ACTA ARITHMETICA
LXVII.1 (1994)

Minoration de la période du développement de $\sqrt{a^2n^2+bn+c}$ en fraction continue

par

Ahmed Farhane (Caen)

I. Introduction. Pour $(a,b,c)\in\mathbb{N}^*\times\mathbb{Z}\times\mathbb{Z}$, nous considérons le polynôme $f(X)=a^2X^2+bX+c$, de discriminant $d=b^2-4a^2c$ supposé non nul et l'ensemble $\widetilde{\mathbb{Z}}$ des entiers n tels que $f(n)$ soit positif non carré. Nous noterons $p(\alpha)$ la longueur de la période du développement en fraction continue du nombre quadratique réel α.

A. Schinzel [5] a déterminé l'ensemble E des entiers rationnels n vérifiant les propriétés suivantes :

(1) La longueur de la période du développement en fraction continue de $\sqrt{f(n)}$ est bornée indépendamment de n lorsque n appartient à $\widetilde{\mathbb{Z}}\setminus E$.

(2) La longueur de la période du développement en fraction continue de $\sqrt{f(n)}$ tend vers l'infini avec n lorsque n appartient à E.

S. Louboutin [4] a montré que pour tout n élément de E

$$p(\sqrt{f(n)})\ge 2\left[\frac{\log\sqrt{f(n)}}{\log|\beta|}\right]+1$$

avec $\beta=(b^2-4a^2c)/\mathrm{pgcd}(2a,b)^2$ et où $[x]$ désigne la partie entière de x.

E. Dubois et R. Paysant Le Roux [1] ont donné une minoration effective lorsque $f(X)=a^2X^{2d}+\ldots+a_{2d}$ avec $a,a_1,\ldots,a_{2d}$ entiers.

Lorsque $f(X)=X^2+h$, avec h dans $\mathbb{N}^*$, l'auteur [2] a prouvé que pour tout n dans $\widetilde{\mathbb{Z}}$ tel que h ne divise pas $4n^2$ (caractérisation de E) on a

$$p(\sqrt{f(n)})\ge 3\left[\frac{\log\sqrt{f(n)}}{\log h}\right].$$

Nous améliorons le résultat de [4] dans le cas où $d<0$ en prouvant :

II. Résultat principal

Théorème. *Soit $f(X)=a^2X^2+bX+c$ un polynôme de discriminant $d=b^2-4a^2c$ strictement négatif. Soit n dans $\widetilde{\mathbb{Z}}$ tel que d ne divise pas*

$4(2a^2n+b)^2$. *Alors la longueur de la période du développement en fraction continue de* $\sqrt{f(n)}$ *vérifie*

$$p(\sqrt{f(n)}) \geq \min(3M_1, 3M-2) \geq 3M - 3\left[\frac{\log u}{\log|\beta|}\right] - 3$$

où

$$g = \mathrm{pgcd}(2a, b), \qquad \beta = (b^2 - 4a^2c)g^{-2}, \qquad u = 2ag^{-1},$$
$$M = \left[\frac{\log\sqrt{f(n)}}{\log|\beta|}\right], \qquad M_1 = \left[\frac{\log\sqrt{f(n)} - \log u}{\log|\beta|}\right].$$

Preuve. Notons $N(\alpha)$ la norme dans le corps quadratique $\mathbb{Q}(\sqrt{f(n)})$ d'un élément α de ce corps, $v := bg^{-1}$, $a_1 := aun + v = (2a^2n+b)g^{-1}$, $b_1 := u = 2ag^{-1}$ et considérons $x = a_1 + b_1\sqrt{f(n)}$. La norme de x est égale à β et en définissant, pour $k \geq 1$, les entiers a_k et b_k par $x^k = a_k + b_k\sqrt{f(n)}$, nous avons $a_k^2 - b_k^2 f(n) = \beta^k$ ainsi que les relations de récurrence

$$a_{k+1} = a_1a_k + b_1b_kf(n), \qquad b_{k+1} = a_kb_1 + a_1b_k. \tag{1}$$

Nous utiliserons les notations classiques du développement en fraction continue : $\sqrt{f(n)} = [t_0, t_1, \ldots]$,

$$\alpha_i = [t_i, t_{i+1}, \ldots], \qquad p_i/q_i = [t_0, \ldots, t_i], \qquad \varphi_i = p_i + q_i\sqrt{f(n)}. \tag{2}$$

Rappelons que si l est la longueur de la période minimale, alors φ_{l-1} est l'unité fondamentale supérieure à 1 de $\mathbb{Z}[\sqrt{f(n)}]$.

LEMME 1. *Sous les hypothèses et les notations du théorème il existe, pour tout entier rationnel k vérifiant $1 \leq k \leq M$, un unique entier rationnel, i_k, tel que le rationnel a_k/b_k soit la réduite p_{i_k}/q_{i_k} de $\sqrt{f(n)}$, et les entiers $N_k = |p_{i_k}^2 - f(n)q_{i_k}^2|$ sont deux à deux distincts.*

Preuve. Notons d_k le plus grand diviseur commun de a_k et b_k et posons $A_k = a_k/d_k$ et $B_k = b_k/d_k$. Nous avons

$$|A_k^2 - B_k^2f(n)| = |\beta|^k/d_k^2 < \sqrt{f(n)}, \qquad \text{pour } 1 \leq k \leq M.$$

Il en résulte (voir [3], chapitre 10) l'existence d'un indice i_k tel que $A_k = p_{i_k}$ et $B_k = q_{i_k}$.

Puisque par hypothèse d ne divise pas $4(2a^2n+b)^2$, il existe un nombre premier p tel que la valuation p-adique, v_p, vérifie

$$v_p(d) > 2v_p(2(2a^2n+b)), \qquad \text{soit} \quad v_p(\beta) > 2v_p(2a_1). \tag{3}$$

A partir des relations (1) et (3) on obtient facilement (voir [2], lemme 2), pour $k \geq 1$,

$$\begin{gathered} v_p(a_k) = (k-1)v_p(2a_1) + v_p(a_1), \qquad v_p(b_k) = (k-1)v_p(2a_1), \\ v_p(d_k) = (k-1)v_p(2a_1). \end{gathered} \tag{4}$$

Par suite $v_p(N_k) = kv_p(\beta) - 2v_p(d_k) = k(v_p(\beta) - 2v_p(2a_1)) + 2v_p(2a_1)$ et les $|N_k|$ sont deux à deux distincts. ■

LEMME 2. *Avec les notations précédentes nous avons, pour tout entier k compris entre* 1 *et* M, $i_k \not\equiv k \bmod 2$ *et* $i_k \geq 3(k-1) + i_1$.

Preuve. Puisque $\beta < 0$ (car $d < 0$) et, pour tout k, $1 \leq k \leq M$, $N(\varphi_{i_k}) = \beta^k/d_k^2$, k et i_k et par suite i_k et i_{k+1} sont de parité contraire.

Soit k un entier compris entre 1 et $M-1$ et montrons que $i_{k+1} - i_k \geq 3$. Puisque $x^k = d_k\varphi_{i_k}$ nous avons $d_{k+1}|\varphi'_{i_{k+1}}| = d_k|\varphi'_{i_k}x'|$ si y' désigne le conjugué algébrique du nombre quadratique y.

Comme $|x'| < 1$ et d_k divise d_{k+1} nous avons $|\varphi'_{i_{k+1}}| < |\varphi'_{i_k}|$ et donc $i_{k+1} - i_k \geq 1$.

S'il existe t tel que $1 \leq t \leq M-1$ et $i_{t+1} - i_t = 1$ nous aurons

$$a_t b_{t+1} - a_{t+1} b_t = (p_{i_t} q_{1+i_t} - p_{1+i_t} q_{i_t}) d_t d_{t+1} = (-1)^{1+i_t} d_t d_{t+1}$$

et puis, en utilisant (1), $b_1(a_t^2 - b_t^2 f(n)) = b_1\beta^t = (-1)^{1+i_t} d_t d_{t+1}$.

Nous obtenons une contradiction avec (3) et (4) puisque

$$v_p(b_1\beta^t) > 2tv_p(2a_1) \geq (2t-1)v_p(2a_1) = v_p(d_t d_{t+1}).$$

En conséquence, $i_{k+1} - i_k \geq 3$ pour $k = 1, \ldots, M-1$ et $i_k \geq 3(k-1) + i_1$ pour $1 \leq k \leq M$. ■

LEMME 3. *Soient $\varepsilon_0 > 1$ l'unité fondamentale de $\mathbb{Z}[\sqrt{f(n)}]$ et*

$$M_1 = \left[\frac{\log\sqrt{f(n)} - \log u}{\log|\beta|}\right].$$

Alors nous avons $\varphi_{i_k} < \varepsilon_0$ pour $1 \leq k \leq M_1$.

Preuve. Si $i_1 = 0$ le lemme 6 de [2] montre que $\varphi_{i_1} < \varphi_{i_2} < \ldots < \varphi_{i_M} < \varepsilon_0$.

Considérons maintenant le cas $i_1 > 0$. Si $\varphi_{i_M} < \varepsilon_0$ le lemme résulte de $M \geq M_1$. Sinon soit s minimal tel que $\varphi_{i_s} \geq \varepsilon_0$. Nous devons montrer $s > M_1$.

Comme le groupe $\mathcal{U}$ des unités de $\mathbb{Z}[\sqrt{f(n)}]$ opère sur l'ensemble $\mathcal{E} = \{\varphi_k : k \geq 0\}$ des meilleures approximations (≥ 1) de $\sqrt{f(n)}$, il existe un indice $j \geq 0$ tel que $\varphi_{i_s} = \varepsilon_0\varphi_j$. Montrons que $j < i_1$.

Sinon, $j \geq i_1$ et $d_s^{-1}x^s = \varphi_{i_s} = \varepsilon_0\varphi_j \geq \varepsilon_0\varphi_{i_1} = \varepsilon_0 x$. Pour $s = 1$ on a une contradiction avec $d_1 = 1$ et $\varepsilon_0 > 1$. Pour $s > 1$ on a une contradiction avec le choix minimal de s puisque

$$\varphi_{i_{s-1}} \geq d_{s-1}d_s^{-1}\varphi_{i_{s-1}} = d_s^{-1}x^{s-1} \geq \varepsilon_0.$$

On a donc $j < i_1$ et par suite

$$q_{j+1} \leq q_{i_1} = u. \tag{5}$$

Par ailleurs, des propriétés des fractions continues :

$$|\varphi'_j| = |q_j\alpha_{j+1} + q_{j-1}|^{-1}, \qquad \alpha_{j+1} < 1 + t_{j+1},\ q_{j+1} = a_{j+1}q_j + q_{j-1}$$

il résulte que

$$|\varphi'_j| > (q_{j+1} + q_j)^{-1}. \tag{6}$$

Or $|\varphi_j\varphi'_j| = |N(\varphi_{i_s})| = |\beta|^s d_s^{-2}$ et donc

$$(q_{j+1} + q_j)|\beta|^s > |\varphi'_j|^{-1}|\beta|^s = d_s^2\varphi_j \ge \varphi_j = p_j + q_j\sqrt{f(n)}. \tag{7}$$

Puisque $s \le M$ on a $q_j|\beta|^s \le q_j[\sqrt{f(n)}] \le [q_j\sqrt{f(n)}] \le p_j$. En composant avec (5), (6) et (7) on obtient

$$u|\beta|^s \ge q_{j+1}|\beta|^s > \varphi_j - q_j|\beta|^s > p_j + q_j\sqrt{f(n)} - p_j \ge \sqrt{f(n)}$$

et donc $s > M_1$, ce qui prouve le lemme 3. ■

Preuve du théorème. Notons l la longueur de la période du développement en fraction continue de $\sqrt{f(n)}$. On sait alors que $\varepsilon_0 = \varphi_{l-1}$. Si $\varepsilon_0 > \varphi_{i_M}$ on a $l-1 \ge i_M$ et d'après le lemme 2, $l \ge 3(M-1)+i_1+1 \ge 3M-2$.

Sinon soit s minimal tel que $\varphi_{i_s} \ge \varepsilon_0$ avec $1 \le s \le M$. On a alors $l-1 \ge i_{s-1}$. Par la preuve du lemme 3 on a $i_1 \ne 0$. Avec le lemme 2 on obtient

$$l \ge 3(s-2) + i_1 + 1 \ge 3(M_1 - 1) + 2 + 1 = 3M_1.$$

Lorsque $\varphi_{i_M} \ge \varepsilon_0$ on a $l \ge 3M_1$ et lorsque $\varphi_{i_M} < \varepsilon_0$ on a $l \ge 3M$ si $i_1 \ne 0$ et $l \ge 3M - 2$ sinon. Par ailleurs, en remarquant que

$$M_1 = \left[\frac{\log\sqrt{f(n)} - \log u}{\log|\beta|}\right] \ge M - \left[\frac{\log u}{\log|\beta|}\right] - 1,$$

on obtient le théorème. ■

Corollaire. *Pour $f(X) = a^2X^2 + bX + c$ de discriminant $d = b^2 - 4a^2c$ supposé non nul on a :*

$$\liminf_{\substack{n\to\infty\\ n\in E}} \frac{p(\sqrt{f(n)})}{M} \ge \begin{cases} 2 & \text{si } d > 0,\\ 3 & \text{si } d < 0\end{cases}$$

où E est l'ensemble des entiers n tels que d ne divise pas $4(2a^2n+b)^2$ et $f(n)$ positif non carré parfait.

Preuve. Le cas $d > 0$ est traité dans [4] et le cas $d < 0$ résulte immédiatement de notre théorème. ■

Remarque. Pour $f(X) = X^2 + X + 1$ nous avons $d = -3$, $u = 2$, $\beta = -3$, $[\log u/\log|\beta|] = 0$ mais $M_1 = M - 1$ (c'est élémentaire à vérifier).

On peut aussi vérifier que $E = \{n : n \ne 0,\ n \ne -1 \text{ et } n \not\equiv 1 \bmod 3\}$ et que $i_1 \ne 0$. Notre énoncé montre que $p(\sqrt{f(n)}) \ge 3M - 3$.

Pour montrer l'optimalité du facteur 3 nous avons déterminé la sous-famille explicite suivante. Pour $n = 3^m$ ($m \geq 1$) nous obtenons, en notant α_i et a_i les quotients complets et incomplets de $\alpha_0 = \sqrt{f(3^m)}$, pour $0 \leq j \leq m$,

$$\alpha_{3j} = \frac{3^m - 1 + \alpha_0}{3^j}, \qquad a_{3j} = 2 \cdot 3^{m-j} - 1,$$

$$\alpha_{3j+1} = \frac{3^m - 3^j + 1 + \alpha_0}{2 \cdot 3^m - 3^{m-j} - 3^j + 2}, \qquad a_{3j+1} = 1,$$

$$\alpha_{3j+2} = \frac{3^m - 3^{m-j} + 1 + \alpha_0}{3^{m-j}},$$

$$a_{3j+2} = \begin{cases} 2 \cdot 3^j - 1 & \text{si } 0 \leq j \leq m-1, \\ 2 \cdot 3^m & \text{si } j = m, \end{cases}$$

ce qui donne $\alpha_{3m+2} = 3^m + \alpha_0, a_{3m+2} = 2 \cdot 3^m$ et donc

$$p(\sqrt{f(3^m)}) = 3m + 2 = 3M + 2 \quad \text{et} \quad \liminf_{\substack{n \to \infty \\ n \in E}} \frac{p(\sqrt{f(n)})}{M} = 3.$$

Pour compléter cet exemple il est facile de vérifier que pour $n \equiv 1 \bmod 3$, $p(\sqrt{f(n)}) = 6$. ∎

Références

[1] E. Dubois et R. Paysant Le Roux, *Sur la longueur du développement en fraction continue de* $\sqrt{f(n)}$, Astérisque 198-199-200 (1991), 107–109.

[2] A. Farhane, *Sur la longueur du développement de* $\sqrt{n^2+h}$ *en fraction continue*, C. R. Acad. Sci. Paris Sér. I 316 (1993), 537–540.

[3] L. K. Hua, *Introduction to Number Theory*, Springer, 1982.

[4] S. Louboutin, *Une version effective d'un théorème de A. Schinzel sur longueurs des périodes de certains développements en fractions continues*, C. R. Acad. Sci. Paris Sér. I 308 (1989), 511–513.

[5] A. Schinzel, *On some problems of the arithmetical theory of continued fractions*, Acta Arith. 6 (1961), 393–413.

UNIVERSITÉ DE CAEN, U.F.R. SCIENCES
DÉPARTEMENT DE MATHÉMATIQUES
ESPLANADE DE LA PAIX
14032 CAEN CEDEX, FRANCE

Reçu le 19.7.1993
et révisé le 1.12.1993 (2465)