ACTA ARITHMETICA
LXXIV.2 (1996)

Sur la longueur de la fraction continue de α^n

par

Guillaume Grisel (Caen)

I. Introduction. Soit x un nombre rationnel. Notons $d(x)$ le nombre de termes de la fraction continue de longueur paire de x. Y. Pourchet dans une lettre à M. Mendès France d'une part et G. Choquet dans une série de comptes rendus à l'Académie des Sciences [2] d'autre part, ont démontré que si x n'est ni un entier ni l'inverse d'un entier, alors $\sup d(x^n) = \infty$. La démonstration de Y. Pourchet, non publiée, est résumée dans l'article de A. J. van der Poorten [7].

Nous nous intéressons à un problème similaire portant sur les nombres quadratiques réels. Si α est un nombre quadratique réel, son développement en fraction continue est périodique, de longueur de période primitive $l(\alpha)$. En Novembre 1992, lors d'un congrés à Tokyo, M. Mendès France posait la question suivante ([5], problème n°6) : pour tout nombre quadratique réel α, est-il vrai que

$$\limsup_{n\to\infty} l(\alpha^n) = \infty?$$

Une première réponse, à mettre en parallèle avec le cas des entiers dans le problème sur les nombres rationnels, peut déjà être faite : R. Paysant-Le Roux et E. Dubois remarquent dans [6] que si α est une unité quadratique, alors $l(\alpha) \leq 2$. La question doit donc être reformulée en ne considérant plus que les nombres quadratiques réels qui ne sont pas des unités quadratiques. L'existence du nombre $l(\alpha^n)$ pour tout $n \geq 1$ est équivalente à $\alpha^2 \notin \mathbb{Q}$, il est donc bien entendu que si ce n'est pas le cas, n désignera un nombre impair. Nous montrons que, pour une large classe de nombres réels quadratiques, la réponse à la question de M. Mendès France est non seulement positive mais que $l(\alpha^n)$ tend vers l'infini avec n et ceci de manière explicite. Nous établissons :

Théorème. *Soit* $\alpha = (a+b\sqrt{d})/c$, $a \in \mathbb{Z}$, $b \in \mathbb{Z}^*$, $c \in \mathbb{N}^*$, $\operatorname{pgcd}(a,b,c) = 1$ *et* $d \geq 2$ *sans facteur carré. Posons* $f_2 = \operatorname{pgcd}(a^2+b^2d, 2ab, c^2)$, $c_2 = c^2/f_2$ *et* $N_2 = (a^2-b^2d)^2/f_2^2$. *Supposons que* α *vérifie l'une des conditions suivantes* :

(i) $N_2 \not\equiv 0 \pmod{c_2}$,
(ii) $\mathrm{pgcd}(a,b) > 1$,
(iii) $\mathrm{pgcd}(a,d) > 1$,
(iv) $a^2 - b^2 d$ *pair et* c *impair.*

Alors il existe une constante effectivement calculable K *strictement positive et indépendante de* n*, telle que pour tout* $n \geq 2$,

$$l(\alpha^n) > K\frac{2^n}{n}.$$

La preuve de ce théorème consiste en la détermination, pour tout $n \geq 1$, d'un générateur de O_n l'anneau des stabilisateurs du module $\mathbb{Z} + \mathbb{Z}\alpha^n$, en fonction de conditions sur α. Plus précisément, il s'agit de faire apparaître des grandes puissances d'entiers dans le conducteur de O_n. Deux minorations, l'une de $l(\alpha^n)$ (proposition 5) due à E. P. Golubeva [4] et faisant intervenir l'unité fondamentale et le discriminant de O_n, et l'autre de l'indice du groupe des unités de O_n dans le groupe des unités du corps $\mathbb{Q}(\alpha)$ (proposition 6), reposant sur un lemme de H. Cohen [3], sont à la base de cette démonstration.

II. La forme canonique de α^n. Considérons $\alpha = (a + b\sqrt{d})/c$, où $a \in \mathbb{Z}$, $b \in \mathbb{Z}^*$, $c \in \mathbb{N}^*$, $\mathrm{pgcd}(a,b,c) = 1$ et $d \geq 2$ sans facteur carré, et posons $N = a^2 - b^2 d$. Notons, pour tout $n \geq 1$,

$$\alpha^n = \left(\frac{a + b\sqrt{d}}{c}\right)^n = \frac{a_n + b_n\sqrt{d}}{c_n}, \quad \text{avec } \mathrm{pgcd}(a_n, b_n, c_n) = 1 \text{ et } c_n > 0.$$

Définissons, pour tout $n \geq 1$, les entiers a'_n et b'_n par $(a+b\sqrt{d})^n = a'_n + b'_n\sqrt{d}$, et posons $f_n = \mathrm{pgcd}(a'_n, b'_n, c^n)$.

Proposition 1. *Pour tout* $n \geq 1$, $f_n = 2^{l'_n}(\mathrm{pgcd}(a,d,c))^{l_n}$, *avec* :

(i) $l_n = [n/2]$;
(ii) *Si l'un des nombres* $a^2 - b^2 d$ *ou* c *est impair, alors* $l'_n = 0$;
(iii) *Si les deux nombres* $a^2 - b^2 d$ *et* c *sont tous les deux pairs, alors*

$$l'_n = \begin{cases} 0 & \text{si } d \equiv 2 \pmod 4, \\ [n/2] & \text{si } d \equiv 3 \pmod 4, \\ n-1 & \text{si } d \equiv 1 \pmod 8, \\ n-1 & \text{si } d \equiv 5 \pmod 8 \text{ et si } 3 \text{ ne divise pas } n, \\ n & \text{si } d \equiv 5 \pmod 8 \text{ et si } 3 \text{ divise } n. \end{cases}$$

Démonstration. Le cas $a = 0$ est trivial : comme $\mathrm{pgcd}(b,c) = 1$ et d est sans facteur carré on a alors $f_{2n+1} = \mathrm{pgcd}(b^{2n+1}d^n, c^{2n+1}) = (\mathrm{pgcd}(c,d))^n$. Nous supposons donc $a \neq 0$ dans la suite de la démonstration.

Posons, pour tout $n \geq 1$, $\delta_n = \mathrm{pgcd}(a'_n, b'_n)$. Nous explicitons dans un premier temps les diviseurs premiers de δ_n, puis nous déterminons les puis-

sances avec lesquelles ils divisent δ_n. Nous en déduisons alors f_n. Les facteurs communs à a et b divisent δ_n, mais ne divisent pas f_n car $\mathrm{pgcd}(a,b,c)=1$. On peut donc supposer, pour l'étude de f_n, $\delta_1=\mathrm{pgcd}(a,b)=1$.

LEMME 1. *Supposons* $\delta_1=1$. *Pour tout* $n\geq 1$, *si* p *premier divise* δ_n *alors* $p=2$ *ou* p *divise* $\mathrm{pgcd}(a,d)$.

Démonstration. On a, pour tout $n\geq 1$,

$$a'_{n+1}=a'_n a+b'_n bd,\qquad b'_{n+1}=a'_n b+b'_n a. \tag{1}$$

Donc si p divise δ_n, il divise aussi δ_{n+1}. Alors quitte à changer n en $n+1$, on peut supposer n pair. En posant $n=2m$, on a alors

$$a'_n=a'^2_m+b'^2_m d,\qquad b'_n=2a'_m b'_m.$$

On en déduit que ou $p=2$, ou p divise δ_m, ou p divise $\mathrm{pgcd}(a'_m,d)$.

Si $m=1$, comme on a supposé $\mathrm{pgcd}(a,b)=1$, alors $p=2$ ou p divise $\mathrm{pgcd}(a'_1,d)=\mathrm{pgcd}(a,d)$.

Si $m>1$, alors ou $p=2$, et c'est fini, ou p divise $\mathrm{pgcd}(a'_m,d)$, ou p divise δ_m.

(a) Si p divise $\mathrm{pgcd}(a'_m,d)$, alors par (1), il divise $\mathrm{pgcd}(a,d)$ ou il divise $\mathrm{pgcd}(a'_{m-1},d)$ et on obtient par récurrence descendante jusqu'à $m=1$, p divise $\mathrm{pgcd}(a,d)$.

(b) Si p divise δ_m, alors soit $[(m+1)/2]=1$, soit $[(m+1)/2]>1$.

Dans ce second cas, on a alors ou $p=2$ et c'est fini, ou p divise $\mathrm{pgcd}(a'_{[(m+1)/2]},d)$ et on effectue (a), ou p divise $\delta_{[(m+1)/2]}$ et on recommence (b).

On s'arrête donc en entrant dans (a), ou lorsque $[(m+1)/2]=1$. Il suit donc $p=2$ ou p divise $\mathrm{pgcd}(a,d)$. ∎

Comme d est sans facteur carré, on peut écrire $\mathrm{pgcd}(a,d,c)=p_1\dots p_s$ où les p_i sont premiers et tous distincts. Or il est facile de voir, en développant $(a+b\sqrt{d})^n$ par la formule du binôme, que pour tout $n\geq 2$, le $\mathrm{pgcd}(a,d,c)$ divise δ_n, et que par conséquent il divise f_n. On en déduit donc par le lemme 1,

$$f_n=2^{l'_n}p_1^{l_{1,n}}\dots p_s^{l_{s,n}},\qquad l_{i,n}\geq 1.$$

• Montrons le point (i) de la proposition 1. Pour tout i compris entre 1 et s, comme par hypothèse $\mathrm{pgcd}(a,b,c)=1$, p_i ne divise pas b, et puisque d est sans facteur carré, p_i divise exactement $N=a^2-b^2d$. D'où, si $v_{p_i}(x)$ désigne la valuation p_i-adique de l'entier x, $v_{p_i}(N^n)=v_{p_i}(a'^2_n-b'^2_n d)=n$. On a alors :

• soit $v_{p_i}(a'_n)\leq v_{p_i}(b'_n)$, et alors $v_{p_i}(N^n)=v_{p_i}(a'^2_n)$, d'où n est pair et $v_{p_i}(\delta_n)=v_{p_i}(a'_n)=n/2$;

• soit $v_{p_i}(b'_n)<v_{p_i}(a'_n)$, et alors $v_{p_i}(N^n)=v_{p_i}(b'^2_n d)=n$; il suit que n est impair et $v_{p_i}(\delta_n)=v_{p_i}(b'_n)=(n-1)/2$.

Comme $v_{p_i}(c^n) \geq n$, on obtient donc $l_{i,n} = l_n = [n/2]$.

• Le point (ii) de la proposition 1 est immédiat.

On déduit le point (iii) de la proposition 1 à partir de la valuation 2-adique de δ_n, qui fait l'objet du lemme suivant :

LEMME 2. *Si* $v_2(\delta_1) = 0$ *et* $N = a^2 - b^2 d$ *pair, alors pour tout* $n \geq 1$,

$$v_2(\delta_n) = \begin{cases} [n/2] & \text{si } d \not\equiv 1 \pmod 4, \\ n-1 & \text{si } d \equiv 1 \pmod 8, \\ n-1 & \text{si } d \equiv 5 \pmod 8 \text{ et si } 3 \text{ ne divise pas } n, \\ n & \text{si } d \equiv 5 \pmod 8 \text{ et si } 3 \text{ divise } n. \end{cases}$$

Démonstration. Si $d \equiv 2 \pmod 4$ et $N = a^2 - b^2 d$ pair, alors $\operatorname{pgcd}(a, d)$ est pair. Il existe donc un indice i tel que $p_i = 2$, et d'après la démonstration du point (i) de la proposition 1, $v_2(\delta_n) = l_n = [n/2]$.

Si $d \equiv 3 \pmod 4$, comme $\delta_1 = 1$ et N pair, alors $v_2(N) = 1$. En reprenant la démonstration du point (i) avec $v_2(N^n)$, on obtient pour tout $n \geq 1$, $v_2(\delta_n) = [n/2]$.

Partant de (1), on peut écrire, pour tout $n \geq 1$,

$$a'_{n+2} = 2aa'_{n+1} - Na'_n, \quad b'_{n+2} = 2ab'_{n+1} - Nb'_n. \tag{2}$$

Comme $\delta_1 = 1$, de N pair et $d \equiv 1 \pmod 4$, on a $v_2(a'_1) = v_2(b'_1) = 0$ et $v_2(a'_2) = v_2(b'_2) = 1$. On raisonne alors par récurrence sur n.

Si $d \equiv 1 \pmod 8$, alors $v_2(N) \geq 3$. Supposons que $v_2(a'_n) = v_2(b'_n) = n-1$ et $v_2(a'_{n+1}) = v_2(b'_{n+1}) = n$, et montrons que $v_2(a'_{n+2}) = v_2(b'_{n+2}) = n+1$.

Par (2), on a $v_2(a'_{n+2}) = \min\{v_2(2aa'_{n+1}), v_2(Na'_n)\} = \min\{n+1, n+2+k\}$ avec $k = v_2(N) - 3$. D'où $v_2(a'_{n+2}) = n+1$. De la même manière, on obtient $v_2(b'_{n+2}) = n+1$.

Si $d \equiv 5 \pmod 8$, alors $v_2(N) = 2$. Supposons que $v_2(a'_{3k+1}) = v_2(b'_{3k+1}) = 3k$ et $v_2(a'_{3k+2}) = v_2(b'_{3k+2}) = 3k+1$. Montrons alors que $v_2(\delta_{3(k+1)}) = 3(k+1)$, $v_2(a'_{3(k+1)+1}) = v_2(b'_{3(k+1)+1}) = 3(k+1)$ et $v_2(a'_{3(k+1)+2}) = v_2(b'_{3(k+1)+2}) = 3(k+1)+1$.

On a

$$v_2\left(\frac{2aa'_{3k+2}}{2^{3k+2}} - \frac{Na'_{3k+1}}{2^{3k+2}}\right) \geq 1,$$

et par (2), $v_2(a'_{3(k+1)}) \geq 3(k+1)$. Avec les mêmes arguments, on déduit $v_2(b'_{3(k+1)}) \geq 3(k+1)$, et donc $v_2(\delta_{3(k+1)}) \geq 3(k+1)$. En utilisant de nouveau les inégalités (2), on obtient

$$v_2(a'_{3(k+1)+1}) = v_2(b'_{3(k+1)+1}) = v_2(\delta_{3(k+1)}) = 3(k+1).$$

Or, d'après (1), si un entier divise δ_n alors il divise δ_{n+1}. Il en suit donc $v_2(\delta_{3(k+1)}) = 3(k+1)$. On obtient finalement, par (2), $v_2(a'_{3(k+1)+2}) = v_2(b'_{3(k+1)+2}) = v_2(\delta_{3(k+1)+2}) = 3(k+1)+1$. ∎

• Montrons le point (iii) de la proposition 1. Si N et c sont pairs, alors $v_2(f_n) = \min\{v_2(\delta_n), v_2(c^n)\}$. Or d'après le lemme 2, $v_2(f_n) \leq n \leq v_2(c^n)$.

Si $d \equiv 2 \pmod 4$, comme $\operatorname{pgcd}(a,b) = 1$ et d est sans facteur carré, alors $v_2(\operatorname{pgcd}(a,d,c)) = 1$. Or, pour tout $n \geq 1$, on a, $f_n = 2^{l'_n}(\operatorname{pgcd}(a,d,c))^{[n/2]}$ et d'après le lemme 2, $v_2(f_n) = [n/2]$. Il suit donc $l'_n = 0$.

Si $d \not\equiv 2 \pmod 4$, alors $\operatorname{pgcd}(a,d,c)$ est impair, et donc pour tout $n \geq 1$, $l'_n = v_2(\delta_n)$ donné par le lemme 2, ce qui termine la démonstration de la proposition 1. ∎

III. Etude de l'anneau des stabilisateurs. Pour tout $n \geq 1$, soit O_n l'anneau des stabilisateurs du module $\mathbb{Z}+\mathbb{Z}\alpha^n$, i.e. l'ensemble des $\gamma \in \mathbb{Q}(\sqrt{d})$ tels que $\gamma(\mathbb{Z}+\mathbb{Z}\alpha^n) \subset \mathbb{Z}+\mathbb{Z}\alpha^n$. Nous nous proposons dans ce paragraphe de donner, au travers de trois propositions, une description de O_n en fonction de α.

Considérons, pour tout $n \geq 1$, l'équation minimale de α^n :

$$\omega_1(n)X^2 + \omega_2(n)X + \omega_3(n) = 0,$$

avec $(\omega_1(n), \omega_2(n), \omega_3(n)) \in \mathbb{Z}^3$, $\omega_1(n) > 0$ et $\operatorname{pgcd}(\omega_1(n), \omega_2(n), \omega_3(n)) = 1$. On peut écrire, en reprenant les notations du paragraphe II,

$$\frac{\omega_3(n)}{\omega_1(n)} = \frac{a_n^2 - b_n^2 d}{c_n^2} \quad \text{et} \quad \frac{\omega_2(n)}{\omega_1(n)} = \frac{2a_n}{c_n}.$$

En posant $\gamma_n = \operatorname{pgcd}(2a_n c_n, a_n^2 - b_n^2 d, c_n^2)$, il suit alors

$$\omega_1(n) = c_n^2/\gamma_n. \tag{3}$$

Remarquons que de manière plus simple, on a $\gamma_n = \operatorname{pgcd}(2c_n, a_n^2 - b_n^2 d, c_n^2)$. En effet, $\operatorname{pgcd}(2c_n, a_n^2 - b_n^2 d, c_n^2)$ divise γ_n. Réciproquement, tous les diviseurs de γ_n divisent $\operatorname{pgcd}(2c_n, a_n^2 - b_n^2 d, c_n^2)$ sauf peut être s'ils divisent a_n. Or, si un premier p divise a_n et γ_n, il divise $b_n^2 d$. Il ne divise pas b_n, car $\operatorname{pgcd}(a_n, b_n, c_n) = 1$ et par suite il divise d. Or comme d est sans facteur carré, il divise exactement $a_n^2 - b_n^2 d$ et par conséquent, il divise exactement γ_n. Mais alors, comme il divise c_n^2, il divise aussi $\operatorname{pgcd}(2c_n, a_n^2 - b_n^2 d, c_n^2)$.

D'après Z. I. Borevitch et I. R. Chafarevitch [1], p. 152, on a

$$O_n = \mathbb{Z}[\omega_1(n)\alpha^n] = \mathbb{Z} + \mathbb{Z}\omega_1(n)\alpha^n.$$

Pour tout $n \geq 1$, posons $N_n = a_n^2 - b_n^2 d$. En considérant les trois cas suivants : c_n ne divise pas N_n, c_n divise N_n mais c_n^2 ne divise pas N_n, et c_n^2 divise N_n, on détermine alors c_n^2/γ_n et donc O_n en fonction de a_n, b_n, c_n et d. On obtient :

PROPOSITION 2. *Pour tout $n \geq 1$, l'ordre O_n est égal à $\mathbb{Z}[\xi_n]$, où l'entier quadratique ξ_n est donné par le tableau suivant* :

Tableau 1

	$N_n \equiv 0 \,(\mathrm{mod}\, c_n^2)$	$N_n \equiv 0 \,(\mathrm{mod}\, c_n)$ *et* $N_n \not\equiv 0 \,(\mathrm{mod}\, c_n^2)$	$N_n \not\equiv 0 \pmod{c_n}$
$d \equiv 2,3 \,(\mathrm{mod}\, 4)$, *ou* $d \equiv 1 \,(\mathrm{mod}\, 4)$ *et* c_n *impair*	$\xi_n = k_n\sqrt{d}$	$\xi_n = k_n\sqrt{d}$	$\xi_n = k_n\sqrt{d}$
$d \equiv 1 \pmod 4$ *et* c_n *pair*	$\xi_n = \dfrac{1+k_n\sqrt{d}}{2}$	$\xi_n = (1+k_n\sqrt{d})/2$ *si* $v_2(N_n) > v_2(c_n)$	$\xi_n = (1+k_n\sqrt{d})/2$ *si* $v_2(N_n) > v_2(c_n)$
		$\xi_n = k_n\sqrt{d}$ *si* $v_2(N_n) = v_2(c_n)$	$\xi_n = k_n\sqrt{d}$ *si* $v_2(N_n) \le v_2(c_n)$

avec k_n *entier vérifiant* :

(i) $k_n = \begin{cases} |c_n b_n/\gamma_n| & \text{si } O_n \subset \mathbb{Z}[\sqrt{d}], \\ |2c_n b_n/\gamma_n| & \text{si } O_n \not\subset \mathbb{Z}[\sqrt{d}]; \end{cases}$

(ii) $k_n > |b_n|$ *si et seulement si* $N_n \not\equiv 0 \pmod{c_n}$.

La divisibilité de N_n par c_n joue un rôle important dans la forme de ξ_n. Nous allons en déterminer des conditions équivalentes.

Proposition 3. *Les assertions suivantes sont équivalentes* :

(i) *Il existe* $n \ge 2$ *tel que* c_n *divise* N_n.
(ii) c *divise* N, $\mathrm{pgcd}(a,d,c) = 1$, $0 < v_2(c) \le v_2(N) - 1$ *ou* $v_2(c) = 0$.
(iii) *Pour tout* $n \ge 1$, c_n *divise* N_n.
(iv) c_2 *divise* N_2.

Démonstration. (iii)⇒(iv) et (iv)⇒(i) sont claires. Nous allons montrer que (i)⇒(ii) et que (ii)⇒(iii).

Pour tout $n \ge 1$, on a $c_n = c^n/f_n$ et $N_n = N^n/f_n^2$, où f_n est le pgcd défini au paragraphe II. On peut donc écrire

$$(c_n \text{ divise } N_n) \Leftrightarrow (c^n \text{ divise } N^n/f_n).$$

D'après la proposition 1, f_n est de la forme $f_n = 2^{l'_n}(\mathrm{pgcd}(a,d,c))^{l_n}$. Posons comme précédemment $\mathrm{pgcd}(a,d,c) = p_1 \dots p_s$ avec les p_i premiers et tous distincts. Alors c_n divise N_n si et seulement si les trois conditions suivantes sont vérifiées :

1) c divise N;
2) pour tout $i = 1, \dots, s$, $v_{p_i}(c^n) \le v_{p_i}(N^n) - v_{p_i}(f_n)$;
3) $v_2(c^n) \le v_2(N^n) - v_2(f_n)$.

(i)⇒(ii). D'après 1), c divise N. Déduisons de 2) que $\mathrm{pgcd}(a,d,c) = 1$. Raisonnons par l'absurde, et supposons que $\mathrm{pgcd}(a,d,c) \ne 1$. D'après la proposition 1, on a $l_n = [n/2]$. Donc, il existe un indice i, $1 \le i \le s$,

tel que $v_{p_i}(f_n) = [n/2] \geq 1$, car $n \geq 2$. De plus, comme par hypothèse $\operatorname{pgcd}(a,b,c) = 1$, p_i ne divise pas b. Il suit alors que $v_{p_i}(N) = v_{p_i}(d) = 1$, car d est sans facteur carré. De 2) on obtient donc $nv_{p_i}(c) \leq n-1$, d'où $v_{p_i}(c) = 0$, ce qui est une contradiction.

Reste à montrer $0 < v_2(c) < v_2(N)$ ou $v_2(c) = 0$. Si $v_2(f_n) \geq 1$, alors $v_2(c) > 0$, et la condition 3) implique

$$0 < v_2(c) \leq v_2(N) - v_2(f_n)/n \leq v_2(N) - 1/n < v_2(N).$$

Si $v_2(f_n) = 0$, 3) devient $v_2(c) \leq v_2(N)$, et d'après la proposition 1, on a $v_2(c) = 0$ ou $v_2(N) = 0$.

(ii)⇒(iii). Si (ii) est vraie alors, pour tout $n \geq 1$, 1) et 2) sont vérifiées. Si $v_2(c) = 0$ alors pour tout $n \geq 1$, $v_2(f_n) = 0$ et 3) est vérifiée. Si $0 < v_2(c) < v_2(N)$, comme d'après la proposition 1, $v_2(f_n) \leq n$, on a alors $0 < v_2(c) \leq v_2(N) - 1 \leq v_2(N) - v_2(f_n)/n$ et 3) est vérifiée. ∎

Nous déterminons maintenant la forme de ξ_n en fonction de conditions sur α.

PROPOSITION 4. (i) *Si* $d \not\equiv 1 \pmod 4$, *alors pour tout* $n \geq 1$, $\xi_n = k_n\sqrt{d}$.

(ii) *Si* $d \equiv 1 \pmod 4$ *et* $\xi_1 = k_1\sqrt{d}$, *alors pour tout* $n \geq 1$, $\xi_n = k_n\sqrt{d}$.

(iii) *Si* $d \equiv 1 \pmod 8$ *et* $\xi_1 = (1 + k_1\sqrt{d})/2$, *alors pour tout* $n \geq 1$, $\xi_n = (1 + k_n\sqrt{d})/2$.

(iv) *Si* $d \equiv 5 \pmod 8$, *et* $\xi_1 = (1 + k_1\sqrt{d})/2$, *alors*

$$\xi_n = \begin{cases} k_n\sqrt{d} & \text{si 3 divise } n, \\ (1 + k_n\sqrt{d})/2 & \text{si 3 ne divise pas } n. \end{cases}$$

Démonstration. (i) Si $d \not\equiv 1 \pmod 4$, alors pour tout $n \geq 1$, l'anneau O_n est inclus dans $\mathbb{Z}[\sqrt{d}]$.

(ii) Si $d \equiv 1 \pmod 4$ et $\xi_1 = k_1\sqrt{d}$, alors d'après le tableau 1, on a $v_2(c) = 0$ ou $v_2(N) \leq v_2(c)$.

Si $v_2(c) = 0$, alors pour tout $n \geq 1$, $v_2(c_n) = nv_2(c) - v_2(f_n) = 0$, et grâce au tableau 1, $\xi_n = k_n\sqrt{d}$.

Si $v_2(N) \leq v_2(c)$, on peut écrire, pour tout $n \geq 1$,

$$v_2(N) \leq v_2(c) + v_2(f_n)/n,$$

c'est-à-dire $v_2(N_n) \leq v_2(c_n)$, et d'après le tableau 1, $\xi_n = k_n\sqrt{d}$.

(iii) De $\xi_1 = (1+k_1\sqrt{d})/2$ il suit, d'après le tableau 1, $v_2(N) > v_2(c) > 0$. Si $d \equiv 1 \pmod 8$, on en déduit alors, par la proposition 1, que pour tout $n \geq 1$, $v_2(f_n) = n - 1$, et on peut écrire

$$0 < v_2(c) < v_2(N) - v_2(f_n)/n,$$

qui équivaut à $v_2(c_n) < v_2(N_n)$. D'où, grâce au tableau 1, $\xi_n = (1+k_n\sqrt{d})/2$.

(iv) De $\xi_1 = (1+k_1\sqrt{d})/2$ on a, comme précédemment, $v_2(N) > v_2(c) > 0$. Si $d \equiv 5 \pmod 8$, il suit alors par la proposition 1, pour tout $n \geq 1$,

$$v_2(f_n) = \begin{cases} n & \text{si 3 divise } n, \\ n-1 & \text{si 3 ne divise pas } n. \end{cases} \tag{4}$$

Si 3 ne divise pas n, en reprenant la démonstration du point (iii), on a $\xi_n = (1 + k_n\sqrt{d})/2$.

Reste à étudier le cas 3 divise n. On a, par hypothèse, $\operatorname{pgcd}(a,b,c) = 1$. Donc, de $v_2(c) > 0$, il suit que $\operatorname{pgcd}(a,b)$ est impair. On déduit alors de $v_2(N) > 0$ et de $d \equiv 5 \pmod 8$, $v_2(N) = 2$. On a donc $v_2(c) = v_2(N) - 1 = 1$. Les égalités (4) impliquent alors, si 3 divise n,

$$v_2(c_n) = nv_2(c) - v_2(f_n) = 0.$$

D'où, d'après le tableau 1, $\xi_n = k_n\sqrt{d}$. ∎

IV. Une inégalité utile. Pour tout $n \geq 1$, soit $(\alpha_i(n))_{i\geq 0}$ la suite des quotients complets du développement en fraction continue de α^n. Notons $\langle 1, \alpha_i(n)\rangle$ le $\mathbb{Z}$-module $\mathbb{Z} + \mathbb{Z}\alpha_i(n)$. En utilisant l'algorithme des fractions continues, on montre que pour tout $i \geq 0$ et $n \geq 1$, $\langle 1, \alpha_{i+1}(n)\rangle = \alpha_{i+1}(n)\langle 1, \alpha_i(n)\rangle$. On en déduit que pour tout i et j, $\langle 1, \alpha_i(n)\rangle$ et $\langle 1, \alpha_j(n)\rangle$ sont des modules semblables et admettent donc le même anneau des stabilisateurs, O_n. Une minoration de $l(\alpha^n)$ en découle :

Proposition 5 (E. P. Golubeva [4]). *Soient φ_n l'unité fondamentale plus grande que 1 du groupe des unités de O_n et D_n le discriminant de O_n. Alors, pour tout $n \geq 1$,*

$$l(\alpha^n) > \frac{\log \varphi_n}{\log 2\sqrt{D_n}}. \tag{5}$$

Démonstration. Posons, pour tout $n \geq 1$ et $i \geq 0$,

$$\alpha_i(n) = \frac{a_i(n) + b_i(n)\sqrt{d}}{c_i(n)}, \quad \operatorname{pgcd}(a_i(n), b_i(n), c_i(n)) = 1 \ \text{ et } \ c_i(n) > 0.$$

Soit i_n le plus petit indice i tel que $\alpha_i(n)$ soit réduit, i.e. $\alpha_i(n) > 1$ et $-1 < \overline{\alpha}_i(n) < 0$. On peut alors écrire, pour tout $i \geq i_n$,

$$\alpha_i(n) < \alpha_i(n) - \overline{\alpha}_i(n) = \frac{2b_i(n)\sqrt{d}}{c_i(n)}. \tag{6}$$

Or, d'après [1], si O est l'anneau des stabilisateurs du module $M = \mathbb{Z} + \mathbb{Z}\beta$, où β non rationnel est racine du polynôme $\lambda_1 X^2 + \lambda_2 X + \lambda_3$ avec $(\lambda_1, \lambda_2, \lambda_3) \in \mathbb{Z}^3$ premiers entre eux et $\lambda_1 \neq 0$, alors D, le discriminant de O, est égal à $D = \lambda_2^2 - 4\lambda_1\lambda_3$. On en déduit $b_i(n)^2 d \leq D_n$, et par (6), pour tout $i \geq i_n$,

$$\alpha_i(n) < 2\sqrt{D_n}.$$

On a, par périodicité de la fraction continue de α^n,

$$\langle 1, \alpha_{i_n}(n)\rangle = \langle 1, \alpha_{i_n+l(\alpha^n)}(n)\rangle.$$

Or

$$\langle 1, \alpha_{i_n+l(\alpha^n)}(n)\rangle = \alpha_{i_n+l(\alpha^n)}(n)\dots\alpha_{i_n+1}(n)\langle 1, \alpha_{i_n}(n)\rangle,$$

et d'après la théorie des fractions continues, $\alpha_{i_n+l(\alpha^n)}(n)\dots\alpha_{i_n+1}(n) = \alpha_{i_n+l(\alpha^n)-1}(n)\dots\alpha_{i_n}(n)$ est l'unité fondamentale strictement plus grande que 1 de l'anneau des stabilisateurs de $\langle 1, \alpha_{i_n}(n)\rangle$, c'est-à-dire φ_n. Mais $\alpha_i(n)$ est réduit pour tout $i \geq i_n$. On a alors, pour tout $n \geq 1$,

$$\varphi_n = \alpha_{i_n+l(\alpha^n)}(n)\dots\alpha_{i_n+1}(n) < (2\sqrt{D_n})^{l(\alpha^n)}.$$

Il suit finalement

$$l(\alpha^n) > \frac{\log \varphi_n}{\log 2\sqrt{D_n}}. \ \blacksquare$$

L'utilisation de l'inégalité (5) nécessite une majoration du discriminant D_n, qui fait l'objet du lemme suivant :

LEMME 3. *Pour tout* $n \geq 1$, $\log 2\sqrt{D_n} \leq n/A$, *où* $A^{-1} = \log(|a| + |b|\sqrt{d}) + \log c + \log 4$.

D é m o n s t r a t i o n. En reprenant les valeurs de ξ_n données par la proposition 2, on a pour tout $n \geq 1$, $D_n \leq 4c_n^2 b_n^2 d$. Comme c_n est toujours inférieur ou égal à c^n, il nous suffit alors de majorer $|b_n|$, pour tout n. Considérons à nouveau les entiers a'_n et b'_n définis au paragraphe II par $(a + b\sqrt{d})^n = a'_n + b'_n\sqrt{d}$. On peut alors écrire, pour tout $n \geq 1$,

$$|b_n|\sqrt{d} \leq |b'_n|\sqrt{d} \leq |a'_n| + |b'_n|\sqrt{d} = (|a| + |b|\sqrt{d})^n.$$

On en déduit

$$\log 2\sqrt{D_n} \leq \log(4|c_n b_n|\sqrt{d}) \leq n\left(\log(|a| + |b|\sqrt{d}) + \log c + \frac{\log 4}{n}\right). \ \blacksquare$$

La minoration (5) donnée dans la proposition 5 ne devient donc effective que si l'on peut minorer de façon non triviale l'unité φ_n. Désignons alors par G le groupe des unités de $\mathbb{Z}[\sqrt{d}]$ si $O_n \subset \mathbb{Z}[\sqrt{d}]$, ou de $\mathbb{Z}[(1+\sqrt{d})/2]$ si $O_n \not\subset \mathbb{Z}[\sqrt{d}]$. Si G_n est le groupe des unités de O_n, on définit, pour tout $n \geq 1$, l'entier μ_n par

$$\mu_n = [G : G_n].$$

Soit alors ε_0 l'unité fondamentale plus grande que 1 de G. Remarquons que ε_0 est l'unité fondamentale plus grande que 1 du corps $\mathbb{Q}(\sqrt{d})$, sauf si $d \equiv 5 \pmod 8$ et $O_n \subset \mathbb{Z}[\sqrt{d}]$, où ε_0 peut éventuellement être le cube de l'unité fondamentale plus grande que 1 du corps $\mathbb{Q}(\sqrt{d})$. On a alors $\varphi_n = \varepsilon_0^{\mu_n}$. Nous obtenons alors par la minoration (5) et le lemme 2 l'inégalité

$$l(\alpha^n) > A\frac{\mu_n}{n}\log \varepsilon_0. \tag{7}$$

Notre problème se ramène donc à la détermination d'une minoration de l'indice de groupe d'unités μ_n, ce qui fait l'objet du paragraphe suivant.

V. Etude de l'indice μ_n. Soit, pour tout $n \geq 1$, ξ_n le générateur de O_n donné par la proposition 2. Posons $\omega = \sqrt{d}$ si $\xi_n = k_n\sqrt{d}$, et $\omega = (1+\sqrt{d})/2$ si $\xi_n = (1 + k_n\sqrt{d})/2$.

Désignons, pour tout $s \geq 0$, par P_s/Q_s les réduites de la fraction continue de ω, et pour tout $n \geq 1$ et par $P_s^{(n)}/Q_s^{(n)}$ les réduites de la fraction continue de ξ_n. Définissons encore $\pi = l(\omega)$ et, pour tout $n \geq 1$, $\pi_n = l(\xi_n)$. D'après la théorie des fractions continues, on peut, pour tout $n \geq 1$, exprimer φ_n à partir des réduites et de la longueur de la période de la fraction continue de ξ_n :

$$\varphi_n = P^{(n)}_{\pi_n-1} + Q^{(n)}_{\pi_n-1}\xi_n.$$

De même, les puissances de ε_0 s'expriment en fonction des réduites et de la longueur de la période de la fraction continue de ω :

$$\varepsilon_0^\nu = P_{\nu\pi-1} + Q_{\nu\pi-1}\omega, \quad \nu \geq 1. \tag{8}$$

Or comme $\varphi_n = \varepsilon_0^{\mu_n}$, on obtient

$$P^{(n)}_{\pi_n-1} + Q^{(n)}_{\pi_n-1}\xi_n = P_{\mu_n\pi-1} + Q_{\mu_n\pi-1}\omega.$$

En remplaçant ξ_n et ω par leurs valeurs, il suit alors

$$k_n Q^{(n)}_{\pi_n-1} = Q_{\mu_n\pi-1}. \tag{9}$$

On déduit de ces égalités une minoration de l'indice $\mu_n = [G : G_n]$.

Proposition 6 (Minoration de l'indice). *Soit $k_n = \prod_{i=1}^{s_n} t_{n,i}^{e_i(n)}$ la décomposition de k_n en facteurs premiers, et pour tout $i = 1, \ldots, s_n$,*

$$\begin{aligned}
\nu_i(n) &= \min\{m \geq 1 :\ t_{n,i} \mid Q_{m\pi-1}\},\\
e'_i(n) &= \max\{e \geq 1 :\ t^e_{n,i} \mid Q_{\nu_i(n)\pi-1}\},\\
\delta_i(n) &= \begin{cases} 0 & \text{si } e'_i(n) \geq e_i(n),\\ e_i(n) - e'_i(n) & \text{si } e'_i(n) < e_i(n).\end{cases}
\end{aligned}$$

Alors $\mu_n \geq \prod_{i=1}^{s_n} t_{n,i}^{\delta_i(n)}$.

Démonstration. La preuve s'articule autour du lemme suivant :

Lemme 4 (H. Cohen [3]). *Soit σ un nombre premier. Supposons que σ^m divise exactement $Q_{\gamma\pi-1}$, $m \geq 1$, $\gamma \geq 1$. Alors σ^{m+1} divise exactement $Q_{\sigma\gamma\pi-1}$ et σ^{m+1} ne divise pas $Q_{u\gamma\pi-1}$, $1 \leq u < \sigma$.*

Démonstration. D'après (8), pour tout $u \in \mathbb{N}^*$, $P_{u\gamma\pi-1} + Q_{u\gamma\pi-1}\omega$ est une unité de G, et $P_{u\gamma\pi-1} + Q_{u\gamma\pi-1}\omega = (P_{\gamma\pi-1} + Q_{\gamma\pi-1}\omega)^u$. Par la

formule du binôme, on a alors

$$Q_{u\gamma\pi-1} = \sum_{j=0}^{[(u-1)/2]} C_u^{2j+1} P_{\gamma\pi-1}^{u-2j-1} Q_{\gamma\pi-1}^{2j+1} d^j \quad \text{si } \omega = \sqrt{d}$$

$$\left(\text{resp. } Q_{u\gamma\pi-1} = \frac{1}{2^{u-1}} \sum_{j=0}^{[(u-1)/2]} C_u^{2j+1} (2P_{\gamma\pi-1} - Q_{\gamma\pi-1})^{u-2j-1} Q_{\gamma\pi-1}^{2j+1} d^j, \right.$$
$$\left. \text{si } \omega = \frac{1+\sqrt{d}}{2}\right).$$

Or par hypothèse, σ^m divise exactement $Q_{\gamma\pi-1}$. Alors σ^{2m} divise tous les membres de la somme, sauf peut être

$$C_u^1 P_{\gamma\pi-1}^{u-1} Q_{\gamma\pi-1} = u P_{\gamma\pi-1}^{u-1} Q_{\gamma\pi-1} \quad \text{si } \omega = \sqrt{d},$$
$$\left(\text{resp. } \frac{C_u^1}{2^{u-1}} (2P_{\gamma\pi-1} - Q_{\gamma\pi-1})^{u-1} Q_{\gamma\pi-1} \right.$$
$$\left. = \frac{u}{2^{u-1}} (2P_{\gamma\pi-1} - Q_{\gamma\pi-1})^{u-1} Q_{\gamma\pi-1}\right).$$

Si $\sigma \neq 2$, alors σ ne divise pas $P_{\gamma\pi-1}$ car sinon, comme $P_{\gamma\pi-1}^2 - Q_{\gamma\pi-1}^2 d = \pm 1$ (resp. $(2P_{\gamma\pi-1} - Q_{\gamma\pi-1})^2 - Q_{\gamma\pi-1}^2 d = \pm 4$), alors σ divise 1 (resp. σ divise 4), ce qui est absurde. On voit alors que σ est le plus petit entier u tel que σ^{m+1} divise $u P_{\gamma\pi-1}^{u-1} Q_{\gamma\pi-1}$ (resp. σ^{m+1} divise $\frac{u}{2^{u-1}}(2P_{\gamma\pi-1} - Q_{\gamma\pi-1})^{u-1} Q_{\gamma\pi-1}$). σ est alors le plus petit u tel que σ^{m+1} divise $Q_{u\gamma\pi-1}$, et de plus, σ^{m+1} divise exactement $Q_{\sigma\gamma\pi-1}$.

Montrons que si $\sigma = 2$, alors $\omega = \sqrt{d}$. Raisonnons par l'absurde, et supposons $\omega = (1+\sqrt{d})/2$. On a alors $d \equiv 1 \pmod 4$, et 2 divise $2P_{\gamma\pi-1} - Q_{\gamma\pi-1}$ si $m > 1$ ou 4 divise $2P_{\gamma\pi-1} - Q_{\gamma\pi-1}$ si $m = 1$. D'où, $(2P_{\gamma\pi-1} - Q_{\gamma\pi-1})^2 - Q_{\gamma\pi-1}^2 d$ est impair, ce qui est absurde.

Donc si $\sigma = 2$ alors $\omega = \sqrt{d}$, et avec les mêmes arguments que précédemment, 2 est le plus petit entier u tel que 2^{m+1} divise $Q_{u\gamma\pi-1}$ et 2^{m+1} divise exactement $Q_{2\gamma\pi-1}$. ∎

Désignons alors par $\mu_i(n)$, $i = 1, \ldots, s_n$, le plus petit entier positif m tel que $t_{n,i}^{e_i(n)}$ divise $Q_{m\pi-1}$, son existence étant assurée par (9). En reprenant la démonstration du lemme 4 en remplaçant σ^m par $t_{n,i}^{e_i(n)}$, on voit que pour tout $u \geq 1$, $t_{n,i}^{e_i(n)}$ divise $Q_{u\mu_i(n)\pi-1}$. Donc si μ'_n est le plus petit entier positif m tel que k_n divise $Q_{m\pi-1}$, on a $\mu'_n = \text{ppcm}(\mu_i(n))$. Or, $t_{n,i}^{e'_i(n)}$ divise exactement $Q_{\nu_i(n)\pi-1}$. On en déduit donc, grâce au lemme 4, $\mu_i(n) = \nu_i(n) t_{n,i}^{\delta_i(n)}$.

Et comme les $t_{n,i}$ sont premiers entre eux,

$$\mu'_n = \operatorname{ppcm}(\nu_i(n)) \prod_{i=1}^{s_n} t_{n,i}^{\delta_i(n)},$$

c'est-à-dire,

$$\mu'_n \geq \prod_{i=1}^{s_n} t_{n,i}^{\delta_i(n)}.$$

Mais par la définition de μ'_n et (8), $\varepsilon_0^{\mu'_n}$ est une unité de O_n. Comme $\varepsilon_0^{\mu_n}$ est l'unité fondamentale de O_n, il suit alors que μ_n divise μ'_n. Or, par (9), $\mu'_n \leq \mu_n$, d'où $\mu_n = \mu'_n$, ce qui termine la démonstration de la proposition 6. ∎

On en déduit le corollaire suivant :

Corollaire. *Si λ est un entier plus grand que 1 et si λ^m divise k_n, il existe un entier r indépendant de m tel que $\mu_n \geq \lambda^{m-r}$.*

VI. Minoration de $l(\alpha^n)$. Il apparaît que la minoration donnée par le corollaire de la proposition 6 est intéressante si k_n est divisible par une puissance élevée d'un nombre entier. L'ensemble des nombres réels quadratiques pour lesquels l'application de ce résultat permet de conclure est donné par le théorème suivant.

Théorème. *Soit $\alpha = (a+b\sqrt{d})/c$, $a \in \mathbb{Z}$, $b \in \mathbb{Z}^*$, $c \in \mathbb{N}^*$, $\operatorname{pgcd}(a,b,c) = 1$ et $d \geq 2$ sans facteur carré. Désignons par ε_0 l'unité fondamentale plus grande que 1 du corps $\mathbb{Q}(\sqrt{d})$ ou son cube. Posons $A^{-1} = \log(|a| + |b|\sqrt{d}) + \log c + \log 4$ et $\varrho = \operatorname{pgcd}(a,d,c)$. Supposons que α vérifie au moins l'une des conditions suivantes* :

(i) $N_2 \not\equiv 0 \pmod{c_2}$;
(ii) $\operatorname{pgcd}(a,b) > 1$;
(iii) $\operatorname{pgcd}(a,d) > 1$;
(iv) *$a^2 - b^2 d$ pair et c impair.*

Alors il existe une constante effectivement calculable r ne dépendant que de α et deux entiers $\lambda \geq 2$ et $f(n) \geq [n/2]$ tels que pour tout $n \geq 2$,

$$l(\alpha^n) \geq A \log \varepsilon_0 \frac{\lambda^{f(n)-r}}{n},$$

où l'on peut prendre comme valeurs de λ et $f(n)$:

- *si α vérifie* (i), *celles données par le tableau* 2;
- *si α vérifie* (ii), *$\lambda = \operatorname{pgcd}(a,b)$ et $f(n) = n$*;
- *si α vérifie* (iii), *$\lambda = \operatorname{pgcd}(a,d)$ et $f(n) = [n/2]$*;
- *si α vérifie* (iv), *$\lambda = 2$ et $f(n) = v_2(\delta_n)$ donné par le lemme* 2.

Tableau 2

	$\xi_n = k_n\sqrt{d}$ *et* c/γ_1 *entier*	$\xi_n = k_n\sqrt{d}$ *et* c/γ_1 *non entier*	$\xi_n = (1 + k_n\sqrt{d})/2$
$N \not\equiv 0 \pmod c$	$\lambda = (c/\gamma_1),\ f(n) = n$ *avec* $c/\gamma_1 > 1$	$\lambda = (2c/\gamma_1),\ f(n) = n$ *avec* $2c/\gamma_1 > 1$	$\lambda = (2c/\gamma_1),\ f(n) = n$ *avec* $2c/\gamma_1 > 1$
$N \equiv 0 \pmod c$ *et* $v_2(c) < v_2(N)$ *ou* $v_2(c) = 0$	$\lambda = \varrho,\ f(n) = [n/2]$ *avec* $\varrho > 1$	$\lambda = \varrho,\ f(n) = [n/2]$ *avec* $\varrho > 1$	$\lambda = \varrho,\ f(n) = [n/2]$ *avec* $\varrho > 1$
$N \equiv 0 \pmod c$ *et* $v_2(c) = v_2(N) > 0$	$\lambda = 2$ *et* $f(n) = l'_n$	*impossible*	*impossible*

Nous justifions dans la remarque suivante les situations impossibles du tableau 2.

R e m a r q u e. Par hypothèse, pour tout $n \geq 1$, $\operatorname{pgcd}(a_n, b_n, c_n) = 1$, et les entiers γ_n et b_n n'ont pas de facteur commun. On en déduit donc, puisque par définition k_1 est entier, que si c/γ_1 n'est pas entier, alors $k_1 = |2cb/\gamma_1|$, et par la proposition 2, $\xi_1 = (1 + k_1\sqrt{d})/2$. D'où, d'après le tableau 1, $0 < v_2(c) < v_2(N)$.

Par conséquent, avoir c/γ_1 non entier et $v_2(c) \geq v_2(N)$ est impossible. De même, si $\xi_n = (1+k_n\sqrt{d})/2$, grâce à la proposition 4, on a $\xi_1 = (1+k_1\sqrt{d})/2$, et par suite $0 < v_2(c) < v_2(N)$.

Afin de dégager des puissances élevées de nombres entiers dans les diviseurs de k_n, nous allons, dans le lemme 6, donner une factorisation de l'entier k_n. D'après la proposition 2, on a $k_n = |c_n b_n/\gamma_n|$ avec $c_n/\gamma_n \in \mathbb{N}^*$ si $\xi_n = k_n\sqrt{d}$, et $k_n = |2c_n b_n/\gamma_n|$ avec $2c_n/\gamma_n \in \mathbb{N}^*$ si $\xi_n = (1 + k_n\sqrt{d})/2$. Il est alors nécessaire de déterminer l'entier γ_n en fonction de α, ce qui fait l'objet du lemme 5.

Lemme 5. *Si pour tout* $n \geq 1$ $\gamma_n = \operatorname{pgcd}(2c_n, a_n^2 - b_n^2 d, c_n^2)$, *alors* $\gamma_1^n = \gamma_n f_n^2$.

D é m o n s t r a t i o n. Soit, pour tout $n \geq 1$, $\omega_1(n)X^2 + \omega_2(n)X + \omega_3(n) = 0$ l'équation minimale de α^n introduite au paragraphe III. Posons, pour alléger l'écriture, $\omega_1 = \omega_1(1)$, $\omega_2 = \omega_2(1)$ et $\omega_3 = \omega_3(1)$. On montre par récurrence sur n que l'équation minimale de α^n est $\omega_1^n X^2 + \omega_2(n)X + \omega_3^n = 0$.

De $(\omega_1\alpha^2 + \omega_3)^2 = \omega_2^2\alpha^2$, on obtient $\omega_1^2\alpha^4 + (2\omega_1\omega_3 - \omega_2^2)\alpha^2 + \omega_3^2 = 0$, ce qui montre la propriété pour $n = 2$. Supposons la propriété vraie jusqu'au

rang n. On peut écrire

$$(\omega_1^n\alpha^{2n}+\omega_3^n)(\omega_1\alpha^2+\omega_2\alpha+\omega_3)=0.$$

En développant, on obtient

$$\omega_1^{n+1}\alpha^{2n+2}+\omega_3^{n+1}+(\omega_1^n\omega_2\alpha^{2n+1}+\omega_1^n\omega_3\alpha^{2n}+\omega_3^n\omega_1\alpha^2+\omega_3^n\omega_2\alpha)=0.$$

Or,

$$\omega_1^n\omega_2\alpha^{2n+1}+\omega_3^n\omega_2\alpha=-\omega_2\omega_2(n)\alpha^{n+1}$$

et

$$\omega_1^n\omega_3\alpha^{2n}+\omega_3^n\omega_1\alpha^2=-\omega_3\omega_1\omega_2(n-1)\alpha^{n+1}.$$

On en déduit alors

$$\omega_1^{n+1}\alpha^{2n+2}-(\omega_1\omega_3\omega_2(n-1)+\omega_2\omega_2(n))\alpha^{n+1}+\omega_3^{n+1}=0.$$

Si $p>1$ premier divise $\operatorname{pgcd}(\omega_1,\omega_3)$, alors il ne divise le coefficient de α^{n+1} que s'il divise ω_2, car d'après l'hypothèse de récurrence p ne divise pas $\omega_2(n)$. Or $\operatorname{pgcd}(\omega_1,\omega_2,\omega_3)=1$. La propriété est donc vérifiée au rang $n+1$.

D'après (3), on a pour tout $n\geq 1$, $\omega_1(n)=c_n^2/\gamma_n$. Il en suit

$$\omega_1(n)=\omega_1^n=\frac{c_n^2}{\gamma_n}=\left(\frac{c^2}{\gamma_1}\right)^n.$$

De $c^n=c_nf_n$, on déduit alors $\gamma_1^n=\gamma_nf_n^2$. ∎

Lemme 6. *Posons* $\varrho=\operatorname{pgcd}(a,d,c)$. *Alors pour tout* $n\geq 1$, *une factorisation de* k_n *est donnée par le tableau suivant* :

Tableau 3

	$\xi_n=k_n\sqrt{d}$ *et* c/γ_1 *entier*	$\xi_n=k_n\sqrt{d}$ *et* c/γ_1 *non entier*	$\xi_n=(1+k_n\sqrt{d})/2$
k_n	$(c/\gamma_1)^n\varrho^{[n/2]}2^{l'_n}\lvert b_n\rvert$	$(2c/\gamma_1)^n\varrho^{[n/2]}\lvert b_n\rvert$	$(2c/\gamma_1)^n\varrho^{[n/2]}\lvert b_n\rvert$

Démonstration. Si $\xi_n=k_n\sqrt{d}$, alors d'après la proposition 2, $k_n=|c_nb_n/\gamma_n|$, et si de plus c/γ_1 est entier, de l'égalité $c^n=c_nf_n$ et du lemme 4, on écrit

$$k_n=(c/\gamma_1)^nf_n|b_n|.$$

Et, d'après la proposition 1, on a $f_n=2^{l'_n}\varrho^{[n/2]}$.

Si $\xi_n=k_n\sqrt{d}$, alors $k_n=|c_nb_n/\gamma_n|$, et si c/γ_1 n'est pas un entier, alors par définition de γ_n, $2c/\gamma_1$ est un entier. D'où, grâce au lemme 4,

$$k_n=(2c/\gamma_1)^n(f_n/2^n)|b_n|=(2c/\gamma_1)^n\varrho^{[n/2]}2^{l'_n-n}|b_n|.$$

Mais de c/γ_1 non entier, on déduit, comme dans la remarque du tableau 2, $\xi_1=(1+k_1\sqrt{d})/2$. Il suit, par le tableau 1, $v_2(N)>v_2(c)>0$. De plus,

comme $\xi_n = k_n\sqrt{d}$, on obtient, grâce à la proposition 4, $d \equiv 5 \pmod 8$ et 3 divise n, d'où finalement, d'après la proposition 1, $l'_n = n$.

Si $\xi_n = (1 + k_n\sqrt{d})/2$, alors $k_n = |2c_nb_n/\gamma_n|$. Par définition, $2c/\gamma_1$ est un entier, et on écrit grâce au lemme 4,

$$k_n = (2c/\gamma_1)^n f_n|b_n| = (2c/\gamma_1)^n \varrho^{[n/2]} 2^{l'_n-(n-1)}|b_n|.$$

De la proposition 4, on déduit $\xi_1 = (1 + k_1\sqrt{d})/2$ et $d \equiv 1 \pmod 8$ ou $d \equiv 5 \pmod 8$ avec n non divisible par 3. Du tableau 1, on tire alors $v_2(N) > v_2(c) > 0$, et par suite, d'après la proposition 1, $l'_n = n - 1$. ∎

Démonstration du théorème. Nous allons, pour chacune des quatre conditions du théorème, déterminer $\lambda \geq 2$ et $f(n) \geq [n/2]$ tels que pour tout $n \geq 2$, $\lambda^{f(n)}$ divise k_n. Par suite, grâce à l'inégalité (7) et au corollaire de la proposition 6, on déduit qu'il existe un entier r indépendant de $f(n)$ tel que pour tout $n \geq 2$,

$$l(\alpha^n) > A \log \varepsilon_0 \frac{\lambda^{f(n)}}{n} \geq A \log \varepsilon_0 \frac{2^{[n/2]}}{n}.$$

(i) $N_2 \not\equiv 0 \pmod{c_2}$. Fixons $n \geq 2$. Comme c_2 ne divise pas N_2, en prenant la contraposée de la proposition 3(i), pour tout $n \geq 2$, c_n ne divise pas N_n. D'où par la proposition 2(ii), $k_n > |b_n|$. C'est-à-dire, d'après le lemme 6 :

$$\frac{k_n}{|b_n|} = \begin{cases} \left(\frac{c}{\gamma_1}\right)^n \varrho^{[n/2]} 2^{l'_n} > 1 \\ \text{ou} \\ \left(\frac{2c}{\gamma_1}\right)^n \varrho^{[n/2]} > 1. \end{cases} \tag{10}$$

Or, grâce à la proposition 3(ii), c_2 ne divise pas N_2 est équivalent à : c ne divise pas N, ou $\varrho = \operatorname{pgcd}(a, d, c) > 1$, ou $v_2(c) = v_2(N) > 0$. Notons que la dernière condition devrait être $v_2(c) \geq v_2(N) > 0$. Mais $v_2(c) = v_2(N) > 0$ suffit, car si $v_2(c) > v_2(N)$ alors c ne divise pas N.

Si c ne divise pas N, alors d'après la proposition 2(ii), $c/\gamma_1 > 1$ ou $2c/\gamma_1 > 1$. On en déduit donc par (10) que pour tout $n \geq 1$, $(c/\gamma_1)^n$ divise k_n si $\xi_n = k_n\sqrt{d}$ et c/γ_1 est entier, ou $(2c/\gamma_1)^n$ divise k_n si $\xi_n \neq k_n\sqrt{d}$ ou si c/γ_1 n'est pas entier.

Si c divise N et $v_2(c) < v_2(N)$ ou $v_2(c) = 0$, alors $\varrho = \operatorname{pgcd}(a, d, c) > 1$, alors par (10), pour tout $n \geq 1$, $\varrho^{[n/2]}$ divise k_n.

Si c divise N et $v_2(c) = v_2(N) > 0$, alors d'après la proposition 1, pour $d \not\equiv 2 \pmod 4$ et pour tout $n \geq 1$, $l'_n \geq [n/2]$. Donc par (10), si $\xi_n = k_n\sqrt{d}$ et c/γ_1 est entier, $2^{[n/2]}$ divise k_n. Si $d \equiv 2 \pmod 4$, alors forcément 2 divise $\operatorname{pgcd}(a, d, c)$ et on revient au cas précédent.

(ii) $\operatorname{pgcd}(a, b) > 1$. Comme $\operatorname{pgcd}(a, b, c) = 1$, il suit que pour tout $n \geq 1$, $(\operatorname{pgcd}(a, b))^n$ divise b_n, et donc divise k_n.

(iii) $\operatorname{pgcd}(a,d) > 1$. Si $\varrho = \operatorname{pgcd}(a,d,c)$, alors d'après la proposition 1, pour tout $n \geq 1$, $\varrho^{[n/2]}$ divise f_n. D'où $(\operatorname{pgcd}(a,d))^{[n/2]}$ divise $\delta_n = \operatorname{pgcd}(a'_n, b'_n)$, et donc $(\operatorname{pgcd}(a,d)/\varrho)^{[n/2]}$ divise b_n. Or, si $\varrho > 1$, en revenant à la démonstration du (i), $\varrho^{[n/2]}$ divise k_n. Par conséquent, $(\operatorname{pgcd}(a,d))^{[n/2]}$ divise k_n.

(iv) $N = a^2 - b^2 d$ pair et c impair. Pour tout $n \geq 1$, b_n, et donc k_n, est divisible par $2^{v_2(\delta_n)}$, avec $v_2(\delta_n)$ donné par le lemme 2. ∎

Références

[1] Z. I. Borevitch et I. R. Chafarevitch, *Théorie des nombres*, Gauthier-Villars, 1967.

[2] G. Choquet, *Répartition des nombres $k(3/2)^n$; et ensembles associés*; *Algorithmes adaptés aux suites $(k\theta^n)$ et aux chaînes associées*; *θ-jeux récursifs et application aux suites $(k\theta^n)$*; *solenoïdes de T^z*, C. R. Acad. Sci. Paris Sér. A 290 (1980), 575–580; 719–724 et 863–868; *Construction effective des suites $k(3/2)^n$. Etude des mesures 3/2-stables de Π*; *Les fermés (3/2)-stables de T*; *structure des fermés dénombrables*; *applications arithmétiques*, ibid. 291 (1980), 69–74 et 239–244; *θ-fermés, θ-chaînes et θ-cycles (pour $\theta = 3/2$)*; *θ-fermés et dimension de Hausdorff. Conjectures de travail. Arithmétique des θ-cycles (où $\theta = 3/2$)*, C. R. Acad. Sci. Paris Sér. I 292 (1981), 5–10 et 339–344.

[3] H. Cohen, *Multiplication par un entier d'une fraction continue périodique*, Acta Arith. 26 (1974), 129–148.

[4] E. P. Golubeva, *On the length of the period of a quadratic irrationality*, Math. USSR-Sb. 51 (1) (1985), 119–129.

[5] M. Mendès France, *Remarks on finite continued fractions*, Enseign. Math. 39 (1993), 249–257.

[6] R. Paysant-Le Roux et E. Dubois, *Une application des nombres de Pisot à l'algorithme de Jacobi–Perron*, Monatsh. Math. 98 (1984), 145–155.

[7] A. J. van der Poorten, *Some problems of recurrent interest*, in: Topics in Classical Number Theory (Colloq. Budapest, 1981), Colloq. Math. Soc. János Bolyai 34, G. Halász (éd.), Vol. 2, North-Holland, 1984, 1265–1294.

DÉPARTEMENT DE MATHÉMATIQUES
UNIVERSITÉ DE CAEN
ESPLANADE DE LA PAIX
14032 CAEN CEDEX, FRANCE
E-mail: GRISEL@MATH.UNICAEN.FR

Reçu le 14.3.1995 (2758)