MATHEMATICS OF COMPUTATION
VOLUME 51, NUMBER 183
JULY 1988, PAGES 315-323

A Lower Bound for the Counting Function of Lucas Pseudoprimes*

By P. Erdős, P. Kiss, and A. Sárközy

Abstract. We show that there is an absolute constant c such that, for any nondegenerate Lucas sequence, the number of Lucas pseudoprimes not exceeding x is greater than $\exp\{(\log x)^c\}$ if x is sufficiently large.

1. Introduction and Summary of Results. Let $R = \{R_n\}_{n=0}^{+\infty}$ be a *Lucas sequence defined by the recursion*

$$R_n = AR_{n-1} - BR_{n-2}$$

for $n > 1$, where A and B are fixed integers and the initial terms are $R_0 = 0$ and $R_1 = 1$. Let α and β be the roots of the *characteristic polynomial*

$$f(x) = x^2 - Ax + B$$

and denote the discriminant of $f(x)$ by D. Thus,

$$D = A^2 - 4B = (\alpha - \beta)^2.$$

In the following we assume that R is a *nondegenerate* sequence, that is, $AB \neq 0$, $(A, B) = 1$ and α/β is not a root of unity. It is well known that the explicit form of the terms of R is

$$R_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \tag{1}$$

for any $n \geq 0$; furthermore, obviously, $A = \alpha + \beta$ and $B = \alpha\beta$.

If n is an odd prime and $(n, B) = 1$, then, as is well known, we have

$$n \mid R_{n-(D/n)}, \tag{2}$$

where (D/n) is the Jacobi symbol. If (2) holds for a composite integer, then n is called a *Lucas pseudoprime with respect to the sequence* R. It is a generalization of the ordinary pseudoprime number. Namely, if R is determined by integer constants $A = b+1$, $B = b$ $(b \geq 2)$ and n is a pseudoprime with respect to R with $(n, b-1) = 1$, then

$$n \mid (b^{n-1} - 1), \tag{3}$$

since in this case $\alpha = b$, $\beta = 1$, $D = (b-1)^2$ is a perfect square and, by (1), $R_m = (b^m - 1)/(b-1)$ for any positive integer m. But a composite n satisfying (3)

Received August 6, 1987.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11A15; Secondary 11B39.
Key words and phrases. Pseudoprime, Lucas sequence, Lucas pseudoprimes.
*Research (partially) supported by Hungarian National Foundation for Scientific Research grant No. 273 and 1811.

is called *pseudoprime to base b*. We say briefly that n is a *pseudoprime* if it is one to base $b = 2$.

Let $\theta_b(x)$ denote the number of pseudoprimes to base b not exceeding x. In case $b = 2$ we denote $\theta_b(x)$ by $\theta(x)$. It is known that there exist positive constants c_1 and c_2 such that for all large x

$$c_1 \cdot \log x \le \theta(x) \le x \cdot \exp\{-c_2(\log x \log\log x)^{1/2}\},$$

where the lower and the upper bound is due to D. H. Lehmer [8] and P. Erdős [2], respectively. C. Pomerance improved these results showing (in [9]) that for all large x

$$\theta_b(x) \ge \exp\{(\log x)^{5/14}\}$$

and (in [10])

$$\theta_b(x) \le x \cdot \exp\{-\log x \log\log\log x/2 \cdot \log\log x\}.$$

We note that by using Theorem 5 of E. Fouvry and F. Grupp [3], together with the method of C. Pomerance [9], one can obtain the estimation

$$\theta_b(x) \ge \exp\{(\log x)^{0.4056\cdots}\} > \exp\{(\log x)^{15/37}\}$$

for $x > x_0(b)$.

Let $R(x)$ denote the number of Lucas pseudoprimes with respect to the sequence R not exceeding x. R. Baillie and S. S. Wagstaff, Jr. [1] proved that there are positive constants c_3 and c_4 such that for all large x

$$R(x) < x \cdot \exp\{-c_3(\log x \log\log x)^{1/2}\}$$

for any sequence R and

$$R(x) > c_4 \cdot \log x$$

for sequences R for which $D > 0$ but D is not a perfect square. This lower bound was extended by P. Kiss [6] to all nondegenerate sequences R.

The purpose of this paper is to improve the lower bound for $R(x)$ and to also extend Pomerance's result for Lucas pseudoprimes. We prove:

THEOREM 1. *Let R be a nondegenerate Lucas sequence. Then there exists an absolute constant c such that if x is large enough (depending on the sequence R), then*

$$R(x) > \exp\{(\log x)^c\}.$$

In the proof of this theorem we show only the existence of c. It would be interesting to get a reasonable numerical estimate for this constant. In this regard, perhaps the methods of C. Pomerance [11] and E. Fouvry and F. Grupp [3] would be of use. We also mention that the Lucas pseudoprimes n constructed in the proof all have $(D/n) = 1$. It would be interesting to see if a similar result can be obtained for Lucas pseudoprimes n with $(D/n) = -1$.

The proof of Theorem 1 is based on some other results.

Let R be a nondegenerate Lucas sequence. A prime p is called a *primitive prime divisor* of a term R_n if $p \mid R_n$ but $p \nmid D$ and $p \nmid R_m$ for $0 < m < n$. We know that there is an absolute constant n_0 such that R_n has a primitive prime divisor for any $n > n_0$ (see A. Schinzel [13] or C. L. Stewart [14]). Let $\mathscr{R}_n$ denote the product of the *primitive prime-power divisors* of R_n, where a primitive prime-power divisor

of R_n means a prime-power p^j for which p is a primitive prime divisor of R_n and $p^j \| R_n$. Then we have $\mathscr{R}_n > 1$ for $n > n_0$.

We derive Theorem 1 from the following theorem.

THEOREM 2. *Let R be a nondegenerate Lucas sequence and let y be an integer with $y > \max(n_0, 2DB)$. Further, let $\{p_i\}_{i=1}^t$ be a set of primes with $y/2 < p_i < y$ and let*

$$M = p_1 \cdot p_2 \cdots p_t$$

and

$$m = [p_1 - 1, p_1 + 1, p_2 - 1, p_2 + 1, \ldots, p_t - 1, p_t + 1],$$

where $[a, b, \ldots]$ denotes the least common multiple of the numbers $a, b, \ldots$. If p is a prime in the arithmetic progression $8Dmk + 1$ $(k = 1, 2, \ldots)$ and if

$$S = \{a_i : a_i \mid M,\ p \nmid R_{a_i}\},$$

then the number

$$n = \prod_{a_i \in S'} \mathscr{R}_{pa_i}$$

is a Lucas pseudoprime with respect to the sequence R for any subset S' of S with cardinality at least 2.

2. Proof of Theorem 2. First we prove our second theorem, since we need it in the proof of Theorem 1.

First of all, we introduce some notations and list some elementary properties of nondegenerate Lucas sequences R.

If n is an integer with $(n, B) = 1$, then there are terms in R divisible by n. The least positive index r for which $n \mid R_r$ is called the *rank of apparition of n in the sequence R*, and we shall denote it by $r(n)$. Thus $n \mid R_{r(n)}$ but $n \nmid R_s$ for $0 < s < r(n)$. A nondegenerate Lucas sequence has the following properties:

If $n, s, k, k_1, \ldots, k_t$ are positive integers and $q, q_1, \ldots, q_t$ are primes such that $(q, B) = (q_i, B) = 1$ for $i = 1, 2, \ldots, t$, then we have

(i) $r(q) \mid (q - (D/q))$, assuming that $(D/q) = 0$ if $q \mid D$.

(ii) $r(q^k) = q^{k-j} r(q)$, where j is defined by $q^j \| R_{r(q)}$.

(iii) $r(n) = [r(q_1^{k_1}), r(q_2^{k_2}), \ldots, r(q_t^{k_t})]$ for $n = q_1^{k_1} q_2^{k_2} \cdots q_t^{k_t}$.

(iv) $q \mid R_n$ if and only if $r(q) \mid n$.

(v) $R_q \equiv (D/q) \pmod{q}$.

(vi) $(R_n, R_s) = R_{(n,s)}$.

(vii) $R_n \mid R_{ns}$.

(For these properties of Lucas sequences we refer to D. H. Lehmer [7].)

In order to prove Theorem 2, we have to show that

$$n \mid R_{n-(D/n)}, \tag{4}$$

where $n = \prod_{a_i \in S'} \mathscr{R}_{pa_i}$. Let $M = p_1 \cdot p_2 \cdots p_t$. It is sufficient to prove that

$$pM \mid (n - (D/n)) \tag{5}$$

since $\mathscr{R}_{pa_i} \mid R_{pa_i}$ and, by (vi), $(\mathscr{R}_{pa_i}, \mathscr{R}_{pa_j}) = 1$ for $i \neq j$, hence, using (vii), (5) implies (4).

If q is a prime factor of $\mathscr{R}_{pa_i}$, then $r(q) = pa_i$ and, by (i), $q \equiv (D/q) \pmod{p}$, from which

$$\mathscr{R}_{pa_i} \equiv (D/\mathscr{R}_{pa_i}) \pmod{p} \tag{6}$$

so that

$$n \equiv (D/n) \pmod{p} \tag{7}$$

follows. We shall show that also

$$n \equiv (D/n) \pmod{M} \tag{8}$$

holds.

Assume first that every $a_i \in S'$ is prime.

Since $r(p) \neq a_i$ (and naturally $r(a_i) \neq p$), by (1) we have

$$\mathscr{R}_{pa_i} = \frac{R_{pa_i}}{R_p R_{a_i}} = \frac{1}{R_p} \cdot \frac{(\alpha^{a_i})^p - (\beta^{a_i})^p}{\alpha^{a_i} - \beta^{a_i}} = \frac{G_p}{R_p}, \tag{9}$$

where G_p is a term of the Lucas sequence $G = \{G_n\}_{n=0}^{+\infty}$ defined by the constants $A' = \alpha^{a_i} + \beta^{a_i}$ and $B' = (\alpha\beta)^{a_i} = B^{a_i}$. The sequence G is nondegenerate, and its discriminant is

$$\begin{aligned} D' &= (A')^2 - 4B' = (\alpha^{a_i} - \beta^{a_i})^2 \\ &= \left(\frac{\alpha^{a_i} - \beta^{a_i}}{\alpha - \beta}\right)^2 (\alpha - \beta)^2 = R_{a_i}^2 \cdot D, \end{aligned}$$

and so

$$(D'/p) = (D/p) = 1,$$

since p has the form $p = 8Dk + 1$ and $p \nmid R_{a_i}$. But, by (v), $G_p \equiv (D'/p) \pmod{p}$ and $R_p \equiv (D/p) \pmod{p}$. Therefore, by (9), we get

$$\mathscr{R}_{pa_i} \equiv 1 \pmod{p} \tag{10}$$

from which, by (6), there follows $(D/\mathscr{R}_{pa_i}) \equiv 1 \pmod{p}$, hence $(D/\mathscr{R}_{pa_i}) = 1$. Thus, when S' is a set of primes, (8) can be written in the form

$$n \equiv 1 \pmod{M}. \tag{11}$$

For the sequence R we have

$$R_{2kt+1} \equiv B^{kt} \pmod{R_t}$$

for any positive integers k and t since, by (1),

$$R_{2kt+1} - B^{kt} = R_{kt}(\alpha^{kt+1} + \beta^{kt+1}),$$

where $\alpha^{kt+1} + \beta^{kt+1}$ is an integer and $R_t \mid R_{kt}$. Using this congruence, we get from the definition of p that

$$R_p = R_{8Dmk+1} \equiv B^{4Dmk} \pmod{R_m},$$

which implies

$$R_p \equiv 1 \pmod{M}, \tag{12}$$

since $\varphi(p_i) \mid m$ for each prime factor of M and $M \mid R_m$ by (i) and by the definitions of m and M ($\varphi(n)$ denotes Euler's function).

On the other hand, $M \mid G_m$. Indeed, $M \mid R_{ma_i} = R_{a_i} G_m$ and $(M, R_{a_i}) = 1$ since any prime factor q of R_{a_i} is primitive (now a_i is a prime) and by (i), $q \geq 2a_i - 1 > y - 1$. Therefore, we obtain similarly as above that

$$G_p \equiv 1 \pmod{M}. \tag{13}$$

Now (9), (12) and (13) imply the congruence

$$\mathscr{R}_{pa_i} \equiv 1 \pmod{M} \tag{14}$$

from which (11) and, as we have seen, (8) follow. But (7) and (8) imply (5), which proves Theorem 2 if S' consists of a set of primes.

We complete the proof by induction. Suppose (10) and (14) hold for all a_i containing at most r prime factors and let $a_j = a_i \cdot p_j$, where $p_j \nmid a_i$. By the definition of $\mathscr{R}_n$ we get

$$\mathscr{R}_{pa_j} = \mathscr{R}_{pa_ip_j} = \frac{R_{pa_ip_j}}{R_{a_ip_j} \cdot \prod \mathscr{R}_{pa_k}}, \tag{15}$$

where the product $\prod$ is extended over a_k's for which $a_k \mid a_i p_j$ and $a_k \neq a_i p_j$, since for every nonprimitive prime divisor q of $R_{pa_j} = R_{pa_ip_j}$ we have $q \mid R_{a_ip_j}$ or $q \mid \mathscr{R}_{pa_k}$ for some k and, by (i), (ii) and the conditions for p, it can easily be seen that R_{pa_j} cannot be divisible by any higher power of q than $R_{a_ip_j}$ or $\mathscr{R}_{pa_k}$, and furthermore $(R_{a_ip_j}, \mathscr{R}_{pa_k}) = 1$. Similarly as above, we can write

$$\frac{R_{pa_j}}{R_{a_j}} = G'_p \equiv 1 \pmod{p} \quad \text{and} \quad G'_p \equiv 1 \pmod{M},$$

where G' is a Lucas sequence, too. Each a_k contains at most r prime factors; therefore, by the induction hypothesis,

$$\mathscr{R}_{pa_k} \equiv 1 \pmod{p} \quad \text{and} \quad \mathscr{R}_{pa_k} \equiv 1 \pmod{M}.$$

Thus, by (15), we have the congruences

$$\mathscr{R}_{pa_j} \equiv 1 \pmod{p} \quad \text{and} \quad \mathscr{R}_{pa_j} \equiv 1 \pmod{M}$$

for any r, since the case $r = 1$ was proved, and they imply the validity of Theorem 2 as above.

3. An Auxiliary Result. In order to derive Theorem 1 from Theorem 2, we need the following lemma.

LEMMA. *There exist positive constants c_5 (< 1) and y_0 such that for $y > y_0$ there exist prime numbers $p_1, p_2, \ldots, p_t$ with*

$$y/2 < p_1 < p_2 < \cdots < p_t < y, \tag{16}$$

$$t > \frac{1}{5} \frac{y}{\log y} \tag{17}$$

and

$$m = [p_1 - 1, p_1 + 1, \ldots, p_t - 1, p_t + 1] < \exp(y^{1-c_5}), \tag{18}$$

where $[a, b, \ldots]$ denotes the least common multiple of the numbers $a, b, \ldots$.

Proof. Throughout Sections 3 and 4, $c_6, c_7, \ldots$ denote positive absolute constants. We denote the greatest prime divisor of the integer $n > 1$ by $P(n)$.

Let δ denote a small positive number which will be fixed later, and let $p_1 < p_2 < \cdots < p_t$ denote all the prime numbers p satisfying

$$y/2 < p < y$$

and

$$P((p-1)(p+1)) \le y^{1-\delta}. \tag{19}$$

Then (16) holds trivially.

Define the prime numbers $q_1 < q_2 < \cdots < q_s$ and the positive integers $k_1, k_2, \ldots, k_s$ by

$$m = [p_1 - 1, p_1 + 1, \ldots, p_t - 1, p_t + 1] = \prod_{i=1}^{s} q_i^{k_i}.$$

Then, clearly, $q_i^{k_i} < y + 1$ for all i, and by (19), $q_1 < q_2 < \cdots < q_s \le y^{1-\delta}$. Thus, by the prime number theorem we have for large y (and $\delta \le c_6 \le 1/4$) that

$$\log m < \log \prod_{i=1}^{s} (y+1) < \sum_{i=1}^{s} \log y^2$$

$$\le 2 \left(\sum_{q \le y^{1-\delta}} 1 \right) \log y < c_7 \frac{y^{1-\delta}}{\log y} \log y = c_7 y^{1-\delta},$$

which proves (18) with $c_5 = \delta/2$.

Finally, we have to show that also (17) holds. By the prime number theorem we have, for large y,

$$t \ge \sum_{y/2<p<y} 1 - N(y) - N'(y) > \frac{2}{5} \frac{y}{\log y} - N(y) - N'(y), \tag{20}$$

where $N(y)$ and $N'(y)$ denote the number of primes $p < y$ for which $P(p-1) > y^{1-\delta}$ and $P(p+1) > y^{1-\delta}$, respectively.

If $x > 2$ is a real number and u is an integer such that $2 \le u < x$, then let $N(x,u)$ denote the number of the prime numbers p such that $p \le x$, $u \mid (p-1)$ and $(p-1)/u$ is a prime number. By using Brun's or Selberg's sieve, it can be shown that if u is even and $2 \le u < x$, then we have

$$N(x,u) < c_8 \frac{x}{\varphi(u) \log^2(x/u)}; \tag{21}$$

in fact, this inequality is identical with (4.43) in [12, p. 51] (see also [5]).

If a prime number p satisfies $p < y$, and $q = P(p-1) > y^{1-\delta}$, then there exists an even integer u such that $uq = p - 1$ and

$$2 \le u = \frac{p-1}{q} < \frac{y}{y^{1-\delta}} = y^{\delta},$$

so that by (21) and the definition of $N(y)$ we have, for $\delta \le 1/4$,

$$N(y) \le \sum_{2 \le u < y^{\delta}} N(y,u) < c_8 y \sum_{2 \le u < y^{\delta}} \frac{1}{\varphi(u) \log^2(y/u)}$$

$$< \frac{c_8}{(1-\delta)^2} \frac{y}{\log^2 y} \sum_{2 \le u < y^{\delta}} \frac{1}{\varphi(u)} \tag{22}$$

$$< 2c_8 \frac{y}{\log^2 y} \sum_{2 \le u < y^{\delta}} \frac{1}{\varphi(u)}.$$

It is well known that

$$\sum_{n\le x}\frac{1}{\varphi(n)} < c_9 \log x$$

for $x \ge 2$ (see, e.g., [12, p. 54]), so that from (22) we obtain, for large y,

$$N(y) < 2c_8\frac{y}{\log^2 y}c_9 \log y^{\delta} = c_{10}\delta\frac{y}{\log y}. \tag{23}$$

It can be shown in the same way that

$$N'(y) < c_{11}\delta\frac{y}{\log y}. \tag{24}$$

We now choose

$$\delta = \min\left\{\frac{1}{4}, \frac{1}{10c_{10}}, \frac{1}{10c_{11}}\right\}. \tag{25}$$

Then (20), (23) and (24) yield that

$$t > \left(\frac{2}{5} - \frac{1}{10} - \frac{1}{10}\right)\frac{y}{\log y} = \frac{1}{5}\frac{y}{\log y},$$

so that also (17) holds. This completes the proof of the lemma (with $c_5 = \delta/2$, where δ is defined in (25)).

4. Proof of Theorem 1. In this section, by using the lemma of Section 3, we derive Theorem 1 from Theorem 2.

Let y be an integer with $y > \max(n_0, y_0, 2DB)$, where n_0 and y_0 are defined above, and let $P = \{p_1, p_2, \dots, p_t\}$ be a set of primes satisfying the conditions of the lemma. If p is the least prime of the form $8Dmk + 1$, then

$$p < (8Dm)^{c_{12}},$$

where we may take $c_{12} = 20$ for large m, i.e., for large y (see Graham [4]). By using the lemma of Section 3, we obtain for large y that

$$p < \exp(y^{1-c_{13}}) \tag{26}$$

(with $c_{13} = c_5/2$).

Let S be a set of positive integers defined by

$$S = \left\{a_i : a_i < \exp\left(y^{1-c_{13}}\right), a_i \mid M,\ p \nmid R_{a_i}\right\},$$

where $M = p_1 \cdot p_2 \cdots p_t$. Then by Theorem 2,

$$n = \prod_{a_i \in S'} \mathscr{R}_{pa_i}$$

is a Lucas pseudoprime for any subset S' of S with cardinality at least 2.

We shall determine a lower bound for the cardinality of the set S. If we omit a prime p_i from the set P for which $p_i \mid r(p)$, then, by (iv), $p \nmid R_{a_i}$ for any a_i with $a_i \mid M$. After this omission, we have for the cardinality of the set P

$$t > c_{14}\frac{y}{\log y}.$$

If $v = [v']$, where v' is defined by

$$y^{v'} = \exp\left(y^{1-c_{13}}\right),$$

and $[v']$ denotes the integer part of v', and if a_i contains v primes from P, then $a_i \in S$. Thus, using that

$$v = [v'] = \left[\frac{y^{1-c_{13}}}{\log y}\right] > c_{15}\frac{y^{1-c_{13}}}{\log y}$$

and

$$v \le \frac{y^{1-c_{13}}}{\log y},$$

we get for the cardinality C_s of the set S

$$C_s \ge \binom{t}{v} \ge \left(\frac{t}{v}\right)^v > \exp\left(c_{16}y^{1-c_{13}}\right). \tag{27}$$

By (1), there is a positive constant c_0 depending on the sequence R such that

$$|R_k| < \exp(c_0 k)$$

for any positive integer k; furthermore, obviously,

$$C_s < \exp\left(y^{1-c_{13}}\right).$$

Therefore, (26) yields

$$\begin{aligned} n = \prod_{a_i \in S'} \mathscr{R}_{pa_i} < \prod_{a_i \in S'} |R_{pa_i}| < \exp\left(c \cdot p \cdot \sum_{a_i \in S'} a_i\right) \\ < \exp\left(c \cdot e^{y^{1-c_{13}}} \cdot e^{y^{1-c_{13}}} \cdot e^{y^{1-c_{13}}}\right) < \exp\left(e^{4y^{1-c_{13}}}\right). \end{aligned} \tag{28}$$

Let x be defined by

$$\log x = e^{4y^{1-c_{13}}}. \tag{29}$$

Then, by (28),

$$n < x.$$

On the other hand, distinct subsets S' with cardinality at least 2 determine distinct Lucas pseudoprimes; therefore, by (27) and (29),

$$R(x) \ge 2^{C_s} - C_s - 1 > \exp\left(e^{c_{17} \cdot y^{1-c_{13}}}\right) = \exp\left\{(\log x)^{c_{17}/4}\right\},$$

which proves Theorem 1 with $c = c_{17}/4$.

Acknowledgment. We would like to thank C. Pomerance and A. Schinzel, who independently of each other suggested a significant improvement of our original result.

Mathematical Institute
of the Hungarian Academy of Sciences
Budapest, Hungary

Department of Mathematics
Teacher's Training College
Eger, Hungary

1. R. BAILLIE & S. S. WAGSTAFF, JR., "Lucas pseudoprimes," *Math. Comp.*, v. 35, 1980, pp. 1391–1417.

2. P. ERDŐS, "On pseudoprimes and Carmichael numbers," *Publ. Math. Debrecen*, v. 4, 1956, pp. 201–206.

3. E. FOUVRY & F. GRUPP, "On the switching principle in sieve theory," *J. Reine Angew. Math.*, v. 370, 1986, pp. 101–126.

4. S. GRAHAM, "On Linnik's constant," *Acta Arith.*, v. 39, 1981, pp. 163–179.

5. H. HALBERSTAM & H.-E. RICHERT, *Sieve Methods*, Academic Press, London, 1974.

6. P. KISS, "Some results on Lucas pseudoprimes," *Ann. Univ. Sci. Budapest. Sect. Math.*, v. 28, 1986, pp. 153–159.

7. D. H. LEHMER, "An extended theory of Lucas' functions," *Ann. of Math.*, v. 31, 1930, pp. 419–448.

8. D. H. LEHMER, "On the converse of Fermat's theorem," *Amer. Math. Monthly*, v. 43, 1936, pp. 347–354.

9. C. POMERANCE, "A new lower bound for the pseudoprime counting function," *Illinois J. Math.*, v. 26, 1982, pp. 4–9.

10. C. POMERANCE, "On the distribution of pseudoprimes," *Math. Comp.*, v. 37, 1981, pp. 587–593.

11. C. POMERANCE, "Popular values of Euler's function," *Mathematika*, v. 27, 1980, pp. 84–89.

12. K. PRACHAR, *Primzahlverteilung*, Springer-Verlag, Berlin and New York, 1957.

13. A. SCHINZEL, "Primitive divisors of the expression $A^n - B^n$ in algebraic number fields," *J. Reine Angew. Math.*, v. 268/269, 1974, pp. 27–33.

14. C. L. STEWART, "Primitive divisors of Lucas and Lehmer numbers," *Transcendence Theory: Advances and Applications* (A. Baker and D. W. Masser, eds.), Academic Press, London and New York, 1977, pp. 79–92.