For $l = 0, 1, 2, \ldots$, put

$$W_l = \begin{cases} a\eta^l + b\varrho^l & \text{if } D \geqslant 0, \\ c\eta^l + d\varrho^l & \text{if } D < 0. \end{cases}$$

Then

$$u_m = \begin{cases} W_{mq}, \\ W_{mq-D}; \end{cases} \qquad v_n = \begin{cases} W_{np+D}, & D \geqslant 0, \\ W_{np}, & D < 0, \end{cases}$$

for $m = 0, 1, 2, \ldots$ and $n = 0, 1, 2, \ldots$

Clearly $\{u_m\}$ and $\{v_n\}$ are subsequences of $\{W_l\}$. Put $r' = (\beta - a) \times \times (\delta - \gamma)$. It is easy to check that the sequence $\{r' W_l\}$ is a non-degenerate binary recursive sequence and its associated polynomial has positive roots.

Remarks. (i) In fact the lemma can be strengthened as follows: Let $\{u_m\}$ and $\{v_n\}$ be non-degenerate binary recursive sequences. Suppose that their associated polynomials have real roots. Then the equation $u_m = v_n$ has finitely many solutions in non-negative integers m, n if and only if the system

$$a\alpha^m = c\gamma^n, \quad b\beta^m = d\delta^n$$

has at most one solution in non-negative integers m, n. Moreover the result is effective.

(ii) It will be very interesting to prove the lemma when the associated polynomials of the sequences $\{u_m\}$ and $\{v_n\}$ have complex roots.

References

[1] A. Baker and D. W. Masser, Ed., *Transcendence theory: Advances and applications*, Academic Press, London 1977, pp. 1–27.

[2] H. Hasse, *Zahlentheorie*, Akademie-Verlag, Berlin 1949.

[3] K. K. Kubota, *On a conjecture of Morgan Ward, II*, Acta Arith. 33 (1977), pp. 29–48.

[4] M. Mignotte, *Une extension du théorème de Skolem–Mahler*, C. R. Acad. Sci. Paris, Serie A, 288 (1979), pp. 233–235.

DEPARTMENT OF MATHEMATICS
PANJAB UNIVERSITY
Chandigarh, India
TATA INSTITUTE OF FUNDAMENTAL RESEARCH
HOMI BHABHA ROAD
Bombay 400 005, India

Received on 14.12.1978
and in revised form on 2.5.1980 (1122)

ACTA ARITHMETICA
XL (1982)

Meilleures approximations d'une forme linéaire cubique

par

EUGÈNE DUBOIS (Caen) et GEORGES RHIN (Metz)

I. Introduction, notations. Le développement d'un nombre réel α en fraction continue permet de bien connaître les approximations rationnelles de α ou de la forme linéaire $q\alpha - p$. Si p_n/q_n est une réduite de α on a les propriétés

(i) $|q_n\alpha - p_n| < 1/q_n$, $n \geqslant 0$,

(ii) $|q\alpha - p| < |q_n\alpha - p_n| \Rightarrow |q| > q_n$,

(iii) Le développement est périodique pour $\alpha = \sqrt{D}$ (D entier non carré).

Beaucoup d'auteurs (Jacobi, O. Perron, N. Pipping, V. Brun, G. Szekeres, ...) ont tenté de généraliser cette théorie à plusieurs nombres réels.

Nous renvoyons à G. Szekeres [5], p. 113–117, pour la discussion des propriétés que l'on peut demander à de tels algorithmes.

Dans cet article nous proposons une nouvelle définition de la notion de meilleure approximation de zéro par une forme linéaire cubique, $p_0 + p_1\alpha_1 + p_2\alpha_2$. Nous montrons au paragraphe II que l'algorithme fournissant ces approximations peut être considéré comme une généralisation des fractions continues. Le développement de $\alpha_1 = \sqrt[3]{m}$, $\alpha_2 = \sqrt[3]{m^2}$, où m est un entier naturel distinct d'un cube, est périodique (théorème 1). Au paragraphe IV on étudie les propriétés générales de cet algorithme appliqué à deux nombres réels α_1, α_2 linéairement indépendants avec 1 et on montre que les approximations de zéro par la forme linéaire $p_0 + p_1\alpha_1 + p_2\alpha_2$ et les approximations simultanées de α_1 et α_2 qui en résultent vérifient le meilleur degré d'approximation possible.

Soient α_1, α_2 deux nombres réels supérieurs à 1 (cette restriction n'est pas fundamentale), p_0, p_1, p_2 trois entiers. Posons:

$$\Omega = (1, \alpha_1, \alpha_2), \quad P = (p_0, p_1, p_2),$$

$$\text{(I.1)} \qquad \psi(P) = P \cdot \Omega = p_0 + p_1\alpha_1 + p_2\alpha_2,$$

$$\mathscr{C}(P) = \tfrac{1}{2}\big((p_0 - p_1\alpha_1)^2 + (p_1\alpha_1 - p_2\alpha_2)^2 + (p_2\alpha_2 - p_0)^2\big).$$

$\mathscr{C}(P)$ peut aussi s'écrire:

(I.2) $$\mathscr{C}(P) = \tfrac{3}{2}(p_0^2+p_1^2\alpha_1^2+p_2^2\alpha_2^2)-\tfrac{1}{2}\big(\psi(P)\big)^2,$$

(I.3) $$\mathscr{C}(P) = (p_0+jp_1\alpha_1+j^2p_2\alpha_2)(p_0+j^2p_1\alpha_1+jp_2\alpha_2)$$
où j vérifie $1+j+j^2 = 0$.

DÉFINITION 1. P est une *meilleure approximation normale* (m.a.n.) de Ω si pour tout triplet d'entiers P', distinct de P, vérifiant:
$$0<\psi(P')\leqslant\psi(P)\leqslant 1$$
on a $\mathscr{C}(P')>\mathscr{C}(P)$.

Nous conviendrons de ranger les m.a.n. P_k de façon que:
$$1\geqslant\psi(P_0)=\psi_0,\qquad \psi_k=\psi(P_k)>\psi_{k+1}=\psi(P_{k+1})\qquad (k\geqslant 0)$$
cette suite est finie si et seulement si α_1 et α_2 sont rationnels.

En effet d'après (I.2), pour tout $\varepsilon>0$ et $C>0$ l'ensemble des triplets d'entiers P vérifiant $0<\psi(P)\leqslant\varepsilon$ et $\mathscr{C}(P)<C$ est fini et donc P_k vérifie:

(I.4) $$\mathscr{C}(P_k) = \min\{\mathscr{C}(P)|\ 0<\psi(P)<\psi(P_{k-1})\}\qquad (k\geqslant 1).$$

Alors la construction des m.a.n. ne s'arrête que si:
$$\{\psi(P)|\ P\in\boldsymbol{Z}^3,\ \psi(P)>0\}$$
admet un minimum, ce qui équivaut à α_1 et α_2 rationnels. Dans le cas contraire la suite $\big(\mathscr{C}(P_k)\big)_{k\geqslant 0}$ est croissante et d'après (I.2) tend vers l'infini.

Nous supposerons dans la suite que 1, α_1, α_2 vérifient

(I.5) $$1<\alpha_1<\alpha_2\quad\text{ et }\quad 1,\alpha_1,\alpha_2 \text{ linéairement indépendants sur } \boldsymbol{Q}.$$

De cette hypothèse, il résulte que $\psi(P)=\psi(P')$ si et seulement si $P=P'$. Si 1, α_1, α_2 sont $\boldsymbol{Q}$ linéairement dépendants, l'étude $\psi(P)$ peut se traiter à l'aide des fractions continues.

DÉFINITION 2. Soient 1, α_1, α_2 vérifiant (I.5), $\Omega=(1,\alpha_1,\alpha_2)$, $(P_k)_{k\geqslant 0}$ la suite des m.a.n. de Ω.

Pour $k\geqslant 1$ soit $\mathscr{F}_k$ l'ensemble des éléments Q de $\boldsymbol{Z}^3$ tels que

(i) $0<\psi(Q)<\psi_{k-1}=\psi(P_{k-1})$,

(ii) P_k, Q, P_{k-1} linéairement indépendants,

(iii) $\mathscr{C}(Q)$ minimum parmi les Q vérifiant (i) et (ii).

Soit Q_k l'élément de $\mathscr{F}_k$ tel que $\varphi_k=\psi(Q_k)$ soit minimum. On pose $Q_0=(0,1,0)$.

Les éléments de la suite $(Q_k)_{k\geqslant 0}$ sont appelés les approximations normales *auxiliaires* de Ω.

Posons $P_{-1}=(0,0,1)$. Pour $k\geqslant 0$ soit $\mathscr{L}_k$ la matrice dont les lignes sont P_k, Q_k, P_{k-1}. Nous montrerons (proposition 4) que $|\det\mathscr{L}_k|=1$. Nous dirons que $\mathscr{L}_k$ est la $k^{\text{ème}}$ *base d'approximation de* Ω.

Soient $\mathscr{S}_k$ la matrice inverse de $\mathscr{L}_k$, $A_k=(a_0^{(k)},a_1^{(k)},a_2^{(k)})$, $B_k=(b_0^{(k)},b_1^{(k)},b_2^{(k)})$, $C_k=(c_0^{(k)},c_1^{(k)},c_2^{(k)})$ ses vecteurs colonnes.

Nous associons à la suite des m.a.n. de Ω les nombres

(I.6) $$\beta_1^{(k)}=\frac{\psi(Q_k)}{\psi(P_k)}=\frac{\varphi_k}{\psi_k},\qquad \beta_2^{(k)}=\frac{\psi_{k-1}}{\psi_k}\qquad (k\geqslant 0)$$

et les matrices Λ_k définies par:

(.7) $$\mathscr{L}_{k+1}=\Lambda_k\cdot\mathscr{L}_k\qquad (k\geqslant 0).$$

DÉFINITION 3. Nous appellerons développement de α_1, α_2 la suite $(\beta_1^{(k)},\beta_2^{(k)})_{k\geqslant 0}$ et nous dirons qu'il est périodique si cette suite l'est.

Définir un algorithme, c'est définir des critères pour déterminer à chaque étape les matrices Λ_k ou Λ_k^{-1} suivant que l'on étudie les approximations de zéro par une forme linéaire ou les approximations simultanées.

Pour l'algorithme de Jacobi–Perron les matrices Λ_k^{-1} sont de la forme
$$\Lambda_k^{-1}=\begin{bmatrix}0&0&1\\1&0&a_1^{(k)}\\0&1&a_2^{(k)}\end{bmatrix}$$
où $a_1^{(k)}$ et $a_2^{(k)}$ sont les parties entières de $\beta_1^{(k)}$, $\beta_2^{(k)}$

Pour l'algorithme de G. Szekeres [5] (restreint à la dimension 2) les matrices Λ_k^{-1} prennent quatre formes suivant certains critères
$$\begin{bmatrix}0&1&0\\1&1&0\\0&0&1\end{bmatrix},\quad\begin{bmatrix}1&1&0\\0&1&0\\0&0&1\end{bmatrix},\quad\begin{bmatrix}0&0&1\\0&1&0\\1&0&0\end{bmatrix},\quad\begin{bmatrix}1&0&1\\0&1&0\\0&0&1\end{bmatrix}.$$

Pour l'algorithme de Minkowski [2] les matrices Λ_k^{-1} sont de la forme
$$\begin{bmatrix}a&\pm b&\pm c\\\pm f&g&\pm h\\\pm j&\pm k&l\end{bmatrix}$$
où $a, b, c, f, g, h, j, k, l$ sont des entiers positifs vérifiant
$$a>\max(b,c),\qquad g>\max(f,h),\qquad l>\max(j,k)$$
et où les signes peuvent prendre six combinaisons (dans chacune d'elles les coefficients sont astreints à des inégalités supplémentaires).

Dans notre définition les Λ_k sont de la forme
$$\Lambda_k=\begin{bmatrix}w&v&u\\w'&v'&u'\\1&0&0\end{bmatrix}$$
où w, v, u, w', v', u' sont des entiers dépendants de P_k, Q_k, P_{k-1} et de la fonction $\mathscr{C}$ suivant les définitions 1 et 2.

II. Restriction de l'algorithme à un seul nombre réel. Soit α un nombre réel irrationnel supérieur à 1. Soit $P = (p, q) \in \mathbf{Z}^2$ et posons:

$$\psi_1(P) = q\alpha + p \quad \text{et} \quad \mathscr{C}_1(P) = |q\alpha - p|$$

et définissons les m.a.n. de α par la définition 1 en remplaçant les fonctions ψ et $\mathscr{C}$ par ψ_1 et $\mathscr{C}_1$.

Habituellement on dit que p/q est une meilleure approximation de α si $q > 0$ et si pour tout $0 < q' \leqslant q$, $(p', q') \neq (p, q)$, on a $|q'\alpha - p'| > |q\alpha - p|$.

Nous allons montrer que ces deux notions sont équivalentes. Ceci résulte essentiellement de ce que $\mathscr{C}_1(P) = |q\alpha - p| = 2|q|\alpha - \psi(P)$.

Proposition 1. *Les m.a.n. de $(1, \alpha)$ définies ci-dessus sont les couples*

$$P_n = (-1)^{n-1}(-p_{n-1}, q_{n-1}), \quad n \geqslant 0,$$

où p_n/q_n désigne la $n^{\text{ème}}$ réduite du développement en fraction continue de α.

Il est clair que le passage au cas $0 < \alpha < 1$ où au cas $\alpha < 0$ ne pose pas de difficulté.

Montrons que $P_0 = (1, 0)$ est la première m.a.n. de $(1, \alpha)$.

Si $P = (p, q)$ est un couple d'entiers, distinct de P_0, tel que $0 < \psi_1(P) < \psi_1(P_0) = 1$. $q = 0$ et $p \neq 1$ est impossible. p et q sont donc de signes contraires et

$$\mathscr{C}_1(P) = |q\alpha - p| = |q|\alpha + |p| > 1 = \mathscr{C}_1(P_0).$$

La deuxième m.a.n. de $(1, \alpha)$ est l'élément P_1 de $\mathbf{Z}^2$ tel que

$$\mathscr{C}_1(P_1) = \min\{\mathscr{C}_1(h, k) |\ 0 < \psi_1(h, k) = k\alpha + h < 1\}.$$

Si $k > 0$

$$h = -[k\alpha] \quad \text{et} \quad \mathscr{C}_1(P_1) = [k\alpha] + k\alpha;$$

Si $k < 0$

$$h = [-k\alpha] + 1 \quad \text{et} \quad \mathscr{C}_1(P_1) = [-k\alpha] + 1 - k\alpha$$

où $[x]$ désigne la partie entière de x.

Il est clair que le minimum est atteint pour $k = 1$. D'où $P_1 = (-[\alpha], 1)$. On raisonne ensuite par récurrence.

III. Cas des corps cubiques purs (¹)

Théorème 1. *Soient m un entier positif qui ne soit pas un cube, $\omega = \sqrt[3]{m}$, le développement de ω, ω^2 est périodique et fournit l'unité fondamentale de l'anneau $\mathbf{Z}(\omega)$.*

(¹) D'après (I.3) si $\alpha_1 = \omega$, $\alpha_2 = \omega^2$, ω^3 entier, $\xi = \eta + i\tau = \psi(P)$ on a $\mathscr{C}(P) = \eta^2 + \tau^2$. La définition 1 des m.a.n. correspond dans ce cas à la définition des minima relatifs de Voronoi ([6], p. 273) exprimée dans un autre réseau. La définition 2 est différente. Il en résulte que les périodes (cas du théorème 1) ont la même longueur. Les propriétés d'approximation obtenues au § IV permettent de montrer des propriétés d'approximation de l'algorithme de Voronoi.

Si U est le groupe des unités de $\mathbf{Z}[\omega]$, on sait qu'il existe η_0, $0 < \eta_0 < 1$, tel que si $u \in U$, il existe un entier n tel que $u = \pm\eta_0^n$.

Si $\mathscr{N} = \mathscr{N}_{K:Q}$ désigne la norme de l'extension $\mathbf{Q} \to K$ on a d'après (I.3):

(III.1) $$\psi(P)\mathscr{C}(P) = \mathscr{N}(\psi(P)), \quad P \in \mathbf{Z}^3.$$

Ceci permet de montrer que $\mathscr{C}$ est injective sur $\mathscr{Z} = \{P \in \mathbf{Z}^3 |\ \psi(P) > 0\}$. En effet si $\mathscr{C}(P) = \mathscr{C}(P')$ on a

$$\psi(P) = \frac{\mathscr{N}(\psi(P))}{\mathscr{N}(\psi(P'))}\psi(P') = \lambda\psi(P')$$

avec λ rationnel. $\mathscr{N}(\psi(P)) = \lambda^3\mathscr{N}(\psi(P'))$ et donc $\mathscr{C}(P) = \lambda^2\mathscr{C}(P')$. Soit $\lambda^2 = 1$ et avec P et P' dans $\mathscr{Z}$ on a $P = P'$.

$\mathscr{C}$ induit alors une relation d'ordre total sur $\mathscr{Z}$ par:

(III.2) $$P \prec Q \Leftrightarrow \mathscr{C}(P) < \mathscr{C}(Q).$$

Ceci permet de définir les m.a.n. et les approximations auxilliaires par:

(III.3) $$\left\{\begin{aligned} \mathscr{C}(P_{k+1}) &= \min\{\mathscr{C}(P) |\ 0 < \psi(P) < \psi(P_k)\}, \quad k \geqslant 1, \\ \text{ou} \quad & \\ P_{k+1} &= \min\{P \in \mathscr{Z} |\ \psi(P) < \psi(P_k)\}, \end{aligned}\right.$$

(III.4) $$\left\{\begin{aligned} \mathscr{C}(Q_{k+1}) &= \min\{\mathscr{C}(Q) |\ \det(P_{k+1}, Q, P_k) \neq 0, \\ &\qquad 0 < \psi(Q) < \psi(P_k)\}, \quad k \geqslant 1, \\ \text{ou} \quad & \\ Q_{k+1} &= \min\{Q \in \mathscr{Z} |\ \det(P_{k+1}, Q, P_k) \neq 0, \\ &\qquad \psi(Q) < \psi(P_k)\}. \end{aligned}\right.$$

Si maintenant η est une unité positive de $\mathbf{Z}[\omega]$ considérons l'application m_η de $\mathscr{Z}$ dans $\mathscr{Z}$ définie par:

(III.5) $$\psi(m_\eta(P)) = \eta\psi(P),$$

η^{-1} étant dans $\mathbf{Z}(\omega)$, $m_\eta \circ m_{\eta^{-1}}$ est l'application identique. m_η est une bijection sur $\mathscr{Z}$ d'après (III.1) m_η est croissante pour l'ordre $\prec$ défini par (III.2).

Nous avons alors le:

Lemme 1. *Si Q est une m.a.n. de Ω et η une unité positive ($\eta \geqslant 1$ ou $\eta \leqslant 1$) de $\mathbf{Z}(\omega)$ telle que $\eta\psi(Q) \leqslant 1$ alors $R = m_\eta(Q)$ est une m.a.n. de Ω.*

En particulier si η est une unité positive dans $]0, 1]$, $P = m_\eta(P_0)$ avec $P_0 = (1, 0, 0)$ (i.e. $\psi(P) = \eta$) est une m.a.n. de Ω.

En effet pour tout R' dans $\mathscr{Z}$ distinct de R tel que $\psi(R') \leqslant \psi(R)$ on a $\psi(m_{\eta^{-1}}(R')) = \dfrac{1}{\eta}\psi(R') \leqslant \dfrac{1}{\eta}\psi(R) = \psi(Q)$.

Puisque Q est une m.a.n. et que Q est distinct de $m_{\eta-1}(R')$ on a $\mathscr{C}(m_{\eta-1}(R')) > \mathscr{C}(Q)$ c'est-à-dire $Q \prec m_{\eta-1}(R')$.

m_η étant croissante on a donc $m_\eta(Q) = R \prec R'$ soit $\mathscr{C}(R') > \mathscr{C}(R)$. Ce qui prouve que R est une m.a.n. et la première assertion du lemme. Puisque $1 < \omega < \omega^2$, $P_0 = (1, 0, 0)$ est une m.a.n. de Ω. En effet si $P \in \mathscr{Z}$ avec $\psi(P) \leqslant 1$ on a d'après (III.1)

$$\mathscr{C}(P) \geqslant \frac{1}{\psi(P)} \geqslant 1 = \mathscr{C}(P_0).$$

La deuxième assertion du lemme résulte alors de la première.

Soit $(P_k)_{k\geqslant 0}$ la suite des m.a.n. Puisque l'ensemble

$$\{P \in \mathscr{Z} \mid \psi(P) < 1 \text{ et } \mathscr{C}(P) < 1/\eta_0\}$$

est fini il existe k_0 tel que $\eta_0 = \psi(P_{k_0})$ (i.e. $P_{k_0} = m_\eta(P_0)$). Alors puisque pour toute unité positive η on a:

$$\psi(P') < \psi(P) \Leftrightarrow \psi(m_\eta(P')) < \psi(m_\eta(P)),$$
$$\mathscr{C}(P') > \mathscr{C}(P) \Leftrightarrow \mathscr{C}(m_\eta(P')) > \mathscr{C}(m_\eta(P))$$

il est clair avec le lemme 1 et (III.3) que

$$P_{k_0+1} = m_{\eta_0}(P_1) \quad \text{et} \quad P_{k_0+n} = m_{\eta_0}(P_{k_0+n}) \quad (n \geqslant 0).$$

De même puisque

$$\det(P_k, Q, P_{k-1}) \neq 0 \Leftrightarrow \det(m_\eta(P_k), m_\eta(Q), m_\eta(P_{k-1})) \neq 0$$

(III.4) montre que

$$Q_{k_0+1} = m_{\eta_0}(Q_1), \quad Q_{k_0+n} = m_{\eta_0}(Q_n) \quad (n \geqslant 1)$$

on a donc

$$\psi_{k_0+n} = \eta_0\psi_n \ (n \geqslant 0), \quad \varphi_{k_0+n} = \eta_0\varphi_n \ (n \geqslant 1)$$

ou pour $i \geqslant 0$

$$\psi_{ik_0+n} = \eta_0^i\psi_n \ (n \geqslant 0), \quad \varphi_{ik_0+n} = \eta_0^i\varphi_n \ (n \geqslant 1)$$

et donc pour $i \geqslant 0$ et $1 \leqslant n \leqslant k_0$

$$(\alpha_1^{(ik_0+n)}, \alpha_2^{(ik_0+n)}) = (\alpha_1^{(n)}, \alpha_2^{(n)}).$$

Il en résulte que

$$A_{ik_0+n} = A_n, \quad 1 \leqslant n \leqslant k_0, \ i \geqslant 0.$$

Les suites $(\alpha_1^{(n)})_{n\geqslant 0}$, $(\alpha_2^{(n)})_{n\geqslant 0}$, $(A_n)_{n\geqslant 0}$ sont donc périodiques avec une prépériode de longueur 1. Nous donnons dans le tableau ci-dessous la longueur k_0 de la période, qui est aussi le nombre d'étapes pour obtenir l'unité fondamentale pour $2 \leqslant m \leqslant 18$.

m	2	3	4	5	6	7	9	10	11	12	13	14	15	16	17	18
k_0	1	3	3	5	5	2	1	3	4	8	5	3	5	10	6	5

IV. Propriétés générales de l'algorithme

Proposition 2. *Soient α_1, α_2 deux nombres réels vérifiant* (I.5), *$(P_k)_{k\geqslant 0}$ la suite des m.a.n. de $\Omega = (1, \alpha_1, \alpha_2)$.*

Alors

$$\psi(P_k)\mathscr{C}(P_{k+1}) \leqslant \theta = \frac{18\alpha_1\alpha_2}{\pi\sqrt{3}}.$$

Soient $V_0 = (\alpha_1\alpha_2, \alpha_2, \alpha_1)$, $V_1 = (\alpha_1\alpha_2, -2\alpha_2, \alpha_1)$, $V_2 = (\alpha_1\alpha_2\sqrt{3}, 0, -\alpha_1\sqrt{3})$. $\{V_0, V_1, V_2\}$ est une base orthogonale de $\boldsymbol{R}^3$ relativement à la forme quadratique $\mathscr{C}$. Son déterminant est $6\sqrt{3}\,\alpha_1^2\alpha_2^2$. Soient $C > 0$ et $\mathscr{A}_C$ l'ensemble des points $M = (x, y, z)$ de $\boldsymbol{R}^3$ tel que:

(IV.1) $$\mathscr{C}(M) < C, \quad |M\cdot\Omega| < \psi(P_k) = \psi_k.$$

$\mathscr{C}(M)$ est défini par (I.1) en remplaçant (p_0, p_1, p_2) par (x, y, z).

Soient (X, Y, Z) les coordonnées de M dans la base $\{V_0, V_1, V_2\}$ les conditions (IV.1) deviennent

(IV.2) $$9\alpha_1^2\alpha_2^2(Y^2+Z^2) < C, \quad 3\alpha_1\alpha_2|X| < \psi_k.$$

$\mathscr{A}_C$ est donc un convexe borné, symétrique par rapport à 0, de volume:

$$\operatorname{vol}(\mathscr{A}_C) = 6\sqrt{3}\alpha_1^2\alpha_2^2\frac{\pi C}{9\alpha_1^2\alpha_2^2}\frac{2\psi_k}{3\alpha_1\alpha_2} = \frac{8}{\theta}C\psi_k.$$

La fonction distance associée au convexe $\mathscr{A}_C$ est pour $M \in \boldsymbol{R}^3$

(IV.3) $$F(M) = \max\left(\sqrt{\frac{\mathscr{C}(M)}{C}}, \frac{|M\cdot\Omega|}{\psi_k}\right).$$

Si $C > \theta/\psi_k$, $\operatorname{vol}(\mathscr{A}_C) > 8$ et d'après le théorème de Minkowski [1]. $\mathscr{A}_C$ contient un point P non nul de $\boldsymbol{Z}^3$. Ce point $P = P(C)$ (en changeant éventuellement de signe) vérifie:

$$0 < \psi(P) < \psi_k \quad \text{et} \quad \mathscr{C}(P) < C.$$

D'après (I.4), pour tout $C > \theta/\psi_k$, $\mathscr{C}(P_{k+1}) < C$ et donc $\psi_k\mathscr{C}(P_{k+1}) \leqslant \theta$.

Proposition 3. *Soient α_1, α_2 deux nombres réels d'un corps de nombres cubique vérifiant* (I.5). *Il existe une constante positive $\varrho = \varrho(\alpha_1, \alpha_2)$ telle que pour toute base d'approximation $\mathscr{L}_k$ $(k \geqslant 0)$ de $\Omega = (1, \alpha_1, \alpha_2)$ on ait pour $k \geqslant 0$:*

$$\psi_k\mathscr{C}(Q_{k+1}) \leqslant \varrho.$$

Puisque P_k est une m.a.n. de Ω, pour tout triplet d'entiers P, non nul, dans $\mathscr{A}_C$ nous avons $|\psi(P)| < \psi_k$ et donc, par la définition 1, $\mathscr{C}(P) > \mathscr{C}(P_k)$.

D'autre part il existe un entier $d \geq 1$ tel que $d\alpha_1, d\alpha_2$ soient des entiers algébriques. Alors $\mathcal{N}(d\psi(P)) \geq 1$. Soient α_i', α_i'' les conjugués de α_i pour $i = 1, 2$, et ψ' et ψ'' les conjugués de $\psi(P)$.

Si $P = (p_0, p_1, p_2)$, $\psi' = p_0 + p_1\alpha_1' + p_2\alpha_2'$, $\psi'' = p_0 + p_1\alpha_1'' + p_2\alpha_2''$ et il existe $\delta_1 \geq 1$ tel que $|\psi'\psi''| \leq \delta_1(p_0^2 + p_1^2 + p_2^2)$. Dès que $0 < \psi(P) \leq 1$ on a d'après (I.2)

$$\mathscr{C}(P) \geq p_0^2 + p_1^2 + p_2^2. \tag{IV.4}$$

Nous avons donc:

$$d^{-3} \leq |\mathcal{N}(\psi(P))| = |\psi(P)|\, |\psi'\psi''| \leq |\psi(P)|\, \delta_1 \mathscr{C}(P)$$

soit avec $\delta = \delta_1 d^3$

$$|\psi(P)|\mathscr{C}(P) \geq \delta^{-1}. \tag{IV.5}$$

Ceci entraîne

$$F(P) \geq \max\left(\sqrt{\frac{\mathscr{C}(P)}{C}},\ \frac{1}{\delta\psi_k\mathscr{C}(P)}\right) \geq (\delta C\psi_k)^{-1/3}$$

car $\inf\limits_{x>0}\left(\max\left(\sqrt{\dfrac{x}{C}}, \dfrac{1}{x\delta\psi_k}\right)\right)$ est atteint pour $x_0 = C^{1/3}(\delta\psi_k)^{-2/3}$.

Donc pour C fixé supérieur à θ/ψ_k

$$\lambda_2 \geq \lambda_1 \geq (C\delta\psi_k)^{-1/3}$$

et d'après le théorème de Minkowski

$$(C\delta\psi_k)^{-2/3}\lambda_3 \operatorname{vol}(\mathscr{A}_C) \leq 8 \quad \text{d'où} \quad \lambda_3 \leq \theta\delta^{2/3}(C\psi_k)^{-1/3}.$$

Donc pour $C > \theta^3\delta^2\psi_k^{-1}$, $\lambda_3 < 1$ et $\mathscr{A}_C$ contient trois points de $\mathbf{Z}^3$, linéairement indépendants. Parmi ces trois points il en existe un qui est linéairement indépendant avec P_k et P_{k+1}. On en déduit que pour tout $C > \theta^3\delta^2\psi_k^{-1}$ on a $\mathscr{C}(Q_{k+1}) < C$. Ce qui prouve la proposition 3 en posant $\varrho = \theta^3\delta^2$.

Proposition 4. *Soient α_1, α_2 deux nombres réels vérifiant* (I.5).

Le déterminant des bases d'approximation $\mathscr{L}_k$ de $\Omega = (1, \alpha_1, \alpha_2)$ et donc des $\mathscr{S}_k$ et Δ_k $(k \geq 0)$ est égal à ± 1.

Le résultat est vrai pour $k = 0$. Supposons le vrai jusqu'à k.

Soient $d = |\det(\mathscr{L}_{k+1})| > 1$ et p un diviseur premier de d.

Nous allons obtenir une contradiction en prouvant l'existence d'un point

$$P = \frac{1}{p}(l_1P_{k+1} + l_2Q_{k+1} + l_3P_k)$$

vérifiant

(i) $P \in \mathbf{Z}^3$ et $|\psi(P)| < \psi_k$,

(ii) $\mathscr{C}(P) < \mathscr{C}(P_{k+1})$ ou $\{\mathscr{C}(P) < \mathscr{C}(Q_{k+1})$ et $\det(P, P_{k+1}, P_k) \neq 0\}$.

Ecrivons pour simplifier l'écriture:

$$R_1 = P_{k+1} = aP_k + bQ_k + cP_{k-1},$$
$$R_2 = Q_{k+1} = a'P_k + b'Q_k + c'P_{k-1},$$
$$R_3 = P_k = P_k$$

on a:

$$d = |\det(R_1, R_2, R_3)| = |bc' - b'c|.$$

Notons $\mathscr{B}$ la forme bilinéaire symétrique associée à la forme quadratique positive $\mathscr{C}$. On a:

$$\text{(IV.6)}\quad \begin{cases} \mathscr{B}(R_i, R_j)^2 \leq \mathscr{C}(R_i)\mathscr{C}(R_j) \leq \mathscr{C}(R_2)^2, \quad i, j \text{ dans}\{1, 2, 3\}, \\ \mathscr{C}(R_3) < \mathscr{C}(R_1) \leq \mathscr{C}(R_2), \\ \mathscr{C}(P) = \dfrac{1}{p^2}\Big(l_1^2\mathscr{C}(R_1) + l_2^2\mathscr{C}(R_2) + l_3^2\mathscr{C}(R_3) + 2l_2l_3\mathscr{B}(R_2, R_3) + \\ \qquad\qquad + 2l_3l_1\mathscr{B}(R_3, R_1) + 2l_1l_2\mathscr{B}(R_1, R_2)\Big). \end{cases}$$

P est dans $\mathbf{Z}^3$ si l_1, l_2, l_3 sont des entiers vérifiant

$$\text{(IV.7)}\quad \begin{aligned} l_1a + l_2a' + l_3 &\equiv 0 \pmod{p}, \\ l_1b + l_2b' &\equiv 0 \pmod{p}, \\ l_1c + l_2c' &\equiv 0 \pmod{p}. \end{aligned}$$

On obtient dans $\mathbf{Z}/p\mathbf{Z}$, un système linéaire dont le déterminant est nul. Il admet donc une solution non triviale. On peut choisir l_1 ou l_2 égal à 1. Il en résulte une solution vérifiant

$$-\left[\frac{p}{2}\right] \leq l_i < \left[\frac{p}{2}\right], \quad i = 1, 2, 3,$$

où $[x]$ désigne la partie entière de x.

Supposons p impair on a:

$$0 < |l_1| + |l_2| + |l_3| \leq 1 + 2\,\frac{p-1}{2} = p. \tag{IV.8}$$

Alors $|\psi(P)| < \dfrac{|l_1| + |l_2| + |l_3|}{p}\psi_k \leq \psi_k$ ce qui prouve (i).

Si $l_2 = 0$ on a d'après (IV.6)

$$\mathscr{C}(P) \leq \frac{1}{p^2}\,(l_1^2 + 2|l_1l_3| + l_3^2)\max(\mathscr{C}(R_1),\ \mathscr{C}(R_3)) \leq \mathscr{C}(R_1)$$

on peut mettre une inégalité stricte puisque si $l_3 \neq 0$, $\mathscr{C}(R_3) < \mathscr{C}(R_1)$ et si $l_3 = 0$, $l_1^2 < p^2$. Ce qui contredit la définition de P_{k+1}.

Si $l_2 \neq 0$ P, P_{k+1}, P_k sont linéairement indépendants et on a d'après (IV.6)

$$\mathscr{C}(P) \leqslant \frac{1}{p^2}(|l_1|+|l_2|+|l_3|)^2 \max\{\mathscr{C}(R_i)|\ i = 1, 2, 3\} \leqslant \mathscr{C}(R_2)$$

on peut mettre une inégalité stricte puisque si $l_3 \neq 0$ $\mathscr{C}(R_3) < \mathscr{C}(R_2)$ et si $l_3 = 0$, $|l_1|+|l_2| \leqslant 1+(p-1)/2 < p$. Ce qui contredit la définition de Q_{k+1} et prouve la proposition 4 si p est impair.

Si $p = 2$ et si l'un des l_i est égal à zéro nous pouvons faire le même raisonnement puisque $|l_1|+|l_2|+|l_3| \leqslant 0+1+2/2 = 2 = p$.

Sinon les points $T_1 = \frac{1}{2}(R_1-R_2-R_3)$, $T_2 = \frac{1}{2}(R_1-R_2+R_3)$ et $T_3 = \frac{1}{2}(R_1+R_2-R_3)$ vérifient (i). Mais

$$\begin{aligned}\mathscr{C}(T_1)+\mathscr{C}(T_2)+\mathscr{C}(T_3) &\\ &= \tfrac{3}{4}\big(\mathscr{C}(R_1)+\mathscr{C}(R_2)+\mathscr{C}(R_3)\big)-\tfrac{1}{2}\big(\mathscr{B}(R_1, R_2)+\mathscr{B}(R_2, R_3)+\mathscr{B}(R_3, R_1)\big)\\ &= \mathscr{C}(R_1)+\mathscr{C}(R_2)+\mathscr{C}(R_3)-\tfrac{1}{4}\mathscr{C}(R_1+R_2+R_3) < 3\mathscr{C}(R_2).\end{aligned}$$

Et donc il existe $i \in \{1, 2, 3\}$ tel que $\mathscr{C}(T_i) < \mathscr{C}(R_2)$. Ce qui contredit la définition de Q_{k+1} et termine la preuve de la proposition 4.

Théorème 2. *Soient α_1, α_2 deux nombres réels vérifiant* (I.5), $(P_k)_{k\geqslant 0}$ *la suite des m.a.n. de $\Omega = (1, \alpha_1, \alpha_2)$, $\psi_k = P_k\cdot\Omega = \psi(P_k)$.*

Pour $k \geqslant 0$ notons

$$\mathscr{L}_k = \begin{bmatrix} p_0^{(k)} & p_1^{(k)} & p_2^{(k)}\\ q_0^{(k)} & q_1^{(k)} & q_2^{(k)}\\ r_0^{(k)} & r_1^{(k)} & r_2^{(k)}\end{bmatrix}, \qquad \mathscr{S}_k = \begin{bmatrix} a_0^{(k)} & b_0^{(k)} & c_0^{(k)}\\ a_1^{(k)} & b_1^{(k)} & c_1^{(k)}\\ a_2^{(k)} & b_2^{(k)} & c_2^{(k)}\end{bmatrix}.$$

Alors on a:

(IV.9) $$\psi_k \max(p_1^{(k)2}, p_2^{(k)2}) \ll 1,$$

(IV.10) $$|b_i^{(k)}-\alpha_i b_0^{(k)}|\ |b_0^{(k)}|^{1/2} \ll 1, \qquad i = 1, 2,$$

où les constantes dans $\ll$ sont calculables en fonction de α_1 et α_2.

Ceci est, d'après W. M. Schmidt [4], le meilleur degré d'approximation que l'on peut obtenir lorsque α_1 et α_2 sont algébriques.

Pour obtenir (IV.9) il suffit d'appliquer la proposition 2 puisque d'après (IV.4) on a $\mathscr{C}(P) \geqslant \max(p_0^2, p_1^2, p_2^2)$ et puisque $\psi_{k-1} > \psi_k$.

Par définition de $\mathscr{L}_k$ on a:

$$\begin{bmatrix}\psi_k\\ \varphi_k\\ \psi_{k-1}\end{bmatrix} = \mathscr{L}_k\cdot\begin{bmatrix}1\\ \alpha_1\\ \alpha_2\end{bmatrix}$$

et donc:

$$\begin{bmatrix}1\\ \alpha_1\\ \alpha_2\end{bmatrix} = \mathscr{S}_k\cdot\begin{bmatrix}\psi_k\\ \varphi_k\\ \psi_{k-1}\end{bmatrix}$$

soit avec $\alpha_0 = 1$:

$$\alpha_i = a_i^{(k)}\psi_k + b_i^{(k)}\varphi_k + c_i^{(k)}\psi_{k-1}, \qquad i = 0, 1, 2.$$

Il en résulte que:

$$\begin{aligned} b_2^{(k)} - \alpha_2 b_0^{(k)} &= \psi_k(b_2^{(k)}a_0^{(k)} - b_0^{(k)}a_2^{(k)}) + \psi_{k-1}(b_2^{(k)}c_0^{(k)} - b_0^{(k)}c_2^{(k)})\\ &= (\det\mathscr{L}_k)^{-1}(-r_1^{(k)}\psi_k + p_1^{(k)}\psi_{k-1}).\end{aligned}$$

Mais d'après (IV.4) pour P_k et P_{k-1} on a:

$$|b_0^{(k)}| = |p_1^{(k)}r_2^{(k)} - p_2^{(k)}r_1^{(k)}| \ll \mathscr{C}(P_k) < \mathscr{C}(P_{k+1}),$$

$$\max(p_1^{(k)2}, p_2^{(k)2}) \ll \mathscr{C}(P_{k+1}), \qquad \max(r_1^{(k)2}, r_2^{(k)2}) \ll \mathscr{C}(P_k) < \mathscr{C}(P_{k+1})$$

et donc d'après les propositions 2 et 4 on a:

$$|b_2^{(k)} - \alpha_2 b_0^{(k)}|\ |b_0^{(k)}|^{1/2} \ll 1$$

ce qui prouve (IV.10) pour $i = 2$. On procède de même pour $i = 1$.

Théorème 3. *Soient α_1, α_2 deux nombres réels d'une extension cubique non totalement réelle vérifiant* (I.5) *et pour $k \geqslant 0$, P_k, Q_k, ψ_k, φ_k, $\alpha_1^{(k)}$, $\alpha_2^{(k)}$ définis aux* I. *Alors la suite $(\alpha_1^{(k)}, \alpha_2^{(k)})_{k\geqslant 0}$ ne prend qu'un nombre fini de valeurs.*

D'après (IV.4) et les propositions 2 et 3 on a:

$$|\mathscr{N}(\psi_k)| \leqslant \delta_1|\psi_k|\mathscr{C}(P_k) \leqslant \delta_1\theta,$$

$$|\mathscr{N}(\varphi_k)| \leqslant \delta_1|\varphi_k|\mathscr{C}(Q_k) \leqslant \delta_1|\psi_{k-1}|\mathscr{C}(Q_k) \leqslant \delta_1\varrho$$

où δ_1, θ, ϱ sont les constantes introduites dans les propositions 2 et 3.

Dans ces inégalités les constantes de droites ne dépendent que de α_1 et α_2 et donc les φ_k et les ψ_k ne prennent qu'un nombre fini de valeurs modulo les unités de $K = \mathbf{Q}(\alpha_1, \alpha_2)$, soient ζ_i, $i = 1, \ldots, N$ une famille de représentants.

D'autre part d'après les propositions 2 et 3 et (IV.5) on a:

$$\alpha_2^{(k)} = \frac{\psi_{k-1}}{\psi_k} = \frac{\psi_{k-1}\mathscr{C}(P_k)}{\psi_k\mathscr{C}(P_k)} \leqslant \theta\delta \quad \text{et} \quad \alpha_2^{(k)} > 1,$$

(IV.11) $$\frac{1}{\alpha_1^{(k)}} = \frac{\psi_k}{\varphi_k} = \frac{\psi_k\mathscr{C}(Q_k)}{\varphi_k\mathscr{C}(Q_k)} \leqslant \theta^3\delta^3 \quad \text{et} \quad \alpha_1^{(k)} \leqslant \alpha_2^{(k)} \leqslant \theta\delta.$$

Soit η_0 une unité fondamentale positive de K.

$$\alpha_2^{(k)} = \eta_0^{u_2}\frac{\zeta_i}{\zeta_j}, \quad \alpha_1^{(k)} = \eta_0^{u_1}\frac{\zeta_h}{\zeta_j}$$

où i, j, h sont des fonctions de k dans $[1, N]$ et u_1, u_2 des entiers dépendants de k.

Les relations (IV.11) permettent de borner les entiers u_2 et u_1. Alors $\alpha_1^{(k)}$ et $\alpha_2^{(k)}$ ne prennent qu'un nombre fini de valeurs.

Références

[1] J. W. S. Cassels, *An introduction to the geometry of numbers*, Springer Verlag, 1959.

[2] H. Minkowski, *Zur Theorie der Kettenbrüche*, Gesammelte Abhandlugen, Vol. I, Teubner, Leipzig 1911, p. 278–292.

[3] O. Perron, *Grundlagen für eine Theorie des Jacobischen Kettenbruchalgorithm*, Math. Ann. 64 (1907), p. 1–76.

[4] W. M. Schmidt, *On simultaneous approximation of two algebraic numbers by rationals*, Acta Math. 119 (1967), p. 27–50.

[5] G. Szekeres, *Multidimensional continued fractions*, Ann. Univ. Sci. Budapest, Eötvos Sect. Math. 13 (1970), p. 113–140.

[6] B. N. Delone and D. K. Faddeev, *The theory of irrationalities of the third degree*, Transl. of Math. Monograph, vol. 10, 1964.

Reçu le 19.1.1979
et dans la forme modifiée le 7.6.1979 (1130)

ACTA ARITHMETICA
XL (1982)

On a conjecture of R. L. Graham

by

R. J. Simpson (Adelaide, S. A., Australia)

Graham [2] has conjectured that if $a_1, a_2, \ldots, a_n$ is any increasing sequence of positive integers, then

$$\max_{1\leqslant i,j\leqslant n}\frac{a_i}{(a_i, a_j)} \geqslant n.$$

Various necessary conditions have been established for a sequence that falsifies the conjecture. Among these are the following:

(1) Not all the a_i are square free (Marica and Schönheim [3]).

(2) n is not a prime (Szemeredi [2]).

(3) $n-1$ is not a prime (Vélez [4]).

(4) If p is a prime, and $p|a_i$ for some i, then $p \leqslant (n-1)/2$ (Boyle [1]).

(5) If any a_i is a prime p then $p = (a_j + a_k)/2$ for some j, k (Weinstein [5]).

In this note we improve (5) by showing:

Theorem. *If $a_1, a_2, \ldots, a_n$ is a sequence that falsifies the conjecture, then no a_i is a prime.*

Proof. The proof is by contradiction. We assume the opposite and separate the sequence in two sets: (i) those integers less than n and (ii) those which are greater than or equal to n.

By (4), p is a member of the first set. It is clear that p must divide each member of the second.

Let $k = \left[\frac{n-1}{p}\right]$, where square brackets denote integer part, let $B = \{b_i\}$ be the set of positive integers which are relatively prime to p and less than n, and let $C = \{c_i\}$ be the set of integers greater than k and less than n. Note that the number of elements of B and the number of elements of C are both equal to $n-k-1$. There are k positive integers less than n and divisible by p.