PERIOD LENGTHS MODULO n AND AVERAGE OF TERMS OF SECOND ORDER LINEAR RECURRENCES

Michal Křížek[1]
Institute of Mathematics, Czech Academy of Sciences, Prague, Czech Republic
krizek@math.cas.cz

Lawrence Somer
Department of Mathematics, Catholic University of America, Washington, D.C.
somer@cua.edu

Received: 7/21/23, Accepted: 3/18/24, Published: 4/8/24

Abstract

We present results concerning when the average of the first n terms of any sequence satisfying a certain second-order linear recurrence is an integer. These results substantially generalize results of Fatehizadeh and Yaqubi concerning the Fibonacci sequence. For particular second-order linear recurrences we also explicitly determine all positive integers n for which the period of this second-order linear recurrence modulo n divides n.

1. Introduction

Let $\{G_n\}$ denote the generalized Fibonacci sequence defined by

$$G_{n+2} = G_{n+1} + G_n, \tag{1.1}$$

with initial terms G_0 and G_1, where G_0 and G_1 are integers. In particular, if $G_0 = 0$ and $G_1 = 1$ we get the classical Fibonacci sequence and denote it by $\{F_n\}$.

We will consider the question of when the average of the first n terms of $\{G_n\}$ starting with $n = 1$ is an integer for all possible values of G_0 and G_1. By induction, it is easily determined that

$$\sum_{i=1}^{n} G_i = G_{n+2} - G_2. \tag{1.2}$$

Let m be a positive integer. Since there are only m^2 possible initial ordered pairs (G_0, G_1) modulo m, it follows that the sequence $\{G_i\}$ is eventually periodic

DOI: 10.5281/zenodo.10944025
[1]The corresponding author

modulo m starting from some term G_{n_0}. Noting that G_{i-1} is uniquely determined by $G_{i-1} = G_{i+1} - G_i$, it is easily seen that $\{G_i\}$ is purely periodic modulo m for all possible initial terms G_0 and G_1. By the recursion relation (1.1) and induction, one sees that

$$G_n = G_0 F_{n-1} + G_1 F_n. \tag{1.3}$$

Let $\pi_G(m)$ denote the period of $\{G_n\}$ modulo m, that is, $\pi_G(m)$ is the least positive integer k such that

$$G_{n+k} \equiv G_n \pmod{m}$$

for all $n \geq 0$. It is easily seen that r is a general period of $\{G_n\}$ modulo m if and only if

$$\pi_G(m) \mid r.$$

It follows from (1.3) that

$$\pi_F(m) \text{ is a general period of } \{G_i\} \text{ modulo } m,$$

where $\pi_F(m)$ is the period of $\{F_n\}$ modulo m.

We observe by (1.2) that

$$\frac{1}{n}\sum_{i=1}^{n} G_i = \frac{1}{n}(G_{n+2} - G_2)$$

is an integer for any initial values G_0 and G_1 if n is equal to a general period of $\{G_i\}$ modulo n, which occurs if

$$\pi_F(n) \mid n.$$

Example 1.1. We observe that $F_{24} = 46368 \equiv 0 \pmod{24}$ and $F_{25} = 75025 \equiv 1 \pmod{24}$. Thus, 24 is equal to a general period of $\{F_n\}$ modulo 24. By inspection, one sees that $\pi_F(24) = 24$. We note by (1.2) that

$$\sum_{i=1}^{24} F_i = F_{26} - F_2 = 121393 - 1 \equiv 0 \pmod{24}.$$

Thus, by our observations above,

$$\sum_{i=1}^{24} G_i = G_{26} - G_2 \equiv 0 \pmod{24}$$

for all generalized Fibonacci sequences $\{G_n\}$ and hence

$$\frac{1}{24}\sum_{i=1}^{24} G_i \text{ is an integer.}$$

In the remainder of this paper, we will investigate when the average of the first n terms of more general second-order linear recurrences is an integer. We will further explore when these second-order linear recurrences are purely periodic modulo m and when the period modulo m of these recurrences is divisible by m. Let $W(a,b)$ denote the sequence satisfying the second-order linear recursion relation

$$W_{n+2} = aW_{n+1} + bW_n \tag{1.4}$$

with discriminant $D = a^2 + 4b$, where a, b, and the initial terms W_0 and W_1 are all integers. We distinguish two recurrences satisfying (1.4), the Lucas sequence $U(a,b)$ with initial terms $U_0 = 0$ and $U_1 = 1$, and the Lucas sequence $V(a,b)$ with initial terms $V_0 = 2$ and $V_1 = a$.

Associated with the recurrence $W(a,b)$ is the characteristic polynomial

$$f(x) = x^2 - ax - b$$

with characteristic roots α and β and discriminant

$$D = a^2 + 4b = (\alpha - \beta)^2.$$

By the Binet formulas,

$$\left.\begin{array}{lll} U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}, & V_n = \alpha^n + \beta^n, & \text{if } D \neq 0, \\ U_n = n\alpha^{n-1}, & V_n = 2\alpha^n, & \text{if } D = 0. \end{array}\right\} \tag{1.5}$$

More generally,

$$W_n = c_\alpha \alpha^n + c_\beta \beta^n \ \text{ if } D \neq 0, \tag{1.6}$$

where

$$c_\alpha = \frac{W_1 - \beta W_0}{\alpha - \beta}, \qquad c_\beta = \frac{\alpha W_0 - W_1}{\alpha - \beta}, \tag{1.7}$$

(see [5, p. 174]), while

$$W_n = (c_1 n + c_2)\alpha^n \ \text{ if } D = 0, \tag{1.8}$$

where

$$c_1 = \frac{W_1 - W_0 \alpha}{\alpha}, \qquad c_2 = W_0, \tag{1.9}$$

see [8, pp. 33–35]. Throughout this article, p will denote a prime, m will denote a positive integer, and n will denote a nonnegative integer. If n is not explicitly given to be a nonnegative integer, we will assume that n is a positive integer.

Lemma 1.1 below follows from the Binet formulas (1.5).

Lemma 1.1. *Consider the Lucas sequences $U(a,b)$ and $V(a,b)$. Then we have:*

(i) $U_{2n} = U_n V_n$.

(ii) $U_{2n+1} = bU_n^2 + U_{n+1}^2$.

(iii) *If* $m \mid n$, *then* $U_m \mid U_n$.

By our argument above, the sequence $W(a,b)$ is purely periodic modulo m if $\gcd(m,b) = 1$ (see also [3, pp. 344–345]). Clearly, if $W(a,b)$ is purely periodic modulo m, then $W(a,b)$ is purely periodic modulo p for each prime divisor p of m.

Consider the recurrence $W(a,b)$ and assume that m is a positive integer such that $\gcd(m,b) = 1$. The (least) period of $W(a,b)$ modulo m, denoted by $\pi_W(m)$, is the least positive integer r such that

$$W_{n+r} \equiv W_n \pmod{m}$$

for all $n \geq n_0$ for some nonnegative integer n_0. We will primarily be interested in the case in which $n_0 = 0$, in which case $W(a,b)$ is purely periodic modulo m. We will usually deal with the period $\pi_U(m)$ of the Lucas sequence $U(a,b)$ modulo m. Since we desire $U(a,b)$ and also $W(a,b)$, in general, to be purely periodic modulo m for all m, we will frequently only consider recurrences $W(a,b)$ for which $b = \pm 1$. The (least) restricted period of the purely periodic recurrence $W(a,b)$ modulo m, denoted by $\rho_W(m)$, is the least positive integer s such that

$$W_{s+n} \equiv MW_n \pmod{m} \tag{1.10}$$

for all $n \geq n_0$ and some integer $M = M_W(m)$ such that $\gcd(M,m) = 1$. Here $M = M_W(m)$ is called the *multiplier of* $W(a,b)$ modulo m. Since $U(a,b)$ is purely periodic modulo m and has initial terms $U_0 = 0$, $U_1 = 1$, it is easily seen that $\pi_U(m)$ is the least positive integer r such that

$$U_r \equiv 0 \pmod{m}, \quad U_{r+1} \equiv 1 \pmod{m}, \tag{1.11}$$

while $\rho_U(m)$ is the smallest positive integer s such that

$$U_s \equiv 0 \pmod{m}, \quad U_{s+1} \equiv MU_1 \equiv M \pmod{m}, \tag{1.12}$$

where $M = M_U(m)$ is the multiplier of $U(a,b)$ modulo m.

Remark 1.1. We now consider the Lucas sequence $U(a,b)$ with $b \neq 0$. Assume that $\gcd(m,b) > 1$. Let p be a prime dividing m such that $\gcd(p,b) > 1$. If $p \nmid a$, then it follows by induction that $p \nmid U_n$ for all $n \geq 1$. If $p \mid a$, then one sees by induction that $p \mid U_n$ for $n \geq 2$. Noting that $U_0 = 0$ and $U_1 = 1$, we see that $U(a,b)$ is not purely periodic modulo p. It now follows that $U(a,b)$ is purely periodic modulo m if and only if $\gcd(m,b) = 1$.

Given the recurrence $W(a,b)$ and the integer m, where $\gcd(m,b) = 1$, it is proved in [3, pp. 354–355] that $\rho_W(m) \mid \pi_W(m)$. Let

$$E_W(m) = \frac{\pi_W(m)}{\rho_W(m)}. \tag{1.13}$$

Then by [3, pp. 354–355], $E_W(m)$ is the multiplicative order of the multiplier $M = M_W(m)$ modulo m. By repeated application of (1.13), we see that if $\rho = \rho_W(m)$, then

$$W_{n+\rho i} \equiv M^i W_n \pmod{m}$$

for all $n \geq 0$ and $i \geq 1$.

Remark 1.2. Consider the recurrence $W(a,b)$ and suppose that $\gcd(m,b) = 1$. It is clear that r is a general period of $W(a,b)$ modulo m and s is a general restricted period of $W(a,b)$ modulo m if and only if

$$\pi_W(m) \mid r \quad \text{and} \quad \rho_W(m) \mid s. \tag{1.14}$$

Remark 1.3. Consider the recurrence $W(a,b)$. Suppose that $\gcd(m,b) = 1$. It is evident that if $m \mid n$, then $\pi_W(n)$ is a general period of $W(a,b)$ modulo m and $\rho_W(n)$ is a general restricted period of $W(a,b)$ modulo m.

Given the recurrences $W(a,b)$ and $U(a,b)$ and the positive integer m, where $\gcd(m,b) = 1$, the following theorem gives a relation between the period of $W(a,b)$ modulo m and the period of $U(a,b)$ modulo m.

Theorem 1.1. *Consider the recurrence $W(a,b)$ and the Lucas sequence $U(a,b)$, where $b \neq 0$. Let m be a positive integer m such that $\gcd(m,b) = 1$. Then $W(a,b)$ and $U(a,b)$ are both purely periodic modulo m. Moreover,*

$$\pi_W(m) \mid \pi_U(m) \quad \textit{and} \quad \rho_W(m) \mid \rho_U(m). \tag{1.15}$$

In particular, $\pi_U(m)$ is a general period of $W(a,b)$ modulo m and $\rho_U(m)$ is a general restricted period of $W(a,b)$ modulo m.

Proof. Since $\gcd(m,b) = 1$, we see by our earlier observations that $W(a,b)$ and $U(a,b)$ are both purely periodic modulo m. It follows by induction that

$$W_n = bW_0U_{n-1} + W_1U_n. \tag{1.16}$$

We now see that (1.15) holds. The last assertion in Theorem 1.1 follows from Remark 1.2. □

Given the positive integer m, we define $\pi_U^i(m)$ iteratively as follows for $i \geq 0$. We let $\pi_U^0(m) = m$ and $\pi_U^{i+1}(m) = \pi_U(\pi_U^i(m))$. We define $\rho_U^i(m)$ similarly for $i \geq 0$. See [11] for a study of the properties of $\pi_U^i(m))$ and $\rho_U^i(m)$.

Theorem 1.2. *Consider the Lucas sequence $U(a,b)$, where $b \neq 0$. Let m and n be positive integers such that $\gcd(mn,b) = 1$. Then*

$$\pi_U(\operatorname{lcm}(m,n)) = \operatorname{lcm}(\pi_U(m), \pi_U(n)) \quad \textit{and} \quad \rho_U(\operatorname{lcm}(m,n)) = \operatorname{lcm}(\rho_U(m), \rho_U(n)), \tag{1.17}$$

where $\operatorname{lcm}(m,n)$ *denotes the least common multiple of* m *and* n*. Furthermore,*

$$\pi_U^i(\operatorname{lcm}(m,n)) = \operatorname{lcm}(\pi_U^i(m), \pi_U^i(n)) \quad \text{and} \quad \rho_U^i(\operatorname{lcm}(m,n)) = \operatorname{lcm}(\rho_U^i(m), \rho_U^i(n)) \tag{1.18}$$

for $i \geq 1$*.*

Proof. Assertion (1.17) follows from (1.14) and Remark 1.3. Then (1.18) follows by induction from (1.14), Remark 1.3, and (1.17). ☐

The recurrence $W(a,b)$ with discriminant D and characteristic roots α and β is called *degenerate* if $ab = 0$ or α/β is a root of unity. Note that $W(a,b)$ is degenerate if $D = 0$. We observe by the Binet formulas (1.5) that $U_n = 0$ for some $n \geq 1$ only if $U(a,b)$ is degenerate. Theorem 1.3 characterizes the degenerate recurrences $W(a,b)$ when $b = \pm 1$ or $(a,b) = (\pm 1, 0)$.

Theorem 1.3. *Consider the recurrences* $W(a,b)$*, where* $b = \pm 1$ *or* $(a,b) = (\pm 1, 0)$*. Then we have:*

(i) $W(a,b)$ *is degenerate if and only if* $(a,b) = (0,1)$, $(0,-1)$, $(1,-1)$, $(-1,-1)$, $(2,-1)$, $(-2,-1)$, $(1,0)$, *or* $(-1,0)$.

(ii) If $(a,b) = (0,1)$*, then* $W_{2n} = W_0$, $W_{2n+1} = W_1$ *for* $n \geq 0$.

(iii) If $(a,b) = (0,-1)$*, then* $W_{4n} = W_0$, $W_{4n+1} = W_1$, $W_{4n+2} = -W_0$, $W_{4n+3} = -W_1$ *for* $n \geq 0$.

(iv) If $(a,b) = (1,-1)$*, then* $W_{6n} = W_0$, $W_{6n+1} = W_1$, $W_{6n+2} = W_1 - W_0$, $W_{6n+3} = -W_0$, $W_{6n+4} = -W_1$, $W_{6n+5} = W_0 - W_1$ *for* $n \geq 0$.

(v) If $(a,b) = (-1,-1)$*, then* $W_{3n} = W_0$, $W_{3n+1} = W_1$, $W_{3n+2} = -W_1 - W_0$ *for* $n \geq 0$.

(vi) If $(a,b) = (2,-1)$*, then* $\alpha = \beta = 1$, $D = 0$, *and* $W_n = nW_1 - (n-1)W_0$ *for* $n \geq 0$.

(vii) If $(a,b) = (-2,-1)$*, then* $\alpha = \beta = -1$, $D = 0$, *and* $W_n = (-1)^{n+1}(nW_1 + (n-1)W_0)$ *for* $n \geq 0$.

(viii) If $(a,b) = (1,0)$*, then* $W_n = W_1$ *for* $n \geq 1$.

(ix) If $(a,b) = (-1,0)$*, then* $W_n = (-1)^{n+1}W_1$ *for* $n \geq 1$.

Proof. Part (i) follows from [13, p. 613]. Parts (ii)–(v) and (viii)–(ix) follow by induction. Parts (vi) and (vii) follow from (1.8) and (1.9). ☐

The following theorem gives results about the restricted period and period of the nondegenerate Lucas sequence $U(a,b)$ modulo n. Given the nonzero integer r, we let $P(r)$ denote the largest prime dividing r with the convention that $P(\pm 1) = 1$.

Theorem 1.4. *Consider the nondegenerate Lucas sequence $U(a, b)$ with discriminant D. Then the following hold.*

(i) If $p \nmid 2bD$, then $\rho_U(p) > 1$ and $\rho(p) \mid p - (D/p)$, where (D/p) is the Legendre symbol. Moreover, if $p \geq 2$, then $\pi_U(p) = \rho_U(p)E_U(p)$, where $E_U(p) \mid p - 1$. Furthermore, if $p = 2$ and $p \nmid bD$, then $\pi_U(p) = 3$.

(ii) If $p \nmid 2bD$, then $\rho_U(p) \mid (p - (D/p))/2$ if and only if $(-b/p) = 1$.

(iii) If $p \nmid b$ and $p \mid D$, then $\rho_U(p) = p$ and $\pi_U(p) \mid p(p - 1)$.

(iv) If $p \nmid 2b$ and $(D/p) = 1$, then $\pi_U(p) \mid p - 1$.

(v) If $p \nmid 2b$ and $(D/p) = -1$, then $\pi_U(p) \mid p^2 - 1$ and $P(\pi_U(p)) \leq (p + 1)/2$.

(vi) If $p \nmid b$ and $p \mid D$, then $P(\pi_U(p)) = p$.

(vii) Suppose that $p \nmid b$. Let $c \geq 1$ be the largest integer such that $\rho_U(p^c) = \rho(p)$. Then c exists. If $p^c \neq 2$, then

$$\rho_U(p^i) = p^{\max(i-c,0)}\rho_U(p)$$

for $i \geq 1$. If $p^c = 2$, let d be the largest integer such that $\rho_U(4) = \rho_U(2^d)$. Then

$$\rho_U(2^i) = 2^{\max(i+1-d,1)}\rho_U(2)$$

for $i \geq 2$.

(viii) Suppose that $p \nmid b$. Let $e \geq 1$ be the largest integer such that $\pi_U(p^e) = \pi(p)$. Then e exists. If $p^e \neq 2$, then

$$\pi_U(p^i) = p^{\max(i-e,0)}\pi_U(p)$$

for $i \geq 1$. Let $p^e = 2$ and let g be the largest integer such that $\pi_U(4) = \pi_U(2^g)$. Then

$$\pi_U(2^i) = 2^{\max(i+1-g,1)}\pi_U(2)$$

for $i \geq 2$.

(ix) $\rho_U(1) = \pi_U(1) = 1$.

Proof. Parts (i)–(iii) are proved in [6, pp. 423 and 441]. Part (iv) is proved in [2, pp. 44–45].

(v) By part (i) and (1.13), $\rho_U(p) \mid p+1$ and $\pi_U(p) = \rho_U(p) \cdot E_U(p)$. Since $E_U(p)$ is the multiplicative order modulo p of the multiplier $M_W(p)$, we see that $E_U(p) \mid p-1$. Thus, $\pi_U(p) \mid (p + 1)(p - 1) = p^2 - 1$. Let q be an odd prime dividing $\pi_U(p)$. Then $q \mid (p + 1)/2$ or $q \mid (p - 1)/2$, since q is odd. Hence, $P(\pi_U(p)) \leq (p + 1)/2$, since $(p + 1)/2 \geq 2$.

(vi) By part (iii) and the proof of part (v), $p \mid \pi_U(p)$, so $p \mid p(p-1)$. It now follows that $P(\pi(p)) = p$.

(vii) and (viii) Since $U(a,b)$ is nondegenerate, $U_n \neq 0$ for $n > 0$. It now follows from (1.11) and (1.12) that c, d, e and g all exist. The rest of part (vii) follows from Theorem X of [2], while the remainder of part (viii) follows from [12, pp. 619–620, 627–628].

(ix) It is evident that $\rho_U(1) = \pi_U(1) = 1$. □

Theorem 1.5. *Let $U(a,b)$ be a nondegenerate Lucas sequence with discriminant D. Suppose that $\gcd(p,b) = 1$, $p \mid D$ and $p \nmid \gcd(a,b)$. Let $\nu_p(m)$ denote the largest nonnegative integer r such that $p^r \mid m$. Then the following hold.*

(i) *$\rho_U(p) = p$ and $U(a,b)$ is uniformly distributed modulo p with each residue (mod p) appearing exactly $E_U(p)$ times in a least period of $U(a,b)$ modulo p.*

(ii) *Suppose that $p \geq 5$ and $i \geq 1$. Then $\rho_U(p^i) = p^i$, $\pi_U(p^i) = p^i E_U(p)$, and $U(a,b)$ is uniformly distributed modulo p^i with each residue (mod p^i) appearing exactly $E_U(p)$ times in the least period of $U(a,b)$ modulo p^i.*

(iii) *Suppose that $p = 2$. Then $U_2 = a \equiv 0 \pmod 2$. Moreover, if $a \equiv 2 \pmod 4$ and $i \geq 1$, then $\rho(2^i) = 2^i$. Furthermore, if $a \equiv 2 \pmod 4$, $i \geq 1$, and $b \equiv -1 \pmod 4$, then $U(a,b)$ is uniformly distributed modulo 2^i with each residue $\pmod{2^i}$ appearing exactly once in the least period of $U(a,b)$ modulo 2^i.*

(iv) *Suppose that $p = 3$. Then $U_3 = a^2 + b \equiv 0 \pmod 3$. Further, if $a^2 + b \not\equiv 0 \pmod 9$ and $i \geq 1$, then $\rho(3^i) = 3^i$ and $U(a,b)$ is uniformly distributed modulo 3^i with each residue $\pmod{p^i}$ appearing exactly $E_U(3)$ times in the least period of $U(a,b)$ modulo 3^i.*

(v) *Suppose that $p = 2$ and $\nu_2(a) = c \geq 2$. Then $\rho_U(2^i) = 2^{\max(i+1-c,1)}$ for $i \geq 1$.*

(vi) *Suppose that $p = 3$ and $\nu_3(a^2+b) = d \geq 2$. Then $\rho_U(3^i) = 3^{\max(i+1-d,1)}$ for $i \geq 1$.*

Proof. Parts (i)–(vi) follow from results in [1] and [14]. □

2. The Main Results

From here on, given the recurrence $W(a,b)$, we let $B_W(n) = \sum_{i=1}^{n} W_i$ and $A_W(n) = \frac{1}{n} B_W(n)$. In Theorem 2.1 below, given the degenerate Lucas sequence $U(a,b)$, where $b = \pm 1$ or 0, we will find positive integers n for which $A_W(n)$ is an integer for all possible recurrences $W(a,b)$.

Theorem 2.1. *Consider the degenerate Lucas sequence $U(a,b)$ and the degenerate recurrence $W(a,b)$, where $b = \pm 1$ or $(a,b) = (\pm 1, 0)$. Let n be an arbitrary positive integer.*

(i) *If $(a,b) = (0,1)$, then $B_U(n) = \lceil n/2 \rceil$. Moreover, $A_W(n)$ is an integer for all recurrences $W(a,b)$ if and only if $n = 1$.*

(ii) *If $(a,b) = (0,-1)$, then $B_W(4n) = 0$ for all recurrences $W(a,b)$. Moreover, $A_W(4n) = 0$ and is an integer for all recurrences $W(a,b)$.*

(iii) *If $(a,b) = (1,-1)$, then $B_W(6n) = 0$ for all recurrences $W(a,b)$. Moreover, $A_W(6n) = 0$ and is an integer for all recurrences $W(a,b)$.*

(iv) *If $(a,b) = (-1,-1)$, then $B_W(3n) = 0$ for all recurrences $W(a,b)$. Moreover, $A_W(3n) = 0$ and is an integer for all recurrences $W(a,b)$.*

(v) *If $(a,b) = (2,-1)$, then $B_W(n) = \frac{1}{2}(W_1 - W_0)n(n+1) + W_0 n$. Moreover, $A_W(n)$ is an integer for all recurrences $W(a,b)$ if and only if $n \equiv 1 \pmod{2}$. In particular, $A_W(2n-1) = n(W_1 - W_0) + W_0$ for $n \geq 1$.*

(vi) *If $(a,b) = (-2,-1)$, then $B_U(n) = (-1)^{n+1}\lceil n/2 \rceil$. Moreover, $A_W(n)$ is an integer for all recurrences $W(a,b)$ if and only if $n = 1$.*

(vii) *If $(a,b) = (1,0)$, then $B_W(n) = nW_1$. Moreover, $A_W(n) = W_1$ and is an integer for $n \geq 1$ for all recurrences $W(a,b)$.*

(viii) *If $(a,b) = (-1,0)$, then $B_W(2n) = 0$ for all recurrences $W(a,b)$. Moreover, $A_W(2n) = 0$ and is an integer for all recurrences $W(a,b)$.*

Proof. Parts (i)–(viii) follow from Theorem 1.3 and induction. □

Theorem 2.2. *Consider the recurrence $W(a,b)$ and the Lucas sequence $U(a,b)$ with characteristic roots α and β, where $bD \neq 0$.*

(i) *If $a + b - 1 \neq 0$, then*

$$B_W(n) = \frac{1}{a+b-1}(W_{n+1} - W_1 + b(W_n - W_0)) = \frac{J(n)}{a+b-1}, \tag{2.1}$$

where $J(n) = W_{n+1} - W_1 + b(W_n - W_0)$. Moreover, if $\gcd(n,b) = 1$ and $\pi_U(n) \mid r$, then $J(r) \equiv 0 \pmod{n}$.

(ii) *If $a + b - 1 = 0$, then*

$$B_W(n) = \frac{1}{-b-1}((W_1 - W_0)U_{n+1} - n(W_1 + bW_0) + W_0 - W_1 = \frac{K(n)}{-b-1}, \tag{2.2}$$

where $K(n) = (W_1 - W_0)U_{n+1} - n(W_1 + bW_0) + W_0 - W_1$. Furthermore, if $\gcd(n,b) = 1$ and $\pi_U(n) \mid s$, then $K(s) \equiv 0 \pmod{n}$.

Proof. Equations (2.1) and (2.2) follow from (1.6)–(1.9), and [5, pp. 176–177]. If $a+b-1 \neq 0$, $\gcd(n,b)=1$, and $\pi_U(n) \mid r$, then r is a general period of $U(a,b)$ modulo n, and consequently, r is also a general period of $W(a,b)$ modulo n by Remark 1.2 and Theorem 1.1. Hence, $W_{r+1} \equiv W_1$ and $W_r \equiv W_0 \pmod{n}$. It follows from (2.1) that $J(r) \equiv 0 \pmod{n}$. Now suppose that $a+b-1=0$, $\gcd(n,b)=1$, and $\pi_U(n) \mid s$. Then s is a general period of $U(a,b)$ modulo n. Hence, $U_{s+1} \equiv U_1 \equiv 1 \pmod{n}$. It now follows from (2.2) that $K(s) \equiv 0 \pmod{n}$. □

Remark 2.1. The formulas given in [5, pp. 176–177] evaluate $\sum_{i=0}^{n} W_i$. We obtain (2.1) and (2.2) by subtracting W_0 from $\sum_{i=0}^{n} W_i$. We observe that if $a+b-1=0$, then either $\alpha = 1$ or $\beta = 1$, where α and β are the characteristic roots of $W(a,b)$ (see [5, p. 176]).

We have the following two corollaries to Theorem 2.2. The first of these corollaries follows immediately from Theorem 2.2.

Corollary 2.1. *Consider the Lucas sequence $U(a,b)$, where $b \neq 0$.*

(i) If $a+b-1 \neq 0$, then

$$B_U(n) = \frac{1}{a+b-1}(U_{n+1} - 1 + bU_n).$$

(ii) If $a+b-1 = 0$, then

$$B_U(n) = \frac{1}{-b-1}(U_{n+1} - 1 - n).$$

Corollary 2.2. *Consider the Lucas sequence $U(a,b)$.*

(i) Let $a+b-1 \neq 0$ and let n be a positive integer such that $\gcd(n, b(a+b-1)) = 1$. Then $U(a,b)$ is purely periodic modulo n. Suppose that $\pi_U(n) \mid r$. Then

$$B_W(r) \equiv 0 \pmod{n}$$

for all recurrences $W(a,b)$.

(ii) Let $a+b-1 = 0$ and let n be a positive integer such that $\gcd(n, b(-b-1)) = 1$. Then $U(a,b)$ is purely periodic modulo n. Suppose that $\pi_U(n) \mid s$. Then

$$B_W(s) \equiv 0 \pmod{n}$$

for all recurrences $W(a,b)$.

Proof. (i) Since $\gcd(b,n)=1$, $W(a,b)$ is purely periodic modulo n for all recurrences $W(a,b)$. We note that r is a general period of $U(a,b)$ modulo n. Then according to Theorem 1.1, r is also a general period of any recurrence $W(a,b)$ modulo n. Since

$\gcd(n, a+b-1) = 1$, it follows from Theorem 2.2 (i) that $B_W(r) \equiv 0 \pmod{n}$ for all recurrences $W(a,b)$.

(ii) We find by the observations in the proof of part (i) that $W(a,b)$ is purely periodic modulo n for all recurrences $W(a,b)$ and that s is a general period of $U(a,b)$ modulo n. Since $\gcd(n, -b-1) = 1$, it follows from Theorem 2.2 (ii) that $B_W(s) \equiv 0 \pmod{n}$ for all recurrences $W(a,b)$. □

Remark 2.2. Given the Lucas sequence $U(a,b)$, where $b \neq 0$, we let $S(U)$ denote the set of all positive integers n such that $\gcd(n,b) = 1$ and $\pi_U(n) \mid n$. By our discussion above, $U(a,b)$ is purely periodic modulo n if $n \in S(U)$, which implies that all recurrences $W(a,b)$ are then purely periodic modulo n. In Theorems 4.2 and 4.3, we explicitly find all members of $S(U)$ for the nondegenerate Lucas sequences $U(a, \pm 1)$, $U(-b+1, b)$, and $U(b-1, b)$. We further let $S'(U)$ denote the set of all positive integers n such that $n \in S(U)$ and $B_U(n) \equiv 0 \pmod{n}$, or equivalently, such that $n \in S(U)$ and $A_U(n)$ is an integer. We note that $1 \in S(U)$ and $1 \in S'(U)$ for any Lucas sequence $U(a,b)$. Given the positive integer n such that $\gcd(n,b) = 1$, we define $C(n)$ to be the least positive integer m, if it exists, such that $n \mid m$ and $m \in S(U)$. We also define $C'(n)$ to be the least positive integer m, if it exists, such that $n \mid m$ and $m \in S'(U)$. We let $T(U)$ denote the set of positive integers n coprime to b such that $n \mid U_n$, or equivalently, $\rho_U(n) \mid n$. Clearly if $n \in S(U)$, then $n \in T(U)$. Theorems 2.3, 2.4, and 2.5 and Corollary 2.3 below present results about elements in $S(U)$ and $S'(U)$ and results concerning $C(n)$ and $C'(n)$.

Theorem 2.3. *Consider the Lucas sequence $U(a,b)$, where $b \neq 0$. Suppose that $n \in S(U)$ and that $p \mid n$. Then $pn \in S_U$. Moreover, pn is also a member of $S'(U)$ and $A_W(pn)$ is an integer for all recurrences $W(a,b)$ if it is the case that $a+b-1 \neq 0$ and $\gcd(a+b-1, n) = 1$, or it is the case that $a+b-1 = 0$ and $\gcd(-b-1, n) = 1$.*

Proof. Since $\gcd(n,b) = 1$, we have that $\gcd(pn, b) = 1$, and $U(a,b)$ is purely periodic modulo pn. Let $n = p^i r$, where $i \geq 1$ and $\gcd(p,r) = 1$. By assumption,

$$\pi_U(n) \mid n. \tag{2.3}$$

By Theorem 1.2,

$$\pi_U(p^i r) = \operatorname{lcm}(\pi_U(p^i), \pi_U(r)). \tag{2.4}$$

By Theorem 1.4 (viii),

$$\pi_U(p^i) \mid \pi_U(p^{i+1}), \text{ so } \quad \pi_U(p^i) \mid p\pi_U(p^i). \tag{2.5}$$

It now follows from (2.3), (2.4), and (2.5) that

$$\pi_U(pn) \mid pn.$$

Hence, $pn \in S(U)$.

Furthermore, suppose that $a + b - 1 \neq 0$ and $\gcd(a + b - 1, n) = 1$. Then $\gcd(a + b - 1, pn) = 1$. It now follows from Theorem 1.2, Theorem 1.4 (viii), and Corollary 2.2 that $np \in S'(U)$ and $A_W(np)$ is an integer for all recurrences $W(a, b)$. Finally, suppose that $a + b - 1 = 0$ and $\gcd(-b - 1, n) = 1$. Then $\gcd(-b-1, pn) = 1$. It again follows that $np \in S'(U)$ and $A_W(np)$ is an integer for all recurrences $W(a, b)$. $\square$

We have the following immediate corollary of Theorem 2.3, which is proved by repeatedly applying Theorem 2.3.

Corollary 2.3. *Consider the Lucas sequence $U(a, b)$, where $b \neq 0$. Suppose that $n \in S(U)$ and that each prime divisor of m divides n. Then $mn \in S(U)$. Moreover, if it is the case that $a + b - 1 \neq 0$ and $\gcd(a + b - 1, n) = 1$ or it is the case that $a + b - 1 = 0$ and $\gcd(-b - 1, n) = 1$, then $mn \in S'(U)$ and $A_W(mn)$ is an integer for all recurrences $W(a, b)$.*

Theorem 2.4. *Consider the Lucas sequence $U(a, b)$, where $b \neq 0$. Suppose that m and $n \in S(U)$. Then $\operatorname{lcm}(m, n)$ and $mn \in S(U)$. Suppose further that it is the case that $a+b-1 \neq 0$ and $\gcd(a+b-1, mn) = 1$ or it is the case that $a+b-1 = 0$ and $\gcd(-b - 1, mn) = 1$. Then m, n, $\operatorname{lcm}(m, n)$, and mn are all members of $S'(U)$. Moreover, $A_W(m)$, $A_W(n)$, $A_W(\operatorname{lcm}(m, n))$, and $A_W(mn)$ are all integers for all recurrences $W(a, b)$. In particular, if r is a positive integer such that $C(r)$ exists and either it is the case that $a + b - 1 \neq 0$ and $\gcd(a + b - 1, C(r)) = 1$ or it is the case that $a+b-1 = 0$ and $\gcd(-b-1, C(r)) = 1$, then $C(r) = C'(r)$ and $A_W(C(r))$ is an integer for all recurrences $W(a, b)$.*

Proof. We first show that $\operatorname{lcm}(m, n) \in S(U)$. We observe that $\gcd(\operatorname{lcm}(m, n), b) = 1$, because $\gcd(m, b) = \gcd(n, b) = 1$. Since $\pi_U(m) \mid m$ and $\pi_U(n) \mid n$, it follows from Theorem 1.2 that

$$\pi_U(\operatorname{lcm}(m, n)) = \operatorname{lcm}(\pi_U(m), \pi_U(n)) \mid \operatorname{lcm}(m, n).$$

Thus, $\operatorname{lcm}(m, n) \in S(U)$.

We now demonstrate that $mn \in S(U)$. Let $n = n_1 n_2$, where n_2 is the largest factor of n that is relatively prime to m. Then $mn_1 \in S(U)$ by Corollary 2.3. Since $\gcd(mn_1, n_2) = 1$, it follows by our argument above that $mn = mn_1 n_2 \in S(U)$.

Finally, suppose that it is the case that $a + b - 1 \neq 0$ and $\gcd(a + b - 1, mn) = 1$ or it is the case that $a + b - 1 = 0$ and $\gcd(-b - 1, mn) = 1$. It then follows from Corollary 2.2 that m, n, $\operatorname{lcm}(m, n)$, and mn are all members of $S'(U)$, and that each of $A_W(m)$, $A_W(n)$, $A_W(\operatorname{lcm}(m, n))$, and $A_W(mn)$ is an integer for all recurrences $W(a, b)$. The last assertion follows, since $C(r) \in S(U)$ and $C'(r) \in S'(U)$ by definition. $\square$

Theorem 2.5. *Consider the Lucas sequence $U(a,b)$, where $b \neq 0$. Suppose that m and $n \in S'(U)$ and $m \mid r$. Then $B_U(r) \equiv 0 \pmod{m}$. Moreover, $\operatorname{lcm}(m,n) \in S'(U)$. Furthermore, $A_W(m)$, $A_W(n)$, and $A_W(\operatorname{lcm}(m,n))$ are all integers for all recurrences $W(a,b)$. Additionally, $B_W(r) \equiv 0 \pmod{m}$ for all recurrences $W(a,b)$.*

Proof. It follows from the definition of $S'(U)$ that $\gcd(m,b) = 1$, $\pi_U(m) \mid m$, and $B_U(m) \equiv 0 \pmod{m}$. Suppose that $m \mid r$. Then m and r are both general periods of $U(a,b)$ modulo m. It now follows that

$$B_U(r) \equiv (r/m)B_U(m) \equiv (r/m) \cdot 0 \equiv 0 \pmod{m}.$$

Since $m \in S'(U)$, $n \in S'(U)$, $m \mid \operatorname{lcm}(m,n)$, and $n \mid \operatorname{lcm}(m,n)$, we see by our argument above that

$$B_U(\operatorname{lcm}(m,n)) \equiv 0 \pmod{m} \quad \text{and} \quad B_U(\operatorname{lcm}(m,n)) \equiv 0 \pmod{n}.$$

Hence,

$$B_U(\operatorname{lcm}(m,n)) \equiv 0 \pmod{\operatorname{lcm}(m,n)}.$$

Since $\operatorname{lcm}(m,n) \in S(U)$ by Theorem 2.4, we have that $\operatorname{lcm}(m,n) \in S'(U)$.

Now suppose that $m \in S'(U)$ and $W(a,b)$ is an arbitrary recurrence. Next we show that $A_W(m)$ is an integer. Noting that m is also in $S(U)$, we have that $U(a,b)$ is purely periodic modulo m and m is equal to a general period of $U(a,b)$ modulo m. Then $U_m \equiv U_0 \equiv 0 \pmod{m}$. Let $W(a,b)$ be an arbitrary recurrence. Then, by (1.16),

$$W_m = bW_0U_{m-1} + W_1U_m. \tag{2.6}$$

Noting that $U_m \equiv U_0 \equiv 0 \pmod{m}$ and $B_U(m) \equiv 0 \pmod{m}$, we find that

$$\sum_{i=1}^{m} U_i \equiv \sum_{i=1}^{m} U_{i-1} \equiv 0 \pmod{m}. \tag{2.7}$$

Hence, by (2.6) and (2.7),

$$\sum_{i=1}^{m} W_i \equiv bW_0 \sum_{i=1}^{m} U_{i-1} + W_1 \sum_{i=1}^{m} U_i \equiv bW_0 \cdot 0 + W_1 \cdot 0 \equiv 0 \pmod{m}. \tag{2.8}$$

It now follows from (2.8) that $A_W(m)$ is an integer. Since m and r are both general periods of $W(a,b)$ modulo m and $W(a,b)$ is purely periodic modulo m by Theorem 1.1, we see by (2.8) and our above argument that $B_W(r) \equiv 0 \pmod{m}$. □

Remark 2.3. By Theorem 2.5, given the ordered pair of integers (a,b) such that $b \neq 0$, if $n \in S(U)$ and one wishes to demonstrate that $A_W(n)$ is an integer for all recurrences $W(a,b)$, it suffices to show that $B_U(n) \equiv 0 \pmod{n}$, which implies that $A_U(n)$ is an integer for the Lucas sequence $U(a,b)$. In particular, if $C'(n)$ exists, then $A_W(C'(n))$ is an integer for all recurrences $W(a,b)$. We also note that in Theorem 2.5, we do not necessarily assume that $\gcd(a+b-1,n) = 1$ if $a+b-1 \neq 0$ or that $\gcd(-b-1,n) = 1$ if $a+b-1 = 0$ as in Theorem 2.4.

Theorem 2.6. *Consider the Lucas sequence $U(a,b) = U(1,b)$, where $b \neq 0$. If $\gcd(n,b) = 1$, then $B_U(n) \equiv 0 \pmod{n}$ if and only if $U_{n+2} \equiv 1 \pmod{n}$.*

Proof. We observe that $U(1,b)$ is purely periodic modulo n, since $\gcd(n,b) = 1$. Noting that $a = 1$, we see that $a + b - 1 = b \neq 0$. It now follows from Corollary 2.1 (i) that

$$\begin{aligned} B_U(n) =& \frac{1}{a+b-1}(U_{n+1} + bU_n - 1) = \frac{1}{b}(U_{n+2} - 1) \equiv 0 \pmod{n} \\ &\iff U_{n+2} \equiv 1 \pmod{n}. \end{aligned}$$

This ends the proof. □

Theorem 2.6 was proved for the case of the Fibonacci sequence $U(1,1)$ in Theorem 7 of [4].

Example 2.1. In contradistinction to Theorem 2.5, we show by two examples that there are instances of Lucas sequences $U(a,b)$ for which $n \notin S(U)$ and $A_U(n)$ is an integer, but $A_W(n)$ is not an integer for infinitely many recurrences $W(a,b)$. First consider the Fibonacci sequence $U(1,1)$ and let $n = 319 = 11 \cdot 29$. By inspection, $\pi_U(11) = 10$ and $\pi_U(29) = 14$. We confirm that $B_U(319) \equiv 0 \pmod{319}$, which implies that $A_U(319)$ is an integer. Since $\pi_U(11) = 10 \mid 320$, we see that $U_{321} \equiv U_1 \equiv 1 \pmod{11}$. Since $\pi_U(29) = 14 \mid 322$, we find that $U_{321} \equiv U_{323} - U_{322} \equiv 1 - 0 \equiv 1 \pmod{29}$. Thus, by Theorem 2.6, $11 \mid B_U(319)$ and $29 \mid B_U(319)$, which yields that $319 \mid B_U(319)$.

Now we evaluate $B_W(319)$ for an arbitrary generalized Fibonacci sequence $W(1,1)$. Notice that by (1.2), $B_W(319) = W_{321} - W_2$. We observe that 10 is equal to a general period of $W(1,1) \pmod{11}$ and 14 is equal to a general period of $W(1,1) \pmod{29}$. Then

$$W_{321} - W_2 \equiv W_1 - W_2 \equiv -W_0 \pmod{11}, \tag{2.9}$$

while

$$\begin{aligned} W_{321} - W_2 &\equiv W_{323} - W_{322} - W_2 \equiv W_1 - W_0 - W_2 \\ &\equiv -(W_2 - W_1) - W_0 \equiv -2W_0 \pmod{29}. \end{aligned} \tag{2.10}$$

Suppose that $11 \cdot 29 = 319 \mid B_W(319)$. Then by (2.9) and (2.10), $B_W(319) \equiv -W_0 \equiv 0 \pmod{11}$ and $B_W(319) \equiv -2W_0 \equiv 0 \pmod{29}$, which implies that $W_0 \equiv 0 \pmod{319}$. Hence, $A_W(319)$ is not an integer if $W_0 \not\equiv 0 \pmod{319}$. We note that for the Fibonacci sequence $U(1,1)$, Sequences A331976, A331870, and A111035 in the On-Line Encyclopedia of Integer Sequences [7] give further examples of integers n for which $A_U(n)$ is an integer, but $n \notin S(U)$.

As a second example, we consider the Lucas sequence $U(1,-2)$ and let $n = 21 = 3 \cdot 7$. We will show that $B_U(21) \equiv 0 \pmod{21}$, which implies that $A_U(21)$ is an integer. By the proof of Theorem 2.6 and inspection,

$$B_U(21) = \frac{1}{-2}(U_{23} - U_2) = -\frac{1}{2}(967 - 1) = -483 \equiv 0 \pmod{21}.$$

We now evaluate $B_W(21)$ for an arbitrary recurrence generalized Fibonacci sequence $W(1, -2)$. By examination, $\pi_U(3) = 8$ and $\pi_U(7) = 21$. Hence, $\pi_W(3) \mid 8$, so $\pi_W(3) \mid 24$ and $\pi_W(7) \mid 21$. Suppose that $B_W(21) \equiv 0 \pmod{21}$. Then by Theorem 2.2 (i),

$$B_W(21) = \frac{1}{-2}(W_{23} - W_2) \equiv W_{23} - W_2 \equiv 0 \pmod{3}. \tag{2.11}$$

Since 24 is equal to a general period of $U(1, -2)$ modulo 3, we see that

$$W_{23} \equiv (-2)^{-1}(W_{25} - W_{24}) \equiv W_1 - W_0 \pmod{3}. \tag{2.12}$$

Thus, by (2.11) and (2.12),

$$B_W(21) \equiv W_{23} - W_2 \equiv W_1 - W_0 - W_2 \equiv W_0 \equiv 0 \pmod{3}. \tag{2.13}$$

Hence, by (2.13), $W_0 \equiv 0 \pmod{3}$. Therefore, $A_W(21)$ is not an integer if $W_0 \not\equiv 0 \pmod{3}$.

Theorem 2.7. *Consider the Lucas sequence $U(a, b)$. Suppose that $W(a, b)$ is purely periodic modulo n starting from the term W_1 for all recurrences $W(a, b)$ and that the period of $W(a, b)$ modulo n divides n. Suppose further that $A_W(n)$ is an integer for all recurrences $W(a, b)$. Let $m \in S'(U)$. Then $A_W(\text{lcm}(m, n))$ is an integer for all recurrences $W(a, b)$.*

Proof. Let $W(a, b)$ be an arbitrary recurrence. It follows from the hypotheses that $B_W(r) \equiv 0 \pmod{n}$ if $n \mid r$. Thus, $B_W(\text{lcm}(m, n)) \equiv 0 \pmod{n}$. By Theorem 2.5, $B_W(\text{lcm}(m, n)) \equiv 0 \pmod{m}$. It now follows that $B_W(\text{lcm}(m, n)) \equiv 0 \pmod{\text{lcm}(m, n)}$, and thus, $A_W(\text{lcm}(m, n))$ is an integer. $\square$

Remark 2.4. Suppose that we are given the Lucas sequence $U(a, b)$ and positive integer n such that $\gcd(n, b) = 1$. We define $\omega(n) = \omega$ to be the least nonnegative integer k, if it exists, such that both $\pi_U^{k+1}(n) = \pi_U^j(n)$ for some j for which $0 \le j \le k$ and $\gcd(\pi_U^i(n), b) = 1$ for all i such that $0 \le i \le k$. We define the *radical* of the nonzero integer r, denoted by $\text{rad}(r)$ as follows: let $\text{rad}(\pm 1) = 1$ and let $\text{rad}(r)$ be the product of all the distinct primes dividing r when $|r| > 1$.

Theorem 2.8. *Consider the Lucas sequence $U(a, b)$, where $b \neq 0$. Suppose that $\gcd(n, b) = 1$ and $\omega(n) = \omega$ exists. Then $C(n)$ exists. Moreover,*

$$C(n) = L(n) := \text{lcm}(\pi_U^0(n), \pi_U^1(n), \ldots, \pi_U^\omega(n)). \tag{2.14}$$

Further, if $C(n)$ exists and either it is the case that $a + b - 1 \neq 0$ and $\gcd(C(n), a + b - 1) = 1$ or it is the case that both $a + b - 1 = 0$ and $\gcd(C(n), -b - 1) = 1$, then $C'(n) = C(n)$ and $A_W(C(n))$ is an integer for all recurrences $W(a, b)$.

Proof. Suppose that $n \mid m$ and $m \in S(U)$. Then $\gcd(m, b) = 1$ and $\pi_U(m) \mid m$. It follows by Remark 1.2 that $\pi_U(n) \mid \pi_U(m)$, so $\pi_U(n) \mid m$. Similarly, $\pi_U^2(n) \mid \pi_U(m)$, so $\pi_U^2(n) \mid m$. It follows that $\pi_U^0(n) = n \mid m$ and $\pi_U^i(n) \mid \pi_U(m)$, so $\pi_U^i(n) \mid m$ for all i such that $1 \le i \le \omega(n)$. Thus,

$$L = L(n) = \operatorname{lcm}(\pi_U^0(n), \pi_U^1(n), \ldots, \pi_U^{\omega}(n)) \mid m.$$

Let $k = \omega(n)$. Since $\pi_U^{k+1}(n) = \pi_U^j(n)$ for some j such that $0 \le j \le k$, we find by Theorem 1.2 that

$$\pi_U(L) \mid L \mid m.$$

It now follows that $L = C(n)$.

Now suppose that it is the case that $a + b - 1 \neq 0$ and $\gcd(n, a + b - 1) = 1$, or it is the case that $a + b - 1 = 0$ and $\gcd(n, -b - 1) = 1$. Since $\gcd(n, b) = 1$, it follows from our above observations that $W(a, b)$ is purely periodic modulo n and that $\pi_U(n)$ is a general period of $W(a, b)$ modulo n for all recurrences $W(a, b)$. Noting that $C(n) \in S(U)$, it now follows from Theorem 2.4 that $A_W(C(n))$ is an integer for all recurrences $W(a, b)$ and that $C'(n) = C(n)$. □

Remark 2.5. By Theorem 2.11 below, if $b = \pm 1$, then both $\omega(n)$ and $L(n)$ exist for all n. By Theorem 2.8, $C(n)$ then exists for all n and $C(n) = L(n)$.

Corollary 2.4. *Consider the Lucas sequence $U(a, b)$, where $b \neq 0$. Suppose that* $\gcd(n, b) = 1$ *and $\omega(n)$ exists. Then the following hold.*

(i) Suppose that $m \mid n$. Then $L(m)$ and $L(n)$ both exist and $L(m) \mid L(n)$, where $L(m)$ and $L(n)$ are defined as in Theorem 2.8.

(ii) Suppose that $g \mid \pi_U^i(n)$ for some $i \ge 0$. Then $L(g) \mid L(n)$.

(iii) Suppose that $\gcd(r, b) = \gcd(s, b) = \gcd(r, s) = 1$ *and both $\omega(r)$ and $\omega(s)$ exist. Then $L(r)$ and $L(s)$ both exist and* $L(rs) = \operatorname{lcm}(L(r), L(s))$.

(iv) Suppose that $\gcd(p, b) = 1$ *and $\omega(p)$ exists. Let $i \ge 1$. Then $L(p^i)$ exists and*

$$L(p^i) = \operatorname{lcm}(p^i, L(p)).$$

Proof. (i) We observe by Theorem 1.2 that if $m \mid n$ and $\gcd(n, b) = 1$, then $\pi_U(m) \mid \pi_U(n)$. It follows that

$$\pi_U^i(m) \mid \pi_U^i(n) \tag{2.15}$$

for $i \ge 0$. Since $\omega(n)$ exists, we see that there exists a nonnegative integer $i \le \omega(n)$ such that $\pi_U^j(n) = \pi_U^i(n)$ for infinitely many integers j. Since $\pi_U^i(n)$ has only finitely many divisors, it follows from (2.15) that $\omega(m)$ exists. It now follows from the definition of $L(m)$ and $L(n)$ that $L(m) \mid L(n)$.

(ii) This follows from the construction of $L(n)$.

(iii) By Theorem 2.8, $L(r) = C(r)$ and $L(s) = C(s)$. By definition, $C(r)$ and $C(s) \in S(U)$. It now follows from Theorem 1.2 that $L(rs) = \text{lcm}(L(r), L(s))$.

(iv) This follows from Theorem 1.4 (viii) and the definition of $L(p^i)$. $\square$

Remark 2.6. If $L(n)$ exists, it follows from the construction of $L(n)$ that both n and $\pi_U(n)$ divide $L(n)$. We will make use of this observation later in some of our proofs to prove that $C'(n)$ exists. Moreover, we see from the definition of $L(n)$ that $L(n) = \text{lcm}(n, L(\pi_U(n)))$.

For some of our future work, we will need to make use of results in Theorem 2.9 involving the evaluation of $L(2)$ and $L(3)$ if they exist.

Theorem 2.9. *Consider the Lucas sequence $U(a, b)$. Then the following hold.*

(i) If $a \equiv b \equiv 1 \pmod 2$, then $L(2)$ exists if and only if $\gcd(b, 3) = 1$.

(ii) If $a \equiv 0 \pmod 2$, then $L(2)$ exists if and only if $b \equiv 1 \pmod 2$.

(iii) If $L(3)$ exists, then either $L(3) = 3$ or $6 \mid L(3)$.

(iv) $L(3) = 3$ if and and only if $a \equiv b \equiv -1 \pmod 3$.

(v) $6 \mid L(3)$ if and only if $\gcd(b, 6) = 1$ and it is not the case that $a \equiv -1 \pmod 3$ and $b \equiv -1 \pmod 6$.

(vi) If $a \equiv 0 \pmod 2$ and $b \equiv 1 \pmod 2$, then $L(2) = 2$.

(vii) If $a \equiv \pm 1 \pmod 6$ and $b \equiv 1 \pmod 6$, then $L(2) = L(3) = 24$.

(viii) If $a \equiv 1 \pmod 6$ and $b \equiv -1 \pmod 6$ or it is the case that $a \equiv 3 \pmod 6$ and $b \equiv 1 \pmod 6$, then $L(2) = L(3) = 6$.

(ix) If $a \equiv b \equiv -1 \pmod 6$, then $L(2) = 6$ and $L(3) = 3$.

(x) If $a \equiv 0 \pmod 6$ and $b \equiv 1 \pmod 6$, then $L(3) = 6$, while if $a \equiv 0 \pmod 6$ and $b \equiv -1 \pmod 6$, then $L(3) = 12$.

(xi) If $a \equiv 3 \pmod 6$ and $b \equiv -1 \pmod 6$, then $L(2) = L(3) = 12$.

(xii) If $a \equiv \pm 2 \pmod 6$ and $b \equiv 1 \pmod 6$, then $L(3) = 24$, whereas if $a \equiv \pm 2 \pmod 6$ and $b \equiv -1 \pmod 6$, then $L(3) = 6$.

(xiii) Suppose that $\text{rad}(n) \mid 6$. If $L(n)$ exists, then $\text{rad}(L(n)) \mid 6$.

Proof. Parts (i)–(xii) follow by inspection. Part (xiii) follows from parts (i)–(xii), Theorem 2.8, and Corollary 2.4 (iii) and (iv). $\square$

Theorem 2.10 refines Theorem 2.1 (vii) and (viii).

Theorem 2.10. *Consider the Lucas sequence $U(a,b)$ and arbitrary recurrence $W(a,b)$, where $b \neq 0$. Let $n > 1$. Suppose that $m \in S'(U)$, where $m \geq 1$.*

(i) If $n \mid b$ and $a \equiv 1 \pmod{n}$, then $A_W(n)$ and $A_W(mn)$ are both integers.

(ii) If n is even, $n \mid b$, and $a \equiv -1 \pmod{n}$, then $A_W(n)$ and $A_W(mn)$ are both integers.

Proof. We observe that $\gcd(m,n) = 1$, since $n \mid b$ and $\gcd(m,b) = 1$. We treat the parameters a and b and the terms W_0 and W_1 as residues modulo n when considering $W(a,b)$ modulo n and as rational integers when considering $W(a,b)$ modulo m. The theorem now follows from Theorems 1.3 (viii) and (ix), 2.1 (vii) and (viii), 2.4, 2.5, and 2.7. □

Remark 2.7. Given the nonzero integer r, we let $Q(r)$ denote the least prime dividing r with the convention that $Q(\pm 1) = \infty$.

Theorem 2.11. *Consider the nondegenerate Lucas sequence $U(a,b)$ with discriminant D. Suppose that $Q(b) \geq 5$. Then $C(1) = 1$ and $C(n)$ exists for all n such that $n \geq 2$ and $P(n) < Q(b)$. Specifically, if $b = \pm 1$, then $C(n)$ exists for all n. Moreover, if $P(n) < Q(b)$ and $\gcd(C(n), a+b-1) = 1$, then $A_W(C(n))$ is an integer for all recurrences $W(a,b)$. In particular, if $a+b-1 \neq 0$, $Q(a+b-1) \geq 5$, and $P(n) < Q(b(a+b-1))$, then $A_W(C(n))$ is an integer for all recurrences $W(a,b)$. Specifically, if $(a,b) = (1,1)$, $(-1,1)$, or $(3,-1)$, then $|a+b-1| = |b| = 1$ and $A_W(C(n))$ is an integer for all n and for all recurrences $W(a,b)$.*

Proof. Let $n \geq 2$ be an integer such that $P(n) < Q(b)$. Then $\gcd(n,b) = 1$. We first prove that $L(n)$ exists. Then $L(n) = C(n)$ by (2.14). Let

$$n = \prod_{i=1}^{r} p_i^{k_i} \tag{2.16}$$

be the prime power factorization of n, where $p_1 < p_2 < \cdots < p_r$. By Corollary 2.4 (iv), if $p \mid n$ and $L(p)$ exists, then $L(p^i)$ also exists and

$$L(p^i) = \operatorname{lcm}(p^i, L(p)).$$

It follows by (2.16), by Theorem 1.4 (i), (iii), (iv), and (viii), and by repeated applications of Theorem 1.4 (v) and (vi) that if $p_1 = 2$, then

$$P(\pi_U^j(p_1^{k_1})) \leq 3 < Q(b),$$

while if $1 \leq i \leq r$ and $p_i > 2$, then

$$P(\pi_U^j(p_i^{k_i})) \leq p_i \leq p_r < Q(b). \tag{2.17}$$

By Theorem 1.2,

$$\pi_U^j(n) = \mathrm{lcm}(\pi_U^j(p_1^{k_1}), \pi_U^j(p_2^{k_2}), \ldots, \pi_U^j(p_r^{k_r}))$$

if $j \geq 1$. If $L(p_i)$ exists for $i = 1, 2, \ldots, r$, we further see by Corollary 2.4 (iii) and (iv) that

$$L(n) = \mathrm{lcm}(p_1^{k_1}L(p_1), p_2^{k_2}L(p_2), \ldots, p_r^{k_r}L(p_r)). \tag{2.18}$$

It follows by (2.18) that if we can show that $L(p)$ exists for any prime p dividing n, then $L(n)$ exists. By Theorem 2.9, if $p = 2$ or $p = 3$, then $L(p)$ exists and $L(p) \mid 24$. Now suppose that $p \geq 5$ and $p \mid n$. Then by (2.17), $\pi_U^i(p) \leq p \leq P(n) < Q(b)$, and consequently, $\gcd(\pi_U^i(p), b) = 1$ for all $i \geq 0$. We show that $L(p)$ exists in this case. By Theorem 1.4 (iii)–(v),

$$\pi_U(p) \mid p(p+1)(p-1). \tag{2.19}$$

Suppose that q is an odd prime and $q^j \parallel \pi_U(p)$ for some $j \geq 1$, where $q^i \parallel m$ for $i \geq 0$ means that $q^i \mid m$, but $q^{i+1} \nmid m$. Since $q \geq 3$ and both $p+1$ and $p-1$ are even, we see that $q^j \mid p$, or $q^j \mid (p+1)/2$, or $q^j \mid (p-1)/2$. Thus, if $q = p$, then $q^j = p$, which occurs if and only if $p \mid D$ by Theorem 1.4 (iii)–(vi). If $q \neq p$, then $q^j \leq (p+1)/2 < p$. Now suppose that $2^k \parallel \pi_U(p)$. Then by (2.19), $2^k \mid (p+1)(p-1)$.

We note that $\gcd(p+1, p-1) = 2$. If $p \equiv 1 \pmod 4$, then $2 \parallel p+1$ and $4 \mid p-1$. If $p \equiv 3 \pmod 4$ then $2 \parallel p-1$ and $4 \mid p+1$. It now follows that $2^k \leq 2(p+1) = 2p+2$. Hence, by our discussion above, we can write $\pi_U(p)$ as the prime power factorization given by

$$\pi_U(p) = 2^k p^{\epsilon} q_1^{j_1} q_2^{j_2} \cdots q_s^{j_s}, \tag{2.20}$$

where $1 \leq 2^k \leq 2p+2$, $\epsilon = 1$ if $p \mid D$, $\epsilon = 0$ if $p \nmid D$, and both $q_i \nmid 2p$ and $q_i^{j_i} \leq (p+1)/2$ for $1 \leq i \leq s$.

We now consider $\pi_U^2(p)$. Then by Theorem 1.2 and (2.20),

$$\pi_U^2(p) = \pi_U(\pi_U(p)) = \mathrm{lcm}(\pi_U(2^k), \pi_U(p^{\epsilon}), \pi_U(q_1^{j_1}), \pi_U(q_2^{j_2}), \ldots, \pi_U(q_s^{j_s})), \tag{2.21}$$

Let $2^\gamma \parallel \pi_U^2(p)$. Then by (2.21), $2^\gamma \parallel \pi_U(2^k)$, or $2^\gamma \parallel \pi_U(p^\epsilon)$, or $2^\gamma \parallel \pi_U(q_i^{j_i})$ for some i such that $1 \leq i \leq s$. If $2^\gamma \parallel \pi_U(2^k)$, then by Theorem 1.4 (i), (iii) and (viii), $2^\gamma \mid 3 \cdot 2^k$. Hence by (2.20), $2^\gamma \leq 2^k \leq 2p+2$. Suppose that $2^\gamma \parallel \pi_U(p^\epsilon)$. Then $2^\gamma \leq p-1$ if $p \mid D$ and $\epsilon = 1$, since $\pi_U(p) \mid p(p-1)$ by Theorem 1.4 (iii). If $\epsilon = 0$, then $2^\gamma = 1$. If $2^\gamma \parallel \pi_U(q_i^{j_i})$ for some i such that $1 \leq i \leq s$, then by Theorem 1.4 (iii)–(v) and (viii), $2^\gamma \mid q_i^{j_i}(q_i+1)(q_i-1)$. In this case, we see by our above discussion that

$$2^\gamma \leq 2q_i + 2 \leq 2\frac{p+1}{2} + 2 = p+3 < 2p+2.$$

Hence, by examining all cases, we find that $2^\gamma \leq 2p+2$.

We now suppose that $p^\delta \parallel \pi_U^2(p)$. Let us point out that $\pi_U(2^k) \mid 3 \cdot 2^k$ and $\pi_U(q_i^{j_i}) \mid q_i^{j_i}(q_i+1)(q_i-1)$ for $1 \le i \le s$. Thus, $p \nmid \pi_U(2^k)$ and $p \nmid \pi_U(q_i^{j_i})$ for any i such that $1 \le i \le s$, since $p \ge 5$ and $q_i^{j_i} \le (p+1)/2$. Hence, by (2.19), $p^\delta \mid p(p+1)(p-1)$. Then $\delta = 0$ if $p \nmid D$ and $\delta = 1$ if $p \mid D$.

Finally, suppose that $q^\lambda \parallel \pi_U^2(p)$, where $\lambda \ge 1$ and q is a prime such that $q \nmid 2p$. If $q^\lambda \parallel \pi_U(2^k)$, then $q^\lambda \mid 3 \cdot 2^k$, and $q^\lambda = 3 \le (p+1)/2$. If $q^\lambda \parallel \pi_U(p^\epsilon)$, then $q^\lambda \mid p(p+1)(p-1)$ and $q^\lambda \le (p+1)/2$. If $q^\lambda \parallel \pi_U(q_i^{j_i})$ for some i such that $1 \le i \le s$, then

$$q^\lambda \mid q_i^{j_i}(q_i+1)(q_i-1), \tag{2.22}$$

where $q_i^{j_i} \le \frac{p+1}{2}$. Then by (2.22), $q^\lambda \mid q_i^{j_i} \le \frac{p+1}{2}$, or

$$q^\lambda \,\Big|\, \frac{q_i+1}{2} \le \frac{p+3}{4} < \frac{p+1}{2},$$

or $q^\lambda \mid \frac{q_i-1}{2} < \frac{p+1}{2}$. Thus, in all cases, $q^\lambda \le (p+1)/2$.

We note that $p \ge 5$ and $\pi_U^0(p) = p$. The following observations follow by our above arguments and by induction. Let $i \ge 0$. If $2^k \parallel \pi_U^i(p)$, then $2^k \le 2p+2$. If $p^\delta \parallel \pi_U^i(p)$, then $p^\delta = 1$ if $p \nmid D$ and $p^\delta = p$ if $p \mid D$. If $q^\lambda \parallel \pi_U^i(p)$, where $\lambda \ge 1$ and q is a prime such that $q \nmid 2p$, then $q^\lambda \le \frac{p+1}{2}$. Hence, there are at most $J = \pi(\frac{p+1}{2}) - 1$ odd primes $q \ne p$ such that $q \mid \pi_U^i(p)$ for any $i \ge 0$, where $\pi(x)$ is the number of primes less than or equal to the real number x. We thus find that

$$\pi_U^i(p) \le (2p+2)p\Big(\frac{p+1}{2}\Big)^J$$

for all $i \ge 0$. Therefore, by the pigeonhole principle, there exists a nonnegative integer $\omega = \omega(p)$ such that $\pi_U^{\omega+1}(p) = \pi_U^j(p)$ for some j for which $0 \le j \le \omega$, which implies that $L(p)$ exists. Hence, $L(n)$ exists and $C(n) = L(n)$ by Theorem 2.8.

Now suppose that $a+b-1 \ne 0$ and $\gcd(a+b-1, C(n)) = 1$. By Theorem 2.8, $C(n) = C'(n)$ and $A_W(C(n))$ is an integer for all recurrences $W(a,b)$.

Finally, suppose that $a+b-1 \ne 0$, $Q(a+b-1) \ge 5$, and $P(n) < Q(b(a+b-1))$. It follows from our arguments above that $L(n) = C(n)$ exists, $P(L(n)) < Q(b)$, and $P(L(n)) < Q(a+b-1)$. It again follows from Theorem 2.8 that $A_W(C(n))$ is an integer for all recurrences $W(a,b)$. □

Remark 2.8. We found in Theorem 2.11 that for the nondegenerate Lucas sequences $U(a,b)$, where $(a,b) = (1,1)$, $(-1,1)$, or $(3,-1)$, given any positive integer n, $C(n)$ exists and $A_W(C(n))$ is an integer for all recurrences $W(a,b)$. We will see later in Theorems 2.24 and 2.25 that this property holds for the more general Lucas sequences $U(a,1)$ and $U(a,-1)$ when a is an odd integer.

In Theorem 2.12, we apply Theorems 2.11 and 2.8 to a large class of Lucas sequences $U(a,b)$ so that for each given Lucas sequence $U(a,b)$, we will find infinitely many positive integers $n \in S(U)$ for which $\mathrm{rad}(n) \mid 6$ and $A_W(n)$ is an integer for all recurrences $W(a,b)$. Before presenting Theorem 2.12, we will need to make use of Lemma 2.1 given below.

Lemma 2.1. *Consider the nondegenerate Lucas sequence $U(a,b)$, where $ab \neq 0$ and $a+b-1 \neq 0$. Suppose that p is odd and $p^e \parallel a$, where $e \geq 1$. Suppose further that $b \equiv 1 \pmod{p^{e+1}}$. Then $p^e \parallel a+b-1$. Moreover, if $m \geq 1$, then*

$$B_U(2mp^i) \equiv 0 \pmod{p^i}$$

for all $i \geq 1$.

Proof. Let p be an odd prime such that $p^e \parallel a$ and $b \equiv 1 \pmod{p^{e+1}}$. Then it is easily seen that $p^e \parallel a+b-1$. Then $U_2 = a \equiv 0 \pmod{p^e}$ and $U_3 = a^2+b \equiv 1 \pmod{p^e}$. Since $p^{e+1} \nmid a$, it follows that $\pi_U(p^e) = 2$ and $\pi_U(p^{e+1}) > 2$. By Theorem 1.4 (viii), we now see that

$$\pi_U(p^{e+i}) = 2p^i$$

for $i \geq 1$. Hence, $2mp^i$ is a general period of $U(a,b)$ modulo p^{e+i} for $m \geq 1$. We note by Theorem 2.2 (i) and Corollary 2.1 (i) that

$$B_U(2mp^i) = \frac{J(2mp^i)}{a+b-1}, \tag{2.23}$$

where $J(2mp^i) = U_{2mp^i+1} - 1 + bU_{2mp^i}$ and $J(2mp^i) \equiv 0 \pmod{p^{i+e}}$. Since $p^e \parallel a+b-1$, we find from (2.23) that

$$B_U(2mp^i) \equiv 0 \pmod{p^i}$$

for all $i \geq 1$. □

Theorem 2.12. *Consider the nondegenerate Lucas sequence $U(a,b)$, where $b(a+b-1) \neq 0$. Then $n \in S(U)$ and $A_W(n)$ is an integer for all recurrences $W(a,b)$ in the following cases, where $\mathrm{rad}(n) \mid 6$, i and j are nonnegative integers, and $e \geq 1$:*

(i) $a \equiv \pm 1 \pmod 6$, $b \equiv 1 \pmod 6$, *and* $n = 1$ *or* $n = 2^{i+3}3^{j+1}$.

(ii) $a \equiv 1 \pmod 6$, $b \equiv -1 \pmod 6$, *and* $n = 1$ *or* $n = 2^{i+1}3^{j+1}$.

(iii) $a \equiv 3 \pmod 6$, $b \equiv -1 \pmod 6$, *and* $n = 1$ *or* $n = 2^{i+2}3^{j+1}$.

(iv) $a \equiv 3 \pmod 6$, $3^e \parallel a$, $b \equiv 1 \pmod{2 \cdot 3^{e+1}}$, *and* $n = 1$ *or* $n = 2^{i+1}3^{j+1}$.

Proof. Clearly, we can assume that $n > 1$. For each of parts (i)–(iv), it follows from Theorem 2.8, Corollaries 2.3 and 2.4, and Theorems 2.9 and 2.11 that $L(n) = n = C(n)$, which then implies that $n \in S(U)$. In each of the cases of (i)–(iii), we observe that $b(a+b-1) \equiv \pm 1 \pmod 6$. It then follows that $Q(b(a+b-1)) \geq 5$

and $P(n) = 3$. Hence, $P(n) < Q(b(a+b-1))$. By Corollary 2.4, Theorem 2.9, and Theorem 2.11, it then follows that $C'(n)$ exists, $C'(n) = C(n) = L(n) = n$, and $A_W(C(n))$ is an integer for all recurrences $W(a,b)$ in the cases of parts (i)–(iii).

We now prove part (iv). We note that $a+b-1 \equiv 3+1-1 \equiv 3 \pmod 6$. Thus, $\gcd(2^{i+1}, (b(a+b-1)) = 1$. Since $L(n) = n$, we see that n is a general period of $U(a,b)$ modulo 2^{i+1}. It now follows from Theorem 2.2 (i) that $B_U(n) \equiv 0 \pmod{2^{i+1}}$. Since $3 \mid a$, it follows from Lemma 2.1 that $B_U(2 \cdot 3^{j+1}) \equiv 0 \pmod{3^{j+1}}$.

Since $2 \cdot 3^{j+1} \mid n$, we see that $B_U(n) \equiv 0 \pmod{3^{j+1}}$. Thus, $B_U(n) \equiv 0 \pmod n$. It now follows that $C'(n) = C(n) = L(n) = n$, and $A_W(C(n))$ is an integer for all recurrences $W(a,b)$. □

Theorem 2.13. *Consider the nondegenerate Lucas sequence $U(a,b)$, where $d = \gcd(a,b) > 1$. Suppose that $\gcd(n,d) = e > 1$. Then $A_U(n)$ is not an integer.*

Proof. By inspection, $U_1 = 1$ and $U_i \equiv 0 \pmod e$ for $i \geq 2$. Thus, $B_U(n) \equiv 1 \pmod e$. Since $e \mid n$, we see that $A_U(n)$ is not an integer. □

Theorem 2.14. *Consider the nondegenerate Lucas sequence $U(a,b)$, where $a \equiv 0 \pmod 2$ and $b \equiv 1 \pmod 2$. If $n \equiv 2 \pmod 4$, then $B_U(n) \equiv 1 \pmod 2$ and $A_U(n)$ is not an integer. Moreover, $C(2^k) = 2^k$ for $k \geq 0$.*

Proof. Suppose that $a \equiv 0 \pmod 2$ and $b \equiv 1 \pmod 2$. We see by induction that $U_{2i-1} \equiv 1 \pmod 2$ and $U_{2i} \equiv 0 \pmod 2$ for $i \geq 1$. We now observe that if $n \equiv 2 \pmod 4$, then $B_U(n) \equiv n/2 \equiv 1 \pmod 2$ and $A_U(n)$ is not an integer.

We now determine $C(2^k)$ for $k \geq 0$. Clearly, $C(1) = 1$. Since $U_2 = a \equiv 0 \pmod 2$ and $U_3 = aU_2 + bU_1 \equiv 0 + 1 \equiv 1 \pmod 2$, we find that $\pi_U(2) = L(2) = 2$. By Corollary 2.4 (iv), it follows that $L(2^k) = C(2^k) = 2^k$ if $k \geq 1$. □

Theorem 2.15. *Consider the nondegenerate Lucas sequence $U(a,b)$, where $a \equiv 2 \pmod 4$ and $b \equiv 1 \pmod 4$. Then $2^i \in S(U)$ for $i \geq 1$. Suppose that $2^k \parallel n$, where $k \geq 2$. Then $B_U(n) \equiv 0 \pmod{2^k}$. In particular, $C'(2) = 4 = 2C(2)$ and $C'(2^k) = 2^k = C(2^k)$ for $k \geq 2$. Moreover, if $k \geq 2$, then $A_W(2^k)$ is an integer for all recurrences $W(a,b)$.*

Proof. Consider the Lucas sequence $V(a,b)$. By inspection, $V_i \equiv 2 \pmod 4$ for $i \geq 0$. By examination and Lemma 1.1 (i), $U_0 = 0$, $U_1 = 1$, $U_2 = a \equiv 2 \pmod 4$, $U_3 = a^2 + b \equiv 1 \pmod 4$, $U_4 = U_2V_2 \equiv 4 \pmod 8$. By Lemma 1.1 (ii), $U_5 \equiv bU_2^2 + U_3^2 \equiv 5 \pmod 8$. Consequently, $\pi_U(2) = 2$, $\pi_U(4) = 4$, and $\pi_U(8) \neq \pi_U(4)$. By Theorem 1.4 (viii), $\pi_U(2^k) = 2^k$ for $k \geq 1$. We claim that $U_{2^k+1} \equiv 2^k + 1 \pmod{2^{k+1}}$ for $k \geq 2$. We proceed by induction.

The result is true for $k = 2$. Assume that the result is true up to k, where $k \geq 2$. Then $2^k \parallel U_{2^k}$ and $U_{2^k+1} \equiv 2^k + 1 \pmod{2^{k+1}}$. By Lemma 1.1 (ii),

$$U_{2^{k+1}+1} = bU_{2^k}^2 + U_{2^k+1}^2 \equiv 0 + 2^{k+1} + 1 \equiv 2^{k+1} + 1 \pmod{2^{k+2}},$$

as desired. Noting that $2 \parallel V_{2^k}$ for $k \geq 1$, $2 \parallel U_2$, and $U_{2^{k+1}} = U_{2^k} V_{2^k}$, we see by induction that $2^k \parallel U_{2^k}$ for $k \geq 1$.

We now show that $B_U(2^k) \equiv 0 \pmod{2^k}$ for $k \geq 2$. We observe that $a+b-1 \equiv 2+1-1 \equiv 2 \pmod 4$, and thus $a+b-1 \neq 0$. By Corollary 2.1 (i),

$$B_U(2^k) = \frac{1}{a+b-1}(U_{2^k+1} - 1 + bU_{2^k}).$$

We note that

$$U_{2^k+1} - 1 + bU_{2^k} \equiv 2^k + 2^k \equiv 0 \pmod{2^{k+1}}.$$

Since $2 \parallel a+b-1$, we see that $B_U(2^k) \equiv 0 \pmod{2^k}$ and $C'(2^k) = C(2^k)$ for $k \geq 2$. Noting that $C'(2) \neq 2$ by Theorem 2.14, we observe that $C'(2) = 4 = 2C(2)$. By Remark 2.3, if $k \geq 2$, then $A_W(2^k)$ is an integer for all recurrences $W(a,b)$. $\square$

Theorem 2.16. *Consider the nondegenerate Lucas sequence $U(a,b)$, where $a \equiv 0 \pmod 4$ and $b \equiv 1 \pmod 4$. Suppose that $2^k \parallel n$, where $k \geq 1$. Then $B_U(n) \not\equiv 0 \pmod{2^k}$, and $C'(n)$ does not exist if n is even. In particular, $A_U(m)$ is an integer only if m is odd.*

Proof. Consider the Lucas sequence $V(a,b)$. By inspection, $V_i \equiv 0 \pmod 2$ for $i \geq 0$. By examination and Lemma 1.1 (ii), $U_0 = 0$, $U_1 = 1$, $U_2 = a \equiv 0 \pmod 4$, and $U_3 = a^2 + b \equiv 1 \pmod 4$. Thus, $\pi_U(4) = 2$. It follows from Theorem 1.4 (viii) that 2^{k-1} is a general period of $U(a,b)$ modulo 2^k for $k \geq 2$. Then

$$B_U(4) = U_1 + U_2 + U_3 + U_4 \equiv 1 + 0 + 1 + 0 \equiv 2 \pmod 4.$$

We claim that $B_U(2^k) \equiv 2^{k-1} \pmod{2^k}$ for $k \geq 2$. We proceed by induction.

The result is true for $k = 2$. Assume the result is true up to k, where $k \geq 2$. By our earlier observation, 2^k is a general period of $U(a,b)$ modulo 2^{k+1}. By assumption, $B_U(2^k) \equiv 2^{k-1}\ell \pmod{2^{k+1}}$, where $\ell = 1$ or 3. Since 2^k is a general period of $U(a,b)$ modulo 2^{k+1}, we find that

$$B_U(2^{k+1}) \equiv 2 \cdot 2^{k-1}\ell \equiv 2^k \ell \equiv 2^k \pmod{2^{k+1}},$$

as desired. Since $n = 2^k i$ for some odd integer i and 2^k is a general period of $U(a,b)$ modulo 2^{k+1}, we see that

$$B_U(n) \equiv 2^{k-1} i \equiv 2^{k-1} \pmod{2^k}. \tag{2.24}$$

and $B_U(n) \not\equiv 0 \pmod n$. It now follows from (2.24) and Theorem 2.14 that $C'(m)$ does not exist for any even integer m. $\square$

Theorem 2.17. *Consider the nondegenerate Lucas sequence $U(a,b)$, where $a \equiv 0 \pmod 4$ and $b \equiv -1 \pmod 4$. Then $2^i \in S(U)$ for $i \geq 1$. Suppose that $2^k \parallel n$, where $k \geq 2$. Then $B_U(n) \equiv 0 \pmod{2^k}$. In particular, $C'(2) = 4 = 2C(2)$ and $C'(2^k) = 2^k = C(2^k)$ for $k \geq 2$. Moreover, if $k \geq 2$, then $A_W(2^k)$ is an integer for all recurrences $W(a,b)$.*

Proof. By Theorem 2.14, $B_U(2) \equiv 1 \pmod 2$. Consider the Lucas sequence $V(a,b)$. By induction, $V_i \equiv 0 \pmod 2$ and $V_{2i} \equiv 2 \pmod 4$ for $i \geq 0$. By examination and Lemma 1.1 (i) and (ii), we observe that $U_0 = 0$, $U_1 = 1$, $U_2 = a \equiv 0 \pmod 4$, $U_3 = a^2 + b \equiv -1 \pmod 4$, $U_4 = U_2V_2 \equiv 0 \pmod 8$, and $U_5 = bU_2^2 + U_3^2 \equiv 0+1 \equiv 1 \pmod 8$. Hence, $\pi_U(4) = \pi_U(8) = 4$. It follows from Theorem 1.4 (viii) that 2^k is a general period of $U(a,b)$ modulo 2^{k+1} for $k \geq 2$ and 2^k is a general period of $U(a,b)$ modulo 2^k for $k = 1$ or 2. Thus, $U_{2^k} \equiv 0 \pmod{2^{k+1}}$ and $U_{2^k+1} \equiv 1 \pmod{2^{k+1}}$ for $k \geq 2$. We observe that $a + b - 1 \equiv 0 - 1 - 1 \equiv 2 \pmod 4$. It now follows by Corollary 2.1 (i) and our previous observations that,

$$B_U(2^k) = \frac{1}{a+b-1}(U_{2^k+1} - 1 + bU_{2^k}) \equiv 0 \pmod{2^k}. \tag{2.25}$$

Since $B_U(2) \equiv 1 \pmod 2$ by Theorem 2.14, it follows from (2.25) that $C'(2) = 4 = 2C(2)$ and $C'(2^k) = 2^k = C(2^k)$ for $k \geq 2$. We now see by Remark 2.3 that $A_W(2^k)$ is an integer for all recurrences $W(a,b)$. □

Theorem 2.18. *Consider the nondegenerate Lucas sequence $U(a,b)$, where $a \equiv 2 \pmod 4$ and $b \equiv -1 \pmod 4$. Suppose that $2^k \parallel n$, where $k \geq 1$. Then $B_U(n) \not\equiv 0 \pmod{2^k}$. In particular, $C'(n)$ does not exist if n is even, and $A_U(n)$ is an integer only if n is odd.*

Proof. By Theorem 1.5 (iii), $2 \mid D$ if $i \geq 1$, and $U(a,b)$ is uniformly distributed modulo 2^k with each residue appearing exactly once in a least period of $U(a,b)$ modulo 2^k. Moreover, $\pi_U(2^k) = 2^k$ for $k \geq 1$. It now follows that

$$B_U(2^k) \equiv 1 + 2 + \cdots + 2^k \equiv \frac{2^k(2^k+1)}{2} \equiv 2^{k-1} \pmod{2^k}.$$

By the induction argument given in the proof of Theorem 2.16, it follows that

$$B_U(n) \equiv 2^{k-1} \pmod{2^k}$$

for $k \geq 1$. This yields that $B_U(n) \not\equiv 0 \pmod{2^k}$ and $A_U(n)$ is an integer only if n is odd. □

Theorems 2.19–2.23 sharpen Theorem 2.1.

Theorem 2.19. *Consider the nondegenerate Lucas sequence $U(a,b)$ with discriminant D such that $a+b-1 \neq 0$. Let n be an odd integer such that $a \equiv 2 \pmod{\operatorname{rad}(n)}$, $b \equiv -1 \pmod{\operatorname{rad}(n)}$. Then $\operatorname{rad}(n) \mid D$. Moreover, $C'(n) = C(n) = n$ and $A_W(n)$ is an integer for all recurrences $W(a,b)$.*

Proof. Clearly, $\gcd(n,b) = 1$. Since $D = a^2 + 4b \equiv 2^2 + 4(-1) \equiv 0 \pmod{\operatorname{rad}(n)}$, it follows that $\operatorname{rad}(n) \mid D$. Suppose that $p^{e(p)} \parallel n$, where $e(p) \geq 1$. Let $e = e(p)$. By Theorem 1.3 (vi), $U_p \equiv p \equiv 0 \pmod p$ and $U_{p+1} \equiv p + 1 \equiv 1 \pmod p$. Hence,

$\pi_U(p) = p$ and $E_U(p) = 1$. By Theorem 1.4 (viii), p^i is equal to a general period of $U(a,b)$ modulo p^i for $i \geq 1$. Thus, n is a general period of $U(a,b)$ modulo p^e.

Suppose now that it is not the case that $p = 3$, $e \geq 2$, and $U_3 \equiv 0 \pmod 9$. It follows from Theorem 1.5 (i), (ii), and (iv) that $U(a,b)$ is uniformly distributed modulo p^e with each residue appearing exactly once in a least period of $U(a,b)$ modulo p^e. Then

$$B_U(n) \equiv B_U(p^e) \equiv 1 + 2 + \cdots + p^e \equiv \frac{p^e(p^e+1)}{2} \equiv 0 \pmod{p^e}. \tag{2.26}$$

Next suppose that $p = 3$, $e \geq 2$, and $U_3 = a^2 + b \equiv 0 \pmod 9$. Then $b \equiv -a^2 \pmod 9$. Furthermore,

$$U_4 = aU_3 + bU_2 \equiv a \cdot 0 + ba \equiv -a^3 \pmod 9. \tag{2.27}$$

Since $a \equiv -1 \pmod 3$, we have that $a = -1 + 3j$ for some integer j. By the binomial theorem, $a^3 = (-1+3j)^3 \equiv -1 \pmod 9$. Hence, by (2.27), $U_4 \equiv 1 \pmod 9$. It follows that $\pi_U(9) = 3$. Therefore, by Theorem 1.4 (viii), 3^i is equal to a general period of $U(a,b)$ modulo 3^{i+1} for $i \geq 1$. We prove by induction that $B_U(3^i) \equiv 0 \pmod{3^i}$ for $i \geq 1$. This is true for $i = 1$ by (2.26). Assume that this is true up to i, where $i \geq 1$. Then $B_U(3^i) = 3^i m$ for some integer m. Since 3^i is a general period of $U(a,b)$ modulo 3^{i+1}, we have that

$$B_U(3^{i+1}) \equiv 3(3^i m) \equiv 0 \pmod{3^{i+1}}.$$

It thus follows that

$$B_U(n) \equiv B_U(3^e) \equiv 0 \pmod{3^e}. \tag{2.28}$$

We now see by (2.26) and (2.28) that $B_U(n) \equiv 0 \pmod n$, and thus, $C'(n) = C(n)$ and $A_W(n)$ is an integer for all recurrences $W(a,b)$. $\square$

Theorem 2.20. *Consider the nondegenerate Lucas sequence $U(a,b)$ with discriminant D such that $a+b-1 \neq 0$. Suppose that $n = 2^k n_1$ is an integer such that $k \geq 1$, $n_1 > 1$, n_1 is odd, a is even, and $a \equiv -2 \pmod{\operatorname{rad}(n_1)}$, $b \equiv -1 \pmod{4\operatorname{rad}(n_1)}$. Then $\operatorname{rad}(n_1) \mid D$ and $C(n) = n$. Moreover, the following hold.*

- *(i) Suppose that $a \equiv 2 \pmod 4$. Then $C'(n)$ does not exist.*
- *(ii) Suppose that $a \equiv 0 \pmod 4$. If $n \equiv 2 \pmod 4$, then $C'(n) = 2C(n) = 2n$, and $A_W(2n)$ is an integer for all recurrences $W(a,-1)$. If $n \equiv 0 \pmod 4$, then $C'(n) = C(n) = n$, and $A_W(n)$ is an integer for all recurrences $W(a,-1)$.*

Proof. It is evident that $\gcd(n,b) = 1$. Since $D = a^2 + 4b \equiv (-2)^2 + 4(-1) \equiv 0 \pmod{\operatorname{rad}(n_1)}$, it follows that $\operatorname{rad}(n_1) \mid D$. Suppose that $p^{e(p)} \parallel n_1$, where $e(p) \geq 1$. Let $e = e(p)$. By Theorem 1.3 (vii),

$$\begin{aligned} U_p &\equiv p \equiv 0 \pmod p, & U_{p+1} &\equiv (-1)^{p+2}(p+1) \equiv -1 \pmod p, \\ U_{2p} &\equiv -2p \equiv 0 \pmod p, & U_{2p+1} &\equiv (-1)^{2p+2}(2p+1) \equiv 1 \pmod p. \end{aligned} \tag{2.29}$$

Hence, $\pi_U(p) = 2p$ and $E_U(p) = 2$. Furthermore, since $a \equiv 0 \pmod 2$, we see that $\pi_U(2) = 2$. It now follows from Theorem 1.4 (viii) that $2p^e$ is equal to a general period of $U(a,b)$ modulo p^e and 2^k is equal to a general period of $U(a,b)$ modulo 2^k. We see by the definition of $L(n)$, by Theorem 2.8, and by Corollary 2.4 that $L(n_1) = 2n_1$, $L(2^k) = 2^k$, and hence,

$$L(n) = \mathrm{lcm}(L(2^k), L(n_1)) = \mathrm{lcm}(2^k, 2n_1) = 2^k n_1 = n.$$

Furthermore, if $C'(n_1)$ exists, then $C(n_1) = 2n_1 \mid C'(n)$. Noting that $2n_1 \equiv 2 \pmod 4$, it follows from Theorem 2.14 that $B_U(2n_1) \equiv 1 \pmod 2$, which implies that $C'(n_1) \neq 2n_1$. Hence, if $C'(n_1)$ exists, then $C'(n_1) \geq 4n_1$.

Now suppose that $a \equiv 2 \pmod 4$. Suppose that $C'(n)$ exists. Then $n \mid C'(n)$ and $C'(n)$ is even. Suppose that $2^\ell \parallel C'(n)$, where $\ell \geq k \geq 1$. We now see from Theorem 2.18 that $B_U(C'(n)) \not\equiv 0 \pmod{2^\ell}$. Hence, $C'(n)$ does not exist, and part (i) is established.

Next suppose that $a \equiv 0 \pmod 4$. Suppose it is not the case that $p = 3$ and $U_3 \equiv 0 \pmod 9$. Recall that $p \mid D$ and $p^e \parallel n_1 \mid n$. It then follows from Theorem 1.5 (i), (ii), and (iv) that $U(a,b)$ is uniformly distributed modulo p^e with each residue appearing exactly twice in a least period of $U(a,b)$ modulo p^e. Then $\pi_U p^e) = 2p^e$ and n is a general period of $U(a,b)$ modulo p^e. Hence,

$$B_U(n) \equiv B_U(2p^e) \equiv 2(1 + 2 + \cdots + p^e) \equiv \frac{2p^e(p^e+1)}{2} \equiv 0 \pmod{p^e}. \tag{2.30}$$

Now suppose that $p = 3$, $e \geq 2$, and $U_3 = a^2 + b \equiv 0 \pmod 9$. Then $b \equiv -a^2 \pmod 9$. Moreover,

$$U_4 = aU_3 + bU_2 \equiv a \cdot 0 + ba \equiv -a^3 \pmod 9. \tag{2.31}$$

Since $a \equiv -2 \equiv 1 \pmod 3$, we have that $a = 1 + 3j$ for some integer j. By the binomial theorem, $a^3 = (1+3j)^3 \equiv 1 \pmod 9$. Hence, by (2.31), $U_4 \equiv -1 \pmod 9$. It follows from Lemma 1.1 (i) and (ii) that

$$U_6 = U_3V_3 \equiv V_3 \cdot 0 \equiv 0 \pmod 9 \quad \text{and} \quad U_7 = U_4^2 + bU_3^2 \equiv (-1)^2 + b \cdot 0^2 \equiv 1 \pmod 9.$$

Thus, $\pi_U(9) = 6$. Therefore, by Theorem 1.4 (viii), $2 \cdot 3^i$ is equal to a general period of $U(a,b)$ modulo 3^{i+1} for $i \geq 1$. By a similar induction argument as that given in the proof of Theorem 2.19, we find that $B_U(2 \cdot 3^i) \equiv 0 \pmod{3^i}$ for $i \geq 1$. Noting that n is a general period of $U(a,b)$ modulo 3^e, we see that

$$B_U(n) \equiv B_U(3^e) \equiv 0 \pmod{3^e}. \tag{2.32}$$

It follows from Theorems 2.14 and 2.17 that

$$B_U(n) \equiv B_U(2^k) \equiv 1 \pmod 2 \quad \text{if} \quad k = 1 \tag{2.33}$$

and

$$B_U(n) \equiv B_U(2^k) \equiv 0 \pmod{2^k} \quad \text{if} \quad k \geq 2. \tag{2.34}$$

Now from (2.30), (2.32), (2.33), and (2.34) we get that $C'(n) = 2C(n) = 2n$ if $n \equiv 2 \pmod 4$, while $C'(n) = C(n) = n$ if $n \equiv 0 \pmod 4$. Assertion (ii) now follows. $\square$

Theorem 2.21. *Consider the nondegenerate Lucas sequence $U(a,b)$. Let n be an integer such that $6 \mid n$ and $a \equiv 1 \pmod{\mathrm{rad}(n)}$, $b \equiv -1 \pmod{\mathrm{rad}(n)}$. Then $C'(n) = C(n) = n$ and $A_W(n)$ is an integer for all recurrences $W(a,b)$.*

Proof. We first note that $a + b - 1 \equiv 1 - 1 - 1 \equiv -1 \pmod{\mathrm{rad}(n)}$. Hence, $\gcd(b(a+b-1), n) = 1$. Suppose that $p^{e(p)} \parallel n$, where $e(p) \geq 1$. Let $e = e(p)$. By Theorem 1.3 (iv),

$$U_4 \equiv -1 \pmod{\mathrm{rad}(n)}, \quad U_3 \equiv U_6 \equiv 0 \pmod{\mathrm{rad}(n)}, \quad U_7 \equiv 1 \pmod{\mathrm{rad}(n)}.$$

Thus, $\pi_U(p) = 6$ if p is odd and $\pi_U(2) = 3$. Hence, by Theorem 1.4 (viii), $\mathrm{lcm}(6, p^e)$ is a general period of $U(a,b)$ modulo p^e. We note that $\mathrm{lcm}(6, p^e) \mid n$. Therefore, n is also equal to a general period of $U(a,b)$ modulo p^e for each prime p dividing n. Then by Theorem 1.2, n is equal to a general period of $U(a,b)$ modulo n. We now see by Theorem 2.2 (i) that

$$B_U(n) = \frac{1}{a+b-1} J(n),$$

where $J(n) \equiv 0 \pmod n$. Since $\gcd(a+b-1, n) = 1$, we find that $B_U(n) \equiv 0 \pmod n$. Consequently, $C'(n) = C(n) = n$ and $A_W(n)$ is an integer for all recurrences $W(a,b)$. $\square$

Theorem 2.22. *Consider the nondegenerate Lucas sequence $U(a,b)$ with discriminant D. Let n be an integer such that $3 \mid n$ and $a \equiv -1 \pmod{\mathrm{rad}(n)}$, $b \equiv -1 \pmod{\mathrm{rad}(n)}$. Then $C'(n) = C(n) = n$ and $A_W(n)$ is an integer for all recurrences $W(a,b)$.*

Proof. We observe that $a + b - 1 \equiv -1 - 1 - 1 \equiv -3 \pmod{\mathrm{rad}(n)}$. Suppose that $p^{e(p)} \parallel n$. Let $e = e(p)$. Then $\gcd(b(a+b-1), p^e) = 1$ if $p \neq 3$. By Theorem 1.3 (v),

$$U_2 = a \equiv -1 \pmod{\mathrm{rad}(n)}, \quad U_3 \equiv 0 \pmod{\mathrm{rad}(n)}, \quad U_4 \equiv 1 \pmod{\mathrm{rad}(n)}.$$

Thus, $\pi_U(p) = 3$. Therefore, by Theorem 1.4 (viii), $\mathrm{lcm}(3, p^e)$ is a general period of $U(a,b)$ modulo p^e. We note that $\mathrm{lcm}(3, p^e) \mid n$. Therefore, n is also equal to a general period of $U(a,b)$ modulo p^e for each prime p dividing n. Then by Theorem 1.2, n is equal to a general period of $U(a,b)$ modulo n. First suppose that $p \neq 3$. It now follows from Corollary 2.2 (i) that

$$B_U(n) = \frac{1}{a+b-1} J(n),$$

where $J(n) \equiv 0 \pmod{p^e}$. Since $\gcd(a+b-1, p^e) = 1$, we see that

$$B_U(n) \equiv 0 \pmod{p^e}.$$

Now suppose that $p = 3$. Since $U_3 \equiv 0 \pmod 3$, we see from Theorem 1.5 that $3 \mid D$. Moreover, $a \equiv 2 \pmod 3$, $b \equiv -1 \pmod 3$. It now follows from (2.28) in the the proof of Theorem 2.19 that

$$B_U(n) \equiv 0 \pmod{3^e}.$$

Consequently, $C'(n) = C(n) = n$ and $A_W(n)$ is an integer for all recurrences $W(a, b)$. □

Theorem 2.23. *Consider the nondegenerate Lucas sequence $U(a, b)$ with discriminant D. Suppose that $n = 2^k n_1$ is an integer such that $k \geq 2$, n_1 is odd, and $a \equiv 0 \pmod{4 \operatorname{rad}(n_1)}$, $b \equiv -1 \pmod{4 \operatorname{rad}(n_1)}$. Then $C'(n) = C(n) = n$ and $A_W(n)$ is an integer for all recurrences $W(a, b)$.*

Proof. We observe that $a + b - 1 \equiv 0 - 1 - 1 \equiv -2 \pmod{\operatorname{rad}(n_1)}$. Then $\gcd(b(a + b-1), n_1) = 1$. Suppose that $p^{e(p)} \parallel n_1$, where $e(p) \geq 1$. Let $e = e(p)$. By Theorem 1.3 (iii),

$$\begin{aligned} &U_3 \equiv -1 \pmod{\operatorname{rad}(n_1)}, \quad U_2 = a \equiv U_4 \equiv 0 \pmod{\operatorname{rad}(n_1)}, \\ &U_5 \equiv 1 \pmod{\operatorname{rad}(n_1)}. \end{aligned}$$

Thus, $\pi_U(p) = 4$. Therefore, by Theorem 1.4 (viii), $4p^e$ is a general period of $U(a, b)$ modulo p^e. We note that $4p^e \mid n$. Therefore, n is also equal to a general period of $U(a, b)$ modulo p^e for each prime p dividing n_1. Then by Theorem 1.2, n is equal to a general period of $U(a, b)$ modulo n_1. Then by Theorem 2.2 (i), we see that

$$B_U(n) = \frac{1}{a+b-1} J(n_1),$$

where $J(n_1) \equiv 0 \pmod{n_1}$. Since $\gcd(a + b - 1, n_1) = 1$, we see that

$$B_U(n) \equiv 0 \pmod{n_1}. \tag{2.35}$$

By Theorem 2.17, we observe that

$$B_U(n) \equiv 0 \pmod{2^k}. \tag{2.36}$$

Consequently, by (2.35) and (2.36), $C'(n) = C(n) = n$ and $A_W(n)$ is an integer for all recurrences $W(a, b)$. □

Consider the nondegenerate Lucas sequence $U(a, b)$ with characteristic roots α and β, where b$D \neq 0$ and $|\alpha| \geq |\beta|$. Suppose that $b = \pm 1$ or $\beta = \pm 1$. In Theorems 2.24, 2.25, 2.26, and 2.27 below, as well as Corollaries 2.5 and 2.6, we present comprehensive results for these specific Lucas sequences concerning the determination of those positive integers n for which $A_W(n)$ is an integer for all recurrences $W(a,b)$. The proofs of these results are given in Section 5. In Section 4, we explicitly find all elements of $S(U)$ for these particular Lucas sequences.

Theorem 2.24. *Consider the nondegenerate Lucas sequence $U(a,1)$, where $a \neq 0$. Then the following hold.*

(i) *$C(n) = L(n)$ exists for all $n \geq 1$. If $n > 1$, then $C(n)$ is even and $L(2) \mid C(n)$. If $n \geq 3$, then $\pi_U(n)$ is even. Moreover, if a is even, then $\pi_U(2)$ is also even.*

(ii) *Suppose that a is odd. If $n \geq 1$, then $C'(n) = C(n)$ and $A_W(C(n))$ is an integer for all recurrences $W(a,1)$. Moreover, if $a \equiv \pm 1 \pmod 6$, then $L(2) = 24$. Further, if $a \equiv 3 \pmod 6$, then $L(2) = 6$.*

(iii) *Suppose that $a \equiv 2 \pmod 4$. If n is odd or $4 \mid n$, then $C'(n) = C(n)$ and $A_W(C(n))$ is an integer for all recurrences $W(a,1)$. If $n \equiv 2 \pmod 4$, then $C'(n) = 2C(n)$ and $A_W(2C(n))$ is an integer for all recurrences $W(a,1)$. In particular, $C'(n)$ exists for all $n \geq 1$. Moreover, $L(2) = 2$.*

(iv) *Suppose that $a \equiv 0 \pmod 4$. If $n \geq 2$, then $n \notin S'(U)$ and $C'(n)$ does not exist for $n \geq 2$. Furthermore, if n is even, then $B_U(n) \not\equiv 0 \pmod n$. In particular, $A_U(n)$ is an integer only if n is odd.*

Below, given the Lucas sequence $U(a,1)$ with discriminant D, we present explicit instances of positive integers n for which $\mathrm{rad}(n) \mid 6D$, $n \in S'(U)$ and $A_W(n)$ is an integer for all recurrences $W(a,1)$.

Corollary 2.5. *Consider the Lucas sequence $U(a,1)$ with discriminant $D = a^2+4$. Let $q \geq 1$ be an arbitrary positive integer such that $Q(q) \geq 5$, and $\mathrm{rad}(q) \mid D$. Then $n \in S'(U)$ and $A_W(n)$ is an integer for all recurrences $W(a,1)$ in the following cases, where $n > 1$, $\mathrm{rad}(n) \mid 6D$, and i and j are nonnegative integers:*

(i) $a \equiv \pm 1 \pmod 6$ *and* $n = 2^{i+3}3^{j+1}q$.

(ii) $a \equiv 3 \pmod 6$ *and we have* $n = 2^{i+1}3^{j+1}$ *or* $n = 2^{i+2}3^{j+1}q$.

(iii) $a \equiv \pm 2 \pmod{12}$ *and we have* $n = 2^{i+2}q$ *or* $n = 2^{i+3}3^{j+1}q$.

(iv) $a \equiv \pm 6 \pmod{12}$ *and* $n = 2^{i+2}3^{j}q$.

Yaqubi and Fatehizadeh prove Corollary 2.5 (i) for the specific cases of the Fibonacci sequence $U(1,1)$ and Lucas sequence $V(1,1)$ in Theorems 3.5 and 3.6 of [16].

Theorem 2.25. *Consider the nondegenerate Lucas sequence $U(a,-1)$ with discriminant $D = a^2 - 4 = (a-2)(a+2)$. Let $n = 2^k n_1 n_2$, where $k \geq 0$, n_1 and n_2 are both odd, $\mathrm{rad}(n_1) \mid a-2$, and $\gcd(n_2, a-2) = 1$. Then the following hold.*

(i) *$C(n)$ exists for all $n \geq 1$. If $n > 1$, then $C(n) > 1$ and $\gcd(\mathrm{rad}(6D), C(n)) > 1$.*

(ii) *Suppose that $a \neq 0$, ± 1, or ± 2. Then $C(n_1) = n_1 = C'(n_1)$ and $A_W(n_1)$ is an integer for all recurrences $W(a, -1)$. Moreover, if $C(n)$ is odd, then n is odd, $C'(n) = C(n)$, and $A_W(C(n))$ is an integer for all recurrences $W(a, -1)$.*

(iii) *Suppose that a is odd. If $n \geq 1$, then $C'(n) = C(n)$ and $A_W(C(n))$ is an integer for all recurrences $W(a, -1)$.*

(iv) *Suppose that $a \equiv 0 \pmod 4$. If $C(n) \equiv 2 \pmod 4$, then $C'(n) = 2C(n)$ and $A_W(2C(n))$ is an integer for all recurrences $W(a, -1)$. Moreover, if $C(n) \equiv 0 \pmod 4$, then $C'(n) = C(n)$ and $A_W(C(n))$ is an integer for all recurrences $W(a, -1)$. In particular, $C'(n)$ exists for all $n \geq 1$.*

(v) *Suppose that $a \equiv 2 \pmod 4$. If $C(n)$ is even, then $C'(n)$ does not exist. In particular, if n is even or $\gcd(n, a + 2) > 1$, then $C'(n)$ does not exist.*

Corollary 2.6. *Consider the nondegenerate Lucas sequence $U(a, -1)$ with discriminant $D = a^2 - 4 = (a + 2)(a - 2)$. Let q_1 be an arbitrary positive odd integer such that $\mathrm{rad}(q_1) \mid a - 2$. Let q_2 be an arbitrary positive odd integer such that $Q(q_2) \geq 5$ and $\mathrm{rad}(q_2) \mid D$. Let q_3 be an arbitrary positive odd integer such that $\mathrm{rad}(q_3) \mid D$. Then $n \in S'(U)$ and $A_W(n)$ is an integer for all recurrences $W(a, 1)$ in the following cases given in parts (i)–(v), where $n > 1$, $\mathrm{rad}(n) \mid 6D$, and i and j are nonnegative integers:*

(i) *$n = q_1$, where a is an arbitrary integer such that $a \neq 0, \pm 1$, or ± 2.*

(ii) *$a \equiv \pm 1 \pmod 6$ and $n = 2^{i+1}3^{j+1}q_2$.*

(iii) *$a \equiv 3 \pmod 6$ and $n = 2^{i+2}3^{j+1}q_2$.*

(iv) *$a \equiv 0 \pmod 4$ and $n = 2^{i+2}q_3$.*

(v) *$a \equiv 0 \pmod{12}$ and $n = 2^{i+2}3^{j+1}q_2$.*

Theorem 2.26. *Consider the nondegenerate Lucas sequence $U(a, b) = U(a, -a+1)$ with discriminant $D = (a - 2)^2 = (-b - 1)^2$ and characteristic roots $\alpha = a - 1$ and $\beta = 1$, where $a \neq 0, 1$, or 2. Let n be a positive integer. Then the following hold.*

(i) *If $\gcd(n, b) = \gcd(n, -a + 1) = 1$, then $E_U(n) = 1$.*

(ii) *If $n \mid b = -a+1$ and $m \in S'(U)$, then $A_W(mn)$ is an integer for all recurrences $W(a, -a + 1)$.*

(iii) *$n \in S(U)$ if and only if $n \in T(U)$, where $T(U)$ is as defined in Remark 2.2.*

(iv) *Suppose that a is odd. Then $n \in S'(U)$ if and only if $n \in S(U)$, which occurs if and only if $n \in T(U)$. In particular, if $n \in S(U)$, then $A_W(n)$ is an integer for all recurrences $W(a, -a+1)$. Moreover, if $a = 3$, then $D = 1$ and $n \in S(U)$ if and only if $n = 1$. Furthermore, if $n \mid b$, then it also occurs that $A_W(n)$ is an integer for all recurrences $W(a, -a+1)$.*

(v) *Suppose that a is even. Then $n \in S'(U)$ if and only if n is odd and $n \in S(U)$. In particular, if $a = 2 + 2^k$ for some $k \geq 1$, then $n \notin S'(U)$ for $n > 1$. If n is odd and $n \in S(U)$, then $A_W(n)$ is an integer for all recurrences $W(a, -a+1)$.*

Theorem 2.27. *Consider the nondegenerate Lucas sequence $U(a, b) = U(b-1, b)$ with discriminant $D = (b+1)^2 = (a+2)^2$ and characteristic roots $\alpha = b$ and $\beta = -1$, where $a \neq 0, -1$, or -2. If $n > 1$ and $\gcd(n, b) = 1$, then $\pi_U(n)$ is even. Moreover, the following hold.*

(i) *If b is even, $n \mid b$, and n is even, then $A_W(n)$ is an integer for all recurrences $W(b-1, b)$.*

(ii) *If $n > 1$, a is even, and $n \in S(U)$, then $A_U(n)$ is not an integer. In particular, $S'(U) = \{1\}$ if a is even. Moreover, $S(U) = \{1\}$ if a is odd.*

(iii) *Suppose that a is odd. Then b is even. Let m be an even integer such that $m \mid b$ and let t be an integer such that $t \in T(U)$. Then t is odd and $A_W(mt)$ is an integer for all recurrences $W(b-1, b)$.*

The following example illustrates Theorem 2.27.

Example 2.2. Consider the Lucas sequence $U(7, 8)$ with discriminant $D = 81 = 3^4$ and characteristic roots $\alpha = 8$ and $\beta = -1$. We observe that $U_3 = 7^2 + 8 = 57 = 3 \cdot 19$. It follows from Theorem 4.1 below that $3 \cdot 19 = 57 \in T(U)$. Then by Theorem 2.27 (iii),

$$B_U(8 \cdot 3 \cdot 19) = B_U(456) \equiv 0 \pmod{456},$$

and $A_W(456)$ is an integer for all recurrences $W(7, 8)$.

3. Auxiliary Results

In this section, we provide results that will be needed for the proofs of Theorems 2.24–2.27 as well as Corollaries 2.5 and 2.6. We let $\text{ord}_m(n)$ denote the multiplicative order of n modulo m.

Theorem 3.1. *Let $U(a, b)$ be a nondegenerate Lucas sequence and let $m \geq 2$ be an integer such that $\gcd(m, b) = 1$. Let $h = \text{ord}_m(-b) = 2^c h'$ and $\rho = \rho_U(m) = 2^d \rho'$, where h' and ρ' are odd integers. Let $\pi = \pi_U(m)$ and $H = \text{lcm}(h, \rho)$.*

(i) *Either* $\pi = H$ *or* $\pi = 2H$.

(ii) *Suppose that* $m = p^i$, *where* p *is an odd prime and* $i \geq 1$. *If* $c \neq d$, *then* $\pi = 2H$. *If* $c = d > 0$, *then* $\pi = H$.

This is proved in Theorems 3 and 4 of Wyler [15].

We have the following corollaries of Theorem 3.1 corresponding to the cases in which $b = \pm 1$.

Corollary 3.1. *Consider the nondegenerate Lucas sequence* $U(a, 1)$ *and let* $m \geq 2$. *Let* $\pi = \pi_U(m)$ *and* $\rho = \rho_U(m)$. *Let* $E = E_U(m) = \pi/\rho$. *Then the following hold.*

(i) $E = 1, 2,$ *or* 4.

(ii) *Suppose that* $m = p^i$, *where* p *is an odd prime and* $i \geq 1$.

(a) *If* $\rho \equiv 2 \pmod 4$, *then* $E = 1$.

(b) *If* $\rho \equiv 0 \pmod 4$, *then* $E = 2$.

(c) *If* $\rho \equiv 1 \pmod 2$, *then* $E = 4$.

(iii) $\pi_U(m)$ *is even if it is not the case that* $m = 1$ *or both* $m = 2$ *and* $a \equiv 1 \pmod 2$.

(iv) $L(m)$ *is even if* $m \geq 2$.

Proof. Parts (i) and (ii) are direct consequences of Theorem 3.1 upon noting that $h = \text{ord}_m(-1) = 2$ for $m \geq 3$ and $h = 1$ for $m = 2$.

We now prove part (iii). Suppose that $m > 1$ and it is not the case that $m = 2$ and a is odd. Suppose first that m is not a power of 2. Then m has an odd prime divisor p. Since $\pi(p) = \rho(p)E_U(p)$, it follows from part (ii) that $\pi_U(p)$ is even. Thus, $\pi_U(m)$ is even by Theorem 1.2.

Now suppose that m is a power of 2. If $a \equiv 0 \pmod 2$, then $\pi_U(2) = 2$, which implies that $\pi_U(m)$ is even. If $a \equiv 1 \pmod 2$, then $U_3 = a^2 + 1 \equiv 2 \pmod 4$, and $\pi_U(2) = 3 < \pi_U(4)$. We now see by Theorem 1.4 (viii) that $\pi_U(4) = 6$. It again follows that $\pi_U(m)$ is even if $m > 2$, and part (iii) is established. Since $2 \mid L(2)$ and $\pi_U(m) \mid L(m)$, it follows from part (iii) that part (iv) holds. $\square$

Corollary 3.2. *Consider the nondegenerate Lucas sequence* $U(a, -1)$ *and assume that* $m \geq 2$. *Let* $\pi = \pi_U(m)$ *and* $\rho = \rho_U(m)$. *Let* $E = E_U(m) = \pi/\rho$. *Then the following hold.*

(i) $E = 1$ *or* 2.

(ii) *Suppose that* $m = p^i$, *where* p *is an odd prime and* $i \geq 1$.

(a) *If* $\rho \equiv 0 \pmod 2$, *then* $E = 2$.

(b) *If* $\rho \equiv 1 \pmod 2$*, then* $E = 1$ *or* 2.

Proof. This follows immediately from Theorem 3.1 upon noting that $\mathrm{ord}_m(-b) = \mathrm{ord}_m(1) = 1$. □

Remark 3.1. We show that both possibilities for E can occur in part (ii) (b) of Corollary 3.2. Consider the Lucas sequence $U(3,-1)$. Then $\rho_U(13) = \rho_U(29) = 7$, while $\pi_U(29) = 7$, whereas $\pi_U(13) = 14$. Hence, $E_U(29) = 1$, whereas $E_U(13) = 2$.

Theorem 3.2. *Let* $U(a,b)$ *be a Lucas sequence with discriminant* D*, where* $b = \pm 1$*. Suppose that* $p \mid D$*. Then the following hold.*

(i) *If* $b = 1$*, then* $p = 2$ *or* $p \equiv 1 \pmod 4$*.*

(ii) *Suppose that* $b = -1$*. Then* $a \equiv \pm 2 \pmod p$*. If* $a \equiv 2 \pmod p$*, then* $E_U(p^i) = 1$ *for* $i \geq 1$*. If* $a \equiv -2 \pmod p$ *and* $p > 2$*, then* $E_U(p^i) = 2$ *for* $i \geq 1$*.*

Proof. (i) Since $D = a^2 + 4 \equiv 0 \pmod p$, we see that $p = 2$ or $(-4/p) = 1$ for $p > 2$. Then $p = 2$ or $p \equiv 1 \pmod 4$ by the law of quadratic reciprocity.

(ii) We note that $D = a^2 - 4 = (a-2)(a+2) \equiv 0 \pmod p$. Thus, $a \equiv \pm 2 \pmod p$. First, suppose that $a \equiv 2 \pmod p$. Then by the proof of Theorem 2.19, $E_U(p) = 1$. It now follows from Theorem 1.4 (vii) and (viii) and Theorem 1.5 (i), (ii), and (iv) that $E_U(p^i) = 1$ for $i \geq 1$. Now suppose that $a \equiv -2 \pmod p$ and $p > 2$. Then by the proof of Theorem 2.20, $E_U(p) = 2$. It then follows from Theorem 1.4 (vii) and (viii) and Theorem 1.5 (i), (ii), and (iv) that $E_U(p^i) = 2$ for $i \geq 1$. □

Theorems 3.3 and 3.4 treat particular cases in which exactly one of the characteristic roots of $U(a,b) = \pm 1$.

Theorem 3.3. *Consider the nondegenerate Lucas sequence* $U(a,b) = U(-b+1, b)$*, where* $b \neq 0$ *and* $b \neq \pm 1$*, with characteristic roots* α *and* β*, where* $|\alpha| \geq |\beta|$*. Then* $\alpha = -b$*,* $\beta = 1$*, and* $D = (-b-1)^2 = (a-2)^2$*. Suppose that* $\gcd(n,b) = 1$*. Then* $U_{n+1} = (-b)U_n + 1$*. Furthermore,* $E_U(n) = 1$ *and* $\pi_U(n) = \rho_U(n)$*. Moreover,* $U_i \equiv 1 \pmod b$ *for* $i \geq 1$*.*

Proof. It is easily seen that $\alpha = -b$, $\beta = 1$, and $D = (a-2)^2$. Since $\gcd(n,b) = 1$, $\rho(n)$ exists. By the Binet formula (1.5),

$$U_n = \frac{(-b)^n - 1^n}{-b-1} = (-b)^{n-1} + (-b)^{n-2} + \cdots + (-b) + 1.$$

Thus,

$$U_{n+1} = (-b)U_n + 1. \tag{3.1}$$

Let $\rho = \rho_U(n)$. Then $U_\rho \equiv 0 \pmod n$ and $U_{\rho+1} \equiv 1 \pmod n$ by (3.1). Hence, $E_U(n) = 1$. □

Theorem 3.4. *Consider the nondegenerate Lucas sequence $U(a,b) = U(b-1,b)$, where $b \neq 0$ and $b \neq \pm 1$, with characteristic roots α and β, where $|\alpha| \geq |\beta|$. Then $\alpha = b$, $\beta = -1$, and $D = (b+1)^2 = (a+2)^2$. Suppose that $\gcd(n,b) = 1$. Then $U_{n+1} = bU_n + (-1)^n$. Moreover, $E_U(n) = 1$ if $\rho_U(n)$ is even and $E_U(n) = 2$ if $\rho_U(n)$ is odd. Additionally, $M_U(n) \equiv 1 \pmod{n}$ if $\rho(n)$ is even and $M_U(n) \equiv -1 \pmod{n}$ if $\rho_U(n)$ is odd, where $M_U(n)$ is the multiplier of $U(b-1,b)$ modulo n and is defined in (1.10). Furthermore, $\pi_U(n)$ is even if $n > 1$.*

Proof. It is easy to see that $\alpha = b$, $\beta = -1$, and $D = (b+1)^2 = (a+2)^2$. Since $\gcd(n,b) = 1$, $\rho(n)$ exists. We observe that b is odd if n is even. Thus, if $n = 2$, then $U_2 = b - 1 \equiv 0 \pmod{2}$, and $\rho(2)$ is even. By the Binet formula (1.5),

$$U_n = \frac{b^n - (-1)^n}{b+1} = b^{n-1} - b^{n-2} + \cdots + (-1)^n b + (-1)^{n+1}.$$

Hence,

$$U_{n+1} = bU_n + (-1)^n. \tag{3.2}$$

Let $\rho = \rho_U(n)$. Then $U_\rho \equiv 0 \pmod{n}$ and $U_{\rho+1} \equiv M_U(n) \equiv (-1)^n \pmod{n}$ by (3.2). Therefore, $E_U(n) = 1$ if $\rho_U(n)$ is even and $E_U(n) = 2$ if $\rho_U(n)$ is odd. Since $\pi_U(n) = \rho_U(n)E_U(n)$, we find that $\pi_U(n)$ is always even for $n > 1$. ☐

4. Necessary and Sufficient Conditions for $\pi_U(n)$ to Divide n

Suppose that we are given the Lucas sequence $U(a,b)$, where $\gcd(a,b) = 1$. Theorem 4.1 due to Smyth [9] gives a necessary and sufficient condition for U_n to be divisible by n when $\gcd(n,b) = 1$. By (1.12) and (1.10), $n \mid U_n$ if and only if $\rho_U(n) \mid n$. We let $T(U)$ denote the set of positive integers n coprime to b such that $n \mid U_n$, or equivalently, $\rho_U(n) \mid n$.

Theorem 4.1. *Consider the nondegenerate Lucas sequence $U(a,b)$ with discriminant D, where $\gcd(a,b) = 1$. Let $q_0 = 1$ or 6 if $a \equiv 3 \pmod{6}$ and $b \equiv \pm 1 \pmod{6}$. Let $q_0 = 1$ or 12 if $a \equiv \pm 1 \mod 6$ and $b \equiv 1 \pmod{6}$. In all other cases, let $q_0 = 1$ only. Then $q_0 \in T(U)$.*

Moreover, $n \in T(U)$ if and only if n can be written in the form

$$q_0 q_1 \cdots q_r \tag{4.1}$$

for some $r \geq 0$, where for $i = 1, 2, \ldots, r$, q_i is a prime such that $q_i \mid DU_{q_0 q_1 \cdots q_{i-1}}$. We allow the possibility that $q_i = q_j$ for $1 \leq i < j$. Moreover, if n has the form given in (4.1), then $q_0 q_1 \cdots q_i \in T(U)$ for $i = 0, 1, \ldots, r$. Furthermore, if $D = 1$, then $n \in T(U)$ if and only if $n = 1$.

This follows from results in Theorem 1 of [9] and Theorem 8 (iii) of [10].

Theorem 4.2. *Consider the nondegenerate Lucas sequence $U(a,b)$ with discriminant D, where $a = -b+1$. Then $n \in S(U)$ if and only if $n \in T(U)$.*

Proof. By Theorem 3.3, $E(n) = 1$ and $\pi_U(n) = \rho_U(n)$ for all $n \geq 1$. The result now follows immediately. □

Given the Lucas sequence $U(-b+1, b)$, we can now use Theorem 4.1 to explicitly find all integers $n \in S(U)$. Theorem 4.3 below makes further use of Theorem 4.1 to give necessary and sufficient conditions for n to be a member of $S(U)$ for particular Lucas sequences $U(a,b)$ for which $b = \pm 1$ or $a = b-1$. We let $\nu_p(m)$ denote the largest nonnegative integer i such that $p^i \mid m$.

Theorem 4.3. *Consider the nondegenerate Lucas sequence $U(a,b)$ with discriminant D, where $b = \pm 1$ or b is odd and $a = b-1$. Let p be an arbitrary prime. Then $E(p) \mid 4$ if $b = 1$ and $E(p) \mid 2$ if $b = -1$ or it is the case that b is odd and $a = b-1$. Let $s_0 = 1$ or 6 if $a \equiv 3 \pmod 6$ and $b = 1$ or it is the case that $a \equiv \pm 1 \pmod 6$ and $b = -1$. Let $s_0 = 1$ or 24 if $a \equiv \pm 1 \pmod 6$ and $b = 1$. Let $s_0 = 1$ or 12 if $a \equiv 3 \pmod 6$ and $b = -1$. Let $s_0 = 1$ or 2 if b is odd and $a = b-1$. In all other cases, let $s_0 = 1$ only. Then $s_0 \in S(U)$. Furthermore, $n \in S(U)$ if and only if $n = 1$ or n can be written in the form*

$$s_0 2^{\epsilon(s_0)} s_1 2^{\epsilon(s_1)} \cdots s_r 2^{\epsilon(s_r)}, \tag{4.2}$$

where $\epsilon(s_0) = 0$, and s_i and $\epsilon(s_i)$ are defined as follows for $i = 1, 2, \ldots, r$. Let

$$n_{i-1} = s_0 2^{\epsilon(s_0)} s_1 2^{\epsilon(s_1)} \cdots s_{i-1} 2^{\epsilon(s_{i-1})}.$$

for $i = 1, 2, \ldots, r$. Let s_i be a prime such that $s_i \mid DU_{n_{i-1}}$ and define

$$\epsilon(s_i) = \max(\nu_2(\pi(s_i)) - \nu_2(n_{i-1}), 0).$$

In addition to n_r being a member of $S(U)$, $n_i \in S(U)$ for $i = 0, 1, \ldots, r-1$.

Proof. We observe that if $n \in S(U)$, then $n \in T(U)$. Moreover, $\pi_U(p) = \rho_U(p) E_U(p)$ for all primes p. The assertions regarding $E_U(p)$ are proved in Corollaries 3.1 and 3.2 and in Theorem 3.4. Moreover, by Corollary 3.1 (iii) and Theorem 3.4, if $b = 1$, then $\pi_U(n)$ is even for $n > 2$, while it is the case that if b is odd, $a = b-1$, $n > 1$, and $\gcd(n, b) = 1$, then $\pi_U(n)$ is even. Let $L(n)$ be defined as in Theorem 2.8. Then by Theorem 2.8, $L(n) = C(n)$ and $L(n) \in S(U)$. We note that if $n \in S(U)$, then $n = L(n)$. Since $n \in T(U)$, it follows by Theorem 4.1 that $\gcd((L(n), 6D) > 1$ if $n > 1$. By Theorem 2.9 (vii), $L(2) = L(3) = 24$ if $a \equiv \pm 1 \pmod 6$ and $b \equiv 1 \pmod 6$. Moreover, by Theorem 2.9 (xi), $L(2) = L(3) = 12$ if $a \equiv 3 \pmod 6$ and $b \equiv -1 \pmod 6$. Further, by Theorem 2.9 (viii), $L(2) = L(3) = 6$ if $a \equiv 3 \pmod 6$ and $b \equiv 1 \pmod 6$. In all other cases, $D = 1$ or $\gcd(L(2), D) > 1$ or $\gcd(L(3), D) > 1$. The rest of the proof of Theorem 4.3 follows from Smyth's proof of Theorem 1 in [9]. □

Remark 4.1. We note that in formula (4.2) of the statement of Theorem 4.3, we have that $0 \leq \epsilon(s_i) \leq 2$ if $b = 1$, while $0 \leq \epsilon(s_i) \leq 1$ if $b = -1$ or $a = b - 1$, where $1 \leq i \leq r$. This follows from the fact that $E(p) \mid 4$ if $b = 1$, whereas $E(p) \mid 2$ if $b = -1$ or $a = b - 1$.

5. Proofs of the Main Results

We are now ready for the proofs of Theorems 2.24–2.27 and also of Corollaries 2.5 and 2.6.

Proof of Theorem 2.24. Part (i) follows from Corollary 3.1 (iii) and (iv), Theorem 2.11, Theorem 2.8, and Corollary 2.4 (i).

We now prove parts (ii)–(iv) together. The assertions in parts (ii) and (iii) concerning $L(2)$ follow from Theorem 2.9. By Remark 2.3, in order to show that $A_W(C'(n))$ is an integer for all recurrences $W(a, 1)$, it suffices to show that $C'(n)$ exists which implies by definition that $B_U(C'(n)) \equiv 0 \pmod{C'(n)}$. Since $b = 1$, we see from Theorem 2.2 (i) and Corollary 2.1 (i) that if $n \geq 1$, then

$$B_U(n) = \frac{1}{a} J(n), \tag{5.1}$$

where $J(n) = U_{n+1} - 1 + U_n$. Then

$$J(C(n)) \equiv 0 \pmod{C(n)} \tag{5.2}$$

by Theorem 2.2 (i), since $C(n) \in S(U)$ by the definition of $C(n)$. Suppose that $\gcd(p, a) = 1$ and $p^{e(p)} \parallel C(n)$, where $e(p) \geq 1$. Let $e = e(p)$. Then by (5.1) and (5.2),

$$B_U(C(n)) \equiv 0 \pmod{p^e} \quad \text{if} \quad \gcd(p, a) = 1. \tag{5.3}$$

We note that $C(n)$ is even by part (i). Thus, if $2^i \parallel C(n)$, where $i \geq 1$, then

$$B_U(C(n)) \equiv 0 \pmod{2^i}$$

when a is odd.

Now suppose that p is odd, $p \mid a$, where a is not necessarily odd, and $p^{j(p)} \parallel C(n)$, where $j(p) \geq 1$. Let $j = j(p)$. By Lemma 2.1,

$$B_U(2mp^j) \equiv 0 \pmod{p^j} \tag{5.4}$$

for all $m \geq 1$. Since $C(n)$ is even, we see that $2p^j \mid C(n)$. It now follows from (5.4) that

$$B_U(C(n)) \equiv 0 \pmod{p^j} \ \text{ if } \ p \ \text{ is odd and } \ p \mid a. \tag{5.5}$$

By (5.3) and (5.5), it follows that if a is odd, then

$$B_U(C(n)) \equiv 0 \pmod{C(n)},$$

which implies that $C'(n) = C(n)$ for all $n \geq 1$.

Next suppose that $a \equiv 2 \pmod 4$. Suppose that $2^k \parallel C(n)$, where $k \geq 1$. By Theorems 2.14 and 2.15, if m is a positive odd integer, then

$$B_U(2^k m) \not\equiv 0 \pmod{2^k} \quad \text{if} \quad k = 1, \tag{5.6}$$

while

$$B_U(2^k m) \equiv 0 \pmod{2^k} \quad \text{if} \quad k \geq 2. \tag{5.7}$$

It now follows from (5.3), (5.5), (5.6), and (5.7) that if $a \equiv 2 \pmod 4$, then $C'(n)$ exists for all $n \geq 1$. Moreover, $C'(n) = 2C(n)$ if $n \equiv 2 \pmod 4$, while $C'(n) = C(n)$ in all other cases.

Finally, suppose that $a \equiv 0 \pmod 4$. Suppose further that n is even and $2^\ell \parallel n$. Then by Theorem 2.16,

$$B_U(n) \not\equiv 0 \pmod{2^\ell}.$$

Since $C(n)$ is always even for $n \geq 2$, we see that $C'(n)$ does not exist if $n \geq 2$. □

Proof of Corollary 2.5. This follows from Theorems 2.24, 2.9, 2.11, 2.12 (i) and (iv), 3.2 (i) and 4.3, and from Corollaries 2.3 and 3.1. □

Proof of Theorem 2.25. (i) By Theorem 2.11, $C(n)$ exists for all n. By Theorem 2.8 and Remark 2.6, if $n > 1$, then $n \mid C(n)$. As $C(n) \in S(U)$, it follows from the fact that $\rho(n) \mid \pi(n)$ that $C(n) \in T(U)$. We now see from Theorem 4.1 that $C(n) \in T(U)$ implies that $\gcd(\mathrm{rad}(6D), C(n)) > 1$.

We now prove parts (ii)–(v) together. Noting that $b = -1$, we see from Theorem 2.2 (i) and Corollary 2.1 (i) that

$$B_U(C(n)) = \frac{1}{a-2} J(C(n)), \tag{5.8}$$

where $J(C(n)) = U_{C(n)+1} - 1 - U_{C(n)}$. Then by Theorem 2.2 (i),

$$J(C(n)) \equiv 0 \pmod{C(n)}, \tag{5.9}$$

since $\pi_U(C(n)) \mid C(n)$ by Remark 2.6. Hence,

$$J(C(n)) \equiv 0 \pmod{n_2}, \tag{5.10}$$

Since $\gcd(n_2, a-2) = 1$, it follows from (5.8) and (5.10) that

$$B_U(C(n)) \equiv 0 \pmod{n_2}. \tag{5.11}$$

We now note that it follows from Theorem 2.19 that $C'(n_1) = C(n_1) = n_1$. Hence,

$$B_U(n_1) \equiv 0 \pmod{n_1}. \tag{5.12}$$

Since $n_1 \mid C(n)$, we see that

$$B_U(C(n)) \equiv 0 \pmod{n_1}. \tag{5.13}$$

Noting that $\gcd(n_1, n_2) = 1$, it now follows from (5.11) and (5.13) that

$$B_U(C(n)) \equiv 0 \pmod{n_1 n_2}. \tag{5.14}$$

We now find from (5.14) that

$$B_U(C(n)) \equiv 0 \pmod{C(n)} \quad \text{if} \quad C(n) \text{ is odd}, \tag{5.15}$$

which yields that $C'(n) = C(n)$ in this case. Since $n \mid L(n) = C(n)$, we also see that if $C(n)$ is odd, then n is odd.

We next suppose that a is odd. Then $a-2$ is odd. It follows from (5.8) and (5.9) that

$$B_U(C(n)) \equiv 0 \pmod{2^k n_2}, \tag{5.16}$$

because $J(C(n)) \equiv 0 \pmod{C(n)}$, $2^k n_2 \mid C(n)$, and $\gcd(2^k n_2, a-2) = 1$. We now see by (5.13) and (5.16) that

$$B_U(C(n)) \equiv 0 \pmod{n} \text{ for } n \geq 1 \text{ if } a \text{ is odd}, \tag{5.17}$$

which implies that $C'(n) = C(n)$ for all n if a is odd. Parts (ii) and (iii) are now established.

We now suppose that a and $C(n)$ are both even. First suppose that $a \equiv 2 \pmod 4$. Then by Theorem 2.18, if m is even, then $B_U(m) \not\equiv 0 \pmod m$. Suppose that $C'(n)$ exists. Since $C(n)$ is even and $C(n) \mid C'(n)$, this would imply that $C'(n)$ is even and $B_U(C'(n)) \equiv 0 \pmod{C'(n)}$, which is a contradiction. Hence, $C'(n)$ does not exist if $n \equiv 2 \pmod 4$ and $C(n)$ is even. Since $n \mid C(n)$ by definition, we see that $C(n)$ is even if n is even. Now suppose that p is odd and $p \mid \gcd(n, a+2)$. It follows from (2.29) in the proof of Theorem 2.20 that $\pi_U(p) = 2p$. Since $\pi_U(p) \mid \pi_U(n)$, so $\pi_U(p) \mid L(n) = C(n)$, we see that $C(n)$ is also even in this case. Part (v) is now proven.

We next suppose that $a \equiv 0 \pmod 4$. Then by Theorems 2.14 and 2.17, if m is even and $2^k \parallel m$, then $B_U(m) \not\equiv 0 \pmod{2^k}$ if $k = 1$, while $B_U(m) \equiv 0 \pmod{2^k}$ if $k \geq 2$. Since $2^k \mid C(n)$, we then have that

$$B_U(C(n)) \equiv 1 \pmod{2^k} \text{ if } k = 1, \tag{5.18}$$

while

$$B_U(C(n)) \equiv 0 \pmod{2^k} \text{ if } k \geq 2. \tag{5.19}$$

Noting that $\operatorname{lcm}(2^k, n_1, n_2) = 2^k n_1 n_2 = n$, it now follows from (5.14), (5.18), and (5.19) that

$$B_U(C(n)) \not\equiv 0 \pmod{n} \quad \text{if} \quad k = 1, \tag{5.20}$$

while

$$B_U(C(n)) \equiv 0 \pmod{n} \quad \text{if} \quad k \geq 2. \tag{5.21}$$

By (5.20) and (5.21), we see that $C'(n) = 2C(n)$ if $k = 1$, whereas $C'(n) = C(n)$ if $k \geq 2$. Part (iv) now follows. □

Proof of Corollary 2.6. This follows from Theorems 2.25, 2.9, 2.11, 2.12 (ii) and (iii), 3.2 (ii) and 4.3, and from Corollaries 2.3 and 3.2. □

Proof of Theorem 2.26. We observe that $a + b - 1 = 0$. By Theorem 3.3, $\alpha = a - 1$ and $\beta = 1$, $D = (a-2)^2$, and $E_U(n) = 1$ if $\gcd(n, b) = 1$. Hence, part (i) holds. Part (ii) follows from Theorem 2.10 (i). Part (iii) follows from Theorems 4.1 and 4.2.

We now prove parts (iv) and (v) together. Suppose that $n \in S(U)$. Then $\gcd(n, b) = 1$. We observe that it follows from Theorem 4.1 that if $D = 1$, then $S(U) = \{1\}$. Let $n = n_1 n_2$, where n_2 is the largest divisor of n that is relatively prime to $a - 2 = -b - 1$. Since $n \in S(U)$, it follows by definition that n is equal to a general period of $U(a, b)$ modulo n. Noting that $\gcd(n_2, b(-b-1)) = 1$, it follows by Corollary 2.2 (ii) that

$$B_U(n) \equiv 0 \pmod{n_2}. \tag{5.22}$$

Now suppose that $p^{e(p)} \parallel n_1$, where p is odd. Let $e = e(p)$. Then $p \mid a - 2$, which implies that $p \mid D$. We claim that if $p = 3$ and $e \geq 2$, then $U_3 \not\equiv 0 \pmod{9}$. We note that $U_3 = a^2 + b = a^2 - a + 1$. By inspection, one sees that $U_3 \not\equiv 0 \pmod{9}$ for $a = 0, 1, \ldots, 8$. Thus, $U_3 \not\equiv 0 \pmod{9}$ for any integer a. It now follows from Theorem 1.5 (i), (ii), and (iv) that $U(a, b)$ is uniformly distributed modulo p^e with each residue appearing exactly $E(p) = 1$ time in a least period of $U(a, b)$ modulo p^e. Since n is a general period of $U(a, b)$ modulo p^e, we find that

$$B_U(n) \equiv B_U(p^e) \equiv 1 + 2 + \cdots + p^e = \frac{p^e(p^e+1)}{2} \equiv 0 \pmod{p^e}. \tag{5.23}$$

If n is odd or it is the case that both a is odd and n is even, it follows from (5.22) and (5.23) that $B_U(n) \equiv 0 \pmod{n}$, which implies that $n \in S'(U)$ and $A_W(n)$ is an integer for all recurrences $W(a, -a+1)$.

Now suppose that a is even and n is even. If $a \equiv 2 \pmod{4}$, then $b = -a+1 \equiv -1 \pmod{4}$, while if $a \equiv 0 \pmod{4}$, then $b = -a + 1 \equiv 1 \pmod{4}$. In both cases, it follows from Theorems 2.16 and 2.18 that

$$B_U(r) \not\equiv 0 \pmod{r} \quad \text{if} \quad a \quad \text{is even and} \quad r \quad \text{is even.} \tag{5.24}$$

By definition, $n \in S'(U)$ only if $n \in S(U)$. It now follows by (5.24) that if $n \in S(U)$, n is even, and a is even, then $n \notin S'(U)$. Finally, suppose that $a = 2 + 2^k$ for some

$k \geq 1$. Then $D = (a-2)^2 = 2^{2k}$. It follows from Theorems 4.1 and 4.2 that $n \in S(U)$ only if $n = 1$ or n is even. Thus in this case, $S'(U) = \{1\}$. Parts (iv) and (v) now follow. □

Proof of Theorem 2.27. By Theorem 3.4, $\alpha = b$ and $\beta = -1$, $D = (b+1)^2 = (a+2)^2$, and $\pi_U(n)$ is even if $n > 1$ and $\gcd(n, b) = 1$. Part (i) follows from Theorem 2.10 (ii) upon noting that $a \equiv -1 \pmod{b}$.

(ii) Suppose that $n > 1$ and $n \in S(U)$. Then $\gcd(n, b) = 1$ and $\pi_U(n) \mid n$. Since $\pi_U(n)$ is even, this implies that n is even.

Now suppose that a is odd. Then b is even, which is a contradiction. Hence, $S(U) = \{1\}$ in this case. Next suppose that a is even. If $a \equiv 2 \pmod 4$, then $b = a + 1 \equiv -1 \pmod 4$. If $a \equiv 0 \pmod 4$, then $b = a + 1 \equiv 1 \pmod 4$. In both cases, we see by Theorems 2.16 and 2.18 that if r is even, then $B_U(r) \not\equiv 0 \pmod{r}$. Since n is even if $n \in S(U)$, this implies that $S'(U) = \{1\}$.

(iii) Let $W(b-1, b)$ be an arbitrary recurrence. We observe that t is odd and $\gcd(m, t) = 1$, since $\gcd(t, b) = 1$ and $m \mid b$. By Theorem 2.10 (ii) and the proof of Theorem 2.7,

$$B_W(mt) \equiv 0 \pmod{m}. \tag{5.25}$$

By the definition of $T(U)$, $\rho_U(t) \mid t$. Thus, $\rho_U(t)$ is odd. It follows from Theorem 3.4 that $\pi_U(t) = 2\rho_U(t)$ and $M_U(t) \equiv -1 \pmod{t}$. Let $\rho = \rho_U(t)$. Then by (1.10),

$$U_{\rho+i} \equiv -U_i \pmod{t} \tag{5.26}$$

for $1 \leq i \leq \rho$. It now follows from (5.26) and (1.16) that

$$W_{\rho+i} \equiv -W_i \pmod{t} \tag{5.27}$$

for $1 \leq i \leq \rho$. Thus,

$$B_W(2\rho) \equiv 0 \pmod{t}. \tag{5.28}$$

Since $\pi_W(t) \mid \pi_U(t)$, $\pi_U(t) = 2\rho_U(t)$, $\rho_U(t) \mid t$, and $2 \mid m$, we see that mt is a general period of $W(b-1, b)$ modulo t. Thus, by (5.28),

$$B_W(mt) \equiv 0 \pmod{t}. \tag{5.29}$$

It now follows from (5.25) and (5.29) that $B_W(mt) \equiv 0 \pmod{mt}$, and thus $A_W(mt)$ is an integer for all recurrences $W(b-1, b)$. □

Acknowledgments. The authors are indebted to Hana Bílková for fruitful discussions. Supported by the Czech Academy of Sciences (RVO 67985840).

References

[1] R. T. Bumby, A distribution property for linear recurrence of the second order, *Proc. Amer. Math. Soc.* **50** (1975), 101-106.

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

[3] R. D. Carmichael, On sequences of integers defined by recurrence relations, *Quart. J. Pure Appl. Math.* **48** (1920), 343-372.

[4] A. Fatehizadeh and D. Yaqubi, Average of the Fibonacci numbers, *J. Integer Seq.* **25** (2022), no. 2, Article 22.2.6, 10 pp.

[5] D. Kalman and R. Mena, The Fibonacci numbers–exposed, *Math. Mag.* **76** (2003), 167-181.

[6] D. H. Lehmer, An extended theory of Lucas' functions, *Ann. of Math.* **31** (1930), 419-448.

[7] *On-Line Journal of Integer Sequences*, https://oeis.org, 2022.

[8] T. N. Shorey and R. Tijdeman, *Exponential Diophantine Equations*, Cambridge Univ. Press, Cambridge, 1986.

[9] C. Smyth, The terms in Lucas sequences divisible by their indices, *J. Integer Seq.* **13** (2010), no. 2, Article 10.2.4, 18 pp.

[10] L. Somer, Divisibility of terms in Lucas sequences by their subscripts, in *Applications of Fibonacci Numbers*, vol. 5, G. E. Bergum et al. (eds), Kluwer Acad. Publ., Dordrecht, 1993, 515-524.

[11] L. Somer and M. Křížek, Iteration of certain arithmetical functions of particular Lucas sequences, *Fibonacci Quart.* **58** (2020), 55-69.

[12] M. Ward, The arithmetical theory of linear recurring series, *Trans. Amer. Math. Soc.* **35** (1933), 600-628.

[13] M. Ward, Prime divisors of second order recurring sequences, *Duke Math. J.* **21** (1954), 607-614.

[14] W. A. Webb and C. T. Long, Distribution modulo p^h of the general linear second order recurrence, *Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur.* **58** (8) (1975), 92-100.

[15] O. Wyler, On second-order recurrences, *Amer. Math. Monthly* **72** (1965), 500-506.

[16] D. Yaqubi and A. Fatehizadeh, Some results on average of Fibonacci and Lucas sequences, preprint `ArXiv: 2001.11839`.