ln\left(\frac{q}{\pi}\right)\right| + \frac{61}{14} + \ln(U+T)\right)T + \ln(T+\sqrt{T^2+1})\right) \\
&\leq \varepsilon(T,U)
\end{aligned}
$$

avec $\varepsilon(T,U) \to 0$ quand $U \to \infty$ (cela nous suffira). Comme le contour de $H_\chi(x,T,U)$ est plus éloigné des pôles, on privilégie cette fois la deuxième inégalité du lemme 4.4 pour majorer cette intégrale : pour $s = \sigma \pm iT$ avec $\sigma \leq -1/4$ et $T \geq 2$, on a

$$
\left|\frac{\mathrm{L}'}{\mathrm{L}}(s,\chi)\right| \leq -\frac{2}{\sigma} + \left|\ln\left(\frac{q}{\pi}\right)\right| + \frac{3\pi}{4} + \frac{\pi+1}{2T} + \ln\left(\frac{1+a-\sigma+T}{2}\right)
$$

et donc

$$
\begin{aligned}
(25) \qquad |H_\chi(x,T,U)| &\\
&\leq \frac{1}{\pi T} \int_{-\infty}^{-1/4} x^\sigma \left(\frac{29}{3} + \left|\ln\left(\frac{q}{\pi}\right)\right| + \frac{\pi+1}{2T} + \ln(1+a-\sigma+T)\right) d\sigma \\
&\leq \frac{x^{-1/4}}{\pi T \ln(x)}\left(\frac{29}{3} + \left|\ln\left(\frac{q}{\pi}\right)\right| + \frac{\pi+1}{2T} + \ln\left(\frac{5}{4}+a+T\right)\right) \\
&\quad + \frac{x^{-1/4}}{\pi T(\ln(x))^2}\,\frac{1}{5/4+a+T},
\end{aligned}
$$

Estimer l'intégrale $H^*_\chi(x,T)$ est plus ardu, puisque sa valeur est d'autant plus grande que le contour est près de zéros de $\mathrm{L}(\cdot,\chi)$. Commençons par remplacer l'intégrande par les fractions rationnelles $1/(s-\rho)$, afin de mieux étudier l'influence des zéros. Ceci nécessite le lemme suivant.

LEMME 4.7. *Soient $\sigma \in [-1/4, \sigma_0]$ et $T \geq 2$. Alors*

$$
\begin{aligned}
\left|\frac{\mathrm{L}'}{\mathrm{L}}(\sigma - iT,\chi) - \sum_{\substack{\rho \\ |\gamma+T|\leq 1}} \frac{1}{\sigma - iT - \rho}\right| &\leq \frac{1}{\pi}\left(6 + \frac{1}{2+2\sigma}\right)\ln\left(\frac{q(T+1)}{2\pi e}\right) \\
&\quad + \frac{0{,}317}{2+2\sigma}\ln(q(T+1)) + \left(\frac{1}{2+2\sigma}\left(2 + \frac{1}{\pi} + 6{,}401\right) + \frac{2}{\pi}\right) + f_q(T),
\end{aligned}
$$

où

$$
f_q(T) = \frac{2{,}634}{\pi(T-1)}\ln\left(\frac{q(T+1)}{2\pi e}\right) + \frac{5{,}59}{T-1} + \frac{12{,}802}{(T-1)^2} + \frac{(2T-1)\ln(T+1)}{(T-1)^2T^2}.
$$

Démonstration. On évalue l'identité (22) en $s = \sigma - iT$ puis en $s' = (\sigma+2) - iT$, et on soustrait les deux égalités résultantes. On a

$$\frac{\mathrm{L}'}{\mathrm{L}}(s,\chi) - \frac{\mathrm{L}'}{\mathrm{L}}(s',\chi) = \sum_\rho \left(\frac{1}{s-\rho} - \frac{1}{s'-\rho}\right) - \frac{1}{2}\frac{\Gamma'}{\Gamma}\left(\frac{s+a}{2}\right) + \frac{1}{2}\frac{\Gamma'}{\Gamma}\left(\frac{s'+a}{2}\right).$$

Or

$$\left|\frac{\Gamma'}{\Gamma}\left(\frac{s'+a}{2}\right) - \frac{\Gamma'}{\Gamma}\left(\frac{s+a}{2}\right)\right| \le \frac{1}{2}\sum_{k=0}^{\infty}\int_\sigma^{\sigma+2} \frac{dx}{((x+a)/2+k)^2 + (T/2)^2} \le \frac{\pi}{T},$$

puis

$$\left|\frac{\mathrm{L}'}{\mathrm{L}}(s,\chi) - \sum_{\substack{\rho \\ |\gamma+T|\le 1}} \frac{1}{s-\rho}\right| \le \sum_{\substack{\rho \\ |\gamma+T|>1}} \left|\frac{1}{s-\rho} - \frac{1}{s'-\rho}\right| \tag{26}$$

$$+ \sum_{\substack{\rho \\ |\gamma+T|\le 1}} \left|\frac{1}{s'-\rho}\right| + \frac{1}{\sigma+1} + \frac{\pi}{T}. \tag{27}$$

On a $|s'-\rho| \ge 1+\sigma$ pour tout zéro ρ non trivial car $0 < \mathrm{Re}(\rho) < 1$, donc

$$\sum_{\substack{\rho \\ |\gamma+T|\le 1}} \left|\frac{1}{s'-\rho}\right| \le \frac{1}{2+2\sigma}\left(\frac{1}{\pi}\left(\ln\left(\frac{q(T+1)}{2\pi e}\right)+1\right) + 0{,}317\ln(q(T+1)) + 6{,}401\right)$$

grâce au lemme 4.6, d'où une majoration de (27). À présent, (26) se calcule progressivement, à l'aide d'une intégration par parties et du lemme 4.6 :

$$\begin{aligned}\sum_{\substack{\rho \\ |\gamma+T|>1}} \left|\frac{1}{s-\rho} - \frac{1}{s'-\rho}\right| &= \sum_{\substack{\rho \\ |\gamma+T|>1}} \frac{2}{|s-\rho|\,|s'-\rho|} \\ &\le 2\Big(\int_1^{T-1} + \int_{T+1}^{\infty}\Big)\frac{dn_\chi(\gamma)}{(\gamma-T)^2} \le 4\left[\Big(\int_1^{T-1} + \int_{T+1}^{\infty}\Big)\frac{n_\chi(\gamma)\,d\gamma}{(\gamma-T)^3}\right] \\ &\le 4\int_1^{T-1}\left(\frac{\gamma}{\pi}\ln\left(\frac{q\gamma}{2\pi e}\right) + 0{,}317\ln(q\gamma) + 6{,}401\right)\frac{d\gamma}{(\gamma-T)^3} \\ &\quad + \int_{T+1}^{\infty}\left(\frac{\gamma}{\pi}\ln\left(\frac{q\gamma}{2\pi e}\right) + 0{,}317\ln(q\gamma) + 6{,}401\right)\frac{d\gamma}{(\gamma-T)^3}.\end{aligned}$$

Or

$$\int_{T+1}^{\infty}\left(\frac{\gamma}{\pi}\ln\left(\frac{q\gamma}{2\pi e}\right)+0{,}317\ln(q\gamma)+6{,}401\right)\frac{d\gamma}{(\gamma-T)^3}$$
$$\leq\frac{1}{\pi}\left(\ln\left(\frac{q(T+1)}{2\pi e}\right)\left(\frac{T}{2}+1\right)+\frac{\ln(T+1)}{2T}+\frac{1}{2}\right)$$
$$+\frac{0{,}317}{2}\left(\ln(q(T+1))-\frac{\ln(T+1)}{T^2}+\frac{1}{T}\right)+\frac{6{,}401}{2},$$

puis

$$\int_{1}^{T-1}\left(\frac{\gamma}{\pi}\ln\left(\frac{q\gamma}{2\pi e}\right)+0{,}317\ln(q\gamma)+6{,}401\right)\frac{d\gamma}{(\gamma-T)^3}$$
$$\leq\left(\frac{1}{(1-T)^2}-1\right)\times\left(\frac{T-1}{2\pi}\ln\left(\frac{q(T-1)}{2\pi e}\right)+\frac{0{,}317}{2}\ln(q(T-1))+\frac{6{,}401}{2}\right),$$

et donc, après avoir repris son souffle,

$$\frac{1}{4}\sum_{\substack{\rho\\|\gamma+T|>1}}\left|\frac{1}{s-\rho}-\frac{1}{s'-\rho}\right|$$
$$\leq\left(\frac{3}{2\pi}+\frac{0{,}317}{2\pi(T-1)}\right)\ln\left(\frac{q(T+1)}{2\pi e}\right)+\frac{1}{2\pi}+\frac{\ln(T+1)}{2\pi T}$$
$$+\frac{6{,}401}{2(T-1)^2}+\frac{0{,}317}{2}\left(\frac{1}{T}+\frac{\ln(q)}{(T-1)^2}+\frac{(2T-1)\ln(T+1)}{(T-1)^2T^2}\right),$$

d'où le résultat, après avoir regroupé et réordonné les différentes estimations. ∎

On a donc

$$\left|H_\chi^*(x,T)-\frac{1}{\pi}\operatorname{Im}\left(\int_{-1/4}^{\sigma_0}\frac{x^{\sigma-iT}}{\sigma-iT}\sum_{\substack{\rho\\|\gamma+T|\leq1}}\frac{1}{\sigma-iT-\rho}\,d\sigma\right)\right|$$
$$\leq\frac{ex-x^{-1/4}}{\pi T\ln(x)}\left(\frac{20}{3\pi}\ln\left(\frac{q(T+1)}{2\pi e}\right)+0{,}212\ln(q(T+1))+6{,}45+f_q(T)\right),$$

en majorant grossièrement les intégrales suivantes :

$$\int_{-1/4}^{\sigma_0}\frac{x^\sigma}{\sqrt{\sigma^2+T^2}\,(\sigma+1)}\,d\sigma\leq\frac{4}{3}\int_{-1/4}^{\sigma_0}\frac{x^\sigma}{\sqrt{\sigma^2+T^2}}\,d\sigma\leq\frac{4}{3}\,\frac{ex-x^{-1/4}}{T\ln(x)}.$$

Pour en finir avec l'estimation de $H_\chi^*(x,T)$, on doit encore vérifier que l'intégrale ci-dessus reste assez « petite ».

LEMME 4.8. *Soit $\rho = \beta + i\gamma$ avec $0 < \beta < 1$ et $\gamma \neq t$. Si $|t| \geq 2$, $x \geq 2$ et $1 < \sigma_1 \leq 3$, alors*

$$\left| \int_{-1/4}^{\sigma_1} \frac{x^{\sigma+it}}{(\sigma+it)(\sigma+it-\rho)}\, d\sigma \right| \leq \left(\sigma_1 + \frac{9}{4}\right) \frac{x^{\sigma_1}}{(|t|-1)(\sigma_1-\beta)}.$$

Démonstration. Supposons d'abord que $\gamma > t$. Soit B le rectangle (orienté dans le sens trigonométrique) dont les sommets ont pour affixes $\sigma_1 + i(t-1)$, $\sigma_1 + it$, $-1/4 + it$ et $-1/4 + i(t-1)$. Le théorème de Cauchy assure que

$$\int_B \frac{x^s}{s(s-\rho)}\, ds = 0,$$

puisque l'intégrande n'a pas de singularité à l'intérieur du rectangle. En outre, sur les arêtes du rectangle, à l'exception de celle joignant $-1/4+it$ et $\sigma_1 + it$, on peut le majorer par $x^{\sigma_1}/((|t|-1)(\sigma_1-\beta))$, d'où le résultat pour $\gamma > t$. On procède de même si $\gamma < t$, en changeant $i(t-1)$ en $i(t+1)$ dans les affixes des sommets du rectangle. ∎

Ceci prouve que

$$\left| \frac{1}{\pi} \operatorname{Im}\left(\int_{-1/4}^{\sigma_0} \frac{x^{\sigma-iT}}{\sigma-iT} \left(\sum_{\substack{\rho \\ |\gamma+T|\leq 1}} \frac{1}{\sigma-iT-\rho} \right) d\sigma \right) \right|$$
$$\leq \frac{\sigma_0+2{,}25}{\pi(T-1)} \left(\frac{1}{\pi} \left(\ln\left(\frac{q(T+1)}{2\pi e}\right) + 1 \right) + 0{,}317 \ln(q(T+1)) + 6{,}401 \right) ex \ln(x),$$

en recourant également au lemme 4.6. En fin de compte, on obtient

$$(28) \quad |H_\chi^*(x,T)|$$
$$\leq \frac{ex - x^{-1/4}}{\pi T \ln(x)} \left(\frac{20}{3\pi} \ln\left(\frac{q(T+1)}{2\pi e}\right) + 0{,}212 \ln(q(T+1)) + 6{,}45 + f_q(T) \right)$$
$$+ \frac{\sigma_0+2{,}25}{\pi(T-1)} \left(\frac{1}{\pi} \left(\ln\left(\frac{q(T+1)}{2\pi e}\right) + 1 \right) + 0{,}317 \ln(q(T+1)) + 6{,}401 \right) ex \ln(x).$$

En combinant (24), (25) et (28), on obtient

$$(29) \quad |R_\chi(x,T,U)|$$
$$\leq \frac{3{,}25ex\ln(x) + ex}{\pi(T-1)} \left(\frac{1}{\pi} \left(\ln\left(\frac{q(T+1)}{2\pi e}\right) + 1 \right) + 0{,}317 \ln(q(T+1)) + 6{,}401 \right)$$
$$+ \frac{ex}{\pi T \ln(x)} \left(\frac{20}{3\pi} \ln\left(\frac{q(T+1)}{2\pi e}\right) + 0{,}212 \ln(q(T+1)) + 6{,}45 + f_q(T) \right)$$
$$+ 9{,}24 \frac{x^{-1/4}}{\pi T \ln(x)} + \frac{x^{-1/4}}{\pi T (\ln(x))^2} \frac{1}{5/4+T} + \varepsilon(T,U).$$

On a fait le choix, pour simplifier, de ne pas retenir les contributions négatives en $x^{-1/4}/\ln(x)$, qui affectent très peu la suite des calculs.

4.1.3. *La formule explicite.* On en arrive enfin à une formule explicite pour ψ_χ en fonction des zéros ρ. On revient à la définition de $I_\chi(x,T,U)$ donnée en (23) ; soit $T \geq 2$ différent de la partie imaginaire d'un zéro non trivial. Par le théorème de Cauchy, $I_\chi(x,T,U)$ égale la somme des résidus de l'intégrande aux pôles à l'intérieur de $B_{T,U}$. On a donc, en prenant garde au résidu en $s=0$, selon la valeur de a,

$$I_\chi(x,T,U) = \sum_{\substack{\rho \\ |\gamma|<T}} \frac{x^\rho}{\rho} - \sum_{1\leq m\leq (U+1)/2} \frac{x^{a-2m}}{2m-a} + (1-a)\ln(x) + r(\chi), \tag{30}$$

où $r(\chi) = B(\chi) - \frac{1}{2}\ln(q/\pi) - \frac{1}{2}\frac{\Gamma'}{\Gamma}(1-a/2)$. Quand $U\to\infty$, (29) donne la formule explicite suivante, valide pour tout $x\geq 2$ et tout $T\geq 2$ différent de la partie imaginaire d'un zéro non trivial :

$$\begin{aligned}
&\left| I_\chi(x,T) - \sum_{\substack{\rho \\ |\gamma|<T}} \frac{x^\rho}{\rho} + \sum_{m=1}^{\infty} \frac{x^{a-2m}}{2m-a} - r(\chi) - (1-a)\ln(x) \right| \\
&\quad \leq \frac{3{,}25ex\ln(x)+ex}{\pi(T-1)}\left(\frac{1}{\pi}\left(\ln\left(\frac{q(T+1)}{2\pi e}\right)+1\right) + 0{,}317\ln(q(T+1)) + 6{,}401\right) \\
&\qquad + 9{,}24\frac{x^{-1/4}}{\pi T\ln(x)} + \frac{ex}{\pi T\ln(x)}\left(\frac{20}{3\pi}\ln\left(\frac{q(T+1)}{2\pi e}\right)\right. \\
&\qquad \left. + 0{,}212\ln(q(T+1)) + 6{,}45 + f_q(T)\right) + \frac{x^{-1/4}}{\pi T(\ln(x))^2}\,\frac{1}{(5/4+T)}.
\end{aligned}$$

On a alors presque ce qu'on veut :

THÉORÈME 4.9. *Si $x\geq 3$ et $T\geq 2$, alors*

$$\begin{aligned}
&|\psi_\chi(x) + S(x,T)| \\
&\quad \leq 8{,}37\frac{x(\ln(x))^2}{T} + \frac{e}{\pi}\,\frac{x(3{,}25\ln(x)+1)}{(T-1)}\big(0{,}64\ln(q(T+1)) + 5{,}82\big) \\
&\qquad + 7{,}84\ln(x+1) + 1{,}43\frac{\ln(x)}{T} + (6{,}09\ln(q) + 30{,}44) \\
&\qquad + \frac{e}{\pi}\,\frac{x}{T\ln(x)}(2{,}34\ln(q(T+1)) + 0{,}43 + f_q(T)) \\
&\qquad + \frac{x^{-1/4}}{T\ln(x)}\left(2{,}95 + \frac{1}{\pi\ln(x)(5/4+T)}\right),
\end{aligned}$$

où

$$S(x,T) = \sum_{\substack{\rho \\ |\gamma|\le T}} \frac{x^\rho}{\rho} - \sum_{\substack{\rho \\ |\rho|<1/2}} \frac{1}{\rho}, \tag{31}$$

les deux dernières sommes étant indexées par les zéros non triviaux de $\mathrm{L}(\cdot,\chi)$.

Démonstration. Écrivons

$$S'(x,T) = \sum_{\substack{\rho \\ |\gamma|< T}} \frac{x^\rho}{\rho} - \sum_{\substack{\rho \\ |\rho|<1/2}} \frac{1}{\rho}.$$

D'après (18), (19) et l'inégalité qui suit (30), on a

$$\begin{aligned}
&|\psi_\chi(x)+S'(x,T)| \\
&\le \frac{4^{1-1/\ln(3)}e^2}{T}x(\ln(x))^2+\frac{\ln(x)}{T\pi\ln(5/4)}+\frac{7}{\pi}\left(\frac{3}{2}\right)^{1+1/\ln(3)}\ln(x+1)+3\ln(x) \\
&\quad+\frac{3{,}25ex\ln(x)+ex}{\pi(T-1)}\left(\frac{1}{\pi}\left(\ln\left(\frac{q(T+1)}{2\pi e}\right)+1\right)+0{,}317\ln(q(T+1))+6{,}401\right) \\
&\quad+\frac{ex}{\pi T\ln(x)}\left(\frac{20}{3\pi}\ln\left(\frac{q(T+1)}{2\pi e}\right)+0{,}212\ln(q(T+1))+6{,}45+f_q(T)\right) \\
&\quad+\frac{1}{2}\ln\left(\frac{9}{8}\right)+9{,}24\frac{x^{-1/4}}{\pi T\ln(x)}+\frac{x^{-1/4}}{\pi T(\ln(x))^2}\,\frac{1}{(5/4+T)}+\left|r(\chi)+\sum_{\substack{\rho \\ |\rho|<1/2}}\frac{1}{\rho}\right|
\end{aligned}$$

pour $x \ge 3$ et $T \ge 2$ différent de la partie imaginaire d'un zéro non trivial. Avant de simplifier cette expression, estimons la dernière quantité :

$$\left|r(\chi)+\sum_{\substack{\rho \\ |\rho|<1/2}}\frac{1}{\rho}\right| \le \left|B(\chi)+\sum_{\substack{\rho \\ |\rho|<1/2}}\frac{1}{\rho}\right| + \frac{1}{2}\left|\ln\left(\frac{q}{\pi}\right)\right| + \frac{\gamma}{2} + \ln(2).$$

Admettons provisoirement le lemme suivant :

Lemme 4.10. *On a*

$$\left|B(\chi)+\sum_{\substack{\rho \\ |\rho|<1/2}}\frac{1}{\rho}\right| \le \frac{9}{\pi}\ln\left(\frac{q}{2\pi e}\right)+2{,}219\ln(q)+\frac{1}{2}\left|\ln\left(\frac{q}{\pi}\right)\right|+34{,}248.$$

Alors, ce lemme et les inégalités ci-dessus donnent le théorème si $T \neq \mathrm{Im}(\rho)$ pour tout zéro ρ de $\mathrm{L}(\cdot,\chi)$ (puisque dans ce cas $S(x,T) = S'(x,T)$). Par continuité du membre de droite de l'inégalité (comme fonction de T), on déduit l'inégalité pour $T = \mathrm{Im}(\rho)$ en remarquant que $S(x,T) = S'(x,T+\varepsilon)$ pour tout ε assez près de 0.

Il reste à démontrer le lemme. On a

$$\left|B(\chi)+\sum_{|\rho|<1/2}\frac{1}{\rho}\right| \le \left|B(\chi)+\sum_{\rho}\left(\frac{1}{2-\rho}+\frac{1}{\rho}\right)\right| + \left|\sum_{|\rho|<1}\frac{1}{2-\rho}\right| + \left|\sum_{|\rho|\ge 1}\left(\frac{1}{2-\rho}+\frac{1}{\rho}\right)\right| + \left|\sum_{1/2<|\rho|<1}\frac{1}{\rho}\right|$$

Posons $s=2$ dans (22). Alors, grâce au lemme 4.3,

$$\left|B(\chi)+\sum_{\rho}\left(\frac{1}{2-\rho}+\frac{1}{\rho}\right)\right| \le 1+\frac{1}{2}\left|\ln\left(\frac{q}{\pi}\right)\right|+\frac{\gamma}{2}.$$

De plus, si $|\rho|<1$, alors $|2-\rho|>1$, donc

$$\left|\sum_{|\rho|<1}\frac{1}{2-\rho}\right| \le n_\chi(1) \le \frac{1}{\pi}\ln\left(\frac{q}{2\pi e}\right)+0{,}317\ln(q)+6{,}401,$$

et de même

$$\left|\sum_{1/2<|\rho|<1}\frac{1}{\rho}\right| \le 2n_\chi(1) \le \frac{2}{\pi}\ln\left(\frac{q}{2\pi e}\right)+0{,}634\ln(q)+12{,}802.$$

Enfin, comme $\left|\frac{1}{2-\rho}+\frac{1}{\rho}\right| = \frac{2}{|(2-\rho)\rho|} \le \frac{2}{|\rho|^2}$, on a

$$\begin{aligned}\left|\sum_{|\rho|\ge 1}\left(\frac{1}{2-\rho}+\frac{1}{\rho}\right)\right| &\le 2n_\chi(1)+4\int_1^\infty \frac{n_\chi(t)\,dt}{t^3}\\ &\le \frac{6}{\pi}\ln\left(\frac{q}{2\pi e}\right)+1{,}268\ln(q)+13{,}756.\end{aligned}$$

En regroupant toutes ces estimations, on obtient le lemme annoncé. ∎

Remarque 4.11. Si on suppose HRG, alors la somme indexée par les zéros non triviaux de module au plus 1/2 est nulle. De plus, toujours sous cette hypothèse, on peut directement borner $B(\chi)$, puisque

$$\begin{aligned}B(\chi) &= -\sum_\rho \frac{1}{\rho} = -\frac{1}{2}\int_0^\infty \frac{dn_\chi(t)}{1/4+t^2} = -\int_0^\infty \frac{n_\chi(t)t\,dt}{(1/4+t^2)^2}\\ &\ge -\left(\frac{1}{2}\ln\left(\frac{q}{4\pi}\right)+0{,}634\ln\left(\frac{q}{2}\right)+12{,}802\right).\end{aligned}$$

C'est nettement mieux que l'estimation du lemme ci-dessus. Dans ce cas, le terme « constant » (comme fonction de x) du théorème précédent devient $1{,}64\ln(q)+12{,}14$.

Il reste à estimer $S(x,T)$. Si on suppose HRG, on peut avoir une bonne borne à partir des résultats déjà établis ; si on veut un résultat incondition-

nel, on doit montrer que les zéros ρ ne s'approchent pas trop de la droite $\mathrm{Re}(s) = 1$.

THÉORÈME 4.12. *Si* $\mathrm{L}(\cdot,\chi)$ *vérifie HRG, alors pour tout* $x \geq 3$,

$$|\psi_\chi(x)| \leq \sqrt{x}\ln(x)\left[\frac{1}{2\pi}\ln(x) + \frac{1}{\pi}\ln\left(\frac{q}{2\pi}\right) + 9{,}68 + \varepsilon_q(x)\right],$$

où

$$\varepsilon_q(x) = \frac{1{,}91\ln(q) + 34{,}16}{\ln(x)} + \frac{2{,}03}{(\ln(x))^2} + \frac{0{,}38}{(\ln(x))^3} + \frac{7{,}84}{\sqrt{x}} + \frac{1{,}64\ln(q) + 12{,}43}{\sqrt{x}\ln(x)} + \frac{0{,}58\ln(q) + 9{,}19}{\sqrt{x}\,(\ln(x))^2}.$$

Démonstration. Si $\mathrm{L}(\cdot,\chi)$ vérifie HRG, alors $|x^\rho| = \sqrt{x}$ pour tout zéro non trivial ρ, et par [Kad08, lemme 2.4] (où l'on remplace les constantes numériques par celles du lemme 4.6), on a

$$|S(x,T)| \leq \sqrt{x}\left(\frac{1}{\pi}\ln\left(\frac{q}{2\pi}\right)(\ln(T)+2) + \frac{(\ln(T))^2}{2\pi} + \left(\frac{1}{\pi} + 0{,}951\right)\ln(q) + 19{,}26 - \frac{0{,}317}{T}\right). \tag{32}$$

Considérant la majoration du théorème 4.9 et la remarque 4.11, on a donc, pour tout $T \geq 2$,

$$\begin{aligned}
&|\psi_\chi(x)| \\
&\leq 8{,}37\frac{x(\ln(x))^2}{T} + \frac{e}{\pi}\,\frac{x(3{,}25\ln(x)+1)}{(T-1)}\big(0{,}64\ln(q(T+1)) + 5{,}82\big) \\
&\quad + 7{,}84\ln(x+1) \\
&\quad + \sqrt{x}\left(\frac{1}{\pi}\ln\left(\frac{q}{2\pi}\right)(\ln(T)+2) + \frac{(\ln(T))^2}{2\pi} + 1{,}27\ln(q) + 19{,}26 - \frac{0{,}317}{T}\right) \\
&\quad + 1{,}43\frac{\ln(x)}{T} + (1{,}64\ln(q) + 12{,}14) \\
&\quad + \frac{e}{\pi}\,\frac{x}{T\ln(x)}\big(2{,}34\ln(q(T+1)) + 0{,}43 + f_q(T)\big) \\
&\quad + \frac{x^{-1/4}}{T\ln(x)}\left(2{,}95 + \frac{1}{\pi\ln(x)(5/4+T)}\right),
\end{aligned}$$

On pose $T = 1 + \frac{2\sqrt{x}\ln(x)}{\sqrt{3}\ln(3)}$ (on a $x \geq T \geq 3$ pour $x \geq 3$) pour obtenir le résultat désiré (on majore $f_q(T)$ par $(0{,}73\ln(q) + 9{,}67)x^{-1/2}$). ∎

Remarque 4.13. On a $\varepsilon_q(x) \leq 2{,}88\ln(q) + 48{,}08$ pour tout $x \geq 3$.

Si on ne suppose plus HRG, alors il est nécessaire d'en savoir davantage sur la proximité entre ρ et la droite $\mathrm{Re}(s) = 1$, à cause du traitement des termes x^ρ/ρ. Voici ce que nous savons.

Théorème 4.14 ([Kad02] et [AK14, remarque 2]). *La fonction* $\mathrm{L}(\cdot,\chi)$ *a au plus un zéro* $\rho = \beta + i\gamma$ *dans la région*

$$\beta \geq 1 - \frac{1}{4{,}0904\ln(q)}, \qquad |\gamma| \leq \frac{1}{4\ln(q)}.$$

Ce zéro, s'il existe, est réel et s'appelle zéro de Siegel. *De plus, il n'y a pas d'autre zéro dans la région*

$$\beta \geq 1 - \frac{1}{6{,}5\ln(q\max(1,|\gamma|))}.$$

Cela nous permet d'en déduire :

Théorème 4.15. *Pour tout* $x \geq \exp(6{,}5(\ln(3q))^2)$, *on a*

$$\left|\psi_\chi(x) + \frac{x^{\beta_0}}{\beta_0}\right| \leq 2200x\exp\left(-\frac{\sqrt{\ln(x)}}{10{,}2}\right)$$

où β_0 *est l'éventuel zéro de Siegel de* $\mathrm{L}(\cdot,\chi)$ *; le terme* x^{β_0} *peut être supprimé si* β_0 *n'existe pas.*

Démonstration. Pour tout $T \geq 2$ on a

$$\left|\psi_\chi(x) + \frac{x^{\beta_0}}{\beta_0}\right| \leq |\psi_\chi(x) + S(x,T)| + \left|S(x,T) - \frac{x^{\beta_0}}{\beta_0}\right|.$$

Pour majorer le second terme, remarquons que si ρ est un zéro non trivial différent du zéro de Siegel, et tel que $|\mathrm{Im}(\rho)| \leq T$, alors d'après le théorème 4.14 on a

$$|x^\rho| \leq x\exp\left(-\frac{\ln(x)}{6{,}5\ln(qT)}\right),$$

et donc

$$\begin{aligned}\left|S(x,T) - \frac{x^{\beta_0}}{\beta_0}\right| &= \left|\sum_{\substack{\rho\\ |\gamma|\leq T\\ \rho\neq\beta_0}} \frac{x^\rho}{\rho} - \sum_{\substack{\rho\\ |\rho|<1/2}} \frac{1}{\rho}\right| \\ &\leq \sum_{\substack{|\rho|\geq 1/2\\ |\gamma|\leq T\\ \rho\neq\beta_0}} \frac{x}{|\rho|}\exp\left(-\frac{\ln(x)}{6{,}5\ln(qT)}\right) + \left|\sum_{|\rho|<1/2}\left(\frac{x^\rho}{\rho} - \frac{1}{\rho}\right)\right|.\end{aligned}$$

Suivant un raisonnement analogue à celui fait pour obtenir (32), on sait estimer la première somme. Dans la seconde somme, $1/|\rho|$ est d'autant plus grand que ρ est « près » de 0 ; or, d'après le théorème 4.14 et grâce à la

symétrie $s \leftrightarrow 1-s$ de l'équation fonctionnelle vérifiée par $\mathrm{L}(\cdot,\chi)$, $1-\beta_0$ est le zéro le plus « proche » de 0, et les autres zéros ρ vérifient $|\rho| \geq \frac{1}{6{,}5\ln(q)}$, donc

$$\begin{aligned}\Big|\sum_{|\rho|<1/2}\Big(\frac{x^\rho}{\rho}-\frac{1}{\rho}\Big)\Big| &= \Big|\frac{x^{1-\beta_0}}{1-\beta_0}-\frac{1}{1-\beta_0}\Big| + \sum_{\substack{|\rho|<1/2\\ \rho\neq 1-\beta_0}}\frac{\sqrt{x}+1}{|\rho|}\\ &\leq x^{1/(4\ln(q))}\ln(x)+6{,}5\ln(q)(\sqrt{x}+1)\Big(\frac{1}{\pi}\ln\Big(\frac{q}{2\pi e}\Big)+0{,}317\ln(q)+6{,}401\Big),\end{aligned}$$

la quantité dépendant de $1-\beta_0$ étant majorée grâce à l'inégalité des accroissements finis.

Pour résumer, en regroupant les estimations ci-dessus et la majoration du théorème 4.9, pour tout $T \geq 2$ on a

$$\begin{aligned}\Big|\psi_\chi(x)+\frac{x^{\beta_0}}{\beta_0}\Big| &\leq \Big(\frac{1}{\pi}\ln\Big(\frac{q}{2\pi}\Big)(\ln(T)+2)+\frac{(\ln(T))^2}{2\pi}+1{,}27\ln(q)+19{,}26-\frac{0{,}317}{T}\Big)\\ &\qquad\times x\exp\Big(-\frac{\ln(x)}{6{,}5\ln(qT)}\Big)\\ &\quad+8{,}37\frac{x(\ln(x))^2}{T}+\frac{e}{\pi}\,\frac{x(3{,}25\ln(x)+1)}{(T-1)}(0{,}64\ln(q(T+1))+5{,}82)\\ &\quad+x^{1/4}\ln(x)+1{,}43\frac{\ln(x)}{T}+6{,}5\sqrt{x}\ln(q)(0{,}64\ln(q)+5{,}5)\\ &\quad+7{,}84\ln(x+1)+4{,}12(\ln(q))^2+35{,}74\ln(q)+30{,}44\\ &\quad+\frac{e}{\pi}\,\frac{x}{T\ln(x)}\big(2{,}34\ln(q(T+1))+0{,}43+f_q(T)\big)\\ &\quad+\frac{x^{-1/4}}{T\ln(x)}\Big(2{,}95+\frac{1}{\pi\ln(x)(5/4+T)}\Big).\end{aligned}$$

Posons $T=(1/q)\exp\big(2\sqrt{\ln(x)/6{,}5}\big)$, de sorte qu'on ait

$$6{,}5\ln(qT)=2\sqrt{6{,}5\ln(x)}.$$

En particulier, pour tout $x \geq \exp(6{,}5(\ln(3q))^2)$, on a

$$T \geq 3\exp\big(\sqrt{\ln(x)/6{,}5}\big) \geq 3,$$

et $\ln(q) \leq \sqrt{\ln(x)/6{,}5}-\ln(3)$, ce qui permet d'obtenir une majoration exclusivement en fonction de x :

$$\begin{aligned}\left|\psi_\chi(x)+\frac{x^{\beta_0}}{\beta_0}\right| &\le \left(\frac{3}{2\pi}\,\frac{\ln(x)}{6{,}5}+0{,}2\sqrt{\frac{\ln(x)}{6{,}5}}+15{,}48\right)x\exp\left(-\frac{1}{2}\sqrt{\frac{\ln(x)}{6{,}5}}\right)\\ &+\left(2{,}79(\ln(x))^2+\frac{e}{2\pi}(3{,}25\ln(x)+1)\left(1{,}28\sqrt{6{,}5\ln(x)}+6{,}01\right)\right)\\ &\qquad\qquad\times x\exp\left(-\sqrt{\frac{\ln(x)}{6{,}5}}\right)\\ &+\frac{e}{3\pi}\left(11{,}94\sqrt{\ln(x)}+0{,}68\right)\frac{x}{\ln(x)}\exp\left(-\sqrt{\frac{\ln(x)}{6{,}5}}\right)\\ &+\frac{e}{3\pi}\left(2{,}18\sqrt{\ln(x)}+11{,}35\right)\frac{x}{\ln(x)}\exp\left(-2\sqrt{\frac{\ln(x)}{6{,}5}}\right)\\ &+\sqrt{6{,}5x\ln(x)}\left(0{,}64\sqrt{\frac{\ln(x)}{6{,}5}}+4{,}8\right)+x^{\frac{1}{4}}\ln(x)+7{,}84\ln(x+1)+4{,}12\frac{\ln(x)}{6{,}5}\\ &+\left(0{,}48\ln(x)+\frac{x^{-1/4}}{3\ln(x)}\left(2{,}95+\frac{4}{17\pi\ln(x)}\right)\right)\exp\left(-\sqrt{\frac{\ln(x)}{6{,}5}}\right)+26{,}69\sqrt{\frac{\ln(x)}{6{,}5}}.\end{aligned}$$

À présent, une simple étude de fonctions permet de comparer les quantités en jeu de la forme $x^\alpha(\ln(x))^\beta$ (où $\alpha<1$ et $\beta\in\mathbb{R}$) à $x\exp\bigl(-\frac{1}{4}\sqrt{\ln(x)/6{,}5}\bigr)$ et de la forme $(\ln(x))^\gamma$ (où $\gamma\in\mathbb{R}$) à $\exp\bigl(\pm\frac{1}{4}\sqrt{\ln(x)/6{,}5}\bigr)$ pour obtenir le résultat : en effet, pour $a>0$ on a

$$x^\alpha(\ln(x))^\beta \le \begin{cases}\dfrac{\exp\bigl(2\beta-\bigl(\frac{1+\sqrt{1+16\beta a^2(1-\alpha)}}{4a\sqrt{1-\alpha}}\bigr)^2\bigr)}{\bigl(\frac{1+\sqrt{1+16\beta a^2(1-\alpha)}}{4a}\bigr)^{2\beta}}\,x\exp\left(-\dfrac{\sqrt{\ln(x)}}{a}\right) & \text{si } \beta\ge 0,\\[2ex] \dfrac{1}{3}\exp\left(\dfrac{1}{a}\sqrt{\dfrac{\ln(3)}{1-\alpha}}\right)\left(\dfrac{\ln(3)}{1-\alpha}\right)^\beta x\exp\left(-\dfrac{\sqrt{\ln(x)}}{a}\right) & \text{si } \beta<0 \text{ et } a>-1/4\sqrt{\beta}\end{cases}$$

et

$$(\ln(x))^\gamma \le \begin{cases}(2a\gamma/e)^{2\gamma}\exp\bigl(\sqrt{\ln(x)}/a\bigr) & \text{si } \gamma\ge 0,\\ (\ln(3))^\gamma\exp\bigl(-\sqrt{\ln(3)}/a\bigr) & \text{si } \gamma<0.\end{cases}$$ ∎

Remarquons, enfin, que suivant des calculs qui nous furent montrés par Raabe, il n'est pas difficile d'obtenir une mesure effective de l'écart entre 1 et le zéro éventuel de Siegel dans le cas qui nous intéresse.

Proposition 4.16. *Si β_0 est le zéro de Siegel de $\mathrm{L}(\cdot,\chi)$ pour $\chi=\left(\frac{q}{\cdot}\right)$ avec $q\le -3$, alors*

$$1-\beta_0 \ge \frac{0{,}4}{\sqrt{|q|}\,(\ln(e|q|))^2}.$$

Démonstration. On majore $\mathrm{L}'(\cdot,\chi)$ sur le segment $\big[1-\frac{1}{4{,}0904\ln(q)},1\big]$, et on utilise l'inégalité des accroissements finis. Or nous avons, pour $\sigma\in\big[1-\frac{1}{4{,}0904\ln(|q|)},1\big]$,

$$|\mathrm{L}'(\sigma,\chi)|\le\int_1^{e\sqrt{|q|}}\frac{\ln(x)}{x^\sigma}\,dx+\sigma\int_{e\sqrt{|q|}}^{\infty}\Big|\sum_{n\le x}\chi(n)\Big|\frac{\ln(x)-1}{x^{\sigma+1}}\,dx.$$

Il est démontré dans [Pom11, théorème 1] que pour tout $x\ge 1$,

$$\Big|\sum_{n\le x}\chi(n)\Big|\le\sqrt{|q|}\bigg(\frac{2}{\pi^2}\ln(|q|)+\frac{4}{\pi^2}\ln(\ln(|q|))+\frac{3}{2}\bigg),\tag{33}$$

donc, comme $1-\sigma\le(4{,}0904\ln(|q|))^{-1}$,

$$\begin{aligned}|\mathrm{L}'(\sigma,\chi)|&\le\bigg(4\ln(|q|)+\frac{1}{e}\bigg(\frac{2}{\pi^2}\ln(|q|)+\frac{4}{\pi^2}\ln(\ln(|q|))+\frac{3}{2}\bigg)\bigg)\\&\quad\times\ln\big(e\sqrt{|q|}\big)\big(e\sqrt{|q|}\big)^{1/(4\ln(|q|)))}\\&\le 2{,}6(\ln(e|q|))^2.\end{aligned}$$

On conclut avec l'inégalité

$$1-\beta_0\ge\frac{\mathrm{L}(1,\chi)}{\max\limits_{[\beta_0,1]}(|\mathrm{L}'(\cdot,\chi)|)},$$

puisqu'on sait que $\mathrm{L}(1,\chi)\ge\pi/\big(3\sqrt{|q|}\big)$ d'après la formule des classes. ∎

4.2. Fonctions réciproques de Lambert. La fonction

$$\text{ʍ}:\mathbb{R}\to\mathbb{R},\qquad x\mapsto xe^x,$$

admet le tableau de variations suivant :

x	$-\infty$		-1		$+\infty$
$\text{ʍ}'(x)$		$-$	0	$+$	
$\text{ʍ}(x)$	0	↘	$-1/e$	↗	$+\infty$

Elle définit donc deux applications réciproques $\mathrm{w}_1:]-1/e,+\infty[\to]-1,+\infty[$ et $\mathrm{w}_{-1}:]-1/e,0[\to]-\infty,-1[$, la première étant strictement croissante et la seconde strictement décroissante. Leurs comportements asymptotiques sont connus.

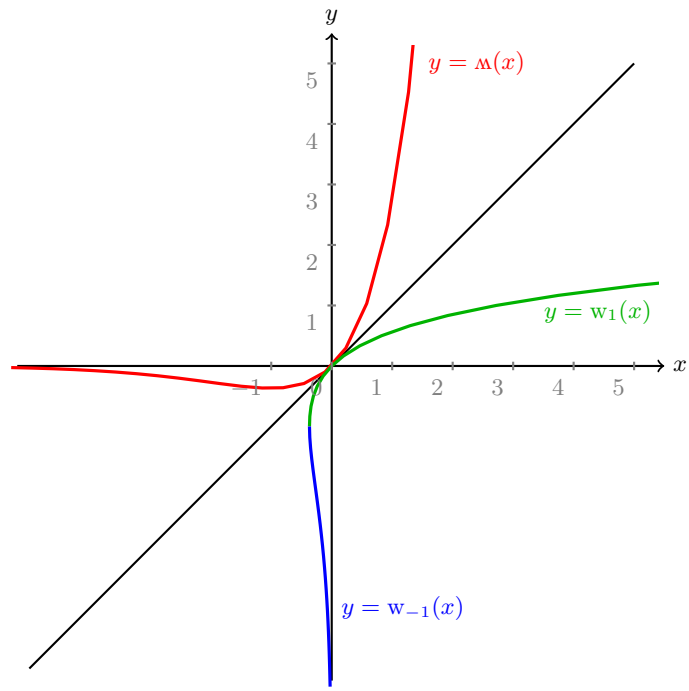

Fig. 2. La fonction ʍ et ses réciproques

PROPOSITION 4.17 ([CGH+96, (4.18)]). *Les fonctions* w_1 *et* w_{-1} *vérifient les comportements asymptotiques suivants :*

$$\mathrm{w}_{-1}(x) = \ln(-x) - \ln(-\ln(-x)) + O\left(\frac{\ln(-\ln(-x))}{\ln(-x)}\right), \quad x \to 0,$$

$$\mathrm{w}_1(x) = \ln(x) - \ln(\ln(x)) + O\left(\frac{\ln(\ln(x))}{\ln(x)}\right), \qquad x \to \infty.$$

COROLLAIRE 4.18. *Les fonctions de Lambert vérifient les inégalités*

$$\ln(-x) - \ln(-\ln(-x)) - 1/2 \le \mathrm{w}_{-1}(x) \le \ln(-x) - \ln(-\ln(-x)) \qquad \textit{pour } -1/e \le x < 0,$$

et

$$\ln(x) - \ln(\ln(x)) \le \mathrm{w}_1(x) \le \ln(x) - \ln(\ln(x)) + 1/2 \qquad \textit{pour } x \ge e.$$

Démonstration. La proposition 4.17 démontre que l'application

$$f :]-1/e, 0[\to \mathbb{R}, \qquad x \mapsto \mathrm{w}_{-1}(x) - (\ln(-x) - \ln(-\ln(-x))),$$

tend vers 0 quand x tend vers 0, et elle s'annule aussi en $-1/e$. De plus, comme

$$f'(x) = \frac{1}{x}\left(\frac{1}{1 + 1/\mathrm{w}_{-1}(x)} - \frac{1}{\ln(-x)} + 1\right),$$

une étude rapide montre que f_{-1} change de variation une seule fois (en le réel x tel que $\mathrm{w}_{-1}(x) = \ln(-x) - 1$), en commençant par décroître. Donc f_{-1} est toujours négative, de minimum $f_{-1}(x) > -1/2$ d'après toute méthode d'approximation des extremums, d'où le résultat pour w_{-1}. On procède exactement de la même manière pour démontrer le second encadrement. ∎

On en déduit le corollaire suivant, que nous utilisons à loisir dans la section 3. Comme on peut s'en douter, en voyant les inégalités vérifiées par les fonctions de Lambert et la démonstration du corollaire à suivre, les inégalités sont près d'être optimales.

COROLLAIRE 4.19. *Soient $\alpha > 0$, $b > 0$ et $s \geq 2$ trois réels.*

(1) *Si $s \geq e^{1/(2\alpha)}(\alpha b/\ln(\alpha b))^{1/\alpha}$, alors $s^\alpha \ln(s) \geq b$.*

(2) *Si $s \geq e^{1/(2\alpha)}((b/\alpha)\ln(b/\alpha))^{1/\alpha}$, alors $s^\alpha/\ln(s) \geq b$.*

Démonstration. L'inégalité $s^\alpha \ln(s) \geq b$ peut se réécrire $\mathrm{m}(\ln(s^\alpha)) \geq \alpha b$, qui est équivalente à $\ln(s^\alpha) \geq \mathrm{w}_1(\alpha b)$, d'où le premier résultat en invoquant le corollaire 4.18. Le deuxième s'obtient semblablement. ∎

Remerciements. Nous remercions Pascal Autissier, Fabien Pazuki et Gaël Rémond pour leurs indications très précieuses.

Références

[AK14] J.-H. Ahn and S.-H. Kwon, *Some explicit zero-free regions for Hecke L-functions*, J. Number Theory 145 (2014), 433–473.

[BP05] M. Baker and C. Petsche, *Global discrepancy and small points on elliptic curves*, Int. Math. Res. Notices 2005, no. 61, 3791–3834.

[Col98] P. Colmez, *Sur la hauteur de Faltings des variétés abéliennes à multiplication complexe*, Compos. Math. 111 (1998), 359–368.

[CGH+96] R. M. Corless, G. H. Gonnet, D. E. G. Hare, D. J. Jeffrey and D. E. Knuth, *On the Lambert W function*, Adv. Comput. Math. 5 (1996), 329–359.

[CS86] G. Cornell and J. H. Silverman, *Arithmetic Geometry*, Springer, New York, 1986.

[Dav67] H. Davenport, *Multiplicative Number Theory*, Markham, Chicago, IL, 1967.

[Dav97] S. David, *Points de petite hauteur sur les courbes elliptiques*, J. Number Theory 64 (1997), 104–129.

[Fal84] G. Faltings, *Calculus on arithmetic surfaces*, Ann. of Math. (2) 119 (1984), 387–424.

[GM17] A. Galateau and V. Mahé, *Some consequences of Masser's counting theorem on elliptic curves*, Math. Z. 285 (2017), 613–629.

[GR14] É. Gaudron et G. Rémond, *Polarisations et isogénies*, Duke Math. J. 163 (2014), 2057–2108.

[GS00] A. Granville and H. M. Stark, *abc implies no "Siegel zeros" for L-functions of characters with negative discriminant*, Invent. Math. 139 (2000), 509–523.

[Hab10] P. Habegger, *Weakly bounded height on modular curves*, Acta Math. Vietnam. 35 (2010), 43–69.

[HS88] M. Hindry and J. H. Silverman, *The canonical height and integral points on elliptic curves*, Invent. Math. 93 (1988), 419–450.

[HS99] M. Hindry et J. Silverman, *Sur le nombre de points de torsion rationnels sur une courbe elliptique*, C. R. Acad. Sci. Paris Sér. I Math. 329 (1999), 97–100.

[HS00] M. Hindry and J. H. Silverman, *Diophantine Geometry. An Introduction*, Grad. Texts in Math. 201, Springer, New York, 2000.

[Hri85] P. Hriljac, *Heights and Arakelov's intersection theory*, Amer. J. Math. 107 (1985), 23–38.

[IMS09] Y. Ihara, V. K. Murty and M. Shimura, *On the logarithmic derivatives of Dirichlet L-functions at $s = 1$*, Acta Arith. 137 (2009), 253–276.

[Kad02] H. Kadiri, *An explicit zero-free region for Dirichlet L-functions*, thèse, Univ. de Lille 1, 2002.

[Kad08] H. Kadiri, *Short effective intervals containing primes in arithmetic progressions and the seven cubes problem*, Math. Comp. 77 (2008), 1733–1748.

[Lan78] S. Lang, *Elliptic Curves: Diophantine Analysis*, Grundlehren Math. Wiss. 231, Springer, Berlin, 1978.

[Lan83] S. Lang, *Fundamentals of Diophantine Geometry*, Springer, New York, 1983.

[Lan88] S. Lang, *Introduction to Arakelov Theory*, Springer, New York, 1988.

[Lau83] M. Laurent, *Minoration de la hauteur de Néron–Tate*, dans : Seminar on Number Theory, Paris 1981–82, Progr. Math. 38, Birkhäuser Boston, Boston, MA, 1983, 137–151.

[Mas89] D. W. Masser, *Counting points of small height on elliptic curves*, Bull. Soc. Math. France 117 (1989), 247–265.

[Pet06] C. Petsche, *Small rational points on elliptic curves over number fields*, New York J. Math. 12 (2006), 257–268.

[Pom11] C. Pomerance, *Remarks on the Pólya–Vinogradov inequality*, Integers 11 (2011), 531–542.

[Ram07] O. Ramaré, *Eigenvalues in the large sieve inequality*, Funct. Approx. Comment. Math. 37 (2007), 399–427.

[Rat04] N. Ratazzi, *Théorème de Dobrowolski–Laurent pour les extensions abéliennes sur une courbe elliptique à multiplication complexe*, Int. Math. Res. Notices 2004, no. 58, 3121–3152.

[Rém17] G. Rémond, *Variétés abéliennes et ordres maximaux*, Rev. Mat. Iberoamer. 33 (2017), 1173–1195.

[RS62] J. B. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. 6 (1962), 64–94.

[Ser81] J.-P. Serre, *Quelques applications du théorème de densité de Chebotarev*, Inst. Hautes Études Sci. Publ. Math. 54 (1981), 323–401.

[ST61] G. Shimura and Y. Taniyama, *Complex Multiplication of Abelian Varieties and its Applications to Number Theory*, Publ. Math. Soc. Japan 6, Math. Soc. Japan, Tokyo, 1961.

[Sil94] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Grad. Texts in Math. 151, Springer, New York, 1994.

[Sil09] J. H. Silverman, *The Arithmetic of Elliptic Curves*, $2^{\text{ème}}$ éd., Grad. Texts in Math. 106, Springer, Dordrecht, 2009.

[Szp90] L. Szpiro, *Sur les propriétés numériques du dualisant relatif d'une surface arithmétique*, dans : The Grothendieck Festschrift, Vol. III, Progr. Math. 88, Birkhäuser Boston, Boston, MA, 1990, 229–246.

[Tôy55] H. Tôyama, *A note on the different of the composed field*, Kōdai Math. Sem. Rep. 7 (1955), 43–44.

[Tru15] T. S. Trudgian, *An improved upper bound for the error in the zero-counting formulae for Dirichlet L-functions and Dedekind zeta-functions*, Math. Comp. 84 (2015), 1439–1450.

[Win15] B. Winckler, *Intersection arithmétique et problème de Lehmer elliptique*, thèse, Univ. de Bordeaux, 2015.

Bruno Winckler
École Normale Supérieure (ENS) de Lyon
Unité de Mathématiques Pures et Appliquées
46, allée d'Italie
69364 Lyon Cedex 07, France
E-mail: bruno.winckler@ens-lyon.fr

Abstract (will appear on the journal's web site only)

We consider the problem of lower bounds for the canonical height on elliptic curves, aiming for the conjecture of Lehmer. Our main result is an explicit version of a theorem of Laurent (who proved this conjecture for elliptic curves with CM up to an ε exponent) using arithmetic intersection, emphasizing the dependence on parameters linked to the elliptic curve; if GRH holds, then our lower bound for the canonical height of a non-torsion point only depends on the relative degree of the point, and on the degree of the base field of its elliptic curve. We also provide explicit estimates for the Faltings height of an elliptic curve with CM, thanks to an explicit version of Dirichlet's theorem on arithmetic progressions, in some sense.