ON LUCASIAN NUMBERS

Peter Hilton
Department of Mathematical Sciences, State University of New York, Binghamton, NY 13902-6000
and Department of Mathematics, University of Central Florida, Orlando FL 32816-6990

Jean Pedersen
Department of Mathematics, Santa Clara University, Santa Clara, CA 95053

Lawrence Somer
Department of Mathematics, Catholic University of America, Washington, DC 20064
(*Submitted June 1995*)

1. INTRODUCTION

Let $u(r, s)$ and $v(r, s)$ be Lucas sequences satisfying the same second-order recursion relation

$$w_{n+2} = rw_{n+1} + sw_n \tag{1}$$

and having initial terms $u_0 = 0, u_1 = 1, v_0 = 2, v_1 = r$, respectively, where r and s are integers. We note that $\{F_n\} = u(1, 1)$ and $\{L_n\} = v(1, 1)$. Associated with the sequences $u(r, s)$ and $v(r, s)$ is the characteristic polynomial

$$f(x) = x^2 - rx - s \tag{2}$$

with characteristic roots α and β. Let $D = (\alpha - \beta)^2 = r^2 + 4s$ be the discriminant of both $u(r, s)$ and $v(r, s)$. By the Binet formulas

$$u_n = (\alpha^n - \beta^n) / (\alpha - \beta) \tag{3}$$

and

$$v_n = \alpha^n + \beta^n. \tag{4}$$

We say that the recurrences $u(r, s)$ and $v(r, s)$ are *degenerate* if $\alpha\beta = -s = 0$ or α / β is a root of unity. Since α and β are the zeros of a quadratic polynomial with integer coefficients, it follows that α / β can be an n^{th} root of unity only if $n = 1, 2, 3, 4,$ or 6. Thus, $u(r, s)$ and $v(r, s)$ can be degenerate only if $r = 0$, $s = 0$, or $D \le 0$.

We say that the integer m is a *divisor* of the recurrence $w(r, s)$ satisfying the relation (1) if $m | w_n$ for some $n \ge 1$. Carmichael [2, pp. 344-45], showed that, if $(m, s) = 1$, then m is a divisor of $u(r, s)$. Carmichael [1, pp. 47, 61, and 62], also showed that if $(r, s) = 1$, then there are infinitely many primes which are not divisors of $v(r, s)$. In particular, Lagarias [4] proved that the set of primes which are divisors of $\{L_n\}$ has density $2/3$. Given the Lucas sequence $v(r, s)$, we say that the integer m is *Lucasian* if m is a divisor of $v(r, s)$. In Theorems 1 and 2, we will show that, if $u(r, s)$ and $v(r, s)$ are nondegenerate, then u_n is not Lucasian for all but finitely many positive integers n. We will obtain stronger results in the case for which $(r, s) = 1$ and $D > 0$.

A related question is to determine all a and b such that v_a divides u_b. Using the identity $u_a v_a = u_{2a}$, one sees that v_a always divides u_{2a}. Since $u_{2a} | u_b$ if $2a | b$, we have that $v_a | u_b$ if $2a | b$. We will show later that if $rs \ne 0$, $(r, s) = 1$, $|v_a| \ge 3$, and $v_a | u_b$, then $2a | b$.

Theorem 1: Consider the Lucas sequences $u(r, s)$ and $v(r, s)$. Suppose that $rs \neq 0$, $(r, s) = 1$, and $D > 0$. Let a and b be positive integers. Then $u_a | v_b$ if and only if one of the following conditions holds:

(i) $a = 1$;
(ii) $|r| = 1$ or 2 and $a = 2$;
(iii) $|r| \geq 3, a = 2$, and b is odd;
(iv) $|r| = 1, s = 1, a = 3$, and $3|b$;
(v) $|r| = 1, a = 4$, and $2|b$ oddly, where $m|n$ oddly if n/m is an odd integer.

In particular, $u_n, n \geq 5$, is not Lucasian.

Theorem 2: Consider the nondegenerate Lucas sequences $u(r, s)$ and $v(r, s)$. If $(r, s) = 1$ and $D < 0$, then u_n is not Lucasian for $n > e^{452}2^{68}$. If $(r, s) > 1$, then there exists a constant $N(r, s)$ dependent on r and s such that u_n is not Lucasian for $n \geq N(r, s)$.

2. NECESSARY LEMMAS AND THEOREMS

The following lemmas and theorems will be needed for the proofs of Theorems 1 and 2.

Lemma 1: $u_{2n} = u_n v_n$.

Proof: This follows from the Binet formulas (3) and (4) and is proved in [6, p. 185] and [3, Section 5]. □

Lemma 2:

$$u_n(-r, s) = (-1)^{n+1} u_n(r, s). \tag{5}$$
$$v_n(-r, s) = (-1)^n v_n(r, s). \tag{6}$$

Proof: Equations (5) and (6) follow from the Binet formulas (3) and (4) and can be proved by induction. □

Lemma 3: Let $u(r, s)$ and $v(r, s)$ be Lucas sequences such that $rs \neq 0$ and $D = r^2 + 4s > 0$. Then $|u_n|$ is strictly increasing for $n \geq 2$. Moreover, if $|r| \geq 2$, then $|u_n|$ is strictly increasing for $n \geq 1$. Furthermore, $|v_n|$ is strictly increasing for $n \geq 1$.

Proof: By Lemma 2, we can assume that $r \geq 1$. The results for $|u_n|$ and $|v_n|$ clearly hold if $s \geq 1$. We now assume that $r \geq 1$ and $s \leq -1$. Since $D > 0$, we must have that $-r^2/4 < s \leq -1$, which implies that $r \geq 3$. We will show by induction that, if $w(r, s)$ is any recurrence satisfying the recursion relation (1) for which $w_0 \geq 0$, $w_1 \geq 1$, and $w_1 \geq (r/2)w_0$, then $w_n \geq 1$ and $w_n \geq (r/2)w_{n-1}$ for all $n \geq 1$. Our results for $u(r, s)$ and $v(r, s)$ will then follow. Assume that $n \geq 1$, and that $w_n \geq 1$, $w_{n-1} \geq 0$, $w_n \geq (r/2)w_{n-1}$. Then $w_{n-1} \leq (2/r)w_n$. By the recursion relation defining $w(r, s)$, we now have

$$w_{n+1} = rw_n + sw_{n-1} > rw_n - (r^2/4)(2/r)w_n = (r/2)w_n,$$

so that $w_{n+1} \geq 1$ and the lemma follows. □

Lemma 4: Consider the Lucas sequences $u(r, s)$ and $v(r, s)$. Then $u_n | u_{in}$ for all $i \geq 1$ and $v_n | v_{(2j+1)n}$ for all $j \geq 0$.

Proof: These results follow from the Binet formulas (3) and (4). □

Lemma 5: Consider the Lucas sequences $u(r, s)$ and $v(r, s)$ for which $(r, s) = 1$ and r and s are both odd. Then u_n even $\Leftrightarrow v_n$ even $\Leftrightarrow 3|n$.

Proof: Both sequences are congruent modulo 2 to the Fibonacci sequence, for which the result is trivial. □

For the Lucas sequence $u(r, s)$, the *rank of apparition** of the positive integer m, denoted by $\omega(m)$, is the least positive integer n, if it exists, such that $m|u_n$. The rank of apparition of m in $v(r, s)$, denoted by $\overline{\omega}(m)$, is defined similarly.

Lemma 6: Consider the Lucas sequences $u(r, s)$ and $v(r, s)$. Let p be an odd prime such that $p \nmid (r, s)$. If $\omega(p)$ is odd, then $\overline{\omega}(p)$ does not exist and p is not Lucasian.

Proof: This was proved by Carmichael [1, p. 47] for the case in which $(r, s) = 1$. The proof extends to the case in which $p \nmid (r, s)$. □

Lemma 7: Consider the Lucas sequences $u(r, s)$ and $v(r, s)$. Suppose that p is an odd prime such that $p \nmid (r, s)$ and $\omega(p) = 2n$. Then $\overline{\omega}(p) = n$.

Proof: This is proved in Proposition 2(iv) of [10]. □

We let $[n]_2$ denote the 2-valuation of the integer n, that is, the largest integer k such that $2^k|n$.

Lemma 8: Consider the Lucas sequence $v(r, s)$. Suppose that m is Lucasian and that p and q are distinct odd prime divisors of m such that $pq \nmid (r, s)$. Then $[\overline{\omega}(p)]_2 = [\overline{\omega}(q)]_2$.

Proof: This is proved in Proposition 2(ix) of [10]. □

Theorem 3: Let $u(r, s)$ and $v(r, s)$ be Lucas sequences such that $rs \neq 0$ and $(r, s) = 1$. Let a and b be positive integers and let $d = (a, b)$.

(i) $(u_a, u_b) = u_d$;

(ii) $(v_a, v_b) = \begin{cases} v_d & \text{if } [a]_2 = [b]_2, \\ 1 \text{ or } 2 & \text{otherwise;} \end{cases}$

(iii) $(u_a, v_b) = \begin{cases} v_d & \text{if } [a]_2 > [b]_2, \\ 1 \text{ or } 2 & \text{otherwise.} \end{cases}$

Proof: This is proved in [7] and [3, Section 5]. □

Remark: It immediately follows from the formula for (v_a, u_b) that if $rs \neq 0$, $(r, s) = 1$, and $|v_a| \geq 3$, then $v_a | u_b$ if and only if $2a|b$. Noting that $v_2 = r^2 + 2s$, we see by Lemma 3 that if $rs \neq 0$ and $D = r^2 + 4s > 0$, then $|v_a| \geq 3$ for $a \geq 2$.

We say that the prime p is a primitive prime divisor of u_n if $p|u_n$ but $p \nmid u_i$ for $1 \leq i < n$.

---

* Plainly, "apparition" is an intended English translation of the French "apparition." Thus, "appearance" would have been a better term, since no ghostly connotation was intended!

Theorem 4 (Schinzel and Stewart): Let the Lucas sequence $u(r, s)$ be nondegenerate. Then there exists a constant $N_1(r,s)$ dependent on r and s such that u_n has a primitive odd prime divisor for all $n \geq N_1(r, s)$. Moreover, if $(r, s) = 1$, then u_n has a primitive odd prime divisor for all $n > e^{452}2^{67}$.

Proof: The fact that the constant $N_1(r,s)$ exists for all nondegenerate Lucas sequences $u(r, s)$ was proved by Lekkerkerker [5] for the case in which $D > 0$ and by Schinzel [8] for the case in which $D < 0$. The fact that if $u(r, s)$ is a nondegenerate Lucas sequence for which $(r, s) = 1$, then an absolute constant N, independent of r and s, exists such that u_n has a primitive odd prime divisor if $n > N$ was proved by Schinzel [9]. Stewart [11] showed that N can be taken to be $e^{452}2^{67}$. □

3. PROOFS OF THE MAIN THEOREMS

We are now ready for the proofs of Theorems 1 and 2.

Proof of Theorem 1

By Lemma 4 and inspection, it is evident that any of conditions (i)-(iv) implies that $u_a | v_b$. Now suppose that $|r| \geq 3, a = 2$, and $u_a | v_b$. Then $|u_a| = |v_1| = |r| \geq 3$. By Theorem 3(ii), we see that b is odd. By Lemma 5, if $r = \pm 1$, $s = 1, u_a | v_b$, and $a = 3$, then $3 | b$. Suppose next that $|r| = 1$, $a = 4$, and $u_a | v_b$. Since $D = r^2 + 4s > 0$, we must have that $s \geq 1$. Then, by Lemma 1, $|u_a| = |v_2| = 2s + 1 \geq 3$. By Theorem 3(ii), it follows that $2 | b$ oddly.

We now note that if $D > 0$ and $rs \neq 0$, then $|u_a| \leq 2$ if and only if $a = 1$, *or* $|r| \leq 2$ and $a = 2$, *or* $|r| = 1, s = 1$, and $a = 3$. Thus it remains to prove that

$$\begin{aligned} &\textit{if } u_a | v_b \text{ and } |u_a| \geq 3, \text{ then either} \\ &\quad |r| \geq 3 \text{ and } a = 2, \text{ or} \\ &\quad |r| = 1 \text{ and } a = 4. \end{aligned} \tag{7}$$

We prove (7) by first proving a lemma which is, in fact, a weaker statement, namely,

Lemma 9: If $D > 0$, $rs \neq 0$, $(r, s) = 1$, $|u_a| = |v_b|$, and $|u_a| \geq 3$, then either $|r| \geq 3$ and $a = 2$, *or* $|r| = 1$ and $a = 4$.

Proof of Lemma 9: Since $|u_a| = |v_b| \geq 3$, $(u_a, v_b) = |v_b| \geq 3$. Thus, by Theorem 3(iii), we conclude that $[a]_2 > [b]_2$; hence, $(u_a, v_b) = |v_d|$, where $d = (a, b)$. Thus, $|v_b| = |v_d|$; but by Lemma 3, $|v_n|$ is an increasing function of n for n positive. Therefore, $b = d$ and $b | a$. Since $[a]_2 > [b]_2$, we have that $2b | a$ and so, by Lemmas 1 and 4, $v_b | u_{2b} | u_a$. But $|u_a| = |v_b|$. Hence, by Lemma 1, $|u_{2b}| = |v_b| = |v_b u_b|$, and so $|u_b| = 1$. Since $|u_n|$ is an increasing function of n for $n \geq 2$ by Lemma 3, we see that $b = 1$ or 2. We can only have that $b = 2$ if $|r| = 1$. However, $|v_b| \geq 3$, so either $b = 1$ and $|u_a| = |v_b| = |r| \geq 3$, implying that $a = 2$, *or* $b = 2$, $|r| = 1$, $s \geq 1$, and $|u_a| = |v_b| = 2s + 1 \geq 3$, which implies that $a = 4$.

Proof of (7): Since $u_a | v_b$ and $|u_a| \geq 3$, we have that $(u_a, v_b) = |u_a| \geq 3$. Using Theorem 3(iii), we infer as in the proof of Lemma 9 that $|u_a| = |v_d|$, where $d = (a, b)$. Hence, by Lemma 9, either $|r| \geq 3$ and $a = 2$, *or* $|r| = 1$ and $a = 4$. □

Proof of Theorem 2

First, suppose that $(r, s) = 1$. Now suppose that $n > 3^{452}2^{68}$ and n is odd. By Theorem 4, u_n has a primitive odd prime divisor p. By Lemma 6, p is not Lucasian and hence u_n is not Lucasian. Now suppose that $n > 3^{452}2^{68}$ and n is even. Then, by Theorem 4, $u_{n/2}$ has a primitive odd prime divisor p_1, and u_n has a primitive odd prime divisor p_2. By Lemma 8, p_1p_2 is not Lucasian. Since $u_{n/2} \mid u_n$ by Lemma 4, we see that u_n is not Lucasian.

Now suppose that $(r, s) > 1$. By Theorem 4, there exists a constant $N_1(r, s) > 2$, dependent on r and s, such that if $n > N_1(r, s)$, then u_n has a primitive odd prime divisor. We note that if p is a prime and $p \mid (r, s)$, then $\omega(p) = 2$. Taking $N(r, s) = 2N_1(r, s)$, we complete our proof by using a completely similar argument to the one above. □

ACKNOWLEDGMENT

We wish to thank the anonymous referee for several suggestions which helped to improve this paper.

REFERENCES

1. R. D. Carmichael. "On the Numerical Factors of the Arithmetic Forms $\alpha^n \pm \beta^n$." *Ann. Math.* (Second Series) **15** (1913):30-70.
2. R. D. Carmichael. "On Sequences of Integers Defined by Recurrence Relations." *Quart. J. Pure Appl. Math.* **48** (1920):343-72.
3. P. Hilton & J. Pedersen. "Fibonacci and Lucas Numbers in Teaching and Research." *Journées Mathématiques & Informatique* **3** (1991-1992):36-57.
4. J. Lagarias. "The Set of Primes Dividing the Lucas Numbers Has Density 2/3." *Pacific J. Math.* **118** (1985):449-61.
5. C. G. Lekkerkerker. "Prime Factors of the Elements of Certain Sequences of Integers." *Proc. Amsterdam Akad.* (Series A) **56** (1953):265-80.
6. E. Lucas. "Théorie des fonctions numériques simplement périodiques." *Amer. J. Math.* **1** (1878):184-220, 289-321.
7. W. L. McDaniel. "The G.C.D. in Lucas and Lehmer Sequences." *The Fibonacci Quarterly* **29.1** (1991):24-29.
8. A. Schinzel. "The Intrinsic Divisors of Lehmer Numbers in the Case of Negative Discriminant." *Ark. Mat.* **4** (1962):413-16.
9. A. Schinzel. "Primitive Divisors of the Expression $A^n - B^n$ in Algebraic Number Fields." *J. Reine Angew. Math.* **268/269** (1974):27-33.
10. L. Somer. "Divisibility of Terms in Lucas Sequences of the Second Kind by Their Subscripts." To appear in *Applications of Fibonacci Numbers* **6**.
11. C. L. Stewart. "Primitive Divisors of Lucas and Lehmer Numbers." In *Transcendence Theory: Advances and Applications*, pp. 79-92. Ed. A. Baker and D. W. Masser. London: Academic Press, 1977.

AMS Classification Number: 11B39

❖❖❖