On some new arithmetic properties of the generalized Lucas sequences

Dorin Andrica and Ovidiu Bagdasar

Abstract. Some arithmetic properties of the generalized Lucas sequences are studied, extending a number of recent results obtained for Fibonacci, Lucas, Pell, and Pell-Lucas sequences. These properties are then applied to investigate certain notions of Fibonacci, Lucas, Pell, and Pell-Lucas pseudoprimality, for which we formulate some conjectures.

Mathematics Subject Classification (2010). 11A51, 11B39, 11B50.

Keywords. generalized Lucas sequences, Pell sequence, Pell-Lucas sequence, Legendre symbol, pseudoprimality.

1. Introduction

The Fibonacci, Lucas, Pell, or Pell-Lucas sequences are classical examples of second-order recurrences. Being the subject of intensive research for centuries, many new properties and applications of these sequences are still discovered.

The Fibonacci numbers are the terms of the sequence $(F_n)_{n\geq 0}$ given by

$$F_0 = 0,\ F_1 = 1, \quad F_{n+2} = F_{n+1} + F_n.$$

Fibonacci numbers are linked to data structures [16], search algorithms [21], various optimality problems [23], [24], or optimal geometric patterns [27].

The Lucas numbers are the terms of the sequence $(L_n)_{n\geq 0}$ defined by

$$L_0 = 2,\ L_1 = 1, \quad L_{n+2} = L_{n+1} + L_n.$$

The Pell numbers are the terms of the sequence $(P_n)_{n\geq 0}$ defined by

$$P_0 = 0,\ P_1 = 1, \quad P_{n+2} = 2P_{n+1} + P_n,$$

being linked to approximations of $\sqrt{2}$ by rationals and Diophantine equations.

The Pell-Lucas numbers are the terms of sequence $(Q_n)_{n\geq 0}$ given by

$$Q_0 = 2,\ Q_1 = 2, \quad Q_{n+2} = 2Q_{n+1} + Q_n,$$

and are a natural companion to the Pell numbers. These sequences have also been extended and generalized for quaternions and octonions (see, e.g., [8]).

The Online Encyclopedia of Integer Sequences (OEIS) [28] has more than 350000 entries, including the Fibonacci, Lucas, Pell, and Pell-Lucas sequences indexed as A000045, A000032, A000129, and A002203, respectively.

The terms of these sequences can be obtained directly by the so-called "Binet formulae". Besides the ever expanding collection of algebraic relations between these numbers, there are also numerous arithmetic properties satisfied by the terms of these sequences. Here we outline some recent results obtained for Fibonacci and Lucas numbers, obtained by Andrica *et al.* [5].

Proposition 1.1 (Lemma 1, [5]**).** *Let p be an odd prime, k a positive integer, and r an arbitrary integer. The following relations hold:*

$$2F_{kp+r} \equiv \left(\frac{p}{5}\right) F_k L_r + F_r L_k \pmod{p}, \tag{1.1}$$

$$2L_{kp+r} \equiv 5\left(\frac{p}{5}\right) F_k F_r + L_k L_r \pmod{p}, \tag{1.2}$$

where $\left(\frac{p}{5}\right)$ is the Legendre's symbol.

Particular instances of these formulae recover some well-known results and help to derive new properties of the generalized Lucas sequences.

The classical relations (3.7) and (3.8) are shown in [5], to be just the first in a sequence of divisibility relations, as illustrated by the following result.

Proposition 1.2 (Theorem 1, [5]**).** *If p is an odd prime and k a positive integer, then the following identities hold:*

1. $F_{kp-\left(\frac{p}{5}\right)} \equiv F_{k-1} \pmod{p}$;
2. $L_{kp-\left(\frac{p}{5}\right)} \equiv \left(\frac{p}{5}\right) L_{k-1}$ (mod p).

Proposition 1.3 (Remark 2, [5]**).** *For every odd prime p, there exists a progression $a_0, a_1, \ldots$ with ratio p, such that*

1. $(F_{a_0}, F_{a_1}, F_{a_2}, ...) \equiv (F_0, F_1, F_2, ...) \pmod{p}$;
2. $(L_{a_0}, L_{a_1}, L_{a_2}, ...) \equiv \left(\frac{5}{p}\right)(L_0, L_1, L_2, ...) \pmod{p}$.

In the present paper we study properties of generalized Lucas sequences and generalized Pell-Lucas sequences reduced modulo a prime. We extend recent results obtained for Fibonacci and Lucas sequences, while other results obtained for Pell and Pell-Lucas numbers are recovered as a particular case.

The structure of this paper is as follows. In Section 2 we present some preliminary results for the sequences $\{U_n(a,b)\}_{n\in\mathbb{Z}}$ and $\{V_n(a,b)\}_{n\in\mathbb{Z}}$, highlighting important particular cases like k-Fibonacci and k-Lucas sequences, investigated in many papers, including [6], [9], [10], and [29]. The main results presented in Section 3 include extensions of Propositions 1.1, 1.2 and 1.3, and other results in [5], to the cases when a is an arbitrary integer and $b = \pm 1$. Then, in Section 4 we apply the main results to derive new properties of the Pell and Pell-Lucas sequences. Finally, we present some results concerning the pseudoprimality of Pell and Pell-Lucas sequences, completing the results formulated in [5] for Fibonacci and Lucas numbers.

2. Preliminary results

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

$$U_{n+2} = aU_{n+1} - bU_n, \quad U_0 = 0,\, U_1 = 1, \quad n = 0,1,\ldots \tag{2.1}$$

$$V_{n+2} = aV_{n+1} - bV_n, \quad V_0 = 2,\, V_1 = a, \quad n = 0,1,\ldots \tag{2.2}$$

where a and b are arbitrary integers. The standard method to study these sequences involves the roots of the characteristic equation

$$z^2 - az + b = 0. \tag{2.3}$$

For $D = a^2 - 4b \neq 0$, the distinct roots of (2.3) are given by

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

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

Using these notations, the following Binet formulae are obtained

$$U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} = \frac{1}{\sqrt{D}}\left(\alpha^n - \beta^n\right), \quad n = 0,1,\ldots \tag{2.4}$$

$$V_n = \alpha^n + \beta^n, \quad n = 0,1,\ldots. \tag{2.5}$$

These formulae extend naturally to negative indices. For example, one has

$$U_{-1} = \frac{1}{\sqrt{D}}\left(\alpha^{-1} - \beta^{-1}\right) = -\frac{1}{b}, \quad V_{-1} = \alpha^{-1} + \beta^{-1} = \frac{a}{b}, \tag{2.6}$$

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

$$U_{-n} = \frac{1}{\sqrt{D}}\left(\alpha^{-n} - \beta^{-n}\right) = -\frac{1}{b^n}U_n, \quad V_{-n} = \alpha^{-n} + \beta^{-n} = \frac{1}{b^n}V_n. \tag{2.7}$$

Note that the Fibonacci and Lucas numbers are obtained as $F_n = U_n(1,-1)$, $L_n = V_n(1,-1)$ with $D = 5$, while the Pell and Pell-Lucas numbers are generated by $P_n = U_n(2,-1)$ and $Q_n = V_n(2,-1)$, with $D = 8$.

When $b = -1$, sequences $U_n(a,b)$ and $V_n(a,b)$ present special interest. Indeed, for any positive real number k, the *k-Fibonacci numbers* and *k-Lucas numbers* are recovered from the formulae

$$F_{k,n} = U_n(k,-1), \quad L_{k,n} = V_n(k,-1).$$

Properties of these sequences and some extensions are studied in [8], [13], [14], or [15]. Clearly, $F_{1,n}$ and $L_{1,n}$ represent the Fibonacci and Lucas numbers, while $F_{2,n}$ and $L_{2,n}$ are the Pell and Pell-Lucas numbers, respectively.

Denote by $\sigma_k = \frac{k+\sqrt{k^2+4}}{2}$, the positive root of the characteristic equation $z^2 - kz - 1 = 0$. The following important cases are obtained (see, e.g., [15]):

- If $k = 1$, $\sigma_1 = \frac{1+\sqrt{5}}{2}$ is the *Golden Ratio*;
- If $k = 2$, $\sigma_2 = 1 + \sqrt{2}$ is the *Silver Ratio*;
- If $k = 3$, $\sigma_3 = \frac{3+\sqrt{13}}{2}$ is the *Bronze Ratio*.

The *bronze Fibonacci numbers* denoted by $F_{3,n}$, are indexed as A006190 in OEIS, and begin with the terms

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

The sequence has been linked to lipidomics and the enumeration of fatty acids in [31], or to the Z-index (see, e.g., Hosoya [18]), used for counting special classes of graphs (caterpillar, cycle, comb, path) in chemistry.

In the particular case $b = 1$, the sequences $U_n(a, b)$ and $V_n(a, b)$ are related 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: $h_n(x) = V_n(x, 1)$.

The terms of $U_n(a, 1)$ also have an interesting combinatorial interpretation. For an integer $a \geq 3$, by Corollary 37 in [19], they represent the number of 01-avoiding words of length $n - 1$ over the alphabet $\{0, 1, 2, \dots, a - 1\}$. For $a = 3, 4, 5$, they recover the OEIS sequences A001906, A001353, and A004254.

On the other hand, the terms of $V_n(a, 1)$ have meanings related to the solutions to certain special Pell equations (see [2, Section 4.4.2]). For example, for $V_n(3, 1)$ we obtain the OEIS sequence A005248, giving the non-negative integer solutions for x to $x^2 - 5y^2 = 4$; $V_n(4, 1)$ is A003500, giving all positive values of x for which $x^2 - 3y^2 = 4$; $V_n(5, 1)$ is A003501, giving positive values of x solving $x^2 - 21y^2 = 4$. Notice that $U_n(3, 1) = F_{2n}$, and $V_n(3, 1) = L_{2n}$, called the bisection of Fibonacci, and Lucas numbers, respectively.

Derived from the generalized Lucas and Pell-Lucas sequences, we have the *Lehmer sequence* $\{U_n(\sqrt{R}, Q)\}_{n\geq 0}$, and the *companion Lehmer sequence* $\{V_n(\sqrt{R}, Q)\}_{n\geq 0}$, studied in [25], where R and Q are relatively prime integers, with $R > 0$. This extension introduced by Lehmer circumvents the limitation of $D = a^2 - 4b$, which could not be of the form $4n + 2$ or $4n + 3$. These sequences have important applications in primality testing. We present a few key formulae and notations following [20].

The roots of the characteristic equation

$$z^2 - \sqrt{R}z + Q = 0,$$

are

$$\theta = \frac{\sqrt{R} + \sqrt{\Delta}}{2}, \quad \phi = \frac{\sqrt{R} - \sqrt{\Delta}}{2},$$

where $\Delta = R - 4Q$ denotes the discriminant. The Lehmer sequence and its companion can be written explicitly as

$$U_n(\sqrt{R}, Q) = \frac{\theta^n - \phi^n}{\theta - \phi}, \quad n = 0, 1, \dots$$

$$V_n(\sqrt{R}, Q) = \theta^n + \phi^n, \quad n = 0, 1, \dots.$$

For simplicity, for a and b arbitrary integers, we denote the terms of the sequences $\{U_n(a,b)\}_{n\geq 0}$ and $\{V_n(a,b)\}_{n\geq 0}$ by U_n and V_n. In what follows we will present some algebraic identities involving the numbers U_n and V_n.

Lemma 2.1. *The following identities hold for every integer n:*

1. $aU_n - V_n = 2bU_{n-1}$;
2. $DU_n - aV_n = -2bV_{n-1}$.

Proof. The proofs follow directly from relations (2.4) and (2.5). Clearly

$$\begin{aligned} aU_n - V_n &= \frac{a}{\sqrt{D}}\left(\alpha^n - \beta^n\right) - \left(\alpha^n + \beta^n\right) \\ &= \frac{\alpha}{\sqrt{D}}\left(a - \sqrt{D}\right)\alpha^{n-1} - \frac{\beta}{\sqrt{D}}\left(a + \sqrt{D}\right)\beta^{n-1} \\ &= \frac{2b}{\sqrt{D}}\left(\alpha^{n-1} - \beta^{n-1}\right) = 2bU_{n-1}, \end{aligned}$$

where we have used the relations $a + \sqrt{D} = 2\alpha$ and $a - \sqrt{D} = 2\beta$. Similarly,

$$\begin{aligned} DU_n - aV_n &= \sqrt{D}\left(\alpha^n - \beta^n\right) - a\left(\alpha^n + \beta^n\right) \\ &= -\alpha\left(a - \sqrt{D}\right)\alpha^{n-1} - \beta\left(a + \sqrt{D}\right)\beta^{n-1} \\ &= -2b\left(\alpha^{n-1} + \beta^{n-1}\right) = -2bV_{n-1}. \end{aligned}$$

This ends the proof. □

3. Main results

From formula (2.7), one may notice that all the sequence terms $U_n(a,b)$ and $V_n(a,b)$ are integers, if and only if $b = \pm 1$. We shall focus on these cases.

The following result is an extension of Proposition 1.1 for the sequences $U_n(a,b)$ and $V_n(a,b)$.

Theorem 3.1. *Let p be an odd prime, k be 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 a perfect square, then the sequences U_n and V_n defined by* (2.1) *and* (2.2) *satisfy the following relations:*

$$2U_{kp+r} \equiv \left(\frac{D}{p}\right) U_k V_r + V_k U_r \pmod{p}, \tag{3.1}$$

$$2V_{kp+r} \equiv D\left(\frac{D}{p}\right) U_k U_r + V_k V_r \pmod{p}. \tag{3.2}$$

Proof. We first prove that relation (3.1) holds, using the Binet formulae (2.4), (2.5) and (2.7). For any integer s, one may write

$$\alpha^s = \frac{V_s + U_s\sqrt{D}}{2}, \quad \beta^s = \frac{V_s - U_s\sqrt{D}}{2}.$$

Since $b=\pm 1$, the terms U_k, U_r and V_k, V_r are integers. We have

$$\begin{aligned}
U_{kp+r} &= \frac{1}{\sqrt{D}}\left[\alpha^{kp+r}-\beta^{kp+r}\right]\\
&= \frac{1}{\sqrt{D}}\left[\left(\frac{V_k+U_k\sqrt{D}}{2}\right)^p\frac{V_r+U_r\sqrt{D}}{2}-\left(\frac{V_k-U_k\sqrt{D}}{2}\right)^p\frac{V_r-U_r\sqrt{D}}{2}\right]\\
&= \frac{1}{2^{p+1}\sqrt{D}}\left[(V_k+U_k\sqrt{D})^p(V_r+U_r\sqrt{D})-(V_k-U_k\sqrt{D})^p(V_r-U_r\sqrt{D})\right]\\
&= \frac{1}{2^{p+1}\sqrt{D}}\Bigg[(V_r+U_r\sqrt{D})\sum_{j=0}^{p}\binom{p}{j}V_k^{p-j}\left(U_k\sqrt{D}\right)^j\\
&\qquad -(V_r-U_r\sqrt{D})\sum_{j=0}^{p}\binom{p}{j}(-1)^jV_k^{p-j}\left(U_k\sqrt{D}\right)^j\Bigg]\\
&= \frac{1}{2^{p+1}\sqrt{D}}\Bigg[V_r\sum_{j=0}^{p}\left(1-(-1)^j\right)\binom{p}{j}V_k^{p-j}\left(U_k\sqrt{D}\right)^j\\
&\qquad +U_r\sqrt{D}\sum_{j=0}^{p}\left(1+(-1)^j\right)\binom{p}{j}V_k^{p-j}\left(U_k\sqrt{D}\right)^j\Bigg]\\
&= \frac{1}{2^{p+1}\sqrt{D}}\Bigg[2V_r\left(U_k\sqrt{D}\right)^p+2V_r\sqrt{D}V_k^p+\\
&\quad +\sum_{j=1}^{p-1}\left[V_r\left(1-(-1)^j\right)+U_r\sqrt{D}\left(1+(-1)^j\right)\right]\binom{p}{j}V_k^{p-j}\left(U_k\sqrt{D}\right)^j\Bigg].
\end{aligned}$$

Since p divides $\binom{p}{j}$ for $j=1,\ldots,p-1$, it follows that

$$2^{p+1}U_{kp+r}\equiv 2V_rU_k^p\,D^{\frac{p-1}{2}}+2V_k^pU_r \pmod{p}.$$

By Fermat's Little Theorem, we have $2^p\equiv 2 \pmod{p}$, $U_k^p\equiv U_k \pmod{p}$, and $V_k^p\equiv V_k \pmod{p}$. Since $\left(\frac{D}{p}\right)\equiv D^{\frac{p-1}{2}} \pmod{p}$, we deduce that

$$2U_{kp+r}\equiv\left(\frac{D}{p}\right)U_kV_r+V_kU_r \pmod{p},$$

hence (3.1) holds.

The relation (3.2) satisfied by V_n follows from similar computations.

$$
\begin{aligned}
V_{kp+r} &= \alpha^{kp+r} + \beta^{kp+r} \\
&= \frac{1}{2^{p+1}} \left[(V_k + U_k\sqrt{D})^p (V_r + U_r\sqrt{D}) + (V_k - U_k\sqrt{D})^p (V_r - U_r\sqrt{D}) \right] \\
&= \frac{1}{2^{p+1}} \left[(V_r + U_r\sqrt{D}) \sum_{j=0}^{p} \binom{p}{j} V_k^{p-j} \left(U_k\sqrt{D}\right)^j \right. \\
&\qquad \left. + (V_r - U_r\sqrt{D}) \sum_{j=0}^{p} \binom{p}{j} (-1)^j V_k^{p-j} \left(U_k\sqrt{D}\right)^j \right] \\
&= \frac{1}{2^{p+1}} \left[V_r \sum_{j=0}^{p} \left(1 + (-1)^j\right) \binom{p}{j} V_k^{p-j} \left(U_k\sqrt{D}\right)^j \right. \\
&\qquad \left. + U_r\sqrt{D} \sum_{j=0}^{p} \left(1 - (-1)^j\right) \binom{p}{j} V_k^{p-j} \left(U_k\sqrt{D}\right)^j \right] \\
&= \frac{1}{2^{p+1}} \left[2V_rV_k^p + 2U_r\sqrt{D}\left(U_k\sqrt{D}\right)^p + \right. \\
&+ \left. \sum_{j=1}^{p-1} \left[V_r\left(1 + (-1)^j\right) + U_r\sqrt{D}\left(1 - (-1)^j\right) \right] \binom{p}{j} V_k^{p-j} \left(U_k\sqrt{D}\right)^j \right].
\end{aligned}
$$

Since p divides $\binom{p}{j}$ for $j = 1, \ldots, p-1$, it follows that

$$2^{p+1} V_{kp+r} \equiv 2V_rV_k^p + 2U_rU_k^pD^{\frac{p+1}{2}} \pmod{p}.$$

Following similar computations as for U_n, one obtains

$$
\begin{aligned}
2V_{kp+r} &\equiv D^{\frac{p+1}{2}} U_kU_r + V_kV_r \pmod{p} \\
&\equiv D\left(\frac{D}{p}\right) U_kU_r + V_kV_r \pmod{p},
\end{aligned}
$$

hence the relation (3.2) follows. □

Corollary 3.2. *Under the hypotheses of Theorem 3.1, we have*

1. *If k is a nonnegative integer, then*

$$U_{kp} \equiv \left(\frac{D}{p}\right) U_k \pmod{p}. \tag{3.3}$$

In particular, one has

$$U_p \equiv \left(\frac{D}{p}\right) \pmod{p}. \tag{3.4}$$

2. *If k is a nonnegative integer, then*

$$V_{kp} \equiv V_k \pmod{p}, \tag{3.5}$$

which for $k = 1$ yields

$$V_p \equiv a \pmod{p}. \tag{3.6}$$

For $a = 1$ and $b = -1$, from (3.3) and (3.5) one obtains the following known results for Fibonacci and Lucas sequences [5]:

$$F_{kp} \equiv \left(\frac{5}{p}\right) F_k \pmod{p},$$
$$L_{kp} \equiv L_k \pmod{p},$$

while from (3.4) and (3.6), one recovers the classical relations

$$p \mid F_{p-\left(\frac{5}{p}\right)}. \tag{3.7}$$
$$p \mid L_{p-\left(\frac{5}{p}\right)} - 2\left(\frac{5}{p}\right). \tag{3.8}$$

Some interesting divisibility properties involving k-Fibonacci and k-Lucas sequences can be obtained from the relations (3.4) and (3.6) in Corollary 3.2.

For example, when $b = -1$ and $a = 3$ we have $D = 13$ and

$$p \mid F_{3,p-\left(\frac{13}{p}\right)}, \quad p \mid L_{3,p-\left(\frac{13}{p}\right)} - 2\left(\frac{13}{p}\right). \tag{3.9}$$

Also, when $b = -1$ and $a = 5$ we have $D = 29$ and

$$p \mid F_{5,p-\left(\frac{29}{p}\right)}, \quad p \mid L_{5,p-\left(\frac{29}{p}\right)} - 2\left(\frac{29}{p}\right). \tag{3.10}$$

The case when D is prime present special interest. The following result extends a well known divisibility property of Fibonacci numbers.

Corollary 3.3. *Under the hypotheses of Theorem 3.1, whenever k_1, k_2 are integers with $p \mid U_{k_1} - U_{k_2}$, by (3.3), we have $p \mid U_{k_1 p} - U_{k_2 p}$. In particular, whenever $p \mid U_p$, it follows that $p \mid U_{kp}$ for all integers $k \geq 0$.*

Corollary 3.4. *In the conditions of Theorem 3.1, the following properties hold:*

1. $p \mid U_{p-\left(\frac{D}{p}\right)}$;
2. *If $b = -1$ (as for Lucas and Pell-Lucas numbers), then*

$$p \mid V_{p-\left(\frac{D}{p}\right)} - 2\left(\frac{D}{p}\right).$$

Proof. 1. Taking $k = 1$ and $r = \pm 1$ in (3.1) and using (2.6), we get

$$2U_{p+1} \equiv \left(\frac{D}{p}\right) a + a \pmod{p} \tag{3.11}$$
$$2U_{p-1} \equiv \left(\frac{D}{p}\right) \frac{a}{b} + a\frac{-1}{b} \pmod{p}. \tag{3.12}$$

If $\left(\frac{D}{p}\right) = -1$, then from (3.11) we have $p \mid U_{p+1}$. On the other hand, if $\left(\frac{D}{p}\right) = 1$, from (3.12) one obtains $p \mid U_{p-1}$.

2. Taking $k = 1$ and $r = \pm 1$ in relation (3.2) and using (2.6), we get

$$2V_{p+1} \equiv D\left(\frac{D}{p}\right) + a^2 \pmod{p} \tag{3.13}$$

$$2V_{p-1} \equiv D\left(\frac{D}{p}\right)\frac{-1}{b} + \frac{a^2}{b} \pmod{p}. \tag{3.14}$$

Since $D = a^2 - 4b$, if $\left(\frac{D}{p}\right) = -1$, then from (3.13) we have $p \mid V_{p+1} - 2b$. In the case $\left(\frac{D}{p}\right) = 1$, from (3.14) one obtains $p \mid V_{p-1} - 2$. □

3.1. Results for $b = -1$

The following result generalizes Proposition 1.2 (Lemma 1 in [5]), which was formulated for the Fibonacci and Lucas numbers. It can also be applied for Pell and Pell-Lucas numbers, as seen in Section 4.

Theorem 3.5. *Let p be an odd prime and k a positive integer. If $U_n = U_n(a, -1)$, $V_n = V_n(a, -1)$ and a is an integer such that $D = a^2 + 4 > 0$ is not a perfect square, then the following relations hold:*

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

Proof. 1. Setting in (3.1) $r = 1$ and $r = -1$, respectively, by (2.6) we obtain

$$2U_{kp+1} \equiv \left(\frac{D}{p}\right) aU_k + V_k \pmod{p} \tag{3.15}$$

$$2U_{kp-1} \equiv \left(\frac{D}{p}\right) \frac{a}{b}U_k - \frac{1}{b}V_k \pmod{p}. \tag{3.16}$$

By Lemma 2.1, considering $\left(\frac{D}{p}\right) = -1$ in (3.15), one obtains

$$2U_{kp-\left(\frac{D}{p}\right)} \equiv -aU_k + V_k \equiv -2bU_{k-1} \pmod{p}. \tag{3.17}$$

Furthermore, replacing $\left(\frac{D}{p}\right) = 1$ in (3.16), we have

$$2U_{kp-\left(\frac{D}{p}\right)} \equiv \frac{1}{b}\left(aU_k - V_k\right) \equiv 2U_{k-1} \pmod{p}. \tag{3.18}$$

Since $b = -1$, combining (3.17) and (3.18), it follows that

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

2. By setting $r = 1$ and $r = -1$ in (3.2), respectively, by (2.6) we obtain

$$2V_{kp+1} \equiv D\left(\frac{D}{p}\right) U_k + aV_k \pmod{p} \tag{3.19}$$

$$2V_{kp-1} \equiv D\left(\frac{D}{p}\right) U_k\frac{-1}{b} + \frac{a}{b}V_k \pmod{p}. \tag{3.20}$$

By Lemma 2.1, replacing $\left(\frac{D}{p}\right) = -1$ in (3.19), one obtains

$$2V_{kp-\left(\frac{D}{p}\right)} \equiv -DU_k + aV_k \equiv 2bV_{k-1} \equiv -2b\left(\frac{D}{p}\right)V_{k-1} \pmod{p}. \quad (3.21)$$

Furthermore, setting $\left(\frac{D}{p}\right) = 1$ in (3.20), we get

$$2V_{kp-\left(\frac{D}{p}\right)} \equiv -\frac{1}{b}\left(DU_k - aV_k\right) \equiv 2\left(\frac{D}{p}\right)V_{k-1} \pmod{p}. \quad (3.22)$$

Combining (3.21) and (3.22), we deduce that

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

This ends the proof. □

The following result generalises Proposition 1.3, which was originally formulated for the particular case of Fibonacci and Lucas sequences.

Remark 3.6. From the two statements of Theorem 3.5, we deduce that for every odd prime p, whenever a is an integer such that $D = a^2 + 4 > 0$ is not a perfect square, there is an arithmetic progression $a_0, a_1, \ldots$ with ratio p, such that the following two relations hold:

$$(U_{a_0}, U_{a_1}, U_{a_2}, \ldots) \equiv (U_0, U_1, U_2, \ldots) \pmod{p},$$
$$(V_{a_0}, V_{a_1}, V_{a_2}, \ldots) \equiv \left(\frac{D}{p}\right)(V_0, V_1, V_2, \ldots) \pmod{p}.$$

3.2. Results for $b = 1$

The following result is a counterpart of Proposition 1.2 (Lemma 1 in [5]), which was formulated for the Fibonacci and Lucas numbers ($b = -1$).

Theorem 3.7. *Let p be an odd prime and k a positive integer. If $U_n = U_n(a, 1)$, $V_n = V_n(a, 1)$ and a is an integer such that $D = a^2 - 4 > 0$ is not a perfect square, 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. $V_{kp-\left(\frac{D}{p}\right)} \equiv V_{k-1} \pmod{p}$.

Proof. Similar to Theorem 3.5, but using $b = 1$ in (3.17) and (3.21). □

Remark 3.8. Also, from the two statements of Theorem 3.7, we deduce that for every odd prime p, whenever a is an integer such that $D = a^2 - 4 > 0$ is not a perfect square, there is an arithmetic progression $a_0, a_1, \ldots$ with ratio p, such that the following two relations hold:

$$(U_{a_0}, U_{a_1}, U_{a_2}, \ldots) \equiv \left(\frac{D}{p}\right)(U_0, U_1, U_2, \ldots) \pmod{p},$$
$$(V_{a_0}, V_{a_1}, V_{a_2}, \ldots) \equiv (V_0, V_1, V_2, \ldots) \pmod{p}.$$

4. Applications to the classical Pell and Pell-Lucas numbers

Here we recover arithmetic properties of the Pell and Pell-Lucas numbers.

Theorem 4.1. *Let p be an odd prime, k a positive integer, and r an arbitrary integer. The following relations hold:*

$$2P_{kp+r} \equiv (-1)^{\frac{p^2-1}{8}} P_k Q_r + P_r Q_k \pmod{p}, \tag{4.1}$$

$$2Q_{kp+r} \equiv 8(-1)^{\frac{p^2-1}{8}} P_k P_r + Q_k Q_r \pmod{p}. \tag{4.2}$$

Proof. It follows by Theorem 3.1 used for $P_n = U_n(2,-1)$, and $Q_n = V_n(2,-1)$, together with the identities $\alpha = 1+\sqrt{2}$, $\beta = 1-\sqrt{2}$, $D = 8$, and the properties of Legendre's function. Notice the following identity $(-1)^{\frac{p^2-1}{8}} = \left(\frac{8}{p}\right) = \left(\frac{2}{p}\right)$, proved by Euler (see, e.g., [1, Theorem 9.1.2]). $\square$

Below we present some consequences of Theorem 4.1.

Corollary 4.2. *If k is a positive integer, then*

$$P_{kp} \equiv (-1)^{\frac{p^2-1}{8}} P_k \pmod{p},$$
$$Q_{kp} \equiv Q_k \pmod{p}.$$

In particular, when $k = 1$, one obtains

$$P_p \equiv (-1)^{\frac{p^2-1}{8}} \pmod{p},$$
$$Q_p \equiv 2 \pmod{p}.$$

The proofs follow easily by setting $r = 0$ in (4.1) and (4.2), respectively.

Corollary 4.3. *From relation* (4.3) *it follows that for two positive integers k and s, p divides $P_{kp} - P_{sp}$ if and only if p divides $P_k - P_s$. Moreover, we have*

$$P_{kp} - P_{sp} \equiv (-1)^{\frac{p^2-1}{8}} (P_k - P_s) \pmod{p}.$$

In particular, since $P_2 = 2$ and $P_1 = 1$, we get

$$P_{2p} - P_p \equiv (-1)^{\frac{p^2-1}{8}} \pmod{p}.$$

Proposition 4.4. *Under the conditions of Theorem 4.1, we have*

$$p \mid P_{p-(-1)^{\frac{p^2-1}{8}}},$$

$$p \mid Q_{p-(-1)^{\frac{p^2-1}{8}}} - 2(-1)^{\frac{p^2-1}{8}}.$$

Proof. Clearly, for $p \equiv 5 \pmod{8}$, we have $(-1)^{\frac{p^2-1}{8}} = -1$, while for $p \equiv 1, 3, 7 \pmod{8}$, we have $(-1)^{\frac{p^2-1}{8}} = 1$.

1) Taking $k = 1$ and $r = \pm 1$ in (4.1) we get

$$P_{p+1} = (-1)^{\frac{p^2-1}{8}} + 1 \pmod{p}, \tag{4.3}$$

$$P_{p-1} = -(-1)^{\frac{p^2-1}{8}} + 1 \pmod{p}. \tag{4.4}$$

If $p \equiv 5 \pmod 8$ then from (4.3) we have $p \mid P_{p+1}$. In the cases $p \equiv 1, 3, 7 \pmod 8$, from (4.4) one obtains $p | P_{p-1}$.

2) Taking $k = 1$ and $r = \pm 1$ in relation (4.2) we obtain

$$Q_{p+1} \equiv 4(-1)^{\frac{p^2-1}{8}} + 2 \pmod p$$

$$Q_{p-1} \equiv 4(-1)^{\frac{p^2-1}{8}} - 2 \pmod p.$$

This ends the proof. □

From Theorem 3.5 we recover the following property of the Pell and Pell-Lucas sequences, which represents a counterpart for the results given in [5] for Fibonacci and Lucas sequences.

Theorem 4.5. *Let p be an odd prime and k a positive integer. We have:*

1. $P_{kp-\left(\frac{8}{p}\right)} \equiv P_{k-1} \pmod p$*;*
2. $Q_{kp-\left(\frac{8}{p}\right)} \equiv \left(\frac{8}{p}\right) Q_{k-1} \pmod p$.

Proof. One just needs to consider $a = 2$ in Theorem 2, combined with the fact that $D = 8$ is not a perfect square. □

5. Pseudoprimality results concerning the classical sequences

In this section we review some key definitions of pseudoprimality related to the Fibonacci, Lucas, Pell and Pell-Lucas sequences.

5.1. Review on Fibonacci and Lucas pseudoprimality

We recall some notions of Fibonacci and Lucas pseudoprimality. A composite integer n is called a **Fibonacci pseudoprime** if $n \mid F_{n-\left(\frac{n}{5}\right)}$. Lehmer proved in [26] that there exist infinitely many pseudoprimes. The list of even such pseudoprimes is indexed as A141137 in the OEIS [28]. The list of known odd Fibonacci pseudoprimes indexed as A081264 begins with:

$$323, 377, 1891, 3827, 4181, 5777, 6601, 6721, 8149, 10877, 11663, 13201, 13981,$$
$$15251, 17119, 17711, 18407, 19043, 23407, 25877, 27323, 30889, 34561, 34943,$$
$$35207, 39203, 40501, 50183, 51841, 51983, 52701, 53663, 60377, 64079, \ldots$$

There is no prime such that $p^2 \mid F_{p-\left(\frac{p}{5}\right)}$ for $p < 2.8 \times 10^{16}$, in contrast to relation (3.7). R. Crandall, K. Dilcher and C. Pomerance called in [11] such a prime p satisfying $p^2 \mid F_{p-\left(\frac{p}{5}\right)}$ a **Wall-Sun-Sun prime**. There is no known example of a Wall-Sun-Sun prime and there is also no known way to check the congruence $F_{p-\left(\frac{p}{5}\right)} \equiv 0 \pmod{p^2}$, other than through explicit powering computations. Further remarks on this topic can be found in [3] or [17].

Taking $k = 1$ and $r = 0$ in the relation (1.2), we obtain

$$L_p \equiv 1 \pmod p.$$

A composite integer n satisfying $n \mid L_n - 1$ is called a **Bruckman-Lucas pseudoprime**. In 1964, Lehmer [26] proved that the set of Lucas pseudoprimes is infinite. This sequence indexed in the OEIS [28] as A005845, begins with:

$$705, 2465, 2737, 3745, 4181, 5777, 6721, 10877, 13201, 15251, 24465, 29281, 34561, 35785, 51841, 54705, 64079, 64681, 67861, 68251, 75077, 80189, 90061, 96049, 97921, 100065, 100127, 105281, 113573, 118441, 146611, \dots$$

A composite integer n is called a **Fibonacci-Bruckner-Lucas pseudoprime** if it satisfies simultaneously the properties

$$n \mid F_{n-\left(\frac{p}{5}\right)} \text{ and } n \mid L_n - 1.$$

These numbers produce the sequence [28] as A212424, beginning with

$$4181, 5777, 6721, 10877, 13201, 15251, 34561, 51841, 64079, 64681, \dots$$

Bruckman proved that there are infinitely many integers n with this property, in 1994 [7]. These were shown to correspond to the Frobenius pseudoprimes for the Fibonacci polynomial $x^2 - x - 1$ (see, e.g., [12], [30]).

5.2. New results on Pell and Pell-Lucas pseudoprimality

Some of the results in this section have been included in our book [4].

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 [28], starting with the terms:

$$169, 385, 741, 961, 1121, 2001, 3827, 4879, 5719, 6215, 6265, 6441, 6479, 6601, 7055, 7801, 8119, 9799, 10945, 11395, 13067, 13079, 13601, 15841, 18241, 19097, 20833, 20951, 24727, 27839, 27971, 29183, 29953, 31417, 31535, 34561, \dots$$

Kiss, Phong, and Lieuwen [22] showed that this sequence is infinite. By analogy with Wall-Sun-Sun primes, we call a prime p **strong Pell prime** if

$$p^2 \mid P_{p-(-1)^{\frac{p^2-1}{8}}}.$$

Finding examples of such primes and algorithms to check the sequence

$$P_{p-(-1)^{\frac{p^2-1}{8}}} \equiv 0 \pmod{p^2}$$

are interesting open problems.

Definition 5.1. We say that an odd composite integer n is a **Pell-Lucas pseudoprime** if n divides $Q_n - 2$.

The list of the Pell-Lucas pseudoprimes starts with the numbers

$$169, 385, 961, 1105, 1121, 3827, 4901, 6265, 6441, 6601, 7107, 7801, 8119, 10945, 11285, 13067, 15841, 18241, 19097, 20833, 24727, 27971, 29953, 31417, 34561, 35459, 37345, 37505, 38081, 39059, 42127, 45451, 45961, 47321, 49105, \dots,$$

recently indexed in the OEIS as A330276 [28]. Also, it seems that the following property is true, but at this moment we don't know a proof.

Conjecture 1. There exist infinitely many Pell-Lucas pseudoprimes.

We now define another concept of pseudoprimality, for which we formulate a conjecture based on numerical experiments.

Definition 5.2. An odd composite integer n is called a **Pell-Pell-Lucas pseudoprime** if it satisfies simultaneously the properties

$$n \mid P_{n-(-1)^{\frac{n^2-1}{8}}} \text{ and } n \mid Q_n - 2.$$

Conjecture 2. There exist infinitely many Pell-Pell-Lucas pseudoprimes.

The list of such pseudoprimes that we know at this moment is

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

which are recently indexed in the OEIS as A327652.

References

[1] Andreescu, T., Andrica, D.: Number Theory. Structures, Examples, and Problems. Birkhauser Verlag, Boston-Berlin-Basel (2009)

[2] Andreescu, T., Andrica, D.: Quadratic Diophantine Equations. Developments in Mathematics, Springer (2015)

[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, to appear (2020)

[5] 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)

[6] Borges, A., Catarino, P., Aires A. P., Vasco, P., Campos, H.: Two-by-two matrices involving k-Fibonacci and k-Lucas sequences. Appl. Math. Sci. **8**(34), 1659–1666 (2014)

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

[8] Catarino, P., Vasco, P.: On Dual k-Pell Quaternions and Octonions. Mediterr. J. Math. **14**, 75 (2017)

[9] Catarino, P.: A note involving two-by-two matrices of the k-Pell and k-Pell-Lucas sequences. Int. Math. Forum **8**(32), 1561–1568 (2013)

[10] Catarino, P., Vasco, P., Borges, A., Campos, H., Aires A. P.: Sums, products and identities involving k-Fibonacci and k-Lucas sequences. JP J of Algebra, Number Theory and Appl. **32**(1), 63–77 (2014)

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

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

[13] Falcon, S., Plaza, A.: On the Fibonacci k-numbers, Chaos Soliton Fract. **32**(5), 1615–1624 (2007)

[14] Falcon, S.: On the Lucas triangle and its relationship with the k-Lucas numbers. J. Math. Comput. Sci. **2**, 425–434 (2012)

[15] Falcon, S.: Relationships between some k-Fibonacci sequences. Applied Mathematics, **5**, 2226–2234 (2014)

[16] Fredman, M. L., Tarjan, R. E.: Fibonacci heaps and their uses in improved network optimization algorithms. J. ACM. **34**(3), 596–615 (1987)

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

[18] Hosoya, H.: What Can Mathematical Chemistry Contribute to the Development of Mathematics?. International Journal for Philosophy of Chemistry, **19**(1), 87-105 (2013).

[19] Jancić, M.: On linear recurrence equations arising from compositions of positive integers. J. Int. Seq. **18**, Article 15.4.7 (2015)

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

[21] Kiefer, J.: Sequential minimax search for a maximum. Proc. Am. Math. Soc. **4**, 502–506 (1953)

[22] 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)

[23] Knuth, D. E.: The Art of Computer Programming. Vol. 3, Addison Wesley, Second Edition (2003)

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

[25] Lehmer, D. H.: An extended theory of Lucas' functions. Ann. Math., 2nd Ser. **2**(3), 419–448 (1930)

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

[27] Noonea, C. J., Torrilhonb, M., Mitsosa, A.: Heliostat field optimization: A new computationally efficient model and biomimetic layout. Solar Energy **86**(2), 792–803 (2012)

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

[29] Rabago J. F. T.: On k-Fibonacci numbers with applications to continued fractions. Proceedings of ICMAME 2015, J. Phys.: Conf. Ser. **693** 012005 (2016)

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

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

Dorin Andrica
Faculty of Mathematics and Computer Science
Babeş-Bolyai University of Cluj-Napoca
Kogălniceanu Street, Nr. 1
400084 Cluj-Napoca, Romania
e-mail: dandrica@math.ubbcluj.ro

Ovidiu Bagdasar
Department of Electronics, Computing and Mathematics
University of Derby
Markeaton Street, Derby, DE22 3AW
United Kingdom
e-mail: o.bagdasar@derby.ac.uk