Czechoslovak Mathematical Journal

Walter Carlip; Lawrence Somer

Square-free Lucas d-pseudoprimes and Carmichael-Lucas numbers

Czechoslovak Mathematical Journal, Vol. 57 (2007), No. 1, 447–463

Persistent URL: http://dml.cz/dmlcz/128183

Czechoslovak Mathematical Journal, 57 (132) (2007), 447–463

SQUARE-FREE LUCAS d-PSEUDOPRIMES AND CARMICHAEL-LUCAS NUMBERS

W. Carlip, Lancaster, L. Somer, Washington, D. C.

(Received April 27, 2005)

Abstract. Let d be a fixed positive integer. A Lucas d-pseudoprime is a Lucas pseudoprime N for which there exists a Lucas sequence $U(P,Q)$ such that the rank of N in $U(P,Q)$ is exactly $(N-\varepsilon(N))/d$, where ε is the signature of $U(P,Q)$. We prove here that all but a finite number of Lucas d-pseudoprimes are square free. We also prove that all but a finite number of Lucas d-pseudoprimes are Carmichael-Lucas numbers.

Keywords: Lucas, Fibonacci, pseudoprime, Fermat

MSC 2000: 11B39, 11A51, 11B37

1. Introduction

An odd composite integer N is a Lucas pseudoprime if there exists a Lucas sequence $U(P,Q)$ with signature ε for which the rank of N divides $U_{N-\varepsilon(N)}$. If, in addition, the rank $\varrho(N)$ is equal to $(N-\varepsilon(N))/d$, then N is a Lucas d-pseudoprime. The concept of Lucas d-pseudoprimes generalizes that of Fermat d-pseudoprimes, and was introduced by the second author in [10]. In this paper, we consider the question of when a Lucas d-pseudoprime is square free. We prove that all but a finite number Lucas d-pseudoprimes are square free.

Carmichael-Lucas numbers are analogous to the Carmichael numbers associated with Fermat pseudoprimes: they are integers N that are Lucas pseudoprimes for every Lucas sequence with a given signature. H. C. Williams studied Carmichael-Lucas numbers in [11] and proved that Carmichael-Lucas numbers are always square free. This leads us to wonder when Lucas d-pseudoprimes are Carmichael-Lucas numbers. We prove that all but a finite number of Lucas d-pseudoprimes are, in fact, Carmichael-Lucas numbers.

A good account of Lucas pseudoprimes may be found in [1] and primality tests involving Lucas pseudoprimes are presented in [1] and [2]. A discussion of Lucas d-pseudoprimes appears in [8, pp. 131–132] and also in [9].

2. Basic properties of Lucas pseudoprimes

Throughout this paper, let N denote a positive odd composite integer with prime decomposition

$$N = \prod_{i=1}^{t} p_i^{k_i}, \tag{1}$$

where $p_1 < p_2 < \ldots < p_t$ are primes and $k_i \geqslant 1$ are integers. Let $U(P,Q)$ be the recurrence sequence defined by $U_0 = 0$, $U_1 = 1$, and

$$U_{n+2} = PU_{n+1} - QU_n \tag{2}$$

for all $n \geqslant 0$. The sequence $U(P,Q)$ is called a *Lucas sequence of the first kind* with parameters P and Q, and also sometimes referred to as a *generalized Fibonacci sequence*. The integer $D = P^2 - 4Q$ is said to be the *discriminant* of $U(P,Q)$.

The semigroup homomorphism $\varepsilon\colon \mathbb{N} \to \{-1,0,1\}$ given by the Jacobi symbol $\varepsilon(n) = \left(\frac{D}{n}\right)$ is called the *signature function* of the sequence $U(P,Q)$. In general, we refer to any semigroup homomorphism from the natural numbers $\mathbb{N}$ to the multiplicative semigroup $\{-1,0,1\}$ as a *signature* function. If N is an integer with decomposition (1), $\delta(N) = \{p_1, \ldots, p_t\}$, the set of prime divisors of N, and ε a given signature function, then the restriction $\varepsilon\colon \delta(N) \to \{-1,0,1\}$ is called the *signature* of N, and N is said to be *supported* by ε if $\varepsilon(N) \neq 0$. Since the signature functions of interest to us here arise as a Jacobi function $\varepsilon(n) = \left(\frac{D}{n}\right)$, for $D = P^2 - 4Q$ the discriminant of a Lucas sequence, such signature functions are called *admissible*.

We denote by $\varrho_U(N)$, or simply $\varrho(N)$ when the sequence U is evident, the *rank of appearance*, or simply the *rank*, of N, i.e., the least positive integer n such that N divides U_n. If the greatest common divisor $(N,Q) = 1$, then it is well known that $U(P,Q)$ is purely periodic modulo N and, since $U_0 = 0$, it follows that $\varrho(N)$ exists. Moreover, in this case, $U_n \equiv 0 \pmod{N}$ if and only if $\varrho(N)$ divides n. It was proven by Lucas [7] that if an odd prime p does not divide QD, then $U_{p-\varepsilon(p)} \equiv 0 \pmod{p}$, and therefore $\varrho(p)$ divides $p - \varepsilon(p)$. Lucas' observation leads to the following definition.

Definition 2.1. An odd composite integer N is called a *Lucas pseudoprime* with respect to the Lucas sequence $U(P,Q)$, with discriminant D and signature ε, if $(N, QD) = 1$ and $U_{N-\varepsilon(N)} \equiv 0 \pmod{N}$.

If there exists a Lucas sequence $U(P,Q)$ such that N is a Lucas pseudoprime with respect to $U(P,Q)$ and $\varrho(N) = (N - \varepsilon(N))/d$, then N is said to be a *Lucas d-pseudoprime*.

Note that if N is a Lucas pseudoprime with signature $\varepsilon(n) = \left(\frac{D}{n}\right)$, then the requirement that $(N, D) = 1$ implies that ε supports N. Thus every Lucas pseudoprime is supported by its own signature.

We define several number theoretic functions that are useful for studying Lucas pseudoprimes (see, e.g., [4]). If N an odd integer with decomposition (1) that is supported by signature ε, define

$$\lambda(N,\varepsilon) = \operatorname{lcm}\{p_i^{k_i-1}(p_i - \varepsilon(p_i))\colon\ 1 \leqslant i \leqslant t\}, \tag{3}$$

$$\lambda'(N,\varepsilon) = \operatorname{lcm}\{p_i - \varepsilon(p_i)\colon\ 1 \leqslant i \leqslant t\}, \tag{4}$$

$$\psi(N,\varepsilon) = \frac{1}{2^{t-1}}\prod_{i=1}^{t}(p_i - \varepsilon(p_i)), \tag{5}$$

$$\xi(N,\varepsilon) = \frac{1}{N}\prod_{i=1}^{t}(p_i - \varepsilon(p_i)) = \prod_{i=1}^{t}\frac{p_i - \varepsilon(p_i)}{p_i^{k_i}} \tag{6}$$

and

$$T(N,\varepsilon) = \frac{\prod\limits_{i=1}^{t}(p_i - \varepsilon(p_i))}{\operatorname{lcm}\{p_i - \varepsilon(p_i)\colon\ 1 \leqslant i \leqslant t\}} = \frac{N\xi(N,\varepsilon)}{\lambda'(N,\varepsilon)}. \tag{7}$$

Each of these functions depends only on the value of ε on the primes that divide N, that is, they depend only on the signature of N. When N is a Lucas pseudoprime, we always have in mind a corresponding Lucas sequence $U(P,Q)$ with signature function ε. When no signature is explicitly given, it is this signature that appears in the evaluation of the functions defined above.

Carmichael [6] proved that if $U(P,Q)$ is a Lucas sequence with signature ε and discriminant D satisfying $(N, QD) = 1$, then

$$U_{\lambda(N,\varepsilon)} \equiv 0 \pmod{N}. \tag{8}$$

It follows that $\varrho(N) \mid \lambda(N,\varepsilon)$, and $\lambda(N,\varepsilon)$ is called the *universal rank* of N. If N is a Lucas d-pseudoprime with signature ε, then $(N - \varepsilon(N))/d$ divides $\lambda(N,\varepsilon)$ and, since $(N, N - \varepsilon(N)) = 1$,

$$\frac{N - \varepsilon(N)}{d} \,\Big|\, \lambda'(N,\varepsilon). \tag{9}$$

If p_i is any prime divisor of N, then $\varrho(p_i) \mid \varrho(N)$. Therefore, if N is a Lucas d-pseudoprime, then $\varrho(p_i) \mid (N - \varepsilon(N))/d$. Since $\varrho(p_i)$ also divides $p_i - \varepsilon(p_i)$ and $\varrho(p_i) > 1$, it follows that

$$\Big(\frac{N - \varepsilon(N)}{d}, p_i - \varepsilon(p_i)\Big) > 1, \tag{10}$$

for all prime factors p_i of N.

In fact, (9) and (10) together characterize Lucas d-pseudoprimes. To show this we require several preliminary results.

Lemma 2.2. *Let $U(P, Q)$ be a Lucas sequence of the first kind with signature ε_U. For a fixed positive integer k, let W be the subsequence of U given by $W_n = U_{kn}$. Then W is a second-order recurrence sequence with the property that $\varepsilon_W(p) = \varepsilon_U(p)$ for all primes p such that $(p, U_k) = 1$.*

P r o o f. Let $V(P, Q)$ be the Lucas sequence of the second kind, i.e., the second-order recurrence sequence that satisfies (2) and has initial terms $V_0 = 2$ and $V_1 = P$. By Lemma 2.10 of [5], W is, indeed, a second-order recurrence sequence, and satisfies the relation

$$W_{n+2} = P'W_{n+1} - Q'W_n, \tag{11}$$

where $P' = V_k$ and $Q' = Q^k$. Thus it remains only to show that $\varepsilon_W(p) = \varepsilon_U(p)$ when $p \nmid U_k$.

Let $D = P^2 - 4Q$ be the discriminant of U and $D' = (P')^2 - 4Q'$ the discriminant of W. By Lemma 2.9 of [5], $(V_k)^2 - D(U_k)^2 = 4Q^k$, and therefore

$$D' = (P')^2 - 4Q' = (V_k)^2 - 4Q^k = D(U_k)^2.$$

Consequently D and D' differ by the square factor U_k^2, and therefore, if p is relatively prime to U_k, then D' is a square modulo p if and only if D is a square modulo p. Thus $\varepsilon_W(p) = \left(\frac{D'}{p}\right) = \left(\frac{D}{p}\right) = \varepsilon_U(p)$ when $(p, U_k) = 1$, as desired. □

Lemma 2.3. *Let $U(P, Q)$ be the Lucas sequence of the first kind satisfying recursion (2) and $W(P, Q)$ any second-order recurrence sequence satisfying (2) with $W_0 = 0$. Then U and W have identical signature functions. Furthermore, if $(N, W_1) = 1$, then $\varrho_U(N) = \varrho_W(N)$.*

P r o o f. Since U and W satisfy recursion (2), both have discriminant $D = P^2 - 4Q$, and hence both have signature $\varepsilon(n) = \left(\frac{D}{n}\right)$. The hypotheses imply that the sequence W is simply a multiple of U by the integer W_1, that is, for all n, we have $W_n = W_1U_n$. If $(W_1, N) = 1$, it follows that $N \mid W_n$ if and only if $N \mid U_n$. Therefore $\varrho_U(N) = \varrho_W(N)$, as desired. □

The next theorem generalizes a theorem of H. C. Williams (Theorem 3 of [11]).

Theorem 2.4. *Let ε be an admissible signature function, p an odd prime such that $\varepsilon(p) \neq 0$, $s \neq 1$ a divisor of $p - \varepsilon(p)$, and k any positive integer. Then for each $l \leqslant k-1$ there exists a Lucas sequence $W(P,Q)$ with signature ε_W that satisfies $\varrho_W(p^k) = p^l s$ and $\varepsilon(p) = \varepsilon_W(p)$.*

P r o o f. When $l = k-1$, the theorem follows immediately from Williams' theorem. In fact, by Williams' theorem, we can find a Lucas sequence $U(P,Q)$ with discriminant D satisfying $\varepsilon(p) = \left(\frac{D}{p}\right)$ such that $\varrho_U(p^k) = p^{k-1}s$. Define the subsequence W of U by $W_i = U_{(p^{k-l-1})i}$.

By Lemma 2.2, W is a second-order recurrence sequence with the property that $\varepsilon_W(q) = \varepsilon_U(q)$ for all primes q such that $(q, U_{p^{k-l-1}}) = 1$. However, if $p \mid U_{p^{k-l-1}}$, then $\varrho(p) \mid p^{k-l-1}$. But $\varrho(p) \mid p - \varepsilon(p)$ and $\varepsilon(p) = \pm 1$, from which it follows that $\varrho(p) \mid (p^{p^{k-l-1}}, p - \varepsilon(p)) = 1$, a contradiction. Therefore $(p, U_{p^{k-l-1}}) = 1$, and hence $\varepsilon_W(p) = \varepsilon_U(p)$.

Since it is clear that $\varrho_W(p^k) = p^l s$, Lemma 2.3 completes the proof. □

We can generalize Williams' theorem even more.

Theorem 2.5. *Suppose that ε is an admissible signature, N is an integer that is supported by ε and has prime decomposition* (1)*, and s is any divisor of $\lambda'(N,\varepsilon)$ such that $(s, p_i - \varepsilon(p_i)) \neq 1$ for all prime divisors p_i of N. Then there exists a Lucas sequence $U(P,Q)$ that satisfies $\varrho_U(N) = s$ and $\varepsilon_U(p_i) = \varepsilon(p_i)$ for each prime divisor p_i of N.*

P r o o f. Let $s_i = (s, p_i - \varepsilon(p_i))$. By hypothesis, $s_i > 1$ and, since $s \mid \lambda'(N,\varepsilon)$, it is clear that $s = \operatorname{lcm}\{s_i\}$. By Theorem 2.4, for each i we can find a sequence $U_i(P_i, Q_i)$ such that $\varrho_{U_i}(p_i^{k_i}) = s_i$ and $\varepsilon_{U_i}(p_i) = \varepsilon(p_i)$. Then, by the Chinese remainder theorem, we can find integers P and Q such that $P \equiv P_i \pmod{p_i^{k_i}}$ and $Q \equiv Q_i \pmod{p_i^{k_i}}$ for each i. By setting $D = (P)^2 - 4Q$ and $D_i = (P_i)^2 - 4Q_i$, we obtain $D \equiv D_i \pmod{p_i^{k_i}}$ for each i. Let $U = U(P,Q)$. Then $\varrho_U(N) = \operatorname{lcm}\{\varrho_U(p_i^{k_i})\} = \operatorname{lcm}\{s_i\} = s$. Finally, $\varepsilon_U(p_i) = \left(\frac{D}{p_i}\right) = \left(\frac{D_i}{p_i}\right) = \varepsilon_{U_i}(p_i) = \varepsilon(p_i)$ for each i. □

Theorem 2.6. *An integer N is a Lucas d-pseudoprime with signature ε if and only if* (9) *and* (10) *are true.*

P r o o f. Suppose that N is a Lucas d-pseudoprime with signature ε. Then, by the argument preceding (9), we know that (9) and (10) are true.

To prove the converse, suppose that N is an integer and ε is an admissible signature such that (9) and (10) are true. Then, by Theorem 2.5 with $s = (N - \varepsilon(N))/d$, there

exists a Lucas sequence $U(P,Q)$ that satisfies $\varepsilon_U(p_i) = \varepsilon(p_i)$ for all prime divisors p_i of N and $\varrho(N) = s = (N - \varepsilon(N))/d$. Thus N is, indeed, a Lucas d-pseudoprime. □

We also require several basic lemmas on Lucas d-pseudoprimes, some of which are stated in [3].

Lemma 2.7. *If N is an odd composite integer with decomposition* (1) *and ε is any signature that supports N, then*

$$\frac{\lambda'(N,\varepsilon)}{N} \leqslant \frac{\psi(N,\varepsilon)}{N} < 2\Big(\frac{2}{3}\Big)^t \quad \text{and} \quad \frac{\psi(N,\varepsilon)}{N-\varepsilon(N)} < 2\Big(\frac{2}{3}\Big)^t. \tag{12}$$

P r o o f. Since N is odd, p_i is odd, and $\varepsilon(p_i) = \pm 1$, it follows that $p_i - \varepsilon(p_i)$ is even. Therefore 2^{t-1} divides $\prod_{i=1}^{t}(p_i - \varepsilon(p_i))$, and $\psi(N,\varepsilon)$ is an integer. For each i,

$$\frac{p_i - \varepsilon(p_i)}{p_i^{k_i}} \leqslant \frac{p_i + 1}{p_i^{k_i}} = \frac{1 + 1/p_i}{p_i^{k_i - 1}} \leqslant \frac{1 + 1/3}{3^0} = \frac{4}{3}. \tag{13}$$

Furthermore, (13) is strict if either $p_i > 3$ or $k_i > 1$. Consequently

$$\frac{\psi(N,\varepsilon)}{N} = \frac{1}{2^{t-1}} \prod_{i=1}^{t} \frac{p_i - \varepsilon(p_i)}{p_i^{k_i}} < \frac{1}{2^{t-1}}\Big(\frac{4}{3}\Big)^t = 2\Big(\frac{2}{3}\Big)^t. \tag{14}$$

Since $\lambda'(N,\varepsilon) \mid \psi(N,\varepsilon)$, the first inequality of (12) follows from (14).

Note that the last inequality of (12) now follows if $\varepsilon(N) = -1$ and, in any case, $N/(N - \varepsilon(N)) < 4/3$. If $\varepsilon(p_i) = 1$ or $k_i > 1$, then $(p_i - \varepsilon(p_i))/p_i^{k_i} < 1$, and the last inequality follows from (13). Thus we may assume that $\varepsilon(p_i) = -1$ and $k_i = 1$, for each i, and that $\varepsilon(N) = 1$. It follows that $t \geqslant 2$ and

$$\frac{p_2 - \varepsilon(p_2)}{p_2^{k_2}} \frac{N}{N - \varepsilon(N)} \leqslant \frac{6}{5} \frac{3 \cdot 5}{3 \cdot 5 - 1} = \frac{9}{7} < \frac{4}{3}, \tag{15}$$

and the final inequality of (12) follows. □

Lemma 2.8. *If $N = nm$ is an odd integer with $n \geqslant 3$, $m \geqslant 3$, and $(n,m) = 1$, and ε is any signature that supports N, then*

$$\frac{\lambda'(N,\varepsilon)}{N} = \frac{\lambda'(nm,\varepsilon)}{nm} \leqslant \frac{2}{3} \frac{\lambda'(n,\varepsilon)}{n}. \tag{16}$$

P r o o f. The definition of λ' implies that $\lambda'(nm,\varepsilon) \mid \frac{1}{2}\lambda'(n,\varepsilon)\lambda'(m,\varepsilon)$. Therefore, by Lemma 2.7,

$$\frac{\lambda'(nm,\varepsilon)}{nm} \leqslant \frac{1}{2} \frac{\lambda'(n,\varepsilon)}{n} \frac{\lambda'(m,\varepsilon)}{m} \leqslant \frac{2}{3} \frac{\lambda'(n,\varepsilon)}{n}. \tag{17}$$

□

Lemma 2.9. *If N is a d-pseudoprime with respect to signature ε, then*

$$\frac{\lambda'(N,\varepsilon)}{N} > \frac{1}{d+1}. \tag{18}$$

P r o o f. By (9), $N-\varepsilon(N) \mid d\lambda'(N,\varepsilon)$. Therefore $d\lambda'(N,\varepsilon) \geqslant N-\varepsilon(N) \geqslant N-1$. Since $\lambda'(N,\varepsilon) \geqslant 2$, it follows that $(d+1)\lambda'(N,\varepsilon) > d\lambda'(N,\varepsilon)+1 \geqslant N$. The lemma follows immediately. □

Lemma 2.10 (Lemma 4.1 of [3])**.** *If N is a Lucas d-pseudoprime, then $(N,d)=1$ and there exist integers b and c such that*

$$\frac{\lambda'(N,\varepsilon)}{N-\varepsilon(N)} = \frac{b}{d} \leqslant \frac{\psi(N,\varepsilon)}{N-\varepsilon(N)} = \frac{c}{d}. \tag{19}$$

P r o o f. Since $d \mid N-\varepsilon(N)$ and $\varepsilon(N) = \pm 1$, it is clear that $(N,d)=1$. The existence of the integer b follows immediately from (9). Similarly, since $\lambda'(N,\varepsilon) \mid \psi(N,\varepsilon)$, (9) implies that $(N-\varepsilon(N))/d$ divides $\psi(N,\varepsilon)$, which in turn guarantees the existence of the integer c and verifies inequality (19). □

Lemma 2.11 (Lemma 4.3 of [3])**.** *If N is a Lucas d-pseudoprime with prime decomposition* (1) *and $k_i \geqslant 2$, then*

$$p_i^{k_i-1} < 2\left(\tfrac{2}{3}\right)^t (d+1). \tag{20}$$

In particular, N is square free when t is sufficiently large.

P r o o f. Suppose that $p_i^2 \mid N$. By induction, Lemma 2.8, and Lemma 2.9,

$$\frac{1}{d+1} < \frac{\lambda'(N,\varepsilon)}{N} = \frac{\lambda'\Big(\prod\limits_{j=1}^{t} p_j^{k_j}, \varepsilon\Big)}{\prod\limits_{j=1}^{t} p_j^{k_i}} \leqslant \left(\frac{2}{3}\right)^{t-1} \frac{\lambda'(p_i^{k_i},\varepsilon)}{p_i^{k_i}} \leqslant \left(\frac{2}{3}\right)^{t-1} \frac{p_i+1}{p_i^{k_i}}.$$

Thus

$$p_i^{k_i-1} < \left(\frac{2}{3}\right)^{t-1} \frac{p_i+1}{p_i}(d+1) \leqslant \left(\frac{2}{3}\right)^{t-1} \left(\frac{4}{3}\right)(d+1) = 2\left(\frac{2}{3}\right)^t (d+1).$$

□

Lemma 2.12 (Lemma 4.2 of [3]). *If N is a Lucas d-pseudoprime with prime decomposition* (1), *then $t < \log_{3/2}(2d)$.*

P r o o f. Lemma 2.7 and Lemma 2.10 imply that $1/(2d) \leqslant c/(2d) < (2/3)^t$, and therefore $2d > (3/2)^t$. The lemma follows immediately. □

3. Basic properties of Carmichael-Lucas numbers

We define Carmichael-Lucas numbers and describe some of their fundamental properties.

Definition 3.1. An odd composite integer N is a *Carmichael-Lucas* number with respect to a fixed signature ε that supports N if $U_{N-\varepsilon(N)} \equiv 0 \pmod N$ for *every* Lucas sequence $U(P,Q)$ whose signature restricts to ε on $\delta(N)$ and satisfies $(N,Q) = 1$.

Theorem 3.2. *If N is a Carmichael-Lucas number with signature ε, then N is square free and $\lambda'(N,\varepsilon) \mid N - \varepsilon(N)$.*

P r o o f. This is essentially Theorem 4 of [11]. □

Theorem 3.3. *If N is square free and ε is a signature function that supports N and for which $\lambda'(N,\varepsilon) \mid N - \varepsilon(N)$, then N is a Carmichael-Lucas number.*

P r o o f. Let $U(P,Q)$ be a Lucas sequence with a signature that coincides with ε on $\delta(N)$. Then $\varrho_U(N) \mid \lambda(N,\varepsilon)$. Since N is square free, $\lambda(N,\varepsilon) = \lambda'(N,\varepsilon)$, and therefore $\varrho_U(N) \mid \lambda'(N,\varepsilon)$. But then $\varrho_U(N) \mid N - \varepsilon(N)$, and it follows that N is a Carmichael-Lucas number. □

4. Square-free conditions

We now turn to the question of when Lucas d-pseudoprimes are square free.

Theorem 4.1. *If $M > 1$ is an integer, then there are at most a finite number of Lucas d-pseudoprimes N with the following properties:*

(a) *N has exactly t distinct prime divisors;*

(b) *M divides N with $(N/M, M) = 1$; and*

(c) *N/M is square free.*

P r o o f. Fix the integer $M > 1$ and suppose that M has s distinct prime factors. Let Ω be the set of all Lucas d-pseudoprimes that satisfy the conditions of the theorem. Then each $N \in \Omega$ can be written in the form

$$N = M \cdot \prod_{i=s+1}^{t} p_i, \tag{21}$$

where $s \geqslant 1$, for each i, p_i is a prime that does not divide M, and $p_i < p_j$ when $i < j$.

We proceed by induction on $t - s$.

Clearly, if $t - s = 0$, then $t = s$ and $N = M$, and at most one Lucas d-pseudoprime satisfies (b).

We may now assume that $t > s \geqslant 1$.

Claim. *There are only finitely many possible values for the prime p_{s+1} in* (21).

Before we prove the claim, we observe that the theorem follows immediately from this claim and the induction hypothesis, as follows. Partition Ω according to the value of p_{s+1}, that is, into subsets Ω_p such that $N \in \Omega_p$ if and only if $p_{s+1} = p$. By the claim, Ω is the union of a finite number of such subsets Ω_p, and it suffices to show that each of these is finite. However, if $N \in \Omega_p$, then N satisfies the conditions of the theorem with $M' = Mp$ in place of M. But then M' has $s + 1$ distinct prime factors and $t - (s + 1) < t - s$. By the induction hypothesis, only a finite number of Lucas d-pseudoprimes satisfy the hypotheses of the theorem with M' in place of M, and therefore Ω_p is finite as desired.

P r o o f of Claim. We begin with the simple observation that the function $\xi(N, \varepsilon)$ is multiplicative, that is, if $(N_1, N_2) = 1$, then $\xi(N_1 N_2, \varepsilon) = \xi(N_1, \varepsilon)\xi(N_2, \varepsilon)$. In particular, if $N \in \Omega$ has signature ε, then $\xi(N, \varepsilon) = \xi(M, \varepsilon)\xi(M/N, \varepsilon)$.

Let

$$\delta = \frac{1}{3} \min_{\substack{n \geqslant 1 \\ 1 \leqslant i \leqslant d-1}} \Big| \frac{\xi(M, \varepsilon)}{n} - \frac{i}{d} \Big|. \tag{22}$$

We claim that $\delta > 0$. Otherwise, by (6),

$$in M = d \prod_{i=1}^{s} (p_i - \varepsilon(p_i)). \tag{23}$$

Since, by Lemma 2.10, $(M, d) = 1$, (23) implies that the largest prime divisor p_s of M divides $\prod_{i=1}^{s} (p_i - \varepsilon(p_i))$, which is impossible since each Lucas d-pseudoprime $N \in \Omega$ is supported by its signature ε.

Let $N \in \Omega$ and choose b as in Lemma 2.10. Note that Lemma 2.7 implies that $b < d$ since $t > 1$. By the triangle inequality and the definition of δ,

$$
\begin{aligned}
(24) \qquad 3\delta &\leqslant \Big|\frac{\xi(M,\varepsilon)}{T(N,\varepsilon)} - \frac{b}{d}\Big| \\
&\leqslant \Big|\frac{\xi(M,\varepsilon)}{T(N,\varepsilon)} - \frac{\lambda'(N,\varepsilon)}{N}\Big| + \Big|\frac{\lambda'(N,\varepsilon)}{N} - \frac{\lambda'(N,\varepsilon)}{N-\varepsilon(N)}\Big| + \Big|\frac{\lambda'(N,\varepsilon)}{N-\varepsilon(N)} - \frac{b}{d}\Big| \\
&= \Big|\frac{\xi(M,\varepsilon)}{T(N,\varepsilon)} - \frac{\lambda'(N,\varepsilon)}{N}\Big| + \Big|\frac{\lambda'(N,\varepsilon)}{N} - \frac{\lambda'(N,\varepsilon)}{N-\varepsilon(N)}\Big|.
\end{aligned}
$$

We now bound the two terms on the right-hand side of (24). Since $(p_i - \varepsilon(p_i))/p_i^{k_i} \leqslant 4/3$ for all p_i and $T(N,\varepsilon) \geqslant 1$, we observe that

$$
\frac{\xi(M,\varepsilon)}{T(N,\varepsilon)} \leqslant \Big(\frac{4}{3}\Big)^s.
$$

Furthermore, since N/M is square free and $(1 - \varepsilon(p_i)/p_i)$ becomes arbitrarily close to 1 when p_i is sufficiently large, we can find an integer α_1 such that $|1 - \xi(N/M,\varepsilon)| < \delta/(4/3)^s$ when $p_{s+1} > \alpha_1$. Therefore, if $p_{s+1} > \alpha_1$, then

$$
\begin{aligned}
(25) \qquad \Big|\frac{\xi(M,\varepsilon)}{T(N,\varepsilon)} - \frac{\lambda'(N,\varepsilon)}{N}\Big| &= \Big|\frac{\xi(M,\varepsilon)}{T(N,\varepsilon)} - \frac{\xi(N,\varepsilon)}{T(N,\varepsilon)}\Big| \\
&= \Big|\frac{\xi(M,\varepsilon)}{T(N,\varepsilon)} - \frac{\xi(M,\varepsilon)\xi(N/M,\varepsilon)}{T(N,\varepsilon)}\Big| \\
&= \Big(\frac{\xi(M,\varepsilon)}{T(N,\varepsilon)}\Big)|1 - \xi(N/M,\varepsilon)| \\
&< \Big(\frac{4}{3}\Big)^s \frac{\delta}{(4/3)^s} = \delta.
\end{aligned}
$$

Now consider the second term on the right-hand side of (24). Since, $t \geqslant 2$ we know that $N \geqslant 15$. Then Lemma 2.7 implies that $\lambda'(N,\varepsilon) < (8/9)N < N - 1$. Let $\alpha_2 = 1/\delta$. If $p_{s+1} > \alpha_2$, then certainly $N > \alpha_2$ and

$$
(26) \qquad \Big|\frac{\lambda'(N,\varepsilon)}{N} - \frac{\lambda'(N,\varepsilon)}{N-\varepsilon(N)}\Big| \leqslant (N-1)\Big|\frac{1}{N} - \frac{1}{N-1}\Big| = \frac{1}{N} < \frac{1}{\alpha_2} = \delta.
$$

Let $\alpha = \max\{\alpha_1, \alpha_2\}$. Combining the bounds in (25) and (26) with (24), we discover that if $p_{s+1} > \alpha$, then

$$
3\delta \leqslant \Big|\frac{\xi(M,\varepsilon)}{T(N,\varepsilon)} - \frac{\lambda'(N,\varepsilon)}{N}\Big| + \Big|\frac{\lambda'(N,\varepsilon)}{N} - \frac{\lambda'(N,\varepsilon)}{N-\varepsilon(N)}\Big| < 2\delta,
$$

which is a contradiction. It follows that $3 \leqslant p_{s+1} \leqslant \alpha$ and there are only a finite number of possible values for p_{s+1}, as claimed.

The theorem now follows from the claim, as shown above. □

Theorem 4.2. *All but a finite number of Lucas d-pseudoprimes are square free.*

P r o o f. It is a consequence of Lemma 2.11 that there are only a finite number of integers M of the form

$$M = \prod_{i=1}^{s} p_i^{k_i},$$

with $k_i > 1$ for all i, that divide a Lucas d-pseudoprime N with t distinct prime divisors. If we apply Theorem 4.1 to each of these integers, we see that only a finite number of Lucas d-pseudoprimes with t distinct prime divisors can be divisible by a square.

The theorem now follows from Lemma 2.12, which implies that there are only a finite number of possible values for t. □

Theorem 4.3. *Let M be any integer. Then there are at most a finite number of Lucas d-pseudoprimes N such that $M \mid N$.*

P r o o f. By Theorem 4.2, all but a finite number of Lucas d-pseudoprimes are square free, so it suffices to prove the theorem for square-free Lucas d-pseudoprimes. Moreover, by Lemma 2.12 we only need to prove the theorem for Lucas d-pseudoprimes that have exactly t distinct prime divisors. But then M and N satisfy the conditions of Theorem 4.1. □

5. Carmichael-Lucas numbers

In this section we prove our claim that all but a finite number of d-pseudoprimes are Carmichael-Lucas numbers. This result follows from Theorem 4.2 along with Theorem 5.4 of [4], which is proven there using techniques developed in [3]. We begin with a definition.

Definition 5.1. A Lucas d-pseudoprime N is called *standard* if

$$bT(N, \varepsilon) = d \tag{27}$$

and *exceptional* otherwise, where, as usual, b is given by (19).

Observe that condition (27) is equivalent to

$$1 = \frac{b}{d} T(N, \varepsilon) = \frac{\lambda'(N, \varepsilon)}{N - \varepsilon(N)} \frac{\prod_{i=1}^{t} (p_i - \varepsilon(p_i))}{\lambda'(N, \varepsilon)} = \frac{\prod_{i=1}^{t} (p_i - \varepsilon(p_i))}{N - \varepsilon(N)}. \tag{28}$$

Theorem 5.2. *All but a finite number of Lucas d-pseudoprimes are standard.*

P r o o f. This is Theorem 5.4 of [4]. □

Theorem 5.3. *Every square-free standard Lucas d-pseudoprime is a Carmichael-Lucas number.*

P r o o f. Suppose that N is a square-free standard Lucas d-pseudoprime. Then

$$N - \varepsilon(N) = \lambda'(N,\varepsilon)\frac{N-\varepsilon(N)}{\lambda'(N,\varepsilon)} = \lambda'(N,\varepsilon)\frac{d}{b} = \lambda'(N,\varepsilon)T(N,\varepsilon).$$

Since it is clear from the definition of $T(N,\varepsilon)$ that $T(N,\varepsilon)$ is an integer, we see that $\lambda'(N,\varepsilon) \mid N - \varepsilon(N)$. Then, by Theorem 3.3, N is a Carmichael-Lucas number. □

Theorem 5.4. *All but a finite number of Lucas d-pseudoprimes are Carmichael-Lucas numbers.*

P r o o f. By Theorem 4.2 and Theorem 5.2, all but finitely many Lucas d-pseudoprimes are square free and standard, so the result follows from Theorem 5.3. □

6. Square-free conditions: computations

In Section 4 we proved that all but a finite number of Lucas d-pseudoprimes are square free. In this final section we examine this question from a computational perspective and provide conditions on t, the number of distinct prime divisors of a Lucas d-pseudoprime N, that force N to be square free. We begin by considering what happens when t is large.

In Lemma 2.11 we observed that if t is sufficiently large (depending upon d, of course), then all Lucas d-pseudoprimes are square free. The next theorem makes this more precise.

Theorem 6.1. *If N is a Lucas d-pseudoprime with prime factorization* (1) *and $t \geqslant \log(d+1)/\log\frac{3}{2} - 1$, then N is square free.*

P r o o f. This follows from Lemma 2.11. Suppose that N is a Lucas d-pseudoprime and p^2 divides N for some prime p. By an easy computation, if $t \geqslant \log(d+1)/\log\frac{3}{2} - 1$, then $2\left(\frac{2}{3}\right)^t(d+1) \leqslant 3$ and, by Lemma 2.11, $p < 2\left(\frac{2}{3}\right)^t(d+1) \leqslant 3$, a contradiction. □

Example 6.2. The function $\log(d+1)/\log\frac{3}{2} - 1$ grows rather slowly. Thus, for example, if $d \leqslant 984$, then every Lucas d-pseudoprime with 16 or more distinct prime factors must be square free. If $d \leqslant 20000000$, then every Lucas d-pseudoprime with 41 or more distinct prime factors is square free.

For standard Lucas d-pseudoprimes N, (28) suggests a computational method to show that N is square free when t is sufficiently small. The method is motivated by the following lemma.

Lemma 6.3. *If N is an odd integer with decomposition* (1) *with $t \leqslant 15$, ε is a signature function that supports N, and*

$$\frac{\prod_{i=1}^{t}(p_i - \varepsilon(p_i))}{N - \varepsilon(N)} = 1, \tag{29}$$

then N is square free.

P r o o f. Suppose that $k_i > 1$ for some i. Then the maximal value of the left-hand side of equation (29) is attained when t is maximal and N is minimal, i.e., when $N = 3^2 \cdot 5 \cdot 7 \cdot \ldots \cdot 53$:

$$\begin{aligned}\frac{\prod_{i=1}^{t}(p_i - \varepsilon(p_i))}{N - \varepsilon(N)} &= \frac{\prod_{i=1}^{t}(p_i - \varepsilon(p_i))}{p_1^{k_1}p_2^{k_2}p_3^{k_3}\ldots p_t^{k_t} - \varepsilon(N)} \leqslant \frac{\prod_{i=1}^{t}(p_i + 1)}{p_1^2 p_2 p_3 \ldots p_t - 1} \\ &\leqslant \frac{(3+1)(5+1)(7+1)\ldots(53+1)}{3^2 \cdot 5 \cdot 7 \cdot \ldots \cdot 53 - 1} \\ &= 24349275917490585600/24441868857892533547 < 1.\end{aligned}$$

Therefore $k_i = 1$ for all i and N is square free. □

Theorem 6.4. *Every standard Lucas d-pseudoprime N with 15 or fewer distinct prime factors is square free.*

P r o o f. The theorem follows immediately from (5.2) and Lemma 6.3. □

Example 6.5. By Theorems 6.1 and 6.4, if $d \leqslant 984$, then every standard Lucas d-pseudoprime is square free.

Stronger results than Theorem 6.4 can be obtained by observing that the primes p_i in the factorization (1) of a Lucas d-pseudoprime are not arbitrary—they are subject to constraints.

Definition 6.6. If $L = p_1, p_2, \ldots, p_t$ is a list of distinct odd primes, and ε is a signature function that supports L, then we say that L is *special* with respect to ε if for all $i \neq j$,

$$p_i \nmid p_j - \varepsilon(p_j). \tag{30}$$

Lemma 6.7. *Suppose that N is an odd integer with decomposition* (1), *ε is a signature function that supports N, and*

$$\frac{\prod_{i=1}^{t}(p_i - \varepsilon(p_i))}{N - \varepsilon(N)} = c \tag{31}$$

is an integer that is relatively prime to N. Then the list of primes $p_1, p_2, \ldots, p_t$ is special with respect to ε.

P r o o f. Let p_i be a prime in the decomposition of N. It follows from (31) that

$$cN - \prod_{i=1}^{t}(p_i - \varepsilon(p_i)) = c\varepsilon(N) = \pm c. \tag{32}$$

If p_i divides $p_j - \varepsilon(p_j)$ for some prime p_j in the decomposition of N, then, by (32), p_i divides c, contrary to our hypotheses. It follows that $p_i \nmid p_j - \varepsilon(p_j)$ for all i and j, and hence the prime divisors of N form a special list with respect to ε. □

Theorem 6.8. *For every standard Lucas d-pseudoprime N with decomposition* (1) *the list of prime factors $p_1, p_2, \ldots, p_t$ of N is special with respect to the signature ε of N.*

P r o o f. The theorem follows immediately from (28) and Lemma 6.7. □

Suppose now that ε is a fixed signature function and $p_1, p_2, \ldots, p_t$ is an increasing list of primes, special with respect to ε, such that the expression

$$N_t^*(\varepsilon) = \frac{\prod_{i=1}^{t}(p_i - \varepsilon(p_i))}{N - \varepsilon(N)} = \frac{N}{N - \varepsilon(N)} \frac{\prod_{i=1}^{t}(p_i - \varepsilon(p_i))}{N} \tag{33}$$

is maximal, where $N = p_1^2 p_2 \ldots p_t$. If $N_t^*(\varepsilon) < 1$, then, as in Lemma 6.3, every standard Lucas d-pseudoprime with t distinct prime factors is square free.

Unfortunately, identifying the primes $p_1, \ldots, p_t$ for which (33) is maximal, much less determining the rate of growth of the expressions $N_t^*(\varepsilon)$ as a function of t, depends upon the signature ε and is a difficult problem. In the remainder of this section, we describe a heuristic for estimating the growth $N_t^*(\varepsilon)$, and offer some computational results and conjectures.

We first observe that for any signature ε,

$$N_t^*(\varepsilon) = \frac{\prod_{i=1}^{t}(p_i - \varepsilon(p_i))}{N - \varepsilon(N)} \leqslant \frac{\prod_{i=1}^{t}(p_i + 1)}{N - 1} \leqslant \frac{\prod_{i=1}^{t}(p_i + 1)}{3\prod_{i=1}^{t} p_i - 1}. \tag{34}$$

It follows that the maximal value of the expression

$$\frac{\prod_{i=1}^{t}(p_i+1)}{3\prod_{i=1}^{t}p_i-1}, \tag{35}$$

taken over all special lists of primes with respect to ε, is an upper bound for $N_t^*(\varepsilon)$.

To bound the maximal value of (35), we computed (35) for lists of primes that are special with respect to the signature ε that is identically -1 and obtained by the greedy algorithm, that is, lists $L = p_1, p_2, \ldots, p_t$ obtained by setting $p_1 = 3$ and including successive primes p_j if $p_i \nmid p_j + 1$ for all $i < j$. It seems reasonable to hypothesize that lists produced in this fashion yield upper bounds for (35) with respect to the signature $\varepsilon = -1$. Moreover, since any prime p that satisfies $\varepsilon(p) = 1$ contributes a factor of $(p-1)/p < 1$ to the rightmost term of (33), we suspect that our computations yield upper bounds for (35) with respect to any signature.

Our computational results are summarized in Tab. 1 and Fig. 1 below. Values of (35) were computed using a straightforward sieve program written in Java using the BigInteger package and verified with a program written in C++ using the `gnu` multiprecision package (`gmp`).

Sieve Size	t	(35)	$f(t)$	Sieve Size	t	(35)	$f(t)$
1000000	19633	0.7931	0.7948	16000000	247180	0.8288	0.8291
2000000	36715	0.8026	0.8033	17000000	261467	0.8295	0.8298
3000000	53170	0.8079	0.8083	18000000	275608	0.8301	0.8306
4000000	69164	0.8117	0.8119	19000000	289672	0.8308	0.8312
5000000	84888	0.8145	0.8146	20000000	303670	0.8314	0.8319
6000000	100332	0.8168	0.8169	21000000	317707	0.8319	0.8325
7000000	115502	0.8187	0.8188	22000000	331722	0.8325	0.8331
8000000	130605	0.8204	0.8205	23000000	345567	0.8330	0.8336
9000000	145597	0.8218	0.8219	24000000	359335	0.8335	0.8342
10000000	160487	0.8231	0.8232	25000000	373337	0.8340	0.8347
11000000	175236	0.8243	0.8244	26000000	387103	0.8344	0.8352
12000000	189789	0.8253	0.8255	27000000	400901	0.8348	0.8356
13000000	204281	0.8263	0.8265	28000000	414703	0.8353	0.8361
14000000	218688	0.8272	0.8274	29000000	428348	0.8357	0.8365
15000000	233017	0.8280	0.8283	30000000	441947	0.8360	0.8369

Table 1. Summary of Estimate (35) Computation.

In the graph, the values of (35) are plotted against t. Each value of (35) is computed from the largest greedy list $p_1, p_2, \ldots, p_t$ satisfying $p_t \leqslant n$, for various sizes n of sieves. The largest sieve tested had $n = 30000000$.

Since

$$\frac{\prod_{i=1}^{t}(p_i+1)}{\prod_{i=1}^{t}p_i-1}\sim\prod_{i=1}^{t}\frac{p_i+1}{p_i}\leqslant\prod_{i=1}^{t}\frac{p_i}{p_i-1}=\prod_{i=1}^{t}\frac{1}{1-1/p_i}\sim\log(t),$$

when the product is taken over *all* primes, we expect (35) to be bounded by a function of the form $\alpha\log(t)+\beta$. We used a linear regression algorithm to find a function $f(t)$ of this form to approximate and bound the computed data. For the sake of comparison, we have included the resulting function, $f(t)=0.013528\log(t)+0.6611$ in Fig. 1.

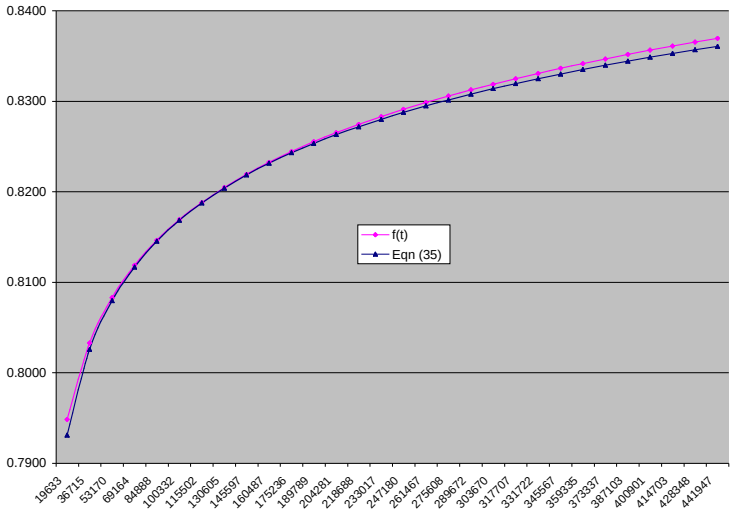

Figure 1. Graph of Estimate (35) and $f(t)$.

Based on our computations, we offer the following result.

Proposition 6.9. *If the greedy algorithm does produce special lists of primes for which* (35) *is maximized, then all standard Lucas d-pseudoprimes with respect to the signature* $\varepsilon=-1$ *having decomposition* (1) *with* $t\leqslant 441947$ *are square free.*

We note that Proposition 6.9 and Theorem 6.1 together imply that all standard Lucas d-pseudoprimes with respect to $\varepsilon=-1$ for which $d<\left(\frac{3}{2}\right)^{441948}-1\sim 1.5\cdot 10^{77823}$ are square free, and conjecture that a similar bound applies to Lucas d-pseudoprimes with respect to any signature.

Finally, since the function $f(t)=0.013528\log(t)+0.6611$ appears to provide an upper bound for (35), and $f(t)<1$ when $t<7.58\times 10^{10}$, we offer the following conjecture.

Conjecture 6.10. *All standard Lucas d-pseudoprimes having decomposition* (1) *with* $t \leqslant 7.58 \times 10^{10}$ *are square free.*

If, indeed, Conjecture 6.10 is correct, Theorem 6.1 implies that all standard Lucas d-pseudoprimes for which $d < 20^{10^{10}}$ are square free, and hence, it is unlikely that anyone will ever encounter a standard Lucas d-pseudoprime that is not square free.

References

[1] *R. Baillie, S. S. Wagstaff, Jr.*: Lucas pseudoprimes. Math. Comput. *35* (1980), 1391–1417. Zbl 0458.10003

[2] *J. Brillhart, D. H. Lehmer, and J. L. Selfridge*: New primality criteria and factorizations of $2^m \pm 1$. Math. Comput. *29* (1975), 620–647. Zbl 0311.10009

[3] *W. Carlip, E. Jacobson, and L. Somer*: Pseudoprimes, perfect numbers, and a problem of Lehmer. Fibonacci Quart. *36* (1998), 361–371. Zbl 0934.11005

[4] *W. Carlip, L. Somer*: Primitive Lucas d-pseudoprimes and Carmichael-Lucas numbers. Colloq. Math. To appear.

[5] *W. Carlip, L. Somer*: Bounds for frequencies of residues of regular second-order recurrences modulo p^r. In: Number Theory in Progress, Vol. 2 (Zakopané-Kościelisko, 1997). de Gruyter, Berlin (1999), 691–719. Zbl 0928.11010

[6] *R. D. Carmichael*: On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$. Ann. of Math. (2) *15* (1913), 30–70. Zbl JFM 44.0216.01

[7] *É. Lucas*: Théorie des fonctions numériques simplement périodiques. Amer. J. Math. *1* (1878), 184–240, 289–321. (In French.) Zbl JFM 10.0134.05

[8] *P. Ribenboim*: The New Book of Prime Number Records. Springer-Verlag, New York, 1996. Zbl 0856.11001

[9] *J. Roberts*: Lure of the Integers. Mathematical Association of America, Washington, DC, 1992.

[10] *L. Somer*: On Lucas d-pseudoprimes. In: Applications of Fibonacci Numbers, Vol. 7 (Graz, 1996). Kluwer Academic Publishers, Dordrecht (1998), 369–375. Zbl 0919.11008

[11] *H. C. Williams*: On numbers analogous to the Carmichael numbers. Can. Math. Bull. *20* (1977), 133–143. Zbl 0368.10011

Authors' addresses: Walter Carlip, Department of Mathematics, Franklin & Marshall College, Lancaster, Pennsylvania, 17604, USA, e-mail: `c3ar@math.uchicago.edu`; Lawrence Somer, Department of Mathematics, Catholic University of America, Washington, D. C. 20064, USA, e-mail: `somer@cua.edu`.