DOI: 10.2478/auom-2023-0002
An. Şt. Univ. Ovidius Constanţa **Vol. 31(1),2023, 23–46**

On some links between the generalised Lucas pseudoprimes of level k

Dorin Andrica, Ovidiu Bagdasar and Michael Th. Rassias

Abstract

Pseudoprimes are composite integers sharing behaviours of the prime numbers, often used in practical applications like public-key cryptography. Many pseudoprimality notions known in the literature are defined by recurrent sequences. In this paper we first establish new arithmetic properties of the generalized Lucas and Pell-Lucas sequences. Then we study the recent notion of generalized Pell and Pell-Lucas pseudoprimes of level k, and find inclusions between the sets of pseudoprimes on different levels. In this process we extend several results concerning Fibonacci, Lucas, Pell, and Pell-Lucas sequences.

1 Introduction

Recurrent sequences present both theoretical and practical importance, and many interesting properties and applications of these sequences are still being discovered. Famous examples of second-order recurrences with integer coefficients include the classical Fibonacci, Lucas, Pell, or Pell-Lucas sequences.

For a and b integers, the **generalized Lucas** sequence $\{U_n(a,b)\}_{n\geq 0}$ and its companion, the **generalized Pell-Lucas** sequence $\{V_n(a,b)\}_{n\geq 0}$ whose terms will be denoted by U_n and V_n for convenience, are defined by

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

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

Key Words: Generalised Lucas sequences, Jacobi symbol, Pseudoprimality, Pseudoprimality of level k.
2010 Mathematics Subject Classification: Primary 11A51; Secondary 11B39, 11B50.
Received: 01.07.2022
Accepted: 30.09.2022

A standard method to study these sequences involves the quadratic equation $z^2 - az + b = 0$, which for $D = a^2 - 4b \neq 0$ has the distinct roots

$$\alpha = \frac{a + \sqrt{D}}{2}, \quad \beta = \frac{a - \sqrt{D}}{2}. \tag{3}$$

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

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

$$U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} = \frac{1}{\sqrt{D}} \left(\alpha^n - \beta^n \right), \quad n = 0, 1, \dots \tag{4}$$

$$V_n = \alpha^n + \beta^n, \quad n = 0, 1, \dots. \tag{5}$$

These formulae extend naturally to negative indices, and we have

$$U_{-1} = \frac{1}{\sqrt{D}} \left(\alpha^{-1} - \beta^{-1} \right) = -\frac{1}{b}, \quad V_{-1} = \alpha^{-1} + \beta^{-1} = \frac{a}{b}, \tag{6}$$

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

$$U_{-n} = \frac{1}{\sqrt{D}} \left(\alpha^{-n} - \beta^{-n} \right) = -\frac{1}{b^n} U_n, \quad V_{-n} = \alpha^{-n} + \beta^{-n} = \frac{1}{b^n} V_n. \tag{7}$$

Note that the terms U_n and V_n are integers for all $n \in \mathbb{Z}$ if and only if $b = \pm 1$, when these sequences have interesting divisibility properties [10]. We also mention that the general term formula for U_n and V_n can also be written using bivariate cyclotomic polynomials in α and β [11, p. 99].

For $b = -1$ and $k > 0$, one obtains the k-Fibonacci and k-Lucas number $F_{k,n} = U_n(k, -1)$ and $L_{k,n} = V_n(k, -1)$, where $D = k^2 + 4$. In particular, for $k = 1$ we get the classical Fibonacci and Lucas numbers $F_n = U_n(1, -1)$ and $L_n = V_n(1, -1)$ where $D = 5$, while for $k = 2$ we get the Pell and Pell Lucas numbers $P_n = U_n(2, -1)$ and $Q_n = V_n(2, -1)$, when $D = 8$.

For $b = 1$, the integers $U_n(a, 1)$ have combinatorial interpretations, while the terms $V_n(a, 1)$ relate to the number of solutions for certain Diophantine equations [3], and to important classes of polynomials, including Chebysev polynomials of the first and second kinds [2, Chapter 2.2].

The generalized Pell and Pell-Lucas sequences have attracted much interest in recent years. New arithmetic properties were established in [3], while identification formulae for the sequence terms and density results have been derived in [7]. Conjectures on the infinity of certain sets of pseudoprimes inspired by [3] have been recently solved by J. Grantham [13].

The arithmetic properties of generalized Lucas and Pell-Lucas sequences [3], inspired the concept of **generalized Lucas pseudoprimes of level** k [5], which led to new additions to the Online Encyclopedia of Integer Sequences (OEIS) [17]. The connections between the pseudoprimes of levels 1 and 2 studied in [4] showed that the extension to level 3 are not trivial.

In this paper we first derive new arithmetic properties which can be used to obtain links between the pseudoprimes of levels $2k$. In Section 2 we review basic properties of generalised Lucas sequences and pseudoprimality notions. Then, in Section 3 we establish some new relations and arithmetic properties of the generalised Pell and Pell-Lucas sequences. These are used in Section 4 to to prove new links between the generalised pseudoprimes of level k, extending earlier work related to levels 1 and 2, and to Fibonacci and Lucas numbers.

Given the applications of pseudoprimes in public key cryptography [15], computational number theory [16], and IT security [19], further works can be dedicated to the use of pseudoprimes of level k in a cryptography context.

2 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 denoted by U_n and V_n.

2.1 Useful identities and arithmetic properties

We first present some Cassini-type identities generalising Lemma 2.4 in [4].

Lemma 1. *Let m, M, r, R be integers with $r+R=m+M$. We have:*

$$1^\circ \quad U_mU_M - U_rU_R = b^rU_{m-r}U_{M-r}, \tag{8}$$
$$2^\circ \quad U_mV_M - U_rV_R = b^rU_{m-r}V_{M-r}, \tag{9}$$
$$3^\circ \quad V_mV_M - V_rV_R = -Db^rU_{m-r}U_{M-r}, \tag{10}$$
$$4^\circ \quad V_mV_M - DU_rU_R = b^rV_{m-r}V_{M-r}. \tag{11}$$

Proof. For 1°, from (4), (5), $\alpha\beta = b$ and $R-r=m+M-2r$ we obtain

$$\begin{aligned}
U_mU_M - U_rU_R &= \frac{\alpha^m-\beta^m}{\alpha-\beta}\cdot\frac{\alpha^M-\beta^M}{\alpha-\beta} - \frac{\alpha^r-\beta^r}{\alpha-\beta}\cdot\frac{\alpha^R-\beta^R}{\alpha-\beta} \\
&= \frac{\alpha^r\beta^R-\alpha^m\beta^M-\alpha^M\beta^m+\alpha^R\beta^r}{(\alpha-\beta)^2} \\
&= (\alpha\beta)^r\,\frac{\beta^{m+M-2r}-\alpha^{m-r}\beta^{M-r}-\alpha^{M-r}\beta^{m-r}+\alpha^{m+M-2r}}{(\alpha-\beta)^2} \\
&= (\alpha\beta)^r\left(\frac{\alpha^{m-r}-\beta^{m-r}}{\alpha-\beta}\right)\left(\frac{\alpha^{M-r}-\beta^{M-r}}{\alpha-\beta}\right) = b^rU_{m-r}U_{M-r}.
\end{aligned}$$

For 2° we use the formulae (4) and (5) to deduce that

$$\begin{aligned} U_m V_M - U_r V_R &= \left(\frac{\alpha^m - \beta^m}{\alpha - \beta}\right)\left(\alpha^M + \beta^M\right) - \left(\frac{\alpha^r - \beta^r}{\alpha - \beta}\right)\left(\alpha^R + \beta^R\right) \\ &= \frac{\alpha^m\beta^M - \alpha^M\beta^m - \alpha^r\beta^R + \alpha^R\beta^r}{\alpha - \beta} \\ &= (\alpha\beta)^r \frac{\alpha^{m-r} - \beta^{m-r}}{\alpha - \beta}\left(\alpha^{M-r} + \beta^{M-r}\right) = b^r U_{m-r} V_{M-r}. \end{aligned}$$

Similar arguments and $(\alpha - \beta)^2 = D$ are used to prove 3° and 4°. □

We now summarise some arithmetic properties proved in [3].

Theorem 2 ([3], Theorem 3.1)**.** *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 defined by (1) and (2) satisfy the following relations:*

$$1)\quad 2U_{kp+r} \equiv \left(\frac{D}{p}\right) U_k V_r + V_k U_r \pmod{p} \tag{12}$$

$$2)\quad 2V_{kp+r} \equiv D\left(\frac{D}{p}\right) U_k U_r + V_k V_r \pmod{p}, \tag{13}$$

where $\left(\frac{D}{p}\right)$ is the Legendre symbol (see, e.g., [1]).

Proposition 3 ([3], Theorem 3.5)**.** *Let p be an odd prime, and let $k > 0$ and a be integers so 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) $V_{kp-\left(\frac{D}{p}\right)} \equiv \left(\frac{D}{p}\right) V_{k-1} \pmod{p}$.

Proposition 4 ([3], Theorem 3.7)**.** *Let p be an odd prime, and let $k > 0$ and a be integers so 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) $U_{kp-\left(\frac{D}{p}\right)} \equiv \left(\frac{D}{p}\right) U_{k-1} \pmod{p}$,

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

Classical identities known to E. Lucas (see, e.g., [20]) are obtained as particular instances. For example, given that $U_0 = 0$ and $V_0 = 2$, by using $k = 1$ and $r = 0$ in Theorem 2 one obtains

$$U_p \equiv \left(\frac{D}{p}\right) \pmod{p}, \quad V_p \equiv a \pmod{p}, \tag{14}$$

while replacing $k = 1$ in Propositions 3 and 4 one has

$$U_{p-\left(\frac{D}{p}\right)} \equiv 0 \pmod{p}, \quad V_{p-\left(\frac{D}{p}\right)} \equiv 2\left(\frac{D}{p}\right)^{\frac{1-b}{2}} \pmod{p}. \tag{15}$$

2.2 Pseudoprimality generated by $\{U_n(a,b)\}_{n\geq 0}$ and $\{V_n(a,b)\}_{n\geq 0}$

Pseudoprimes are composite numbers which share certain properties of prime numbers, which have found applications in primality testing, cryptography, or the factorization of large integers. Important classes of pseudoprimes 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 relations (14) and (15).

Grantham [12] unified various pseudoprimality notions under the name of Frobenius pseudoprimes and several examples are listed in Rotkiewicz [18]. Here we briefly recall the key pseudoprime notions relevant to this paper.

Definition 5. *[[5], Definition 1.4] An odd composite integer n is said to be a* ***generalized Lucas pseudoprime of parameters*** a ***and*** b *if* $\gcd(n,b) = 1$ *and n divides $U_{n-\left(\frac{D}{n}\right)}$, where $\left(\frac{D}{n}\right)$ is the Jacobi symbol.*

By (14), one has $U_p^2 \equiv 1 \pmod{p}$, and in our paper [6] we have defined some weak pseudoprimality notions for the sequences $U_n(a,b)$ and $V_n(a,b)$, for which we have explored related properties and novel integer sequences.

Definition 6. *A composite integer n for which $n \mid U_n^2 - 1$ is called a* ***weak generalized Lucas pseudoprime*** *of parameters a and b.*

Definition 7. *A composite integer n is said to be a* ***generalized Bruckman-Lucas pseudoprime of parameters*** a ***and*** b *if $n \mid V_n(a,b) - a$.*

3 Arithmetic properties of $\{U_n(a,b)\}_{n\geq 0}$ and $\{V_n(a,b)\}_{n\geq 0}$

In this section we use Propositions 3 and 4 to derive some divisibility properties modulo a composite number. These allow to connect some classes of generalized Lucas and Pell-Lucas pseudoprimes proposed in [4].

If p is prime and a is an odd integer, then for $b = \pm 1$ we have $D = a^2 \mp 4$, and by the law of quadratic reciprocity for the Jacobi symbol one has

$$\left(\frac{D}{p}\right)\left(\frac{p}{D}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{D-1}{2}} = 1, \tag{16}$$

therefore one can deduce that

$$\left(\frac{D}{p}\right) = \left(\frac{p}{D}\right). \tag{17}$$

This property allows us to rewrite Propositions 3 and 4.

3.1 Results for $b = -1$

We shortly denote $U_n = U_n(a, -1)$ and $V_n = V_n(a, -1)$. By substituting (17) in Proposition 3, we obtain the relations

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

We now investigate some identities modulo an odd composite number n.

Recall that by (7) we have $U_{-n} = -\frac{1}{b^n}U_n$, and $V_{-n} = \frac{1}{b^n}V_n$, which for $b = -1$ and $n = 1$ gives $U_{-1} = U_1 = 1$ and $V_{-1} = -V_1 = -a$.

Lemma 8. *Consider the integers a, s, k and n, and let D be an odd number relatively prime with n. The following identities hold:*

$$U_{(k+1)s-\left(\frac{n}{D}\right)} = U_s U_{ks} + U_{s-\left(\frac{n}{D}\right)} U_{ks-\left(\frac{n}{D}\right)}, \tag{18}$$

$$U_{(k+1)s} = U_s U_{ks-\left(\frac{n}{D}\right)} + U_{s-\left(\frac{n}{D}\right)} U_{ks} + a\left(\frac{n}{D}\right) U_s U_{ks}. \tag{19}$$

Proof. Applying Lemma 1 part 1° for $m = s-\left(\frac{n}{D}\right)$, $M = ks-\left(\frac{n}{D}\right)$, $r = -\left(\frac{n}{D}\right)$, and $R = (k+1)s - \left(\frac{n}{D}\right)$, we obtain

$$U_{s-\left(\frac{n}{D}\right)} U_{ks-\left(\frac{n}{D}\right)} - U_{-\left(\frac{n}{D}\right)} U_{(k+1)s-\left(\frac{n}{D}\right)} = (-1)^{-\left(\frac{n}{D}\right)} U_s U_{ks}. \tag{20}$$

We can easily check that for $b = -1$ we have $U_{-1} = U_1 = 1$, hence $U_{-\left(\frac{n}{D}\right)} = 1$. Since $(n, D) = 1$ and $\left(\frac{n}{D}\right) = \pm 1$, we have $(-1)^{-\left(\frac{n}{D}\right)} = -1$, hence (18) holds.

Similarly, using $m = s$, $M = ks + 1$, $r = 1$, $R = (k+1)s$ in (8), we get

$$U_{(k+1)s} = U_s U_{ks+1} + U_{s-1} U_{ks}. \tag{21}$$

From the recurrence (1) satisfied by U_n, one obtains

$$U_{ks+1} = aU_{ks} + U_{ks-1}, \qquad U_{ks-1} = -aU_{ks} + U_{ks+1}$$
$$U_{s+1} = aU_s + U_{s-1}, \qquad U_{s-1} = -aU_s + U_{s+1}.$$

The following two cases are possible.

Case 1. If $\left(\frac{n}{D}\right) = 1$, then

$$\begin{aligned} U_{(k+1)s} &= U_s \left[aU_{ks} + U_{ks-\left(\frac{n}{D}\right)} \right] + U_{ks} U_{s-\left(\frac{n}{D}\right)} \\ &= U_s U_{ks-\left(\frac{n}{D}\right)} + U_{s-\left(\frac{n}{D}\right)} U_{ks} + aU_s U_{ks}. \end{aligned}$$

Case 2. If $\left(\frac{n}{D}\right) = -1$, then

$$\begin{aligned} U_{(k+1)s} &= U_s U_{ks-\left(\frac{n}{D}\right)} + U_{ks} \left[-aU_s + U_{s-\left(\frac{n}{D}\right)} \right] \\ &= U_s U_{ks-\left(\frac{n}{D}\right)} + U_{s-\left(\frac{n}{D}\right)} U_{ks} - aU_s U_{ks}. \end{aligned}$$

The two cases are summarised by the unitary formula (19). $\square$

Some particular examples of Lemma 8 present special interest, and here we provide the relations obtained for $s = n$ and $k = 0, 1, 2$.

$$\begin{aligned} U_{2n-\left(\frac{n}{D}\right)} &= U_n^2 + U_{n-\left(\frac{n}{D}\right)}^2, \\ U_{2n} &= 2U_n U_{n-\left(\frac{n}{D}\right)} + a \left(\frac{n}{D}\right) U_n^2, \\ U_{3n-\left(\frac{n}{D}\right)} &= U_n U_{2n} + U_{n-\left(\frac{n}{D}\right)} U_{2n-\left(\frac{n}{D}\right)}, \\ U_{3n} &= U_n U_{2n-\left(\frac{n}{D}\right)} + U_{n-\left(\frac{n}{D}\right)} U_{2n} + a \left(\frac{n}{D}\right) U_n U_{2n}. \end{aligned}$$

Under the supplementary assumptions $n \mid U_{n-\left(\frac{n}{D}\right)}$ and $n \mid U_n^2 - 1$ (linked to Definitions 5 and 6), one obtains the congruences

$$\begin{aligned} &U_{2n-\left(\frac{n}{D}\right)} \equiv 1 \pmod{n}, \quad U_{2n} \equiv a \left(\frac{n}{D}\right) \pmod{n}, \qquad (22) \\ &U_{3n-\left(\frac{n}{D}\right)} \equiv a \left(\frac{n}{D}\right) U_n \pmod{n}, \quad U_{3n} \equiv (1 + a^2) U_n \pmod{n}. \end{aligned}$$

We investigate some identities modulo a composite number. Recall that a is odd and $D = a^2 + 4$, while $U_0 = 0$, $U_1 = 1$, $U_2 = a$ and $U_3 = a^2 + 1$.

Theorem 9. *Let a and $n>0$ be odd integers such that n and D are coprime. If $n \mid U_{n-\left(\frac{n}{D}\right)}$ and $n \mid U_n^2-1$, then for all positive integers $k \geq 1$, we have:*

$$U_{(2k-1)n-\left(\frac{n}{D}\right)} \equiv \left(\frac{n}{D}\right) U_{2k-2} U_n \pmod{n}, \tag{23}$$

$$U_{(2k-1)n} \equiv U_{2k-1} U_n \pmod{n}, \tag{24}$$

and also,

$$U_{(2k)n-\left(\frac{n}{D}\right)} \equiv U_{2k-1} \pmod{n}, \tag{25}$$

$$U_{(2k)n} \equiv \left(\frac{n}{D}\right) U_{2k} \pmod{n}. \tag{26}$$

Proof. By the hypothesis, using $t=k$ and $n=s$ in (18) and (19) we get

$$U_{(t+1)n-\left(\frac{n}{D}\right)} \equiv U_{tn} U_n \pmod{n}, \tag{27}$$

$$U_{(t+1)n} \equiv U_{tn-\left(\frac{n}{D}\right)} U_n + a\left(\frac{n}{D}\right) U_{tn} U_n \pmod{n}. \tag{28}$$

We prove (23), (24), (25) and (26) by induction on $k \geq 1$.

For the anchor step $k=1$ the relations (23) and (24) clearly follow:

$$U_{n-\left(\frac{n}{D}\right)} \equiv 0 \equiv \left(\frac{n}{D}\right) U_0 U_n \pmod{n},$$
$$U_n \equiv U_1 U_n \pmod{n}.$$

Also, (25) and (26) follow directly from relation (22) written as

$$U_{2n-\left(\frac{n}{D}\right)} \equiv 1 \equiv U_1 \pmod{n},$$
$$U_{2n} \equiv \left(\frac{n}{D}\right) a \equiv \left(\frac{n}{D}\right) U_2 \pmod{n}.$$

Assume that (23), (24), (25) and (26) hold for k. We then prove that these statements also hold for $k+1$.

Indeed, by substituting $t=2k$ and $t=2k+1$ in (27) and from the induction hypothesis, one obtains

$$U_{(2k+1)n-\left(\frac{n}{D}\right)} \equiv \left(\frac{n}{D}\right) U_{(2k)n} U_n \equiv \left(\frac{n}{D}\right) U_{2k} U_n \pmod{n},$$
$$U_{(2k+2)n-\left(\frac{n}{D}\right)} \equiv U_{(2k+1)n} U_n \equiv \left(U_{2k+1} U_n\right) U_n \equiv U_{2k+1} \pmod{n}.$$

Also, by substituting $t = 2k$ and $t = 2k+1$ in (28), and using the induction hypotheses, we deduce the following relations

$$\begin{aligned} U_{(2k+1)n} &\equiv U_{(2k)n-\left(\frac{n}{D}\right)}U_n + a\left(\frac{n}{D}\right)U_{(2k)n}U_n \pmod{n} \\ &\equiv U_{2k-1}U_n + a\left(\frac{n}{D}\right)^2 U_{2k}U_n^2 \pmod{n} \\ &\equiv \left(U_{2k-1} + aU_{2k}\right)U_n \equiv U_{2k+1}U_n \pmod{n}, \\ U_{(2k+2)n} &\equiv U_{(2k+1)n-\left(\frac{n}{D}\right)}U_n + a\left(\frac{n}{D}\right)U_{(2k+1)n}U_n \pmod{n} \\ &\equiv \left(\frac{n}{D}\right)U_{2k}(U_n)^2 + a\left(\frac{n}{D}\right)U_{(2k+1)n}(U_n)^2 \pmod{n} \\ &\equiv \left(\frac{n}{D}\right)\left(U_{2k} + aU_{2k+1}\right) \equiv \left(\frac{n}{D}\right)U_{2k+2} \pmod{n}. \end{aligned}$$

This ends the proof. □

Similarly, we now derive some useful results concerning V_n.

Lemma 10. *Consider the integers a, s, k and n, and let D be an odd number relatively prime with n. The following identities hold:*

$$V_{(k+1)s-\left(\frac{n}{D}\right)} = U_sV_{ks} + U_{s-\left(\frac{n}{D}\right)}V_{ks-\left(\frac{n}{D}\right)}, \tag{29}$$

$$V_{(k+1)s} = U_sV_{ks-\left(\frac{n}{D}\right)} + U_{s-\left(\frac{n}{D}\right)}V_{ks} + a\left(\frac{n}{D}\right)U_sV_{ks}. \tag{30}$$

Proof. Applying Lemma 1 part 2° for $m = s-\left(\frac{n}{D}\right)$, $M = ks-\left(\frac{n}{D}\right)$, $r = -\left(\frac{n}{D}\right)$, and $R = (k+1)s - \left(\frac{n}{D}\right)$, we obtain

$$U_{s-\left(\frac{n}{D}\right)}V_{ks-\left(\frac{n}{D}\right)} - U_{-\left(\frac{n}{D}\right)}V_{(k+1)s-\left(\frac{n}{D}\right)} = (-1)^{-\left(\frac{n}{D}\right)}U_sV_{ks}. \tag{31}$$

As in Lemma 8, we have $U_{-\left(\frac{n}{D}\right)} = 1$ and $(-1)^{-\left(\frac{n}{D}\right)} = -1$, hence (29) holds. Similarly, for $m = s$, $M = ks+1$, $r = 1$, and $R = (k+1)s$, we obtain

$$V_{(k+1)s} = U_sV_{ks+1} + U_{s-1}V_{ks}. \tag{32}$$

From the recurrence (2) satisfied by V_n, one obtains

$$\begin{aligned} V_{ks+1} &= aV_{ks} + V_{ks-1}, & V_{ks-1} &= -aV_{ks} + V_{ks+1} \\ V_{s+1} &= aV_s + V_{s-1}, & V_{s-1} &= -aV_s + V_{s+1}. \end{aligned}$$

The following two cases are possible.

Case 1. If $\left(\frac{n}{D}\right) = 1$, then

$$\begin{aligned} V_{(k+1)s} &= U_s \left[aV_{ks} + V_{ks-\left(\frac{n}{D}\right)} \right] + V_{ks} U_{s-\left(\frac{n}{D}\right)} \\ &= U_s V_{ks-\left(\frac{n}{D}\right)} + U_{s-\left(\frac{n}{D}\right)} V_{ks} + aU_s V_{ks}. \end{aligned}$$

Case 2. If $\left(\frac{n}{D}\right) = -1$, then

$$\begin{aligned} V_{(k+1)s} &= U_s V_{ks-\left(\frac{n}{D}\right)} + V_{ks} \left[-aU_s + U_{s-\left(\frac{n}{D}\right)} \right] \\ &= U_s V_{ks-\left(\frac{n}{D}\right)} + U_{s-\left(\frac{n}{D}\right)} V_{ks} - aU_s V_{ks}. \end{aligned}$$

The two cases are summarised by the unitary formula (30). □

Some particular examples from Lemma 10 present special interest, and here we show the relations obtained for $s = n$ and $k = 0, 1, 2$. Recall that $V_0 = 2$, $V_1 = a$, $V_2 = a^2 + 2$, $V_3 = a^3 + 3a$ and $V_{-\left(\frac{n}{D}\right)} = -a\left(\frac{n}{D}\right)$. We have

$$\begin{aligned} V_{n-\left(\frac{n}{D}\right)} &= U_n V_0 + U_{n-\left(\frac{n}{D}\right)} V_{-\left(\frac{n}{D}\right)} = 2U_n - a\left(\frac{n}{D}\right) U_{n-\left(\frac{n}{D}\right)}, \\ V_n &= U_n V_{-\left(\frac{n}{D}\right)} + U_{n-\left(\frac{n}{D}\right)} V_0 + a\left(\frac{n}{D}\right) U_n V_0 = 2U_{n-\left(\frac{n}{D}\right)} + a\left(\frac{n}{D}\right) U_n, \\ V_{2n-\left(\frac{n}{D}\right)} &= U_n V_n + U_{n-\left(\frac{n}{D}\right)} V_{n-\left(\frac{n}{D}\right)}, \\ V_{2n} &= U_n V_{n-\left(\frac{n}{D}\right)} + U_{n-\left(\frac{n}{D}\right)} V_n + a\left(\frac{n}{D}\right) U_n V_n, \\ V_{3n-\left(\frac{n}{D}\right)} &= U_n V_{2n} + U_{n-\left(\frac{n}{D}\right)} V_{2n-\left(\frac{n}{D}\right)}, \\ V_{3n} &= U_n V_{2n-\left(\frac{n}{D}\right)} + U_{n-\left(\frac{n}{D}\right)} V_{2n} + a\left(\frac{n}{D}\right) U_n V_{2n}. \end{aligned}$$

Under the supplementary assumptions $n \mid U_{n-\left(\frac{n}{D}\right)}$ and $n \mid U_n^2 - 1$ (linked to Definitions 5 and 6), one obtains the following congruences

$$V_{n-\left(\frac{n}{D}\right)} \equiv V_0 U_n \pmod{n}, \quad V_n \equiv V_1 \left(\frac{n}{D}\right) U_n \pmod{n}, \tag{33}$$

$$V_{2n-\left(\frac{n}{D}\right)} \equiv \left(\frac{n}{D}\right) V_1 \pmod{n}, \quad V_{2n} \equiv V_2 \pmod{n}, \tag{34}$$

$$V_{3n-\left(\frac{n}{D}\right)} \equiv V_2 U_n \pmod{n}, \quad V_{3n} \equiv V_3 \left(\frac{n}{D}\right) U_n \pmod{n}.$$

We now investigate relations modulo a composite number when $D = a^2 + 4$.

Theorem 11. *Let a and $n > 0$ be odd integers such that n and D are coprime. If $n \mid U_{n-\left(\frac{n}{D}\right)}$ and $n \mid U_n^2 - 1$, then for all positive integers k, we have:*

$$V_{(2k-1)n-\left(\frac{n}{D}\right)} \equiv V_{2k-2}U_n \pmod{n}, \tag{35}$$

$$V_{(2k-1)n} \equiv \left(\frac{n}{D}\right) V_{2k-1}U_n \pmod{n}, \tag{36}$$

and also,

$$V_{(2k)n-\left(\frac{n}{D}\right)} \equiv \left(\frac{n}{D}\right) V_{2k-1} \pmod{n}, \tag{37}$$

$$V_{(2k)n} \equiv V_{2k} \pmod{n}. \tag{38}$$

Proof. By the hypothesis, using $t = k$ and $n = s$ in (29) and (30) we get

$$V_{(t+1)n-\left(\frac{n}{D}\right)} \equiv V_{tn}U_n \pmod{n}, \tag{39}$$

$$V_{(t+1)n} \equiv V_{tn-\left(\frac{n}{D}\right)}U_n + a\left(\frac{n}{D}\right) V_{tn}U_n \pmod{n}. \tag{40}$$

We will prove (35), (36), (37), (38) by induction on $k \geq 1$. The anchor step relations for $k = 1$ are confirmed by the formulae (33) and (34).

For the induction step, assume that (35), (36), (37), (38) hold for $1, \ldots, k$, and we then prove that these relations also hold for $k + 1$.

Indeed, replacing $t = 2k$ and $t = 2k + 1$ in (39), one obtains

$$V_{(2k+1)n-\left(\frac{n}{D}\right)} \equiv V_{(2k)n}U_n \equiv \left(\frac{n}{D}\right) V_{2k}U_n \pmod{n},$$
$$V_{(2k+2)n-\left(\frac{n}{D}\right)} \equiv \left(\frac{n}{D}\right) V_{(2k+1)n}U_n \equiv \left(V_{(2k+1)}U_n\right) U_n \equiv \left(\frac{n}{D}\right) V_{(2k+1)} \pmod{n}.$$

Also, by using $t = 2k$ and $t = 2k + 1$ in relation (40) we deduce that

$$\begin{aligned}
V_{(2k+1)n} &\equiv V_{(2k)n-\left(\frac{n}{D}\right)}U_n + a\left(\frac{n}{D}\right) V_{(2k)n}U_n \pmod{n} \\
&\equiv \left(\frac{n}{D}\right) V_{2k-1}U_n + a\left(\frac{n}{D}\right)^2 V_{(2k)}U_n^2 \pmod{n} \\
&\equiv \left(\frac{n}{D}\right) \left(V_{2k-1} + aV_{2k}\right) U_n \equiv \left(\frac{n}{D}\right) V_{2k+1}U_n \pmod{n}, \\
V_{(2k+2)n} &\equiv V_{(2k+1)n-\left(\frac{n}{D}\right)}U_n + a\left(\frac{n}{D}\right) V_{(2k+1)kn}U_n \pmod{n} \\
&\equiv V_{2k}(U_n)^2 + a\left(\frac{n}{D}\right)^2 V_{(2k+1)n}(U_n)^2 \pmod{n} \\
&\equiv V_{2k} + aV_{2k+1} \equiv V_{2k+2} \pmod{n}.
\end{aligned}$$

This ends the proof. ∎

3.2 Results for $b = 1$

We denote for simplicity $U_n = U_n(a, 1)$ and $V_n = V_n(a, 1)$. Substituting (17) in Proposition 4, we obtain the relations

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

First, we derive some results which will be useful in the proof of the main theorem. Recall that by (7) we have $U_{-n} = -\frac{1}{b^n} U_n$, and $V_{-n} = \frac{1}{b^n} V_n$, which for $b = 1$ and $n = 1$ gives $U_{-1} = -U_1 = -1$ and $V_{-1} = -V_1 = a$.

Lemma 12. *Consider the integers a, s, k and n, and let D be an odd number relatively prime with n. The following identities hold:*

$$U_{(k+1)s-\left(\frac{n}{D}\right)} = \left(\frac{n}{D}\right) \left[U_s U_{ks} - U_{s-\left(\frac{n}{D}\right)} U_{ks-\left(\frac{n}{D}\right)}\right], \tag{41}$$

$$U_{(k+1)s} = \left(\frac{n}{D}\right) \left[aU_s U_{ks} - U_s U_{ks-\left(\frac{n}{D}\right)} - U_{s-\left(\frac{n}{D}\right)} U_{ks}\right]. \tag{42}$$

Proof. Applying Lemma 1 part 1° for $m = s - \left(\frac{n}{D}\right)$, $M = ks - \left(\frac{n}{D}\right)$, $r = -\left(\frac{n}{D}\right)$, and $R = (k+1)s - \left(\frac{n}{D}\right)$, we obtain

$$U_{s-\left(\frac{n}{D}\right)} U_{ks-\left(\frac{n}{D}\right)} - U_{-\left(\frac{n}{D}\right)} U_{(k+1)s-\left(\frac{n}{D}\right)} = U_s U_{ks}. \tag{43}$$

For $b = 1$ we have $U_{-\left(\frac{n}{D}\right)} = -\left(\frac{n}{D}\right)$, hence (41) holds.

Similarly, using $m = s$, $M = ks + 1$, $r = 1$, $R = (k+1)s$ in (8), we get

$$U_{(k+1)s} = U_s U_{ks+1} - U_{s-1} U_{ks}. \tag{44}$$

From the recurrence (1) satisfied by U_n for $b = 1$, one obtains

$$\begin{aligned} U_{ks+1} &= aU_{ks} - U_{ks-1}, & \qquad U_{ks-1} &= aU_{ks} - U_{ks+1} \\ U_{s+1} &= aU_s - U_{s-1}, & \qquad U_{s-1} &= aU_s - U_{s+1}. \end{aligned}$$

The following two cases are possible.

Case 1. If $\left(\frac{n}{D}\right) = 1$, then

$$\begin{aligned} U_{(k+1)s} &= U_s \left[aU_{ks} - U_{ks-\left(\frac{n}{D}\right)}\right] - U_{ks} U_{s-\left(\frac{n}{D}\right)} \\ &= aU_s U_{ks} - U_s U_{ks-\left(\frac{n}{D}\right)} - U_{ks} U_{s-\left(\frac{n}{D}\right)}. \end{aligned}$$

Case 2. If $\left(\frac{n}{D}\right) = -1$, then

$$\begin{aligned} U_{(k+1)s} &= U_s U_{ks-\left(\frac{n}{D}\right)} - U_{ks} \left[aU_s - U_{s-\left(\frac{n}{D}\right)}\right] \\ &= -aU_s U_{ks} + U_s U_{ks-\left(\frac{n}{D}\right)} + U_{s-\left(\frac{n}{D}\right)} U_{ks}. \end{aligned}$$

The two cases are summarised in the unitary formula (42). $\square$

Some particular instances of Lemma 12 present special interest. We show the relations obtained for $s = n$ and $k = 1, 2$ (the case $k = 0$ is trivial).

$$\begin{aligned} U_{2n-\left(\frac{n}{D}\right)} &= \left(\frac{n}{D}\right)\left[U_n^2 - U^2_{n\left(\frac{n}{D}\right)}\right], \\ U_{2n} &= \left(\frac{n}{D}\right)\left[aU_n^2 - 2U_n U_{n-\left(\frac{n}{D}\right)}\right] \\ U_{3n-\left(\frac{n}{D}\right)} &= \left(\frac{n}{D}\right)\left[U_n U_{2n} - U_{n-\left(\frac{n}{D}\right)} U_{2n-\left(\frac{n}{D}\right)}\right], \\ U_{3n} &= \left(\frac{n}{D}\right)\left[aU_n U_{2n} - U_n U_{2n-\left(\frac{n}{D}\right)} - U_{n-\left(\frac{n}{D}\right)} U_{2n}\right]. \end{aligned}$$

Under the supplementary assumptions $n \mid U_{n-\left(\frac{n}{D}\right)}$ and $n \mid U_n^2 - 1$ (linked to Definitions 5 and 6), one obtains the following congruences

$$\begin{aligned} &U_{2n-\left(\frac{n}{D}\right)} \equiv \left(\frac{n}{D}\right) U_1 \pmod{n}, \quad U_{2n} \equiv \left(\frac{n}{D}\right) U_2 \pmod{n} \\ &U_{3n-\left(\frac{n}{D}\right)} \equiv U_2 U_n \pmod{n}, \quad U_{3n} = U_3 U_n \pmod{n}. \end{aligned} \tag{45}$$

We now investigate some identities modulo a composite number. Recall that a is odd, $D = a^2 - 4$, while $U_0 = 0$, $U_1 = 1$, $U_2 = a$ and $U_3 = a^2 - 1$.

Theorem 13. *Let a and $n > 0$ be odd integers such that n and D are coprime. If $n \mid U_{n-\left(\frac{n}{D}\right)}$ and $n \mid U_n^2 - 1$, then for all positive integers k, we have:*

$$U_{(2k-1)n-\left(\frac{n}{D}\right)} \equiv U_{2k-2} U_n \pmod{n}, \tag{46}$$

$$U_{(2k-1)n} \equiv U_{2k-1} U_n \pmod{n}, \tag{47}$$

and also,

$$U_{(2k)n-\left(\frac{n}{D}\right)} \equiv \left(\frac{n}{D}\right) U_{2k-1} \pmod{n}, \tag{48}$$

$$U_{(2k)n} \equiv \left(\frac{n}{D}\right) U_{2k} \pmod{n}. \tag{49}$$

Proof. By the hypothesis, using $t = k$ and $n = s$ in (41) and (42) we get

$$U_{(t+1)n-\left(\frac{n}{D}\right)} \equiv \left(\frac{n}{D}\right) U_{tn} U_n \pmod{n}, \tag{50}$$

$$U_{(t+1)n} \equiv \left(\frac{n}{D}\right)\left[aU_{tn} - U_{tn-\left(\frac{n}{D}\right)}\right] U_n \pmod{n}. \tag{51}$$

We prove (46), (47), (48) and (49) by induction in $k \geq 1$. The anchor step $k = 1$ clearly follows by (45) and the relation below

$$\begin{aligned} U_{n-\left(\frac{n}{D}\right)} &\equiv 0 \equiv \left(\frac{n}{D}\right) U_0 U_n \pmod{n}, \\ U_n &\equiv U_1 U_n \pmod{n}. \end{aligned}$$

For the induction step, assume that (46), (47), (48) and (49) hold for $1, \dots, k$, and we prove that they also hold for $k+1$. Indeed, substituting $t = 2k$ and $t = 2k+1$ in (50), the following relations hold

$$\begin{aligned} U_{(2k+1)n-\left(\frac{n}{D}\right)} &\equiv \left(\frac{n}{D}\right) U_{(2k)n} U_n \equiv \left(\frac{n}{D}\right) \left[\left(\frac{n}{D}\right) U_{2k}\right] U_n \equiv U_{2k} U_n \pmod{n}, \\ U_{(2k+2)n-\left(\frac{n}{D}\right)} &\equiv \left(\frac{n}{D}\right) U_{(2k+1)n} U_n \equiv \left(\frac{n}{D}\right) \left(U_{2k+1} U_n\right) U_n \pmod{n} \\ &\equiv \left(\frac{n}{D}\right) U_{2k+1} \pmod{n}. \end{aligned}$$

At the same time, by using $t = 2k$ and $t = 2k+1$ in (51) we deduce that

$$\begin{aligned} U_{(2k+1)n} &\equiv \left(\frac{n}{D}\right) \left[a U_{(2k)n} - U_{(2k)n-\left(\frac{n}{D}\right)}\right] U_n \pmod{n} \\ &\equiv \left(\frac{n}{D}\right) \left[a \left(\frac{n}{D}\right) U_{2k} - \left(\frac{n}{D}\right) U_{2k-1}\right] U_n \pmod{n} \\ &\equiv U_{2k+1} U_n \pmod{n}, \\ U_{(2k+2)n} &\equiv \left(\frac{n}{D}\right) \left[a U_{(2k+1)n} - U_{(2k+1)n-\left(\frac{n}{D}\right)}\right] U_n \pmod{n} \\ &\equiv \left(\frac{n}{D}\right) \left[a U_{2k+1} U_n - U_{2k} U_n\right] U_n \pmod{n} \\ &\equiv \left(\frac{n}{D}\right) U_{2k+2} \pmod{n}. \end{aligned}$$

This ends the proof. $\square$

Similarly, we derive some useful results for V_n, used in the proof of a related theorem. Recall that by (7), $U_{-n} = -\frac{1}{b^n} U_n$, and $V_{-n} = \frac{1}{b^n} V_n$, which for $b = 1$ and $n = 1$ gives $U_{-1} = -U_1 = -1$ and $V_{-1} = -V_1 = a$.

Lemma 14. *Consider the integers a, s, k and n, and let D be an odd number relatively prime with n. The following identities hold:*

$$V_{(k+1)s-\left(\frac{n}{D}\right)} = \left(\frac{n}{D}\right) \left[U_s V_{ks} - U_{s-\left(\frac{n}{D}\right)} V_{ks-\left(\frac{n}{D}\right)}\right], \tag{52}$$

$$V_{(k+1)s} = \left(\frac{n}{D}\right) \left[a U_s V_{ks} - U_s V_{ks-\left(\frac{n}{D}\right)} - U_{s-\left(\frac{n}{D}\right)} V_{ks}\right]. \tag{53}$$

Proof. Applying Lemma 1 part 5° for $m = s - \left(\frac{n}{D}\right)$, $M = ks - \left(\frac{n}{D}\right)$, $r = -\left(\frac{n}{D}\right)$, and $R = (k+1)s - \left(\frac{n}{D}\right)$, when $b = 1$ we obtain

$$U_{s-\left(\frac{n}{D}\right)} V_{ks-\left(\frac{n}{D}\right)} - U_{-\left(\frac{n}{D}\right)} V_{(k+1)s-\left(\frac{n}{D}\right)} = U_s V_{ks}. \tag{54}$$

Since we have $U_{-\left(\frac{n}{D}\right)} = -\left(\frac{n}{D}\right)$, (52) holds.

Similarly, for $m = s$, $M = ks + 1$, $r = 1$, and $R = (k+1)s$, we obtain

$$V_{(k+1)s} = U_s V_{ks+1} - U_{s-1} V_{ks}. \tag{55}$$

From the recurrence (2) satisfied by V_n, when $b = 1$ one obtains

$$\begin{aligned} V_{ks+1} &= aV_{ks} - V_{ks-1}, & V_{ks-1} &= aV_{ks} - V_{ks+1} \\ V_{s+1} &= aV_s - V_{s-1}, & V_{s-1} &= aV_s - V_{s+1}. \end{aligned}$$

The following two cases are possible.
Case 1. If $\left(\frac{n}{D}\right) = 1$, then

$$\begin{aligned} V_{(k+1)s} &= U_s \left[aV_{ks} - V_{ks-\left(\frac{n}{D}\right)} \right] - U_{s-\left(\frac{n}{D}\right)} V_{ks} \\ &= aU_s V_{ks} - U_s V_{ks-\left(\frac{n}{D}\right)} - U_{s-\left(\frac{n}{D}\right)} V_{ks}. \end{aligned}$$

Case 2. If $\left(\frac{n}{D}\right) = -1$, then

$$\begin{aligned} V_{(k+1)s} &= U_s V_{ks-\left(\frac{n}{D}\right)} - \left[aU_s - U_{s-\left(\frac{n}{D}\right)} \right] V_{ks} \\ &= -aU_s V_{ks} + U_s V_{ks-\left(\frac{n}{D}\right)} + U_{s-\left(\frac{n}{D}\right)} V_{ks}. \end{aligned}$$

The two cases are summarised in the unitary formula (53). □

Some particular examples from Lemma 14 present special interest. We show here the relations obtained when $s = n$ and $k = 0, 1, 2$. Recall that $V_0 = 2$, $V_1 = a$, $V_2 = a^2 - 2$, $V_3 = a^3 - 3a$ and $V_{-\left(\frac{n}{D}\right)} = a$.

$$\begin{aligned} V_{n-\left(\frac{n}{D}\right)} &= \left(\frac{n}{D}\right) \left[U_n V_0 - U_{n-\left(\frac{n}{D}\right)} V_{-\left(\frac{n}{D}\right)} \right] = \left(\frac{n}{D}\right) \left[V_0 U_n - V_1 U_{n-\left(\frac{n}{D}\right)} \right], \\ V_n &= \left(\frac{n}{D}\right) \left[aU_n V_0 - U_n V_{-\left(\frac{n}{D}\right)} - U_{n-\left(\frac{n}{D}\right)} V_0 \right] = \left(\frac{n}{D}\right) \left[V_1 U_n - V_0 U_{n-\left(\frac{n}{D}\right)} \right] \\ V_{2n-\left(\frac{n}{D}\right)} &= \left(\frac{n}{D}\right) \left[U_n V_n - U_{n-\left(\frac{n}{D}\right)} V_{n-\left(\frac{n}{D}\right)} \right], \\ V_{2n} &= \left(\frac{n}{D}\right) \left[aU_n V_n - U_n V_{n-\left(\frac{n}{D}\right)} - U_{n-\left(\frac{n}{D}\right) V_n} \right], \\ V_{3n-\left(\frac{n}{D}\right)} &= \left(\frac{n}{D}\right) \left[U_n V_{2n} - U_{n-\left(\frac{n}{D}\right)} V_{2n-\left(\frac{n}{D}\right)} \right], \\ V_{3n} &= \left(\frac{n}{D}\right) \left[aU_n V_{2n} - U_n V_{2n-\left(\frac{n}{D}\right)} - U_{n-\left(\frac{n}{D}\right) V_{2n}} \right]. \end{aligned}$$

Under the supplementary assumptions $n \mid U_{n-\left(\frac{n}{D}\right)}$ and $n \mid U_n^2 - 1$ (linked to Definitions 5 and 6), one obtains the following congruences

$$V_{n-\left(\frac{n}{D}\right)} \equiv \left(\frac{n}{D}\right) V_0 U_n \pmod{n}, \quad V_n \equiv \left(\frac{n}{D}\right) V_1 U_n \pmod{n}, \tag{56}$$

$$V_{2n-\left(\frac{n}{D}\right)} \equiv V_1 \pmod{n}, \quad V_{2n} \equiv V_2 \pmod{n}, \tag{57}$$

$$V_{3n-\left(\frac{n}{D}\right)} \equiv \left(\frac{n}{D}\right) V_2 U_n \pmod{n}, \quad V_{3n} \equiv \left(\frac{n}{D}\right) V_3 \left(\frac{n}{D}\right) U_n \pmod{n}.$$

We now investigate relations modulo a composite number, with $D = a^2 - 4$.

Theorem 15. *Let a and $n > 0$ be odd integers such that n and D are coprime. If $n \mid U_{n-\left(\frac{n}{D}\right)}$ and $n \mid U_n^2 - 1$, then for all positive integers k, we have:*

$$V_{(2k-1)n-\left(\frac{n}{D}\right)} \equiv \left(\frac{n}{D}\right) V_{2k-2} U_n \pmod{n}, \tag{58}$$

$$V_{(2k-1)n} \equiv \left(\frac{n}{D}\right) V_{2k-1} U_n \pmod{n}, \tag{59}$$

and also,

$$V_{(2k)n-\left(\frac{n}{D}\right)} \equiv V_{2k-1} \pmod{n}, \tag{60}$$

$$V_{(2k)n} \equiv V_{2k} \pmod{n}. \tag{61}$$

Proof. By the hypothesis, using $t = k$ and $n = s$ in (52) and (53) we get

$$V_{(t+1)n-\left(\frac{n}{D}\right)} \equiv \left(\frac{n}{D}\right) V_{tn} U_n \pmod{n}, \tag{62}$$

$$V_{(t+1)n} \equiv \left(\frac{n}{D}\right) \left[a V_{tn} - V_{tn-\left(\frac{n}{D}\right)}\right] U_n \pmod{n}. \tag{63}$$

We now prove the relations (58), (59), (60), (61) by induction in $k \geq 1$. The anchor step $k = 1$ follows directly by (56) and (57).

For the induction step, we assume that (58), (59), (60), (61) hold for $1, \ldots, k$, and we prove that they also hold for $k+1$. Substituting $t = 2k$ in (62) and (63), by the induction hypothesis we get

$$\begin{aligned} V_{(2k+1)n-\left(\frac{n}{D}\right)} &\equiv \left(\frac{n}{D}\right) V_{(2k)n} U_n \equiv \left(\frac{n}{D}\right) V_{2k} U_n \pmod{n}, \\ V_{(2k+1)n} &\equiv \left(\frac{n}{D}\right) \left[a V_{(2k)n} - V_{(2k)n-\left(\frac{n}{D}\right)}\right] U_n \pmod{n} \\ &\equiv \left(\frac{n}{D}\right) \left[a V_{2k} - V_{2k-1}\right] U_n \equiv \left(\frac{n}{D}\right) V_{2k+1} U_n \pmod{n}. \end{aligned}$$

Also, using $t = 2k+1$ in (62) and (63), by the hypotheses we deduce

$$\begin{aligned} V_{(2k+2)n-\left(\frac{n}{D}\right)} &\equiv \left(\frac{n}{D}\right) V_{(2k+1)n} U_n \equiv \left(V_{2k+1} U_n\right) U_n \equiv V_{2k+1} \pmod{n}, \\ V_{(2k+2)n} &\equiv \left(\frac{n}{D}\right) \left[a V_{(2k+1)n} - V_{(2k+1)n-\left(\frac{n}{D}\right)}\right] U_n \pmod{n} \\ &\equiv \left(\frac{n}{D}\right) \left[a \left(\frac{n}{D}\right) V_{2k+1} U_n - \left(\frac{n}{D}\right) V_{2k} U_n\right] U_n \pmod{n} \\ &\equiv \left(\frac{n}{D}\right)^2 \left[a V_{2k+1} - V_{2k}\right] U_n^2 \equiv V_{2k+2} \pmod{n}. \end{aligned}$$

This ends the proof. □

4 Results on pseudoprimality of level k

In this section we use the arithmetic properties proved earlier, to establish connections between the generalized Lucas and Pell-Lucas pseudoprimes of levels k^- and k^+ defined in [4] and [5]. We start with some preliminaries.

Fibonacci and Lucas pseudoprimes of level k

For a prime p, the following relations hold

$$F_p \equiv \left(\frac{p}{5}\right) \pmod{p}, \quad F_{p-\left(\frac{p}{5}\right)} \equiv 0 \pmod{p}. \tag{64}$$

A composite integer n is called a **Fibonacci pseudoprime** if $n \mid F_{n-\left(\frac{n}{5}\right)}$. The odd Fibonacci pseudoprimes indexed $A081264$ in OEIS [17] start with

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

For $k \geq 1$ integer, the set of **Fibonacci pseudoprimes of level** k and denoted by $\mathcal{F}_k$ consists of all the composite integers n satisfying [8]:

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

Proposition 1 in [8] states that if $\gcd(n, 10) = 1$, 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 [4] we have proved that if n is a composite integer with $\gcd(n, 10) = 1$ and $n \in \mathcal{F}_1$, then $n \in \mathcal{F}_2$ if and only if $n \mid F_n^2 - 1$. We have also provided a counterexample, showing that $n = 323$ is the first composite integer for which $n \in \mathcal{F}_1$ and $n \mid F_n^2 - 1$, but $n \notin \mathcal{F}_3$.

Here $D = 5$, $\left(\frac{n}{5}\right) = -1$ and the calculations involving large numbers are implemented using Matlab's *vpi* (variable precision integer) library.

$$\begin{aligned}
F_{324} = {} & 23041483585524168262220906489 \\
& 64201807510161746678049679057369028996 8
\end{aligned}$$

$$\begin{aligned}
F_{324} &= 230414835855241682622209064 8\\
&\quad 964201807510161746678049679057369028996 8\\
F_{647} &= 73369952779993091352807862470137544645640492430927104043499069001 4\\
&\quad 584668246528603476477043108568806527592562210693671820824200536283472\\
F_{970} &= 2336286181815299653746750781129919541766943951168971092522786214 2\\
&\quad 275523753399638967783310781704529676533897971172191948004316934631842\\
&\quad 045065771638088947558424515687624190113122357319209227560059859345334.
\end{aligned}$$

For a prime number p, the following congruences hold

$$L_p \equiv 1 \pmod{p}, \quad L_{p-\left(\frac{p}{5}\right)} \equiv 2\left(\frac{p}{5}\right) \pmod{p}. \tag{65}$$

We recall that a composite integer satisfying $n \mid L_n - 1$ is called a **Bruckman-Lucas pseudoprime**, whose set was proved to be infinite in 1964 by Lehmer [14]. The composite integers which also satisfy $n \mid F_{n-\left(\frac{n}{5}\right)}$ are called **Fibonacci-Bruckman-Lucas pseudoprimes**, proved to be infinite in [9]. The infinity of sets of pseudoprimes related to other notions in this paper was proved in 2021 by Grantham [13].

In [5], the congruences (65) involving Lucas numbers modulo a prime led to the concept of **Lucas pseudoprimes of level** k denoted by $\mathcal{L}_k$, defined for $k \geq 1$, consisting of the composite numbers n satisfying

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

For these numbers we have proved that if n is a composite integer which is coprime with 10, then if $n \in \mathcal{L}_1$, then $n \in \mathcal{L}_2$ if and only if $n \mid F_n^2 - 1$. Moreover, we have shown that $n = 323$ is also the first composite integer n for which $n \in \mathcal{L}_1$ and $n \mid F_n^2 - 1$, but $n \notin \mathcal{L}_3$.

Furthermore, in the same paper we have introduced the generalized Lucas pseudoprimes of levels k^- (defined for $b = -1$) and k^+ (defined for $b = 1$), and calculated many novel related integer sequences obtained for $k = 1, 2, 3$ and $a = 1, 3, 5, 7$, indexed in the OEIS [17] by us.

Finally, we have also proved that when $n \mid U_n^2 - 1$ (see Definition 6), the pseudoprimes of level 1 (i.e., the classical pseudoprime numbers satisfying Definitions 5 or 7) are also of level 2, but not always of level 3, providing numerous counterexamples and conjectures.

We here use the results in Section 3 to establish further inclusions.

In what follows a, k and n are non-negative integers with a and n odd.

4.1 Results for U_n and $b = -1$

The set $\mathcal{U}_k^-(a)$ of **generalised Lucas pseudoprimes of level** k^- **and parameter** a contains the odd composite integers n satisfying the relation

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

We recall a result linking $\mathcal{U}_1^-(a)$ and $\mathcal{U}_2^-(a)$ with the property $n \mid U_n^2 - 1$.

Proposition 16 ([4], Theorem 4.3)**.** *Let $a, n > 0$ be odd integers with $\gcd(D, n) = 1$. If $n \in \mathcal{U}_1^-(a)$, then $n \in \mathcal{U}_2^-(a)$ if and only if $n \mid U_n^2 - 1$.*

By Theorem 9 we deduce the following general result.

Theorem 17. *Let $a, n > 0$ be odd integers with $\gcd(D, n) = 1$, and let k be a positive integer. If $n \in \mathcal{U}_1^-(a)$ and $n \mid U_n^2 - 1$, then $n \in \mathcal{U}_{2k}^-(a)$.*

Proof. Since $U_0 = 0$, notice that $n \in \mathcal{U}_1^-(a)$ is equivalent to $n \mid U_{n-\left(\frac{n}{D}\right)}$. As Theorem 9 hypotheses are fulfilled, by (25) we have $U_{(2k)n-\left(\frac{n}{D}\right)} \equiv U_{2k-1} \pmod{n}$, that is equivalent to $n \in \mathcal{U}_{2k}^-(a)$. $\square$

By Proposition 16 we also deduce the following property.

Corollary 18. *Let $a, n > 0$ be odd integers with $\gcd(D, n) = 1$, and let $k \geq 2$ be a positive integer. If $n \in \mathcal{U}_1^-(a)$ and $n \in \mathcal{U}_2^-(a)$, then $n \in \mathcal{U}_{2k}^-(a)$.*

When $a = 1$ the set $\mathcal{U}_k^-(a)$ consists of the Fibonacci pseudoprimes of level k denoted $n \in \mathcal{F}_k$, and one has the following result.

Corollary 19. *If n is a composite integer with $\gcd(n, 10) = 1$, then if $n \in \mathcal{F}_1$ and $n \mid F_n^2 - 1$, then for all integers $k \geq 1$ we have $n \in \mathcal{F}_{2k}$.*

The inclusions obtained between the first few sets $\mathcal{F}_k$ in the previous corollary are strict. As noted in [5], the sequence $\mathcal{F}_1$ of Fibonacci pseudoprimes indexed $A081264$ in OEIS [17] starting with

$$323, 377, 1891, 3827, 4181, 5777, 6601, 6721, 8149, 10877, 11663, 13201, 13981,$$
$$15251, 17119, 17711, 18407, 19043, 23407, 25877, 27323, 30889, 34561, \ldots,$$

while the sequence $\mathcal{F}_2$ indexed $A340118$ is given by

$$323, 377, 609, 1891, 3081, 3827, 4181, 5777, 5887, 6601, 6721, 8149, 10877, 11663,$$
$$13201, 13601, 13981, 15251, 17119, 17711, 18407, 19043, 23407, 25877, 27323, \ldots.$$

The intersection $\mathcal{F}_1 \cap \mathcal{F}_2$ starting with the elements

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

was proven to be included in the sequence $\mathcal{F}_4$ starting with

$$21, 33, 323, 329, 377, 451, 861, 1081, 1463, 1819, 1891, 2033, 2211, 3383, 3647,$$
$$3653, 3741, 3827, 4089, 4163, 4181, 4323, 5071, 5671, 5777, 6083, 6541, 6601, \ldots$$

but this also contains new terms like 21, 33, or 329.

4.2 Results for V_n and $b = -1$

The set $\mathcal{V}_k^-(a)$ of **generalised Pell-Lucas pseudoprimes of level k^- and parameter** a contains the odd composite integers n satisfying the relation

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

By Theorem 11 one can obtain the following result, linking $\mathcal{U}_1^-(a)$, $\mathcal{U}_2^-(a)$, and $\mathcal{V}_{2k}^-(a)$, for positive integers k.

Theorem 20. *Let $a, n > 0$ be odd integers with $\gcd(D, n) = 1$, and let k be a positive integer. If $n \in \mathcal{U}_1^-(a)$ and $n \mid U_n^2 - 1$, then $n \in \mathcal{V}_{2k}^-(a)$.*

Proof. If $n \in \mathcal{U}_1^-(a)$ then we clearly have $n \mid U_{n-\left(\frac{n}{D}\right)} - U_0$, that is $n \mid U_{n-\left(\frac{n}{D}\right)}$.

As the hypotheses in Theorem 11 are fulfilled, by relation (37) it follows that $V_{(2k)n-\left(\frac{n}{D}\right)} \equiv \left(\frac{n}{D}\right) V_{2k-1} \pmod{n}$, hence $n \in \mathcal{V}_{2k}^-(a)$. $\square$

For $a = 1$ one recovers the sets $\mathcal{U}_k^-(1) = \mathcal{F}_k$ and $\mathcal{V}_k^-(1) = \mathcal{L}_k$, the Fibonacci and Lucas pseudoprimes of level k. We have the following result.

Corollary 21. *If n is a composite integer with $\gcd(n, 10) = 1$, then if $n \in \mathcal{F}_1$ and $n \mid F_n^2 - 1$ (or $n \in \mathcal{F}_2$), then for all integers $k \geq 1$ we have $n \in \mathcal{L}_{2k}$.*

The inclusions obtained between the first few sets $\mathcal{L}_k$ in the previous corollary are strict. As noted in [5], the sequence $\mathcal{L}_1$ of Lucas pseudoprimes of level 1 was indexed $A339125$ in OEIS [17], beginning with

$$9, 49, 121, 169, 289, 361, 529, 841, 961, 1127, 1369, 1681, 1849, 2209, 2809, 3481,$$
$$3721, 3751, 4181, 4489, 4901, 4961, 5041, 5329, 5777, 6241, 6721, 6889, 7381,$$
$$7921, 9409, 10201, 10609, 10877, 11449, 11881, 12769, 13201, 15251, 16129, \ldots,$$

while the sequence $\mathcal{L}_2$ indexed $A339517$ started with

$323, 377, 1001, 1183, 1729, 1891, 3827, 4181, 5777, 6601, 6721, 8149, 8841, 10877,$
$11663, 13201, 13981, 15251, 17119, 17711, 18407, 19043, 23407, 25877, \ldots.$

At the same time, the terms of the new sequence $\mathcal{L}_4$ start with

$21, 323, 329, 377, 451, 861, 1081, 1403, 1819, 1891, 2033, 2211, 3653, 3827, 4089,$
$4181, 4407, 4427, 5671, 5777, 6601, 6721, 8149, 8557, 9503, 10877, 11309, 11663,$
$12443, 13201, 13861, 13981, 14701, 15251, 16321, 17119, 17193, 17513, 17711, \ldots$

As proved, one has $\mathcal{F}_1 \cap \mathcal{F}_2 \subseteq \mathcal{L}_2$ and $\mathcal{F}_1 \cap \mathcal{F}_2 \subseteq \mathcal{L}_4$, but the inclusions are not strict, as $\mathcal{L}_2$ also includes $9, 49, 121, \ldots$, while $\mathcal{L}_4$ has $21, 329, 451, \ldots$.

Interestingly, $23407 \in (\mathcal{F}_1 \cap \mathcal{F}_2) \cap (\mathcal{L}_2 \setminus \mathcal{L}_4)$, while it seems that we have the relation $(\mathcal{F}_1 \cap \mathcal{F}_2) \cap (\mathcal{L}_4 \setminus \mathcal{L}_2) = \emptyset$, i.e., $\mathcal{F}_1 \cap \mathcal{F}_2 \cap \mathcal{L}_2 \subseteq \mathcal{F}_1 \cap \mathcal{F}_2 \cap \mathcal{L}_4$.

4.3 Results for U_n and $b = 1$

The set $\mathcal{U}_k^+(a)$ of **generalised Lucas pseudoprimes of level k^+ and parameter a** contains the odd composite integers n satisfying the relation

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

We recall a result linking $\mathcal{U}_1^+(a)$ and $\mathcal{U}_2^+(a)$ with the property $n \mid U_n^2 - 1$.

Proposition 22 ([4], Theorem 4.9)**.** *Let $a, n > 0$ be odd integers satisfying $\gcd(D, n) = 1$. If $n \in \mathcal{U}_1^+(a)$, then $n \in \mathcal{U}_2^+(a)$ if and only if $n \mid U_n^2 - 1$.*

By Theorem 13 we deduce the following result, linking $\mathcal{U}_1^+(a)$, $\mathcal{U}_2^+(a)$, and $\mathcal{V}_{2k}^+(a)$, for positive integers k.

Theorem 23. *Let $a, n > 0$ be odd integers with $\gcd(D, n) = 1$, and let k be a positive integer. If $n \in \mathcal{U}_1^+(a)$ and $n \mid U_n^2 - 1$, then $n \in \mathcal{U}_{2k}^+(a)$.*

Proof. Notice that since $U_0 = 0$, $n \in \mathcal{U}_1^+(a)$ is equivalent to $n \mid U_{n-\left(\frac{n}{D}\right)}$.

As the hypothesis of Theorem 13 is satisfied, by relation (49) it follows that $U_{(2k)n-\left(\frac{n}{D}\right)} \equiv \left(\frac{n}{D}\right) U_{2k-1} \pmod{n}$, that is equivalent to $n \in \mathcal{U}_{2k}^+(a)$. $\square$

As for $b = -1$, by Proposition 22 we also deduce the property.

Corollary 24. *Let $a, n > 0$ be odd integers with $\gcd(D, n) = 1$, and let $k \geq 2$ be a positive integer. If $n \in \mathcal{U}_1^+(a)$ and $n \in \mathcal{U}_2^+(a)$, then $n \in \mathcal{U}_{2k}^+(a)$.*

4.4 Results for V_n and $b = 1$

The set $\mathcal{V}_k^+(a)$ of **generalised Pell-Lucas pseudoprimes of level** k^+ **and parameter** a contains the odd composite integers n satisfying the relation

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

By Theorem 15 the following result can be proved.

Theorem 25. *Let $a, n > 0$ be odd integers with $\gcd(D, n) = 1$, and let $k \geq 1$ be an integer. If $n \in \mathcal{U}_1^+(a)$ and $n \mid U_n^2 - 1$, then $n \in \mathcal{V}_{2k}^+(a)$.*

Proof. If $n \in \mathcal{U}_1^+(a)$ then we clearly have $n \mid U_{n-\left(\frac{n}{D}\right)} - U_0$, that is $n \mid U_{n-\left(\frac{n}{D}\right)}$.

Since the hypotheses in Theorem 15 are satisfied, by relation (60) it follows that $V_{(2k)n-\left(\frac{n}{D}\right)} \equiv V_{2k-1} \pmod{n}$, that is equivalent to $n \in \mathcal{V}_{2k}^+(a)$. □

Note that $U_n(1,-1) = F_n$ and $V_n(1,-1) = L_n$, while $U_n(3,1) = F_{2n}$ ($A001906$) and $V_n(3,1) = L_{2n}$ ($A005248$) are the bisection of Fibonacci and Lucas sequences, respectively. Having tested that the first Fibonacci pseudoprimes given by

$$323, 377, 1891, 3827, 4181, 5777, 6601, 6721, 8149,$$

can be found amongst the elements of $\mathcal{U}_1^+(3)$.

Numerical simulations tested for $n \leq 10000$ suggest that [5]:

$$\mathcal{U}_1^-(1) \subset \mathcal{U}_1^+(3), \quad \mathcal{V}_1^-(1) \subset \mathcal{V}_1^+(3),$$

Further investigations may reveal other unexpected connections between the pseudoprimes of level k mentioned in this paper.

References

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

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

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

[4] D. Andrica, O. Bagdasar, *Pseudoprimality related to the generalised Lucas sequences*, Math. Comput. Simul., **201**, 528–542 (2022)

[5] D. Andrica, O., Bagdasar, *On Generalised Lucas Pseudoprimality of Level k*, Mathematics, **9(8), 838** (2021)

[6] D. Andrica, O. Bagdasar, M. Th. Rassias, *Weak pseudoprimality associated to the generalized Lucas sequences*, In: Approximation and Computation in Science and Engineering, 53–75. Eds. N. J., Daras, Th. M., Rassias, Springer, Cham (2022)

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

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

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

[10] K.-W. Chen, Y.-R. Pan, *Greatest common divisors of shifted Horadam sequences*, J. Integer Sequences, **23**, Article 20.5.8 (2020)

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

[12] J. Grantham, *Frobenius pseudoprimes*, Math. Comp., **70**, 873–891 (2000)

[13] J. Grantham, *Proof of two conjectures of Andrica and Bagdasar*, INTEGERS, **21**, Article A111 (2021)

Vol. 3, Addison Wesley, Second Edition (2003)

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

[15] P. Mihăilescu, M. Th. Rassias, *Public key cryptography, number theory and applications*, EMS Newsletter **86**, 25–30 (2012)

[16] P. Mihăilescu, M. Th. Rassias, *Computational number theory and cryptography*, In: Applications of Mathematics and Informatics in Science and Engineering, 349–373. Ed. N. J. Daras, Springer (2014)

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

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

[19] B. Tams, M. Th. Rassias, P. Mihăilescu, *Current challenges for IT security with focus on Biometry*, In: Computation, Cryptography, and Network Security, 461–491. Ed. N. J. Daras, M. T. Rassias, Springer (2015)

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

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

Ovidiu BAGDASAR
School of Computing and Engineering
University of Derby
Kedleston Road, Derby DE22 1GB, England, UK.
Email: o.bagdasar@derby.ac.uk

Michael Themistocles RASSIAS
Department of Mathematics and Engineering Sciences,
Hellenic Military Academy,
16673 Vari, Attikis, Greece.
Email: mrassias@sse.gr