Astérisque

E. DUBOIS
R. PAYSANT-LE ROUX

Sur la longueur du développement en fraction continue de $\sqrt{f(n)}$

Astérisque, tome 198-199-200 (1991), p. 107-119
<http://www.numdam.org/item?id=AST_1991__198-199-200__107_0>

© Société mathématique de France, 1991, tous droits réservés.

L'accès aux archives de la collection « Astérisque » (http://smf4.emath.fr/Publications/Asterisque/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM
Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

SUR LA LONGUEUR DU DEVELOPPEMENT EN FRACTION CONTINUE DE $\sqrt{f(n)}$

par

E. DUBOIS ET R. PAYSANT-LE ROUX

Introduction

On considère un polynôme $f(X)$ de degré pair à coefficients entiers dont le terme de plus haut degré est un carré et l'on s'intéresse à la longueur $\ell p(\sqrt{f}(n))$ de la période du développement en fraction continue de $\sqrt{f}(n)$ lorsque n est un entier rendant $f(n)$ positif non carré. SCHMIDT [1948] a considéré le cas $f(x) = X^2 + h$; SCHINZEL [1961] pour $f(X) = a^2X^2 + bX + c$, a introduit l'ensemble

$$E = \{n \in \mathbf{Z} \mid (b^2 - 4ac) \textit{ ne divise pas } 4(2a^2n + b)\}$$

et a montré que :

(1) Pour les entiers n n'appartenant pas à E, la longueur de la période de $\sqrt{f}(n)$ est bornée ;

(2) Pour les entiers n de E, la limite de $\ell p(\sqrt{f}(n)$ tend vers l'infini avec n.

SCHINZEL [1962] a généralisé ce résultat pour un polynôme à coefficients entiers dont le terme de plus haut degré est un carré. LOUBOUTIN [1987] a donné une version effective de (2). Nous nous proposons de généraliser ce résultat à un polynôme $f(X)$ du type précédent et nous pourrons en déduire si le développement en fraction continue formelle de $\sqrt{f}(X)$ est périodique. Signalons que dans le cas d'un polynôme $f(X) = aX^d + \ldots$ avec d impair et a positif ou avec d pair et a positif non carré, SCHINZEL [1961] a montré que la limite supérieure de $\ell p(\sqrt{f}(n)$ est infinie. Dans une autre direction, on peut citer les résultats de COHN [1977] : pour m entier non carré on a avec une constante effective :

$$\ell p(\sqrt{m}) \ll \sqrt{m}\ log\ m.$$

1. Le cadre des meilleures approximations

1.1. les fractions continues formelles

Un élément $\alpha = \sum_{-h}^{\infty} a_i X^{-i}$ du corps des séries de Laurent $\mathbf{Q}((1/X))$ se décompose en $E(\alpha) + F(\alpha)$ où $E(\alpha) = a_{-h}X^h + ... + a_{-1}X + a_0$ joue le rôle de la partie entière, ou partie polynômiale ; on pose deg $\alpha = h$ si a_{-h} est non nul. A partir de $\alpha_0 = \alpha$ on détermine la suite (α_k) par $\alpha_k = F(\alpha_{k-1})^{-1}$. En posant $u_k = E(\alpha_k)$ on obtient le développement en fraction continue formelle $[u_0, u_1, ..., u_k, \ldots]$ de α auquel on associe les réduites A_k/B_k par les formules de récurrences habituelles provenant de $A_k/B_k = [u_0, u_1, \ldots, u_k]$.

PROPOSITION 1. — *Soit* $W \in \mathbf{Q}((1/X))$ *avec* $W^2 \in \mathbf{Z}[X]$. *Si le développement en fraction continue formelle de W est périodique, la prépériode est de longueur 1 et la période possède une symétrie. Si*

$$W = [u_0, \overline{u}_1, \ldots, u_\ell],$$

on a

$$u_\ell(X) = 2u_0(X), u_j(X) = u_{\ell-j}(X) \text{ pour } 1 \leq j \leq \frac{\ell}{2}.$$

Cette proposition semble classique mais tous les résultats bien connus du cas réel ne se prolongent pas toujours au cas formel. Par exemple on sait que le développement d'un nombre quadratique n'est pas toujours périodique.

Démonstration (schéma). Si

$$\beta = (A(X) + B(X)W)D(X)^{-1} = c_d X^d + c_{d-1}X^{d-1} + \ldots$$

dans $\mathbf{Q}((1/X))$ avec $c_d \neq 0$ on pose

$$d = deg\beta, \beta' = (A(X) - B(X)W)D(X)^{-1}.$$

On dit que β est spécial si deg $(\beta) \geq 1$ et deg $(\beta') \leq 0$. On montre facilement les points suivants :

- si la fraction continue formelle de β est purement périodique alors β est spécial ;
- le successeur d'un nombre spécial est spécial ;

- parmi les prédécesseurs possibles d'un nombre spécial, il y a un seul nombre spécial ;
- si la fraction continue de W, avec $W^2 = f(X)$, est périodique, alors le développement de $\alpha = W + E(W)$ est purement périodique.

Soit maintenant $W = [u_0, u_1, \ldots]$ périodique ; alors

$$\alpha = [2u_0, u_1, ..., \overline{u_k, u_{k+1}, ..., u_{k+\ell-1}}]$$

est aussi périodique. Posons $\beta = [\overline{u_k, u_{k+1}, ..., u_{k+\ell-1}}]$. Le nombre α étant spécial tous ses successeurs le sont. Pour $k > 1$ les nombres $\gamma = u_{k-1}\beta^{-1}$ sont deux prédécesseurs spéciaux de β. Il sont donc égaux et on a $u_{k-1} = U_{k+\ell-1}$. De proche en proche on obtient $\alpha = [2u_0, u_1, \ldots, u_{\ell-1}]$. En remarquant que

$$-1/\alpha' = \alpha_1 = [\overline{u_1, u_2, ..., u_{\ell-1}, 2u_0}],$$

on obtient la symétrie annoncée et la proposition.

1.2. Meilleures approximations et fractions continues

Soit $f(X) = a^2X^{2d} + ... \in \mathbf{Z}[X]$ avec a entier positif. On considère $W = aX^d + ... \in \mathbf{Q}((1/X))$ vérifiant $W^2 = f(X)$. Pour tout entier n rendant $f(n)$ positif non carré, on pose $w = \sqrt{f}(n)$. On note $\mathbf{O}_x$ l'anneau $\mathbf{Q}[X]+\mathbf{Q}[X]W$ et $\mathbf{O}_n$ l'anneau $\mathbf{Z} + \mathbf{Z}w$.

Nous définissons ici les meilleures approximations de w et de W et nous donnons rapidement, le lien avec les fractions continues réelles ou formelles, et la manière de lire les propriétés classiques des fractions continues (voir [2] et [7]).

Traitons d'abord le cas réel. Pour $\zeta = p - qw$, avec $(p, q) \in \mathbf{Z}^2$, on pose $| \zeta |_1 = | \zeta |$ et $| \zeta |_2 = | p + qw |$. On dit que ζ est *une meilleure approximation* de w si et seulement si pour tout $\delta \in \mathbf{O}_n = \mathbf{Z} + \mathbf{Z}w$, vérifiant $| \delta |_1 < | \zeta |_1$ et $| \delta |_2 < | \xi |_2$ on a $\delta = 0$. Ces meilleures approximations sont définies au signe près. L'ensemble des meilleures approximations de w dans $]0, 1]$ forment une suite $1, \zeta_1, \zeta_2, ...$ ordonnée par $| \zeta |$ décroissant et tendant vers 0. Cette suite est en bijection avec la suite des réduites p_k/q_k du développement en fraction continue de w par la relation $\zeta_{k+1} = | p_k - q_k w |$ pour $k \geq 0$. De même les meilleures approximations supérieures a 1 sont rangées par $| \zeta |_1$ croissant : $1, \zeta_{-1}, \zeta_{-2}, ...$

On note ε l'unité fondamentale dans $]0,1[$ de l'ordre $\mathbf{O}_n$. La périodicité du développement en fraction continue s'exprime par $\zeta_{k+\ell} = \pm\varepsilon\zeta_k$ pour tout $k \in \mathbf{Z}$. D'autre part, la définition montre que si $\zeta = p - qw$ est une meilleure approximation de w, son conjugué $\zeta' = p + qw$ l'est aussi. On obtient alors la suite des meilleures approximations positives :

$$\ldots \mid \zeta'_\ell \mid, \mid \zeta'_{\ell-1} \mid, \ldots, \mid \zeta'_1 \mid, 1, \zeta_1, \zeta_2, \ldots, \zeta_{\ell-1}, \zeta_\ell = \varepsilon, \ldots$$

Pour tout entier k,on a $\mid \zeta'_k \mid = \zeta_{\zeta-k}$ et avec la périodicité on a $\zeta_j = \varepsilon \mid \zeta'_{\ell-j} \mid$ pour $j = 1, 2, \ldots, \ell$. Ceci exprime la propriété de symétrie de la période du développement $w = [a_0, \overline{a_1, a_2, \ldots a_2, a_1, 2a_0}]$. Si la longueur ℓ est paire, il y a un terme médiant a'_h avec $h = \frac{\ell}{2}$, et on a $\zeta_h = \pm\zeta'_h$. En résumé :

PROPOSITION 2. — *Avec les définitions et notations précédentes, les meilleures approximations positives de w forment une suite (ζ_k) vérifiant $\zeta_0 = 1, \zeta_\ell = \varepsilon$ et $\zeta_{k+\ell} = \varepsilon\zeta_k$; on a $\zeta_j = \varepsilon \mid \zeta'_{\ell-j} \mid$ pour $j = 1, 2, \ldots, \ell$. Le lien avec les réduites s'exprime par $\zeta_{k+1} = \mid p_k - q_k w \mid$ pour $k \geq 0$.*

Revenons au cas formel. Pour $\beta = A(X) + B(X)W \in \mathbf{O}_x$ on définit les deux valeurs absolues $\mid \beta \mid_1 = e^{deg\beta}$ et $\mid \beta \mid_2 = \mid \beta' \mid_1$. On peut prendre la même définition que dans le cas réel : β est une meilleure approximation de W si et seulement si pour tout γ de $\mathbf{O}_x$ tel que $\mid \gamma \mid_1 < \mid \beta \mid_1$ et $\mid \gamma \mid_2 < \mid \beta \mid_2$ on a $\gamma = 0$. Ces meilleures approximations sont définies à un facteur multiplicatif rationnel non nul près. Les meilleures approximations de W de degré négatif forment une suite $1, \beta_1, \beta_2, \ldots$ qui est en bijection avec la suite des réduites de W par la relation $\beta_{k+1} = A_k - B_k W$ modulo $\mathbf{Q}*$. La périodicité (de longueur ℓ) du développement en fraction continue de W se traduit par l'existence d'une unité ε de $\mathbf{O}_x$ telle que

$$\beta_{k+\ell} = \varepsilon\beta_k \ (modulo\ \mathbf{Q}*)$$

pour tout $k \geq 0$, mais contrairement au cas réel ε n'est pas toujours l'unité fondamentale de $\mathbf{O}_x$, même si ℓ est minimale. Nous précisons cette particularité au paragraphe suivant.

Signalons que toute unité ε de $\mathbf{O}_x$ est une meilleure approximation, que si ζ est une meilleure approximation, il en va de même pour $\varepsilon\zeta$, et que comme dans le cas réel la notion de meilleure approximation ainsi exprimée donne une démonstration élégante de la propriété de symétrie de la période de W et de la

propriété de conjugaison

$$(\beta_j = \varepsilon\beta'_{\ell-j} modulo \mathbf{Q}*, 1 \leq j \leq \ell).$$

1.3. Groupes d'unités de $\mathbf{O}_x$

Un élément $\eta \in \mathbf{O}_x$ est une unité si et seulement si sa norme $N(\eta) = \eta\eta'$ est un nombre rationnel non nul. Si η est une unité de $\mathbf{O}_x, \lambda\eta$ l'est aussi pour tout $\lambda \in \mathbf{Q}*$. On considère donc le groupe G des unités modulo $\mathbf{Q}^*$. On sait [3] que le rang de ce groupe est soit 0 soit 1. Il est de rang 1 si est seulement si la fraction continue de W est périodique. Puisque nous supposons le développement en fraction continue de

$$W = [u_0, \overline{u_1, \ldots, u_{\ell-1}, 2u_0}]$$

périodique de longueur ℓ minimale, nous savons que $\varepsilon = A_{l-1}(X) - B_{l-1}(X)W$ est une unité de G de norme ± 1. Le groupe G_1 des unités de norme ± 1 sera donc aussi de rang 1.

Nous établissons maintenant le lien entre ε et les générateurs de G et de G_1 que nous notons respectivement φ et ψ. Montrons d'abord que la première unité dans la suite des meilleures approximations, de degré négatif, est située soit à la fin de la période du développement en fraction continue de W, soit au milieu et dans ce cas $\ell \equiv 2 \bmod 4$. Si parmi les $\ell - 1$ premières meilleures approximations de degré négatif de $W, \beta_1, \beta_2, \ldots, \beta_{\ell-1}$, il y a une unité $\beta_h = A_{h-1} - B_{h-1}W$ de G écrivons, pour $k \geq 0$:

$$W_k = [u_k, u_{k+1}, \ldots] = (P_k + W)C_1^{-1};$$

alors

$$C_h = (-1)^h(A_{h-1}^2 - B_{h-1}^2 f(X))$$

est de degré nul. De l'égalité

$$W_h = (P_h + E(W))C_h^{-1} + (W - E(W))C_h^{-1}$$

on déduit $W_{h+1} = C_h W_1$ puis $W_{h+2} = W_2 C_h^{-1}$, etc. Si h est impair on a $W_{2h} = C_h W_h = P_h + W, W_{2h+1} = W_1$ et donc $\ell = 2h$. Si h est pair $W_{2h} = W_h W_h^{-1}, W_{3h} = W_h C_h^{-2}, \ldots$, ce qui conduit à une infinité de quotients partiels distincts et le développement de W ne serait pas périodique contrairement l'hypothèse. Si ℓ est impair on peut prendre $\varphi = \Psi = \varepsilon = (A_{\ell-1} - B_{\ell-1}W)$

comme générateur de G et de G_1. Si maintenant ℓ est pair, notons $h = \ell/2$, considérons $\beta_h = A_{h-1} - B_{h-1}W$ et notons $C = N(\beta_h) = A_{h-1}^2 - B_{h-1}^2 f(X)$. Il faut ensuite discuter suivant C. Si C est de degré non nul, β_h n'est pas dans G et on peut prendre ε comme générateur de G modulo $\mathbf{Q}*$ et de G_1 au signe prs. Si $C = \pm c^2$ avec c rationel, β_h est dans G et $\beta_h c^{-1}$ est dans G_1. Dans les autres cas, β_h est dans G et $\beta_h^2 C^{-1}$ est dans G_1. En résumé on a :

PROPOSITION 3. — *Avec les notations précédentes, soit ℓ la longueur de la période du développement en fraction continue de $\sqrt{f}(X)$ et notons $\varepsilon = \beta_\ell = A_{\ell-1} - B_{\ell-1}W$.*

1. *Si ℓ est impair, ε est un générateur de G modulo $\mathbf{Q}^*$ et de G_1.*
2. *Si ℓ est pair, notons $h = \ell/2$ et $C = N(\beta_h)$; alors :*
   a. *Si $deg(C)$ est non nul, ε est un générateur de G modulo $\mathbf{Q}^*$ et de G_1.*
   b. *Si $deg(C) = 0$ avec $C = \pm c^2$ et c rationnel, β_h est un générateur de G modulo $\mathbf{Q}^*$ et $\beta_h c^{-1}$ est un générateur de G_1.*
   c. *Si $deg(C) = 0$ avec $\mid C \mid$ non carré dans $\mathbf{Q}$, β_h est un générateur de G modulo $\mathbf{Q}^*$ et $\varepsilon = \beta_\ell$ est un générateur de G_1.*

2 - Le résultat principal

2.2. Enoncé

THÉORÈME — *Soit $f(X) = a^2X^{2d} + \ldots$ un polynôme non carré dans $\mathbf{Z}[X]$ tel que le développement en fraction continue d'un élément $W = aX^d + \ldots$ vérifiant $W^2 = f(X)$, soit périodique. Notons $W = [u_0, \overline{u_1, \ldots, u_\ell}]$ et A_k/B_k les réduites du développement en fraction continue de W et considérons l'ensemble :*

$$E = \{n \in \mathbf{Z} \mid 2A_{\ell-1}(n) \notin \mathbf{Z}, f(n) \text{ positif non carré } \}.$$

Alors il existe une constante C ne dépendant que de f telle que pour tout $n \in E$, la longueur de la période du développement en fraction continue de $\sqrt{f(n)}$ soit minorée par $1 + 2[\log \sqrt{f(n)}/\log C]$ où $[z]$ désigne la partie entière de z.

L'idée de la démonstration est la suivante : on considère un générateur $\varphi(X)$ du groupe des unités G et on montre que pour $n \in E$ et pour $k = 1, 2, \ldots, k_0 = [\log \sqrt{f(n)}/\log C]$ on peut associer aux $\varphi^k(n)$ des meilleures approximations de $\sqrt{f(n)}$ non congrues modulo les unités. La longueur de la

période sera alors minorée par k_0. On précise la minoration en utilisant les propriétés particulières des meilleures approximations de la racine carrée d'un entier (positif non carré).

LEMME 1 — *Soit $\varphi = T + UW$ une unité fondamentale de G vérifiant $|\varphi|_1 < 1$. Il existe une partition des entiers rationnels $\mathbf{Z}$ en un nombre fini de classes F_j, $j = 1, \ldots, s$ et des polynômes $T^{(j)}, U^{(j)} \in \mathbf{Q}[X]$ à valeurs entières sur F_j tels que pour tout $j \in \{1, 2, \ldots, s\}$:*

a) le polynôme $T^{(j)}(n)$ est premier à $U^{(j)}(n)$ pour tout $n \in E_j$;

b) la série $\varphi_j = T^{(j)} + U^{(j)}W$ est équivalente à φ (i.e. $\varphi_j \varphi^{-1} \in \mathbf{Q}^*$) ;

c) En posant $C_j = N_{[\mathbf{Q}(X,W):\mathbf{Q}(X)]}(\varphi_j)$ on a $C_{j_1} \neq C_{j_2}$ dès que $j_1 \neq j_2$.

Démonstration. On se ramène à un représentant de φ tel que T et U soient à valeurs entières sur $\mathbf{Z}$ en multipliant éventuellement par un rationnel. Soit $C = T^2(X) - U^2(X)f(X)$. Le nombre C est un entier non nul et pour tout entier n le pgcd de $T(n)$ et de $U(n)$ divise C. On obtient le lemme en considérant les diviseurs d_j de C (en nombre fini) tels que

$$F_j = \{n \in \mathbf{Z} \text{ t.q pgcd } (T(n), U(n)) = d_j\}$$

soit non vide, en posant $(T^{(j)}, U^{(j)}) = (T, U)d_j^{-1}$ et en remarquant que $C = C_j d_j^2$.

On peut montrer que les classes F_j sont en fait des réunions de progressions arithmétiques. Elles sont donc infinies.

Dans la suite, nous omettons l'indice j pour alléger l'écriture.

LEMME 2 — *Soient (F, T, U, φ, C) l'une des classes du lemme 1 avec $\varphi(n) = T(n) + U(n)w$ $(w^2 = f(n))$ et $C = T^2(n) - U^2(n)f(n)$.*
Pour tout $n \in F \cap E$ il existe un nombre premier p divisant C tel que

$$2v_p(2T(n)) < v_p(C) \tag{3}$$

où v_p désigne la valuation p-adique. En notant $\varphi^k(X) = T_k(X) + U_k(X)W$ les puissances de φ on a :

$$v_p(f(n)) = v_p(T^2(n)) \tag{4}$$

$$v_p(T_k(n)) = (k-1)v_p(2T(n)) + v_p(T(n)) \quad \text{pour } k \geq 1 \tag{5}$$

$$v_p(U_k(n)) = (k-1)v_p(2T(n)) \quad \text{pour } k \geq 1\ . \tag{6}$$

Démonstration : D'après le lien mis en évidence dans la proposition 3 entre l'unité formelle génératrice de G et l'unité $\varepsilon = A_{\ell-1} - B_{\ell-1}W$ provenant de la fraction continue formelle, nous avons deux cas à considérer suivant que ε est ou non un générateur de G. Si ε engendre G on a $\varphi = a\varepsilon$ avec a entier et donc $2A_{\ell-1}(n) = \pm 2T(n)$ et $C = \pm a^2$. Mais pour $n \in E$, $2A_{\ell-1}(n)$ n'est entier et il existe donc p vérifiant (3). Dans l'autre cas $\varepsilon = \pm\varphi^2 C^{-1} = \pm(T^2 + U^2 f + 2TUW)C^{-1}$ et on a $2A_{\ell-1} = \pm 2(T^2 + U^2 f)C^{-1}$. Pour $n \in E$, le nombre $2(T^2(n) + U^2(n)f(n))C^{-1}$ n'est pas entier et en tenant compte de $T^2 - U^2 f = C$ on en déduit que $4T^2(n)C^{-1}$ n'est pas entier et il existe p tel que $2v_p(2T(n)) < v_p(C)$. On peut considérer que p est indépendant de n dans F. En effet, comme il n'y a qu'un nombre fini de p possibles, il suffit de partitionner F.

Pour la deuxième partie du lemme, on écrit :

$$T^2(n) - U^2(n)f(n) = C \ ; \tag{7}$$

d'après (3), on a $v_p(U^2(n)f(n)) = v_p(T^2(n) - C) = v_p(T^2(n))$ mais $T(n)$ est premier avec $U(n)$ et donc $v_p(f(n)) = v_p(T^2(n))$. Pour prouver (5) et (6) on remarque que les entiers $T_k(n)$ et $U_k(n)$ vérifient les relations de récurrence linéaire

$$\begin{cases} T_{k+2}(n) = & 2T_{k+1}(n)T(n) - CT_k(n) \\ U_{k+2}(n) = & 2U_{k+1}(n)T(n) - CU_k(n), \quad k \geq 1 \ . \end{cases} \tag{8}$$

En effet, à partir de $\varphi^{k+1} = \varphi^k \varphi$ on tire

$$\begin{pmatrix} T_{k+1} \\ U_{k+1} \end{pmatrix} = \begin{pmatrix} T & Uf \\ U & T \end{pmatrix} \begin{pmatrix} T_k \\ U_k \end{pmatrix}$$

et en écrivant que $M = \begin{pmatrix} T & Uf \\ U & T \end{pmatrix}$ est racine de son polynôme caractéristique $M^2 - 2TM - CI = 0$ on obtient la relation (8). On peut alors montrer (5) et (6) par récurrence. En tenant compte de (7) on a $T_1(n) = T(n)$ et $T_2(n) = T^2(n) + U^2(n)f(n) = 2T^2(n) - C$. Ce qui montre (5) pour $k = 1$ et $k = 2$. D'autre part, $U_1(n) = U(n)$ et on veut $v_p(U(n)) = 0$. Si $v_p(T(n)) > 0$ on a $v_p(U(n)) = 0$ car $T(n)$ et $U(n)$ sont des entiers premiers entre eux. Si maintenant $v_p(T(n)) = 0$ la relation (7)et $v_p(C) > 0$ entraîne $v_p(U(n)) = 0$. Puisque $U_2(n) = 2T(n)U(n)$ on a donc (6) pour $k = 1$ et $k = 2$. Pour $k > 2$ les relations (5) et (6) se vérifient facilement par récurrence à partir de (8).

LEMME 3 — *Avec les notations du lemme* 2, *considérons pour* $n \in F \cap E$ *le pgcd* $d_{k,n}$ *des entiers* $T_k(n), U_k(n)$ *et posons*

$$T_{k,n} = T_k(n)/d_{k,n}, U_{k,n} = U_k(n)/d_{k,n} \ .$$

Les entiers algébriques $\varphi_{k,n} = T_{k,n} + U_{k,n}w$ *du corps quadratique* $\mathbf{Q}(w)$ *ont des normes distinctes et sont donc non congrus deux à deux modulo les unités du corps pour tout* $k \geq 1$.

Démonstration : Soit $n \in F \cap E$ et p un nombre premier divisant la norme C de $\varphi(n)$ tel que (n,p) vérifie (3). Il résulte de (5) et (6) que $v_p(d_{k,n}) = (k-1)v_p(2T(n))$ et donc la norme C'_k de $\varphi_{k,n}$ vérifie

$$v_p(C'_k) = kv_p(C) - 2(k-1)v_p(2T(n)) .$$

$v_p(C'_{k_1}) = v_p(C'_{k_2})$ entraîne $(k_1 - k_2)(v_p(C) - 2v_p(2T(n))) = 0$ et donc $k_1 = k_2$. Ce qui prouve le lemme 3.

LEMME 4 — *Avec les notations des lemmes* 2 *et* 3, *soient* $\varphi = T + UW$ *et* n *un entier de* $F \cap E$. *Si* k *est un entier vérifiant* $w > |C^k|$, *la fraction* $T_{k,n}U_{k,n}^{-1} = T_k(n)U_k^{-1}(n)$ *est une réduite du développement en fraction continue de* W. *De plus, en notant* $\varphi'_{k,n} = T_{k,n} - U_{k,n}w$ *le conjugué de* $\varphi_{k,n}$, *le nombre* $\varphi'_{k,n}\varphi_{k_1,n}^{-1}$ *n'est pas une unité du corps* $K_n = \mathbf{Q}(w)$ *quels que soient les entiers* k, k_1 *et* n *dans* $F \cap E$.

Démonstration : La première partie résulte directement de la proposition 2 et du chapitre 10 de HUA [1982] affirmant que si t et u sont des entiers tels que $|t^2 - wu^2| < w$ alors t/u est une réduite de w. La seconde partie pour $k \neq k_1$ résulte du lemme 3. Soient maintenant $n \in F \cap E$ et p un premier divisant $C = N(\varphi(n))$ tel que (n,p) vérifie (3). Posons $2\alpha = 2v_p(2T(n))$ et supposons $p \neq 2$. Il résulte du lemme 2 que $p^{2\alpha}$ divise exactement $T^2(n)$ et $f(n)$ et que $p^{2\alpha+1}$ divise C. L'égalité $T^2(n)p^{-2\alpha} - f(n)p^{-2\alpha}U^2(n) = Cp^{-2\alpha}$ montre que $f(n)p^{-2\alpha}$ est un carré modulo p. Si on note $\mathbf{O}_{K_n}$ l'anneau des entiers du corps $K_n = \mathbf{Q}(w)$, l'idéal $(p\mathbf{O}_{K_n})$ est donc décomposé. On en déduit les égalités :

$$(T + Uw)\mathbf{O}_{K_n} = p^\alpha P^{\gamma-2\alpha}Q,$$
$$(T - Uw)\mathbf{O}_{K_n} = p^\alpha P'^{\gamma-2\alpha}Q',$$

où $\gamma = v_p(C)$, où P, P' sont les idéaux premiers distincts au-dessus de p et où Q est un idéal étranger à P.

Dans le cas $p = 2$, le lemme 2 entraîne que $2^{2(\alpha-1)}$ divise exactement $T^2(n)$ et $f(n)$. D'autre part, $v_2(C) > 2v_2(2T(n)) = 2\alpha$ et donc 8 divise $C2^{-2(\alpha-1)}$. L'égalité

$$T^2(n)2^{2-2\alpha} - f(n)2^{2-2\alpha}U^2(n) = C2^{2-2\alpha}$$

montre que l'idéal $2\mathbf{O}_{K_n}$ est encore décomposé. On en déduit

$$(T + Uw)\mathbf{O}_{K_n} = 2^{\alpha-1}P^{\gamma-2(\alpha-1)}Q,$$
$$(T - Uw)\mathbf{O}_{K_n} = 2^{\alpha-1}P'^{\gamma-2(\alpha-1)}Q';$$

Il en résulte que les idéaux $\varphi'_{k,n}\mathbf{O}_{K_n}$ et $\varphi_{k,n}\mathbf{O}_{K_n}$ sont distincts, ce qui équivaut à dire $\varphi'_{k,n}\varphi_{k,n}^{-1}$ n'est pas une unité de $\mathbf{O}_{K_n}$.

Démonstration du théorème : Considérons l'un des ensembles F_j définis au lemme 1. Posons $F = F_j, C = C_j$ et pour $n \in F \cap E$, considérons l'entier

$$k_0 = [\log\left(\sqrt{f(n)}\right) / \log c] \ .$$

Avec les notations des lemmes précédents, il résulte des lemmes 3 et 4 que les nombres

$$\varphi_{1,n}, \varphi_{2,n}, \ldots, \varphi_{k_0 n}, \varphi'_{1,n}, \varphi'_{2,n}, \ldots, \varphi'_{k_0 n} \tag{9}$$

sont des meilleures approximations de w et qu'elles sont non congrues deux à deux modulo les unités de l'anneau $\mathbf{O}_{K_n}$, on a donc $\ell p(w) \geq 2k_0$. Si $\ell p(w)$ est impair, on en déduit immédiatement $\ell p(w) \geq 2k + 1$. Si $\ell p(w)$ est pair, on va montrer que : $\ell p(w) \geq 2k_0 + 2$. En effet, la proposition 2 nous dit que la meilleure approximation $\zeta_h = |p_{h-1} - q_{h-1}w|$ avec $h = \dfrac{\ell p(w)}{2}$, qui se trouve au milieu de la période, vérifie $\zeta_h = \pm\zeta'_h\varepsilon$ (ε unité de $\mathbf{O}_{K_n}$). Or, d'après le lemme 4, les meilleures approximations $(\varphi_{i,n})_{1\leq i\leq k_0}$ $(\varphi'_{i,n})_{1\leq i\leq k_0}$ que l'on considère ne peuvent être associées modulo les unités de $\mathbf{O}_{K_n}$ à ζ_h. Alors $\ell p(w) \geq 2k_0 + 1$ et comme $\ell p(w)$ est pair on a $\ell p(w) \geq 2k_0 + 2$.

2.2. Un exemple

Dans le cas $f(X) = a^2X^2 + bX + c$ le développement en fraction continue formelle est toujours périodique de longueur 1 ou 2. On a :

$$\sqrt{f(X)} = \left[aX + \frac{b}{2a}\ , \overline{\frac{8a^3X + 4ab}{4a^2c - b^2}, 2aX + \frac{b}{a}}\right]$$

L'exemple $F(X) = X^2 + 9X + 16$ avec $n = 17^m$ donné par LOUBOUTIN [1989] montre que la minoration obtenue est optimale puisque $\ell p(\sqrt{f(17^m)}) = 1 + 2m$ et que $m = k_0$.

Nous donnons ci-dessous un exemple explicite, avec $\deg(f) = 4$, dans lequel la longueur du développement formel est $\ell = 10$. Si

$$f(X) = X^4 + 4X^3 - 6X^2 + 4X + 1, \ \textit{et}\ W(X) = X^2 + 2X - 5 + \ldots,$$

on obtient facilement le développement en écrivant les quotients complets W_k sous la forme $(B_k + W)C_k^{-1}$ car on a les formules de récurrence classiques :

$$u_k(X) = E(B_k + W)C_k^{-1}, \ B_{k+1} = u_kC_k - B_k, \ C_{k+1} = (f(X) - B_{k+1}^2)C_k^{-1}.$$

La suite des quotients partiels est :

$u_0(X) = X^2 + 2X - 5$, $u_1(X) = (X+3)/12$, $u_2(X) = -6(X+2)$,
$u_3(X) = (X+2)/18$, $u_4(X) = -9(X+3)$, $u_5(X) = -(X^2+2X-5)/54$,
$u_6 = u_4 \ldots \quad u_{10}(X) = 2u_0(X)$.

La suite des normes de la suite des meilleures approximations $\beta_k = A_{k-1} - B_{k-1}W$, $k \geq 1$, est :

$N(\beta_0) = 1$, $N(\beta_1) = -24(X-1)$, $N(\beta_2) = -X/3$, $N(\beta_3) = -36X$,
$N(\beta_4) = -2(X-1)/9$, $N(\beta_5) = 108$, $N(\beta_6) = N(\beta_4), \ldots, N(\beta_10) = 1$.

L'élément suivant :

$$\varphi(X) = 4\beta_5 = (X^6 + 12X^5 + 45X^4 - 33X^2 - 43) - (X^4 + 10X^3 + 30X^2 + 22X - 11)W$$

est un générateur de G ; nous posons $\varphi(X) = T(X) + U(X)W$.

Déterminons l'ensemble E : Puisque $C = N(\varphi) = 16.108$ n'est pas un carré, on a d'après le paragraphe I.3 :

$$\varepsilon = \beta_{10} = \beta_5^2 C^{-1} = A_9 - B_9 W$$

et donc $2A_9(n) = \pm 2(T^2 + U^2 f)C^{-1}$.

Pour tout entier n, $2A_9(n)$ n'est jamais entier car $n \equiv 0$ ou $1 (\mathrm{mod}\ 3)$ implique $T^2 + U^2 f \equiv 2$ ou $1 \pmod 3$ et que $n \equiv 2 \pmod 3$ implique $T^2 + U^2 f$ divisible par 9 mais non par 27. D'autre part, $f(0)$ et $f(1)$ sont carrés et $f(n)$ est négatif pour $n = -1, -2,$
$-3, -4, -5$. On a donc

$$E = \mathbf{Z} \setminus \{0, 1, -1, -2, -3, -4, -5\}.$$

En explicitant les résultats du lemme 1 pour ce générateur φ et en utilisant les notations de ce lemme on a la partition suivante de E :

$$F_1 = \{n \in E \mid n \equiv 0 \bmod 2 \text{ et } n \equiv 0 \text{ ou } 1 \bmod 3\}$$
avec $T^{(1)} = T$, $U^{(1)} = U$, $C_1 = 2^6.3^3$

$$F_2 = \{n \in E \mid n \equiv 0 \bmod 2 \text{ et } n \equiv 2 \bmod 3\}$$
avec $T^{(2)} = T/3$, $U^{(2)} = U/3$, $C_2 = 2^6.3$

$$F_3 = \{n \in E \mid n \equiv 1 \bmod 2 \text{ et } n \equiv 0 \text{ ou } 1 \bmod 3\}$$
avec $T^{(3)} = T/2$, $U^{(2)} = U/2$, $C_3 = 2^4.3^3$

$$F_4 = \{n \in E \mid n \equiv 0 \bmod 2 \text{ et } n \equiv 2 \bmod 3\}$$
avec $T^{(4)} = T/6$, $U^{(4)} = U/6$, $C_4 = 2^4.3$

Le théorème donne la minoration :

$$\ell p(\sqrt{f(n)}) \geq 1 + 2[\log \sqrt{f(n)} / \log C],$$

avec $C = \max C_j = 2^6 3^3$ mais la démonstration permet de l'améliorer suivant que n appartient à F_2, F_3 ou à F_4 en remplaçant C par C_2, C_3 ou C_4.

REFERENCES

[1] COHN J.H.E. *The length of the period of the simple continued fraction of* $d^{1/2}$. Pacific J.Math.Vol. 71 n° 1, 1977,pp.31-32.

[2] DUBOIS E. *Approximations diophantiennes simultanées de nombres algébriques.* Thèse, Paris VI, 1980.

[3] HELLEGOUARCH Y., MC QUILLAN D.L., PAYSANT-LE ROUX R. *Unités de certains sous anneaux de corps de fonctions algébriques.* Acta Arith. (1987), p. 9-47.

[4] HUA L.K. *Introduction to number theory.* Springer-Verlag, 1982.

[5] LOUBOUTIN S. *Une version effective d'un théorème de A. Schinzel sur les longueurs des périodes de certains développements en fractions continues.* C.R.A.S. Paris t.308, série I, p. 511-513, 1987.

[6] NEUBRAND M. *Einheiten in algebraischen Funktionen und Zahlhörpen.* J. Reine Angew. Math. 303/304 (1978) p.170-204.

[7] PAYSANT-LE ROUX R. *Calibre d'un corps arithmétique et unités.* Thèse, Caen 1987.

[8] PAYSANT-LE ROUX R. et DUBOIS E. *Meilleures approximations formelles ou réelles.* Colloque de théorie des Nombres. Alger 1989.

[9] SCHINZEL A. *On some problems of the arithmetical theory of continued fractions.* Acta Arith. 6 (1961) p.393-413.

[10] SCHINZEL A. *On some problems of the arithmetical theory of continued fractions.* Acta Arith. 7 (1962) p.287-298.

[11] SCHMIDT H. *Zur Approximation und Kettenbruchentwicklung quadratischer Zahlen.* Math.Z. (1948) p.168-192.

DUBOIS E.
ISMA & Département de Mathématiques
Université de Caen
14032 CAEN

et

PAYSANT-LE ROUX R.
Département de Mathématiques
Université de Caen
14032 CAEN