Acta Math. Hung.
57 (3—4) (1991), 201—211.

ON GENERALIZED LEHMER SEQUENCES

BUI MINH PHONG (Budapest)*

1. Introduction

Let $G=G(G_0, G_1, A, B)=\{G_n\}_0^\infty$ be a second order linear recurrence defined by integer constants G_0, G_1, A, B and the recurrence

$$G_n = AG_{n-1}-BG_{n-2} \quad (n>1), \tag{1}$$

where $AB\neq 0$, $D=A^2-4B\neq 0$ and $|G_0|+|G_1|\neq 0$. If $G_0=0$ and $G_1=1$, then we denote the sequence $G(0, 1, A, B)$ by $R=R(A, B)$. The sequence R is called Lucas sequence and R_n is called a Lucas number.

In 1930 D. H. Lehmer [2] generalized some results of Lucas on the divisibility properties of Lucas numbers to the terms of the sequence $U=U(L, M)=\{U_n\}_0^\infty$ which is defined by integer constants $L, M, U_0=0$, $U_1=1$ and the recurrence

$$U_n = \begin{cases} LU_{n-1}-MU_{n-2} & \text{for } n \text{ odd} \\ U_{n-1}-MU_{n-2} & \text{for } n \text{ even,} \end{cases}$$

where $LM\neq 0$ and $K=L-4M\neq 0$. The sequence U is called a Lehmer sequence and U_n is a Lehmer number. It should be observed that Lucas numbers are also Lehmer numbers up to a multiplicative factor.

Here we shall define generalized Lehmer sequences. Let H_0, H_1, L and M be integers with the conditions $LM\neq 0$, $K=L-4M\neq 0$ and $|H_0|+|H_1|\neq 0$. A generalized Lehmer sequence is a sequence $H_0, H_1, \ldots, H_n, \ldots$ of integers satisfying a relation

$$H_n = \begin{cases} LH_{n-1}-MH_{n-2} & \text{for } n \text{ odd} \\ H_{n-1}-MH_{n-2} & \text{for } n \text{ even.} \end{cases} \tag{2}$$

We shall denote it by $H=H(H_0, H_1, L, M)=\{H_n\}_{n=0}^\infty$, and so $H(0, 1, L, M)$ is the Lehmer sequence $U(L, M)$.

The purpose of this paper is to study the properties of the generalized Lehmer sequences $H(H_0, H_1, L, M)$. We show that the terms of sequences G are also terms of sequences H up to a multiplicative factor and we give and explicit form of H_n. We improve a result of P. Kiss [1] concerning the zero terms in the sequences G and H. Furthermore we give lower and upper bounds for the terms of the sequences H.

* Research (partially) supported by Hungarian National Foundation for Scientific Research Grant No. 907.

2. Preliminary results

Throughout this paper we shall use the notation

$$\varepsilon(n)=\begin{cases}1 & \text{for } n \text{ odd}\\ 0 & \text{for } n \text{ even.}\end{cases}$$

Using the function $\varepsilon(n)$, the relation (2) can be written in the form

$$H_n = L^{\varepsilon(n)} H_{n-1} - MH_{n-2} \quad (\text{for } n > 1). \tag{3}$$

We prove some properties of the sequence $H(H_0, H_1, L, M)$.

PROPOSITION 1. *If* $H_0=G_0$, $H_1=AG_1$, $L=A^2$ *and* $M=B$, *then*

$$G_n(G_0, G_1, A, B) = A^{-\varepsilon(n)} H_n(G_0, AG_1, A^2, B) \tag{4}$$

for any $n \geqq 0$.

PROOF. We shall prove (4) by induction on n. The statement is obvious for $n=0$ and $n=1$. If (4) is true for $n-1$ and n $(n \geqq 1)$, then using (1) and (3), we have

$$G_{n+1} = AG_n - BG_{n-1} = A^{\varepsilon(n+1)+\varepsilon(n)} G_n - BA^{\varepsilon(n-1)-\varepsilon(n+1)} G_{n-1} =$$

$$= A^{-\varepsilon(n+1)} [A^{2\varepsilon(n+1)} H_n - BH_{n-1}] = A^{-\varepsilon(n+1)} [L^{\varepsilon(n+1)} H_n - MH_{n-1}] = A^{-\varepsilon(n+1)} H_{n+1},$$

which proves the assertion.

REMARKS. a) From Proposition 1 it follows that the sequences $H(H_0, H_1, L, M)$ are more general than the sequences $G(G_0, G_1, A, B)$.

b) In particular we have

$$R_n(A, B) = A^{-\varepsilon(n)} H_n(0, A, A^2, B) = A^{1-\varepsilon(n)} U_n(A^2, B). \tag{5}$$

PROPOSITION 2. *If* $U_n=U_n(L, M)$ *and* $H_n=H_n(H_0, H_1, L, M)$ *then*

$$H_n = H_1 U_n - L^{\varepsilon(n)} MH_0 U_{n-1} \tag{6}$$

for any $n \geqq 0$ *with the convention* $MU_{-1}=-1$.

PROOF. From the definition of the sequences U and H, (6) is obvious for $n=0$ and $n=1$. Suppose that (6) is true for $n-1$ and n. Then by (3) using that $\varepsilon(n+1)= =\varepsilon(n-1)$ we have

$$H_{n+1} = L^{\varepsilon(n+1)} H_n - MH_{n-1} = L^{\varepsilon(n+1)} [H_1 U_n - L^{\varepsilon(n)} MH_0 U_{n-1}] -$$

$$- M[H_1 U_{n-1} - L^{\varepsilon(n-1)} MH_0 U_{n-2}] = H_1 [L^{\varepsilon(n+1)} U_n - MU_{n-1}] -$$

$$- L^{\varepsilon(n+1)} MH_0 [L^{\varepsilon(n)} U_{n-1} - MU_{n-2}] = H_1 U_{n+1} - L^{\varepsilon(n+1)} MH_0 U_n,$$

which proves (6) by induction on n.

PROPOSITION 3. *Let α and β be the roots of the equation $z^2-\sqrt{L}\,z+M=0$. If $a=H_1-\sqrt{L}\,H_0\beta$ and $b=H_1-\sqrt{L}\,H_0\alpha$, then we have*

$$H_n(H_0, H_1, L, M) = (\sqrt{L})^{\varepsilon(n)}\frac{a\alpha^n-b\beta^n}{\alpha^2-\beta^2}. \tag{7}$$

PROOF. It is well-known that

$$U_n = U_n(L, M) = (\sqrt{L})^{\varepsilon(n)}\frac{\alpha^n-\beta^n}{\alpha^2-\beta^2} \tag{8}$$

(see e.g. [7]). Since $\alpha+\beta=\sqrt{L}$ and $\alpha\beta=M$, using (6) and (8) we get

$$H_n = H_1U_n-L^{\varepsilon(n)}MH_0U_{n-1} =$$
$$= \frac{H_1(\sqrt{L})^{\varepsilon(n)}(\alpha^n-\beta^n)-L^{\varepsilon(n)}H_0(\alpha^n\beta-\alpha\beta^n)(\sqrt{L})^{\varepsilon(n-1)}}{\alpha^2-\beta^2} =$$
$$= \frac{(\sqrt{L})^{\varepsilon(n)}}{\alpha^2-\beta^2}\left[(H_1-\sqrt{L}H_0\beta)\alpha^n-(H_1-\sqrt{L}H_0\alpha)\beta^n\right] =$$
$$= (\sqrt{L})^{\varepsilon(n)}\frac{a\alpha^n-b\beta^n}{\alpha^2-\beta^2},$$

where $a=H_1-\sqrt{L}H_0\beta$ and $b = H_1-\sqrt{L}H_0\alpha$.

REMARKS. a) From (4) and (7) we get the well-known formula

$$G_n(G_0, G_1, A, B) = \frac{c\delta^n-d\gamma^n}{\delta-\gamma}, \tag{9}$$

where δ and γ are the roots of the equation $x^2-Ax+B=0$ and $c=G_1-G_0\gamma$, $d=G_1-G_0\delta$ (see e.g. [5]).

b) In what follows we say that the sequences $G(G_0, G_1, A, B)$ and $H(H_0, H_1, L, M)$ are non-degenerate if $cd\delta\gamma\neq 0$, δ/γ and $ab\alpha\beta\neq 0$, α/β are not roots of unity, respectively.

PROPOSITION 4. *For any $n\geqq 0$*

$$H_n(H_0, H_1, L, M) = -i^{n+\varepsilon(n)}H_n(-H_0, H_1, -L, -M), \tag{10}$$

where $i^2=-1$.

PROOF. We shall prove (10) by induction on n. Our statement is obvious for $n=0$ and $n=1$. If (10) is true for $n-1$ and n, then using (3) and $i^2=-1$, we have

$$H_{n+1}(H_0, H_1, L, M) = H_{n+1} = L^{\varepsilon(n+1)}H_n-MH_{n-1} =$$
$$= i^{2\varepsilon(n+1)}(-L)^{\varepsilon(n+1)}(-i^{n+\varepsilon(n)})H_n(-H_0, H_1, -L, -M)-$$
$$-M(-i^{n-1+\varepsilon(n-1)})H_{n-1}(-H_0, H_1, -L, -M) =$$
$$= -i^{n+1+\varepsilon(n+1)}[(-L)^{\varepsilon(n+1)}H_n(-H_0, H_1, -L, -M)-$$
$$-(-M)H_{n-1}(-H_0, H_1, -L, -M)] = -i^{(n+1)+\varepsilon(n+1)}H_{n+1}(-H_0, H_1, -L, -M),$$

which proves (10).

PROPOSITION 5. *Let $d=(L, M)$, $L'=L/d$ and $M'=M/d$. Then*

$$H_n(H_0, H_1, L, M) = (\sqrt{d})^{n+\varepsilon(n)-2} H_n(dH_0, H_1, L', M'). \tag{11}$$

PROOF. If α and β are roots of $z^2-\sqrt{L}\,z+M=0$, then $\alpha_1=\alpha/\sqrt{d}$ and $\beta_1=\beta/\sqrt{d}$ are roots of $z^2-\sqrt{L'}\,z+M'=0$. Let

$$a = H_1-\sqrt{L}H_0\beta, \quad b = H_1-\sqrt{L}H_0\alpha,$$

and

$$a_1 = H_1-\sqrt{L'}(dH_0)\,\beta_1, \quad b_1 = H_1-\sqrt{L'}(dH_0)\,\alpha_1.$$

It can be easily seen that $a_1=a$, $b_1=b$. Thus by (7) we have

$$H_n(H_0, H_1, L, M) = (\sqrt{L})^{\varepsilon(n)} \frac{a\alpha^n-b\beta^n}{\alpha^2-\beta^2} = (\sqrt{d})^{\varepsilon(n)+n-2}(\sqrt{L'})^{\varepsilon(n)}\cdot\frac{a\alpha_1^n-b\beta_1^n}{\alpha_1^2-\beta_1^2} =$$

$$= (\sqrt{d})^{n+\varepsilon(n)-2}\cdot(\sqrt{L'})^{\varepsilon(n)} \frac{a_1\alpha_1^n-b_1\beta_1^n}{\alpha_1^2-\beta_1^2} = (\sqrt{d})^{n+\varepsilon(n)-2}\cdot H_n(dH_0, H_1, L', M'),$$

which proves (11).

3. Zero terms in the sequences H

Some authors have studied the lower and upper bounds for the terms of non-degenerate sequences $G=G(G_0, G_1, A, B)$. Let γ and δ be the roots of the equation $x^2-Ax+B=0$. We can assume that $|\gamma|\geqq|\delta|$. In [3] K. Mahler proved that if $D=A^2-4B<0$ and ε is a positive constant, then there is an effectively computable constant n_0 depending only on ε such that

$$|G_n| \geqq |\gamma|^{(1-\varepsilon)n} \quad \text{for} \quad n > n_0.$$

From a result of T. N. Shorey and C. L. Stewart [6] it follows that

$$|G_n| \geqq |\gamma|^{n-c_1 \log n}$$

for $n>c_2$, where c_1, c_2 are positive numbers which are effectively computable in terms of G_0, G_1, A and B.

A similar result was obtained by M. Mignotte [4] for linear recurrences of higher order.

In [1] P. Kiss gave the explicit value of the constants proving that $G_n\neq 0$ for $n>n_1$, where

$$n_1 = \max\left[2^{510}(\log|8B|)^{25}, \frac{4}{\log 2}\left(\log|G_0|+\log 4\sqrt{|D|}\right)\right],$$

furthermore if $D<0$ and $n>n_1$, then

$$\frac{|c|}{2\sqrt{|D|}}|\gamma|^n n^{-c_3} < |G_n| \leqq \frac{2|c|}{\sqrt{|D|}}|\gamma|^n,$$

where $c=G_1-G_0\gamma$ and

$$c_3 = 2e\cdot 200^{40}\log|8B|\cdot(1+\log\log|8B|)\cdot\log|16B|(G_0^2+G_1^2).$$

We extend the results mentioned above to the sequences $H(H_0, H_1, L, M)$. We give necessary and sufficient conditions for sequences H which have zero terms, and give lower and upper bounds for the terms. These improve the reults of P. Kiss [1].

THEOREM 1. *Let $H=H(H_0, H_1, L, M)$ be a non-degenerate generalized Lehmer sequence with $(L, M)=1$ and $(H_0, H_1)=h$. Then the following statements are equivalent:*

(i) $H_n = 0 \quad (n \geqq 0)$,

(ii) $H_0 = \varrho h U_n, \quad H_1 = \varrho h L^{\varepsilon(n)} M U_{n-1}$,

(iii) $H_k = \varrho h L^{\varepsilon(n)\varepsilon(k)} M^k U_{n-k}$ *for* $k = 0, 1, \dots, n$,

where $U_n = U_n(L, M)$, $MU_{-1} = -1$, *and* $\varrho = 1$ *or* $\varrho = -1$.

COROLLARY. *Let $H=H(H_0, H_1, L, M)$ be a non-degenerate generalized Lehmer sequence with $(L, M)=d$. Then $H_n=0$ if and only if*

$$(\sqrt{d})^{n+\varepsilon(n)} H_0 = \pm(dH_0, H_1)\, U_n,$$

and

$$(\sqrt{d})^{n+\varepsilon(n)} H_1 = \pm(dH_0, H_1) L^{\varepsilon(n)} M U_{n-1},$$

where $U_n = U_n(L, M)$.

THEOREM 2. *Let $H=H(H_0, H_1, L, M)$ be a non-degenerate generalized Lehmer sequence with $(L, M)=d$.*

If $LK>0$ then $H_n \neq 0$ for $n > \max[13, \min(|H_0|+1, |H_1|+2)]$.

If $LK<0$ then $H_n \neq 0$ for $n > \max(N_1, N_2) = N_0$, where

$$N_1 = \min(2^{67} \log|4M|, e^{398})$$

and

$$N_2 = \min\left[\frac{4}{\log 2}\log|dH_0|, \frac{4}{\log 2}\log|H_1|\right].$$

THEOREM 3. *Let $H=H(H_0, H_1, L, M)$ be a non-degenerate generalized Lehmer sequence with condition $LK<0$. Then for*

$$n > 2^{67}\log|4M|(H_0^2+H_1^2)$$

we have

$$\frac{|a|}{2\sqrt{|LK|}}|\alpha|^n n^{-c_0} < |H_n| < \frac{2|a|}{\sqrt{|K|}}|\alpha|^n,$$

where

$$c_0 = 2^{80}\log|4M|\cdot\log\log|4M|\cdot\log|4M|(H_0^2+H_1^2),$$

and α is any solution of $z^2-\sqrt{L}z+M=0$.

PROOF OF THEOREM 1. Let first $H_n=0$ for an integer $n \geqq 0$. If $n=0$ or $n=1$ then (ii) follows easily. Suppose $n>1$. By (6) $H_n=0$ implies that

$$H_1 U_n = L^{\varepsilon(n)} M H_0 U_{n-1},$$

from which it follows

$$H_1' U_n = L^{\varepsilon(n)} M H_0' U_{n-1}, \tag{12}$$

where $H_0' = H_1/h$ and $H_0' = H_0/h$. Since $(L, M) = 1$, it can be easily seen that $(U_n, L^{\varepsilon(n)}) = 1$, $(U_n, M) = 1$ and $(U_n, U_{n-1}) = 1$. Thus by (12) we get

$$H_0 = \pm h \cdot U_n \quad \text{and} \quad H_1 = \pm h \cdot L^{\varepsilon(n)} \cdot M U_{n-1},$$

which proves that (i) implies (ii).

Now we prove that (ii) implies (iii). Suppose

$$H_0 = h \cdot U_n \quad \text{and} \quad H_1 = h \cdot L^{\varepsilon(n)} M U_{n-1}.$$

Thus (iii) is true for $k=0$ and $k=1$. If (iii) is true for $k-1$ and k, where $k<n$, and $\varrho=1$, then from (3) we have

$$H_{k+1} = L^{\varepsilon(k+1)} H_k - M H_{k-1} =$$

$$= L^{\varepsilon(k+1)} h L^{\varepsilon(n)\varepsilon(k)} M^k U_{n-k} - M h L^{\varepsilon(n)\varepsilon(k-1)} M^{k-1} U_{n-k+1} =$$

$$= h L^{\varepsilon(n)\varepsilon(k+1)} M^k [L^{\varepsilon(n-k+1)} U_{n-k} - U_{n-k+1}] = h L^{\varepsilon(n)\varepsilon(k+1)} M^{k+1} U_{n-(k+1)},$$

since

$$\varepsilon(k+1) + \varepsilon(n)\varepsilon(k) - \varepsilon(n)\varepsilon(k+1) = \varepsilon(n-k+1)$$

and

$$\varepsilon(k+1) = \varepsilon(k-1).$$

This proves (iii) in the case $\varrho=1$. If $\varrho=-1$, then we can similarly show that (ii) implies (iii).

Finally (i) follows clearly from (iii) with $k=n$. $\square$

Proof of the Corollary. Let $d=(L, M)$ and $L'=L/d$, $M'=M/d$. By (11) it can be easily seen that $H_n = H_n(H_0, H_1, L, M) = 0$ if and only if $H_n(dH_0, H_1, L', M') = 0$. From Theorem 1 we obtain that $H_n=0$ if and only if

$$dH_0 = \pm(dH_0, H_1) U_n(L', M') \quad \text{and} \quad H_1 = \pm(dH_0, H_1) L'^{\varepsilon(n)} M' U_{n-1}(L', M'). \tag{13}$$

Since

$$U_n(L, M) = (\sqrt{d})^{n+\varepsilon(n)-2} \cdot U_n(L', M'),$$

by (13) and its conclusion we have

$$(\sqrt{d})^{n+\varepsilon(n)} H_0 = \pm(dH_0, H_1) U_n(L, M)$$

and

$$(\sqrt{d})^{n+\varepsilon(n)} H_1 = \pm(dH_0, H_1) L^{\varepsilon(n)} M U_{n-1}(L, M),$$

which proves the corollary.

Before proving Theorem 2 we introduce some notations and recall some results due to M. Waldschmidt [8], M. Ward [9] and C. L. Stewart [7].

Denote

$$a_0 x^N + \ldots + a_N = a_0 \prod_{i=1}^{N} (x - \alpha_i) \in \mathbf{Z}[x]$$

the minimal polynomial of an algebraic number $\alpha=\alpha_1$. Put

$$M(\alpha)=|a_0|\cdot\prod_{i=1}^{N}\max\{1,|\alpha_i|\}$$

and

$$h(\alpha)=\frac{1}{N}\log M(\alpha).$$

THEOREM A (M. Waldschmidt [8]). *Let $\alpha_1,\ldots,\alpha_m$ be non-zero algebraic numbers, and let $\beta_0,\beta_1,\ldots,\beta_m$ be algebraic numbers. For $1\leqq i\leqq m$ let $\log\alpha_i$ be any determination of the logarithm of α_i. Let D be a positive integer, and let $V_1,\ldots,V_m, W, E$ be positive real numbers, satisfying*

$$D\geqq[Q(\alpha_1,\ldots,\alpha_m,\beta_0,\beta_1,\ldots,\beta_m):Q],$$

$$V_i\geqq\max\{h(\alpha_i),\ |\log\alpha_i|/D,\ 1/D\},\quad 1\leqq i\leqq m,$$

$$W\geqq\max_{0\leqq i\leqq m}\{h(\beta_i)\},\quad V_1\leqq\ldots\leqq V_m$$

and

$$1<E\leqq\min\left[e^{DV_1};\ \min_{1\leqq i\leqq m}\{4DV_i/|\log\alpha_i|\}\right].$$

Finally define $V_i^+=\max\{V_i,1\}$ for $i=m$ and $i=m-1$, with $V_0^+=1$ in the case $m=1$. If the number

$$\Lambda:=\beta_0+\beta_1\log\alpha_1+\ldots+\beta_m\log\alpha_m$$

does not vanish, then

$$|\Lambda|>\exp\left\{-c(m)D^{m+2}V_1\ldots V_m(W+\log(EDV_m^+))(\log EDV_{m-1}^+)(\log E)^{-m-1}\right\}$$

where $c(1)\leqq 2^{35}$, $c(2)\leqq 2^{53}$, $c(3)\leqq 2^{71}$ and $c(m)\leqq 2^{8m+51}\cdot m^{2m}$ for $m>3$.

We shall use a result of C. L. Stewart [7] on a linear form in two logarithms. Let α be an algebraic number of height at most A $(\geqq 4)$ and degree d; further let b_1 and b_2 denote integers with absolute values at most B $(\geqq 4)$. Set

$$\Lambda=b_1\log(-1)+b_2\log\alpha,$$

where the logarithms are assumed to take their principal values.

THEOREM B (C. L. Stewart [7]). *If $\Lambda\neq 0$ then $|\Lambda|>\exp(-C\log A\log B)$, where $C=2^{435}\cdot(3d)^{49}$.*

Finally, we recall a result due to M. Ward [9] on primitive prime divisors of Lehmer numbers. Recall that a primitive prime divisors of the Lehmer number $U_n(L,M)$ is a prime dividing U_n but it does not divide $LKU_3\ldots U_{n-1}$, where $K=L-4M$.

THEOREM C (M. Ward [9]). *Let $U(L,M)$ be a non-degenerate Lehmer sequence with conditions $L>0$ and $K>0$. Then $U_n(L,M)$ has a primitive prime divisor for $n>12$. Every primitive prime divisor of $U_n(L,M)$ is of the form $nx\pm 1$.*

Now we prove the following result.

LEMMA. *Let* $U(L, M)$ *be a non-degenerate Lehmer sequence with conditions* $L>0$ *and* $K<0$. *Then* $M \geqq 2$ *and*

$$|U_n(L, M)| > M^{n/4} \tag{14}$$

for

$$n > \min(2^{67} \log 4M, e^{398}) =: N_1.$$

PROOF. Since $L>0$ and $U(L, M)$ is a non-degenerate Lehmer sequence, we have

$$\langle L, M\rangle \neq \langle 1, 1\rangle, \langle 2, 1\rangle, \langle 3, 1\rangle, \langle 4, 1\rangle.$$

Thus if $K=L-4M<0$ then $M \geqq 2$.

Let α and β be the roots of $z^2-\sqrt{L}z+M=0$. By our conditions we obtain

$$|\alpha| = |\beta| = \sqrt{M}. \tag{15}$$

By (8) we have

$$|U_n| = |U_n(L, M)| = \left|(\sqrt{L})^{\varepsilon(n)} \frac{\alpha^n-\beta^n}{\alpha^2-\beta^2}\right| \geqq \tag{16}$$

$$\geqq \frac{|\alpha|^n}{\sqrt{L|K|}} \left|1-\left(\frac{\beta}{\alpha}\right)^n\right| \geqq \frac{|\alpha|}{2\sqrt{L|K|}} \left|t \log(-1) - n \log \frac{\beta}{\alpha}\right|$$

where log denotes the principal value of the logarithm function and $|t| \leqq 2n$, because $\left|1-\left(\frac{\beta}{\alpha}\right)^n\right|$ is the length of a chord of the unit circle which is greater than the half of the smaller circular arc. Set

$$\Lambda := t \log(-1) - n \log \frac{\beta}{\alpha}. \tag{17}$$

Since β/α is not a root of unity, we have $\Lambda \neq 0$.

First we prove that (14) holds if $n > 2^{67} \log 4M$. We apply Theorem A to (17). In this case $m=2$, $W=\log 2n$; $\alpha_1=-1$, $M(\alpha_1)=1$, $h(\alpha_1)=0$; $\alpha_2=\beta/\alpha$, $M(\alpha_2)=M$. The algebraic number $\alpha_2=\beta/\alpha$ is a root of the equation

$$Mx^2-(L-2M)x+M = 0$$

so $h(\alpha_2) = \frac{1}{2} \log M$. From these

$$D = 2, \quad V_1 = V_1^+ = \frac{\pi}{2}, \quad V_2 = V_2^+ = \log 4M, \quad E = 4$$

follow. By Theorem A we have

$$|\Lambda| > \exp\left\{-c(2) \cdot 2^4 \frac{\pi}{2} \log 4M \left(\log 2n + \log(8 \log 4M)\right) \cdot \log 4\pi \cdot (\log 4)^{-3}\right\} >$$

$$> \exp\left\{-9 \cdot 2^{56} \cdot \log M \left(\log 2n + \log(8 \log 4M)\right)\right\},$$

and so if $n > 4\log 4M$ then

$$(18)\qquad |\Lambda| > \exp\{-9\cdot 2^{57}\cdot\log M\cdot\log 2n\} = M^{-9\cdot 2^{57}\cdot\log 2n}.$$

On the other hand it follows from $0<L<4M$ that

$$|K| \leqq |L-2M|+2M \leqq 2M+2M = 4M,$$

and so

$$(19)\qquad \frac{1}{2\sqrt{L|K|}} > \frac{1}{2\sqrt{4M\cdot 4M}} = \frac{1}{8M} \geqq M^{-4}.$$

By (15), (16), (18) and (19) we get

$$(20)\qquad |U_n| > M^{n/2-9\cdot 2^{57}\cdot\log 2n-4}$$

for $n > 4\log 4M$; furthermore a short calculation shows that

$$(21)\qquad \frac{n}{2}-9\cdot 2^{57}\log 2n-4 > \frac{n}{4}$$

if $n > 2^{68}$.

Thus by (20) and (21)

$$(22)\qquad |U_n| > M^{n/4}$$

for $n > 2^{67}\log 4M$.

Now we prove that (14) holds if $n > e^{398}$. We apply Theorem B to (17). It is easily seen that in our case $A=2M$ and $B=2n$, furthermore $d=2$. From Theorem B we get

$$(23)\qquad |\Lambda| = \left|t\log(-1)-n\log\frac{\beta}{\alpha}\right| > \exp(-2^{484}\cdot 3^{49}\cdot\log 2M\cdot\log 2n) \geqq$$

$$\geqq \exp(-2^{485}\cdot 3^{49}\cdot\log M\cdot\log 2n) = M^{-2^{485}\cdot 3^{49}\cdot\log 2n}.$$

Thus by (15), (16), (19) and (23) we obtain

$$|U_n| > M^{n/2-2^{485}\cdot 3^{49}\log 2n-4},$$

and so

$$(24)\qquad |U_n| > M^{n/4}$$

if $n > e^{398}$.

By (22) and (24)

$$|U_n| > M^{n/4} \quad \text{if} \quad n > \min(2^{67}\log 4M, e^{398}) = N_1,$$

which proves the Lemma. □

PROOF OF THEOREM 2. Let $H_n = H_n(H_0, H_1, L, M) = 0$. By Proposition 4 we can assume without any essential loss of generality that $L > 0$.

First we assume that $K > 0$. By Theorem C and the Corollary of Theorem 1, if $n > 13$ then U_n has a primitive divisor of the form $nx\pm 1$ which divides H_0; and U_{n-1} has a primitive divisor of the form $(n-1)y\pm 1$ dividing H_1. Thus

$$n \leqq |H_0|+1 \quad\text{and}\quad n \leqq |H_1|+2,$$

from which

$$n \leqq \min(|H_0|+1, |H_1|+2) =: N_3$$

follows. This implies that $H_n \neq 0$ if $n > \max(13, N_3)$.

Now let $K<0$. If $(L, M)=1$, then by Theorem 1 we have

$$H_0 = \pm(H_0, H_1)\, U_n \quad \text{and} \quad H_1 = \pm(H_0, H_1) L^{\varepsilon(n)} M U_{n-1}.$$

If $n \geqq N_1$, then by the Lemma

$$|H_0| \geqq |U_n| > M^{n/4} \geqq 2^{n/4}$$

and

$$|H_1| \geqq |MU_{n-1}| > M \cdot M^{(n-1)/4} > 2^{n/4}$$

which imply

$$n < \min\left(\frac{4}{\log 2}\log|H_0|, \frac{4}{\log 2}\log|H_1|\right) := N_4.$$

Thus $H_n \neq 0$ if $n \geqq \max(N_1, N_4)$.

Finally let $K<0$ and $(L, M)=d$. By Proposition 5 it follows that

$$H_n(H_0, H_1, L, M) = 0 \quad \text{if and only if} \quad H_n(dH_0, H_1, L/d, M/d) = 0.$$

But we have proved that if $H_n(dH_0, H_1, L/d, M/d)=0$ and $n > N_1$, then

$$n < \min\left(\frac{4}{\log 2}\log|dH_0|, \frac{4}{\log 2}\log|H_1|\right) =: N_2.$$

Thus $H_n(H_0, H_1, L, M) \neq 0$ if $n > \max(N_1, N_2) =: N_0$.

Proof of Theorem 3. As in the proof of Theorem 2 we can assume without any essential loss of generality that $L>0$.

Let $K<0$ and $n>N_0$ (N_0 is defined in Theorem 2) and so $|H_n|>0$. The numbers $a=H_1-\sqrt{L}H_0\beta$, $b=H_1-\sqrt{L}H_0\alpha$ are complex conjugates therefore — as in the proof of the Lemma — for some integer t

$$(25) \qquad |H_n| = \left|(\sqrt{L})^{\varepsilon(n)}\frac{a\alpha^n - b\beta^n}{\alpha^2-\beta^2}\right| \geqq \frac{|a|\,|\alpha|^n}{\sqrt{|LK|}}\left|1-\frac{b}{a}\left(\frac{\beta}{\alpha}\right)^n\right| \geqq$$

$$\geqq \frac{|a|\,|\alpha|^n}{2\sqrt{|LK|}}\left|t\log(-1) - n\log\frac{\beta}{\alpha} - \log\frac{b}{a}\right|,$$

where the logarithms take their principal values and $t \leqq 2n+2$.

Theorem A can be applied to

$$0 \neq \Lambda = t\log(-1) - n\log\frac{\beta}{\alpha} - \log\frac{b}{a}.$$

In this case $m=3$, $W=2\log n$, $\alpha_1=-1$, $\alpha_2=\beta/\alpha$, $\alpha_3=b/a$, $D=2$ since a/b is a root of $ux^2-vx+u=0$, where

$$u = H_1^2 - LH_0H_1 + LMH_0^2, \quad v = 2H_1^2 - 2LH_0H_1 + L^2H_0^2 + 2LMH_0^2.$$

Using these, $V_1=\pi/2$, $V_2=V_2^+=\log 4M$, $V_3=V_3^+=2\log 4M(H_0^2+H_1^2)$ and $E=4$ follow. Thus for $n>N_0$ we have

$$|\Lambda|>\exp\{-c_4\log 4M\cdot\log(8\log 4M)\cdot\log(4M(H_0^2+H_1^2))\times \times(2\log n+\log 16\log 4M(H_0^2+H_1^2))\},$$

where

$$c_4=0{,}86\cdot 2^{76}>c(3)2^5\cdot\frac{\pi}{2}\cdot 2\cdot(\log 4)^{-4}.$$

Since $\log(8\log 4M)<4\log\log 4M$, we have

$$(26)\quad |\Lambda|>\exp\{-4c_4\log 4M\log\log 4M\log 4M(H_0^2+H_1^2)(2\log n+\log n)\}= = n^{-12c_4\log 4M\cdot\log\log 4M\cdot\log 4M(H_0^2+H_1^2)},$$

if $n>2^{67}\cdot\log 4M(H_0^2+H_1^2)(\geqq N_0)$.

Thus, by (25) and (26), we get

$$|H_n|>\frac{|a|\cdot|\alpha|^n}{2\sqrt{|LK|}}\cdot n^{-c_0}$$

for $n>2^{56}\cdot\log 4M(H_0^2+H_1^2)$, where

$$c_0=2^{80}\log 4M\cdot\log\log 4M\cdot\log 4M(H_0^2+H_1^2)> >12c_4\log 4M\cdot\log\log 4M\cdot\log 4M(H_0^2+H_1^2),$$

which proves the first inequality of Theorem 3. The second inequality is obvious by the explicit form of H_n.

References

[1] P. Kiss, Zero terms in second order linear recurrences, *Math. Seminar Notes (Kobe Univ.)*, **7** (1979), 145—152.

[2] D. H. Lehmer, An extended theory of Lucas' functions, *Ann. Math.*, **31** (1930), 419—448.

[3] K. Mahler, A remark on recursive sequences, *Jour. Math. Sci.*, **1** (1966), 12—17.

[4] M. Mignotte, A note on linear recursive sequences, *Jour. Austral. Math. Soc.*, **20** (1975), 242—244.

[5] I. Niven and H. S. Zuckerman, *An introduction to the theory of numbers*, J. Wiley (New York, 1960).

[6] T. N. Shorey and C. L. Stewart, On the Diophantine equations $ax^{2t}+bx^ty+cy^2=d$ and pure powers in recurrence sequences, *Math. Scand.*, **52** (1983), 24—36.

[7] C. L. Stewart, Primitive divisors of Lucas and Lehmer numbers, *Transcendence theory: Advances and Applications*, Proceedings of the Conference (Cambridge, 1976), London—New York—San Francisco, 1977.

[8] M. Waldschmidt, A lower bound for linear forms in logarithms, *Acta Arith.*, **37** (1979), 257—283.

[9] M. Ward, The intrinsic divisors of Lehmer numbers, *Ann. of Math.*, **2 (62)** (1955), 230—236.

(Received September 8, 1987)

EÖTVÖS LORÁND UNIVERSITY
COMPUTER CENTER
BOGDÁNFY U. 10/B
1117 BUDAPEST, HUNGARY