Pseudoprimality related to the generalised Lucas sequences

Dorin Andrica

Babeş-Bolyai University, Faculty of Mathematics and Computer Science, 400084 Cluj-Napoca, Romania

Ovidiu Bagdasar*

School of Computing and Engineering, University of Derby, Kedleston Road, DE22 1GB, United Kingdom

Abstract

Some arithmetic properties and new pseudoprimality results concerning generalized Lucas sequences are presented. The findings are connected to the classical Fibonacci, Lucas, Pell, and Pell-Lucas pseudoprimality. During the process new integer sequences are found and some conjectures are formulated.

Key words: Generalised Lucas sequences, Legendre symbol, Jacobi symbol, Pseudoprimality

1. Introduction

Despite being subject to intensive research for many centuries, the classical Fibonacci, Lucas, Pell, or Pell-Lucas sequences have many interesting properties and applications which are still being discovered. Also, some of their generalizations have significant theoretical and practical importance [2, 4, 10].

Let a and b be integers. The *generalized Lucas* sequence $\{U_n(a,b)\}_{n\geq 0}$ and its companion, the *generalized Pell-Lucas* sequence $\{V_n(a,b)\}_{n\geq 0}$, are defined by

$$U_{n+2} = aU_{n+1} - bU_n, \quad U_0 = 0, U_1 = 1, \quad n = 0, 1, \ldots \tag{1}$$

$$V_{n+2} = aV_{n+1} - bV_n, \quad V_0 = 2, V_1 = a, \quad n = 0, 1, \ldots. \tag{2}$$

The standard method to study these sequences involves the roots of the characteristic equation $z^2 - az + b = 0$. Assuming that $D = a^2 - 4b \neq 0$ this quadratic has the distinct roots

$$\alpha = \frac{a + \sqrt{D}}{2}, \quad \beta = \frac{a - \sqrt{D}}{2}.$$

By Viéte's relations, we clearly have $\alpha + \beta = a$, $\alpha\beta = b$, while $\alpha - \beta = \sqrt{D}$.

Using these notations, the following Binet-type formulae are obtained

$$U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} = \frac{1}{\sqrt{D}}\left(\alpha^n - \beta^n\right), \quad n = 0, 1, \ldots \tag{3}$$

$$V_n = \alpha^n + \beta^n, \quad n = 0, 1, \ldots. \tag{4}$$

*Corresponding author

Email addresses: dandrica@math.ubbcluj.ro (Dorin Andrica), o.bagdasar@derby.ac.uk (Ovidiu Bagdasar)

These formulae extend naturally to negative indices. We have

$$U_{-1} = \frac{1}{\sqrt{D}}\left(\alpha^{-1} - \beta^{-1}\right) = -\frac{1}{b}, \quad V_{-1} = \alpha^{-1} + \beta^{-1} = \frac{a}{b},$$

and in general, the following relations hold for any integer $n \geq 0$

$$U_{-n} = \frac{1}{\sqrt{D}}\left(\alpha^{-n} - \beta^{-n}\right) = -\frac{1}{b^n}U_n, \quad V_{-n} = \alpha^{-n} + \beta^{-n} = \frac{1}{b^n}V_n. \tag{5}$$

Formula (3) can be expressed using the bivariate cyclotomic polynomials in α and β [15, p. 99], as

$$U_n = \prod_{d|n, d\geq 2} \Phi_d(\alpha, \beta),$$

where $\Phi_d(\alpha,\beta) = \prod_{j=1,\gcd(j,n)=1}^{n}(\alpha - \zeta^j\beta)$, and ζ is a primitive n-th root of unity. One may check that $\Phi_d(\alpha,\beta)$ is an integer for $d \geq 2$. This formula is useful in the study of some arithmetic properties of the integers U_n. A similar formula for V_n is

$$V_n = \prod_{d|n} \Phi_d(\alpha, \omega\beta),$$

where ω is an n-th root of -1. However, this formula has limited use as $\Phi_d(\alpha,\omega\beta)$ is not an integer.

For $b = -1$, if k is a positive real number, then the k-Fibonacci and k-Lucas numbers are obtained as $F_{k,n} = U_n(k,-1) = \frac{1}{\sqrt{D}}\left(\left(\frac{k+\sqrt{D}}{2}\right)^n - \left(\frac{k-\sqrt{D}}{2}\right)^n\right)$ and $L_{k,n} = V_n(k,-1) = \left(\frac{k+\sqrt{D}}{2}\right)^n + \left(\frac{k-\sqrt{D}}{2}\right)^n$, $D = k^2+4$. The classical Fibonacci and Lucas numbers are obtained as $F_n = U_n(1,-1)$ and $L_n = V_n(1,-1)$ with $D = 5$, while the classical Pell and Pell-Lucas numbers are given by $P_n = U_n(2,-1)$ and $Q_n = V_n(2,-1)$, for $D = 8$. Interestingly, the sequence $F_{3,n}$ of the "bronze" Fibonacci numbers indexed as A006190 in OEIS

$$0, 1, 3, 10, 33, 109, 360, 1189, 3927, 12970, 42837, 141481, \ldots,$$

is linked to lipidomics and the enumeration of fatty acids in [30]. For more applications see [22].

When $b = 1$, the sequences $U_n(a,1)$ have interesting combinatorial interpretations, while the terms $V_n(a,1)$ can be linked to the solutions of certain Diophantine equations (see [5]). There are also connections to important classes of polynomials (see [4, Chapter 2.2]). We mention

- Chebyshev polynomials of the first kind $T_n(x) = \frac{1}{2}V_n(2x,1)$;
- Chebyshev polynomials of the second kind $u_n(x) = U_n(2x,1)$;
- Hoggatt-Bicknell-King polynomial of Fibonacci kind $g_n(x) = U_n(x,1)$;
- Hoggatt-Bicknell-King polynomial of Lucas kind $h_n(x) = V_n(x,1)$.

For these sequences we have proved various density results, established necessary conditions to identify the terms, and shown that they can only contain finitely many perfect powers [8].

For $a = b+1$ with $b \geq 1$ we have $D = b-1$, $\alpha = b$, $\beta = 1$, where $U_n = \frac{b^n-1}{b-1}$ and $V_n = b^n + 1$. This case presents interest as here the terms U_n are linked to the Carmichael numbers.

In this paper we study properties of generalised Lucas sequences, when they are reduced modulo an integer. We extend and refine recent results obtained in [9] for Fibonacci sequences. The structure of this paper is as follows. In Section 2 we present some preliminary results and arithmetic properties, recently proved by the authors in [4] and [5]. In Section 3 we briefly review some classical pseudoprimality concepts. Section 4 is devoted to the notion of generalised Lucas and Pell-Lucas pseudoprimality of level k defined by the authors in [6], for which we here investigate the relationship between different levels. The results involve some weak pseudoprimality notions also defined by us in [7]. We also correct [Proposition 1, [9]] previously formulated for Fibonacci numbers. The definition of new primality concepts for generalized Lucas sequences enables one to formulate new primality tests. We give numerical simulations illustrating these concepts, some conjectures and links to recent entries in the *Online Encyclopedia of Integer Sequences* (OEIS). Finally, in Section 5 we suggest further developments and directions of research.

2. Some preliminary results

For a and b arbitrary integers, the terms of the sequences $\{U_n(a,b)\}_{n\geq 0}$ and $\{V_n(a,b)\}_{n\geq 0}$ will be shortly denoted by U_n and V_n. From (5), it follows that U_n and V_n are integers for all $n \in \mathbb{Z}$ if and only if $b = \pm 1$, therefore we shall focus on this case.

The following result has been recently proved by the authors [5].

Theorem 2.1 (Theorem 3.1, [5]). *Let p be an odd prime, k a non-negative integer, and r an arbitrary integer. If $b = \pm 1$ and a is an integer such that $D = a^2 - 4b > 0$ is not perfect square, then the sequences U_n and V_n satisfy the relations*

1) $2U_{kp+r} \equiv \left(\frac{D}{p}\right) U_k V_r + V_k U_r \pmod{p}$
2) $2V_{kp+r} \equiv D\left(\frac{D}{p}\right) U_k U_r + V_k V_r \pmod{p}$,

where $\left(\frac{D}{p}\right)$ denotes the Legendre symbol.

For $b = \pm 1$, the results below have been proved in [5].

Theorem 2.2 (Theorem 3.5, [5]). *Let p be an odd prime, and let $k > 0$ and a be integers with the property that $D = a^2 + 4 > 0$ is not a perfect square. If $U_n = U_n(a,-1)$ and $V_n = V_n(a,-1)$, then we have*

1) $U_{kp-\left(\frac{D}{p}\right)} \equiv U_{k-1} \pmod{p}$;
2) $V_{kp-\left(\frac{D}{p}\right)} \equiv \left(\frac{D}{p}\right) V_{k-1} \pmod{p}$.

Theorem 2.3 (Theorem 3.7, [5]). *Let p be an odd prime, and let $k > 0$ and a be integers with the property that $D = a^2 - 4 > 0$ is not a perfect square. If $U_n = U_n(a, 1)$ and $V_n = V_n(a, 1)$, then the following relations hold*

1) $U_{kp-\left(\frac{D}{p}\right)} \equiv \left(\frac{D}{p}\right) U_{k-1} \pmod{p}$;
2) $V_{kp-\left(\frac{D}{p}\right)} \equiv V_{k-1} \pmod{p}$.

Applying Theorem 2.1 for an integer $k \geq 0$ and $r = 0$, we obtain

$$U_{kp} \equiv \left(\frac{D}{p}\right) U_k \pmod{p};$$
$$V_{kp} \equiv V_k \pmod{p}.$$

In particular, when $k = 1$, these relations reduce to the well-known results (see, e.g., [31])

$$U_p \equiv \left(\frac{D}{p}\right) \pmod{p}; \tag{6}$$
$$V_p \equiv a \pmod{p}. \tag{7}$$

Also, applying Theorems 2.2 and 2.3 for $k = 1$, and since $U_0 = 0$ and $V_0 = 2$, one obtains the relations

$$U_{p-\left(\frac{D}{p}\right)} \equiv 0 \pmod{p}; \tag{8}$$
$$V_{p-\left(\frac{D}{p}\right)} \equiv 2\left(\frac{D}{p}\right)^{\frac{1-b}{2}}. \tag{9}$$

The following Cassini-type identities are useful for proving the main results in Section 4.

Lemma 2.4. *Let m and r be integers. The following identities hold*

1) $U_m^2 - U_{m-r}U_{m+r} = b^{m-r}U_r^2$;
2) $V_m^2 - V_{m-r}V_{m+r} = -Db^{m-r}U_r^2$;
3) $V_m^2 - DU_{m-r}U_{m+r} = b^{m-r}V_r^2$;
4) $DU_m^2 - V_{m-r}V_{m+r} = -b^{m-r}V_r^2$;
5) $U_mV_m - U_{m-r}V_{m+r} = b^{m-r}U_rV_r$.

Proof. Using the relations (3), (4), $\alpha\beta = b$, $\alpha - \beta = \sqrt{D}$, and $(\alpha - \beta)^2 = D$, we obtain successively.

1) $$U_m^2 - U_{m-r}U_{m+r} = \left(\frac{\alpha^m - \beta^m}{\alpha - \beta}\right)^2 - \frac{\alpha^{m-r} - \beta^{m-r}}{\alpha - \beta} \cdot \frac{\alpha^{m+r} - \beta^{m+r}}{\alpha - \beta}$$
$$= \frac{\alpha^{m+r}\beta^{m-r} - 2\alpha^m\beta^m + \alpha^{m-r}\beta^{m+r}}{(\alpha - \beta)^2} = \alpha^{m-r}\beta^{m-r}\left(\frac{\alpha^r - \beta^r}{\alpha - \beta}\right)^2 = b^{m-r}U_r^2.$$

$$2)\quad V_m^2 - V_{m-r}V_{m+r} = (\alpha^m+\beta^m)^2 - \left(\alpha^{m-r}+\beta^{m-r}\right)\left(\alpha^{m+r}+\beta^{m+r}\right)$$
$$= 2\alpha^m\beta^m - \alpha^{m-r}\beta^{m-r}\left(\alpha^{2r}+\beta^{2r}\right) = -(\alpha\beta)^{m-r}\left(\alpha^r-\beta^r\right)^2$$
$$= -b^{m-r}(\alpha-\beta)^2\left(\frac{\alpha^r-\beta^r}{\alpha-\beta}\right)^2 = -Db^{m-r}U_r^2.$$

$$3)\quad V_m^2 - DU_{m-r}U_{m+r} = (\alpha^m+\beta^m)^2 - D\frac{\alpha^{m-r}-\beta^{m-r}}{\alpha-\beta}\cdot\frac{\alpha^{m+r}-\beta^{m+r}}{\alpha-\beta}$$
$$= 2\alpha^m\beta^m + \alpha^{m+r}\beta^{m-r} + \alpha^{m-r}\beta^{m+r}$$
$$= 2\alpha^{m-r}\beta^{m-r}(\alpha^r+\beta^r)^2 = b^{m-r}V_r^2.$$

$$4)\quad DU_m^2 - V_{m-r}V_{m+r} = D\left(\frac{\alpha^m-\beta^m}{\alpha-\beta}\right)^2 - \left(\alpha^{m-r}+\beta^{m-r}\right)\cdot\left(\alpha^{m+r}+\beta^{m+r}\right)$$
$$= -2\alpha^m\beta^m - \alpha^{m+r}\beta^{m-r} + \alpha^{m-r}\beta^{m+r}$$
$$= -\alpha^{m-r}\beta^{m-r}(\alpha^r+\beta^r)^2 = -b^{m-r}V_r^2.$$

$$5)\quad U_mV_m - U_{m-r}V_{m+r} = \left(\frac{\alpha^m-\beta^m}{\alpha-\beta}\right)(\alpha^m+\beta^m) - \left(\frac{\alpha^{m-r}-\beta^{m-r}}{\alpha-\beta}\right)\left(\alpha^{m+r}+\beta^{m+r}\right)$$
$$= \frac{-\alpha^{m-r}\beta^{m+r}+\alpha^{m+r}\beta^{m-r}}{\alpha-\beta}$$
$$= (\alpha\beta)^{m-r}\frac{1}{\alpha-\beta}(\alpha^r-\beta^r)(\alpha^r+\beta^r) = b^rU_rV_r. \qquad \square$$

3. Primality tests and pseudoprimality properties

3.1. Jacobi's symbol

Let $n = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$ be the prime factorization of an odd integer n. The Jacobi symbol is defined as

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1}\left(\frac{a}{p_2}\right)^{\alpha_2}\cdots\left(\frac{a}{p_k}\right)^{\alpha_k},$$

where a is an integer. Clearly, when n is a prime, the Jacobi and Legendre symbols coincide.

Many properties of Jacobi's symbol are known. For example, it is completely multiplicative in both the numerator and denominator, that is for m, n, m_1, m_2, n_1, n_2 integers, we have

$$\left(\frac{m_1m_2}{n}\right) = \left(\frac{m_1}{n}\right)\left(\frac{m_2}{n}\right), \quad \text{so } \left(\frac{m^2}{n}\right) = \left(\frac{m}{n}\right)^2 = 1 \text{ or } 0;$$
$$\left(\frac{m}{n_1n_2}\right) = \left(\frac{m}{n_1}\right)\left(\frac{m}{n_2}\right), \quad \text{so } \left(\frac{m}{n^2}\right) = \left(\frac{m}{n}\right)^2 = 1 \text{ or } 0.$$

The Jacobi symbol also satisfies the law of quadratic reciprocity. This states that if m and n are odd positive coprime integers, then the following identity holds

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}} = \begin{cases} 1 & \text{if } n \equiv 1 \pmod 4 \text{ or } m \equiv 1 \pmod 4, \\ -1 & \text{if } n \equiv m \equiv 3 \pmod 4. \end{cases}$$

3.2. Some classical pseudoprimality concepts

Pseudoprimes are composite numbers which under certain conditions behave as the prime numbers. They have applications in the factorization of large integers, primality testing, and cryptography [20, 27].

Here we list some classical pseudoprimes, as well as some more recent examples.

3.2.1. Pseudoprimality of base a

Let p be a prime and let a be an integer. By Fermat's Little Theorem, the following relation holds

$$a^{p-1} \equiv 1 \pmod p.$$

A composite number n satisfying Fermat's congruence $a^{n-1} \equiv 1 \pmod n$ with $\gcd(a, n) = 1$, is called **pseudoprime to base** a. When $a = 2$, such a number is often simply called **pseudoprime**, or **Fermat pseudoprime**. They are indexed as A001567 in the OEIS [26], starting with the numbers

$$341, 561, 645, 1105, 1387, 1729, 1905, 2047, 2465, 2701, 2821, 3277, 4033, 4369, 4371, 4681, 5461, 6601, 7957, 8321,$$
$$8481, 8911, 10261, 10585, 11305, 12801, 13741, 13747, 13981, 14491, 15709, 15841, 16705, 18705, 18721, \ldots.$$

The composite integers which satisfy this property for every base are called **Carmichael numbers**. These are indexed as A002997 in the OEIS [26], and start with the terms

$$561, 1105, 1729, 2465, 2821, 6601, 8911, 10585, 15841, 29341, 41041, 46657, 52633, 62745, 63973, 75361, \ldots.$$

In 1994, Alford *et al.* in the paper [1], proved that there are infinitely many Carmichael numbers.

Many classes of pseudoprimes are defined by means of recurrent sequences.

3.2.2. Fibonacci pseudoprimes

If p is a prime, then the following relations follow by (6) and (8) applied for $a = 1$ and $b = -1$.

$$F_p \equiv \left(\frac{p}{5}\right) \pmod p; \tag{10}$$

$$F_{p-\left(\frac{p}{5}\right)} \equiv 0 \pmod p. \tag{11}$$

A composite number n is called a **Fibonacci pseudoprime** if $n \mid F_{n-\left(\frac{n}{5}\right)}$. The even pseudoprimes are indexed as A141137 in OEIS [26], while the odd Fibonacci pseudoprimes, indexed as A081264, start with

$$323, 377, 1891, 3827, 4181, 5777, 6601, 6721, 8149, 10877, 11663, 13201, 13981, 15251, 17119, 17711,$$
$$18407, 19043, 23407, 25877, 27323, 30889, 34561, 34943, 35207, 39203, 40501, 50183, 51841, 51983, \ldots.$$

Remark 3.1. (*i*) *Lehmer proved in [23] that there exist infinitely many Fibonacci pseudoprimes. However, we do not yet know if the Fibonacci sequence contains infinitely many primes.*

(*ii*) *Crandall et al. [13] called a prime p satisfying $p^2 \mid F_{p-(\frac{p}{5})}$ a* **Wall-Sun-Sun prime**. *There is no such prime smaller than 2.8×10^{16}. The only known way to check the congruence $F_{p-(\frac{p}{5})} \equiv 0 \pmod{p^2}$, is by explicit powering computations (see, e.g., [3] or [18]).*

In [9] the authors have introduced the notion of **Fibonacci pseudoprimes of level** k denoted by $\mathcal{F}_k$, which are composite numbers n satisfying the relation

$$n \mid F_{kn-(\frac{n}{5})} - F_{k-1}.$$

Clearly, for $k = 1$ one obtains the classical Fibonacci pseudoprimes.

3.2.3. Bruckman-Lucas pseudoprimes

For a prime p the following relations follow by replacing $a = 1$ and $b = -1$ in (7) and (9).

$$L_p \equiv 1 \pmod{p}; \tag{12}$$

$$L_{p-(\frac{p}{5})} \equiv 2\left(\frac{p}{5}\right) \pmod{p}. \tag{13}$$

A composite integer n satisfying $n \mid L_n - 1$ is called a **Bruckman-Lucas pseudoprime**. The sequence is indexed in the OEIS [26] as A005845, and begins with

$$705, 2465, 2737, 3745, 4181, 5777, 6721, 10877, 13201, 15251, 24465, 29281, 34561, 35785, 51841, 54705,$$
$$64079, 64681, 67861, 68251, 75077, 80189, 90061, 96049, 97921, 100065, 100127, 105281, 113573, \ldots.$$

Remark 3.2. *In 1964, Lehmer [23] proved that the set of Bruckman-Lucas pseudoprimes is infinite.*

In our paper [6] we have also defined the **Lucas pseudoprimes of level** k denoted by $\mathcal{L}_k$, which are composite numbers n satisfying the relation

$$n \mid L_{kn-(\frac{n}{5})} - \left(\frac{n}{5}\right) L_{k-1}.$$

For level $k = 1$, the first few odd composite integers satisfying $n \mid L_{n-(\frac{n}{5})} - 2\left(\frac{n}{5}\right)$ are

$$9, 49, 121, 169, 289, 361, 529, 841, 961, 1127, 1369, 1681, 1849, 2209, 2809, 3481, 3721,$$
$$3751, 4181, 4489, 4901, 4961, 5041, 5329, 5777, 6241, 6721, 6889, 7381, 7921, 9409, \ldots,$$

which we have added to OEIS as A339125. Numerical simulations suggest that no even numbers with this property exist, but at the moment we do not have a proof of this statement.

3.2.4. Pell and Pell-Lucas pseudoprimes

Similar primality and pseudoprimality notions are defined for Pell and Pell-Lucas numbers, P_n and Q_n. We will use the following identity $\left(\frac{8}{p}\right) = \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$, proved by Euler (see, e.g., [2, Theorem 9.1.2]).

The following well-known relations follow from (6), (7), (8) and (9) for $a = 2$ and $b = -1$.

If p is a prime, then the following relations hold (see Corollary 4.2 and Proposition 4.4 in [5])

$$\begin{aligned} P_p &\equiv \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} \pmod{p}; \\ P_{p-\left(\frac{2}{p}\right)} &\equiv 0 \pmod{p}; \\ Q_p &\equiv 2 \pmod{p}; \\ Q_{p-\left(\frac{p}{2}\right)} &\equiv 2\left(\frac{2}{p}\right) = 2(-1)^{\frac{p^2-1}{8}} \pmod{p}. \end{aligned}$$

An odd composite integer n is called a **Pell pseudoprime** if n divides $P_{n-(-1)^{\frac{n^2-1}{8}}}$.

The Pell pseudoprimes are indexed as A099011 in OEIS [26], starting with the terms

169, 385, 741, 961, 1121, 2001, 3827, 4879, 5719, 6215, 6265, 6441, 6479, 6601, 7055, 7801, 8119, 9799,

10945, 11395, 13067, 13079, 13601, 15841, 18241, 19097, 20833, 20951, 24727, 27839, 27971, 29183, ...

Remark 3.3. (*i*) *Kiss, Phong, and Lieuwen showed in 1986 that this sequence is infinite [21].*

(*ii*) *A prime number satisfying* $p^2 \mid P_{p-(-1)^{\frac{p^2-1}{8}}}$ *is called a Pell-Wieferich prime. Such numbers seem to be very few [25], and only* 13, 31, 1546463 *satisfy this property for* $p \leq 10^{14}$ *(see A238736 in [26]).*

The following concepts of pseudoprimality were defined by us in [4, Chapter 3.2], and [5], respectively.

An odd composite integer n is a **Pell-Lucas pseudoprime** if n divides $Q_n - 2$. The list of Pell-Lucas pseudoprimes is indexed as A330276 in OEIS [26], and starts with

169, 385, 961, 1105, 1121, 3827, 4901, 6265, 6441, 6601, 7107, 7801, 8119, 10945, 11285, 13067, 15841, 18241,

19097, 20833, 24727, 27971, 29953, 31417, 34561, 35459, 37345, 37505, 38081, 39059, 42127, 45451, ...

We have conjectured in [5] that this sequence is infinite.

Other classes of pseudoprimes have been defined by combining multiple properties.

3.2.5. Pseudoprimality defined by two properties

A composite number n is called a **Fibonacci-Bruckner-Lucas pseudoprime** if it satisfies the properties $n \mid F_{n-\left(\frac{p}{5}\right)}$ and $n \mid L_n - 1$. These numbers produce the sequence A212424, starting with

4181, 5777, 6721, 10877, 13201, 15251, 34561, 51841, 64079, 64681, ...

Bruckman showed in [12] that Fibonacci-Bruckner-Lucas pseudoprimes are infinitely many. These correspond to Frobenius pseudoprimes for the polynomial $x^2 - x - 1$ (see, e.g., [14], [29]).

An odd composite integer n is called a **Pell-Pell-Lucas pseudoprime** if it satisfies simultaneously $n \mid P_{n-(-1)^{\frac{n^2-1}{8}}}$ and $n \mid Q_n - 2$. The list of such pseudoprimes is

$$169, 385, 961, 1121, 3827, 6265, 6441, 6601, 7801, 8119, 10945, 13067, 15841,$$
$$18241, 19097, 20833, 24727, 27971, 29953, 31417, 34561, 35459, 37345, \ldots,$$

recently indexed in the OEIS as A327652. We have conjectured in [5] that this sequence is infinite.

3.3. Pseudoprimes defined by general recurrences and primality testing

Many notions of pseudoprimality are linked to the generalized Lucas sequences $\{U_n(a,b)\}_{n\geq 0}$ and $\{V_n(a,b)\}_{n\geq 0}$ given by (1) and (2), based on the identities (6), (7), (8) and (9). Details and various pseudoprimality tests for generalised Lucas sequences are given in [10] and [11].

Definition 3.4. *A composite integer n is called **Lucas pseudoprime** of parameters a and b if* $\gcd(n,b) = 1$ *and n divides $U_{n-\left(\frac{D}{n}\right)}$.*

Clearly, under the current assumptions that $b = \pm 1$, the condition $\gcd(n,b) = 1$ is superfluous. A primality test involving generalised Lucas sequences is given below.

Theorem 3.5 (Lucas test). *If n does not divide $U_{n-\left(\frac{D}{n}\right)}$, then n is composite.*

The particular version of this results when $\left(\frac{D}{n}\right) = -1$ is stated as Theorems 5-2 and 5-3 in [24].

An interesting divisibility result linking the sequences U_n and V_n was stated in [10, Section 2].

Proposition 3.6. *If n is an odd composite number such that* $\gcd(n, 2abD) = 1$*, then any two of the following statements imply the other two.*

1) $U_n \equiv \left(\frac{D}{n}\right) \pmod{n}$;
2) $V_n \equiv V_1 = a \pmod{n}$;
3) $U_{n-\left(\frac{D}{n}\right)} \equiv U_0 = 0 \pmod{n}$;
4) $V_{n-\left(\frac{D}{n}\right)} \equiv 2b^{\frac{1-\left(\frac{D}{n}\right)}{2}} \pmod{n}$ *(valid whenever* $\gcd(n, D) = 1$*).*

The following concepts of weak pseudoprimality have been introduced in our paper [7], where we have also provided more than 40 integer sequences added by us to OEIS. A composite integer n is said to be a

1. *generalized Bruckman-Lucas pseudoprime* of parameters a and b if $n \mid V_n(a,b) - a$.

2. *weak generalized Lucas pseudoprime* of parameters a and b if $n \mid U_n^2 - 1$. In particular, when $b = -1$ and $a = 1$ one obtains the weak Fibonacci pseudoprimes for which $n \mid F_n^2 - 1$. We have indexed the odd numbers with this property as A337231, and the even ones as A337232. For $a = 2$ the weak Pell pseudoprimes satisfy $n \mid P_n^2 - 1$, which we have added to [26] as A337233.
3. *weak generalized Lucas-Bruckner pseudoprime* of parameters a and b if $n \mid U_n^2 - 1$ and $n \mid V_n - a$.

Notice that these definitions do not require the Jacobi symbol. For $b = \pm 1$ and $(a, b) \neq (1, 1)$, using results from [28], we have shown that there are infinitely many weak generalized Lucas-Bruckner pseudoprimes. The numerical simulations in [7] were performed for $b = -1$ with $a = 1, \ldots, 7$, and $b = 1$ with $a = 3, \ldots, 7$.

Other types of Lucas and Frobenius pseudoprimes are listed by Rotkiewics [29], together with detailed historical information. Grantham unified numerous pseudoprimality concepts under the name of Frobenius pseudoprimes [16], and showed that the Perrin pseudoprimes (defined by third-order sequence given by $A_{n+3} = A_{n+1} + A_n$, where $A_0 = 3$, $A_1 = 0$ and $A_2 = 2$) are infinitely many [17].

4. Main results

In this section we use Theorems 2.2 and 2.3 to derive results for the divisibility of certain expressions modulo a composite number. This research is inspired by the Fibonacci pseudoprimes of level k introduced in [9], whose set is denoted by $\mathcal{F}_k$.

Proposition 4.1 (Proposition 1, [9]). *Let $n \in \mathbb{N}$ be coprime with 10. Then $n \in \mathcal{F}_k$ for all $k \geq 1$ if and only if $n \in \mathcal{F}_1$ and $n \mid F_n^2 - 1$. In particular, if $n \mid F_{n-\left(\frac{n}{5}\right)}$ and $n | F_n - \left(\frac{n}{5}\right)$, then $n \in \mathcal{F}_k$ for all $k \geq 1$.*

Notice that the conditions in the particular case are given by equations (10) and (11). The authors first show that under the hypotheses above, one has $n \in \mathcal{F}_2$. The proof is based on Catalan's identity, which states for all integers $m \geq r \geq 0$, the relation $F_m^2 - F_{m+r}F_{m-r} = (-1)^{m-r}F_r^2$ holds.

Catalan's identity is then used to also show that

$$\begin{aligned} F_{(k+1)n-\left(\frac{n}{5}\right)}F_{k-2} &\equiv F_{k-1}^2 + (-1)^k \pmod{n} \\ F_kF_{k-2} &\equiv F_{k-1}^2 + (-1)^k \pmod{n}, \end{aligned}$$

from where the authors incorrectly deduce that $n \mid F_{(k+1)n-\left(\frac{n}{5}\right)} - F_k$. In fact, one only has

$$\left[F_{(k+1)n-\left(\frac{n}{5}\right)} - F_k\right] F_{k-2} \equiv 0 \pmod{n}.$$

The deduction holds when n is coprime with F_{k-2}, but cannot be guaranteed in general.

We present a numerical counterexample involving large Fibonacci numbers, which gives an integer n which satisfies the hypotheses, but is not in $\mathcal{F}_3$. This contradicts the statement in [9, Proposition 1].

Remark 4.2. *The first composite number n for which $n \mid F_{n-\left(\frac{n}{5}\right)}$ and $n \mid F_n^2 - 1$ is $n = 323$. One can check that $n \mid F_{2n-\left(\frac{n}{5}\right)} - F_1$ but also that $F_{3n-\left(\frac{n}{5}\right)} - F_2 \equiv 321 \pmod{n}$, where $\left(\frac{n}{5}\right) = -1$. The numerical calculations involving large numbers below are implemented with the* vpi *(variable precision integer) library in Matlab.*

$$F_{n-\left(\frac{n}{5}\right)} = 2304148358552416826222090648964201807510161746678049679057369028996 8 \equiv 0 \pmod{n}$$

$$F_{2n-\left(\frac{n}{5}\right)} = 7336995277999309135280786247013754464564049243092710404349906900145 8$$

$$4668246528603476477043108568806527592562210693671820824200536283473 \equiv 1 = F_1 \pmod{n}$$

$$F_{3n-\left(\frac{n}{5}\right)} = 2336286181815299653746750781129919541766943951168971092522786214227 5$$

$$5237533996389677833107817045296765338979711721919480043169346318420450 65$$

$$7716380889475584245156876241901131223573192092275600598593453 35 \equiv 322 \pmod{n}.$$

Out of curiosity, we give the factorizations of these numbers, which share many divisors

$F_{324} = 2^4 \cdot 3^5 \cdot 17 \cdot 19 \cdot 53 \cdot 107 \cdot 109 \cdot 2269 \cdot 3079 \cdot 4373 \cdot 5779 \cdot 19441 \cdot$

$864769886865217995872266489383518 1229$

$F_{647} - 1 = 2^4 \cdot 3^5 \cdot 17 \cdot 19 \cdot 53 \cdot 107 \cdot 109 \cdot 2269 \cdot 3079 \cdot 3571 \cdot 4373 \cdot 5779 \cdot 9349 \cdot 19441 \cdot$

$82480891977832786085961539583907800762919444772817440580540336052855989604886463822949768687430 29$

We now present some extensions of these results for generalised Lucas sequences.

4.1. Results for $b = -1$

Let D and p be prime numbers which satisfy the identity

$$\left(\frac{D}{p}\right)\left(\frac{p}{D}\right) = 1. \tag{14}$$

We shortly denote $U_n = U_n(a, -1)$ and $V_n = V_n(a, -1)$. Since $\left(\frac{D}{p}\right) = \left(\frac{p}{D}\right)$, by Theorem 2.2 we get

1) $U_{kp-\left(\frac{p}{D}\right)} \equiv U_{k-1} \pmod{p}$;
2) $V_{kp-\left(\frac{p}{D}\right)} \equiv \left(\frac{p}{D}\right) V_{k-1} \pmod{p}$.

Similarly to Theorem 3.5, these properties can be used to formulate new primality tests. For a positive integer k, if n does not divide $U_{kn-\left(\frac{n}{D}\right)} - U_{k-1}$, or $V_{kn-\left(\frac{n}{D}\right)} - \left(\frac{n}{D}\right) V_{k-1}$ respectively, then n is composite.

We shall now investigate some identities modulo a composite number. Since we are using the Jacobi symbol, $D = a^2 + 4$ and a must be odd. Recall the following notions introduced in [6, Definition 3].

Let a, k and n be non-negative integers with n odd. The composite number n is called a

1. **generalised Lucas pseudoprime of level k^- and parameter a** if

$$n \mid U_{kn-\left(\frac{n}{D}\right)} - U_{k-1}.$$

The set of all such numbers is denoted by $\mathcal{U}_k^-(a)$.

2. **generalised Pell-Lucas pseudoprime of level k^- and parameter a** if it satisfies the property

$$n \mid V_{kn-\left(\frac{n}{D}\right)} - \left(\frac{n}{D}\right) V_{k-1}.$$

The set of all such numbers is denoted by $\mathcal{V}_k^-(a)$.

Numerous novel integer sequences have been obtained from $\mathcal{U}_k^-(a)$ and $\mathcal{V}_k^-(a)$ in [6], where the computations have been performed for $b=-1$ with $a=1,3,5,7$ and for the levels $k=1,2,3$.

The following result links the sets $\mathcal{U}_1^-(a)$ and $\mathcal{U}_2^-(a)$ to the weak generalized Lucas pseudoprimes.

Theorem 4.3. *Let $a, n>0$ be odd integers such that $\gcd(D,n)=1$ and consider the statements*

1) $n \in \mathcal{U}_1^-(a)$;

2) $n \in \mathcal{U}_2^-(a)$;

3) $n \mid U_n^2 - 1$.

The following implications are true.

(i) If 1) and 2) are verified, then 3) holds;

(ii) If 1) and 3) are verified, then 2) holds.

Proof. Replacing $b=-1$ in (5) and Lemma 2.4 1), for all integers m and r we have

$$U_m^2 - U_{m-r}U_{m+r} = (-1)^{m-r}U_r^2, \quad U_{-m} = -(-1)^m U_m.$$

Applying this identity for $m = n - \left(\frac{n}{D}\right)$ and $r=n$, one obtains

$$U_{n-\left(\frac{n}{D}\right)}^2 - U_{2n-\left(\frac{n}{D}\right)}U_{-\left(\frac{n}{D}\right)} = (-1)^{-\left(\frac{n}{D}\right)}U_n^2.$$

Since n and D are relatively prime, we have $U_{-\left(\frac{n}{D}\right)} = -(-1)^{-\left(\frac{n}{D}\right)}U_{\left(\frac{n}{D}\right)}$, while from $\left(\frac{n}{D}\right) = \pm 1$, it follows that $(-1)^{-\left(\frac{n}{D}\right)} = -1$. We deduce that

$$U_{n-\left(\frac{n}{D}\right)}^2 - \left(U_{2n-\left(\frac{n}{D}\right)} - 1\right) = -\left(U_n^2 - 1\right). \tag{15}$$

We now take the results modulo n and use that $U_0=0$ and $U_1=1$. Clearly, $n \in \mathcal{U}_1^-(a)$ is equivalent to $U_{n-\left(\frac{n}{D}\right)} \equiv 0 \pmod{n}$, while $n \in \mathcal{U}_2^-(a)$ is equivalent to $U_{2n-\left(\frac{n}{D}\right)} \equiv 1 \pmod{n}$.

(*i*) If 1) and 2) hold, then the left hand-side of (15) vanishes modulo n, hence $n \mid U_n^2 - 1$, i.e., 3) holds.

(*ii*) If 1) and 3) hold, then the middle bracket of (15) vanishes modulo n, hence 2) holds. □

Remark 4.4. *(i) If the assertions 2) and 3) in Theorem 4.3 hold, then taking the relation (15) modulo n we deduce that $U_{n-\left(\frac{n}{D}\right)}^2 \equiv 0$. However, this does do not imply 1), i.e, $U_{n-\left(\frac{n}{D}\right)} \equiv 0$. A counterexample is given by the bronze Fibonacci numbers $U_n = U_n(3,-1)$, where $D=13$. It can be checked numerically that*

for $n=9$ we have $U_n=12970$, $\left(\frac{n}{13}\right)=1$, $n \mid U_{2n-\left(\frac{n}{13}\right)}-U_1$ and $n \mid U_n^2-1$, but $U_{n-\left(\frac{n}{13}\right)} \equiv 3 \neq 0 \pmod{n}$. The calculations below were implemented with the vpi *(variable precision integer) library in Matlab.*

$$\begin{aligned} U_{n-\left(\frac{n}{13}\right)} &= 3927 \equiv 3 \pmod{n} \\ U_{2n-\left(\frac{n}{13}\right)} &= 183642229 \equiv 1 \pmod{n} \\ U_n^2-1 &= 168220899 \equiv 0 \pmod{n}. \end{aligned}$$

The odd composite integers $n \mid U_n^2-1$ for $b=-1$ and $a=3$, have been indexed as A337234 in OEIS by us. The even such numbers have been indexed also by us as A337235.

(ii) If $n \in \mathcal{U}_1^-(a)$ and $n \mid U_n^2-1$, by this theorem it follows that $n \in \mathcal{U}_2^-(a)$. However, in general, one does not have $n \in \mathcal{U}_3^-(a)$. A counterexample for Fibonacci numbers was given in Remark 4.2.

Conjecture 1. For all positive integers a there are counterexamples such as in Remark 4.4.

Remark 4.5. *The condition* (15) *gives an identity valid for the a-Fibonacci numbers $U_n=U_n(a,-1)$*

$$U_{2n-\left(\frac{n}{D}\right)} = U_{n-\left(\frac{n}{D}\right)}^2 + U_n^2.$$

In fact, a more general relation holds, that is

$$U_{2n-\varepsilon} = U_{n-\varepsilon}^2 + U_n^2, \quad \varepsilon \in \{-1,1\}. \tag{16}$$

In particular, writing the condition (16) *for $(a,b)=(1,-1)$ and $(a,b)=(2,-1)$ and $\varepsilon=\pm 1$, we obtain*

$$\begin{aligned} F_{2n-\varepsilon} &= F_{n-\varepsilon}^2 + F_n^2 \\ P_{2n-\varepsilon} &= P_{n-\varepsilon}^2 + P_n^2. \end{aligned}$$

The Two Squares Theorem [19, Theorem 366] states that a positive integer N is the sum of two squares if and only if each prime factor p of N such that $p \equiv 3 \pmod 4$ occurs to an even power in the prime factorization of N. Combined with Remark 4.5, we deduce that for any integer m, a prime factor p of U_{2m+1} which is congruent with $3 \pmod 4$, may only appear with an even exponent.

The following result links the sets $\mathcal{V}_1^-(a)$ and $\mathcal{V}_2^-(a)$ to the weak generalized Lucas pseudoprimes.

Theorem 4.6. *Let $a,n>0$ be a odd integers such that $\gcd(n,aD)=1$. Consider the following statements.*

1) $n \in \mathcal{V}_1^-(a)$;
2) $n \in \mathcal{V}_2^-(a)$;
3) $n \mid U_n^2-1$.

Then the following implications are true.

(*i*) *If* 1) *and* 2) *are verified, then* 3) *holds;*

(*ii*) *If* 1) *and* 3) *are verified, then* 2) *holds.*

Proof. Using $b=-1$ in (5) and Lemma 2.4 2), for any integers m and r we have

$$V_m^2 - V_{m+r}V_{m-r} = -D(-1)^{m-r}U_r^2, \quad V_{-m} = (-1)^m V_m.$$

Using this identity for $m = n - \left(\frac{n}{D}\right)$ and $r = n$, one obtains

$$V_{n-\left(\frac{n}{D}\right)}^2 - V_{2n-\left(\frac{n}{D}\right)}V_{-\left(\frac{n}{D}\right)} = -D(-1)^{-\left(\frac{n}{D}\right)}U_n^2.$$

Since n and D are relatively prime, we have $V_{-\left(\frac{n}{D}\right)} = (-1)^{-\left(\frac{n}{D}\right)}V_{\left(\frac{n}{D}\right)}$ and $V_{\left(\frac{n}{D}\right)} = a\left(\frac{n}{D}\right)$, while from $\left(\frac{n}{D}\right) = \pm 1$, it follows that $(-1)^{-\left(\frac{n}{D}\right)} = -1$. We can now deduce that

$$V_{n-\left(\frac{n}{D}\right)}^2 + a\left(\frac{n}{D}\right)V_{2n-\left(\frac{n}{D}\right)} = DU_n^2. \tag{17}$$

Since $D = a^2+4$, this identity can be further written as

$$\left(V_{n-\left(\frac{n}{D}\right)}^2 - 4\right) + a\left(\frac{n}{D}\right)\left(V_{2n-\left(\frac{n}{D}\right)} - a\left(\frac{n}{D}\right)\right) = D\left(U_n^2 - 1\right). \tag{18}$$

Clearly $n \in \mathcal{V}_1^-(a)$ means $V_{n-\left(\frac{n}{D}\right)} \equiv 2\left(\frac{n}{D}\right) \pmod n$, while $n \in \mathcal{V}_2^-(a)$ means $V_{2n-\left(\frac{n}{D}\right)} \equiv a\left(\frac{n}{D}\right) \pmod n$. Notice that if two of the brackets in relation (18) vanish, then the third vanishes as well.

(*i*) If 1) and 2) hold, then the left hand-side of (18) vanishes modulo n, hence $n \mid U_n^2 - 1$, i.e., 3) holds.

(*ii*) If 1) and 3) hold, then the middle bracket of (18) vanishes modulo n, hence 2) holds. □

Remark 4.7. *If the assertions* 2) *and* 3) *in Theorem 4.6 hold, then taking the relation* (18) *modulo n we deduce that* $V_{n-\left(\frac{n}{D}\right)}^2 - 4$. *However, this does do not imply* 1), *i.e,* $V_{n-\left(\frac{n}{D}\right)} \equiv 2\left(\frac{n}{D}\right)$. *A counterexample is given by Lucas sequence. From Remark 4.3, we know that for* $n = 323$ *we have* $n \mid F_n^2 - 1$. *One can check that* $n \mid L_{2n-\left(\frac{n}{5}\right)} - \left(\frac{n}{5}\right)L_1$, *but* $L_{n-\left(\frac{n}{5}\right)} \equiv 2 \neq 2\left(\frac{n}{5}\right) \pmod n$, *where* $\left(\frac{n}{5}\right) = -1$. *The calculations below were implemented with the* vpi *(variable precision integer) library in Matlab.*

$$L_{n-\left(\frac{n}{5}\right)} = 515223235996776294967379903295286389565835483043780536155810435356 82 \equiv 2 \pmod n$$

$$L_{2n-\left(\frac{n}{5}\right)} - \left(\frac{n}{5}\right)L_1 = 164060201922014224280717425066245025764781124891271838619807402041846262156924015992064406990410128506570256616706671043831467653299288 0 \equiv 0 \pmod n.$$

For illustrative purposes we present the factorizations of these numbers

$L_{324} = 2 \cdot 7 \cdot 23 \cdot 647 \cdot 6263 \cdot 103681 \cdot 380849771727852696238048983043797803947188436064312641$

$L_{324} + 2 = 2^2 \cdot 3^{10} \cdot 107^2 \cdot 1380313302869110147637320280892$

$L_{647} + 1 = 2^4 \cdot 3^5 \cdot 5^1 \cdot 17 \cdot 19 \cdot 37 \cdot 53 \cdot 107 \cdot 109 \cdot 113 \cdot 1597 \cdot 2269 \cdot 3079 \cdot 4373 \cdot 5779 \cdot 19441 \cdot$

$184432848160992652721725076951938254420106936369020829042604619568405641706724988100330796739038 29$

Conjecture 2. We claim that for all positive integers a there are counterexamples such as in Remark 4.7.

Remark 4.8. *(i) From the relation* (17) *we can deduce that the general Pell equation*

$$x^2 - Dy^2 = -a\left(\frac{n}{D}\right) V_{2n-\left(\frac{n}{D}\right)}$$

has solutions for all integers n.

(ii) In fact, relation (17) *suggests the more general relation*

$$V_{n-\varepsilon}^2 + \varepsilon \cdot aV_{2n-\varepsilon} = DU_n^2, \quad \varepsilon \in \{-1, 1\}. \tag{19}$$

In particular, when $(a, b) = (1, -1)$ *and* $(a, b) = (2, -1)$, *from* (19) *we obtain the following relations valid for* $\varepsilon \in \{-1, 1\}$, *which connect the Fibonacci, Lucas, Pell and Pell-Lucas numbers*

$$\varepsilon \cdot L_{2n-\varepsilon} = 5F_n^2 - L_{n-\varepsilon}^2;$$
$$\varepsilon \cdot 2Q_{2n-\varepsilon} = 8P_n^2 - Q_{n-\varepsilon}^2.$$

4.2. Results for $b = 1$

Assume that $b = 1$ and the primes p and D satisfy (14). Denoting $U_n = U_n(a, 1)$ and $V_n = V_n(a, 1)$, Theorem 2.3 can be rewritten as

1) $U_{kp-\left(\frac{p}{D}\right)} \equiv \left(\frac{p}{D}\right) U_{k-1} \pmod{p}$;
2) $V_{kp-\left(\frac{p}{D}\right)} \equiv V_{k-1} \pmod{p}$.

Similarly to Theorem 3.5, properties 1) and 2) can be used to get new primality tests. For a positive integer k, if n does not divide $U_{kn-\left(\frac{n}{D}\right)} - \left(\frac{n}{D}\right) U_{k-1}$, or $V_{kn-\left(\frac{n}{D}\right)} - V_{k-1}$ respectively, then n is composite.

We now investigate similar properties for the composite numbers. By (5), we have $U_{-1} = -U_1 = -1$ and $V_{-1} = V_1 = a$. Since we are using the Jacobi symbol, both $D = a^2 - 4$ and a must be odd.

Recall the following notions introduced in [6, Definition 4].

Let a, k and n be non-negative integers such that a is odd. A composite number n is a

1. **generalised Lucas pseudoprime of level** k^+ **and parameter** a if

$$n \mid U_{kn-\left(\frac{n}{D}\right)} - \left(\frac{n}{D}\right) U_{k-1}.$$

The set of all such numbers is denoted by $\mathcal{U}_k^+(a)$.

2. **generalised Pell-Lucas pseudoprime of level** k^+ **and parameter** a if it satisfies the property

$$n \mid V_{kn-\left(\frac{n}{D}\right)} - V_{k-1}.$$

The set of all such numbers is denoted by $\mathcal{V}_k^+(a)$.

Numerous novel integer sequences have been obtained from $\mathcal{U}_k^+(a)$ and $\mathcal{V}_k^+(a)$ in [6], where the computations have been performed for $b = -1$ with $a = 3, 5, 7$ and for the levels $k = 1, 2, 3$.

The following result links the sets $\mathcal{U}_1^+(a)$ and $\mathcal{U}_2^+(a)$.

Theorem 4.9. *Let $a, n > 0$ be odd integers such that $\gcd(n, D) = 1$. Consider the following statements*

1) $n \in \mathcal{U}_1^+(a)$;

2) $n \in \mathcal{U}_2^+(a)$;

3) $n \mid U_n^2 - 1$.

Then the implications below are true.

(*i*) *If* 1) *and* 2) *are verified, then* 3) *holds;*

(*ii*) *If* 1) *and* 3) *are verified, then* 2) *holds.*

Proof. Applying Lemma 2 part 1) for $b = 1$ one obtains

$$U_m^2 - U_{m+r}U_{m-r} = U_r^2,$$

hence for $m = n - \left(\frac{n}{D}\right)$ and $r = n$ we get

$$U_{n-\left(\frac{n}{D}\right)}^2 - U_{2n-\left(\frac{n}{D}\right)}U_{-\left(\frac{n}{D}\right)} = U_n^2.$$

We can easily check that for $b = 1$ we have $U_{-\left(\frac{n}{D}\right)} = -U_{\left(\frac{n}{D}\right)} = -\left(\frac{n}{D}\right)$, therefore

$$U_{n-\left(\frac{n}{D}\right)}^2 + U_{2n-\left(\frac{n}{D}\right)}\left(\frac{n}{D}\right) = U_n^2. \tag{20}$$

We now take the results modulo n and use that $U_0 = 0$ and $U_1 = 1$. Clearly, $n \in \mathcal{U}_1^+(a)$ is equivalent to $U_{n-\left(\frac{n}{D}\right)} \equiv 0 \pmod{n}$, while $n \in \mathcal{U}_2^+(a)$ is equivalent to $U_{2n-\left(\frac{n}{D}\right)} \equiv \left(\frac{n}{D}\right) \pmod{n}$.

(*i*) If 1) and 2) hold, then the left hand-side of (20) vanishes modulo n, hence $n \mid U_n^2 - 1$, i.e., 3) holds.

(*ii*) If 1) and 3) hold, then the middle bracket of (20) vanishes modulo n, hence 2) holds. □

Remark 4.10. *If the assertions* 2) *and* 3) *in Theorem 4.9 hold, then taking the relation* (20) *modulo n we deduce that $U_{n-\left(\frac{n}{D}\right)}^2 \equiv 0$. However, this does do not imply* 1)*, i.e, $U_{n-\left(\frac{n}{D}\right)} \equiv 0$. A counterexample is given by the bisection of Fibonacci numbers $U_n = U_n(3, 1)$, where $D = 5$. One can check that for $n = 9$ we have $U_n = 2584$, $n \mid U_{2n-\left(\frac{n}{5}\right)} - U_1$ and $n \mid U_n^2 - 1$, but $U_{n-\left(\frac{n}{5}\right)} \equiv 6 \neq 0 \pmod{n}$, where $\left(\frac{n}{5}\right) = 1$. The calculations below were implemented with the* vpi *(variable precision integer) library in Matlab.*

$$\begin{aligned} U_{n-\left(\frac{n}{5}\right)} &= 987 \equiv 6 \pmod{n} \\ U_{2n-\left(\frac{n}{5}\right)} - U_1 &= 5702886 \equiv 0 \pmod{n} \\ U_n^2 - 1 &= 6677055 \equiv 0 \pmod{n}. \end{aligned}$$

For $b = 1$ and $a = 3$, we have indexed the odd composite integers with $n \mid U_n^2 - 1$ as A338007 in OEIS, while the even ones have been indexed also by us as A337782.

Conjecture 3. We claim that for all positive integers a there are counterexamples such as in Remark 4.10.

Remark 4.11. *From* (20), *the numbers* $U_n = U_n(a,1)$ *satisfy the identity*

$$\left(\frac{n}{D}\right) U_{2n-\left(\frac{n}{D}\right)} = U_n^2 - U_{n-\left(\frac{n}{D}\right)}^2.$$

In fact, the more general relation can be checked

$$\varepsilon U_{2n-\varepsilon} = U_n^2 - U_{n-\varepsilon}^2, \quad \varepsilon \in \{-1,1\}. \tag{21}$$

In the particular case $(a,b) = (3,1)$ *we have* $D = 5$ *and* $U_n = F_{2n}$, *this gives the identity*

$$\varepsilon F_{4n-2\varepsilon} = F_{2n}^2 - F_{2n-2\varepsilon}^2, \quad \varepsilon \in \{-1,1\}.$$

We now present a result linking $\mathcal{V}_1^+(a)$ and $\mathcal{V}_2^+(a)$ to the weak generalized Lucas pseudoprimes.

Theorem 4.12. *Let* $a, n > 0$ *be a odd integers such that* $\gcd(n, aD) = 1$. *Consider the following statements.*

1) $n \in \mathcal{V}_1^+(a)$;

2) $n \in \mathcal{V}_2^+(a)$;

3) $n \mid U_n^2 - 1$.

Then the following implications are true.

(*i*) *If* 1) *and* 2) *hold, then* 3) *holds;*

(*ii*) *If* 1) *and* 3) *hold, then* 2) *holds.*

Proof. Similarly to Theorem 4.6, by Lemma 2 2) for the integers m and r and $b = 1$, we get

$$V_m^2 - V_{m+r}V_{m-r} = -DU_r^2.$$

Using this identity for $m = n - \left(\frac{n}{D}\right)$ and $r = n$, one obtains

$$V_{n-\left(\frac{n}{D}\right)}^2 - V_{2n-\left(\frac{n}{D}\right)}V_{-\left(\frac{n}{D}\right)} = -DU_n^2.$$

When $b = 1$ we have $V_{-\left(\frac{n}{D}\right)} = V_{\left(\frac{n}{D}\right)} = a$, hence

$$V_{n-\left(\frac{n}{D}\right)}^2 - aV_{2n-\left(\frac{n}{D}\right)} + DU_n^2 = 0. \tag{22}$$

Since $D = a^2 - 4$, this identity can be further written as

$$\left(V_{n-\left(\frac{n}{D}\right)}^2 - 4\right) - a\left(V_{2n-\left(\frac{n}{D}\right)} - a\right) + D\left(U_n^2 - 1\right) = 0. \tag{23}$$

Clearly, $n \in \mathcal{V}_1^+(a)$ is $V_{n-\left(\frac{n}{D}\right)} \equiv V_0 = 2 \pmod{n}$, while $n \in \mathcal{V}_2^+(a)$ is $V_{2n-\left(\frac{n}{D}\right)} \equiv V_1 = a \pmod{n}$. Notice that if two of the brackets in relation (23) vanish, then the third vanishes as well.

(*i*) If 1) and 2) hold, then the first two brackets of (23) vanish modulo n, hence 3) holds.

(*ii*) If 1) and 3) hold, then the middle bracket of (23) vanishes modulo n, hence 2) holds. □

Remark 4.13. *If* 2) *and* 3) *in Theorem 4.12 hold, then taking* (23) *modulo* n *we get* $V^2_{n-\left(\frac{n}{D}\right)}-4$. *However, this does do not imply* 1), *i.e,* $V_{n-\left(\frac{n}{D}\right)}\equiv 2$. *A counterexample is given by the bisection of Lucas numbers* $V_n=V_n(3,1)=L_{2n}$, *where* $D=5$. *One can check that for* $n=21$ *we get* $V_n=599074578$, $n\mid V_{2n-\left(\frac{n}{5}\right)}-V_1$ *and* $n\mid U_n^2-1$, *but* $V_{n-\left(\frac{n}{5}\right)}-V_0\equiv 6\neq 0 \pmod n$, *where* $\left(\frac{n}{5}\right)=1$. *The calculations below were implemented with the* vpi *(variable precision integer) library in Matlab.*

$$V_{n-\left(\frac{n}{5}\right)}=228826125\equiv 5\neq 2 \pmod n$$
$$V_{2n-\left(\frac{n}{5}\right)}-V_1=137083915467899400\equiv 0 \pmod n$$
$$U_n^2-1=71778070001175615\equiv 0 \pmod n.$$

We claim that for all positive integers a *there are counterexamples such as in Remark 4.13.*

Remark 4.14. *From* (22), *the numbers* $U_n=U_n(a,1)$ *and* $V_n=V_n(a,1)$ *satisfy the identity*

$$aV_{2n-\left(\frac{n}{D}\right)}=V^2_{n-\left(\frac{n}{D}\right)}+DU_n^2.$$

The more general relation can be checked

$$aV_{2n-\varepsilon}=V^2_{n-\varepsilon}+DU_n^2,\quad \varepsilon\in\{-1,1\}.$$

In particular, for $(a,b)=(3,1)$, *we have* $U_n=F_{2n}$ *and* $V_n=L_{2n}$, *and we deduce the identity*

$$3L_{4n-2\varepsilon}=L^2_{2n-2\varepsilon}+5F^2_{2n}.$$

5. Summary and future work

In this paper we established connections between the weak generalized Lucas pseudoprimes introduced by us in [7], and the generalized Lucas and Pell-Lucas pseudoprimes of levels k^- and k^+ defined in [6]. These notions are inspired by the paper [9], and by the identities proved by the authors in [5]. First, we have found a counterexample disproving a claim in [9] for Fibonacci pseudoprimes of level k (see Remark 4.2 above). In Remark 4.7 we provide a similar result for Lucas pseudoprimes of level k. Theorems 4.7, 4.6, 4.9 and 4.12 established links between the generalized Lucas and Pell-Lucas pseudoprimes of levels 1 and 2.

For the future it would be interesting to explore more properties and relations between the classes of pseudoprimes referred to in this paper (e.g., generalized Bruckman-Lucas pseudoprime, weak generalized Lucas pseudoprimes, generalized Lucas and Pell-Lucas pseudoprimes levels k^- and k^+), new integer sequences arising from these notions, as well as to investigate the general connections between the generalized Lucas and Pell-Lucas pseudoprimes of arbitrary levels k^- and k^+.

References

[1] Alford, W. R., Granville, A., Pomerance, C.: There are infinitely many Carmichael numbers. Annals of Math. **140**, 703–722 (1994)

[2] Andreescu, T., Andrica, D.: Number Theory. Structures, Examples, and Problems. Birkhauser Verlag, (2009)

[3] Andrejic, V.: On Fibonacci powers. Univ. Beograd. Publ. Elektrotehn. Fak. Ser. Mat. **17**, 38–44 (2006)

[4] Andrica, D., Bagdasar, O.: Recurrent Sequences: Key Results, Applications and Problems. Springer (2020)

[5] Andrica, D., Bagdasar, O.: On some arithmetic properties of the generalised Lucas sequences, Mediterr. J. Math. **18**, Article 47 (2021)

[6] Andrica, D., Bagdasar, O.: On generalized Lucas pseudoprimality of level k (submitted)

[7] Andrica, D., Bagdasar, O.: Weak pseudoprimality associated with the generalized Lucas sequences (submitted)

[8] Andrica, D., Bagdasar, O., and Ţurcaş, G. C.: On some new results for the generalized Lucas sequences, An. Şt. Univ. Ovidius Constanţa, **XXIX**(1), 17–36 (2021)

[9] Andrica, D., Crişan, V., Al-Thukair, F.: On Fibonacci and Lucas sequences modulo a prime and primality testing. Arab J. Math. Sci. **24**(1), 9–15 (2018)

[10] Baillie, R., Wagstaff, S. S. Jr.: Lucas Pseudoprimes. Math. Comput. **35**(152), 1391–1417 (1980)

[11] Brillhart, J., Lehmer, D. H., Selfridge, J. L.: New primality criteria and factorizations of $2^m \pm 1$. Math. Comput. **29**(130), 620–647 (1975)

[12] Bruckman, P. S.: On the infinitude of Lucas pseudoprimes. Fibonacci Quart. **32**(2), 153–154 (1994)

[13] Crandall, R., Dilcher, K., Pomerance, C.: A search for Wieferich and Wilson primes. Math. Comput. **66**(5), 433–449 (1997)

[14] Crandall, R., Pomerance, C.: Prime Numbers: A Computational Perspective. Springer, New York, Second Edition (2005)

[15] Everest, G., van der Poorten, A., Shparlinski, I., Ward, T. Recurrence Sequences. Mathematical Surveys and Monographs **104**, American Mathematical Society, Providence, U.S.A. (2003)

[16] Grantham, J.: Frobenius pseudoprimes. Math. Comput. **70**(234), 873–891 (2000)

[17] Grantham, J.: There are infinitely many Perrin pseudoprimes. J Number Theory **130**, 1117–1128 (2010)

[18] Halton, J.: Some properties associated with square Fibonacci numbers. Fibonacci Quart. **5**(4), 347–354 (1967)

[19] Hardy, G. H., Wright, E. M.: An Introduction to the Theory of Numbers. Oxford University Press, London (1954)

[20] Jaroma, J. H.: Note on the Lucas–Lehmer Test. Irish Math. Soc. Bulletin. **54**, 63–72 (2004)

[21] Kiss, P., Phong, B. M., Lieuwens, E.: On Lucas Pseudoprimes Which Are Products of s Primes. In: Fibonacci Numbers and Their Applications **1**, 131–139. Ed. Philippou, A. N., Bergum, G. E., Horadam, A. F., Dordrecht: Reidel (1986)

[22] Koshy, T.: Fibonacci and Lucas Numbers with Applications. John Wiley & Sons, Inc., Hoboken, NJ, USA (2001)

[23] Lehmer, E.: On the infinitude of Fibonacci pseudoprimes. Fibonacci Quart. **2**(3), 229–230 (1964)

[24] McGregor-Dorsey, Z. S.: Methods of Primality Testing., MIT Undergraduate of Mathematics, **1**, 133–142 (1999)

[25] McIntosh, R. J., Roettger, E. L.: A search for Fibonacci-Wieferich and Wolstenholme primes. Math. Comput. **76**(260), 2087–2094 (2007)

[26] The On-Line Encyclopedia of Integer Sequences, http://oeis.org, OEIS Foundation Inc. (2011)

[27] Ribenboim, P.: The Little Book of Bigger Primes. Springer-Verlag New York, Second Edition (2004)

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

[29] Rotkiewicz, A.: Lucas and Frobenius pseudoprimes. Ann. Math. Sil. **17**, 17–39 (2003)

[30] Schuster, S., Fitchner, M., Sasso, S.: Use of Fibonacci numbers in lipidomics - Enumerating various classes of fatty acids. Nature Sci. Rep. **7**, 39821 (2017)

[31] Williams, H. C.: Edouard Lucas and Primality Testing. Wiley-Blackwell (2011)