NONDEFECTIVE INTEGERS WITH RESPECT TO CERTAIN LUCAS SEQUENCES OF THE SECOND KIND

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

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

Received: 4/13/17, Revised: 1/3/18, Accepted: 4/4/18, Published: 4/13/18

Abstract

Let $v(a, b)$ denote the Lucas sequence of the second kind defined by the second-order recursion relation $v_{n+2} = av_{n+1} + bv_n$ with initial terms $v_0 = 2$ and $v_1 = a$, where a and b are integers. The positive integer m is said to be nondefective if $v(a, b)$ contains a complete system of residues modulo m. All possibilities for m to be nondefective are found when $b = \pm 1$. This paper generalizes results of Avila and Chen for the Lucas sequence $\{L_n\} = v(1, 1)$.

1. Introduction

Consider the sequence $w = w(a, b)$ satisfying the second-order linear recursion relation

$$w_{n+2} = aw_{n+1} + bw_n \tag{1}$$

with discriminant $D = a^2 + 4b$, where the parameters a and b and the initial terms w_0 and w_1 are all integers and $\gcd(a, b) = 1$. We specify two special recurrences, the Lucas sequence of the first kind (LSFK) $u = u(a, b)$ with initial terms $u_0 = 0$ and $u_1 = 1$, and the Lucas sequence of the second kind (LSSK) $v = v(a, b)$ with initial terms $v_0 = 2$ and $v_1 = a$. Given the recurrence $w(a, b)$ and the positive integer m, we let $z_w(m)$, called the rank of appearance of m in w, or simply the rank of m in w, denote the least positive integer r, if it exists, such that $w_r \equiv 0 \pmod{m}$. Throughout this paper, p will denote a prime and m will denote a positive integer.

The positive integer m is said to be *defective with respect to* $w(a, b)$, or simply *defective* if the recurrence $w(a, b)$ is given, if $w(a, b)$ contains an incomplete system of residues modulo m. Otherwise, m is said to be *nondefective* with respect to $w(a, b)$. Shah [12] proved that the prime p is defective with respect to the Fibonacci sequence $\{F_n\} = u(1,1)$ if $p \equiv \pm 1 \pmod{10}$ or $p \equiv 13$ or $17 \pmod{20}$, while 2, 3, 5, and 7 are nondefective with respect to the Fibonacci sequence. Bruckner [2] proved the remaining cases that p is defective with respect to $\{F_n\}$ if $p > 7$ with $p \equiv 3$ or $7 \pmod{20}$. Somer [13] partially generalized the results of Shah and Bruckner by showing that p is defective with respect to $u(a,1)$ if $p > 7$, $p \nmid D = a^2 + 4$, and $p \not\equiv 1$ or $9 \pmod{20}$. Schinzel [11] completely generalized the results of Shah and Bruckner by proving Theorem 1.1 below.

Theorem 1.1. *Consider the LSFK $u(a,1)$. Then p is defective if $p > 7$ and $p \nmid D = a^2 + 4$.*

Li [8] also proved Theorem 1.1 by extending the methods of Somer [13].

Somer [13] also obtained similar results to those in Theorem 1.1 by considering the LSFK $u(a,-1)$.

Theorem 1.2. *Consider the LSFK $u(a,-1)$. Then p is defective if $p \geq 5$ and $p \nmid D = a^2 - 4$.*

In [4], Burr found all nondefective integers m with respect to the Fibonacci sequence. This result will be given in Theorem 2.1. In [16], we generalized Burr's result by finding all nondefective integers m with respect to the LSFK $u(a,\pm 1)$. These results are given in Theorems 2.3 and 2.4. In [1], Avila and Chen analogously determined all nondefective integers with respect to the Lucas sequence $\{L_n\} = v(1,1)$. This result is presented in Theorem 2.2. In this paper, we will extend Avila and Chen's result by finding all nondefective integers m with respect to the LSSK $v(a,\pm 1)$. These results are given in Theorems 2.5 and 2.7.

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

$$f(x) = x^2 - ax - b \tag{2}$$

with characteristic roots α and β and discriminant $D = a^2 + 4b = (\alpha - \beta)^2 \neq 0$. By the Binet formulas, if $D \neq 0$, then

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \quad v_n = \alpha^n + \beta^n, \tag{3}$$

while if $D = 0$, then

$$u_n = n\alpha^{n-1}, \quad v_n = 2\alpha^n. \tag{4}$$

It was shown in [6, pp. 344–345] that $w(a,b)$ is purely periodic modulo m if $\gcd(b,m) = 1$. We will usually take b to be equal to ± 1, so that $w(a,b)$ will then automatically be purely periodic modulo m. Since $u_0 = 0$, we see that $z_u(m)$ exists for all m such that $\gcd(m,b) = 1$. From here on, we assume that $\gcd(p,b) = \gcd(m,b) = 1$. The *period* of $w(a,b)$ modulo m, denoted by $\lambda_w(m)$, where $\gcd(m,b) = 1$, is the least positive integer c such that $u_{n+c} \equiv u_n \pmod{m}$ for all $n \geq 0$.

Given the recurrence w, we let $A_w(d,m)$ denote the number of times that the residue d appears in a full period of w modulo m. Clearly, m is nondefective with respect to w if $A_w(d,m) \geq 1$ for all residues d modulo m. We define $S_w(m)$ to be the set of all residues $i \in \{0,1,\ldots,m-1\}$ such that $A_w(i,m) \geq 1$.

The following results will be useful for our future work.

Theorem 1.3. *Consider the recurrence $w(a,b)$. Suppose that m is defective. Then every positive multiple of m is also defective.*

This is proved in Theorem 2 of [12] for the Fibonacci sequence. The proof is completely similar for the recurrence $w(a,b)$.

Theorem 1.4. *Consider the recurrence $w(a,b)$. If m is nondefective with respect to $w(a,b)$, then m is nondefective with respect to $u(a,b)$.*

Proof. Suppose that m is nondefective with respect to $w(a,b)$. Since $w(a,b)$ is purely periodic modulo m and $A_w(0,m) \geq 1$, we can assume without loss of generality that $w_0 \equiv 0 \pmod{m}$. If $d = \gcd(w_1,m) > 1$, then by the recursion relation (1) defining $w(a,b)$, $d \mid w_n$ for all $n \geq 0$ and $A_w(1,m) = 0$, contrary to assumption. Thus, $w_1 \equiv c \pmod{m}$, where c is invertible modulo m. Then by the recursion relation defining $u(a,b)$,

$$u_n(a,b) \equiv c^{-1} w_n(a,b) \pmod{m}$$

for all $n \geq 0$, and m is also nondefective with respect to $u(a,b)$. □

The proof of Theorem 1.4 is a direct adaptation of the second part of the proof of Lemma 2 of [1].

Theorem 1.5. *Consider the LSFK $u(a,b)$ and the LSSK $v(a,b)$ and let p be an odd prime such that $p \nmid b$. Then $0 \in S_v(p)$ if and only if $z_u(p)$ is even.*

This follows from results in [5, pp. 42, 47]. See also Theorem 1.10 of [7].

Remark 1.6. As a consequence of Theorem 1.4, the set of nondefective integers m with respect to $v(a,b)$ is a subset of the set of nondefective integers with respect to $u(a,b)$. It further follows from Theorems 1.5 and 1.3 that the integer m is defective with respect to $v(a,b)$ if m has an odd prime divisor p for which $p \nmid b$ and $z_u(p)$ is odd.

Theorem 1.7. *Consider the LSFK $u(a,b)$ with discriminant D. Let $\gcd(a,b) = 1$ and let p be a fixed odd prime such that $p \nmid b$ and let m be a fixed positive integer such that $\gcd(m,b) = 1$. Let $z = z_u(p)$ and $\lambda = \lambda_u(p)$.*

(i) If $r \mid s$, then $u_r \mid u_s$.

(ii) If $d = \gcd(r,s)$, then $\gcd(u_r,u_s) = |u_d|$.

(iii) $z > 1$ and $z \mid p - (D/p)$, where (D/p) denotes the Legendre symbol.

(iv) *If* $p \mid D$, *then* $z = p$.

(v) $u_n \equiv 0 \pmod{m}$ *if and only if* $z_u(m) \mid n$.

(vi) *If* $z_u(p^2) \neq z_u(p)$, *then* $z_u(p^e) = p^{e-1} z_u(p)$ *for* $e \geq 2$.

(vii) *If* $n \geq 1$ *is such that* $\gcd(m, n) = 1$, *then* $z_u(mn) = \operatorname{lcm}(z_u(m), z_u(n))$.

(viii) *If* $(D/p) = 1$, *then* $\lambda \mid p - 1$.

Proof. We note that $z > 1$, since $u_0 = 0$ and $u_1 = 1$. Part (i) follows from the Binet formulas in (3) and (4). Part (ii) is proved in Theorem VI of [5]. Parts (iii) and (viii) are proved in [5, pp. 44–45] and [9, pp. 290, 296, 297]. Part (iv) is proved in [7, p. 424]. Part (v) follows from part (ii). Part (vi) is proved in [5, p. 42]. Part (vii) follows from part (i) and (v). $\square$

Consider the LSFK $u(a, b)$ and let p be a fixed prime. By our earlier assumption, $p \nmid b$ and thus $u(a, b)$ is purely periodic modulo p. Since $u_0 = 0$, $u_1 = 1$, we see that $\lambda_u(p)$ is the least positive integer r such that $u_r \equiv 0$, $u_{r+1} \equiv 1 \pmod{p}$. Hence, $z_u(p) \mid \lambda_u(p)$ by Theorem 1.7 (v). Let $z = z_u(p)$. Since $u_z \equiv 0 \equiv u_{z+1} \cdot u_0$, $u_{z+1} \equiv u_{z+1} \cdot u_1 \pmod{p}$, it follows by induction and the second-order recursion relation defining $u(a, b)$ that

$$u_{z+n} \equiv u_{z+1} \cdot u_n \pmod{p} \tag{5}$$

for all $n \geq 0$. Thus by (5),

$$u_{zi+1} \equiv (u_{z+1})^i u_1 \equiv (u_{z+1})^i \pmod{p}. \tag{6}$$

We note that $\gcd(u_{z+1}, p) = 1$. If $\gcd(u_{z+1}, p) = d$, then $d \mid u_n$ for all $n \geq 0$, since it is assumed that $\gcd(b, p) = 1$. However, $u_1 = 1$, which implies that $d = 1$. Let

$$E_u(p) = \frac{\lambda_u(p)}{z_u(p)}.$$

It follows from the discussion in [6, pp. 354–355] that

$$E_u(p) = \operatorname{ord}_p u_{z+1}, \tag{7}$$

where $\operatorname{ord}_p m$ denoted the multiplicative order of m modulo p.

We have the following proposition.

Proposition 1.8. *Consider the LSFK* $u(a, b)$ *and let* p *be a prime such that* $p \nmid b$. *If* $E_u(p) = p - 1$, *then* p *is nondefective with respect to* $u(a, b)$.

Proof. Let $z = z_u(p)$. Since $E_u(p) = p - 1$, it follows from (7) that u_{z+1} is a primitive root modulo p. Noting that $u_0 = 0$, we see by (6) that

$$\{u_0\} \cup \{u_{zi+1}\}_{i=0}^{p-2}$$

is a complete system of residues modulo p. Thus, p is nondefective with respect to $u(a,b)$. ☐

Lemma 1.9. *Consider the LSFK $u(a,b)$, where $\gcd(a,b) = 1$. Assume that $m_1 \mid m_2$, where $m_2 > m_1$ and $z_u(m_1) = z_u(m_2)$. Then $m_1 \notin S_u(m_2)$ and m_2 is defective. In particular, if a is even and $z_u(m_1)$ is even, then $z_u(m_1) = z_u(2m_1)$ and $2m_1$ is defective.*

This is proved in Corollary 1.6 of [16].

The recurrence $w(a,b)$ is said to be *uniformly distributed* (u.d.) modulo m if $A_w(d_1,m) = A_w(d_2,m)$ for all pairs (d_1,d_2) of residues modulo m such that $0 \le d_1 < d_2 \le m-1$. It is clear that m is nondefective with respect to w if w is u.d. modulo m. Then m is said to be *purely nondefective* with respect to w if w is u.d. modulo m, while the nondefective integer m is said to be *impurely nondefective* with respect to w otherwise. In particular, 1 is always considered to be purely nondefective with respect to w. Theorem 1.10 due to Bumby [3] and Webb and Long [17] completely determines all purely nondefective integers m with respect to the recurrence $w(a,b)$ with discriminant D. In particular, it is shown that if m is purely nondefective with respect to $w(a,b)$, then $p \mid D$ for each prime divisor p of m.

Theorem 1.10. *Consider the recurrence $w(a,b)$ with discriminant D. Then*

(i) *$w(a,b)$ is uniformly distributed modulo m if and only if it is u.d. modulo all prime power factors of m. Moreover, $w(a,b)$ is u.d. modulo m if and only if $w(a,b)$ is u.d. modulo m_1 for each divisor m_1 of m.*

(ii) *Suppose that p is odd. Then $w(a,b)$ is u.d. modulo p if and only if $p \mid D$ and $p \nmid a(2w_1 - aw_0)$.*

(iii) *Suppose that $p = 2$. Then $w(a,b)$ is u.d. modulo 2 if and only if $2 \mid a$ and $2 \nmid w_0 + w_1$.*

(iv) *If $p \ge 5$, then $w(a,b)$ is u.d. modulo p^e for $e \ge 2$ if and only if $w(a,b)$ is u.d. modulo p.*

(v) *If $p = 2$, then $w(a,b)$ is u.d. modulo 2^e for $e \ge 2$ if and only if $a \equiv 2 \pmod 4$ and $b \equiv 3 \pmod 4$.*

(vi) *If $p = 3$, then $w(a,b)$ is u.d. modulo 3^e for $e \ge 2$ if and only if $a \equiv \pm 1 \pmod 3$ and $b \equiv -1 \pmod 3$, but $a^2 \not\equiv -b \pmod 9$.*

(vii) If $b = 1$ and $w(a, b)$ is u.d. modulo p, then $p = 2$ or $p \equiv 1 \pmod 4$.

Proof. Parts (i)–(vi) follow from the results in [3] and [17]. We now prove part (vii). Suppose that $w(a, 1)$ is u.d. modulo p. By parts (ii) and (iii), $D = a^2 + 4 \equiv 0 \pmod p$, which implies that either $p = 2$ or $\left(\frac{-4}{p}\right) = \left(\frac{-1}{p}\right) = 1$ if p is odd. By Euler's criterion, $p \equiv 1 \pmod 4$ if p is odd. $\square$

Corollary 1.11. *Consider the LSFK $u(a, b)$ and the LSSK $v(a, b)$ with discriminant D.*

(i) $u(a, b)$ is u.d. modulo p if and only if $p \mid D$.

(ii) If $m > 1$, then m is not purely nondefective with respect to $v(a, b)$.

Proof. Part (i) follows from Theorem 1.10 (ii) and (iii). Part (ii) follows from Theorem 1.10 (i)–(iii). $\square$

Corollary 1.12. *Suppose that the LSFK $u(a, b)$ is uniformly distributed modulo m. Then $z_u(m) = m$.*

Proof. Suppose that $p^i \parallel m$, where $i \geq 1$. Then by Theorem 1.10(i), $u(a, b)$ is u.d. modulo p^j for $j \in \{1, \ldots, i\}$. We now see by Theorem 1.10 (ii) and (iii) that $p \mid D$. Then by Theorem 1.7 (iv), $z(p) = p$. If $i > 1$, then $z_u(p^2) \neq z_u(p)$ by Lemma 1.9. It now follows from parts (iv) and (vi) of Theorem 1.7 that $z_u(p^i) = p^i$. By Theorem 1.7 (vii), we now find that $z_u(m) = m$. $\square$

In the paper [16], we searched for all positive integers that are nondefective with respect to the LSFK $u(a, \pm 1)$, while in this paper, we look for all integers that are nondefective with respect to the LSSK $v(a, \pm 1)$. We now discuss why we chose to investigate the LSFK $u(a, b)$ and the LSSK $v(a, b)$ in these papers, rather than the more general recurrences $w(a, b)$, and why we limited our cases to the ones in which $b = \pm 1$. First of all, if m is nondefective with respect to the recurrence $w(a, b)$, then $0 \in S_w(p)$ for each prime divisor p of m by Theorem 1.3. For the LSFK $u(a, b)$ and the LSSK $v(a, b)$, it is easy to determine when $0 \in S_u(p)$ or $0 \in S_v(p)$. For the LSFK $u(a, b)$, this is trivial, since $u_0 = 0$. Clearly, $0 \in S_v(2)$, since $v_0 = 2$. Theorem 1.5 gives an easy and efficient criterion to determine when $0 \in S_v(p)$. However, for the general recurrence $w(a, b)$, there is no known efficient criterion to ascertain when $0 \in S_w(p)$ in all cases.

We now address the issue concerning why we only consider the cases in which $b = \pm 1$. By Theorem 1.4, if m is nondefective with respect to $w(a, b)$, then m is nondefective with respect to $u(a, b)$. Thus, one need only consider the LSFK $u(a, b)$ when looking for all possible nondefective integers with respect to the recurrence $w(a, b)$. By Theorem 1.3, if m is nondefective with respect to $u(a, b)$, then each prime divisor p of m is nondefective with respect to $u(a, b)$. When $b = \pm 1$, we saw by Theorems 1.1 and 1.2 that the search for all nondefective integers with respect to $u(a,b)$ was rendered tractable, since only finitely many primes p could be nondefective with respect to $u(a,b)$ when $D \neq 0$, and in particular, these nondefective primes p are small when $p \nmid D$. In particular, by Theorem 1.1., if p is nondefective with respect to $u(a,1)$, then $p \leq 7$ or $p \mid D = a^2+4$, while by Theorem 1.2, if p is nondefective with respect to $u(a,-1)$, then $p \leq 3$ or $p \mid D = a^2-4$.

The situation appears to be quite different when b is a fixed integer such that $b \notin \{-1,0,1\}$. In this case, it is highly plausible that there exist infinitely many primes p for which p is nondefective with respect to $u(a,b)$ for some integer a. This would tend to make the problem of determining all nondefective integers with respect to $u(a,b)$ unmanageable. We need only consider the case in which $(D/p) = -1$. When $(D/p) = 1$, then $\lambda_u(p) \mid p-1$ by Theorem 1.7 (viii), and p must be defective in this case. If $(D/p) = 0$ and $D \neq 0$, then there are only finitely many primes p such that $p \mid D$. We exclude the case in which $D = 0$, because we are considering LSSK's $v(a,b)$ in this paper. If $D = a^2+4b = 0$, then a is even, $\alpha = \beta = a/2$, and it follows from (4), that $v_n(a,b) = 2(a/2)^n$. Then p is defective with respect to $v(a,b)$ for all primes p. This follows since $1 \notin S_v(p)$ if $p \mid a$, while $0 \notin S_v(p)$ if $p \nmid a$.

We now suppose that $(D/p) = -1$. We have the following theorem, which follows from Theorem 7 of [15].

Theorem 1.13. *Let p be a fixed odd prime and let b be a fixed integer such that $p \nmid b$. Let $g = \mathrm{ord}_p(-b)$. Let*

$$e = \gcd((p-1)/g, p+1).$$

Then there exists a LSFK $u(a,b)$ for which $(D/p) = -1$ and

$$E_u(p) = eg.$$

In particular, $eg = p-1$ when $g = (p-1)/2$ or $g = p-1$.

We note by Proposition 1.8 that if $E_u(p) = p-1$, then p is nondefective with respect to $u(a,b)$. We recall that p is a Sophie Germain prime if $q = 2p+1$ is also a prime. It is conjectured that there exist infinitely many Sophie Germain primes (see [10, p. 330]). Let $b \notin \{-1,0,1\}$ be a fixed integer and let p be a Sophie Germain prime such that $q = 2p+1 \geq |b|+2$. Since the only positive divisors of $q-1$ are 1, 2, p, and $2p$, and since $b \notin \{-1,0,1\}$, we see that $\mathrm{ord}_q(-b) = (q-1)/2$ when $(-b/q) = 1$ and $\mathrm{ord}_q(-b) = q-1$ when $(-b/q) = -1$. It then follows from Theorem 1.13 that q is nondefective with respect to $u(a,b)$ for some integer a. Hence, if there exist infinitely many Sophie Germain primes p, then there would exist infinitely many primes $q = 2p+1$ for which there exist an integer a such that q is nondefective with respect to $u(a,b)$.

2. The Main Theorems

Theorem 2.1 due to Burr [4] completely determines all nondefective integers m with respect to the Fibonacci sequence.

Theorem 2.1. *Consider the Fibonacci sequence $\{F_n\}$. Then m is nondefective if and only if m has one of the following forms:*

$$5^k,\ 2\cdot 5^k,\ 4\cdot 5^k,\ 3^j\cdot 5^k,\ 6\cdot 5^k,\ 7\cdot 5^k,\ 14\cdot 5^k, \tag{8}$$

where $k \geq 0$ and $j \geq 1$. Moreover, m is purely nondefective if and only if m is of the form 5^k.

Theorem 2.2 due to Avila and Chen [1] complements Theorem 2.1 by finding all nondefective integers m for the Lucas sequence $\{L_n\} = v(1,1)$.

Theorem 2.2. *Consider the Lucas sequence $\{L_n\}$. Then m is nondefective if and only if m is equal to one of the following numbers:*

$$1,\ 2,\ 4,\ 6,\ 7,\ 14,\ 3^k,$$

where $k \geq 1$.

Theorems 2.3 and 2.4 below generalize Burr's result for the LSFK's $u(a,1)$ and $u(a,-1)$ and can be extracted from results appearing in [16].

Theorem 2.3. *Consider the LSFK $u(a,1)$ with discriminant $D = a^2+4$. Let L be the set of integers $\ell \geq 1$ such that each prime divisor of ℓ also divides a^2+4 and $4 \nmid \ell$. If m is nondefective with respect to $u(a,1)$, then m is in L or m is of the form*

$$2\ell,\ 3^k\ell,\ 4\ell,\ 6\ell,\ 7\ell,\ 14\ell, \tag{9}$$

or possibly, if $5 \nmid D$, of the form $5^k\ell$, with ℓ odd in L, and $k \geq 0$. Moreover the following holds:

(i) ℓ *is nondefective for each integer* $\ell \in L$*. Moreover,* a *is even if* $2 \mid \ell$*.*

(ii) 2ℓ (ℓ *odd*) *is nondefective if and only if* a *is odd.*

(iii) 3ℓ *is nondefective if and only if* ℓ *is odd and* $a \equiv \pm 1 \pmod 3$*.*

(iv) $3^k\ell$ *is nondefective for* $k \geq 2$ *if and only if* ℓ *is odd, and* $a \equiv \pm 1$ *or* $\pm 2 \pmod 9$*.*

(v) 4ℓ *is nondefective if and only if* ℓ *is odd and* $a \equiv \pm 1 \pmod 4$*.*

(vi) If $5 \nmid a^2+4$*, then* 5ℓ *is nondefective if and only if* ℓ *is odd and* $a \equiv \pm 2 \pmod 5$*.*

(vii) *If* $5 \nmid a^2+4$, *then* $5^k\ell$ *is nondefective for* $k \geq 2$ *if and only if* ℓ *is odd,* $a \equiv \pm 2 \pmod 5$, *but* $a \not\equiv \pm 7 \pmod{25}$.

(viii) 6ℓ *is nondefective if and only if* ℓ *is odd and* $a \equiv \pm 1 \pmod 6$.

(ix) 7ℓ *is nondefective if and only if* ℓ *is odd, and* $a \equiv \pm 1$ *or* $\pm 3 \pmod 7$.

(x) 14ℓ *is nondefective if and only if* ℓ *is odd, and* $a \equiv \pm 1$ *or* $\pm 3 \pmod{14}$.

Theorem 2.4. *Consider the LSFK* $u(a,-1)$ *with discriminant* $D = a^2 - 4$. *Let* L' *be the set of odd integers* $\ell' \geq 1$ *such that each prime divisor of* ℓ' *divides* $a^2 - 4$ *and is greater than or equal to* 5. *If* m *is nondefective, then* m *is of the form*

$$2^i 3^j \ell', \tag{10}$$

where $i \geq 0$, $j \geq 0$, *and* $\ell' \in L'$. *Moreover,* m *is nondefective if and only if one of the following cases holds:*

(i) $m = \ell'$, $2\ell'$, *or* $3\ell'$,

(ii) $m = 6\ell'$ *and* $a \equiv 2, 3,$ *or* $4 \pmod 6$.

(iii) $m = 2^i\ell'$, $i \geq 2$, *and* $a \equiv 2 \pmod 4$.

(iv) $m = 3^j\ell'$, $j \geq 2$, *and* $a \equiv \pm 2$ *or* $\pm 4 \pmod 9$,

(v) $m = 3 \cdot 2^i$, $i \geq 2$, *and* $a \equiv \pm 2 \pmod{12}$,

(vi) $m = 2 \cdot 3^j$, $j \geq 2$, *and* $a \equiv \pm 2$ *or* $\pm 4 \pmod{18}$.

(vii) $m = 2^i 3^j$, $i \geq 2$, $j \geq 2$, *and* $a \equiv \pm 2$ *or* $\pm 14 \pmod{36}$.

The principal results in this paper, given in Theorems 2.5 and 2.7, extend Theorem 2.2 to all LSSK's $u(a,\pm 1)$ in an analogous manner to the way in which Theorems 2.3 and 2.4 generalized Theorem 2.1 to all LSFK's $u(a,\pm 1)$.

Theorem 2.5. *Consider the LSSK* $v(a,1)$. *If* m *is nondefective, then* m *is one of the following numbers:*

$$1,\ 2,\ 4,\ 6,\ 7,\ 14,\ 3^k, \tag{11}$$

where $k \geq 1$. *Moreover, the following holds:*

(i) 2 *is nondefective if and only if* 4 *is nondefective if and only if* a *is odd.*

(ii) 3 *is nondefective if and only if* $a \equiv \pm 1 \pmod 3$.

(iii) 3^k *is nondefective for* $k \geq 2$ *if and only if* $a \equiv \pm 1$ *or* $\pm 2 \pmod 9$.

(iv) 6 *is nondefective if and only if* $a \equiv \pm 1 \pmod 6$.

(v) 7 *is nondefective if and only if* $a \equiv \pm 1$ *or* $\pm 3 \pmod 7$.

(vi) 14 *is nondefective if and only if* $a \equiv \pm 1$ *or* $\pm 3 \pmod{14}$.

Moreover no $m > 1$ *is purely nondefective.*

Theorem 2.5 will be proved in Section 4.

Corollary 2.6. *Consider the LSSK* $v(a, 1)$*. Then there exists a nondefective integer* m *satisfying each of the possible cases in Theorem 2.5 if and only if*

$$a \equiv 1, 11, 17, 25, 29, 43, 53, 55, 71, 73, 83, 97, 101, 109, 115 \text{ or } 125 \pmod{126}.$$

Proof. This follows from Theorem 2.5 and the Chinese Remainder Theorem. □

Theorem 2.7. *Consider the LSSK* $v(a, -1)$*. If* m *is nondefective, then* m *is one of the following numbers*

$$1,\ 2,\ 3,\ 6. \tag{12}$$

Moreover, the following holds:

(i) 2 *is nondefective if and only if* a *is odd.*

(ii) 3 *is nondefective if and only if* $a \equiv 0 \pmod 3$.

(ii) 6 *is nondefective if and only if* $a \equiv 3 \pmod 6$.

Moreover, no $m > 1$ *is purely nondefective.*

Theorem 2.7 will be proved in Section 4.

Corollary 2.8. *Consider the LSSK* $v(a, -1)$*. Then there exists a nondefective integer* m *satisfying each of the possible cases in Theorem 2.7 if and only if*

$$a \equiv 3 \pmod 6.$$

Proof. This follows from Theorem 2.7 and the Chinese Remainder Theorem. □

3. Auxiliary Lemmas

The following results will be needed for the proofs of our main theorems, Theorem 2.5 and Theorem 2.7.

Lemma 3.1. *Consider the LSFK* $u(a, b)$ *and the LSSK* $v(a, b)$*. Then* $\gcd(u_n, v_n) \mid 2$ *for all* $n \geq 0$.

This is proved in Theorem II of [5].

Lemma 3.2. *Consider the LSFK $u(a,b)$ and LSSK $v(a,b)$, where a and b are both odd. Then u_n and v_n are both even or both odd according as n is or is not a multiple of* 3.

This is proved in Theorem III of [5].

Lemma 3.3. *Consider the LSSK $v(a,b)$ with discriminant $D = a^2 + 4b$. If $\gcd(m, D) > 1$, then m is defective.*

Proof. Let $u = u(a,b)$. Suppose that $\gcd(m, D) > 1$ and let $p \mid \gcd(m, D)$. If p is odd, then $z_u(p) = p$ by Theorem 1.7 (iv). Hence, $0 \notin S_v(p)$ by Theorem 1.5, and m is defective by Theorem 1.3.

Now suppose that $p = 2$. Then $2 \mid D$, which implies that a is even. Then v_n is even for all $n \geq 0$ and 2 is defective. This again implies that m is defective by Theorem 1.3. □

Lemma 3.4. *Consider the LSFK $u(a,b)$ and the LSSK $v(a,b)$. Suppose that m is nondefective with respect to $u(a,b)$.*

(i) If m is odd, then m is nondefective with respect to $v(a,b)$ if and only if $0 \in S_v(m)$.

(ii) If m is even, then m is nondefective with respect to $v(a,b)$ if and only if both a is odd and $0 \in S_v(m)$.

Proof. We note that if m is nondefective with respect to $v(a,b)$, then $0 \in S_v(m)$.

Suppose that $v_r \equiv 0 \pmod{m}$ for some nonnegative integer r. Let $c = v_{r+1}$. We will show that $\gcd(c, m) = 1$ when either condition (i) or (ii) is satisfied. If $\gcd(c, m) = 1$, then it follows by the recursion relation (1) defining both $u(a,b)$ and $v(a,b)$ and the fact that $u_0 = 0$, $u_1 = 1$, that

$$v_{n+r} \equiv cu_n \pmod{m}$$

for all $n \geq 0$. Since $\gcd(c, m) = 1$, we see that m is nondefective with respect to $v(a,b)$ when m is nondefective with respect to $u(a,b)$.

We now demonstrate that indeed $\gcd(c, m) = 1$. First suppose that m is odd, $v_r \equiv 0 \pmod{m}$, and $\gcd(v_{r+1}, m) = d > 1$. Noting that $\gcd(b, m) = 1$, we observe by induction and the recursion relation defining $v(a,b)$ that $d \mid v_n$ for all $n \geq 0$. In particular, $d \mid v_0 = 2$. This is impossible, since m is odd and $d \mid m$.

Now suppose that m is even, a is odd and $v_r \equiv 0 \pmod{m}$. Let $d = \gcd(v_{r+1}, m)$. Arguing as above, we find that $d \mid v_n$ for all $n \geq 0$. In particular, $d \mid \gcd(v_0, v_1) = \gcd(2, a) = 1$. Hence $d = 1$ and the result follows.

Finally suppose that m and a are even. Then $D = a^2 + 4b$ is even. It now follows from Lemma 3.3 that m is defective. □

The idea of the proof above is a direct adaptation of Lemma 2 of [1].

Lemma 3.5. *Consider the LSFK $u(a,b)$ and the LSSK $v(a,b)$ and let p be a fixed odd prime.*

(i) Let $r = z_u(p^i)$, where $i \geq 1$, and suppose that r is even. Then $p^i \mid v_{r/2}$.

(ii) Suppose that a is odd and let $s = z_u(2p^i)$, where $i \geq 1$. Suppose that s is even. Then $2p^i \mid v_{s/2}$.

Proof. (i) It follows from the Binet formulas (3) that $u_r = u_{r/2}v_{r/2}$. Then $u_{r/2} \not\equiv 0 \pmod{p^i}$ by the definition of $z_u(p^i)$. By Lemma 3.1, $\gcd(u_{r/2}, v_{r/2}) \mid 2$. Thus, $v_{r/2} \equiv 0 \pmod{p^i}$.

(ii) Similarly to the proof of part (i), we have that $u_s = u_{s/2}v_{s/2}$ and $u_{s/2} \not\equiv 0 \pmod{2p^i}$. Since $2 \mid u_s$, we see by Lemma 3.2 that $3 \mid s$. Thus $3 \mid \frac{s}{2}$. Hence, by Lemma 3.2, $2 \mid u_{s/2}$ and $2 \mid v_{s/2}$. Since $\gcd(u_{s/2}, v_{s/2}) \mid 2$, it follows that $2p^i \mid v_{s/2}$. □

Lemma 3.6. *Consider the LSSK $v(a,1)$, where a is odd. Then $v_3 \equiv 0 \pmod 4$.*

Proof. By inspection, we see that $v_3 = a(a^2+3) \equiv a(1+3) \equiv 0 \pmod 4$. □

4. Proofs of the Main Theorems

We prove Theorems 2.5 and 2.7 together.

Proof of Theorems 2.5 and 2.7. Let $b = \pm 1$. It follows from Corollary 1.11 (ii) that if $m > 1$, then m is not purely nondefective with respect to $v(a, \pm 1)$. We note that the rank of 5 in $u(a,1)$ is 3 when $a \equiv \pm 2 \pmod 5$. It now follows from Theorems 2.3 and 2.4, Remark 1.6, Theorem 1.7 (iv), and Lemma 3.3, that if m is nondefective with respect to $v(a,b)$, then m is one of the numbers given in (11) or (12) according as $b = 1$ or $b = -1$.

Part (i) of Theorem 2.5 and part (i) of Theorem 2.7 follow from Lemmas 3.2, 3.3, 3.4, and 3.6 and the fact that $2 \mid D = a^2 + 4b$ if a is even. We note by inspection that for the LSFK $u(a,1)$, the rank of 3 is 4 when $a \equiv \pm 1 \pmod 3$, the rank of 6 is 12 when $a \equiv \pm 1 \pmod 6$, the rank of 7 is 8 when $a \equiv \pm 1$ of $\pm 3 \pmod 7$, and the rank of 14 is 24 when $a \equiv \pm 1$ or $\pm 3 \pmod{14}$. It now follows from Theorem 1.7 (vi) and inspection that for the LSFK $u(a,1)$, the rank of 3^k is $4 \cdot 3^{k-1}$ when $k \geq 2$. Moreover, we find that for the LSFK $u(a,-1)$, the rank of 3 is 2 when $a \equiv 0 \pmod 3$ and the rank of 6 is 6 when $a \equiv \pm 1 \pmod 6$.

The remainder of Theorem 2.5 and Theorem 2.7 now follows from Lemma 3.4 and Lemma 3.5. □

Acknowledgment. We thank the anonymous referee for several valuable suggestions which improved the presentation of the paper. It was supported by RVO 67985840 of the Czech Republic.

References

[1] B. Avila and Y. Chen, On moduli for which the Fibonacci numbers contain a complete residue system, *Fibonacci Quart.* **51** (2013), 151-152.

[2] G. Bruckner, Fibonacci sequence modulo a prime $p \equiv 3 \pmod 4$, *Fibonacci Quart.* **8** (1970), 217-220.

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

[4] S. A. Burr, On moduli for which the Fibonacci sequence contains a complete system of residues, *Fibonacci Quart.* **9** (1971), 497-504.

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

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

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

[8] H.-C. Li, Complete and reduced systems of second-order recurrences modulo p, *Fibonacci Quart.* **38** (2000), 272-281.

[9] E. Lucas, Théorie des fonctions numériques simplement périodiques, *Amer. J. Math.* **1** (1878), 184-240, 289-321.

[10] P. Ribenboim, *The New Book of Prime Number Records,* Springer-Verlag, New York, 1996.

[11] A. Schinzel, Special Lucas sequences including the Fibonacci sequence, modulo a prime, *A Tribute to Paul Erdös,* A. Baker et al. (eds.), Cambridge Univ. Press, Cambridge, 1990, 349-357.

[12] A. P. Shah, Fibonacci sequence modulo m, *Fibonacci Quart.* **6** (1968), 139-141.

[13] L. Somer, Primes having an incomplete system of residues for a class of second-order recurrences. *Applications of Fibonacci Numbers,* Vol. 2, A. F. Horadam et al. (eds.), Kluwer Academic Publ., Dordrecht, 1988, 113-141.

[14] L. Somer, Distribution of residues of certain second-order linear recurrences modulo p – II, *Fibonacci Quart.* **29** (1991), 72-78.

[15] L. Somer, Periodicity properties of kth order linear recurrences with irreducible characteristic polynomial over a finite field, *Finite Fields, Coding Theory, and Advances in Communications and Computing* (Las Vegas, NV, 1991), 195-207, LN in Pure and Appl. Math., 141, Dekker, New York, 1993.

[16] L. Somer and M. Křížek, On moduli for which certain second-order linear recurrences contain a complete system of residues modulo m, *Fibonacci Quart.* **55** (2017), 209-228.

[17] 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.