PRIMITIVE LUCAS d-PSEUDOPRIMES AND CARMICHAEL–LUCAS NUMBERS

BY

WALTER CARLIP (Lancaster, PA) and LAWRENCE SOMER (Washington, DC)

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 appearance of \( N \) in \( U(P, Q) \) is exactly \( (N - \varepsilon(N))/d \), where the signature \( \varepsilon(N) = (D/N) \) is given by the Jacobi symbol with respect to the discriminant \( D \) of \( U \). A Lucas \( d \)-pseudoprime \( N \) is a primitive Lucas \( d \)-pseudoprime if \( (N - \varepsilon(N))/d \) is the maximal rank of \( N \) among Lucas sequences \( U(P, Q) \) that exhibit \( N \) as a Lucas pseudoprime.

We derive new criteria to bound the number of \( d \)-pseudoprimes. In a previous paper, it was shown that if \( 4 \nmid d \), then there exist only finitely many Lucas \( d \)-pseudoprimes. Using our new criteria, we show here that if \( d = 4m \), then there exist only finitely many primitive Lucas \( d \)-pseudoprimes when \( m \) is odd and not a square.

We also present two algorithms that produce almost every primitive Lucas \( d \)-pseudoprime with three distinct prime divisors when \( 4 \mid d \) and show that every number produced by these two algorithms is a Carmichael–Lucas number. We offer numerical evidence to support conjectures that there exist infinitely many Lucas \( d \)-pseudoprimes of this type when \( d \) is a square and infinitely many Carmichael–Lucas numbers with exactly three distinct prime divisors.

1. Introduction. Let \( d \) be a fixed, positive integer. In [15], the second author defined a type of Lucas pseudoprime called a Lucas \( d \)-pseudoprime and showed that if \( 4 \mid d \), then there exist only finitely many Lucas \( d \)-pseudoprimes. This was extended in [3] to show that if \( 2^r \) exactly divides \( d \) then there are at most finitely many Lucas \( d \)-pseudoprimes that have at least \( r+2 \) distinct prime divisors. In this paper we offer some useful tools for bounding \( d \)-pseudoprimes and examine in more detail the situation when \( 4 \nmid d \).

In order to generalize the results of [3] and [15] we introduce the concept of a primitive Lucas \( d \)-pseudoprime. A Lucas \( d \)-pseudoprime \( N \) is a primitive Lucas \( d \)-pseudoprime if \( (N - \varepsilon(N))/d \) is the maximal rank of \( N \) among Lucas sequences \( U(P, Q) \) that exhibit \( N \) as a Lucas pseudoprime, or equivalently, if \( N \) is a Lucas \( d \)-pseudoprime, but fails to be a Lucas \( d' \)-pseudoprime for all proper divisors \( d' \) of \( d \). We provide a nice charac-
terization of primitive $d$-pseudoprimes and show that if $d = 4m$, then there exist only finitely many primitive Lucas $d$-pseudoprimes when $m$ is odd and not a square. The proof relies on a more general result that all but a finite number of Lucas $d$-pseudoprimes, for fixed $d$, are standard Lucas $d$-pseudoprimes. Standard Lucas $d$-pseudoprimes are odd composite integers that satisfy $N - \varepsilon(N) = \prod (p - \varepsilon(p))$, where $\varepsilon$ is a signature function that supports $N$ and the product is taken over prime divisors $p$ of $N$. Integers of this form are interesting in their own right.

On the other hand, if $4 \mid d$ and $d$ is a square, then primitive Lucas $d$-pseudoprimes appear to be plentiful. We present two algorithms for generating square-free primitive Lucas $d$-pseudoprimes that have exactly three distinct odd prime divisors when $4 \mid d$ and $d$ is a square. We prove that every number produced by both algorithms is, indeed, a square-free primitive Lucas $d$-pseudoprime with three distinct odd prime divisors and, conversely, that all but a finite number of primitive Lucas $d$-pseudoprimes of this form can be constructed by these algorithms. Moreover, each of the Lucas $d$-pseudoprimes generated by these algorithms is also a Carmichael–Lucas number.

We conjecture that there are an infinite number of primitive Lucas $d$-pseudoprimes with three distinct prime divisors when $d = 4m$ and $m$ is a square, and provide computational evidence supporting our conjecture by finding large numbers of them with our two algorithms. This contrasts with the case that $d = 2m$, with $m$ odd, wherein there are only a finite number of $d$-pseudoprimes with three distinct divisors (see [3]), and with the cases that $d = 1, 2, 3, 5, \text{ or } 6$, wherein there exist at most four Lucas $d$-pseudoprimes (see [15]). Since each of the Lucas $d$-pseudoprimes generated by our algorithms is also a Carmichael–Lucas number, our algorithms also suggest that there are infinitely many Carmichael–Lucas numbers with exactly three distinct prime divisors.

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 [11, pp. 131–132] and also in [12]. Carmichael–Lucas numbers are discussed in [16] and in [4], which also introduces the concept of standard Lucas $d$-pseudoprimes. An algorithm for generating many Carmichael numbers analogous to our algorithm for Carmichael–Lucas numbers was described by J. Chernick in [6].

2. Basic properties of Lucas pseudoprimes. Throughout this paper $N$ denotes a positive odd composite integer with prime decomposition

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

(1)
where \( p_1 < \cdots < p_t \). The Lucas sequence of the first kind with parameters \( P \) and \( Q \) is the second order recurrence sequence \( U(P, Q) = \{U_t\} \) defined by \( U_0 = 0, U_1 = 1 \), and, for all \( n \geq 0 \),

\[
U_{n+2} = PU_{n+1} - QU_n.
\]

The integer \( D = P^2 - 4Q \) is the discriminant of \( U(P, Q) \) and the function \( \varepsilon : \mathbb{N} \to \{-1, 0, 1\} \) given by the Jacobi function \( \varepsilon(n) = (D_n) \) is called the signature of \( U(P, Q) \).

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 \( \varepsilon \) a given signature function, then the restriction \( \varepsilon : \delta(N) \to \{-1, 0, 1\} \) is called the signature of \( N \). We say that \( N \) is supported by \( \varepsilon \) if \( \varepsilon(N) \neq 0 \). Occasionally we need to identify the value of the signature on each prime in the decomposition of an integer \( N \), in which case we sometimes write \( \varepsilon(p_1, \ldots, p_t) \) to denote the \( t \)-tuple \( (\varepsilon(p_1), \ldots, \varepsilon(p_t)) \).

The rank of appearance (or simply the rank) of an integer \( N \) in the sequence \( U(P, Q) \) is the least positive integer \( n \) such that \( N \) divides \( U_n \); it is denoted by \( g(N) \). It is well known that \( g(N) \) always exists when \( (N, QD) = 1 \) and, in this case, \( U_n \equiv 0 \pmod{N} \) if and only if \( g(N) \) divides \( n \). Édouard Lucas [9] proved that if \( (p, QD) = 1 \) for an odd prime \( p \), then \( U_{p-\varepsilon(p)} \equiv 0 \pmod{p} \), and therefore \( g(p) \) divides \( p - \varepsilon(p) \). Composite integers that have a property typical of primes are often known as pseudoprimes, and Lucas’ property motivates the definition of Lucas pseudoprimes.

**Definition 2.1.** An odd composite integer \( N \) is a Lucas pseudoprime with respect to the Lucas sequence \( U(P, Q) \), with discriminant \( D \) and signature \( \varepsilon \), 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 \( g(N) = (N - \varepsilon(N))/d \), then \( N \) is said to be a Lucas \( d \)-pseudoprime.

Note that if \( N \) is a Lucas pseudoprime with signature \( \varepsilon(n) = (D_n) \), then the requirement that \( (N, D) = 1 \) implies that \( \varepsilon \) supports \( N \). Thus every Lucas pseudoprime is supported by its own signature.

We require several number-theoretic functions in our study of pseudoprimes. If \( N \) an odd integer with decomposition (1) that is supported by signature \( \varepsilon \), define

\[
\lambda(N, \varepsilon) = \operatorname{lcm}\{p_i^{k_i-1}(p_i - \varepsilon(p_i)) \mid 1 \leq i \leq t\},
\]

\[
\lambda'(N, \varepsilon) = \operatorname{lcm}\{p_i - \varepsilon(p_i) \mid 1 \leq i \leq t\},
\]

\[
\psi(N, \varepsilon) = \frac{\prod_{i=1}^t (p_i - \varepsilon(p_i))}{2^{t-1}},
\]
\[ \xi(N, \varepsilon) = \prod_{i=1}^{t} \left( \frac{p_i - \varepsilon(p_i)}{N} \right) = \prod_{i=1}^{t} \left( \frac{p_i - \varepsilon(p_i)}{p_i^{k_i}} \right), \]

\[ T(N, \varepsilon) = \frac{\prod_{i=1}^{t} (p_i - \varepsilon(p_i))}{\text{lcm}\{p_i - \varepsilon(p_i) \mid 1 \leq i \leq t\}} = \frac{N \xi(N, \varepsilon)}{\lambda(N, \varepsilon)}. \]

Note that each of these functions depends only on the value of \( \varepsilon \) on the primes that divide \( N \). When \( N \) is a Lucas pseudoprime, we always have in mind a corresponding Lucas sequence \( U(P, Q) \) with signature function \( \varepsilon \), and it is this signature that appears in the evaluation of the functions defined above.

We require several known results on Lucas \( d \)-pseudoprimes. The first is a useful characterization of Lucas \( d \)-pseudoprimes.

**Theorem 2.2.** An integer \( N \) with prime decomposition (1) is a Lucas \( d \)-pseudoprime with signature \( \varepsilon \) if and only if

\[ \frac{N - \varepsilon(N)}{d} \left| \lambda'(N, \varepsilon) \right. \quad \text{and} \quad \left. \left( \frac{N - \varepsilon(N)}{d}, p_i - \varepsilon(p_i) \right) > 1 \right. \]

for all \( i \).

**Proof.** This is Theorem 2.6 of [4].

The final three lemmas in this section describe basic properties of Lucas \( d \)-pseudoprimes and appear in [3].

**Lemma 2.3 (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

\[ \frac{\lambda'(N, \varepsilon)}{N - \varepsilon(N)} = \frac{b}{d} \leq \frac{\psi(N)}{N - \varepsilon(N)} = \frac{c}{d} < 2 \left( \frac{2}{3} \right)^t. \]

**Lemma 2.4 (Lemma 4.2 of [3]).** If \( N \) is a Lucas \( d \)-pseudoprime with prime decomposition (1), then \( t < \log_{3/2}(2d) \).

**Lemma 2.5 (Lemma 4.3 of [3]).** If \( N \) is a Lucas \( d \)-pseudoprime with prime decomposition (1) and \( k_i \geq 2 \), then

\[ p_i^{k_i-1} < 2(2/3)^t(d + 1). \]

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

### 3. Carmichael–Lucas numbers.

Carmichael–Lucas numbers are interesting and oft studied objects (see, e.g., [16], [8], [10], [11], and [4]). For future reference, we define Carmichael–Lucas numbers and present some of their well-known properties.

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

The following two theorems follow immediately from Williams’ work in [16].

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

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

4. **Primitive pseudoprimes.** The primitive Lucas $d$-pseudoprimes compose a subset of the Lucas $d$-pseudoprimes characterized by two extremal conditions. We define primitive $d$-pseudoprimes with a maximal condition as follows.

**Definition 4.1.** Suppose that $N$ is a Lucas pseudoprime with signature $\varepsilon$ and $\Omega$ is the set of all Lucas sequences $U(P, Q)$ with respect to which $N$ is a Lucas pseudoprime with signature $\varepsilon$. Then $N$ is a primitive Lucas $d$-pseudoprime with signature $\varepsilon$ if $(N - \varepsilon(N))/d$ is the maximal rank of $N$ among the sequences in $\Omega$.

Primitive Lucas $d$-pseudoprimes can be characterized by the following theorem.

**Theorem 4.2.** If $N$ is an odd composite integer and $\varepsilon$ a signature that supports $N$, then $N$ is a primitive Lucas $d$-pseudoprime with signature $\varepsilon$ if and only if $(N - \varepsilon(N), \lambda(N, \varepsilon)) = (N - \varepsilon(N))/d$.

**Proof.** Suppose that $\Omega$ is the set of Lucas sequences that exhibit $N$ as a Lucas pseudoprime with signature $\varepsilon$, and let $(N - \varepsilon(N))/d = (N - \varepsilon(N), \lambda(N, \varepsilon))$. Clearly $g_U(N) \mid N - \varepsilon(N)$ for each $U \in \Omega$ and, by a well-known theorem of Carmichael [5], $g_U(N) \mid \lambda(N, \varepsilon)$ as well. It follows that $g_U(N) \mid (N - \varepsilon(N), \lambda(N, \varepsilon))$ for each $U \in \Omega$, and it suffices to show that $g_U(N) = (N - \varepsilon(N))/d$ for some $U \in \Omega$. However, $N - \varepsilon(N)$ is relatively prime to $N$, so $(N - \varepsilon(N), \lambda(N, \varepsilon)) \mid \lambda'(N, \varepsilon)$, and obviously $(N - \varepsilon(N), p_i - \varepsilon(p_i)) > 1$ while $p_i - \varepsilon(p_i) \mid \lambda(N, \varepsilon)$. It follows from Theorem 2.2 that $N$ is a Lucas $d$-pseudoprime, and therefore $(N - \varepsilon(N))/d$ occurs as $g_U(N)$ for some $U \in \Omega$.

If $N$ is a primitive $d$-pseudoprime with signature $\varepsilon$, then $(N - \varepsilon(N))/d$ is the largest rank of $N$ among sequences $U$ that exhibit $N$ as a Lucas pseudoprime and have signature coinciding with $\varepsilon$ on the prime factors of $N$. We note, however, that $N$ may occur with higher rank in Lucas sequences that do not exhibit $N$ as a Lucas pseudoprime, and hence this rank is not
the largest rank of $N$ among all Lucas sequences. This is because the ranks $\varphi_U(N)$ with respect to sequences $U$ that exhibit $N$ as a Lucas pseudoprime all divide $N - \varepsilon(N)$, while in general the rank of $N$ divides $\lambda(N, \varepsilon)$. All ranks higher than $(N - \varepsilon(N))/d$ divide $\lambda(N, \varepsilon)$, but fail to divide $N - \varepsilon(N)$. The following examples from the literature (see, e.g., [14] and [15]) clarify this situation.

**Example 4.3.**

(a) Let $N = 21$ and suppose $\varepsilon(3) = \varepsilon(7) = -1$. It follows that $\varepsilon(N) = 1$, $(N - \varepsilon(N))/5 = 4$, and $\lambda(N, \varepsilon) = \lambda'(N, \varepsilon) = 8$. Clearly $(N - \varepsilon(N), \lambda(N, \varepsilon)) = (20, 8) = 4 = (N - \varepsilon(N))/5$, so $N$ is a primitive Lucas 5-pseudoprime. On the other hand, the maximal rank $\lambda(N, \varepsilon) = 8$ does occur.

(b) Let $N = 25$ and suppose $\varepsilon(5) = 1$. Then $\varepsilon(N) = 1$, $(N - \varepsilon(N))/6 = 4$, and $\lambda(N, \varepsilon) = 20$. Clearly we have $(N - \varepsilon(N), \lambda(N, \varepsilon)) = (24, 20) = 4 = (N - \varepsilon(N))/6$, so $N$ is a primitive Lucas 6-pseudoprime. On the other hand, the maximal rank $\lambda(N, \varepsilon) = 20$ does occur.

(c) Let $N = 49$ and suppose $\varepsilon(7) = -1$. Then $\varepsilon(N) = 1$, $(N - \varepsilon(N))/6 = 8$, and $\lambda(N, \varepsilon) = 56$. Clearly $(N - \varepsilon(N), \lambda(N, \varepsilon)) = (48, 56) = 8 = (N - \varepsilon(N))/6$, so $N$ is a primitive Lucas 6-pseudoprime. On the other hand, the maximal rank $\lambda(N, \varepsilon) = 56$ does occur.

Primitive Lucas $d$-pseudoprimes can also be described by a minimality property.

**Theorem 4.4.** An odd composite integer $N$ is a primitive Lucas $d$-pseudoprime with signature $\varepsilon$ if and only if $N$ is a Lucas $d$-pseudoprime with respect to signature $\varepsilon$, but fails to be a Lucas $d'$-pseudoprime with respect to signature $\varepsilon$ for all proper divisors $d'$ of $d$.

**Proof.** Suppose $N$ is a Lucas $d$-pseudoprime, but not a Lucas $d'$-pseudoprime for any proper divisor $d'$ of $d$. Let $(N - \varepsilon(N))/k = (N - \varepsilon(N), \lambda(N, \varepsilon))$. By [5], $(N - \varepsilon(N))/d \mid \lambda(N, \varepsilon)$ and hence $(N - \varepsilon(N))/d \mid (N - \varepsilon(N))/k$ and $k \mid d$. By Theorem 4.2, $N$ is a primitive Lucas $k$-pseudoprime, and therefore certainly a Lucas $k$-pseudoprime. By hypothesis, $k$ cannot be a proper divisor of $d$, so $k = d$ and $N$ is a primitive Lucas $d$-pseudoprime.

The converse follows immediately from the definition.

**Theorem 4.5.** Suppose that $N$ is a Lucas $d$-pseudoprime with signature $\varepsilon$ and that $b$ is given by (8). Then $N$ is a primitive $d$-pseudoprime if and only if $(b, d) = 1$. If $N$ is also square free, then $N$ is a Carmichael–Lucas number if and only if $b = 1$.

**Proof.** The first assertion follows immediately from Theorem 4.2, and the second from Theorems 3.2 and 3.3.
The example below illustrates the previous theorems. Note that in general each Lucas $d$-pseudoprime is also a primitive $d'$-pseudoprime for some $d'$ dividing $d$.

**Example 4.6.** Let $N = 186961 = 31 \cdot 37 \cdot 163$ and choose a signature $\varepsilon$ such that $\varepsilon(31) = 1$, $\varepsilon(37) = -1$, and $\varepsilon(163) = -1$.

Then $\varepsilon(186961) = 1$, and $(186961 - 1)/12 = ((186961 - 1)/4)/3 = 15580$, which divides $(186961 - 1)/4 = \lambda'(N,\varepsilon)$. Moreover, $((N - \varepsilon(N))/12, 30) = (15580, 30) = 10 \neq 1$, $((N - \varepsilon(N))/12, 38) = (15580, 38) = 38 \neq 1$, and $((N - \varepsilon(N))/12, 164) = (15580, 164) = 164 \neq 1$. By Theorem 2.2, $N$ is a Lucas 12-pseudoprime with respect to the signature $\varepsilon$. However, since $\lambda'(N,\varepsilon)/(N - \varepsilon(N)) = 1/4 = 3/12$, $N$ is not a primitive Lucas 12-pseudoprime with respect to $\varepsilon$.

On the other hand, $\lambda(N,\varepsilon) = \lambda'(N,\varepsilon) = \text{lcm}\{30, 38, 164\} = 46740 = (186961 - 1)/4 = (N - \varepsilon(N))/4$. It follows that $N$ is a primitive 4-pseudoprime with respect to $\varepsilon$ and, since $\lambda'(N,\varepsilon)/(N - \varepsilon(N)) = 1/4$, $N$ is also a Carmichael–Lucas number with respect to $\varepsilon$.

**5. Machinery.** We require the following notation and results from [3]. Define $\delta(N) = \{p \mid p \text{ divides } N\}$ and, if $\Omega$ is a set of natural numbers, define

$$
\delta(\Omega) = \bigcup_{N \in \Omega} \delta(N).
$$

If $N$ has decomposition (1), write

$$
N_1 = \prod_{i=1}^{t} p_i, \quad N_2 = \prod_{i=1}^{t} p_i^{k_i-1},
$$

so that $N = N_1 N_2$ with $N_1$ square free.

The following theorems are the primary tool and the main theorem of [3].

**Theorem 5.1** (Theorem 2.3 of [3]). Suppose that $\Omega$ is an infinite set of positive integers with each $N \in \Omega$ supported by corresponding signature $\varepsilon$ and for which $|\delta(N)| = t$ for all $N \in \Omega$. Suppose as well that $\{N_2 \mid N \in \Omega\}$ is bounded. If $c$ and $d$ are integers such that $(N, d) = 1$ for all $N \in \Omega$ and

$$
\lim_{N \in \Omega} \xi(N) = c/d,
$$

then $c = d$.

**Theorem 5.2** (Theorem 4.4 of [3]). Let $d$ be a fixed positive integer and suppose that $2^r$ exactly divides $d$. Then there are at most a finite number of Lucas $d$-pseudoprimes $N$ such that $|\delta(N)| \geq r + 2$. 

---

**PRIMITIVE LUCAS $d$-PSEUDOPRIMES**

---
6. Bounds. In this section we present our main results on $d$-pseudoprimes, along with a few useful lemmas. Several of these results concern bounds on the number of $d$-pseudoprimes with a fixed number of distinct prime divisors.

**Definition 6.1.** Denote by $\mathcal{N}_d(t)$ the number of distinct $d$-pseudoprimes $N$ with exactly $t$ distinct prime divisors.

**Theorem 6.2.** Let $d$ be a fixed positive integer. Then only a finite number of Lucas $d$-pseudoprimes have exactly one prime divisor. In fact, $\mathcal{N}_d(1) < d \log(2d)$.

**Proof.** It follows immediately from Lemma 2.5 that $\mathcal{N}_d(1)$ is finite. Moreover, for a given prime $p$ and positive integer $k$, for $p^k$ to be a $d$-pseudoprime it is necessary that

\[(12) \quad p^{k-1} < \frac{4(d+1)}{3} \leq 2d.\]

Now $p^{k-1} < 2d$ if and only if $k - 1 < \log(2d)/\log(p) < \log(2d)$. Since $\pi(2d) \leq d$, there are at most $\pi(2d) \log(2d) \approx d \log(2d)$ prime powers less than $2d$, and it follows that $\mathcal{N}_d(1) < d \log(2d)$. \(\blacksquare\)

Of course $d$ is, in general, a poor estimate of $\pi(2d)$. By the prime number theorem, $\pi(2d) \sim 2d/\log(2d)$, which suggests that $2d$ is a better upper bound for $\mathcal{N}_d(1)$.

Before we consider $d$-pseudoprimes divisible by exactly two distinct primes, we prove a general finiteness criterion for an important class of Lucas $d$-pseudoprimes, the standard Lucas $d$-pseudoprimes. We show in Theorem 6.4 that all but a finite number of Lucas $d$-pseudoprimes are standard.

**Definition 6.3.** A Lucas $d$-pseudoprime $N$ is called **standard** if

\[(13) \quad N - \varepsilon(N) = \prod_{i=1}^{t} (p_i - \varepsilon(p_i)),\]

and **exceptional** otherwise.

Observe that the condition (13) may be reformulated as

\[(14) \quad bT(N, \varepsilon) = d,\]

where, as usual, $b$ is given by (8).

We make two easy observations about standard Lucas $d$-pseudoprimes. First, if $N$ is a square-free standard Lucas $d$-pseudoprime, then Theorem 3.3 implies that $N$ is a Carmichael–Lucas number. Second, if $N$ is a primitive standard Lucas $d$-pseudoprime, then Theorem 4.5 implies that $(b, d) = 1$, and therefore $b = 1$ and $T(N, \varepsilon) = d$. 

Theorem 6.4. Let $d$ be a fixed positive integer. Then there exist at most finitely many exceptional Lucas $d$-pseudoprimes.

Proof. For a fixed positive integer $d$, let $\Omega^*$ be the set of Lucas $d$-pseudoprimes that satisfy $bT(N, \varepsilon) \neq d$ and, by way of contradiction, suppose that $\Omega^*$ has infinite cardinality.

By Lemma 2.4, the number of distinct primes in the decomposition of elements of $\Omega^*$ is bounded, so there exists an integer $t$ such that an infinite number of elements of $\Omega^*$ have exactly $t$ distinct prime divisors. By Lemma 2.3, corresponding to each $N \in \Omega^*$ there exist integers $b$ and $c$ satisfying (8), and among those with exactly $t$ distinct prime divisors, there are only a finite number of possible values of $b$ and $c$. Consequently, there exist fixed integers $b$ and $c$ such that the subset $\Omega \subseteq \Omega^*$ consisting of those elements of $\Omega^*$ that have exactly $t$ distinct prime divisors and satisfy (8) for these fixed values of $b$ and $c$ has infinite cardinality.

By Lemma 2.5, the powers of the primes occurring in decompositions of elements of $\Omega$ are bounded. It follows that $\delta(\Omega)$ is unbounded, and consequently

$$\lim_{N \in \Omega} \frac{\varepsilon(N)}{\psi(N)} = 0.$$ 

It then follows that

$$\frac{2^{t-1}c}{d} = 2^{t-1} \frac{\psi(N)}{N - \varepsilon(N)} = 2^{t-1} \lim_{N \in \Omega} \frac{\psi(N)}{N - \varepsilon(N)} = 2^{t-1} \lim_{N \in \Omega} \frac{1}{\frac{N - \varepsilon(N)}{\psi(N)}}$$

$$= 2^{t-1} \lim_{N \in \Omega} \frac{1}{\frac{N}{\psi(N)} - \frac{\varepsilon(N)}{\psi(N)}} = 2^{t-1} \lim_{N \in \Omega} \frac{\psi(N)}{N} = \lim_{N \in \Omega} \lambda(N, \varepsilon).$$

By Lemma 2.5, $\{N \mid N \in \Omega\}$ is bounded and, by Lemma 2.3, $(N, d) = 1$ for all $N \in \Omega$. Moreover, by definition of Lucas $d$-pseudoprime, each Lucas $d$-pseudoprime $N \in \Omega$ is supported by its own signature. Therefore, Theorem 5.1 implies that $2^{t-1}c/d = 1$.

Now,

$$d = d \frac{2^{t-1}c}{d} = d \frac{2^{t-1}\psi(N)}{N - \varepsilon(N)} = d \frac{2^{t-1}\psi(N)}{\lambda'(N, \varepsilon)} \frac{\lambda'(N, \varepsilon)}{N - \varepsilon(N)}$$

$$= dT(N, \varepsilon) \frac{b}{d} = bT(N, \varepsilon).$$

This contradicts our original hypothesis and completes the proof. □

This criterion has several interesting consequences. First of these is that for any fixed integer $d$, there are only a finite number of $d$-pseudoprimes with exactly two distinct prime factors.
Theorem 6.5. Let $d$ be a fixed positive integer. Then only a finite number of Lucas $d$-pseudoprimes have exactly two distinct prime divisors.

Proof. Assume that there are an infinite number of Lucas $d$-pseudoprimes with exactly two distinct prime divisors, and let $\Omega$ be the set of those that are standard. By Theorem 6.4, $\Omega$ has infinite cardinality.

If $N \in \Omega$ has decomposition (1), then
\begin{equation}
(p_1 - \varepsilon(p_1))(p_2 - \varepsilon(p_2)) = N - \varepsilon(N) = p_1^{k_1}p_2^{k_2} - \varepsilon(p_1)^{k_1}\varepsilon(p_2)^{k_2}.
\end{equation}
If either $k_1 > 1$ or $k_2 > 1$, then
\begin{align*}
1 &= \frac{(p_1 - \varepsilon(p_1))(p_2 - \varepsilon(p_2))}{N - \varepsilon(N)} = \frac{(p_1 - \varepsilon(p_1))(p_2 - \varepsilon(p_2))}{p_1^{k_1}p_2^{k_2} - \varepsilon(N)} \\
&\leq \frac{(p_1 + 1)(p_2 + 1)}{p_1^2p_2 - 1} \leq \frac{(3 + 1)(5 + 1)}{9 \cdot 5 - 1} = \frac{24}{44} < 1,
\end{align*}
a contradiction.

Therefore $k_1 = k_2 = 1$ and (15) yields
\begin{equation}
p_1\varepsilon(p_2) + p_2\varepsilon(p_1) = 2\varepsilon(p_1)\varepsilon(p_2).
\end{equation}
If $\varepsilon(p_1) = \varepsilon(p_2)$, then $p_1 + p_2 = \pm 2$, which is impossible. Since $p_2 > p_1$, it follows that $\varepsilon(p_1) = -1$, $\varepsilon(p_2) = 1$, and $p_2 - p_1 = 2$. In particular, $p_1$ and $p_2$ are twin primes. Now (15) implies that
\begin{equation}
\frac{d}{b} = \frac{N - \varepsilon(N)}{\text{lcm}\{p_1 - \varepsilon(p_1), p_2 - \varepsilon(p_2)\}} = \frac{p_1(p_1 + 2) + 1}{\text{lcm}\{p_1 + 1, p_1 + 2 - 1\}} = p_1 + 1,
\end{equation}
and therefore $d = b(p_1 + 1)$. Clearly, there are only finitely many prime twins $p_1$ and $p_1 + 2$ such that $p_1 + 1$ divides $d$, and hence $\Omega$ has finite cardinality, a contradiction.

Next, we consider the consequences of Theorem 6.4 to primitive Lucas $d$-pseudoprimes.

Theorem 6.6. Let $d$ be a fixed positive integer. Then there exist at most finitely many primitive Lucas $d$-pseudoprimes $N$ such that $T(N, \varepsilon) \neq d$.

Proof. By Theorem 6.4 all but a finite number of the primitive Lucas $d$-pseudoprimes are standard and, as previously noted, these satisfy $T(N, \varepsilon) = d$. ■

Our final result of this section applies the main theorem of [3]. To simplify the exposition, we begin with a useful lemma.

Lemma 6.7. If $N = p_1p_2p_3$ is a product of three distinct primes, $\varepsilon$ is a signature function that supports $N$ and
\begin{equation}
(p_1 - \varepsilon(p_1))(p_2 - \varepsilon(p_2))(p_3 - \varepsilon(p_3)) = p_1p_2p_3 - \varepsilon(p_1p_2p_3),
\end{equation}
then the integer
\[ d = \frac{(p_1 - \varepsilon(p_1))(p_2 - \varepsilon(p_2))(p_3 - \varepsilon(p_3))}{\text{lcm}\{p_1 - \varepsilon(p_1), p_2 - \varepsilon(p_2), p_3 - \varepsilon(p_3)\}} = T(N, \varepsilon) \]

is a perfect square.

**Proof.** Suppose that \( p \) is a prime and \( p^k \parallel \text{lcm}\{p_1 - \varepsilon(p_1), p_2 - \varepsilon(p_2), p_3 - \varepsilon(p_3)\} \) and \( p^{k_1} \parallel p_1 - \varepsilon(p_1), p^{k_2} \parallel p_2 - \varepsilon(p_2), \) and \( p^{k_3} \parallel p_3 - \varepsilon(p_3). \) Then \( k = \max\{k_1, k_2, k_3\}. \) Since we have made no assumptions about the ordering of the primes, we may assume, without loss of generality, that \( k = k_1. \) Then (18) implies that
\[ p_1p_2p_3 - \varepsilon(p_1p_2p_3) \equiv (p_1 - \varepsilon(p_1))(p_2 - \varepsilon(p_2))(p_3 - \varepsilon(p_3)) \equiv 0 \pmod{p^{k_2}}, \]
and therefore
\[ \varepsilon(p_1)\varepsilon(p_2)(p_3 - \varepsilon(p_3)) \equiv p_2p_3(p_1 - \varepsilon(p_1)) + \varepsilon(p_1)\varepsilon(p_2)(p_3 - \varepsilon(p_3)) \]
\[ \equiv p_1p_2p_3 - \varepsilon(p_1)\varepsilon(p_2)(p_3 - \varepsilon(p_3)) - \varepsilon(p_1)p_3(p_2 - \varepsilon(p_2)) \]
\[ \equiv 0 \pmod{p^{k_2}}. \]

Since \( \varepsilon(p_1)\varepsilon(p_2) = \pm 1, \) it follows that \( p^{k_2} \mid p_3 - \varepsilon(p_3), \) i.e., \( k_2 \leq k_3. \)

Similarly,
\[ p_1p_2p_3 - \varepsilon(p_1p_2p_3) \equiv (p_1 - \varepsilon(p_1))(p_2 - \varepsilon(p_2))(p_3 - \varepsilon(p_3)) \equiv 0 \pmod{p^{k_3}}, \]
and therefore
\[ \varepsilon(p_1)\varepsilon(p_3)(p_2 - \varepsilon(p_2)) \equiv p_2p_3(p_1 - \varepsilon(p_1)) + \varepsilon(p_1)\varepsilon(p_3)(p_2 - \varepsilon(p_2)) \]
\[ \equiv p_1p_2p_3 - \varepsilon(p_1)\varepsilon(p_3)(p_2 - \varepsilon(p_2)) - \varepsilon(p_1)p_2(p_3 - \varepsilon(p_3)) \]
\[ \equiv 0 \pmod{p^{k_3}}. \]

Now \( \varepsilon(p_1)\varepsilon(p_3) = \pm 1, \) and therefore \( p^{k_3} \mid p_2 - \varepsilon(p_2), \) i.e., \( k_3 \leq k_2. \)

We now see that \( k_2 = k_3 \leq k_1, \) and hence \( p^{k_1} \parallel \lambda'(N, \varepsilon), \) while \( p^{k_1+2k_2} \parallel (p_1 - \varepsilon(p_1))(p_2 - \varepsilon(p_2))(p_3 - \varepsilon(p_3)). \) Thus, \( p^{2k_2} \parallel d, \) and it follows that every prime in the factorization of \( d \) occurs to an even power. Therefore \( d \) is a perfect square. \( \blacksquare \)

**Theorem 6.8.** If \( d = 4m, \) with \( m \) odd and not a square, then there exist only finitely many primitive Lucas \( d \)-pseudoprimes.

**Proof.** Assume that \( d = 4m, \) with \( m \) odd and not a square. By Theorems 6.4, 6.2, 6.5, and 5.2, we need only show that there are at most finitely many primitive standard Lucas \( d \)-pseudoprimes with exactly three distinct prime divisors. In fact, we will show that there are none.

Suppose that \( N \) is a primitive standard Lucas \( d \)-pseudoprime with exactly three distinct prime divisors. Then \( b = 1 \) and
\[ 3 \prod_{i=1}^{3}(p_i - \varepsilon(p_i)) = d\lambda'(N, \varepsilon) = N - \varepsilon(N). \]
Now if $p^2 \mid N$ for some prime $p$, then (20) implies that
\begin{align}
1 &= \frac{\prod_{i=1}^{3}(p_i - \varepsilon(p_i))}{N - \varepsilon(N)} < \frac{\prod_{i=3}^{t}(p_i - \varepsilon(p_i))}{p_1^2 p_2 p_3 - 1} \\
&\leq \frac{(3 + 1)(5 + 1)(7 + 1)}{9 \cdot 5 \cdot 7 - 1} = \frac{192}{314} < 1,
\end{align}
a contradiction. Thus $N$ is square free, and

\[(p_1 - \varepsilon(p_1))(p_2 - \varepsilon(p_2))(p_3 - \varepsilon(p_3)) = p_1 p_2 p_3 - \varepsilon(p_1 p_2 p_3).
\]

By Lemma 6.7, $d$ is a perfect square, contrary to the hypotheses.

7. Numerical results. In this final section we present some computational results. We describe two algorithms that produce Lucas $d$-pseudoprimes with three distinct prime factors. The integer $d$ is a byproduct of the algorithms and is always an even perfect square. We prove that these algorithms always produce primitive Lucas $d$-pseudoprimes that are also Carmichael–Lucas numbers and show that the two algorithms together generate all but a finite number of the primitive $d$-pseudoprimes of this form.

We have implemented the algorithms in Java, C++, and GAP [7], and present computational evidence that the algorithms can be used to produce many primitive Lucas $d$-pseudoprimes (for many values of $d$) and many Carmichael–Lucas numbers. Unfortunately, although it seems likely that these algorithms can produce an infinite number of primitive Lucas $d$-pseudoprimes for any fixed $d$, a proof of this conjecture seems intractable.

**Algorithm 7.1.**

1. Choose an odd positive integer $k > 1$ such that $-3$ is a square modulo $k$ and find $\alpha$ such that $\alpha^2 \equiv -3 \pmod{k}$.
2. Choose an odd prime $p_1$ such that $p_1 \equiv (1 + \alpha)/2 \pmod{k}$ and both $p_2 = p_1 - 1 + k$ and $p_3 = (p_1(p_2 + 1) - p_2)/k$ are primes.
3. Set $m = \text{lcm}\{p_1 - 1, p_2 + 1, p_3 + 1\}$.
4. Set $N = p_1 p_2 p_3$ and $d = (N - 1)/m$.

We prove below that each $N$ generated by Algorithm 7.1 is a primitive Lucas $d$-pseudoprime. For each value of $k$ chosen in Algorithm 7.1, construction of a primitive $d$-pseudoprime $N$ requires finding values of $x$ such that the three functions $f_1(x) = x$, $f_2(x) = x - 1 + k$, and $f_3(x) = (x(x + k) - x + 1 - k)/k = (1/k)(x^2 + (k - 1)x - (k - 1))$ are prime. Thus, Algorithm 7.1 will produce an infinite number of primitive $d$-pseudoprimes (for a possibly infinite number of values for $d$) if Schinzel and Sierpiński’s Hypothesis H (see [13]) is valid.

**Remark.** Although no ordering of the primes $p_1$, $p_2$, and $p_3$ is assumed in Algorithm 7.1, it is easy to see that $p_1 < p_2$. Moreover, by Step 2 of
Algorithm 7.1,

\[ p_3 = \frac{p_1(p_1 + k) - p_1 + 1 - k}{k} = \frac{p_1^2 - p_1 + 1}{k} + p_1 - 1. \]

Since Step 2 of Algorithm 7.1 implies that \( k \mid p_1^2 - p_1 + 1 \), it follows that \( p_3 \) is automatically an integer, and \( p_1 \leq p_3 \). If \( p_1 = p_3 \), then \( k = p_1^2 - p_1 + 1 \), which implies that \( p_2 = p_1^2 \), impossible since \( p_2 \) is prime. Thus \( p_1 < p_3 \). Now, if \( p_2 = p_3 \), then \( kp_2 = p_1(p_2 + 1) - p_2 \), and it follows that \( p_2 \mid p_1 \), which is impossible. Thus, the primes \( p_1, p_2, \) and \( p_3 \) are necessarily distinct. Finally, we note that if \( p_1^2 - p_1 + 1 > k^2 \), then (22) implies that \( p_3 > p_2 \). In this case, we obtain the usual ordering \( p_1 < p_2 < p_3 \).

**Algorithm 7.2.**

1. Choose an odd positive integer \( k \) such that \(-3 \) is a square modulo \( k \) and find \( \alpha \) such that \( \alpha^2 \equiv -3 \pmod{k} \).
2. Choose an odd prime \( p_1 \) such that \( p_1 \equiv (-1 + \alpha)/2 \pmod{k} \) and both \( p_2 = p_1 + 1 + k \) and \( p_3 = (p_1(p_2 - 1) + p_2)/k \) are primes.
3. Compute \( m = \text{lcm}(p_1 + 1, p_2 - 1, p_3 - 1) \).
4. Set \( N = p_1p_2p_3 \) and \( d = (N + 1)/m \).

As with the previous algorithm, Algorithm 7.2 will produce an infinite number of primitive \( d \)-pseudoprimes (again, for a potentially infinite number of values for \( d \)) if Schinzel and Sierpiński’s Hypothesis H is valid, in this case, applied to the polynomials \( g_1(x) = x, g_2(x) = x + 1 + k \), and \( g_3(x) = (x(x + k) + x + 1 + k)/k = (1/k)(x^2 + (k + 1)x + (k + 1)) \).

**Remark.** Although no ordering of the primes \( p_1, p_2, \) and \( p_3 \) is assumed in Algorithm 7.2, it is easy to see that \( p_1 < p_2 \). Moreover, by Step 2 of Algorithm 7.2,

\[ p_3 = \frac{p_1(p_1 + k) + p_1 + 1 + k}{k} = \frac{p_1^2 + p_1 + 1}{k} + p_1 + 1. \]

Since Step 2 of Algorithm 7.2 implies that \( k \mid p_1^2 + p_1 + 1 \), it follows that \( p_3 \) is automatically an integer, and \( p_1 < p_3 \). In addition, if \( p_2 = p_3 \), then \( kp_2 = p_1(p_2 - 1) + p_2 \), and it follows that \( p_2 \mid p_1 \), which is impossible. Thus, the primes \( p_1, p_2, \) and \( p_3 \) are necessarily distinct. Finally, we note that if \( p_1^2 + p_1 + 1 > k^2 \), then (23) implies that \( p_3 > p_2 \). In this case, we obtain the usual ordering \( p_1 < p_2 < p_3 \).

The next two theorems verify that Algorithms 7.1 and 7.2 do, indeed, produce primitive \( d \)-pseudoprimes.

**Theorem 7.3.** Each integer \( N = p_1p_2p_3 \) produced by Algorithm 7.1 is a Carmichael–Lucas number and a primitive Lucas \( d \)-pseudoprime with signature \( \varepsilon \) satisfying \( \varepsilon(p_1, p_2, p_3) = (1, -1, -1) \). Furthermore \( 4 \mid d, 3 \nmid d, \) and \( d \) is a square.
Proof. It is immediate from the construction of $N$ that

$$(24) \quad \lambda(N, \varepsilon) = \lambda'(N, \varepsilon) = \frac{N - \varepsilon(N)}{d} = \frac{(p_1 - \varepsilon(p_1))(p_2 - \varepsilon(p_2))(p_3 - \varepsilon(p_3))}{d},$$

for $\varepsilon(p_1, p_2, p_3) = (1, -1, -1)$ Thus Theorem 4.2 implies that $N$ is a primitive $d$-pseudoprime and $b = 1$. Since $b = 1$ and $N$ is square free and primitive, Theorem 4.5 implies that $N$ is a Carmichael–Lucas number.

The fact that $4 \mid d$ follows immediately from (24), and the fact that $d$ is a square follows from Lemma 6.7. Thus it remains only to prove that $3 \nmid d$.

Since $\left(\frac{-3}{k}\right) = 1$ and $-3$ is not a quadratic residue modulo 9, quadratic reciprocity and the Chinese remainder theorem imply that $k$ has prime decomposition

$$(25) \quad k = 3^r \prod_{i=1}^{s} q_i,$$

where $r = 0$ or $r = 1$ and each prime $q_i$ satisfies $q_i \equiv 1 \pmod{6}$. The primes $q_i$ in (25) need not be distinct.

It follows from (25) that either $k \equiv 1 \pmod{6}$ or $k \equiv 3 \pmod{9}$.

First suppose that $k \equiv 1 \pmod{6}$. If $p_1 = 3$, then $p_2 = p_1 - 1 + k \equiv 0 \pmod{3}$, which is a contradiction, since $p_2 > p_1$. Therefore $p_1 \equiv 1 \pmod{3}$ or $p_1 \equiv 2 \pmod{3}$. In either case, $p_2 \equiv p_1 - 1 + k \equiv p_1 \pmod{3}$ and $p_3 \equiv kp_3 \equiv p_1(p_2 + 1) - p_2 \equiv p_1^2 \equiv 1 \pmod{3}$. In this case, exactly one of $p_1 - 1$, $p_2 + 1$, and $p_3 + 1$ is divisible by 3, and, by (24), $d$ is not divisible by 3.

Now suppose instead that $k \equiv 3 \pmod{9}$. Then $p_2 = p_1 - 1 + k \equiv p_1 + 2 \pmod{9}$ and $3p_3 \equiv kp_3 \equiv p_1(p_2 + 1) - p_2 \equiv p_1^2 + 2p_1 - 2 \pmod{9}$. Thus, if $p_1 - 1$ is divisible by 3, then $p_1 \equiv 1, 4, \text{ or } 7 \pmod{9}$ and $3p_3 \equiv 1, 4, \text{ or } 7 \pmod{9}$. None of these is possible, so $p_1 - 1$ is not divisible by 3. On the other hand, $3p_3 \equiv kp_3 \equiv p_1(p_2 + 1) - p_2 \equiv (p_2 + 1 - k)(p_2 + 1) - p_2 \equiv p_2^2 - 2p_2 - 2 \pmod{9}$. If $p_2 + 1$ is divisible by 3, then $p_2 \equiv 2, 5, \text{ or } 8 \pmod{9}$, and again $3p_3 \equiv 1, 4, \text{ or } 7 \pmod{9}$. None of these is possible, so $p_2 + 1$ is not divisible by 3. It now follows that at most one of $p_1 - 1$, $p_2 + 1$, and $p_3 + 1$ is divisible by 3, and, by (24), $d$ is not divisible by 3.

Thus, in all cases $3 \nmid d$, as desired. \[\blacksquare\]

Theorem 7.4. Each integer $N = p_1p_2p_3$ produced by Algorithm 7.2 is a Carmichael–Lucas number and a primitive Lucas $d$-pseudoprime with signature $\varepsilon$ satisfying $\varepsilon(p_1, p_2, p_3) = (-1, 1, 1)$. Furthermore $4 \mid d$, $d$ is a square and, with the sole exception of the 16-pseudoprime 255, 9 $\mid d$. 
Proof. As before, it is immediate from the construction of $N$ that
\[
\lambda(N, \varepsilon) = \lambda'(N, \varepsilon) = \frac{N - \varepsilon(N)}{d} = \frac{(p_1 - \varepsilon(p_1))(p_2 - \varepsilon(p_2))(p_3 - \varepsilon(p_3))}{d},
\]
for $\varepsilon(p_1, p_2, p_3) = (-1, 1, 1)$. Thus Theorem 4.2 implies that $N$ is a primitive $d$-pseudoprime and $b = 1$. Since $b = 1$ and $N$ is square free and primitive, Theorem 4.5 implies that $N$ is a Carmichael–Lucas number.

The fact that $4 \mid d$ again follows from (26), and the fact that $d$ is a square follows from Lemma 6.7. Thus it remains only to prove that $9 \mid d$ when $N \neq 255$.

As in Theorem 7.3, the fact that $-3$ is a quadratic residue modulo $k$ forces (25) to hold, and again, either $k \equiv 1 \pmod{6}$ or $k \equiv 3 \pmod{9}$.

First suppose that $p_1 = 3$. Since $p_1$ is a root of $x^2 + x + 1$ modulo $k$, we see that $k \mid 13$. Therefore $k = 1$ or $k = 13$. In the former case, we obtain $p_1 = 3$, $p_2 = 5$, and $p_3 = 17$; in the latter case, we obtain $p_1 = 3$, $p_2 = 17$, and $p_3 = 5$. In both cases, $N$ is the primitive 16-pseudoprime 255.

Now assume that $p_1 > 3$ and $k \equiv 1 \pmod{6}$. Then $p_1 \equiv 1 \pmod{3}$ or $p_1 \equiv 2 \pmod{3}$. It follows that $p_2 = p_1 + 1 + k \equiv p_1 + 2 \pmod{3}$. If $p_1 \equiv 1 \pmod{3}$, then this implies that $p_2 \equiv 0 \pmod{3}$, which is impossible, since $p_2 > p_1 > 3$. Therefore $p_1 \equiv 2 \pmod{3}$, $p_2 \equiv 1 \pmod{3}$, and $p_3 \equiv kp_3 \equiv p_1(p_2 - 1) + p_2 \equiv 1 \pmod{3}$. It follows that all three of $p_1 + 1$, $p_2 - 1$, and $p_3 - 1$ are divisible by 3 and, by (26), $d$ is divisible by 9.

Finally, assume that $p_1 > 3$ and $k \equiv 3 \pmod{9}$. Again, either $p_1 \equiv 1 \pmod{3}$ or $p_1 \equiv 2 \pmod{3}$. But $p_1$ is a root of $x^2 + x + 1$ modulo 3, and hence $p_1 \equiv 1 \pmod{3}$. It follows that $p_1 \equiv 1, 4, or 7 \pmod{9}$, and $p_2 = p_1 + 1 + k \equiv 5, 8, or 2 \pmod{9}$. But then, in every case, $3p_3 \equiv kp_3 \equiv p_1(p_2 - 1) + p_2 \equiv 0 \pmod{9}$. It follows that $3 \mid p_3$, a contradiction, since $p_3 > p_1 > 3$. Thus this final case never occurs.

**Theorem 7.5.** Let $d = 4m$ for some integer $m$. Then all but a finite number of primitive Lucas $d$-pseudoprimes with exactly three distinct prime factors can be generated by Algorithm 7.1 or Algorithm 7.2.

**Proof.** Fix $d = 4m$ and let $\Omega$ be the set of standard primitive Lucas $d$-pseudoprimes $N$ that have exactly three distinct prime factors. By Theorem 6.4, $\Omega$ contains all but a finite number of the primitive Lucas $d$-pseudoprimes with exactly three distinct prime factors. By (21) and the argument given in the proof of Theorem 6.8, each $N \in \Omega$ is square free, and we write $N = p_1p_2p_3$ with the usual ordering $p_1 < p_2 < p_3$. Moreover, as in the proof of Theorem 6.8, each $N \in \Omega$ satisfies (20).

Clearly (20) cannot hold if either $\varepsilon(p_1, p_2, p_3) = (1, 1, 1)$ or $\varepsilon(p_1, p_2, p_3) = (-1, -1, -1)$. In fact, it is easy to show that (20) also fails if $\varepsilon(p_1, p_2, p_3)$ is
one of \((1, -1, 1), (1, 1, -1), (-1, 1, -1), \) or \((-1, -1, 1)\). Thus, for example, if 
\[
\varepsilon(p_1, p_2, p_3) = (-1, 1, -1),
\]
then
\[
\prod_{i=1}^{3} (p_i - \varepsilon(p_i)) - N + \varepsilon(N) = (p_1 + 1)(p_2 - 1)(p_3 + 1) - p_1p_2p_3 + 1
\]
\[
= p_1p_2 - p_1p_3 + p_2p_3 - p_1 + p_2 - p_3 = p_3(p_2 - p_1 - 1) + p_1(p_2 - 1) + p_2 > 0,
\]
contrary to (20).

It follows from (29) that \(\varepsilon(p_1, p_2, p_3) = (1, -1, -1)\) or \(\varepsilon(p_1, p_2, p_3) = (-1, 1, 1)\), and 
\(\Omega\) may be partitioned into two subsets \(\Omega_{(-1,1,1)}\) and \(\Omega_{(1,-1,-1)}\) containing 
those elements of \(N\) having each of these two remaining signatures. We claim 
that the elements of \(\Omega_{(1,-1,-1)}\) can be produced by Algorithm 7.1 and those of 
\(\Omega_{(-1,1,1)}\) by Algorithm 7.2.

**Case 1.** If \(N \in \Omega_{(1,-1,-1)}\), then \(N\) may be found by Algorithm 7.1.

Let \(N \in \Omega_{(1,-1,-1)}\). By (20),
\[
(p_1 - 1)(p_2 + 1)(p_3 + 1) - p_1p_2p_3 + 1
\]
\[
= p_1p_2 + p_1p_3 - p_2p_3 + p_1 - p_2 - p_3
\]
\[
= p_3(p_1 - p_2 - 1) + p_1p_2 + p_1 - p_2 = 0.
\]

Set \(k = p_2 - p_1 + 1\). Then
\[
(27) \quad p_1 + k = p_2 + 1
\]
and
\[
(28) \quad p_3 = \frac{-p_1p_2 - p_1 + p_2}{p_1 - p_2 + 1} = \frac{p_1(p_2 + 1) - p_2}{k}.
\]

It follows from (27) that
\[
p_1 \equiv p_2 + 1 \pmod{k}\quad \text{and} \quad p_1(p_2 + 1) - p_2 \equiv p_1^2 - p_1 + 1 \equiv 0 \pmod{k}.
\]

Therefore \(-3\) is a quadratic residue modulo \(k\), and

**Case 2.** If \(N \in \Omega_{(-1,1,1)}\), then \(N\) may be found by Algorithm 7.2.

Let \(N \in \Omega_{(-1,1,1)}\). By (20),
\[
(p_1 + 1)(p_2 - 1)(p_3 - 1) - p_1p_2p_3 + 1
\]
\[
= -p_1p_2 - p_1p_3 + p_2p_3 + p_1 - p_2 - p_3
\]
\[
= p_3(p_2 - p_1 - 1) - p_1p_2 + p_1 - p_2 = 0.
\]

Set \(k = p_2 - p_1 - 1\). Then
\[
(29) \quad p_2 = p_1 + 1 + k\quad \text{and} \quad p_3 = \frac{p_1p_2 - p_1 + p_2}{p_2 - p_1 - 1} = \frac{p_1(p_2 - 1) + p_2}{k}.
\]

It follows from (29) that
$p_2 \equiv p_1 + 1 \pmod{k}$ and $p_1(p_2 - 1) + p_2 \equiv p_1^2 + p_1 + 1 \equiv 0 \pmod{k}$.

Therefore $-3$ is a quadratic residue modulo $k$, and

\begin{equation}
(p_1) \equiv (-1 + \alpha)/2 \pmod{k}
\end{equation}

for some $\alpha$ satisfying $\alpha^2 \equiv -3 \pmod{k}$. Clearly, $k$ will eventually be chosen in Step 1 of Algorithm 7.2, $p_1$ computed in Step 2, and primes $p_2$ and $p_3$ determined by $k$ and $p_1$. Therefore the primitive Lucas $d$-pseudoprime $N$ will eventually be constructed by Algorithm 7.2.

The following corollary follows immediately from the previous results.

**Corollary 7.6.** If $d = 4m$, $m$ odd, then all but a finite number of primitive Lucas $d$-pseudoprimes are Carmichael–Lucas numbers.

**Table 1.** Number $n$ of primitive Lucas $d$-pseudoprimes found with Algorithm 7.1 using $1 \leq k \leq 5000$ and $p_1, p_2 \leq 10^7$ and $p_3 \leq 10^{10}$

<table>
<thead>
<tr>
<th>$d$</th>
<th>$n$</th>
<th>$d$</th>
<th>$n$</th>
<th>$d$</th>
<th>$n$</th>
<th>$d$</th>
<th>$n$</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>10177</td>
<td>6400</td>
<td>14</td>
<td>25600</td>
<td>2</td>
<td>68644</td>
<td>1</td>
</tr>
<tr>
<td>16</td>
<td>2719</td>
<td>6724</td>
<td>4</td>
<td>26896</td>
<td>1</td>
<td>71824</td>
<td>1</td>
</tr>
<tr>
<td>64</td>
<td>690</td>
<td>7396</td>
<td>3</td>
<td>27556</td>
<td>1</td>
<td>73984</td>
<td>1</td>
</tr>
<tr>
<td>100</td>
<td>957</td>
<td>7744</td>
<td>7</td>
<td>28900</td>
<td>1</td>
<td>78400</td>
<td>5</td>
</tr>
<tr>
<td>196</td>
<td>278</td>
<td>8464</td>
<td>15</td>
<td>30976</td>
<td>2</td>
<td>80656</td>
<td>1</td>
</tr>
<tr>
<td>256</td>
<td>151</td>
<td>8836</td>
<td>5</td>
<td>31684</td>
<td>1</td>
<td>81796</td>
<td>1</td>
</tr>
<tr>
<td>400</td>
<td>258</td>
<td>9604</td>
<td>4</td>
<td>33124</td>
<td>2</td>
<td>84100</td>
<td>1</td>
</tr>
<tr>
<td>484</td>
<td>154</td>
<td>10000</td>
<td>11</td>
<td>33856</td>
<td>1</td>
<td>85264</td>
<td>2</td>
</tr>
<tr>
<td>676</td>
<td>63</td>
<td>11236</td>
<td>4</td>
<td>35344</td>
<td>1</td>
<td>87616</td>
<td>1</td>
</tr>
<tr>
<td>784</td>
<td>47</td>
<td>12100</td>
<td>13</td>
<td>36100</td>
<td>3</td>
<td>91204</td>
<td>2</td>
</tr>
<tr>
<td>1024</td>
<td>44</td>
<td>12544</td>
<td>5</td>
<td>37636</td>
<td>1</td>
<td>94864</td>
<td>1</td>
</tr>
<tr>
<td>1156</td>
<td>35</td>
<td>13456</td>
<td>2</td>
<td>38416</td>
<td>3</td>
<td>96100</td>
<td>4</td>
</tr>
<tr>
<td>1444</td>
<td>25</td>
<td>13924</td>
<td>2</td>
<td>40000</td>
<td>5</td>
<td>102400</td>
<td>1</td>
</tr>
<tr>
<td>1600</td>
<td>72</td>
<td>14884</td>
<td>2</td>
<td>40804</td>
<td>3</td>
<td>103684</td>
<td>2</td>
</tr>
<tr>
<td>1936</td>
<td>30</td>
<td>15376</td>
<td>1</td>
<td>43264</td>
<td>2</td>
<td>115600</td>
<td>1</td>
</tr>
<tr>
<td>2116</td>
<td>29</td>
<td>16384</td>
<td>1</td>
<td>45796</td>
<td>1</td>
<td>118336</td>
<td>1</td>
</tr>
<tr>
<td>2500</td>
<td>41</td>
<td>16900</td>
<td>12</td>
<td>47524</td>
<td>2</td>
<td>119716</td>
<td>1</td>
</tr>
<tr>
<td>2704</td>
<td>11</td>
<td>17956</td>
<td>3</td>
<td>48400</td>
<td>2</td>
<td>122500</td>
<td>1</td>
</tr>
<tr>
<td>3136</td>
<td>9</td>
<td>18496</td>
<td>2</td>
<td>50176</td>
<td>1</td>
<td>135424</td>
<td>1</td>
</tr>
<tr>
<td>3364</td>
<td>21</td>
<td>19600</td>
<td>6</td>
<td>52900</td>
<td>1</td>
<td>144400</td>
<td>1</td>
</tr>
<tr>
<td>3844</td>
<td>5</td>
<td>20164</td>
<td>2</td>
<td>53824</td>
<td>1</td>
<td>158404</td>
<td>1</td>
</tr>
<tr>
<td>4096</td>
<td>13</td>
<td>21316</td>
<td>1</td>
<td>55696</td>
<td>1</td>
<td>183184</td>
<td>1</td>
</tr>
<tr>
<td>4624</td>
<td>9</td>
<td>21904</td>
<td>3</td>
<td>58564</td>
<td>1</td>
<td>204304</td>
<td>1</td>
</tr>
<tr>
<td>4900</td>
<td>26</td>
<td>23104</td>
<td>3</td>
<td>62500</td>
<td>2</td>
<td>220900</td>
<td>1</td>
</tr>
<tr>
<td>5476</td>
<td>9</td>
<td>23716</td>
<td>2</td>
<td>64516</td>
<td>2</td>
<td>240100</td>
<td>1</td>
</tr>
<tr>
<td>5776</td>
<td>7</td>
<td>24964</td>
<td>2</td>
<td>67600</td>
<td>2</td>
<td>246016</td>
<td>1</td>
</tr>
</tbody>
</table>
Table 2. Number $n$ of primitive Lucas $d$-pseudoprimes found with Algorithm 7.2 using $1 \leq k \leq 5000$ and $p_1, p_2 \leq 10^7$ and $p_3 \leq 10^{10}$

<table>
<thead>
<tr>
<th>$d$</th>
<th>$n$</th>
<th>$d$</th>
<th>$n$</th>
<th>$d$</th>
<th>$n$</th>
<th>$d$</th>
<th>$n$</th>
</tr>
</thead>
<tbody>
<tr>
<td>16</td>
<td>1</td>
<td>63504</td>
<td>1</td>
<td>419904</td>
<td>1</td>
<td>3422250</td>
<td>1</td>
</tr>
<tr>
<td>36</td>
<td>3116</td>
<td>66564</td>
<td>2</td>
<td>435600</td>
<td>1</td>
<td>34574400</td>
<td>1</td>
</tr>
<tr>
<td>144</td>
<td>744</td>
<td>69696</td>
<td>1</td>
<td>443556</td>
<td>1</td>
<td>40449600</td>
<td>1</td>
</tr>
<tr>
<td>324</td>
<td>357</td>
<td>72900</td>
<td>4</td>
<td>459684</td>
<td>1</td>
<td>45968400</td>
<td>1</td>
</tr>
<tr>
<td>576</td>
<td>165</td>
<td>76176</td>
<td>1</td>
<td>476100</td>
<td>2</td>
<td>81000000</td>
<td>1</td>
</tr>
<tr>
<td>900</td>
<td>319</td>
<td>79524</td>
<td>1</td>
<td>518400</td>
<td>1</td>
<td>85377600</td>
<td>1</td>
</tr>
<tr>
<td>1296</td>
<td>91</td>
<td>82944</td>
<td>1</td>
<td>571536</td>
<td>1</td>
<td>92736900</td>
<td>1</td>
</tr>
<tr>
<td>1764</td>
<td>77</td>
<td>86436</td>
<td>2</td>
<td>589824</td>
<td>1</td>
<td>110880900</td>
<td>1</td>
</tr>
<tr>
<td>2304</td>
<td>47</td>
<td>90000</td>
<td>4</td>
<td>617796</td>
<td>1</td>
<td>118592100</td>
<td>1</td>
</tr>
<tr>
<td>2916</td>
<td>27</td>
<td>97344</td>
<td>1</td>
<td>705600</td>
<td>1</td>
<td>143280900</td>
<td>1</td>
</tr>
<tr>
<td>3600</td>
<td>65</td>
<td>108900</td>
<td>4</td>
<td>736164</td>
<td>1</td>
<td>187142400</td>
<td>1</td>
</tr>
<tr>
<td>4356</td>
<td>30</td>
<td>116964</td>
<td>2</td>
<td>756900</td>
<td>1</td>
<td>191268900</td>
<td>1</td>
</tr>
<tr>
<td>5184</td>
<td>22</td>
<td>121104</td>
<td>1</td>
<td>876096</td>
<td>1</td>
<td>196280100</td>
<td>1</td>
</tr>
<tr>
<td>6084</td>
<td>16</td>
<td>138384</td>
<td>1</td>
<td>1052676</td>
<td>2</td>
<td>211702500</td>
<td>1</td>
</tr>
<tr>
<td>7056</td>
<td>18</td>
<td>142884</td>
<td>2</td>
<td>1115136</td>
<td>1</td>
<td>263412900</td>
<td>1</td>
</tr>
<tr>
<td>8100</td>
<td>42</td>
<td>147456</td>
<td>1</td>
<td>1166400</td>
<td>1</td>
<td>277222500</td>
<td>1</td>
</tr>
<tr>
<td>9216</td>
<td>11</td>
<td>152100</td>
<td>1</td>
<td>1382976</td>
<td>1</td>
<td>326163600</td>
<td>1</td>
</tr>
<tr>
<td>10404</td>
<td>8</td>
<td>156816</td>
<td>1</td>
<td>1397124</td>
<td>1</td>
<td>328334400</td>
<td>1</td>
</tr>
<tr>
<td>11664</td>
<td>10</td>
<td>161604</td>
<td>3</td>
<td>1512900</td>
<td>1</td>
<td>343731600</td>
<td>1</td>
</tr>
<tr>
<td>12996</td>
<td>4</td>
<td>171396</td>
<td>1</td>
<td>1572516</td>
<td>1</td>
<td>366339600</td>
<td>1</td>
</tr>
<tr>
<td>14400</td>
<td>17</td>
<td>176400</td>
<td>3</td>
<td>1602756</td>
<td>1</td>
<td>375584400</td>
<td>1</td>
</tr>
<tr>
<td>15876</td>
<td>8</td>
<td>181476</td>
<td>1</td>
<td>1664100</td>
<td>1</td>
<td>466560000</td>
<td>1</td>
</tr>
<tr>
<td>17424</td>
<td>8</td>
<td>186624</td>
<td>1</td>
<td>1742400</td>
<td>1</td>
<td>476985600</td>
<td>1</td>
</tr>
<tr>
<td>19044</td>
<td>6</td>
<td>191844</td>
<td>1</td>
<td>1988100</td>
<td>1</td>
<td>546156900</td>
<td>1</td>
</tr>
<tr>
<td>20736</td>
<td>2</td>
<td>197136</td>
<td>1</td>
<td>2090916</td>
<td>1</td>
<td>560268900</td>
<td>1</td>
</tr>
<tr>
<td>22500</td>
<td>11</td>
<td>202500</td>
<td>2</td>
<td>2340900</td>
<td>1</td>
<td>714492900</td>
<td>1</td>
</tr>
<tr>
<td>24336</td>
<td>9</td>
<td>207936</td>
<td>1</td>
<td>4161600</td>
<td>1</td>
<td>722534400</td>
<td>1</td>
</tr>
<tr>
<td>26244</td>
<td>5</td>
<td>213444</td>
<td>2</td>
<td>5089536</td>
<td>1</td>
<td>766736100</td>
<td>1</td>
</tr>
<tr>
<td>32400</td>
<td>10</td>
<td>224676</td>
<td>1</td>
<td>5336100</td>
<td>2</td>
<td>864360000</td>
<td>1</td>
</tr>
<tr>
<td>34596</td>
<td>3</td>
<td>230400</td>
<td>1</td>
<td>5531904</td>
<td>1</td>
<td>916272900</td>
<td>1</td>
</tr>
<tr>
<td>36864</td>
<td>2</td>
<td>236196</td>
<td>1</td>
<td>6502500</td>
<td>1</td>
<td>1087020900</td>
<td>1</td>
</tr>
<tr>
<td>39204</td>
<td>5</td>
<td>242064</td>
<td>1</td>
<td>6594624</td>
<td>1</td>
<td>109892250</td>
<td>1</td>
</tr>
<tr>
<td>41616</td>
<td>1</td>
<td>248004</td>
<td>1</td>
<td>7452900</td>
<td>1</td>
<td>1190250000</td>
<td>1</td>
</tr>
<tr>
<td>44100</td>
<td>5</td>
<td>260100</td>
<td>2</td>
<td>7952400</td>
<td>1</td>
<td>1244678400</td>
<td>1</td>
</tr>
<tr>
<td>46656</td>
<td>8</td>
<td>272484</td>
<td>1</td>
<td>11289600</td>
<td>1</td>
<td>1370480400</td>
<td>1</td>
</tr>
<tr>
<td>49284</td>
<td>2</td>
<td>324900</td>
<td>2</td>
<td>11492100</td>
<td>1</td>
<td>1413008100</td>
<td>1</td>
</tr>
<tr>
<td>51984</td>
<td>5</td>
<td>331776</td>
<td>1</td>
<td>18147600</td>
<td>1</td>
<td>1490732100</td>
<td>1</td>
</tr>
<tr>
<td>54756</td>
<td>3</td>
<td>345744</td>
<td>2</td>
<td>19713600</td>
<td>1</td>
<td>1743897600</td>
<td>1</td>
</tr>
<tr>
<td>57600</td>
<td>6</td>
<td>360000</td>
<td>2</td>
<td>21622500</td>
<td>1</td>
<td>1853302500</td>
<td>1</td>
</tr>
<tr>
<td>60516</td>
<td>2</td>
<td>367236</td>
<td>1</td>
<td>24206400</td>
<td>1</td>
<td>1998090000</td>
<td>1</td>
</tr>
</tbody>
</table>
We implemented Algorithms 7.1 and 7.2 in Java, C++, and GAP, and were able to construct many primitive Lucas \( d \)-pseudoprimes for many values of \( d \) when \( d \) is an even perfect square. Thus, beginning with \( k = 1549 \), Algorithm 7.1 produced the primitive \( d \)-pseudoprime \( 5155460949210001 = 52391 \cdot 53939 \cdot 1824349 \), with \( d = 96100 = (2 \cdot 5 \cdot 31)^2 \). Beginning with \( k = 3823 \), Algorithm 7.2 produced the primitive \( d \)-pseudoprime \( 249540023224799 = 29399 \cdot 33223 \cdot 255487 \), with \( d = 86436 = (2 \cdot 3 \cdot 49)^2 \). We applied Algorithms 7.1 and 7.2 for all values of \( k \) such that \( 1 \leq k \leq 5000 \), with the restriction that \( p_1, p_2 < 10^7 \) and \( p_3 < 10^{10} \), and found a total of 16118 \( d \)-pseudoprimes with Algorithm 7.1 and 5471 \( d \)-pseudoprimes with Algorithm 7.2.

As mentioned above, Schinzel and Sierpiński’s Hypothesis H (see [13]) implies that Algorithms 7.1 and 7.2 each generate an infinite number of primitive \( d \)-pseudoprimes (with \( d \) ranging over a possibly infinite set of values) for each choice of \( k \). Even for a fixed even perfect square \( d \), however, primitive \( d \)-pseudoprimes appear to be plentiful. Thus, for example, our experiment produced 10177 primitive 4-pseudoprimes, 2720 primitive 16-pseudoprimes, and 957 primitive 100-pseudoprimes in relatively short order. This stands in stark contrast with the conclusion of Theorem 6.8 that there are only a finite number of them when \( d \) is divisible by four but not a perfect square.

Tables 1 and 2 summarize how many \( d \)-pseudoprimes we constructed for various values of \( d \).

8. Further developments. In this paper we have examined the distribution of primitive Lucas \( d \)-pseudoprimes, concentrating our attention on the case that \( 4 \parallel d \). In this case all but a finite number of the \( d \)-pseudoprimes have exactly three distinct prime divisors. A careful analysis of this situation shows that a necessary condition for the existence of an infinite number of primitive \( d \)-pseudoprimes is that \( d \) be a perfect square. Our algorithms suggest that there may be an infinite number of primitive \( d \)-pseudoprimes with exactly three prime divisors, but a proof of this conjecture remains open. An analysis of our algorithms may prove useful in providing asymptotic estimates of the size of primitive \( d \)-pseudoprimes with three factors.

A broad range of questions generalizing our study remain open. In [3], we showed that if \( 2^t \parallel d \), then only finitely many Lucas \( d \)-pseudoprimes have more than \( r + 1 \) prime factors, but if the number \( t \) of prime divisors satisfies \( 3 < t \leq r + 1 \), there may be infinitely many primitive \( d \)-pseudoprimes. Our main tool, Theorem 6.4, applies in this case and allows us to restrict our attention to numbers satisfying (13) and, in a related paper, [4], we show that almost all Lucas \( d \)-pseudoprimes are square free.

Does the existence of infinitely many \( d \)-pseudoprimes with \( t \) divisors place any constraints on the structure of \( d \)? Are there generalizations of our algorithms to produce \( d \)-pseudoprimes with more than three prime factors?
In the case that there are infinitely many primitive $d$-pseudoprimes, can anything be said about their asymptotic growth? In the case that there are only finitely many primitive $d$-pseudoprimes, can an absolute bound be determined?

We are actively investigating these questions. Our paper [4] includes a preliminary investigation of numbers that satisfy (13), and we are currently working on a paper that provides an absolute bound for the number of Lucas $d$-pseudoprimes in some cases.

REFERENCES

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

Department of Mathematics
Franklin and Marshall College
Lancaster, PA 17604, U.S.A.
E-mail: c3ar@math.uchicago.edu

Department of Mathematics
Catholic University of America
Washington, DC 20064, U.S.A.
E-mail: somer@cua.edu

Received 17 April 2005;
revised 15 May 2006