LUCAS $(a_1, a_2, \ldots, a_k = \pm 1)$ PSEUDOPRIMES

LAWRENCE SOMER AND CURTIS COOPER

Abstract. Cooper and Somer define a Lucas $(a_1, a_2, \ldots, a_k = \pm 1)$ sequence $\{G_n\}$ for all integers n as

$$G_n = x_1^n + x_2^n + \cdots + x_k^n,$$

where $x_1, x_2, \ldots, x_k$ are roots of the equation

$$x^k = a_1 x^{k-1} + a_2 x^{k-2} + \cdots + a_k$$

with integer coefficients. Then they define Lucas $(a_1, a_2, \ldots, a_k = \pm 1)$ pseudoprimes to be composite n such that

$$G_n \equiv G_1 \pmod{n} \quad \text{and} \quad G_{-n} \equiv G_{-1} \pmod{n}.$$

Adams and Shanks and Szekeres had previously used negative indices in describing higher-order pseudoprimes. In this paper, we will relate pseudoprimes occurring in different Lucas $(a_1, a_2, \ldots, a_k = \pm 1)$ sequences. And we will provide substantial numerical tables giving Lucas $(a_1, a_2, \ldots, a_k = \pm 1)$ pseudoprimes for many different Lucas $(a_1, a_2, \ldots, a_k = \pm 1)$ sequences.

1. Introduction

The concept of a pseudoprime with respect to a polynomial has been studied in the mathematical literature by Adams and Shanks [1], Gurak [6], Szekeres [9], Atkin [2], and Grantham [4]. We note that the Frobenius pseudoprimes of Grantham [4] generalize the higher-order pseudoprimes of both Gurak and Szekeres. The higher-order pseudoprime test of Atkin [2] shows some similarities to the Frobenius pseudoprime test of Grantham.

Cooper and Somer [3] define a Lucas $(a_1, a_2, \ldots, a_k = \pm 1)$ sequence as follows.

Definition 1.1. *A Lucas $(a_1, a_2, \ldots, a_k = \pm 1)$ sequence $\{G_n\}$ is defined for all integers n as*

$$G_n = x_1^n + x_2^n + \cdots + x_k^n,$$

where $x_1, x_2, \ldots, x_k$ are roots of the equation

$$x^k = a_1 x^{k-1} + a_2 x^{k-2} + \cdots + a_k$$

with integer coefficients. Associated with the Lucas $(a_1, a_2, \ldots, a_k = \pm 1)$ sequence $\{G_n\}$ is the characteristic polynomial

$$f(x) = x^k - a_1 x^{k-1} - a_2 x^{k-2} - \cdots - a_{k-1} x - a_k$$

with characteristic roots $x_1, x_2, \ldots, x_k$.

They then proved that for prime p,

$$G_p \equiv G_1 \pmod{p} \quad \text{and} \quad G_{-p} \equiv G_{-1} \pmod{p}.$$

Motivated by this result, they define a Lucas $(a_1, a_2, \ldots, a_k = \pm 1)$ pseudoprime as follows.

Definition 1.2. *Let $\{G_n\}$ be a Lucas $(a_1, a_2, \ldots, a_k = \pm 1)$ sequence. A composite n such that*

$$G_n \equiv G_1 \pmod{n} \quad \textit{and} \quad G_{-n} \equiv G_{-1} \pmod{n}$$

is called a Lucas $(a_1, a_2, \ldots, a_k = \pm 1)$ pseudoprime.

Adams and Shanks [1] in referring to third-order pseudoprimes and Szekeres [9] in referring to general higher-order pseudoprimes, both used positive and negative indices in defining higher-order pseudoprimes. In addition, Adams and Shanks and Szekeres even used additional constraints in addition to using both positive and negative indices. Adams and Shanks used the third-order sequence $A(n)$ and they used the signature for the 6 terms $A(-n-1), A(-n), A(-n+1), A(n-1), A(n)$, and $A(n+1)$ to test the pseudoprime n. There are three types of signatures, the S signature, the Q signature, and the I signature. For all three signatures, Adams and Shanks have $A(n) \equiv A(1) \pmod{n}$ and $A(-n) \equiv A(-1) \pmod{n}$.

In this paper we will relate pseudoprimes occurring in different Lucas $(a_1, a_2, \ldots, a_k = \pm 1)$ sequences. And we will provide substantial numerical tables giving Lucas $(a_1, a_2, \ldots, a_k = \pm 1)$ pseudoprimes for many different Lucas $(a_1, a_2, \ldots, a_k = \pm 1)$ sequences.

2. Second Order Lucas Pseudoprimes

We begin with a lemma concerning second-order Lucas sequences.

Lemma 2.1. *Consider the Lucas $(a_1, a_2 = \pm 1)$ sequence. If $a_2 = -1$, then each positive composite integer M satisfying*

$$G_M \equiv G_1 \pmod{M} \tag{2.1}$$

also satisfies

$$G_{-M} \equiv G_{-1} \pmod{M}. \tag{2.2}$$

If $a_2 = 1$, then each positive odd composite integer M satisfying (2.1) also satisfies (2.2).

Proof. Let x_1 and x_2 be the characteristic roots of the Lucas (a_1, a_2) sequence. Then for $n \geq 0$,

$$\begin{aligned} G_{-n} &= x_1^{-n} + x_2^{-n} = (x_1^n + x_2^n)/(x_1 x_2)^n \\ &= (x_1^n + x_2^n)/(-a_2)^n = (-a_2)^n G_n. \end{aligned}$$

The result now follows. □

Traditional Lucas $(a_1, 1)$ pseudoprimes are essentially Lucas $(a_1, 1)$ pseudoprimes. However, a traditional Lucas $(a_1, 1)$ pseudoprime only requires that n is composite and $G_n \equiv G_1 \pmod{n}$. Therefore, every Lucas $(a_1, 1)$ pseudoprime is a traditional Lucas $(a_1, 1)$ pseudoprime. But these pseudoprimes are different. For example, 8 is a traditional Lucas $(2, 1)$ pseudoprime since $G_8 = 1154$, $G_1 = 2$, and $1154 \equiv 2 \pmod{8}$. However, 8 is not a Lucas $(2, 1)$ pseudoprime with the above definition since $G_{-8} = 1154$, $G_{-1} = -2$, and $1154 \not\equiv -2 \pmod{8}$. A similar argument can be made for any 2^k, where $k \geq 3$.

The next theorem will give some elementary results about second order Lucas pseudoprimes.

Theorem 2.2. *Every traditional Lucas $(a_1, -1)$ pseudoprime is a Lucas $(a_1, -1)$ pseudoprime. Every odd traditional Lucas $(a_1, 1)$ pseudoprime is a Lucas $(a_1, 1)$ pseudoprime. If $a_1 \equiv 2 \pmod 4$, then 4 is a Lucas $(a_1, \pm 1)$ pseudoprime. There are only a finite number of even Lucas $(a_1, 1)$ pseudoprimes.*

Proof. Let $\{G_n\}$ be a Lucas $(a_1, \pm 1)$ sequence. It now follows from Lemma 2.1 that every traditional Lucas $(a_1, -1)$ pseudoprime is a Lucas $(a_1, -1)$ pseudoprime and every odd traditional Lucas $(a_1, 1)$ pseudoprime is a Lucas $(a_1, 1)$ pseudoprime.

Next let $a_1 \equiv 2 \pmod 4$ and let $a_2 = \pm 1$. Since $G_1 = a_1$, $G_{-1} = -a_2 a_1$, and $G_4 = G_{-4} = a_1^4 + 4a_2 a_1^2 + 2$, it follows that 4 is a Lucas $(a_1, \pm 1)$ pseudoprime.

Finally, let n be a Lucas $(a_1, 1)$ pseudoprime. First suppose that $a_1 = 0$. Then $G_i = 0$ if i is odd and $G_i = 2$ if i is even. It follows that there is no even traditional Lucas $(a_1, 1)$ pseudoprime, let alone an even Lucas $(a_1, 1)$ pseudoprime. Now assume that $a_1 \neq 0$. Since n is an even Lucas $(a_1, 1)$ pseudoprime, n is composite, $G_n \equiv G_1 \equiv a_1 \pmod n$, and $G_{-n} \equiv G_{-1} \equiv -a_1 \pmod n$. And since n is even, we see from the proof of Lemma 2.1 that $G_n = G_{-n}$. Therefore, $2a_1 \equiv 0 \pmod n$ or $n | 2a_1$. Hence, there are only a finite number of even Lucas $(a_1, 1)$ pseudoprimes. □

3. Higher Order Lucas Pseudoprimes

The next theorem will give necessary and sufficient conditions for finding certain higher order Lucas pseudoprimes.

Theorem 3.1. *Consider the Lucas $(0, \ldots, 0, a_k, 0, \ldots, 0, a_{2k} = \pm 1)$ sequence, where $k \geq 2$ and $a_k \neq 0$. The Lucas $(0, \ldots, 0, a_k, 0, \ldots, 0, a_{2k} = \pm 1)$ pseudoprimes are precisely the composite natural numbers relatively prime to k and the composite natural numbers km for which $m \mid G_m(a_k, a_{2k})$.*

Proof. It follows from the Newton formulas, the recursion relation defining the Lucas $(0, \ldots, 0, a_k, 0, \ldots, 0, a_{2k} = \pm 1)$ sequence, and by induction that

$$G_n = G_{-n} = 0 \qquad \text{if } n \geq 0 \text{ and } n \not\equiv 0 \pmod k, \tag{3.1}$$

$$G_0 = 2k, \tag{3.2}$$

$$G_k = ka_k, \tag{3.3}$$

$$G_{(i+2)k} = a_k G_{(i+1)k} + a_{2k} G_{ik} \qquad \text{for } i \geq 0, \tag{3.4}$$

and

$$G_{-ik} = (-a_{2k})^i G_{ik} \qquad \text{for } i \geq 0. \tag{3.5}$$

In particular, we see by (3.1) that $G_1 = G_{-1} = 0$.

Consider the second-order Lucas sequence $\{G_n(a_k, a_{2k})\}$. Then $G_0(a_k, a_{2k}) = 2$ and $G_1(a_k, a_{2k}) = a_k$. Note that

$$G_0(0, \ldots, 0, a_k, 0, \ldots, 0, a_{2k}) = kG_0(a_k, a_{2k}) \text{ and}$$
$$G_k(0, 0, \ldots, 0, a_k, 0, 0, \ldots, 0, a_{2k}) = kG_1(a_k, a_{2k}).$$

It now follows from (3.4) and the second-order recursion relation defining $\{G_n(a_k, a_{2k})\}$ that

$$G_{ik}(0, \ldots, 0, a_k, 0, \ldots, 0, a_{2k}) = k \cdot G_i(a_k, a_{2k})$$

for $i \geq 0$. The assertions concerning the Lucas $(0, \ldots, 0, a_k, 0, \ldots, 0, a_{2k} = \pm 1)$ pseudoprimes now follow from (3.1)-(3.5). □

The paper by Somer [8] gives comprehensive criteria for determining when $n|G_n(a_1, 1)$, which relates to Theorem 3.1.

We now present an observation that gives further insight on the Lucas $(0, \ldots, 0, a_k, 0, \ldots, 0, a_{2k} = \pm 1)$ sequence, where $k \geq 2$, and provides intuition on why Theorem 3.1 is true. Let

$$f(x) = x^{2k} - a_k x^k - a_{2k}$$

be the characteristic polynomial of the Lucas $(0, \ldots, 0, a_k, 0, \ldots, 0, a_{2k} = \pm 1)$ sequence. Let $x_1, \ldots, x_{2k}$ be the characteristic roots of $f(x)$. Let y_1 and y_2 be the characteristic roots of the Lucas (a_k, a_{2k}) sequence with characteristic polynomial

$$g(x) = x^2 - a_k x - a_{2k}.$$

Then $x_1^k, \ldots, x_{2k}^k$ satisfy the characteristic polynomial $g(x) = x^2 - a_k x - a_{2k}$. In particular, one can order the characteristic roots $x_1, \ldots, x_{2k}$ so that each of $x_1^k, \ldots, x_k^k$ is equal to y_1, and each of $x_{k+1}^k, \ldots, x_{2k}^k$ is equal to y_2.

Example 3.1. *Consider the* $2k$*th-order Lucas sequence* $(0, 0, 2, 0, 0, 1)$ *where* $k = 3$. *We show that* $198 \mid G_{198}(2, 1)$. *It will then follow from Theorem 3.1 that* $3 \cdot 198 = 594$ *is a Lucas* $(0, 0, 2, 0, 0, 1)$ *pseudoprime. It is well-known that if* $m|n$ *and* n/m *is odd, then*

$$G_m(a_1, 1) \mid G_n(a_1, 1).$$

Note that $198 = 6 \cdot 33$. *Thus,*

$$G_6(2, 1) = 198 \mid G_{198}(2, 1),$$

as desired. We also see by Theorem 3.1 that the composite numbers 4, 8, 10, 14, 16, 20, 22, 25, 26, 28, 32, 34, 35, 38, 40, 44, 46, 49, and 50 are also Lucas $(0, 0, 2, 0, 0, 1)$ *pseudoprimes, since they are all relatively prime to* $k = 3$.

The next theorem is an important one to help us relate Lucas pseudoprimes of different sequences.

Theorem 3.2. *Consider the Lucas* $(a_1, a_2, \ldots, a_k = \pm 1)$ *sequence with characteristic polynomial* $f(x)$ *and the Lucas* $(b_1, b_2, \ldots, b_r = \pm 1)$ *sequence with characteristic polynomial* $g(x)$. *Suppose that* $g(x) \mid f(x)$. *Suppose further that*

$$f(x) = g(x) g_1(x) g_2(x) \cdots g_j(x),$$

where $g_1(x), g_2(x), \ldots, g_j(x)$ *are cyclotomic polynomials, not necessarily distinct, of orders* $m_1, m_2, \ldots, m_j$, *respectively. Let* $m = lcm(m_1, m_2, \ldots, m_j)$. *Then the set of Lucas* $(b_1, b_2, \ldots, b_r)$ *pseudoprimes relatively prime to* m *is equal to the set of Lucas* $(a_1, a_2, \ldots, a_k)$ *pseudoprimes relatively prime to* m.

Proof. Let M be a Lucas $(b_1, b_2, \ldots, b_r)$ pseudoprime relatively prime to m. We show that M is also a Lucas $(a_1, a_2, \ldots, a_k)$ pseudoprimes relatively prime to m. Let $x_1, x_2, \ldots, x_r$ be the characteristic roots of $g(x)$. Then by the definition of a Lucas $(b_1, b_2, \ldots, b_r)$ pseudoprime,

$$\begin{aligned} G_M(b_1, b_2, \ldots, b_r) = x_1^M + x_2^M + \cdots + x_r^M &\equiv G_1(b_1, b_2, \ldots, b_r) \\ &= x_1 + x_2 + \cdots + x_r \pmod{M} \end{aligned} \tag{3.6}$$

and

$$\begin{aligned} G_{-M}(b_1, b_2, \ldots, b_r) = x_1^{-M} + x_2^{-M} + \cdots + x_r^{-M} &\equiv G_{-1}(b_1, b_2, \ldots, b_r) \\ &= x_1^{-1} + x_2^{-1} + \cdots + x_r^{-1} \pmod{M}. \end{aligned} \tag{3.7}$$

Let the characteristic roots of $g_i(x)$, $1 \le i \le j$, be $\zeta_{1,i}, \zeta_{2,i}, \ldots, \zeta_{\phi(m_i),i}$, where ϕ is Euler's totient function and $\zeta_{1,i}, \zeta_{2,i}, \ldots, \zeta_{\phi(m_i),i}$ consist of all the distinct primitive (m_i)th roots of unity. Since M is relatively prime to m_i, it follows that

$$\begin{aligned}\zeta_{1,i}^M + \zeta_{2,i}^M + \cdots + \zeta_{\phi(m_i),i}^M &= \zeta_{1,i}^{-M} + \zeta_{2,i}^{-M} + \cdots + \zeta_{\phi(m_i),i}^{-M} \\ &= \zeta_{1,i} + \zeta_{2,i} + \cdots + \zeta_{\phi(m_i),i} = \zeta_{1,i}^{-1} + \zeta_{2,i}^{-1} + \cdots + \zeta_{\phi(m_i),i}^{-1}.\end{aligned} \tag{3.8}$$

Let $x_1, x_2, \ldots, x_r, x_{r+1}, \ldots, x_k$ be the characteristic roots of $f(x)$. It follows from (3.6)-(3.8) that

$$\begin{aligned}&G_M(a_1, a_2, \ldots, a_k) = x_1^M + x_2^M + \cdots + x_r^M + x_{r+1}^M + \cdots + x_k^M \\ &\equiv x_1 + x_2 + \cdots + x_r + x_{r+1} + \cdots + x_k = G_1(a_1, a_2, \ldots, a_k) \pmod{M},\end{aligned} \tag{3.9}$$

and

$$\begin{aligned}&G_{-M}(a_1, a_2, \ldots, a_k) = x_1^{-M} + x_2^{-M} + \cdots + x_r^{-M} + x_{r+1}^{-M} + \cdots + x_k^{-M} \\ &\equiv x_1^{-1} + x_2^{-1} + \cdots + x_r^{-1} + x_{r+1}^{-1} + \cdots + x_k^{-1} = G_{-1}(a_1, a_2, \ldots, a_k) \pmod{M}.\end{aligned} \tag{3.10}$$

Hence, M is a Lucas $(a_1, \ldots, a_k = \pm 1)$ pseudoprime relatively prime to m.

Now let N be a Lucas $(a_1, a_2, \ldots, a_k = \pm 1)$ pseudoprime relatively prime to m. Note that

$$h(x) = f(x)/g(x) = g_1(x)g_2(x)\cdots g_j(x) = x^{k-r} - c_1x^{k-r-1} - \cdots - c_{k-r-1}x - c_{k-r}$$

is a monic polynomial with integer coefficients which has characteristic roots x_{r+1}, x_{r+2}, $\ldots$, x_k. It follows from (3.8) that

$$\begin{aligned}x_{r+1}^N + x_{r+2}^N + \cdots + x_k^N &= x_{r+1}^{-N} + x_{r+2}^{-N} + \cdots + x_k^{-N} \\ &= x_{r+1}^{-1} + x_{r+2}^{-1} + \cdots + x_k^{-1} = x_{r+1} + x_{r+2} + \cdots + x_k = c_1.\end{aligned} \tag{3.11}$$

We now see by (3.9), (3.10), and (3.11) that

$$\begin{aligned}&G_N(a_1, a_2, \ldots, a_k) = (x_1^N + x_2^N + \cdots + x_r^N) + (x_{r+1}^N + x_{r+2}^N + \cdots + x_k^N) \\ &= G_N(b_1, b_2, \ldots, b_r) + c_1 \equiv G_1(a_1, a_2, \ldots, a_k) = (x_1 + x_2 + \cdots + x_r) \\ &+ (x_{r+1} + x_{r+2} + \cdots + x_k) = G_1(b_1, b_2, \ldots, b_r) + c_1 \pmod{N},\end{aligned} \tag{3.12}$$

and

$$\begin{aligned}&G_{-N}(a_1, a_2, \ldots, a_k) = (x_1^{-N} + x_2^{-N} + \cdots + x_r^{-N}) + (x_{r+1}^{-N} + x_{r+2}^{-N} + \cdots + x_k^{-N}) \\ &= G_{-N}(b_1, b_2, \ldots, b_r) + c_1 \equiv G_{-1}(a_1, a_2, \ldots, a_k) = (x_1^{-1} + x_2^{-1} + \cdots + x_r^{-1}) \\ &+ (x_{r+1}^{-1} + x_{r+2}^{-1} + \cdots + x_k^{-1}) = G_{-1}(b_1, b_2, \ldots, b_r) + c_1 \pmod{N}.\end{aligned} \tag{3.13}$$

Congruences (3.12) and (3.13) together imply that $G_N(b_1, b_2, \ldots, b_r) + c_1 \equiv G_1(b_1, b_2, \ldots, b_r) + c_1 \pmod{N}$ and $G_{-N}(b_1, b_2, \ldots, b_r) + c_1 \equiv G_{-1}(b_1, b_2, \ldots, b_r) + c_1 \pmod{N}$. Hence, N is also a Lucas $(b_1, b_2, \ldots, b_r)$ pseudoprime relatively prime to m, and the result follows. □

Some corollaries and examples follow from this theorem.

Corollary 3.3. *Let the Lucas $(b_1, b_2, \ldots, b_k = \pm 1)$ sequence have characteristic polynomial $f(x)$ and the Lucas $(a_1, a_2, \ldots, a_{k+1} = \mp 1)$ sequence have characteristic polynomial $f(x)g(x)$, where $g(x) = x - 1$. Then the sets of Lucas $(b_1, b_2, \ldots, b_k = \pm 1)$ pseudoprimes and Lucas $(a_1, a_2, \ldots, a_{k+1} = \mp 1)$ pseudoprimes are equal.*

Proof. This is an immediate consequence of Theorem 3.2, since $x - 1$ is the cyclotomic polynomial of order 1. □

Corollary 3.4. *Let p be a prime. Consider the Lucas $(b_1, b_2, \ldots, b_r = \pm 1)$ sequence with characteristic polynomial $g(x)$. Let*

$$g_1(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$$

be the cyclotomic polynomial of order p. Let the Lucas $(a_1, a_2, \ldots, a_{r+p-1} = \pm 1)$ sequence have characteristic polynomial $f(x)$, where

$$f(x) = g(x)g_1(x).$$

Then the set of Lucas $(b_1, b_2, \ldots, b_r)$ pseudoprimes relatively prime to p is equal to the set of Lucas $(a_1, a_2, \ldots, a_{r+p-1} = \pm 1)$ pseudoprimes relatively prime to p. Moreover, no Lucas $(a_1, a_2, \ldots, a_{r+p-1} = \pm 1)$ pseudoprime divisible by p can be a Lucas $(b_1, b_2, \ldots, b_r = \pm 1)$ pseudoprime.

Proof. We first observe that $a_{r+p-1} = b_r = \pm 1$, since the constant term of $g_1(x)$ is equal to 1. The first assertion of the corollary regarding pseudoprimes relatively prime to p follows from Theorem 3.2.

Now suppose that M is divisible by p and that M is both a Lucas $(a_1, a_2, \ldots, a_{r+p-1} = \pm 1)$ pseudoprime and a Lucas $(b_1, b_2, \ldots, b_r = \pm 1)$ pseudoprime. Let $x_1, x_2, \ldots, x_r, x_{r+1}, \ldots, x_{r+p-1}$ be the characteristic roots of $f(x)$, where $x_1, x_2, \ldots, x_r$ are the characteristic roots of $g(x)$. Note that $x_{r+1}, x_{r+2}, \ldots, x_{r+p-1}$ are the characteristic roots of the cyclotomic polynomial $g_1(x)$. Noting that M is a Lucas $(a_1, a_2, \ldots, a_{r+p-1} = \pm 1)$ pseudoprime, we see by the proof of Theorem 3.2 that

$$\begin{aligned} G_M(a_1, a_2, \ldots, a_{r+p-1}) &= (x_1^M + x_2^M + \cdots + x_r^M) + (x_{r+1}^M + x_{r+2}^M + \cdots + x_{r+p-1}^M) \\ &= G_M(b_1, b_2, \ldots, b_r) + (1 + 1 + \cdots + 1) \\ &= G_M(b_1, b_2, \ldots, b_r) + p - 1 \\ &\equiv G_1(a_1, a_2, \ldots, a_{r+p-1}) \\ &= (x_1 + x_2 + \cdots + x_r) + (x_{r+1} + x_{r+2} + \cdots + x_{r+p-1}) \\ &= G_1(b_1, b_2, \ldots, b_r) + (-1) \pmod{M}. \end{aligned} \tag{3.14}$$

Since M is also a Lucas $(b_1, b_2, \ldots, b_r = \pm 1)$ pseudoprime, it follows by definition that

$$G_M(b_1, b_2, \ldots, b_r) \equiv G_1(b_1, b_2, \ldots, b_r) \pmod{M}. \tag{3.15}$$

We now derive from (3.14) and (3.15) that

$$p - 1 \equiv -1 \pmod{M},$$

or

$$p \equiv 0 \pmod{M}.$$

This is impossible, since $p \mid M$ and M is composite. The result now follows. □

Example 3.2. *Consider the Lucas $(0, 1, 1, 1, 2, 1)$ sequence with characteristic polynomial $f(x) = x^6 - x^4 - x^3 - x^2 - 2x - 1$ and the Lucas $(1, 1)$ sequence with characteristic polynomial $g(x) = x^2 - x - 1$. Then $f(x) = g(x)g_1(x)$, where*

$$g_1(x) = x^4 + x^3 + x^2 + x + 1$$

is the cyclotomic polynomial of order 5. By computation, one sees that 705, 2465, 3745, 24465, 35785, and 54705 are Lucas $(1, 1)$ pseudoprimes but not Lucas $(0, 1, 1, 1, 2, 1)$ pseudoprimes in agreement with Corollary 3.4.

Corollary 3.5. *Let p be a prime. Consider the Lucas $(b_1, b_2, \ldots, b_r = \pm 1)$ sequence with characteristic polynomial $g(x)$. Let*

$$g_1(x) = x^{p(p-1)} + x^{p(p-2)} + \cdots + x^p + 1$$

be the cyclotomic polynomial of order p^2. Let the Lucas $(a_1, a_2, \ldots, a_{r+p(p-1)} = \pm 1)$ sequence have characteristic polynomial $f(x)$, where

$$f(x) = g(x)g_1(x).$$

Then the set of Lucas $(b_1, b_2, \ldots, b_r)$ pseudoprimes relatively prime to p^2 is equal to the set of Lucas $(a_1, a_2, \ldots, a_{r+p(p-1)} = \pm 1)$ pseudoprimes relatively prime to p^2. Moreover, no Lucas $(a_1, a_2, \ldots, a_{r+p(p-1)} = \pm 1)$ pseudoprime divisible by p can be a Lucas $(b_1, b_2, \ldots, b_r = \pm 1)$ pseudoprime.

Proof. By Theorem 3.2, it suffices to prove that no Lucas $(a_1, a_2, \ldots, a_{r+p(p-1)} = \pm 1)$ pseudoprime divisible by p is also a Lucas $(b_1, b_2, \ldots, b_r = \pm 1)$ pseudoprime. First suppose that M is divisible by p^2 and that M is both a Lucas $(a_1, a_2, \ldots, a_{r+p(p-1)} = \pm 1)$ pseudoprime and a Lucas $(b_1, b_2, \ldots, b_r = \pm 1)$ pseudoprime. Let $x_1, x_2, \ldots, x_r, x_{r+1}, \ldots, x_{r+p(p-1)}$ be the characteristic roots of $f(x)$, where $x_1, x_2, \ldots, x_r$ are the characteristic roots of $g(x)$ and $x_{r+1}, \ldots, x_{r+p(p-1)}$ are the characteristic roots of $g_1(x)$. Then

$$\begin{aligned}
&G_M(a_1, a_2, \ldots, a_{r+p(p-1)}) \\
&= (x_1^M + x_2^M + \cdots + x_r^M) + (x_{r+1}^M + x_{r+2}^M + \cdots + x_{r+p(p-1)}^M) \\
&= G_M(b_1, b_2, \ldots, b_r) + (1 + 1 + \cdots + 1) \\
&= G_M(b_1, b_2, \ldots, b_r) + (p^2 - p) \equiv G_1(a_1, a_2, \ldots, a_{r+p-1}) \\
&= (x_1 + x_2 + \cdots + x_r) + (x_{r+1} + x_{r+2} + \cdots + x_{r+p(p-1)}) \\
&= G_1(b_1, b_2, \ldots, b_r) + 0 \pmod{M}.
\end{aligned} \tag{3.16}$$

Noting that $G_M(b_1, b_2, \ldots, b_r) \equiv G_1(b_1, b_2, \ldots, b_r) \pmod{M}$, we obtain from (3.16) that

$$p^2 - p \equiv 0 \pmod{M},$$

which is a contradiction, since $p^2 \mid M$.

Now suppose that $M = pi$, where $p \nmid i$. We note that

$$x_{r+1}^M, x_{r+2}^M, \ldots, x_{r+p(p-1)}^M$$

comprise the $p - 1$ primitive pth roots of unity, each repeated p times. Then

$$\begin{aligned}
&G_M(a_1, a_2, \ldots, a_{r+p(p-1)}) \\
&= (x_1^M + x_2^M + \cdots + x_r^M) + (x_{r+1}^M + x_{r+2}^M + \cdots + x_{r+p(p-1)}^M) \\
&= G_M(b_1, b_2, \ldots, b_r) + p(-1) = G_M(b_1, b_2, \ldots, b_r) - p \\
&\equiv G_1(a_1, a_2, \ldots, a_{r+p-1}) \\
&= (x_1 + x_2 + \cdots + x_r) + (x_{r+1} + x_{r+2} + \cdots + x_{r+p(p-1)}) \\
&= G_1(b_1, b_2, \ldots, b_r) + 0 \pmod{M}.
\end{aligned} \tag{3.17}$$

Since $G_M(b_1, b_2, \ldots, b_r) \equiv G_1(b_1, b_2, \ldots, b_r) \pmod{M}$, it follows from (3.17) that

$$-p \equiv 0 \pmod{M}.$$

This is a contradiction, since $p \mid M$ and M is composite. The result now follows. □

Remark 3.6. *We use the notation and definitions of Corollaries 3.4 and 3.5. We note that the proof of Corollaries 3.4 and 3.5 show that in fact, no traditional Lucas $(a_1, a_2, \ldots, a_{r+\phi(p^j)} = \pm 1)$ pseudoprime divisible by p can even be a traditional Lucas $(b_1, b_2, \ldots, b_r = \pm 1)$ pseudoprime, where $j = 1$ or 2.*

Using Theorem 3.2, we can find higher order Lucas pseudoprimes which are equal to Lucas $(1, 1)$ pseudoprimes.

Corollary 3.7. *Let the Lucas $(a_1, a_2, \ldots, a_k = 1)$ sequence have the characteristic polynomial $f(x)g(x)$, where $f(x) = x^2 - x - 1$ and $g(x)$ is a product of j polynomials, each of which is a cyclotomic polynomial of order a power of 2. We do not assume that these j cyclotomic polynomials are necessarily distinct. Then the set of Lucas $(a_1, a_2, \ldots, a_k = 1)$ pseudoprimes is equal to the set of Lucas $(1, 1)$ pseudoprimes.*

Proof. First note that $f(x) = x^2 - x - 1$ is the characteristic polynomial of the Lucas $(1, 1)$ sequence. Since $g(x)$ is a product of cyclotomic polynomials, each of which is of order a power of 2 and the Lucas $(1, 1)$ sequence has no even pseudoprimes by [10], it suffices by Theorem 3.2 to show that the Lucas $(a_1, a_2, \ldots, a_k = 1)$ sequence has no even pseudoprimes. Let $L_n = G_n(1, 1)$ as usual, and let $G_n = G_n(a_1, a_2, \ldots, a_k = 1)$. Let $x_1 = (1 + \sqrt{5})/2$ and $x_2 = (1 - \sqrt{5})/2$ be the characteristic roots of $f(x)$ and let $x_3, x_4, \ldots, x_k$ be the characteristic roots of $g(x)$. Suppose that M is an even Lucas $(a_1, a_2, \ldots, a_k = \pm 1)$ pseudoprime. Let 2^t be the largest order of any of the j cyclotomic polynomials dividing $g(x)$. Then each of $x_3, x_4, \ldots, x_k$ is a 2^tth root of unity. Suppose that $M \equiv s \pmod{2^t}$, where $0 \le s \le 2^t - 1$. Note that $L_M = L_{-M}$ by the proof of Lemma 2.1. Then

$$\begin{aligned} G_M &= (x_1^M + x_2^M) + (x_3^M + x_4^M + \cdots + x_k^M) \\ &= (x_1^M + x_2^M) + (x_3^s + x_4^s + \cdots + x_k^s) = L_M + (x_3^s + x_4^s + \cdots + x_k^s) \\ &\equiv G_1 = (x_1 + x_2) + (x_3 + x_4 + \cdots + x_k) = L_1 + (x_3 + x_4 + \cdots + x_k) \\ &= 1 + (x_3 + x_4 + \cdots + x_k) \pmod{M} \end{aligned} \tag{3.18}$$

and

$$\begin{aligned} G_{-M} &= (x_1^{-M} + x_2^{-M}) + (x_3^{-M} + x_4^{-M} + \cdots + x_k^{-M}) \\ &= (x_1^{-M} + x_2^{-M}) + (x_3^{-s} + x_4^{-s} + \cdots + x_k^{-s}) \\ &= L_{-M} + (x_3^{-s} + x_4^{-s} + \cdots + x_k^{-s}) \equiv G_{-1} \\ &= (x_1^{-1} + x_2^{-1}) + (x_3^{-1} + x_4^{-1} + \cdots + x_k^{-1}) \\ &= L_{-1} + (x_3^{-1} + x_4^{-1} + \cdots + x_k^{-1}) \\ &= -1 + (x_3^{-1} + x_4^{-1} + \cdots + x_k^{-1}) \pmod{M}. \end{aligned} \tag{3.19}$$

Noting that $1/x_i$ is a root of $g(x)$ if and only if x_i is a root of $g(x)$, and that x_i and $1/x_i$ each occurs to the same multiplicity in $g(x)$, where $3 \le i \le k$, we see that

$$(x_3^s + x_4^s + \cdots + x_k^s) = (x_3^{-s} + x_4^{-s} + \cdots + x_k^{-s}) \tag{3.20}$$

and

$$(x_3 + x_4 + \cdots + x_k) = (x_3^{-1} + x_4^{-1} + \cdots + x_k^{-1}). \tag{3.21}$$

Let $c_1 = (x_3^s + x_4^s + \cdots + x_k^s)$ and $c_2 = (x_3 + x_4 + \cdots + x_k)$. Since $(x_3^s + x_4^s + \cdots + x_k^s)$ and $(x_3 + x_4 + \cdots + x_k)$ are both symmetric polynomials with integer coefficients in the roots of the polynomial $g(x)$, we see that each of c_1 and c_2 is a rational integer. It follows from (3.18)-(3.21) that

$$L_M + c_1 \equiv L_1 + c_2 = 1 + c_2 \equiv L_{-M} + c_1 \equiv L_{-1} + c_2 = -1 + c_2 \pmod{M}, \tag{3.22}$$

which implies that

$$1 \equiv -1 \pmod{M}.$$

Hence, $M \mid 2$, which is a contradiction since M is composite. □

Example 3.3. *We observe that the characteristic polynomials of the Lucas* $(0, 2, 1)$*,* $(1, 0, 1, 1)$*,* $(1, 0, 1, 1, 2, 1)$*, and* $(1, 1, 0, -1, 1, 1)$ *sequences are* $(x^2 - x - 1)(x + 1)$*,* $(x^2 - x - 1)(x^2 + 1)$*,* $(x^2 - x - 1)(x^2 + 1)(x + 1)$*, and* $(x^2 - x - 1)(x^4 + 1)$*, respectively. Hence, by Corollary 3.7, the sets of Lucas* $(1, 1)$*,* $(0, 2, 1)$*,* $(1, 0, 1, 1)$*,* $(1, 0, 1, 1, 2, 1)$*, and* $(1, 1, 0, -1, 1, 1)$ *pseudoprimes are all equal.*

We next show that certain Lucas sequences have infinitely many pseudoprimes.

Corollary 3.8. *For any* $k \geq 2$*, there exists a Lucas* $(a_1, a_2, \ldots, a_k = \pm 1)$ *sequence having infinitely many Lucas* $(a_1, a_2, \ldots, a_k = \pm 1)$ *pseudoprimes.*

Proof. By [7], there exist infinitely many Lucas $(1, 1)$ pseudoprimes. The result now follows for $k = 2$ by using the Lucas $(1, 1)$ sequence. Suppose that $k > 2$. Let the binary expansion of $k - 2$ be given by

$$2^{b_1} + 2^{b_2} + \cdots + 2^{b_r},$$

where $b_1 > b_2 > \cdots > b_r \geq 0$. Note that $x^{2^i} + 1$ is a cyclotomic polynomial of order 2^{i+1} for $i \geq 0$. Then by Corollary 3.7,

$$(x^2 - x - 1)(x^{2^{b_1}} + 1)(x^{2^{b_2}} + 1) \cdots (x^{2^{b_r}} + 1)$$

is the characteristic polynomial of a Lucas $(a_1, a_2, \ldots, a_k = \pm 1)$ sequence in which the set of Lucas $(1, 1)$ pseudoprimes is equal to the set of Lucas $(a_1, a_2, \ldots, a_k = \pm 1)$ pseudoprimes. □

Remark 3.9. *We note that it also follows from the results in* [5] *that for an arbitrary* $k \geq 2$*, any Lucas* $(a_1, a_2, \ldots, a_k = \pm 1)$ *sequence with square-free characteristic polynomial has infinitely many Lucas* $(a_1, a_2, \ldots, a_k = \pm 1)$ *pseudoprimes.*

4. Numerical Results

We conclude this paper with a table of Lucas $(a_1, a_2, \ldots, a_k = \pm 1)$ pseudoprimes for several different k.

k	$(a_1, a_2, \ldots, a_k)$	pseudoprimes $\leq N$
2	$(0, 1)$	$9, 15, 21, 25, 27, 33, 35, 39, 45, 49, 51, 55, 57 \leq 60$
2	$(0, -1)$	$9, 15, 21, 25, 27, 33, 35, 39, 45, 49, 51, 55, 57 \leq 60$
2	$(1, 1)$	$705, 2465, 2737, 3745, 4181, 5777, 6721 \leq 10000$
2	$(1, -1)$	$25, 35, 49, 55, 65, 77, 85, 91, 95 \leq 100$
2	$(-1, 1)$	≤ 100000
2	$(-1, -1)$	$4, 8, 16, 32, 64, 128, 256, 512, 1024, 2048, 4096 \leq 5000$
2	$(2, 1)$	$4, 169, 385, 961, 1105, 1121, 3827, 4901, 6265, 6441 \leq 6500$
2	$(2, -1)$	$4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20, 21, 22, 24 \leq 24$
2	$(-2, 1)$	$4 \leq 100000$
2	$(-2, -1)$	$4 \leq 100000$
2	$(3, 1)$	$33, 65, 119, 273, 377, 385, 533, 561, 649 \leq 1000$
2	$(3, -1)$	$4, 15, 44, 105, 195, 231, 323, 377, 435, 665, 705 \leq 800$
2	$(-3, 1)$	≤ 100000
2	$(-3, -1)$	≤ 100000
2	$(4, 1)$	$9, 85, 161, 341, 705, 897, 901, 1105, 1281, 1853 \leq 2000$
2	$(4, -1)$	$10, 209, 230, 231, 399, 430, 455, 530, 901, 903, 923, 989 \leq 1000$
2	$(-4, 1)$	≤ 100000
2	$(-4, -1)$	≤ 100000
2	$(5, 1)$	$9, 27, 65, 121, 145, 377, 385, 533, 1035, 1189, 1305 \leq 1500$
2	$(5, -1)$	$15, 21, 35, 105, 161, 195, 255, 345, 385, 399, 465 \leq 500$
2	$(-5, 1)$	≤ 100000
2	$(-5, -1)$	$4 \leq 100000$
3	$(0, 0, 1)$	$4, 8, 10, 14, 16, 20, 22, 25, 26, 28, 32, 34, 35, 38, 40 \leq 40$
3	$(0, 0, -1)$	$4, 8, 10, 14, 16, 20, 22, 25, 26, 28, 32, 34, 35, 38, 40 \leq 40$
3	$(0, 1, 1)$	≤ 100000
3	$(0, 1, -1)$	≤ 100000
3	$(0, -1, 1)$	≤ 100000
3	$(0, -1, -1)$	≤ 100000
3	$(1, 0, 1)$	≤ 100000
3	$(1, 0, -1)$	≤ 100000
3	$(-1, 0, 1)$	≤ 100000
3	$(-1, 0, -1)$	≤ 100000

k	$(a_1, a_2, \ldots, a_k)$	pseudoprimes $\leq N$
3	$(0, 2, 1)$	$705, 2465, 2737, 3745, 4181, 5777, 6721 \leq 10000$
3	$(0, 2, -1)$	$705, 2465, 2737, 3745, 4181, 5777, 6721 \leq 10000$
3	$(0, -2, 1)$	≤ 100000
3	$(0, -2, -1)$	≤ 100000
3	$(2, 0, 1)$	≤ 100000
3	$(2, 0, -1)$	$705, 2465, 2737, 3745, 4181, 5777, 6721, 10877, \leq 13000$
3	$(-2, 0, 1)$	≤ 100000
3	$(-2, 0, -1)$	≤ 100000
3	$(1, 1, 1)$	≤ 100000
3	$(1, 1, -1)$	$9, 15, 21, 25, 27, 33, 35, 39, 45, 49, 51, 55, 57 \leq 60$
3	$(1, -1, 1)$	$9, 15, 21, 25, 27, 33, 35, 39, 45, 49, 51, 55, 57 \leq 60$
3	$(1, -1, -1)$	$30 \leq 100000$
3	$(-1, 1, 1)$	$4 \leq 100000$
3	$(-1, 1, -1)$	≤ 100000
3	$(-1, -1, 1)$	≤ 100000
3	$(-1, -1, -1)$	$4 \leq 100000$
3	$(0, 3, 1)$	≤ 100000
3	$(0, 3, -1)$	≤ 100000
3	$(0, -3, 1)$	≤ 100000
3	$(0, -3, -1)$	≤ 100000
3	$(3, 0, 1)$	≤ 100000
3	$(3, 0, -1)$	≤ 100000
3	$(-3, 0, 1)$	≤ 100000
3	$(-3, 0, -1)$	≤ 100000
3	$(1, 2, 1)$	$4 \leq 100000$
3	$(1, 2, -1)$	$4 \leq 100000$
3	$(1, -2, 1)$	$4 \leq 100000$
3	$(1, -2, -1)$	$4 \leq 100000$
3	$(-1, 2, 1)$	≤ 100000
3	$(-1, 2, -1)$	≤ 100000
3	$(-1, -2, 1)$	≤ 100000
3	$(-1, -2, -1)$	≤ 100000
3	$(2, 1, 1)$	≤ 100000
3	$(2, 1, -1)$	$4 \leq 100000$
3	$(2, -1, 1)$	$4 \leq 100000$
3	$(2, -1, -1)$	≤ 100000
3	$(-2, 1, 1)$	≤ 100000
3	$(-2, 1, -1)$	$4 \leq 100000$
3	$(-2, -1, 1)$	$4 \leq 100000$
3	$(-2, -1, -1)$	≤ 100000

k	$(a_1, a_2, \ldots, a_k)$	pseudoprimes $\leq N$
3	$(0, 4, 1)$	$4 \leq 100000$
3	$(0, 4, -1)$	$4 \leq 100000$
3	$(0, -4, 1)$	$4 \leq 100000$
3	$(0, -4, -1)$	$4 \leq 100000$
3	$(4, 0, 1)$	$4 \leq 100000$
3	$(4, 0, -1)$	$4 \leq 100000$
3	$(-4, 0, 1)$	$4 \leq 100000$
3	$(-4, 0, -1)$	$4 \leq 100000$
3	$(1, 3, 1)$	$169, 385, 961, 1105, 1121, 3827, 4901, 6265, 6441 \leq 6500$
3	$(1, 3, -1)$	≤ 100000
3	$(1, -3, 1)$	≤ 100000
3	$(1, -3, -1)$	$33153, 79003 \leq 100000$
3	$(-1, 3, 1)$	≤ 100000
3	$(-1, 3, -1)$	$4 \leq 100000$
3	$(-1, -3, 1)$	$4, 117 \leq 100000$
3	$(-1, -3, -1)$	$10 \leq 100000$
3	$(3, 1, 1)$	$4, 66, 33153, 79003 \leq 100000$
3	$(3, 1, -1)$	≤ 100000
3	$(3, -1, 1)$	≤ 100000
3	$(3, -1, -1)$	$4, 169, 385, 961, 1105, 1121, 3827, 4901, 6265, 6441 \leq 6500$
3	$(-3, 1, 1)$	≤ 100000
3	$(-3, 1, -1)$	≤ 100000
3	$(-3, -1, 1)$	$6, 18, 66, 198 \leq 100000$
3	$(-3, -1, -1)$	≤ 100000
3	$(2, 2, 1)$	$79003 \leq 100000$
3	$(2, 2, -1)$	$15, 105, 195, 231, 323, 377, 435, 665, 705, 1443, 1551 \leq 1800$
3	$(2, -2, 1)$	$25, 35, 49, 55, 65, 77, 85, 91, 95, 115, 119, 121, 125, 133 \leq 140$
3	$(2, -2, -1)$	$79003 \leq 100000$
3	$(-2, 2, 1)$	≤ 100000
3	$(-2, 2, -1)$	≤ 100000
3	$(-2, -2, 1)$	≤ 100000
3	$(-2, -2, -1)$	≤ 100000
4	$(0, 0, 0, 1)$	$4, 6, 9, 10, 14, 15, 18, 21, 22, 25, 26, 27, 30, 33, 34, 35, 38, 39 \leq 40$
4	$(0, 0, 0, -1)$	$4, 6, 9, 10, 14, 15, 18, 21, 22, 25, 26, 27, 30, 33, 34, 35, 38, 39 \leq 40$
4	$(0, 0, 1, 1)$	≤ 100000
4	$(0, 0, 1, -1)$	$4, 34, 38, 46, 62, 94, 106, 122, 158, 166, 214, 218, 226 \leq 270$
4	$(0, 0, -1, 1)$	$4, 34, 38, 46, 62, 94, 106, 122, 158, 166, 214, 218, 226 \leq 270$
4	$(0, 0, -1, -1)$	≤ 100000
4	$(0, 1, 0, 1)$	$9, 12, 15, 21, 25, 27, 33, 35, 36, 39, 45, 49, 51, 55, 57 \leq 60$
4	$(0, 1, 0, -1)$	$9, 15, 21, 25, 27, 33, 35, 39, 45, 49, 51, 55, 57, 63, 65 \leq 68$
4	$(0, -1, 0, 1)$	$9, 12, 15, 21, 25, 27, 33, 35, 36, 39, 45, 49, 51, 55, 57 \leq 60$
4	$(0, -1, 0, -1)$	$9, 15, 21, 25, 27, 33, 35, 39, 45, 49, 51, 55, 57, 63, 65 \leq 68$

k	$(a_1, a_2, \dots, a_k)$	pseudoprimes $\leq N$
4	$(1, 0, 0, 1)$	$4, 34, 38, 46, 62, 94, 106, 122, 158, 166, 214, 218, 226 \leq 250$
4	$(1, 0, 0, -1)$	$4, 34, 38, 46, 62, 94, 106, 122, 158, 166, 214, 218, 226 \leq 250$
4	$(-1, 0, 0, 1)$	≤ 100000
4	$(-1, 0, 0, -1)$	≤ 100000
4	$(0, 0, 2, 1)$	$6 \leq 100000$
4	$(0, 0, 2, -1)$	≤ 100000
4	$(0, 0, -2, 1)$	≤ 100000
4	$(0, 0, -2, -1)$	$6 \leq 100000$
4	$(0, 2, 0, 1)$	$4, 9, 12, 15, 21, 25, 27, 33, 35, 36, 39, 45, 49, 51, 55, 57, 63 \leq 64$
4	$(0, 2, 0, -1)$	$4, 9, 15, 21, 25, 27, 33, 35, 39, 45, 49, 51, 55, 57, 63, 65, 69 \leq 70$
4	$(0, -2, 0, 1)$	$4, 9, 12, 15, 21, 25, 27, 33, 35, 36, 39, 45, 49, 51, 55, 57, 63 \leq 64$
4	$(0, -2, 0, -1)$	$4, 9, 15, 21, 25, 27, 33, 35, 39, 45, 49, 51, 55, 57, 63, 65, 69 \leq 70$
4	$(2, 0, 0, 1)$	≤ 100000
4	$(2, 0, 0, -1)$	≤ 100000
4	$(-2, 0, 0, 1)$	$10, 38 \leq 100000$
4	$(-2, 0, 0, -1)$	$10, 38 \leq 100000$
4	$(0, 1, 1, 1)$	≤ 100000
4	$(0, 1, 1, -1)$	≤ 100000
4	$(0, 1, -1, 1)$	≤ 100000
4	$(0, 1, -1, -1)$	≤ 100000
4	$(0, -1, 1, 1)$	≤ 100000
4	$(0, -1, 1, -1)$	≤ 100000
4	$(0, -1, -1, 1)$	≤ 100000
4	$(0, -1, -1, -1)$	≤ 100000
4	$(1, 0, 1, 1)$	$705, 2465, 2737, 3745, 4181, 5777, 6721, 10877, 13201 \leq 15000$
4	$(1, 0, 1, -1)$	$4, 8, 10, 14, 16, 20, 22, 25, 26, 28, 32, 34, 35, 38, 40, 44, 46 \leq 48$
4	$(1, 0, -1, 1)$	$4, 8, 10, 14, 16, 20, 22, 25, 26, 28, 32, 34, 35, 38, 40, 44, 46 \leq 48$
4	$(1, 0, -1, -1)$	$49, 119, 161, 497, 679, 721, 791, 1057, 1169, 1351, 1393 \leq 1600$
4	$(-1, 0, 1, 1)$	≤ 100000
4	$(-1, 0, 1, -1)$	≤ 100000
4	$(-1, 0, -1, 1)$	≤ 100000
4	$(-1, 0, -1, -1)$	≤ 100000
4	$(1, 1, 0, 1)$	≤ 100000
4	$(1, 1, 0, -1)$	≤ 100000
4	$(1, -1, 0, 1)$	≤ 100000
4	$(1, -1, 0, -1)$	≤ 100000
4	$(-1, 1, 0, 1)$	≤ 100000
4	$(-1, 1, 0, -1)$	≤ 100000
4	$(-1, -1, 0, 1)$	≤ 100000
4	$(-1, -1, 0, -1)$	≤ 100000

k	$(a_1, a_2, \ldots, a_k)$	pseudoprimes $\leq N$
4	$(0, 0, 3, 1)$	$4 \leq 100000$
4	$(0, 0, 3, -1)$	$25 \leq 100000$
4	$(0, 0, -3, 1)$	≤ 100000
4	$(0, 0, -3, -1)$	$4, 25 \leq 100000$
4	$(0, 3, 0, 1)$	$6, 9, 15, 18, 21, 25, 27, 33, 35, 39, 45, 49, 51, 54, 55, 57, 63 \leq 64$
4	$(0, 3, 0, -1)$	$6, 9, 15, 18, 21, 25, 27, 33, 35, 39, 45, 49, 51, 54, 55, 57, 63 \leq 64$
4	$(0, -3, 0, 1)$	$6, 9, 15, 18, 21, 25, 27, 33, 35, 39, 45, 49, 51, 54, 55, 57, 63 \leq 64$
4	$(0, -3, 0, -1)$	$6, 9, 15, 18, 21, 25, 27, 33, 35, 39, 45, 49, 51, 54, 55, 57, 63 \leq 64$
4	$(3, 0, 0, 1)$	≤ 100000
4	$(3, 0, 0, -1)$	$25 \leq 100000$
4	$(-3, 0, 0, 1)$	$4, 46 \leq 100000$
4	$(-3, 0, 0, -1)$	$4, 46 \leq 100000$
4	$(0, 1, 2, 1)$	$2465, 2737, 3745, 4181, 5777, 6721, 10877, 13201 \leq 15000$
4	$(0, 1, 2, -1)$	$49 \leq 100000$
4	$(0, 1, -2, 1)$	$2465, 2737, 3745, 4181, 5777, 6721, 10877, 13201 \leq 15000$
4	$(0, 1, -2, -1)$	$49 \leq 100000$
4	$(0, -1, 2, 1)$	≤ 100000
4	$(0, -1, 2, -1)$	≤ 100000
4	$(0, -1, -2, 1)$	≤ 100000
4	$(0, -1, -2, -1)$	≤ 100000
4	$(1, 0, 2, 1)$	≤ 100000
4	$(1, 0, 2, -1)$	≤ 100000
4	$(1, 0, -2, 1)$	≤ 100000
4	$(1, 0, -2, -1)$	≤ 100000
4	$(-1, 0, 2, 1)$	≤ 100000
4	$(-1, 0, 2, -1)$	≤ 100000
4	$(-1, 0, -2, 1)$	≤ 100000
4	$(-1, 0, -2, -1)$	≤ 100000
4	$(1, 2, 0, 1)$	$4 \leq 100000$
4	$(1, 2, 0, -1)$	$4 \leq 100000$
4	$(1, -2, 0, 1)$	$4 \leq 100000$
4	$(1, -2, 0, -1)$	$4 \leq 100000$
4	$(-1, 2, 0, 1)$	≤ 100000
4	$(-1, 2, 0, -1)$	≤ 100000
4	$(-1, -2, 0, 1)$	≤ 100000
4	$(-1, -2, 0, -1)$	≤ 100000
4	$(0, 2, 1, 1)$	≤ 100000
4	$(0, 2, 1, -1)$	$4 \leq 100000$
4	$(0, 2, -1, 1)$	$4 \leq 100000$
4	$(0, 2, -1, -1)$	≤ 100000
4	$(0, -2, 1, 1)$	≤ 100000
4	$(0, -2, 1, -1)$	$4 \leq 100000$
4	$(0, -2, -1, 1)$	$4 \leq 100000$
4	$(0, -2, -1, -1)$	≤ 100000

k	$(a_1, a_2, \ldots, a_k)$	pseudoprimes $\leq N$
4	$(2, 0, 1, 1)$	≤ 100000
4	$(2, 0, 1, -1)$	≤ 100000
4	$(2, 0, -1, 1)$	≤ 100000
4	$(2, 0, -1, -1)$	≤ 100000
4	$(-2, 0, 1, 1)$	≤ 100000
4	$(-2, 0, 1, -1)$	$38 \leq 100000$
4	$(-2, 0, -1, 1)$	$38 \leq 100000$
4	$(-2, 0, -1, -1)$	≤ 100000
4	$(2, 1, 0, 1)$	≤ 100000
4	$(2, 1, 0, -1)$	$49 \leq 100000$
4	$(2, -1, 0, 1)$	$2465, 2737, 3745, 4181, 5777, 6721, 10877, 13201 \leq 15000$
4	$(2, -1, 0, -1)$	≤ 100000
4	$(-2, 1, 0, 1)$	≤ 100000
4	$(-2, 1, 0, -1)$	≤ 100000
4	$(-2, -1, 0, 1)$	≤ 100000
4	$(-2, -1, 0, -1)$	≤ 100000
4	$(1, 1, 1, 1)$	$49 \leq 100000$
4	$(1, 1, 1, -1)$	$195, 897, 6213, 11285, 27889, 30745, 38503, 39601 \leq 100000$
4	$(1, 1, -1, 1)$	≤ 100000
4	$(1, 1, -1, -1)$	$9, 33, 51, 57, 121, 123, 129, 177, 201, 219, 249, 267 \leq 275$
4	$(1, -1, 1, 1)$	$49 \leq 100000$
4	$(1, -1, 1, -1)$	$9, 21, 27, 33, 39, 49, 51, 57, 63, 69, 77, 81, 87, 91, 93 \leq 95$
4	$(1, -1, -1, 1)$	≤ 100000
4	$(1, -1, -1, -1)$	$53021 \leq 100000$
4	$(-1, 1, 1, 1)$	$4, 6, 8, 14, 16, 22, 32, 62, 64, 128, 256, 302, 512, 662 \leq 900$
4	$(-1, 1, 1, -1)$	≤ 100000
4	$(-1, 1, -1, 1)$	$60783 \leq 100000$
4	$(-1, 1, -1, -1)$	$4, 8, 16, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192 \leq 15000$
4	$(-1, -1, 1, 1)$	$4, 8, 16, 32, 64, 128, 256, 512, 1024, 2045, 4096, 8192 \leq 15000$
4	$(-1, -1, 1, -1)$	≤ 100000
4	$(-1, -1, -1, 1)$	≤ 100000
4	$(-1, -1, -1, -1)$	$4, 8, 16, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192 \leq 15000$

References

[1] W. W. Adams and D. Shanks, *Strong primality tests that are not sufficient*, Math. Comp., **39** (1982), 255–300.

[2] A. O. L. Atkin, *Intelligent primality test offer*, Computational Perspectives on Number Theory, (Eds. D. A. Buell and J. T. Teitelbaum) AMS/IP Stud. Adv. Math. 7, Amer. Math. Soc., Providence, 1998, 1–11.

[3] C. Cooper and L. Somer, *Lucas* $(a_1, a_2, \ldots, a_k = 1)$ *sequences and pseudoprimes*, Applications of Fibonacci Numbers, Vol 12, (to appear).

[4] J. Grantham, *Frobenius pseudoprimes*, Math. Comp., **70** (2001), 837–891.

[5] J. Grantham, *There are infinitely many Perrin pseudoprimes*, Preprint.

[6] S. Gurak, *Pseudoprimes for higher-order linear recurrence sequences*, Math. Comp., **55** (1980), 783–813.

[7] A. Rotkiewicz, *On the pseudoprimes with respect to the Lucas sequence*, Bull. Acad. Polon. Sci. Ser. Math. Astronom. Phys., **21** (1973), 793–797.

[8] L. Somer, *Divisibility of terms in Lucas sequences of the second kind by their subscripts*, Applications of Fibonacci Numbers, Vol. 6 (Eds. G. E. Bergum et al.), Kluwer Academic Publishers, Dordrecht, 1996, 473–486.

[9] G. Szekeres, *Higher Order Pseudoprimes in Primality Testing*, Combinatorics, Paul Erdős is Eighty, Bolyai Soc. Math. Stud., Vol. 2, János Bolyai Math Soc., Budapest, 1996, 451–458.

[10] D. J. White, J. N. Hunt, and L. A. G. Dresel, *Uniform Huffman sequences do not exist*, Bull. London Math. Soc., 9 (1977), 193–198.

MSC2010: 11B83, 11B50

Department of Mathematics, The Catholic University of America, Washington, DC 20064
E-mail address: somer@cua.edu

Department of Mathematics and Computer Science, University of Central Missouri, Warrensburg, MO 64093
E-mail address: cooper@ucmo.edu