ACTA ARITHMETICA
102.2 (2002)

Approximation d'un nombre p-adique par des nombres algébriques

par

Olivier Teulié (Talence)

1. Introduction. Dans cet article, on s'intéresse à la version p-adique de certains résultats démontrés dans le cas réel par H. Davenport et W. M. Schmidt [3]. Jusqu'ici les seuls résultats p-adiques connus sont dus à J. F. Morrison [4] et concernent l'approximation d'un nombre p-adique par des nombres algébriques de degré borné ; ces résultats ont été obtenus en reprenant la méthode d'E. Wirsing [8] mais ils sont légèrement moins bons que dans le cas réel. Notre but est ici de démontrer l'analogue p-adique du résultat de H. Davenport et W. M. Schmidt [3] concernant l'approximation d'un nombre réel par des entiers algébriques de degré borné et d'appliquer leur méthode afin de démontrer des résultats d'approximation à degré exact comme nous l'avions fait dans le cas réel avec Y. Bugeaud [1]. En outre nous allons voir que cette méthode permet d'approcher des nombres p-adiques par des nombres algébriques appartenant à $\mathbb{Q}_p$ (ce que ne permet pas la méthode de J. F. Morrison).

Pour énoncer les résultats, on définit les suites $(\nu_n)_{n\geq 2}$ et $(d_n)_{n\geq 2}$ comme suit :

$$\begin{aligned} &\nu_2 = 2, && d_2 = 1,\\ &\nu_3 = (3+\sqrt{5})/2, && d_3 = 2,\\ &\nu_4 = 3, && d_4 = 2,\\ &\nu_n = [(n+1)/2], && d_n = [(n-1)/2] \quad \text{pour } n \geq 5. \end{aligned}$$

Enfin, pour un polynôme P à coefficients entiers s'écrivant

$$P(X) = a_n X^n + \ldots + a_1 X + a_0,$$

on note $\mathrm{H}(P)$ sa *hauteur naïve* définie par

$$\mathrm{H}(P) = \max_{0\leq i\leq n} |a_i|,$$

$|\cdot|$ étant la valeur absolue usuelle de $\mathbb{C}$. De plus, par définition, la hauteur

2000 *Mathematics Subject Classification*: Primary 11J04.

d'un nombre algébrique α, notée $\mathrm{H}(\alpha)$, est la hauteur de son polynôme minimal sur $\mathbb{Z}$.

Le résultat principal est le suivant :

THÉORÈME 1. *Soient $n \geq 2$ un entier et ξ un élément de $\mathbb{Q}_p$ qui n'est pas un nombre algébrique de degré au plus d_n. Alors il existe une infinité de nombres algébriques α dans $\mathbb{Q}_p$ de degré exactement $n-1$ tels que*

$$|\xi - \alpha|_p \ll \mathrm{H}(\alpha)^{-\nu_n}.$$

Si de plus $\xi \in \mathbb{Z}_p$, alors il existe une infinité d'entiers algébriques α de degré exactement n tels que

$$|\xi - \alpha|_p \ll \mathrm{H}(\alpha)^{-\nu_n}.$$

La notation $|\cdot|_p$ désigne la valeur absolue p-adique normalisée par $|p|_p = p^{-1}$. La constante numérique sous-entendue par le symbole $\ll$ ne dépend que de ξ, p et n.

REMARQUES. Pour l'approximation par des nombres algébriques, l'exposant est légèrement moins bon que celui trouvé par J. F. Morrison [4] (dans le cas général, pour l'approximation par des nombres algébriques de degré au plus n, l'exposant de J. F. Morrison est $(n+3)/2$ alors qu'ici il n'est que $[n/2+1]$) mais on peut assurer, outre le fait que le nombre algébrique α approchant ξ est de degré exactement n, que α est dans $\mathbb{Q}_p$, ce que la méthode de J. F. Morrison n'assure que pour les petites valeurs de n.

Pour démontrer le théorème 1, on peut se limiter, sans perte de généralité, au cas où $\xi \in \mathbb{Z}_p$. La démonstration se fait, comme dans le cas réel (*cf.* [1] et [3]), en deux étapes décrites par les deux théorèmes suivants :

THÉORÈME 2. *Soient $n \geq 2$ un entier et ξ un entier p-adique qui n'est pas un nombre algébrique de degré au plus d_n, et soit*

$$\lambda_n = 1 - 1/\nu_n.$$

Alors il existe une constante $c > 0$ et une infinité d'entiers positifs h tels que les inégalités

$$\max(|x_0|, \ldots, |x_{n-1}|) \leq c p^{n\lambda_n h},$$
$$|x_m - x_0 \xi^m|_p \leq p^{-hn} \quad \text{pour } m = 1, \ldots, n-1$$

n'aient pas de solutions entières $(x_0, \ldots, x_{n-1})$ autres que $(0, \ldots, 0)$.

THÉORÈME 3. *Soient $n \geq 2$ un entier et ξ un entier p-adique. S'il existe un réel $\lambda > 0$, une constante $c > 0$ et une infinité d'entiers naturels h tels que le système d'inéquations*

$$\max(|x_0|, \ldots, |x_{n-1}|) \leq c p^{n\lambda h},$$
$$|x_m - x_0 \xi^m|_p \leq p^{-nh} \quad \text{pour } m = 1, \ldots, n-1$$

n'ait pas de solution $(x_0, \dots, x_{n-1})$ *entière autre que* $(0, \dots, 0)$, *alors il existe une infinité de nombres algébriques* (*resp. d'entiers algébriques*) α *dans* $\mathbb{Q}_p$ *de degré exactement* $n-1$ (*resp.* n) *tels que*

$$|\xi - \alpha|_p \ll \mathrm{H}(\alpha)^{-1/(1-\lambda)}.$$

Nous allons d'abord démontrer le théorème 3 puis, après avoir introduit quelques notations dans la partie 3, nous démontrerons le théorème 2 dans les parties 4 et 5 ; les valeurs de λ données par le théorème 2 amènent alors au théorème 1 en utilisant le théorème 3.

2. Démonstration du théorème 3. Pour démontrer le théorème 3, nous aurons besoin du lemme suivant :

LEMME 1. *Soient* ξ *un entier p-adique et* P *un polynôme à coefficients dans* $\mathbb{Z}_p$ *tel que*

$$|P(\xi)|_p < 1, \tag{2.1}$$

$$|P'(\xi)|_p = 1. \tag{2.2}$$

Alors il existe une racine α *de* P, *dans* $\mathbb{Z}_p$, *telle que*

$$|\xi - \alpha|_p = |P(\xi)|_p.$$

Démonstration du lemme 1. Soit k le corps résiduel, $k = \mathbb{Z}_p/p\mathbb{Z}_p$, on note ϱ la surjection canonique de $\mathbb{Z}_p$ dans k ainsi que celle induite de $\mathbb{Z}_p[X]$ dans $k[X]$. D'après (2.1) on a $\varrho(P)(\varrho(\xi)) = 0$ et d'après (2.2), $\varrho(P)'(\varrho(\xi)) \neq 0$, donc $\varrho(\xi)$ est une racine simple de $\varrho(P)$. D'après le lemme de Hensel [5, p. 129], P possède une racine α dans $\mathbb{Z}_p$ telle que $\varrho(\alpha) = \varrho(\xi)$; ainsi on peut écrire

$$P(X) = (X - \alpha)Q(X),$$

avec $Q \in \mathbb{Z}_p[X]$. De plus, comme $\varrho(Q)(\varrho(\xi)) = \varrho(P)'(\varrho(\xi)) \neq 0$, on a $|Q(\xi)|_p = 1$ et donc

$$|\xi - \alpha|_p = |P(\xi)|_p. \ \blacksquare$$

Démonstration du théorème 3. Sous les hypothèses du théorème 3, il existe une infinité de h tels que le système

$$\max(|y_0|, \dots, |y_{n-1}|) \leq c p^{n(\lambda-1)h}, \tag{2.3}$$

$$|y_m - y_0 \xi^m|_p \leq 1 \quad \text{pour } m = 1, \dots, n-1 \tag{2.4}$$

n'ait pas de solution dans $(p^{-hn}\mathbb{Z})^n$, autre que $(0, \dots, 0)$. L'ensemble $\Lambda(h)$ des n-uplets $(y_0, \dots, y_{n-1})$ de $(p^{-hn}\mathbb{Z})^n$ vérifiant (2.4) est un sous-réseau de $(p^{-hn}\mathbb{Z})^n$: en effet, il existe des entiers b_m tels que $|\xi^m - b_m|_p \leq p^{-hn}$ pour $1 \leq m \leq n-1$ et on voit que $\Lambda(h)$ est le réseau engendré, dans $(p^{-nh}\mathbb{Z})^n$, par les vecteurs

$$(p^{-hn}, p^{-hn}b_1, \dots, p^{-hn}b_{n-1}),$$
$$(0, 1, 0, \dots, 0),$$
$$\vdots$$
$$(0, \dots, 0, 1).$$

On définit le réseau dual $\Lambda^*(h)$ de $\Lambda(h)$ par

$$\Lambda^*(h) = \{y \in \mathbb{R}^n \mid \forall x \in \Lambda(h),\ \langle x, y\rangle \in \mathbb{Z}\},$$

où $\langle\ ,\ \rangle$ désigne le produit scalaire usuel de $\mathbb{R}^n$. Le réseau $\Lambda^*(h)$ admet alors pour base les vecteurs

$$(p^{hn}, 0, \dots, 0),$$
$$(-b_1, 1, 0, \dots, 0),$$
$$\vdots$$
$$(-b_{n-1}, 0, \dots, 0, 1).$$

Ainsi, $\Lambda^*(h)$ est le sous-réseau de $\mathbb{Z}^n$ formé par les n-uplets $(x_0, \dots, x_{n-1})$ d'entiers tels que

$$|x_{n-1}\xi^{n-1} + \dots + x_1\xi + x_0|_p \le p^{-hn}.$$

On considère alors le convexe K de $\mathbb{R}^n$ défini par $\max(|x_0|, \dots, |x_{n-1}|) \le 1$. Le convexe polaire K^* de K, défini par $K^* = \{y \in \mathbb{R}^n \mid \forall x \in K,\ \langle x, y\rangle \le 1\}$, est alors K lui-même. Enfin, pour un entier m, un convexe C contenant un voisinage de 0 et un réseau L, on note $\tau_m(C, L)$ le m-ième des minima successifs du convexe C relativement au réseau L, c'est-à-dire le plus petit réel tel que le convexe $\tau_m(C, L)C$ contienne au moins m points de L linéairement indépendants. On va alors utiliser l'inégalité suivante [2, théorème VI, p. 219] :

$$\tau_1(C, L)\tau_n(C^*, L^*) \ll 1, \tag{2.5}$$

si C^* est le convexe polaire de C et L^* le réseau dual de L. L'hypothèse du théorème 3 signifie donc que le premier des minima successifs $\tau_1(K, \Lambda(h))$ du convexe K relativement au réseau $\Lambda(h)$ vérifie, pour une infinité d'entiers h,

$$\tau_1(K, \Lambda(h)) \ge cp^{n(\lambda-1)h}.$$

Donc, d'après (2.5), le n-ième des minima successifs du convexe K, relativement au réseau dual $\Lambda^*(h)$, vérifie pour une infinité d'entiers h,

$$\tau_n(K, \Lambda^*(h)) \ll p^{n(1-\lambda)h}.$$

Cela signifie qu'il existe n polynômes $(P_i)_{1\le i\le n}$:

$$P_i(X) = x_{n-1}^{(i)}X^{n-1} + \dots + x_1^{(i)}X + x_0^{(i)}$$

à coefficients entiers, de degré au plus $n-1$ et $\mathbb{Z}$-linéairement indépendants, tels que

$$|P_i(\xi)|_p \leq p^{-hn}, \tag{2.6}$$

$$\mathrm{H}(P_i) \ll p^{n(1-\lambda)h}. \tag{2.7}$$

On peut supposer que les points $\mathbf{x}^{(i)} = (x_m^{(i)})_{0\leq m\leq n-1}$ ont été choisis de sorte que $\mathbf{x}^{(i)} \in \tau_i(K, \Lambda^*(h))K$. On note alors δ le déterminant de la matrice $(\mathbf{x}^{(i)})_{1\leq i\leq n}$ qui est non nul puisque les vecteurs sont linéairement indépendants. Enfin, on note I l'index de ces vecteurs par rapport au réseau $\Lambda^*(h)$, c'est-à-dire le déterminant de la matrice précédente calculé dans une base du réseau $\Lambda^*(h)$. On a alors [2, corollaire du théorème V, p. 219]

$$I \leq n!.$$

Comme $\delta = d(\Lambda^*(h))I$, où $d(\Lambda^*(h))$ est le discriminant du réseau $\Lambda^*(h)$, on a $\delta = p^{hn}I$. Ainsi il existe un nombre premier q, ne dépendant que de ξ, p et n ne divisant pas $p\delta$.

Soit $d \geq n-1$ un nombre entier ; on considère alors le système de n équations à n inconnues $(\theta_i)_{1\leq i\leq n}$ suivant :

$$\begin{aligned}
\xi^d + q\theta_1 P_1(\xi) + \ldots + q\theta_n P_n(\xi) &= p^{hn},\\
d\xi^{d-1} + q\theta_1 P_1'(\xi) + \ldots + q\theta_n P_n'(\xi) &= 1,\\
\theta_1 x_m^{(1)} + \ldots + \theta_n x_m^{(n)} &= 0 \quad \text{pour } m = 2, \ldots, n-1.
\end{aligned}$$

Ce système est de Cramer parce que les P_i sont linéairement indépendants, il admet donc un unique n-uplet solution $(\theta_1, \ldots, \theta_n)$ dans $(\mathbb{Q}_p)^n$. On approche ce n-uplet de la manière suivante : il existe des rationnels r_i tel que

$$|\theta_i - r_i|_p \leq 1/p, \tag{2.8}$$

$$r_i \in \mathbb{Z}[1/p] \cap [-p, p] \tag{2.9}$$

et ceci pour chaque indice i. On considère alors le polynôme suivant :

$$\begin{aligned}
P(X) &= X^d + qr_1 P_1(X) + \ldots + qr_n P_n(X)\\
&= X^d + qx_{n-1}X^{n-1} + qx_{n-2}X^{n-2} + \ldots + qx_0.
\end{aligned}$$

A priori, $x_m \in \mathbb{Z}[1/p]$; on va voir qu'en fait $x_m \in \mathbb{Z}$. D'après la dernière série d'équations du système et (2.8), on a pour $m \geq 2$,

$$|x_m|_p \leq 1\,; \tag{2.10}$$

et donc $x_m \in \mathbb{Z}$ pour $m \geq 2$. D'après la deuxième équation du système, on a

$$P'(\xi) = 1 + q\sum_{i=1}^{n}(r_i - \theta_i)P_i'(\xi)\,;$$

or d'après (2.8),

$$\Big|\sum_{i=1}^{n}(r_i-\theta_i)P_i'(\xi)\Big|_p \le 1/p,$$

en effet $|P_i'(\xi)|_p \le 1$ puisque $\xi \in \mathbb{Z}_p$; par suite, comme $|q|_p = 1$,

$$|P'(\xi)|_p = 1. \tag{2.11}$$

En particulier, compte tenu de (2.10) et puisque $\xi \in \mathbb{Z}_p$ on a

$$|x_1|_p \le 1. \tag{2.12}$$

Enfin, d'après la première équation du système on a

$$P(\xi) = p^{hn} + q\sum_{i=1}^{n}(r_i-\theta_i)P_i(\xi)\,;$$

or, d'après (2.6) et (2.8),

$$\Big|\sum_{i=1}^{n}(r_i-\theta_i)P_i(\xi)\Big|_p \le p^{-(hn+1)},$$

donc

$$|P(\xi)|_p = p^{-hn}. \tag{2.13}$$

On déduit alors que $x_0 \in \mathbb{Z}$ de (2.10), (2.12), (2.13) et du fait que $\xi \in \mathbb{Z}_p$. Ainsi, on a $P \in \mathbb{Z}[X]$.

On va maintenant choisir les rationnels r_i de sorte que le polynôme P soit irréductible ; pour cela on va choisir les r_i afin que P vérifie le critère d'Eisenstein pour le nombre premier q. Pour que le polynôme P soit q-d'Eisenstein, il suffit que q ne divise pas x_0 puisque son coefficient dominant est congru à 1 modulo q. Comme q ne divise pas le déterminant de la matrice $(\mathbf{x}^{(i)})_{1\le i\le n}$, il existe un indice i tel que q ne divise pas $x_0^{(i)}$. Pour simplifier les notations, on supposera que cet indice est $i = 1$. On choisit $r_2, \ldots, r_n$ vérifiant (2.8) et (2.9) ; il reste alors deux choix pour r_1 que l'on peut noter $r_{1,1}$ et $r_{1,2} = r_{1,1} + p$. Comme $x_0 = r_1x_0^{(1)} + r_2x_0^{(2)} + \ldots + r_nx_0^{(n)}$, et comme q ne divise pas $px_0^{(1)}$, q divise au plus l'un des deux nombres $r_{1,1}x_0^{(1)} + r_2x_0^{(2)} + \ldots + r_nx_0^{(n)}$, $r_{1,2}x_0^{(1)} + r_2x_0^{(2)} + \ldots + r_nx_0^{(n)}$. Ainsi pour l'une des deux valeurs de r_1, P est q-d'Eisenstein, donc irréductible.

Enfin, comme $|r_i| \le p$ et d'après (2.7), on a

$$\mathrm{H}(P) \ll p^{n(1-\lambda)h}. \tag{2.14}$$

D'après le lemme 1, il existe une racine α de P dans $\mathbb{Z}_p$, donc un nombre algébrique de $\mathbb{Z}_p$ de degré exactement d, tel que

$$0 < |\xi - \alpha|_p = |P(\xi)|_p.$$

On conclut alors en utilisant (2.13) et (2.14) qu'il existe un nombre algébrique α de $\mathbb{Z}_p$, de degré exactement d, tel que

$$0 < |\xi - \alpha|_p \ll \mathrm{H}(\alpha)^{-1/(1-\lambda)}.$$

En choisissant $d = n-1$, on obtient le résultat annoncé pour l'approximation par des nombres algébriques de degré exactement $n-1$, alors qu'en choisissant $d = n$, on obtient l'approximation par des entiers algébriques de degré exactement n puisque pour $d \geq n$, le polynôme P est unitaire. ∎

Remarques. Si on choisit dans la démonstration précédente $d = n+1$, on obtient comme nous l'avions fait dans le cas réel [1] l'approximation par des entiers algébriques de trace nulle de degré exactement $n+1$.

On pourrait comme dans le cas réel [7] démontrer un résultat similaire pour l'approximation d'un entier p-adique par des unités algébriques de degré donné.

3. Notations et résultats préliminaires. Pour terminer la démonstration du théorème 1, il ne reste plus qu'à prouver le théorème 2. La démonstration proposée est une démonstration par l'absurde : on suppose que le système d'inéquations

$$\max(|x_0|, \ldots, |x_{n-1}|) \leq cp^{n\lambda h},$$
$$|x_m - x_0\xi^m|_p \leq p^{-nh} \quad \text{pour } m = 1, \ldots, n-1$$

possède une solution non triviale pour tout h entier positif suffisamment grand, et on va montrer que cela conduit à une contradiction si la constante c est assez petite. Ainsi, on suppose qu'il existe un entier $h_0 > 0$ tel que pour tout entier $h \geq h_0$, il existe une solution entière non triviale au système $S(h)$ suivant :

$$\max\{|x_0|, \ldots, |x_{n-1}|\} \leq cp^{n\lambda h},$$
$$(\max_{0\leq m\leq n-1} |x_m|)|x_m - x_0\xi^m|_p \leq cp^{-n(1-\lambda)h} \quad \text{pour } m = 1, \ldots, n-1.$$

On va alors définir une suite de points minimaux de la manière suivante. On pose, comme dans [4], pour $\mathcal{X}$ un point de $\mathbb{Z}^n$,

$$L(\mathcal{X}) = \max_{1\leq m\leq n-1} |x_m - x_0\xi^m|_p$$

et

$$E(\mathcal{X}) = \mathrm{H}(\mathcal{X})L(\mathcal{X}),$$

où $\mathrm{H}(\mathcal{X})$ est la hauteur du point $\mathcal{X} \in \mathbb{Z}^n$: $\mathrm{H}(\mathcal{X}) = \max_{0\leq m\leq n-1} |x_m|$. On peut d'abord remarquer que pour une solution non triviale de $S(h)$, on a $x_m \neq 0$ pour tout indice m, si $\lambda \leq 1$ et si c est assez petit. En effet, si $x_0 = 0$ alors on a pour tout indice $m = 1, \ldots, n-1$, $|x_m|_p \leq p^{-nh}$ et $|x_m| \leq cp^{n\lambda h} < p^{nh}$, si $c < 1$, ce qui implique que $x_m = 0$; par ailleurs, si on a $x_m = 0$ pour

un indice m non nul, on a $|x_0\xi^m|_p \leq p^{-nh}$ et $|x_0| \leq cp^{n\lambda h} \leq cp^{nh}$ donc $|x_0|_p \leq |\xi|_p^{-m}p^{-nh}$ et $|x_0| < |\xi|_p^m p^{nh}$, si $c < |\xi|_p^m$, ce qui implique que $x_0 = 0$ et donc que tous les x_m sont nuls. On en déduit que si ξ est irrationnel, $L(\mathcal{X}) \neq 0$, car comme $x_0 \neq 0$, on a $|x_1 - x_0\xi|_p \neq 0$.

On construit alors par récurrence une suite de points $(\mathcal{X}_i)_{i\geq 1}$ et une suite croissante d'entiers $(h_i)_{i\geq 0}$ de la manière suivante : on choisit un point $\mathcal{X}_1$ solution de $S(h_0)$ tel que $E(\mathcal{X}_1)$ soit minimal parmi les solutions de $S(h_0)$ et que $\mathrm{H}(\mathcal{X}_1)$ soit minimum parmi les solutions de $S(h_0)$ rendant minimal $E(\mathcal{X})$. On suppose alors que l'on a construit l'entier $h_{i-1} \geq h_0$ et le point $\mathcal{X}_i$ solution de $S(h_{i-1})$. Comme $\mathcal{X}_i$ est solution de $S(h_{i-1})$, on a

$$E(\mathcal{X}_i) \leq cp^{-n(1-\lambda)h_{i-1}}.$$

On définit alors $h_i \in \mathbb{Z}$ par

$$cp^{-n(1-\lambda)h_i} < E(\mathcal{X}_i) \leq cp^{-n(1-\lambda)(h_i-1)}, \tag{3.1}$$

cet entier existe puisque $\xi \notin \mathbb{Q}$ et donc $E(\mathcal{X}_i) \neq 0$. On a alors

$$h_i > h_{i-1},$$

et en particulier $h_i > h_0$. On choisit alors $\mathcal{X}_{i+1}$ parmi les solutions non triviales de $S(h_i)$ de sorte que $E(\mathcal{X}_{i+1})$ soit minimum parmi ces solutions, et que $\mathrm{H}(\mathcal{X}_{i+1})$ soit minimum parmi les solutions de $S(h_i)$ rendant minimal $E(\mathcal{X})$.

À partir de maintenant, on note $X_i = \mathrm{H}(\mathcal{X}_i)$ et $L_i = L(\mathcal{X}_i)$. Comme $\mathcal{X}_{i+1}$ est solution de $S(h_i)$, on a

$$E(\mathcal{X}_{i+1}) \leq cp^{-n(1-\lambda)h_i},$$

et donc, d'après (3.1), on a

$$E(\mathcal{X}_{i+1}) \leq cp^{-n(1-\lambda)h_i} < E(\mathcal{X}_i) \leq cp^{-n(1-\lambda)(h_i-1)},$$

donc

$$E(\mathcal{X}_{i+1}) < E(\mathcal{X}_i).$$

Enfin

$$X_{i+1} > X_i\,;$$

en effet, si $X_{i+1} \leq X_i$, $\mathcal{X}_{i+1}$ serait solution de $S(h_{i-1})$, ce qui est impossible car $E(\mathcal{X}_{i+1}) < E(\mathcal{X}_i)$. On en déduit alors

$$L_{i+1} < L_i.$$

De plus, les coordonnées de $\mathcal{X}_i$ sont premières entre elles : en effet, dans le cas contraire, on pourrait écrire $\mathcal{X}_i = a\mathcal{Y}$ avec $a > 0$ entier et on aurait $a\mathrm{H}(\mathcal{Y}) = X_i$ et $E(\mathcal{X}_i) = a|a|_p E(\mathcal{Y}) \geq E(\mathcal{Y})$. Pour des raisons similaires, $\mathcal{X}_i$ et $\mathcal{X}_{i+1}$ sont linéairement indépendants : sinon il existerait des entiers $a > 0$ et b premiers entre eux, tels que $a\mathcal{X}_i = b\mathcal{X}_{i+1}$, et comme les coordonnées de

$\mathcal{X}_i$ sont premières entre elles, a diviserait b donc $a = 1$, ce qui est impossible puisque $X_i < X_{i+1}$.

D'après (3.1), on a $E(\mathcal{X}_i) \le cp^{-n(1-\lambda)(h_i-1)}$, et comme $\mathcal{X}_{i+1}$ est solution de $S(h_i)$, on a $X_{i+1} \le cp^{n\lambda h_i}$, donc $p^{-h_i} \le (cX_{i+1}^{-1})^{1/(n\lambda)}$. On en déduit que $E(\mathcal{X}_i) \le cp^{n(1-\lambda)}(cX_{i+1}^{-1})^{n(1-\lambda)/(n\lambda)} \ll c^{1/\lambda}X_{i+1}^{1-1/\lambda}$ et donc que

$$L_i \ll c^{1/\lambda}X_i^{-1}X_{i+1}^{1-1/\lambda}. \tag{3.2}$$

Enfin, on note les coordonnées de $\mathcal{X}_i$ de la manière suivante :

$$\mathcal{X}_i = (x_{i,m})_{0\le m\le n-1}\,,$$

et ceci pour tout $i \ge 1$.

4. Les petites valeurs de n

4.1. *Le cas $n = 2$.* On reprend les notations précédentes avec $n = 2$ et $\lambda = 1/2$; ainsi (3.2) devient

$$L_i \ll c^2X_i^{-1}X_{i+1}^{-1}. \tag{4.1}$$

Comme $\mathcal{X}_i$ et $\mathcal{X}_{i+1}$ sont linéairement indépendants, on a

$$1 \le \left|\begin{matrix} x_{i+1,0} & x_{i+1,1} \\ x_{i,0} & x_{i,1}\end{matrix}\right| \left|\begin{matrix} x_{i+1,0} & x_{i+1,1} \\ x_{i,0} & x_{i,1}\end{matrix}\right|_p.$$

Or

$$\left|\begin{matrix} x_{i+1,0} & x_{i+1,1} \\ x_{i,0} & x_{i,1}\end{matrix}\right|_p = \left|\begin{matrix} x_{i+1,0} & x_{i+1,1}-x_{i+1,0}\xi \\ x_{i,0} & x_{i,1}-x_{i,0}\xi\end{matrix}\right|_p \le \max(L_i, L_{i+1}) \le L_i,$$

et donc, comme

$$\left|\begin{matrix} x_{i+1,0} & x_{i+1,1} \\ x_{i,0} & x_{i,1}\end{matrix}\right| \le 2X_iX_{i+1},$$

d'après (4.1), on a

$$1 \le 2X_iX_{i+1}L_i \ll c^2,$$

ce qui est impossible si c est suffisamment petit. ∎

4.2. *Le cas $n = 3$.* Cette fois, on se place dans le cas $n = 3$, $\lambda = (-1+\sqrt{5})/2$; on vérifie alors que λ est solution de

$$1/\lambda - 1 = \lambda,$$

et donc (3.2) devient

$$L_i \ll c^{1/\lambda}X_i^{-1}X_{i+1}^{-\lambda}. \tag{4.2}$$

Tout d'abord, on montre que la matrice $\left(\begin{smallmatrix} x_{i,0} & x_{i,1} \\ x_{i,1} & x_{i,2}\end{smallmatrix}\right)$ est de rang 2 : si ce n'était pas le cas, comme les coordonnées de $\mathcal{X}_i$ sont premières entre elles, il existerait des entiers k et l, premiers entre eux, tels que

$$x_{i,0} = k^2, \quad x_{i,1} = kl, \quad x_{i,2} = l^2.$$

D'autre part, p ne divise pas $x_{i,0}$: sinon $|x_{i,0}|_p < 1$ et donc $|x_{i,m}|_p < 1$ pour tout m puisque $\xi \in \mathbb{Z}_p$, ce qui signifie que p divise tous les $x_{i,m}$, ce qui est impossible puisqu'ils sont premiers entre eux. Par conséquent,

$$|x_{i,0}|_p = 1.$$

On en déduit que

$$|k\xi - l|_p \leq L_i.$$

Comme la matrice $\left(\begin{smallmatrix} x_{i-1,0} & x_{i-1,1} & x_{i-1,2} \\ x_{i,0} & x_{i,1} & x_{i,2} \end{smallmatrix}\right)$ est de rang 2, puisque $\mathcal{X}_{i-1}$ et $\mathcal{X}_i$ sont linéairements indépendants, et comme $x_{i-1,1}$ et $x_{i,1}$ sont non nuls, l'un des déterminants $\left|\begin{smallmatrix} x_{i-1,0} & x_{i-1,1} \\ x_{i,0} & x_{i,1} \end{smallmatrix}\right|$ ou $\left|\begin{smallmatrix} x_{i-1,1} & x_{i-1,2} \\ x_{i,1} & x_{i,2} \end{smallmatrix}\right|$ est non nul. Supposons par exemple que le premier est non nul, on a alors

$$1 \leq \left|\begin{matrix} x_{i-1,0} & x_{i-1,1} \\ k & l \end{matrix}\right| \left|\begin{matrix} x_{i-1,0} & x_{i-1,1} \\ k & l \end{matrix}\right|_p,$$

et comme

$$\left|\begin{matrix} x_{i-1,0} & x_{i-1,1} \\ k & l \end{matrix}\right| \leq 2X_{i-1}X_i^{1/2},$$

et

$$\left|\begin{matrix} x_{i-1,0} & x_{i-1,1} \\ k & l \end{matrix}\right|_p = \left|\begin{matrix} x_{i-1,0} & x_{i-1,1} - x_{i-1,0}\xi \\ k & l - k\xi \end{matrix}\right|_p \leq \max(L_{i-1}, L_i) \leq L_{i-1},$$

on a, d'après (4.2)

$$1 \leq 2X_{i-1}X_i^{1/2}L_{i-1} \ll c^{1/\lambda}X_i^{1/2-\lambda},$$

ce qui est impossible puisque $\lambda > 1/2$, pour c suffisamment petit. On aboutit au même résultat si on suppose que le deuxième déterminant est non nul.

On a alors

$$1 \leq \left|\begin{matrix} x_{i,0} & x_{i,1} \\ x_{i,1} & x_{i,2} \end{matrix}\right| \left|\begin{matrix} x_{i,0} & x_{i,1} \\ x_{i,1} & x_{i,2} \end{matrix}\right|_p. \tag{4.3}$$

En outre, on a

$$|x_{i,2} - x_{i,1}\xi|_p = |(x_{i,2} - x_{i,0}\xi^2) - \xi(x_{i,1} - x_{i,0}\xi)|_p \leq L_i,$$

donc

$$\left|\begin{matrix} x_{i,0} & x_{i,1} \\ x_{i,1} & x_{i,2} \end{matrix}\right|_p = \left|\begin{matrix} x_{i,0} & x_{i,1} - x_{i,0}\xi \\ x_{i,1} & x_{i,2} - x_{i,1}\xi \end{matrix}\right|_p \leq L_i.$$

On a alors, d'après (4.3),

$$1 \leq 2X_i^2 L_i \ll c^{1/\lambda}X_i X_{i+1}^{-\lambda},$$

et donc

$$X_{i+1}^{\lambda} \ll c^{1/\lambda}X_i. \tag{4.4}$$

Ensuite, on montre que pour une infinité de i, on a $\mathcal{X}_{i-1}$, $\mathcal{X}_i$ et $\mathcal{X}_{i+1}$ linéairement indépendants : si ce n'est pas le cas, comme $\mathcal{X}_{i-1}$ et $\mathcal{X}_i$ sont libres, on a pour tout i assez grand $\mathcal{X}_{i+1} \in \langle \mathcal{X}_{i-1}, \mathcal{X}_i \rangle$, où $\langle \mathcal{X}_{i-1}, \mathcal{X}_i \rangle$ désigne

ici le $\mathbb{Q}$-espace vectoriel engendré par $\mathcal{X}_{i-1}$ et $\mathcal{X}_i$. On a alors $\mathcal{X}_n \in \langle \mathcal{X}_{i-1}, \mathcal{X}_i \rangle$, pour $n \geq i$. On en déduit qu'il existe des entiers a, b et c tels que

$$ax_{n,0} + bx_{n,1} + cx_{n,2} = 0$$

pour tout n assez grand, et donc que

$$|x_{n,0}(a + b\xi + c\xi^2)|_p = |b(x_{n,1} - x_{n,0}\xi) + c(x_{n,2} - x_{n,0}\xi^2)|_p \leq L_n,$$

ce qui est impossible puisque $|x_{n,0}|_p = 1$ et que ξ n'est pas un nombre quadratique.

Enfin, pour de tels i, on a

$$1 \leq \begin{vmatrix} x_{i-1,0} & x_{i-1,1} & x_{i-1,2} \\ x_{i,0} & x_{i,1} & x_{i,2} \\ x_{i+1,0} & x_{i+1,1} & x_{i+1,2} \end{vmatrix} \begin{vmatrix} x_{i-1,0} & x_{i-1,1} & x_{i-1,2} \\ x_{i,0} & x_{i,1} & x_{i,2} \\ x_{i+1,0} & x_{i+1,1} & x_{i+1,2} \end{vmatrix}_p,$$

puisque $\mathcal{X}_{i-1}$, $\mathcal{X}_i$ et $\mathcal{X}_{i+1}$ sont linéairement indépendants. Or,

$$\begin{vmatrix} x_{i-1,0} & x_{i-1,1} & x_{i-1,2} \\ x_{i,0} & x_{i,1} & x_{i,2} \\ x_{i+1,0} & x_{i+1,1} & x_{i+1,2} \end{vmatrix} \ll X_{i-1}X_iX_{i+1},$$

et

$$\begin{aligned} \begin{vmatrix} x_{i-1,0} & x_{i-1,1} & x_{i-1,2} \\ x_{i,0} & x_{i,1} & x_{i,2} \\ x_{i+1,0} & x_{i+1,1} & x_{i+1,2} \end{vmatrix}_p &= \begin{vmatrix} x_{i-1,0} & x_{i-1,1} - x_{i-1,0}\xi & x_{i-1,2} - x_{i-1,0}\xi^2 \\ x_{i,0} & x_{i,1} - x_{i,0}\xi & x_{i,2} - x_{i,0}\xi^2 \\ x_{i+1,0} & x_{i+1,1} - x_{i+1,0}\xi & x_{i+1,2} - x_{i+1,0}\xi^2 \end{vmatrix}_p \\ &\leq \max(L_{i-1}L_i, L_{i-1}L_{i+1}, L_iL_{i+1}) \leq L_{i-1}L_i. \end{aligned}$$

Et donc on a

$$1 \ll X_{i-1}X_iX_{i+1}L_{i-1}L_i,$$

puis, compte tenu de (4.2),

$$1 \ll c^{2/\lambda}X_i^{-\lambda}X_{i+1}^{1-\lambda};$$

enfin, en utilisant (4.4), on obtient

$$1 \ll c^{2/\lambda+(1-\lambda)/\lambda^2}X_i^{-\lambda+(1-\lambda)/\lambda} = c^{1+2/\lambda},$$

compte tenu de l'équation vérifiée par λ. Mais ceci est impossible si c est assez petit. ∎

4.3. *Le cas* $n = 4$. On considère le cas $n = 4$, $\lambda = 2/3$; ainsi (3.2) devient

$$L_i \ll c^{3/2}X_i^{-1}X_{i+1}^{-1/2}. \tag{4.5}$$

Le début de cette preuve est assez similaire à la précédente : on commence par montrer que la matrice $\left(\begin{smallmatrix} x_{i,0} & x_{i,1} & x_{i,2} \\ x_{i,1} & x_{i,2} & x_{i,3} \end{smallmatrix}\right)$ est de rang 2. Si ce n'est pas vrai, alors il existe des entiers k et l, premiers entre eux, tels que

$$x_{i,0} = k^3, \quad x_{i,1} = k^2l, \quad x_{i,2} = kl^2, \quad x_{i,3} = l^3.$$

Comme on a toujours $|x_{i,0}|_p = 1$, on a $|k\xi - l|_p \le L_i$. Puisque $\mathcal{X}_{i-1}$ et $\mathcal{X}_i$ sont linéairement indépendants et que leurs coordonnées sont non nulles, l'un des déterminants $\left|\begin{smallmatrix} x_{i-1,0} & x_{i-1,1} \\ x_{i,0} & x_{i,1}\end{smallmatrix}\right|$, $\left|\begin{smallmatrix} x_{i-1,1} & x_{i-1,2} \\ x_{i,1} & x_{i,2}\end{smallmatrix}\right|$, $\left|\begin{smallmatrix} x_{i-1,2} & x_{i-1,3} \\ x_{i,2} & x_{i,3}\end{smallmatrix}\right|$ est non nul. On aboutit alors à une contradiction comme dans la démonstration précédente.

On définit, pour un point $\mathcal{X}_i$, deux vecteurs linéairement indépendants $\mathcal{Y}_i = (x_{i,0}, x_{i,1}, x_{i,2})$ et $\mathcal{Z}_i = (x_{i,1}, x_{i,2}, x_{i,3})$. On a alors

$$\langle \mathcal{Y}_{i+1}, \mathcal{Z}_{i+1}\rangle = \langle \mathcal{Y}_i, \mathcal{Z}_i\rangle. \tag{4.6}$$

En effet,

$$\begin{vmatrix} x_{i,0} & x_{i,1} & x_{i,2} \\ x_{i,1} & x_{i,2} & x_{i,3} \\ x_{i+1,0} & x_{i+1,1} & x_{i+1,2}\end{vmatrix} = \begin{vmatrix} x_{i,0} & x_{i,1} - x_{i,0}\xi & x_{i,2} - x_{i,0}\xi^2 \\ x_{i,1} & x_{i,2} - x_{i,1}\xi & x_{i,3} - x_{i,1}\xi^2 \\ x_{i+1,0} & x_{i+1,1} - x_{i+1,0}\xi & x_{i+1,2} - x_{i+1,0}\xi^2\end{vmatrix}_p$$
$$\le \max(L_i^2, L_iL_{i+1}) \le L_i^2,$$

car

$$|x_{i,2} - x_{i,1}\xi|_p = |(x_{i,2} - x_{i,0}\xi^2) - \xi(x_{i,1} - x_{i,0}\xi)|_p \le L_i$$

et

$$|x_{i,3} - x_{i,1}\xi^2|_p = |(x_{i,3} - x_{i,0}\xi^3) - \xi^2(x_{i,1} - x_{i,0}\xi)|_p \le L_i.$$

Donc

$$\begin{vmatrix} x_{i,0} & x_{i,1} & x_{i,2} \\ x_{i,1} & x_{i,2} & x_{i,3} \\ x_{i+1,0} & x_{i+1,1} & x_{i+1,2}\end{vmatrix}\begin{vmatrix} x_{i,0} & x_{i,1} & x_{i,2} \\ x_{i,1} & x_{i,2} & x_{i,3} \\ x_{i+1,0} & x_{i+1,1} & x_{i+1,2}\end{vmatrix}_p \ll X_i^2 X_{i+1} L_i^2 \ll c^3.$$

Donc $\mathcal{Y}_{i+1} \in \langle \mathcal{Y}_i, \mathcal{Z}_i\rangle$ pour c assez petit, de même, on a $\mathcal{Z}_{i+1} \in \langle \mathcal{Y}_i, \mathcal{Z}_i\rangle$, ce qui démontre (4.6). Ceci étant vrai pour tout i, il existe des entiers a, b et c tels que $ax_{i,0} + bx_{i,1} + cx_{i,2} = 0$. On a alors

$$|x_{i,0}(a + b\xi + c\xi^2)|_p \le L_i,$$

ce qui est impossible si ξ n'est pas quadratique puisque $|x_{0,i}|_p = 1$. ∎

5. Le cas général

5.1. *Deux résultats préliminaires.* Pour démontrer le cas général, on a besoin des deux lemmes suivants :

Lemme 2. *Soient Q et R deux polynômes non nuls, à coefficients entiers et de degrés respectifs q et r. Alors, si Q et R sont premiers entre eux et si ξ est un nombre p-adique, on a*

$$1 \le (q+r)!\max(1, |\xi|_p^{q-1}, |\xi|_p^{r-1})\mathrm{H}(Q)^r\mathrm{H}(R)^q\max(|Q(\xi)|_p, |R(\xi)|_p).$$

On pose

$$Q(X) = a_0X^q + \ldots + a_q, \qquad R(X) = b_0X^r + \ldots + b_r.$$

On a alors

$$\mathrm{Res}(Q,R)=\begin{vmatrix} a_0 & a_1 & \dots & a_q & & & \\ & a_0 & a_1 & \dots & a_q & & \\ & & \ddots & & & \ddots & \\ & & & a_0 & a_1 & \dots & a_q \\ b_0 & b_1 & \dots & b_r & & & \\ & b_0 & b_1 & \dots & b_r & & \\ & & \ddots & & & \ddots & \\ & & & b_0 & b_1 & \dots & b_r \end{vmatrix}.$$

On en déduit que

$$|\mathrm{Res}(Q,R)|\le (q+r)!\mathrm{H}(Q)^r\mathrm{H}(R)^q. \tag{5.1}$$

D'autre part,

$$\mathrm{Res}(Q,R)=\begin{vmatrix} a_0 & a_1 & \dots & a_q & & & \xi^{r-1}Q(\xi) \\ & a_0 & a_1 & \dots & a_q & & \xi^{r-2}Q(\xi) \\ & & \ddots & & & \ddots & \\ & & & a_0 & a_1 & \dots & Q(\xi) \\ b_0 & b_1 & \dots & b_r & & & \xi^{q-1}R(\xi) \\ & b_0 & b_1 & \dots & b_r & & \xi^{q-2}R(\xi) \\ & & \ddots & & & \ddots & \\ & & & b_0 & b_1 & \dots & R(\xi) \end{vmatrix},$$

et donc,

$$|\mathrm{Res}(Q,R)|_p\le \max(1,|\xi|_p^{q-1},|\xi|_p^{r-1})\max(|Q(\xi)|_p,|R(\xi)|_p). \tag{5.2}$$

Comme Q et R sont premiers entre eux, leur résultant est un entier non nul et donc $1\le |\mathrm{Res}(Q,R)|\cdot|\mathrm{Res}(Q,R)|_p$, ce qui donne le résultat annoncé, compte tenu de (5.1) et (5.2). ∎

Lemme 3. *Soient h et m des entiers tels que $1\le h\le m$, $a_0,\dots,a_h$ des entiers premiers entre eux dans leur ensemble et $\mathcal{Y}_0,\dots,\mathcal{Y}_m$ des points de $\mathbb{Z}^h$ engendrant $\mathbb{R}^h$. On suppose que ces points vérifient le système de relations*

$$a_0\mathcal{Y}_i+a_1\mathcal{Y}_{i+1}+\dots+a_h\mathcal{Y}_{i+h}=0 \quad \textit{pour } 0\le i\le m-h.$$

On suppose également que tout déterminant d'ordre h extrait de la matrice des $\mathcal{Y}_i$ est majoré en valeur absolue usuelle par un réel Z et en valeur absolue p-adique par $p^{-\varrho}$, où ϱ est un entier positif. Alors, on a

$$\max_{0\le i\le h}|a_i|\ll\left(\frac{Z}{p^{\varrho}}\right)^{1/m-h+1}.$$

On reprend la preuve de l'analogue de ce lemme dans le cas réel présentée dans l'article de H. Davenport et W. M. Schmidt [3, théorème 3, p. 396].

Si un seul des a_i est non nul alors le résultat est évident car cet entier vaut ± 1 et $Zp^{-\varrho} \geq 1$. En effet, comme les vecteurs $\mathcal{Y}_i$ engendrent $\mathbb{R}^h$, il existe un déterminant Δ extrait de la matrice de ces vecteurs d'ordre h non nul et pour ce déterminant, on a

$$1 \leq |\Delta| \cdot |\Delta|_p \leq Zp^{-\varrho}.$$

Dans le cas contraire, soit l le plus grand indice tel que $a_l \neq 0$; on a $1 \leq l \leq h$. Si $l = h$, les vecteurs $\mathcal{Y}_0, \ldots, \mathcal{Y}_{h-1}$ forment une base de $\mathbb{R}^h$, et si $l < h$, les vecteurs $\mathcal{Y}_0, \ldots, \mathcal{Y}_{l-1}, \mathcal{Y}_{m-h+l+1}, \ldots, \mathcal{Y}_m$ forment une base de $\mathbb{R}^h$. Pour un l-uplet d'entiers au plus égaux à m, $(\nu_1, \ldots, \nu_l)$, on définit le déterminant suivant :

$$D(\nu_1, \ldots, \nu_l) = \begin{cases} \det(\mathcal{Y}_{\nu_1}, \ldots, \mathcal{Y}_{\nu_l}) & \text{si } l = h, \\ \det(\mathcal{Y}_{\nu_1}, \ldots, \mathcal{Y}_{\nu_l}, \mathcal{Y}_{m-h+l+1}, \ldots, \mathcal{Y}_m) & \text{sinon.} \end{cases}$$

Dans les deux cas, on a $D(0, \ldots, l-1) \neq 0$. On montre alors qu'il existe pour $0 \leq i < l$ des polynômes P_i à coefficients entiers en les variables $a_0, \ldots, a_l$ de la forme

$$P_i = \pm a_i^{m-h+1} + Q_i,$$

où Q_i est homogène de degré $m - h + 1$ et dont chaque terme contient au moins une des variables $a_{i+1}, \ldots, a_l$. En outre, ces polynômes vérifient

$$a_l^{m-h+1} D(0, \ldots, i-1, m-h+i+1, \ldots, m-h+l) = P_i(a_0, \ldots, a_l) D(0, \ldots, l-1).$$

C'est à partir de ces relations et du fait que $|D(\nu_1, \ldots, \nu_l)| \leq Z$ que H. Davenport et W. M. Schmidt déduisent que $\max_{0 \leq i \leq h} |a_i| \leq Z^{1/m-h+1}$. Or la deuxième hypothèse sur ces déterminants signifie qu'ils sont tous divisibles par p^{ϱ}, on peut donc diviser les relations précédentes par p^{ϱ}. Le reste de la démonstration est toujours valide si on remplace Z par $p^{-\varrho}Z$, ce qui mène au résultat annoncé. ∎

5.2. *Preuve du théorème 2.* Pour simplifier les notations, on va remplacer $n - 1$ par n. On considère le système suivant d'inéquations :

$$\max(|x_0|, \ldots, |x_n|) \leq cp^{(n+1)\lambda h},$$
$$|x_m - x_0 \xi^m|_p \leq p^{-h(n+1)} \quad \text{pour } m = 1, \ldots, n,$$

où ξ est un entier p-adique non algébrique de degré au plus $[n/2]$. Enfin, on pose $k = [n/2]$, de sorte que $1/\lambda = 1 + 1/k$, et ainsi, (3.2) devient

$$L_i \ll c^{1+1/k} X_i^{-1} X_{i+1}^{-1/k}. \tag{5.3}$$

Posons

$$k_i = \left\lceil k \frac{\log X_i}{\log X_{i+1}} \right\rceil,$$

où $\lceil x \rceil$ désigne le plus petit entier majorant x ; on a alors

$$1 \leq k_i \leq k.$$

Dans la suite, on pose $\mathcal{Y} = \mathcal{X}_i$ afin d'alléger les notations. Alors si c est assez petit, la matrice

$$\begin{pmatrix} y_0 & y_1 & \cdots & y_{n-k_i} \\ y_1 & y_2 & \cdots & y_{n-k_i+1} \\ \vdots & \vdots & & \vdots \\ y_{k_i} & y_{k_i+1} & \cdots & y_n \end{pmatrix} \tag{5.4}$$

est de rang au plus k_i. En effet, soit M une matrice carrée extraite d'ordre $k_i + 1$:

$$M = \begin{pmatrix} y_{j_0} & y_{j_1} & \cdots & y_{j_{k_i}} \\ y_{j_0+1} & y_{j_1+1} & \cdots & y_{j_{k_i}+1} \\ \vdots & \vdots & & \vdots \\ y_{j_0+k_i} & y_{j_1+k_i} & \cdots & y_{j_{k_i}+k_i} \end{pmatrix}.$$

On a

$$|\det M| \ll X_i^{k_i+1}$$

et

$$|\det M|_p = \begin{vmatrix} y_{j_0} & \xi^{j_1-j_0} y_{j_0} - y_{j_1} & \cdots & \xi^{j_{k_i}-j_0} y_{j_0} - y_{j_{k_i}} \\ y_{j_0+1} & \xi^{j_1-j_0} y_{j_0+1} - y_{j_1+1} & \cdots & \xi^{j_{k_i}-j_0} y_{j_0+1} - y_{j_{k_i}+1} \\ \vdots & \vdots & & \vdots \\ y_{j_0+k_i} & \xi^{j_1-j_0} y_{j_0+k_i} - y_{j_1+k_i} & \cdots & \xi^{j_{k_i}-j_0} y_{j_0+k_i} - y_{j_{k_i}+k_i} \end{vmatrix}_p \leq L_i^{k_i},$$

car

$$|\xi^{a-b} y_b - y_a|_p = |(y_a - \xi^a y_0) - \xi^{a-b}(y_b - \xi^b y_0)|_p \leq L_i.$$

Par conséquent

$$|\det M| \cdot |\det M|_p \ll c^{k_i(1+1/k)} X_i X_{i+1}^{-k_i/k}.$$

Ainsi, tous les déterminants extraits de (5.4) d'ordre $k_i + 1$ sont nuls si c est assez petit.

Soit h_i le plus petit entier, $1 \leq h_i \leq k_i$, tel que la matrice

$$\begin{pmatrix} y_0 & y_1 & \cdots & y_{n-h_i} \\ y_1 & y_2 & \cdots & y_{n-h_i+1} \\ \vdots & \vdots & & \vdots \\ y_{h_i} & y_{h_i+1} & \cdots & y_n \end{pmatrix}$$

soit de rang au plus h_i. On considère alors la matrice

$$\begin{pmatrix} y_0 & y_1 & \cdots & y_{n-h_i+1} \\ y_1 & y_2 & \cdots & y_{n-h_i+2} \\ \vdots & \vdots & & \vdots \\ y_{h_i-1} & y_{h_i} & \cdots & y_n \end{pmatrix}; \tag{5.5}$$

on peut faire deux remarques à propos de cette matrice : d'abord, elle possède une ligne de moins mais une colonne de plus que la matrice précédente, ensuite, comme $h_i \leq n/2$, elle a plus de colonnes que de lignes et donc elle est de rang au plus h_i. En fait, la matrice (5.5) est de rang h_i : c'est évident si $h_i = 1$ et si $h_i > 1$, cela résulte de la minimalité de h_i qui assure que la matrice (5.5) est de rang $> h_i - 1$.

Soit Z_i le maximum des valeurs absolues des déterminants extraits d'ordre h_i de (5.5), alors on a

$$Z_i \ll X_i^{h_i}; \tag{5.6}$$

et soit Z_i' le maximum des valeurs absolues p-adiques des déterminants extraits d'ordre h_i de (5.5). L'argument utilisé pour déterminer le rang de (5.4) montre que

$$Z_i' \leq L_i^{h_i-1}. \tag{5.7}$$

Comme (5.5) est de rang h_i, ses $h_i + 1$ premières colonnes sont linéairement dépendantes, il existe donc des entiers $a_0^{(i)}, \ldots, a_{h_i}^{(i)}$ non tous nuls, premiers entre eux, tels que

$$a_0^{(i)} y_j + a_1^{(i)} y_{j+1} + \ldots + a_{h_i}^{(i)} y_{j+h_i} = 0 \tag{5.8}$$

pour $0 \leq j \leq n - h_i$. On pose alors

$$a^{(i)} = \max_{0 \leq j \leq h_i} |a_j^{(i)}|.$$

Si on note $\mathcal{W}_0, \ldots, \mathcal{W}_m$, avec $m = n - h_i + 1$, les vecteurs colonnes de (5.5), les relations (5.8) signifient que

$$a_0^{(i)} \mathcal{W}_j + a_1^{(i)} \mathcal{W}_{j+1} + \ldots + a_{h_i}^{(i)} \mathcal{W}_{j+h_i} = 0$$

pour $0 \leq j \leq m - h_i$. Ainsi, d'après le lemme 3, compte tenu de (5.6) et (5.7), on a

$$a^{(i)^{m-h_i+1}} \ll Z_i Z_i' \ll c^{(h_i-1)(1+1/k)} X_i X_{i+1}^{-(h_i-1)/k} \ll X_i^{1-(h_i-1)/k},$$

car $X_i < X_{i+1}$ et on peut supposer que $c < 1$.

Donc

$$a^{(i)} \ll X_i^{(1-(h_i-1)/k)/(n-2h_i+2)} \ll X_i^{1/n}, \tag{5.9}$$

la dernière majoration provenant de la décroissance de l'exposant en fonction de h_i.

En revenant à la notation $\mathcal{X}_i$, d'après (5.8), on a

$$a_0^{(i)} x_{i,0} + a_1^{(i)} x_{i,1} + \ldots + a_{h_i}^{(i)} x_{i,h_i} = 0,$$

et donc

$$\begin{aligned} &|x_{i,0}(a_0^{(i)} + a_1^{(i)}\xi + \ldots + a_{h_i}^{(i)}\xi^{h_i})|_p \\ &\qquad = |a_1^{(i)}(x_{i,1} - \xi x_{i,0}) + \ldots + a_{h_i}^{(i)}(x_{i,h_i} - \xi^{h_i} x_{i,0})|_p \le L_i. \end{aligned}$$

À nouveau, on a $|x_{i,0}|_p = 1$, donc

$$|a_0^{(i)} + a_1^{(i)}\xi + \ldots + a_{h_i}^{(i)}\xi^{h_i}|_p \ll c^{1+1/k} X_i^{-1} X_{i+1}^{-1/k}. \tag{5.10}$$

Si on pose $Y_i = X_i^{1/n}$, comme $X_i^k \ge X_{i+1}^{k_i - 1}$ d'après la définition de k_i, on a pour chaque i un polynôme P_i, de degré au plus k_i, à coefficients entiers tel que

$$|P_i(\xi)|_p \ll c^{1+1/k} \min(Y_i^{-n(1+1/k)}, Y_{i+1}^{-nk_i/k}), \tag{5.11}$$

$$\mathrm{H}(P_i) \ll Y_i. \tag{5.12}$$

Soit k_0 le plus petit entier, $1 \le k_0 \le k$, tel que $k_i = k_0$ pour une infinité d'indices i. Il existe une infinité de polynômes irréductibles P, de degré au plus k_0, tels que

$$|P(\xi)|_p \le \mathrm{H}(P)^{-n(1+1/k)}. \tag{5.13}$$

En effet, si ce n'etait pas le cas, on aurait pour tout polynôme irréductible de degré au plus k_0, sauf pour un nombre fini,

$$|P(\xi)|_p > \mathrm{H}(P)^{-n(1+1/k)}.$$

Comme ξ n'est pas algébrique de degré $\le n/2$ et comme $k_0 \le n/2$, l'inégalité

$$|P(\xi)|_p \gg \mathrm{H}(P)^{-n(1+1/k)},$$

est vraie pour tout polynôme irréductible P, à coefficients entiers et de degré au plus k_0. On aurait alors, pour tout polynôme à coefficients entiers de degré au plus k_0,

$$|P(\xi)|_p \gg \mathrm{H}(P)^{-n(1+1/k)}.$$

Mais d'après (5.11) et (5.12), il existe un polynôme P_i de degré au plus k_0 tel que

$$|P_i(\xi)|_p \ll c^{1+1/k} \mathrm{H}(P_i)^{-n(1+1/k)},$$

ce qui est contradictoire si c est assez petit.

D'autre part, d'après le choix de k_0 et d'après (5.11) et (5.12), pour tout Y assez grand, il existe un entier $k(Y)$ vérifiant $k_0 \le k(Y) \le k$, et un polynôme Q non nul, à coefficients entiers, de degré au plus $k(Y)$ tel que

$$|Q(\xi)|_p \ll c^{1+1/k} Y^{-nk(Y)/k}, \tag{5.14}$$

$$\mathrm{H}(Q) \ll Y\,; \tag{5.15}$$

en effet, il suffit de prendre pour Q le polynôme P_i pour l'indice i tel que $Y_i \le Y < Y_{i+1}$.

Un résultat de Gelfond (*cf.* par exemple [6, p. 77]) assure que si P et Q sont deux polynômes à coefficients entiers, de degré au plus n, tels que P divise Q alors $\mathrm{H}(Q) \ge e^{-n}\mathrm{H}(P)$. Soit alors P un polynôme irréductible à coefficients entiers et de degré au plus k_0 vérifiant (5.13). On pose

$$Y = \tfrac{1}{2} c_1^{-1} e^{-n} \mathrm{H}(P),$$

où c_1 est la constante implicite de (5.15). Soit Q un polynôme à coefficients entiers et de degré au plus $k(Y)$ vérifiant (5.14) et (5.15). D'après le choix de Y, (5.15) assure que P ne divise pas Q et donc que P et Q sont premiers entre eux puisque P est irréductible. De plus, d'après (5.14) et (5.15) et d'après le choix de Y, on a

$$|Q(\xi)|_p \ll c^{1+1/k} \mathrm{H}(P)^{-nk(Y)/k}, \tag{5.16}$$

$$\mathrm{H}(Q) \ll \mathrm{H}(P). \tag{5.17}$$

Comme P et Q sont premiers entre eux, on peut appliquer le lemme 2, ce qui nous donne

$$1 \ll \mathrm{H}(P)^{k_0} \mathrm{H}(Q)^{k(Y)} \max(|P(\xi)|_p, |Q(\xi)|_p),$$

donc, compte tenu de (5.13), (5.16) et (5.17),

$$1 \ll c^{1+1/k} \mathrm{H}(P)^{k_0 + k(Y) - nk(Y)/k}.$$

Or ceci est impossible si c est assez petit car

$$k_0 + k(Y) - nk(Y)/k \le k(Y)(2 - n/k) \le 0. \ \blacksquare$$

Références

[1] Y. Bugeaud et O. Teulié, *Approximation d'un nombre réel par des nombres algébriques de degré donné*, Acta Arith. 93 (2000), 77–86.

[2] J. W. S. Cassels, *An Introduction to Geometry of Numbers*, Grundlehren Math. Wiss. 99, Springer, 1959.

[3] H. Davenport and W. M. Schmidt, *Approximation to real numbers by algebraic integers*, Acta Arith. 15 (1969), 393–416.

[4] J. F. Morrison, *Approximation of p-adic numbers by algebraic numbers of bounded degree*, J. Number Theory 10 (1978), 334–350.

[5] J. Neukirch, *Algebraic Number Theory*, Grundlehren Math. Wiss. 322, Springer, 1999.

[6] T. Schneider, *Introduction aux nombres transcendants*, Gauthier-Villars, Paris, 1959.

[7] O. Teulié, *Approximation d'un nombre réel par des unités algébriques*, soumis.
[8] E. Wirsing, *Approximation mit algebraischen Zahlen beschränkten Grades*, J. Reine Angew. Math. 206 (1961), 67–77.

Laboratoire A2X
Université Bordeaux 1
U.F.R. Mathématiques–Informatique
351, cours de la Libération
33405 Talence Cedex, France
E-mail: teulie@math.u-bordeaux.fr

Reçu le 3.8.2000
et révisé le 19.3.2001 (3868)