ACTA ARITHMETICA
XL (1982)

Subsequences of binary recursive sequences

by

J. C. PARNAMI (Chandigarh) and T. N. SHOREY (Bombay)

1. For any sequence of rational integers $u_0, u_1, \ldots, u_m, \ldots$ satisfying $u_m = ru_{m-1} + su_{m-2}$ for integers r, s with $r^2+4s \neq 0$, we have

$$u_m = a\alpha^m + b\beta^m, \quad m = 0, 1, 2, \ldots$$

where α and β are the roots of the polynomial $x^2 - rx - s$ associated to the sequence $\{u_m\}$ and

$$a = \frac{u_0\beta - u_1}{\beta - \alpha}, \quad b = \frac{u_1 - u_0\alpha}{\beta - \alpha}.$$

The sequence $\{u_m\}$ is said to be *non-degenerate binary recursive sequence* if a, b, α and β are non-zero and α/β is not a root of unity. We prove:

THEOREM 1. *Let $u_0, u_1, \ldots, u_m, \ldots$ be a non-degenerate binary recursive sequence. Then there exists an effectively computable number $N > 0$ depending only on the sequence $\{u_m\}$ such that the equation*

$$(1) \qquad u_m = u_n$$

has no solution in non-negative integers m, n with $\max(m, n) > N$ *and $m \neq n$.*

In particular, if $d > \max_{0 \leqslant m \leqslant N} u_m$, then the sequence $\{u_m\}$ can assume the value d at most once only. Compare this with a theorem of Kubota [3]. The proofs of Theorem 1 and all other results of this paper depend on the theory of linear forms in logarithms.

Proof. Put $K = Q(\alpha)$ and denote by $c_1, c_2, \ldots$ effectively computable positive constants depending only on the sequence $\{u_m\}$. Suppose that non-negative integers m, n with $m \neq n$ satisfy (1). It is no loss of generality to assume that $m > n$. We assume that $m > c_1$ with c_1 sufficiently large. If $|\alpha| < |\beta|$ or $|\alpha| > |\beta|$, the theorem follows trivially. Thus we assume that $|\alpha| = |\beta|$. Since α/β is not a root of unity, the numbers α/β and β/α are not integers in K. Thus there exists a prime ideal $\mathfrak{p}$ in K such that $\mathrm{ord}_{\mathfrak{p}}(a/\beta)>0$. Now from (1), we have

$$a\alpha^n(\alpha^{m-n}-1) = b\beta^n(1-\beta^{m-n}).$$

Further

$$c_2+c_3n = \mathrm{ord}_{\mathfrak{p}}\big(b(1-\beta^{m-n})\big) < c_4+c_5\log m.$$

For the last inequality, see Hasse [2], p. 168. Hence, by (1),

(2) $$|a\alpha^m+b\beta^m| < m^{c_6}.$$

The left-hand side of the above inequality does not vanish if c_1 is large enough. Further, by a theorem of Baker [1],

(3) $$|a\alpha^m+b\beta^m| > |\alpha|^m m^{-c_7}.$$

Combining (2), (3) and observing $|\alpha|>1$, we find that $m<c_8$. This completes the proof of Theorem 1.

2. Now we consider the equation $u_m = v_n$ where

$$u_m = a\alpha^m+b\beta^m, \quad v_n = c\gamma^n+d\delta^n \quad (m, n = 0, 1, 2, \ldots)$$

are non-degenerate binary recursive sequences whose associated polynomials have real roots. Assume that

(4) $$|\alpha|<|\beta|, \quad |\gamma|<|\delta|, \quad |\beta|>1, \quad |\delta|>1.$$

Then we have:

LEMMA. *There exists an effectively computable positive number N_0 depending only on a, b, c, d, α, β, γ and δ such that if m, n is a solution of $u_m = v_n$ in non-negative integers, then m, n is either a solution of the system of equations*

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

or

$$\max(m, n) \leqslant N_0.$$

This is a direct consequence of a theorem of Baker [1]. Now we give two applications of the lemma.

THEOREM 2. *Let $u_0, u_1, \ldots, u_m, \ldots$ and $v_0, v_1, \ldots, v_n, \ldots$ be non-degenerate binary recursive sequences whose associated polynomials have real roots. Suppose that $\{v_n\}$ is a subsequence of $\{u_m\}$. Then there exist integers $p>0$ and f depending only on these sequences such that*

$$v_n = u_{pn+f}$$

for all integers $n>|f|$.

Similar result was proved by Mignotte [4].

Proof. Since $\{v_n\}$ is a subsequence of $\{u_m\}$, there exist positive integers m_1 and m_2 such that

$$u_{m_1} = v_{N_0+1}, \quad u_{m_2} = v_{N_0+2}.$$

Now the lemma gives

$$a\alpha^{m_1} = c\gamma^{N_0+1}, \quad b\beta^{m_1} = d\delta^{N_0+1}$$
$$a\alpha^{m_2} = c\gamma^{N_0+2}, \quad b\beta^{m_2} = d\delta^{N_0+2}.$$

These equations give

$$\gamma = \alpha^p, \quad \delta = \beta^p$$

with $p = m_2-m_1$. From (4), we find that $p>0$. Put

$$f = m_1-p(N_0+1).$$

Now, for $n>|f|$, we have

$$v_n = c\gamma^n+d\delta^n = a\alpha^{pn+f}+b\beta^{pn+f} = u_{pn+f}.$$

This completes the proof of Theorem 2.

Now we apply the lemma to prove:

THEOREM 3. *Suppose that $u_0, u_1, \ldots, u_m, \ldots$ and $v_0, v_1, \ldots, v_n, \ldots$ are non-degenerate binary recursive sequences with infinitely many terms in common. Assume that the roots of their associated polynomials are positive. Then they are subsequences of a sequence $W_0, W_1, \ldots, W_l, \ldots$ where $\{r'W_l\}$ is a non-degenerate binary recursive sequence for a fixed integer r' depending only on the sequences $\{u_m\}$ and $\{v_n\}$. Further the polynomial associated to $\{r'W_l\}$ has positive roots.*

Proof. Proceed similarly as in Theorem 2 to conclude that there exist relatively coprime positive integers p and q such that $\alpha^p = \gamma^q$, $\beta^p = \delta^q$. Since $(p, q) = 1$, there exist integers u, v such that $pu+qv = 1$. Therefore

$$\alpha = \alpha^{pu+qv} = (\gamma^u\alpha^v)^q = \eta^q, \quad \text{where} \quad \eta = \gamma^u\alpha^v.$$

Now

$$\gamma^q = \alpha^p = \eta^{pq},$$

which implies that

$$\gamma = \eta^p.$$

Similarly

$$\beta = \varrho^q, \quad \delta = \varrho^p, \quad \text{where} \quad \varrho = \delta^u\beta^v.$$

There exist positive integers m_0, n_0 such that $a\alpha^{m_0} = c\gamma^{n_0}$ and $b\beta^{m_0} = d\delta^{n_0}$. This follows from the lemma. Put $D = m_0q-n_0p$. Then

$$c/a = \eta^D, \quad d/b = \varrho^D.$$

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:

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

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

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