Journal de Théorie des Nombres de Bordeaux

anciennement Séminaire de Théorie des Nombres de Bordeaux

Bernard DE MATHAN

Sur l'approximation rationnelle p-adique

Tome 31, n° 2 (2019), p. 417-430.

<http://jtnb.centre-mersenne.org/item?id=JTNB_2019__31_2_417_0>

Journal de Théorie des Nombres
de Bordeaux **31** (2019), 417–430

Sur l'approximation rationnelle p-adique

par Bernard DE MATHAN

Résumé. We prove that a conjecture of Einsiedler and Kleinbock, about the simultaneous approximation of a p-adic number and of a real number by a rational number, is true when the p-adic number is quadratic.

Abstract. Nous démontrons ici qu'une conjecture d'Einsiedler et Kleinbock, concernant l'approximation d'un nombre p-adique et d'un nombre réel par le *même* nombre rationnel est satisfaite dès que le nombre p-adique est quadratique.

1. Introduction

Soit p un nombre premier. Dans [3], Einsiedler et Kleinbock formulent la conjecture que pour tout couple $(\alpha, \beta) \in \mathbb{Q}_p \times \mathbb{R}$ différent de $(0,0)$, on a :

$$\inf_{rs \neq 0} |s||s\alpha - r|_p |s\beta - r| = 0 \tag{1}$$

($(r,s) \in \mathbb{Z}$). Ils remarquent que cet énoncé englobe la conjecture de Littlewood p-adique [5] selon laquelle on aurait pour tout nombre réel $\beta \neq 0$:

$$\inf_{rs \neq 0} |s|_p |s||s\beta - r| = 0. \tag{2}$$

En effet, pour $\alpha = 0$ et $\beta \neq 0$, la condition (1) :

$$\inf_{rs \neq 0} |s||r|_p |s\beta - r| = 0, \tag{1'}$$

est équivalente à

$$\inf_{rs \neq 0} |r||r|_p |s\beta - r| = 0,$$

qui n'est autre que (2) appliquée à $1/\beta$.

Nous nous intéressons ici à la conjecture d'Einsiedler et Kleinbock dans le cas où $\beta = 0$, c'est-à-dire que l'on demande si la condition

$$\inf_{rs \neq 0} |r||s||s\alpha - r|_p = 0 \tag{3}$$

est satisfaite pour tout $\alpha \in \mathbb{Q}_p \backslash \{0\}$. Cette condition équivaut à :

$$\inf_{rs \neq 0} |r||s| \left| \alpha - \frac{r}{s} \right|_p = 0. \tag{3'}$$

Manuscrit reçu le 15 octobre 2018, accepté le 21 décembre 2018.
Classification Mathématique (2010). 11J13, 11J61, 11J86.
Mots-clefs. Approximation rationnelle, conjecture d'Einsiedler et Kleinbock.

En effet, (3′) implique (3) puisque $|s\alpha - r|_p \leq |\alpha - r/s|_p$. Mais il est clair que dans la condition (3), on peut se limiter aux couples d'entiers (r, s) premiers entre eux, et dès lors, si la condition (3) est satisfaite, (3′) l'est aussi.

On peut aussi remarquer que dans le cas où la condition suivante, plus précise que la condition (3) :

$$\inf_{|r|>|s|>0} |r||s||s\alpha - r|_p = 0 \tag{3''}$$

est réalisée, la condition (1) a lieu pour tout $\beta \in \mathbb{R}$.

Einsiedler et Kleinbock démontrent ([3, Theorem 5.2]) que l'ensemble des couples $(\alpha, \beta) \in \mathbb{Q}_p \times \mathbb{R}$ ne satisfaisant pas à la condition (1) est de dimension de Hausdorff nulle. *A fortiori* l'ensemble des nombres p-adiques α ne satisfaisant pas à (3) est de dimension de Hausdorff nulle, mais nous ignorons si la condition (3) est satisfaite pour tout $\alpha \neq 0$ dans $\mathbb{Q}_p$. On peut remarquer que si le nombre p-adique α est bien approché par des nombres rationnels, c'est-à-dire si

$$\inf_{rs\neq 0} \max\{|r|, |s|\}^2 |s\alpha - r|_p = 0,$$

on a trivialement (3), et même (1) pour tout nombre réel β. Mais d'après une version p-adique du théorème de Liouville, un nombre p-adique quadratique α est en ce sens mal approchable par des nombres rationnels, c'est-à-dire que :

$$\inf_{rs\neq 0} \max\{|r|, |s|\}^2 |s\alpha - r|_p > 0. \tag{4}$$

Une démonstration classique, que l'on peut limiter sans perte de généralité au cas où α est entier algébrique, en est de remarquer que dans ce cas, pour r et s entiers rationnels non nuls, la norme $N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(s\alpha - r)$ est un nombre entier non nul, donc que :

$$|N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(s\alpha - r)||N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(s\alpha - r)|_p \geq 1. \tag{4a}$$

Or si on désigne par σ l'automorphisme différent de l'identité du corps $\mathbb{Q}(\alpha)$, on a

$$N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(s\alpha - r) = (s\alpha - r)(s\sigma(\alpha) - r) = r^2 - rs\,\mathrm{Tr}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha) + s^2 N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha),$$

donc

$$|N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(s\alpha - r)| \leq (1 + |\mathrm{Tr}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha)| + |N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha)|) \max\{|r|, |s|\}^2. \tag{4b}$$

Mais il est clair que pour prouver (4), on peut se limiter au cas où r et s sont premiers entre eux, et où $|s\alpha - r|_p < 1$; comme $|\alpha|_p \leq 1$, cela implique que $|s|_p = 1$. En supposant de plus, ce qui est loisible, que $|s\alpha - r|_p < |\alpha - \sigma(\alpha)|_p \leq 1$, on obtient $|s\sigma(\alpha) - r|_p = |\alpha - \sigma(\alpha)|_p$, donc

$$|N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(s\alpha - r)|_p = |\alpha - \sigma(\alpha)|_p |s\alpha - r|_p. \tag{4c}$$

On déduit alors de (4a), (4b), et (4c), que :

$$|s\alpha - r|_p \geq \frac{1}{|\alpha - \sigma(\alpha)|_p(1 + |\operatorname{Tr}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha)| + |N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha)|)} \max\{|r|, |s|\}^{-2}.$$

Nous allons démontrer que cependant la condition (3), et même la condition (1) pour tout nombre réel β, sont satisfaites si α est un nombre p-adique quadratique. Nous serons conduit à utiliser les notations de Vinogradov entre quantités positives ou nulles, l'écriture $A \ll B$ signifiant qu'il existe une constante $c > 0$ telle que $A \leq cB$, et $A \asymp B$, que l'on a $A \ll B$ et $B \ll A$. D'après le théorème de Liouville rappelé ci-dessus, si α est un nombre p-adique quadratique, et si r et s sont des entiers rationnels non nuls tels que $|\alpha - r/s|_p \leq H^{-2}$ avec $H > 0$, alors $\max\{|r|, |s|\} \gg H$. Mais nous allons montrer qu'il se peut que le *minimum* de $|r|$ et de $|s|$ soit petit devant H. Nous établissons le résultat suivant :

Théorème 1.1. *Soit α un nombre quadratique dans $\mathbb{Q}_p$. Il existe un ensemble infini de couples (Q_0, Q_1) de nombres entiers avec $|Q_1| \geq 2$, tels que*

$$0 < Q_0 \ll \frac{|Q_1|}{\log |Q_1|}, \tag{5}$$

et

$$|\alpha - \frac{Q_1}{Q_0}|_p \asymp Q_1^{-2}, \tag{6}$$

les constantes impliquées ne dépendant que de α. De façon plus précise, il existe une constante $\theta \geq 1$ pour laquelle pour tout $M \geq 1$, il existe un couple (Q_0, Q_1) satisfaisant aux conditions (5) *et* (6)*, avec*

$$M \leq \log |Q_1| \ll M^{\theta}.$$

Ce résultat admet le corollaire évident :

Corollaire 1.2. *Tout nombre quadratique appartenant à $\mathbb{Q}_p$ vérifie la condition* (3)*. De façon plus précise, on a :*

$$\liminf_{|r|>|s|>0} (\log |r|)|r||s| \left|\alpha - \frac{r}{s}\right|_p < +\infty.$$

Il suffit en effet d'appliquer le théorème 1.1 avec $Q_1 = r$ et $Q_0 = s$. La condition (3″) étant vérifiée, une conséquence du corollaire 1.2 est que :

Corollaire 1.3. *Pour tout nombre quadratique α appartenant à $\mathbb{Q}_p$ et tout nombre réel β, le couple (α, β) satisfait à la condition* (1)*, et l'on a :*

$$\liminf_{|r|>|s|>0} (\log |r|)|s||s\alpha - r|_p|s\beta - r| < +\infty.$$

Nous remarquons enfin que le théorème 1.1 est proche d'être optimal, dans le sens que :

Théorème 1.4. *Soit C une constante positive. Il existe une constante $\kappa = \kappa(C) \geq 1$, telle que pour tout couple (Q_0, Q_1) de nombres entiers, avec $0 < Q_0 < |Q_1|$, vérifiant*

$$|\alpha - \frac{Q_1}{Q_0}|_p \leq C|Q_1|^{-2}, \tag{7}$$

on ait

$$Q_0 \gg \frac{|Q_1|}{\log^{\kappa} |Q_1|} \tag{8}$$

(la constante impliquée dans (8) *dépendant également de C).*

La méthode utilisée est celle de Peck [6], adaptée au cas p-adique d'une façon très semblable à ce que l'on trouve dans [7].

2. Nombres quadratiques p-adiques

Nous allons tout d'abord rappeler les formules de Peck, adaptées aux nombres quadratiques. Soit α un nombre quadratique appartenant à $\mathbb{Q}_p$. Le corps $\mathbb{Q}(\alpha)$ est donc considéré comme sous-corps de $\mathbb{Q}_p$. Soit (β_0, β_1) la base duale de la base $(1, \alpha)$ du corps $\mathbb{Q}(\alpha)$, c'est-à-dire que $\mathrm{Tr}(\beta_0) = \mathrm{Tr}(\alpha\beta_1) = 1$ et $\mathrm{Tr}(\beta_1) = \mathrm{Tr}(\alpha\beta_0) = 0$ (donc β_1 et $\alpha\beta_0$ sont des nombres irrationnels dont le carré appartient à $\mathbb{Q}$). Soit σ l'automorphisme différent de l'identité de $\mathbb{Q}(\alpha)$, et soient τ_1 et $\tau_2 = \tau_1 \circ \sigma$ les plongements de $\mathbb{Q}(\alpha)$ dans $\mathbb{C}$.

Lemme 2.1. *Soit $x \in \mathbb{Q}(\alpha)$:*

$$x = q_0\beta_0 + q_1\beta_1, \quad q_i \in \mathbb{Q}, \quad i = 0, 1.$$

On a

$$q_0 = \tau_1(x) + \tau_2(x), \tag{9}$$

$$q_1 = \tau_1(x\alpha) + \tau_2(x\alpha), \tag{10}$$

et

$$q_0\alpha - q_1 = \sigma(x)(\alpha - \sigma(\alpha)). \tag{11}$$

Démonstration. On a

$$q_0 = \mathrm{Tr}(x), \quad q_1 = \mathrm{Tr}(x\alpha),$$

donc

$$q_0 = x + \sigma(x), \quad q_1 = x\alpha + \sigma(x)\sigma(\alpha), \tag{9bis}$$

en sorte que

$$q_0\alpha - q_1 = \sigma(x)(\alpha - \sigma(\alpha)).$$

Mais on peut aussi calculer les traces dans $\mathbb{C}$, et ainsi :

$$q_0 = \tau_1(x) + \tau_2(x), \quad q_1 = \tau_1(x\alpha) + \tau_2(x\alpha). \qquad \square$$

Nous utiliserons la conséquence suivante :

Corollaire 2.2. *Soit $\eta \in \mathbb{Q}(\alpha)$ et soit*

$$\beta_1\eta = q_0\beta_0 + q_1\beta_1, \quad q_i \in \mathbb{Q}, \quad i = 0, 1.$$

On a

$$|q_0| \asymp |\tau_1(\eta) - \tau_2(\eta)|, \tag{9'}$$

$$|q_1| \asymp |\tau_1(\eta\alpha) - \tau_2(\eta\alpha)|, \tag{10'}$$

et

$$|q_0\alpha - q_1|_p \asymp |\sigma(\eta)|_p. \tag{11'}$$

Démonstration. Cela découle immédiatement du lemme 2.1 appliqué à $x = \beta_1\eta$, compte tenu du fait que $\sigma(\beta_1) = -\beta_1$ et $\tau_2(\beta_1) = -\tau_1(\beta_1)$. □

L'anneau $\mathcal{O}$ des entiers algébriques de $\mathbb{Q}(\alpha)$ est aussi l'ensemble des éléments $\xi \in \mathbb{Q}(\alpha)$ tels que $v(\xi) \leq 1$ pour toutes les valeurs absolues non archimédiennes sur $\mathbb{Q}(\alpha)$. Nous considérerons l'anneau $\mathcal{O}_p$ des p-entiers de $\mathbb{Q}(\alpha)$, i.e. les éléments ξ tels que $v(\xi) \leq 1$ pour toutes les valeurs absolues non archimédiennes sur $\mathbb{Q}(\alpha)$, autres que celles prolongeant la valeur absolue p-adique sur $\mathbb{Q}$. L'anneau $\mathcal{O}_p$ est aussi l'ensemble des éléments entiers sur $\mathbb{Z}[1/p]$.

Le groupe U_p des p-unités, i.e. des éléments inversibles de l'anneau $\mathcal{O}_p$, est l'ensemble des éléments ξ tels que $v(\xi) = 1$ pour toutes les valeurs absolues non archimédiennes sur $\mathbb{Q}(\alpha)$, sauf éventuellement pour celles prolongeant la valeur absolue p-adique sur $\mathbb{Q}$. On sait que si l'on désigne par ρ_0 le nombre de valeurs absolues archimédiennes sur $\mathbb{Q}(\alpha)$ et ρ_p, le nombre de valeurs absolues sur $\mathbb{Q}(\alpha)$ prolongeant la valeur absolue p-adique sur $\mathbb{Q}$, le groupe U_p est de rang $\rho_0 + \rho_p - 1$ (cf. [4, p. 66 et suivantes]). Les nombres ρ_0 et ρ_p sont aussi les nombres de facteurs irréductibles sur $\mathbb{R}$, respectivement sur $\mathbb{Q}_p$, du polyôme irréductible de α sur $\mathbb{Q}$. Ici $\rho_p = 2$ puisque α appartient à $\mathbb{Q}_p$, et les deux valeurs absolues prolongeant la valeur absolue p-adique sont la restriction à $\mathbb{Q}(\alpha)$ de la valeur absolue p-adique sur $\mathbb{Q}_p$, notée abusivement $|\cdot|_p$, et $|\cdot|_p \circ \sigma$, i.e., $x \longmapsto |\sigma(x)|_p$. On a $\rho_0 = 2$ ou $\rho_0 = 1$, selon que le corps $\mathbb{Q}(\alpha)$ possède ou non un plongement réel.

3. Démonstration du théorème 1.1

Nous séparons maintenant le cas d'un corps quadratique imaginaire et celui d'un corps quadratique réel.

3.1. Cas d'un corps quadratique imaginaire. Dans ce cas, $\rho_0 = 1$, et il y a deux plongements, τ et $\bar{\tau}$, de $\mathbb{Q}(\alpha)$ dans $\mathbb{C}$, qui induisent la même valeur absolue archimédienne sur $\mathbb{Q}(\alpha)$, $|\cdot| \circ \tau = |\cdot| \circ \bar{\tau}$. Le groupe U_p est de rang 2.

Lemme 3.1. *Il existe un entier $c > 0$ et une p-unité ϵ dans $\mathbb{Q}(\alpha)$ possédant les propriétés suivantes :*

$$|\epsilon|_p = p^c, \tag{12}$$

$$|\sigma(\epsilon)|_p = p^{-c}, \tag{13}$$

et

$$|\tau(\epsilon)| = 1. \tag{14}$$

Démonstration. Le nombre p appartient à U_p, qui est de rang 2, il existe donc une p-unité γ multiplicativement indépendante de p, de norme une unité de $\mathbb{Z}[1/p]$, i.e. $N_{\mathbb{Q}(\alpha):\mathbb{Q}}(\gamma) = p^k$, où $k \in \mathbb{Z}$. Remplaçant γ par $p^{-k}\gamma^2$, on peut supposer $N_{\mathbb{Q}(\alpha):\mathbb{Q}}(\gamma) = 1$. Mais alors $|\gamma|_p \neq 1$, sinon on aurait aussi $|\sigma(\gamma)|_p = 1$, et comme $|\cdot|_p$ et $|\cdot|_p \circ \sigma$ sont les deux valeurs absolues sur $\mathbb{Q}(\alpha)$ prolongeant la valeur absolue p-adique sur $\mathbb{Q}$, γ serait une unité sur $\mathbb{Z}$ de $\mathbb{Q}(\alpha)$, ce qui est impossible, le groupe des unités d'un corps quadratique imaginaire étant réduit à sa composante cyclique. Considérons alors $\epsilon = \gamma^{\pm 1}$ en choisissant l'exposant de façon que $|\epsilon|_p > 1$. On a ainsi (12), puis (13) résulte du fait que $N_{\mathbb{Q}(\alpha):\mathbb{Q}}(\epsilon) = 1$, et (14) du fait que l'on a aussi $N_{\mathbb{Q}(\alpha):\mathbb{Q}}(\epsilon) = \tau(\epsilon)\overline{\tau(\epsilon)} = |\tau(\epsilon)|^2 = 1$. □

Nous pouvons maintenant démontrer le théorème 1.1 dans le cas d'un corps quadratique imaginaire. Soit Δ un nombre rationnel non nul tel que $\Delta\mathcal{O}\beta_1 \subset \mathbb{Z}\beta_0 + \mathbb{Z}\beta_1$. Pour h entier positif, soient $q_0 = q_0(h)$ et $q_1 = q_1(h)$ des nombres rationnels tels que

$$\Delta\beta_1\epsilon^h = q_0\beta_0 + q_1\beta_1.$$

Comme $p^c\epsilon$ est entier sur $\mathbb{Z}$ puisque $|p^c\epsilon|_p = 1$ et $|p^c\sigma(\epsilon)|_p = p^{-2c} < 1$, q_0 et q_1 sont de la forme :

$$q_i = \frac{Q_i}{p^{hc}}, \quad Q_i \in \mathbb{Z}, \quad i = 0, 1.$$

D'autre part, d'après les inégalités ($9'$) et ($10'$) du corollaire 2.2, compte tenu de (14) on a :

$$|q_i| \ll 1, \quad i = 0, 1.$$

Comme il résulte de la définition que

$$\max\{|q_0|, |q_1|\} \gg 1,$$

on en déduit que

$$\max\{|q_0|, |q_1|\} \asymp 1,$$

donc que

$$\max\{|Q_0|, |Q_1|\} \asymp p^{hc}. \tag{15}$$

D'après (13) et (11′) on a

$$|q_0\alpha - q_1|_p \asymp p^{-hc},$$

donc

$$|Q_0\alpha - Q_1|_p \asymp p^{-2hc}. \tag{16}$$

Par ailleurs on peut remarquer que l'égalité déduite de (9bis) :

$$q_0 = \Delta\beta_1(\epsilon^h - \sigma(\epsilon^h)),$$

implique que $q_0 \neq 0$ et $|q_0|_p \asymp p^{hc}$. On a donc $|Q_0|_p \asymp 1$, ce qui permet de passer de (16) à :

$$\left|\alpha - \frac{Q_1}{Q_0}\right|_p \asymp p^{-2hc}. \tag{17}$$

Nous allons montrer que pour certains h, on peut préciser (15). D'après (9′), en posant $\arg(\tau(\epsilon)) = \varphi$, on a

$$|Q_0| \asymp p^{hc}|\Im(\tau(\epsilon^h))| \asymp p^{hc}|\sin h\varphi| \asymp p^{hc}\|h\varphi\|_\pi \tag{18}$$

(où $\|t\|_\pi = \min_{k\in\mathbb{Z}} |t+k\pi|$). Le théorème de Dirichlet montre que pour tout entier $A > 0$, il existe des entiers h et k tels que $0 < h \leq A$ et

$$\left|h\frac{\varphi}{\pi} + k\right| < \frac{1}{A}.$$

Pour un tel entier h, on a donc $\|h\varphi\|_\pi < \pi/h$, et d'après (18), $|Q_0| \ll p^{hc}/h$. Mais puisque $Q_0 \neq 0$, on a $h\varphi + k\pi \neq 0$. Or $e^{i\varphi} = \tau(\epsilon)$ et $e^{i\pi} = -1$ sont des nombres algébriques, et par conséquent les estimations de formes linéaires de logarithmes de nombres algébriques [1, 2], assurent que

$$|h\varphi + k\pi| \gg h^{-\theta}$$

pour une certaine constante $\theta \geq 1$ (ne dépendant que de φ, de même que la constante impliquée dans le symbole $\gg$). On en conclut que

$$A^{1/\theta} \ll h \leq A.$$

En considérant $H = p^{hc}$ on a donc construit des entiers Q_0, Q_1, satisfaisant (17), i.e.,

$$\left|\alpha - \frac{Q_1}{Q_0}\right|_p \asymp H^{-2},$$

avec, au vu de (15) :

$$|Q_0| \ll \frac{H}{\log H}, \quad |Q_1| \asymp H, \tag{19}$$

ce qui conduit à (5) et (6). Cela achève la démonstration du théorème 1.1 dans ce cas puisque de plus

$$A^{1/\theta} \ll \log H \ll A.$$

3.2. Cas d'un corps quadratique réel. Si maintenant le corps $\mathbb{Q}(\alpha)$ admet deux plongements τ_1 et τ_2 dans $\mathbb{R}$, le groupe U_p est de rang 3, et il existe des p-unités γ_1 et γ_2 telles que p, γ_1, et γ_2 soient multiplicativement indépendants. En remplaçant éventuellement γ_1 et γ_2 par leurs carrés, on peut supposer $\tau_i(\gamma_j) > 0,\ i = 1, 2,\ j = 1, 2$. Le lemme 3.1 est remplacé par le résultat suivant :

Lemme 3.2. *Il existe une suite* $(\epsilon_h)_{h\in\mathbb{N}}$ *de p-unités telles que*

$$|\epsilon_h|_p \asymp p^h, \tag{20}$$

$$|\sigma(\epsilon_h)|_p \asymp p^{-h}, \tag{21}$$

$$\tau_i(\epsilon_h) > 0 \quad (i = 1, 2), \quad \textit{et} \quad \tau_1(\epsilon_h) \asymp \tau_2(\epsilon_h) \asymp 1. \tag{22}$$

Démonstration. On cherche ϵ_h sous la forme

$$\epsilon_h = p^\ell \gamma_1^m \gamma_2^n,$$

où ℓ, m et n, sont entiers - cette forme assurant que $\tau_i(\epsilon_h) > 0$ $(i = 1, 2)$. Considérons le système :

$$-\lambda \log p + \mu \log |\gamma_1|_p + \nu \log |\gamma_2|_p = h \log p, \tag{20'}$$

$$-\lambda \log p + \mu \log |\sigma(\gamma_1)|_p + \nu \log |\sigma(\gamma_2)|_p = -h \log p, \tag{21'}$$

$$\lambda \log p + \mu \log \tau_1(\gamma_1) + \nu \log \tau_1(\gamma_2) = 0, \tag{22'}$$

$$\lambda \log p + \mu \log \tau_2(\gamma_1) + \nu \log \tau_2(\gamma_2) = 0, \tag{22''}$$

où les inconnues λ, μ, ν, sont des nombres réels. Ce système est de rang 3. En effet, on a ([4, p. 66 et suivantes]) :

$$\begin{vmatrix} -\log p & \log |\gamma_1|_p & \log |\gamma_2|_p \\ -\log p & \log |\sigma(\gamma_1)|_p & \log |\sigma(\gamma_2)|_p \\ \log p & \log \tau_1(\gamma_1) & \log \tau_1(\gamma_2) \end{vmatrix} \neq 0$$

puisque c'est le déterminant des logarithmes des valeurs absolues prolongeant la valeur absolue p-adique et d'une valeur absolue archimédienne du système de p-unités multiplicativement indépendantes (p, γ_1, γ_2). D'autre part, la somme des équations du système est nulle. En effet γ_1 et γ_2 étant des p-unités, on a

$$N_{\mathbb{Q}(\alpha):\mathbb{Q}}(\gamma_i) = \gamma_i \sigma(\gamma_i) = \tau_1(\gamma_i)\tau_2(\gamma_i) = p^{k_i} \quad (k_i \in \mathbb{Z})$$

en sorte que

$$|N_{\mathbb{Q}(\alpha):\mathbb{Q}}(\gamma_i)|_p N_{\mathbb{Q}(\alpha):\mathbb{Q}}(\gamma_i) = 1,$$

i.e.,

$$\log|\gamma_i|_p + \log|\sigma(\gamma_i)|_p + \log\tau_1(\gamma_i) + \log\tau_2(\gamma_i) = 0 \quad (i = 1, 2).$$

Le système (20′), (21′), (22′), (22″), admet donc une solution réelle (λ, μ, ν), et pour assurer les conditions (20), (21), et (22), il suffit de prendre

$$\epsilon_h = p^\ell \gamma_1^m \gamma_2^n,$$

où ℓ, m, et n sont des entiers tels que

$$\max\{|\ell - \lambda|, |m - \mu|, |n - \nu|\} \leq 1/2. \qquad \square$$

Nous allons montrer maintenant qu'on peut améliorer ce lemme pour certains entiers h :

Lemme 3.3. *Il existe un ensemble infini d'entiers positifs h pour lesquels on peut construire une p-unité ϵ_h satisfaisant aux conditions* (20), (21), (22), *et telle que de plus :*

$$0 < |\tau_1(\epsilon_h) - \tau_2(\epsilon_h)| \ll \frac{1}{h}. \tag{23}$$

De façon plus précise, pour tout entier $A \geq 1$, il existe un tel entier h avec

$$A^{1/\theta} \ll h \ll A,$$

où θ est une constante, $\theta \geq 1$.

Démonstration. Nous cherchons des quadruplets (h, ℓ, m, n) d'entiers de $\mathbb{Z}$ avec $h > 0$, satisfaisant aux conditions :

$$-\ell\log p + m\log|\gamma_1|_p + n\log|\gamma_2|_p = h\log p + O(1), \tag{24}$$

$$-\ell\log p + m\log|\sigma(\gamma_1)|_p + n\log|\sigma(\gamma_2)|_p = -h\log p + O(1), \tag{25}$$

$$\ell\log p + m\log\tau_1(\gamma_1) + n\log\tau_1(\gamma_2) = O(1), \tag{26}$$

et

$$\left|m\log\frac{\tau_2(\gamma_1)}{\tau_1(\gamma_1)} + n\log\frac{\tau_2(\gamma_2)}{\tau_1(\gamma_2)}\right| \ll \frac{1}{h}. \tag{27}$$

Comme $\tau_2(\gamma_i) \neq \tau_1(\gamma_i)$ pour $i = 1,\ 2$, le théorème de Dirichlet assure que pour tout entier positif A, on peut trouver un couple d'entiers (m, n) avec $0 < m \leq A$ satisfaisant à :

$$\left|m\frac{\log\tau_2(\gamma_1) - \log\tau_1(\gamma_1)}{\log\tau_2(\gamma_2) - \log\tau_1(\gamma_2)} + n\right| < \frac{1}{A}.$$

On obtient donc :

$$\left|m\log\frac{\tau_2(\gamma_1)}{\tau_1(\gamma_1)} + n\log\frac{\tau_2(\gamma_2)}{\tau_1(\gamma_2)}\right| \ll \frac{1}{A} \tag{28}$$

avec

$$0 < |m| \leq A, \quad |n| \ll A. \tag{29}$$

On assure la condition (26) en choisissant l'entier ℓ tel que

$$|\ell \log p + m \log \tau_1(\gamma_1) + n \log \tau_1(\gamma_2)| \leq \frac{\log p}{2}, \tag{26'}$$

ce qui implique, compte tenu de (28), que

$$|\ell \log p + m \log \tau_2(\gamma_1) + n \log \tau_2(\gamma_2)| \ll 1. \tag{30}$$

Remplaçant éventuellement ℓ, m et n par leurs opposés, on peut supposer que

$$-\ell \log p + m \log |\gamma_1|_p + n \log |\gamma_2|_p \geq 0.$$

Il existe alors un entier $h > 0$ tel que

$$\begin{aligned} -\ell \log p + m \log |\gamma_1|_p + n \log |\gamma_2|_p &< h \log p \\ &\leq (1-\ell) \log p + m \log |\gamma_1|_p + n \log |\gamma_2|_p, \end{aligned}$$

ce qui est (24). On obtient alors (25) par l'addition de (24), (26) et (30).

Pour un tel entier h, posons

$$\epsilon_h = p^h \gamma_1^m \gamma_2^n.$$

Écrivant (28) sous la forme

$$\left|\log \frac{\tau_2(\epsilon_h)}{\tau_1(\epsilon_h)}\right| \ll \frac{1}{A},$$

comme on a, grâce à (26) et (30), $\tau_i(\epsilon_h) \asymp 1$ $(i = 1, 2)$, on en conclut que

$$|\tau_1(\epsilon_h) - \tau_2(\epsilon_h)| \ll \frac{1}{A}. \tag{23'}$$

Mais l'inversibilité de la matrice des membres de gauche de (24), (25) et (26), assure que

$$h \asymp \max\{|\ell|, |m|, |n|\},$$

et comme d'après (26), $|\ell| \ll \max\{|m|, |n|\}$, on obtient

$$h \asymp \max\{|m|, |n|\},$$

donc

$$0 < h \ll A,$$

et on déduit alors de (23′) que

$$|\tau_1(\epsilon_h) - \tau_2(\epsilon_h)| \ll \frac{1}{h}.$$

Pour obtenir (23), il ne reste qu'à montrer que $\tau_1(\epsilon_h) \neq \tau_2(\epsilon_h)$. Il suffit de remarquer que m et n n'étant pas tous deux nuls, on ne peut avoir $\tau_1(\gamma_1^m \gamma_2^n) \neq \tau_2(\gamma_1^m \gamma_2^n)$, sinon $\gamma_1^m \gamma_2^n$ appartiendrait à $\mathbb{Q}$, et comme c'est une p-unité, on aurait $\gamma_1^m \gamma_2^n = p^t$ avec $t \in \mathbb{Z}$, contrairement à l'hypothèse que p, γ_1 et γ_2 soient multiplicativement indépendants.

Comme nous venons de montrer que

$$m \log \frac{\tau_2(\gamma_1)}{\tau_1(\gamma_1)} + n \log \frac{\tau_2(\gamma_2)}{\tau_1(\gamma_2)} \neq 0,$$

les minorations de formes linéaires de logarithmes de nombres algébriques [1, 2], assurent que

$$\left| m \log \frac{\tau_2(\gamma_1)}{\tau_1(\gamma_1)} + n \log \frac{\tau_2(\gamma_2)}{\tau_1(\gamma_2)} \right| \gg \max\{|m|, |n|\}^{-\theta},$$

où θ est une constante, $\theta \geq 1$. On a donc

$$\max\{|m|, |n|\} \gg A^{1/\theta}. \tag{29'}$$

Par suite

$$A^{1/\theta} \ll h \ll A, \tag{29''}$$

ce qui établit le lemme 3.3. □

La démonstration se termine maintenant comme dans le cas d'un corps quadratique imaginaire. Pour un tel entier h, on écrit

$$\Delta\beta_1\epsilon_h = q_0\beta_0 + q_1\beta_1, \quad q_i \in \mathbb{Q}, \quad i = 0, 1,$$

et on obtient comme précédemment

$$\max\{|q_0|, |q_1|\} \asymp 1, \quad i = 0, 1,$$

et

$$|q_0\alpha - q_1|_p \asymp |\sigma(\epsilon_h)|_p \asymp p^{-h}.$$

On remarque de plus que $q_0 \neq 0$, sinon ϵ_h serait un nombre rationnel, ce qui n'est pas puisque $\tau_1(\epsilon_h) \neq \tau_2(\epsilon_h)$. D'après (20) et (21) il existe un entier $d \geq 0$ tel que $|p^{h+d}\epsilon_h|_p \leq 1$ et $|p^{h+d}\sigma(\epsilon_h)|_p \leq 1$, donc $p^{h+d}\epsilon_h$ est entier sur $\mathbb{Z}$ et par suite q_0 et q_1 sont de la forme

$$q_i = \frac{Q_i}{p^{h+d}}, \quad Q_i \in \mathbb{Z}, \quad i = 0, 1,$$

avec

$$\max\{|Q_0|, |Q_1|\} \asymp p^h \tag{15'}$$

et

$$|Q_0\alpha - Q_1|_p \asymp p^{-2h}. \tag{16'}$$

De plus, comme dans le cas imaginaire, on voit grâce à (9bis), (20) et (21), que $|q_0|_p \asymp p^h$, donc

$$|Q_0|_p \asymp 1,$$

ce qui permet de passer de (16′) à

$$\left| \alpha - \frac{Q_1}{Q_0} \right|_p \asymp p^{-2h}. \tag{17'}$$

D'après (9′) et (23) et (15′) on a :

$$|Q_0| \ll \frac{p^h}{h}, \quad |Q_1| \asymp p^h.$$

En considérant $H = p^h$, on a donc construit pour tout entier $A \geq 1$, un entier $H \geq 2$ tel que

$$A^{1/\theta} \ll \log H \ll A,$$

et des entiers $Q_0 \neq 0$ et Q_1, tels que

$$\left| \alpha - \frac{Q_1}{Q_0} \right|_p \asymp H^{-2}$$

avec

$$|Q_0| \ll \frac{H}{\log H}, \quad |Q_1| \asymp H,$$

ce qui termine la démonstration du théorème 1.1.

4. Démonstration du théorème 1.4

Soit (Q_0, Q_1) un couple d'entiers vérifiant :

(31) $$0 < Q_0 < |Q_1|, \quad |Q_0\alpha - Q_1|_p \leq C|Q_1|^{-2}.$$

On définit c comme au lemme 3.1 dans le cas d'un corps quadratique imaginaire, et on pose $c = 1$ dans le cas d'un corps quadratique réel. Soit alors h l'entier positif déterminé par

$$p^{(h-1)c} \leq |Q_1| < p^{hc},$$

en sorte que

(32) $$|Q_1| \asymp p^{hc}.$$

Dans le cas réel, ϵ_h est comme au lemme 3.2, et dans le cas imaginaire, on pose $\epsilon_h = \epsilon^h$ où ϵ est déterminée comme au lemme 3.1. Posons encore dans les deux cas, $\epsilon_{-h} = \epsilon_h^{-1}$, en sorte que

(33) $$|\epsilon_{-h}|_p \asymp p^{-hc},$$

(34) $$|\sigma(\epsilon_{-h})|_p \asymp p^{hc}.$$

De plus, dans le cas imaginaire

(35) $$|\tau(\epsilon)| = 1,$$

et dans le cas réel, $\tau_i(\epsilon_h) > 0$, et

(35′) $$\tau_i(\epsilon_h) \asymp 1, \quad i = 1, 2.$$

Soit maintenant

$$u = p^{-hc}\epsilon_{-h}(Q_0\beta_0 + Q_1\beta_1).$$

Montrons que l'ensemble des valeurs possibles du nombre p-adique u est fini. Soit $B > 0$ un nombre rationnel tel que $B\beta_0$ et $B\beta_1$ soient entiers sur $\mathbb{Z}$.

Alors Bu est un p-entier. Mais d'après (33), $|u|_p \ll 1$, et d'après (31), (34) et l'égalité (11) du lemme 2.1, on a $|p^{hc}\sigma(u)\sigma(\epsilon_h)|_p \asymp |Q_0\alpha - Q_1|_p \ll p^{-2hc}$, d'où $|\sigma(u)|_p \ll 1$. Il existe donc une constante entière $w \geq 0$ telle que $|Bp^w u|_p \leq 1$ et $|Bp^w\sigma(u)|_p \leq 1$, et ainsi l'élément $v = Bp^w u$ de $\mathbb{Q}(\alpha)$ est entier sur $\mathbb{Z}$. Par ailleurs, en posant dans le cas imaginaire $\tau_1 = \tau$ et $\tau_2 = \bar{\tau}$, d'après (32), (35) et (35′), on a dans les deux cas, $|\tau_i(v)| \ll 1$ $(i = 1, 2)$. L'ensemble formé par les entiers algébriques v est donc fini, et on en conclut qu'il n'y a qu'un nombre fini de valeurs possibles pour u. Par suite, nous pouvons nous restreindre aux couples (Q_0, Q_1) vérifiant (31) tels que

$$Q_0\beta_0 + Q_1\beta_1 = p^{hc}\epsilon_h u$$

avec $u \neq 0$ fixé. Ici, nous séparons le cas imaginaire et le cas réel :

4.1. Cas d'un corps quadratique imaginaire. Posant $\psi = \arg\tau(u)$, on a d'après (9)

$$\begin{aligned} Q_0 = 2p^{hc}\Re(\tau(\epsilon^h u)) &= 2p^{hc}|\tau(u)|\cos(h\varphi + \psi) \\ &= 2(-1)^{k+1}p^{hc}|\tau(u)|\sin\left(h\varphi + \psi + \left(k - \frac{1}{2}\right)\pi\right), \end{aligned}$$

avec $k \in \mathbb{Z}$ tel que $0 \leq h\varphi + \psi + k\pi < \pi$. Donc pour u fixé,

$$Q_0 \asymp p^{hc}\left|h\varphi + \psi + \left(k - \frac{1}{2}\right)\pi\right|.$$

Or $e^{i\varphi} = \tau(\epsilon)$ et $e^{i\psi} = \tau(u)/|\tau(u)|$, c'est-à-dire que $e^{i\varphi}$, et $e^{i\psi}$ sont des nombres algébriques, de même que $e^{i\pi/2}$. De plus $h\varphi + \psi + (2k-1)\pi/2 \neq 0$ puisque $Q_0 \neq 0$. Les estimations de formes linéaires de logarithmes de nombres algébriques [1, 2], assurent que, comme $|k| \ll |h|$ on a

$$\left|h\varphi + \psi + (2k-1)\frac{\pi}{2}\right| \gg h^{-\kappa}$$

pour une constante $\kappa \geq 1$, donc

$$Q_0 \gg \frac{p^{hc}}{h^\kappa},$$

ce qui est le résultat annoncé.

4.2. Cas d'un corps quadratique réel. Pour u fixé, on a d'après (9) :

$$Q_0 = p^h(\tau_1(u)\tau_1(\epsilon_h) + \tau_2(u)\tau_2(\epsilon_h)),$$

et l'on peut aussi écrire

$$Q_0 \asymp p^h\left|\frac{\tau_1(\epsilon_h)}{\tau_2(\epsilon_h)} + \frac{\tau_2(u)}{\tau_1(u)}\right|.$$

Si $\tau_2(u)\tau_1(u) > 0$, on a $Q_0 \asymp p^h$. Sinon

$$\left|\frac{\tau_1(\epsilon_h)}{\tau_2(\epsilon_h)} + \frac{\tau_2(u)}{\tau_1(u)}\right| \asymp \left|\log \frac{\tau_1(\epsilon_h)}{\tau_2(\epsilon_h)} - \log \frac{-\tau_2(u)}{\tau_1(u)}\right|.$$

Revenant à la construction de ϵ_h,

$$\log \frac{\tau_1(\epsilon_h)}{\tau_2(\epsilon_h)} - \log \frac{-\tau_2(u)}{\tau_1(u)} = m \log \frac{\tau_1(\gamma_1)}{\tau_2(\gamma_1)} + n \log \frac{\tau_1(\gamma_2)}{\tau_2(\gamma_2)} - \log \frac{-\tau_2(u)}{\tau_1(u)},$$

et cette quantité n'étant pas nulle, une estimation classique de forme linéaire de logarithmes de nombres algébriques (cf. [1, 2]) assure que

$$\left|\log \frac{\tau_1(\epsilon_h)}{\tau_2(\epsilon_h)} - \log \frac{-\tau_2(u)}{\tau_1(u)}\right| \gg \max\{|m|, |n|\}^{-\kappa}$$

pour une constante $\kappa \geq 1$. Nous avons déjà remarqué que la matrice des membres de gauche des conditions (24), (25) et (26) est inversible, et il en résulte que

$$\max\{|m|, |n|\} \ll h.$$

On a donc

$$Q_0 \gg \frac{p^h}{h^\kappa},$$

ce qui est le résultat annoncé.

Remerciements

Je tiens à exprimer ici ma vive reconnaissance à Yann Bugeaud, pour son écoute et ses encouragements. Je remercie le rapporteur pour sa lecture attentive et pour ses suggestions qui ont contribué à améliorer la présentation des résultats.

Bibliographie

[1] A. Baker, « A sharpening of the bounds for linear forms in logarithms », *Acta Arith.* **21** (1972), p. 117-129.

[2] Y. Bugeaud, *Linear forms in logarithms and applications*, IRMA Lectures in Mathematics and Theoretical Physics, vol. 28, European Mathematical Society, 2018.

[3] M. Einsiedler & D. Kleinbock, « Measure rigidity and p-adic Littlewood-type problems », *Compos. Math.* **143** (2007), n° 3, p. 689-702.

[4] S. Lang, *Algebraic numbers*, Addison-Wesley Series in Mathematics, Addison-Wesley, 1964.

[5] B. de Mathan & O. Teulié, « Problèmes diophantiens simultanés », *Monatsh. Math.* **143** (2004), n° 3, p. 229-245.

[6] L. G. Peck, « Simultaneous rational approximations to algebraic numbers », *Bull. Am. Math. Soc.* **67** (1961), p. 197-201.

[7] O. Teulié, « Approximations simultanées de nombres algébriques de $\mathbb{Q}_p$ par des rationnels », *Monatsh. Math.* **137** (2002), n° 4, p. 313-324.

Bernard de Mathan
28, rue Léon Say
F-33400 Talence, France
E-mail: bernard.demathan@gmail.com