ITERATION OF CERTAIN ARITHMETICAL FUNCTIONS OF PARTICULAR LUCAS SEQUENCES

LAWRENCE SOMER AND MICHAL KŘÍŽEK

Abstract. Let $u(a,b)$ be a Lucas sequence satisfying the second-order recursion relation $u_{n+2} = au_{n+1} + bu_n$, where $b = \pm 1$, a is an integer, and $u_0 = 0$ and $u_1 = 1$. Let m be a positive integer, and let $\pi(m)$ denote the period of $u(a,b)$ modulo m, and $\rho(m)$ denote the restricted period of $u(a,b)$ modulo m. It is shown that iterates of $\pi(m)$ and $\rho(m)$ end in either a fixed point or a cycle of length two, and all these possible fixed points and two-cycles are explicitly determined.

1. Introduction

In the paper [4], Fulton and Morris studied the iteration of the period of the Fibonacci sequence modulo m, where m is a positive integer. We will extend their results to certain second-order linear recurring sequences. We will also obtain similar results for the iteration of the restricted period modulo m. In [4], the authors showed that the process of iterating the period modulo m of the Fibonacci sequence always ends in a fixed point. For particular second-order recurrences, we will demonstrate that the iteration of the period or restricted period modulo m always terminates in either a fixed point or a cycle of length two.

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

$$w_{n+2} = aw_{n+1} + bw_n, \tag{1.1}$$

where the initial terms w_0 and w_1, and the parameters a and b are all integers. We distinguish two recurrences satisfying (1.1), 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 $v_1 = a$.

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

$$f(x) = x^2 - ax - b \tag{1.2}$$

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

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \quad v_n = \alpha^n + \beta^n, \text{ if } D \neq 0, \tag{1.3}$$

whereas

$$u_n = n\alpha^{n-1}, \quad v_n = 2\alpha^n, \text{ if } D = 0, \tag{1.4}$$

where α is an integer if $D = 0$.

Throughout this article, p will denote a prime and m will denote a positive integer. In this paper, we will extend the results given in [4] from the Fibonacci sequence $u(1,1)$ to the LSFK $u(a,\pm 1)$. It is known (see [3, pp. 344–345]) that if $\gcd(m,b) = 1$, then $w(a,b)$ is purely periodic modulo m.

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. It is easy to see that if $u(a,b)$ is purely periodic modulo p,

then $\gcd(p, b) = 1$. It now follows that $u(a, b)$ is purely periodic modulo m if and only if $\gcd(m, b) = 1$. From here on, we always assume 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 $n \geq 0$. We will usually consider the period $\pi_u(m)$ of the LSFK $u(a, b)$. Because we desire $u(a, b)$ to be purely periodic modulo m for all m, we will frequently only consider LSFK's $u(a, b)$ for which $b = \pm 1$. The (least) restricted period $\rho_w(m)$ of $w(a, b)$ modulo m is the least positive integer s such that

$$w_{n+s} \equiv Mw_n \pmod{m} \tag{1.5}$$

for all $n \geq 0$ and some integer M such that $\gcd(M, m) = 1$. Here, $M = M_w(m)$ is called the *multiplier* of $w(a, b)$ modulo m. Because $u(a, b)$ is purely periodic modulo m and has initial terms $u_0 = 0$, $u_1 = 1$, it is easily seen that $\pi_u(p)$ is the least positive integer r such that

$$u_r \equiv 0,\ u_{r+1} \equiv 1 \pmod{m}, \tag{1.6}$$

whereas $\rho_u(m)$ is the smallest positive integer s such that

$$u_s \equiv 0 \pmod{m}. \tag{1.7}$$

It is proved in [3, pp. 354–355] that $\rho_w(m) \mid \pi_w(m)$. Let

$$E_w(m) = \frac{\pi_w(m)}{\rho_w(m)}. \tag{1.8}$$

Then by [3, pp. 354–355], $E_w(m)$ is the multiplicative order of the multiplier $M_w(m)$ modulo m. By repeated applications of (1.5), we see that if $\rho = \rho_w(m)$, then

$$w_{n+\rho i} \equiv M^i w_n \pmod{m} \tag{1.9}$$

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

It is clear that if $\pi_w^*(m)$ is a general period of $w(a, b)$ modulo m and ρ_w^* is a general restricted period of $w(a, b)$ modulo m, then

$$\pi_w(m) \mid \pi_w^*(m) \quad \text{and} \quad \rho_w(m) \mid \rho_w^*(m). \tag{1.10}$$

We say that $\pi'(m)$ is a *fundamental period* of $w(a, b)$ modulo m if $\pi'(m)$ is the least positive integer that is a general period for all recurrences $w'(a, b)$ modulo m. The *fundamental restricted period* $\rho'(m)$ of $w(a, b)$ modulo m is defined similarly.

The following proposition gives a relation between the period and restricted period of $u(a, b)$ modulo m and the corresponding arithmetical functions of $w(a, b)$ modulo m.

Proposition 1.1. *Consider the recurrence $w(a, b)$ and the LSFK $u(a, b)$ modulo m. Then, $\pi_u(m)$ is the fundamental period of $w(a, b)$ modulo m, and $\rho_u(m)$ is the fundamental restricted period of $w(a, b)$ modulo m.*

Proof. It follows by induction that

$$w_n = bu_{n-1}w_0 + u_n w_1 \tag{1.11}$$

for all $n \geq 0$. The result now follows. □

By virtue of Proposition 1.1, we see that results about iterations of the period and restricted period of the LSFK $u(a,b)$ modulo m also give results about iterations of the fundamental period and fundamental restricted period of the general recurrence $w(a,b)$ modulo m. Accordingly, we will largely consider only the LSFK $u(a,b)$ in this paper. When the LSFK $u(a,b)$ is understood, we will frequently write $\pi(m)$, $\rho(m)$, and $E(m)$, rather than $\pi_u(m)$, $\rho_u(m)$, and $E_u(m)$. Given the LSFK $u(a,b)$, we let $\pi^2(m) = \pi(\pi(m))$ and $\pi^{i+1}(m) = \pi(\pi^i(m))$ for $i = 2, 3 \ldots$. We define $\rho^i(m)$ similarly for $i \geq 2$.

Lemma 1.2 below follows from the Binet formulas (1.3) and (1.4).

Lemma 1.2. *Consider the LSFK $u(a,b)$ and the LSSK $v(a,b)$.*

(i) $u_{2n} = u_n v_n$.
(ii) $u_{2n+1} = bu_n^2 + u_{n+1}^2$.
(iii) $v_{2n} = v_n^2 - 2(-b)^n$.

For future reference, we list the first few terms of $u(a,b)$ and $v(a,b)$:

$$v_0 = 2,\ v_1 = a,\ v_2 = a^2 + 2b,\ v_3 = a(a^2 + 3b),\ v_4 = (a^2 + 2b)^2 - 2b^2. \tag{1.12}$$

$$\begin{gathered} u_0 = 0,\ u_1 = 1,\ u_2 = a,\ u_3 = a^2 + b, \\ u_4 = u_2 v_2 = a(a^2 + 2b),\ u_5 = bu_2^2 + u_3^2 = a^2 b + (a^2 + b)^2, \\ u_6 = u_3 v_3 = a(a^2 + b)(a^2 + 3b),\ u_7 = bu_3^2 + u_4^2 = b(a^2 + b)^2 + a^2(a^2 + 2b)^2. \end{gathered} \tag{1.13}$$

The LSFK $u(a,b)$ with characteristic roots α and β is said to be *degenerate* if $\alpha\beta = 0$ or α/β is a root of unity. It follows from (1.3) that $u_n = 0$ for $n > 0$ only if $u(a,b)$ is degenerate. Theorem 1.3 characterizes the degenerate LSFK's $u(a,b)$ when $b = \pm 1$.

Theorem 1.3. *Consider the LSFK $u(a,b)$, where $b = \pm 1$.*

(i) *$u(a,b)$ is degenerate if and only if $(a,b) = (0,1)$, $(0,-1)$, $(1,-1)$, $(-1,-1)$, $(2,-1)$, or $(-2,-1)$.*
(ii) *If $(a,b) = (0,1)$, then $u_{2n} = 0$, $u_{2n+1} = 1$ for $n \geq 0$.*
(iii) *If $(a,b) = (0,-1)$, then $u_{4n} = u_{4n+2} = 0$, $u_{4n+1} = 1$, $u_{4n+3} = -1$ for $n \geq 0$.*
(iv) *If $(a,b) = (1,-1)$, then $u_{6n} = u_{6n+3} = 0$, $u_{6n+1} = u_{6n+2} = 1$, $u_{6n+4} = u_{6n+5} = -1$ for $n \geq 0$.*
(v) *If $(a,b) = (-1,-1)$, then $u_{3n} = 0$, $u_{3n+1} = 1$, $u_{3n+2} = -1$ for $n \geq 0$.*
(vi) *If $(a,b) = (2,-1)$, then $\alpha = \beta = 1$, $D = 0$, and $u_n = n$ for $n \geq 0$.*
(vii) *If $(a,b) = (-2,-1)$, then $\alpha = \beta = -1$, $D = 0$, and $u_n = (-1)^{n+1} n$ for $n \geq 0$.*

Proof. Part (i) follows from [7, p. 613]. Parts (ii)–(v) follow by induction. Parts (vi) and (vii) follow from (1.4). □

2. The Main Theorems

The following theorems present results about the iterations of the functions $\rho(m)$ and $\pi(m)$ given the LSFK $u(a, \pm 1)$. We say that m is a fixed point of π if $\pi(m) = m$. Thus in this case, $\pi^i(m) = m$ for all $i \geq 1$. Fixed points of ρ are defined similarly. Theorem 2.1 treats the case in which $u(a, \pm 1)$ is degenerate.

Theorem 2.1. *Suppose that $u(a,b)$ is degenerate, where $b = \pm 1$.*

(i) *If $(a,b) = (0,1)$, then the only fixed points of both ρ and π are 1 and 2. Moreover, $\rho(m) = \pi(m) = 2$ for $m \geq 2$.*

(ii) *If* $(a,b)=(0,-1)$*, then the only fixed points of* ρ *are* 1 *and* 2*, whereas the only fixed points of* π *are* 1*,* 2*, and* 4*. Further,* $\rho(m)=2$ *for* $m\geq 2$*, and* $\pi(m)=4$ *for* $m\geq 3$*.*

(iii) *If* $(a,b)=(1,-1)$*, then the only fixed points of* ρ *are* 1 *and* 3*, whereas the only fixed points of* π *are* 1 *and* 6*. Moreover,* $\rho(m)=3$ *for all* $m\geq 3$*. Further,* $\pi(2)=3$ *and* $\pi(m)=6$ *for all* $m\geq 3$*. In particular, if* $m\geq 2$*, then* $\pi^i(m)=6$ *for all* $i\geq 2$*.*

(iv) *If* $(a,b)=(-1,-1)$*, then the only fixed points of both* ρ *and* π *are* 1 *and* 3*. Moreover,* $\rho(m)=\pi(m)=3$ *for all* $m\geq 2$*.*

(v) *If* $(a,b)=(2,-1)$*, then* $\rho(m)=\pi(m)=m$ *for* $m\geq 1$*. In particular, each positive integer* m *is a fixed point of both* ρ *and* π*.*

(vi) *If* $(a,b)=(-2,-1)$*, then* $\rho(m)=m$ *for* $m\geq 1$*. Further,* $\pi(m)=m$ *if* $m=1$ *or* m *is even, and* $\pi(m)=2m$ *if* $m\geq 3$ *is odd. In particular,* m *is a fixed point of* ρ *for* $m\geq 1$*, and* m *is a fixed point of* π *if and only if* $m=1$ *or* m *is even. Furthermore,* $\pi^i(m)=m$ *for all* $i\geq 1$ *if* $m=1$ *or* m *is even, whereas* $\pi^i(m)=2m$ *for all* $i\geq 2$ *if* $m\geq 3$ *is odd.*

Theorem 2.1 follows immediately from Theorem 1.3.

From now on, we will always assume that the LSFK $u(a,b)$ is nondegenerate. Given the LSFK $u(a,b)$ and the positive integer m, we let $\omega=\omega(m)$ denote the least positive integer k such that $\pi^{k+1}(m)=\pi^i(m)$ for some i such that $1\leq i\leq k$. We similarly define $\delta=\delta(m)$ to be the least positive integer ℓ such that $\rho^{\ell+1}(m)=\rho^j(m)$ for some j such that $1\leq j\leq \ell$. In Theorems 2.4 and 2.5, we will see that $\omega(m)$ and $\delta(m)$ exist for all $m\geq 1$ and that

$$\rho^{\delta+1}(m)=\rho^{\delta}(m) \quad \text{or} \quad \rho^{\delta-1}(m), \tag{2.1}$$

whereas

$$\pi^{\omega+1}(m)=\pi^{\omega}(m) \quad \text{or} \quad \pi^{\omega-1}(m). \tag{2.2}$$

Thus, the process of iterating $\rho(m)$ or $\pi(m)$ always ends in either a fixed point or a cycle of length 2.

In Theorems 2.2–2.5, given the LSFK $u(a,\pm 1)$ with discriminant D, we let $R\geq 1$ denote an arbitrary integer for which all of its prime divisors are greater than or equal to 5 and divide D. Moreover, given the LSFK $u(a,-1)$ with discriminant $D=a^2-4=(a-2)(a+2)$, we let $S\geq 1$ and $T\geq 1$, be arbitrary integers such that each prime divisor of both S and T is greater than or equal to 5 and divides D, and additionally, $p\mid S$ implies that $p\mid a-2$, whereas $p\mid T$ implies that $p\mid a+2$. Furthermore, ε will denote an element in $\{0,1\}$. The proofs of Theorems 2.2–2.5 will be given in Section 4.

Theorem 2.2. (Fixed-point theorem for $u(a,1)$**.)** *Let* $u(a,1)$ *be a nondegenerate LSFK. Then the following hold:*

(i) *If* $a\equiv \pm 1 \pmod 6$*, then the only fixed points of* ρ *are* $12^{\varepsilon}R$*,* $R\geq 1$*, whereas the only fixed points of* π *are* 1 *and* $24R$*, where* $R\geq 1$*.*

(ii) *If* $a\equiv 3 \pmod 6$*, then the only fixed points of* ρ *are* $6^{\varepsilon}R$*,* $R\geq 1$*, whereas the only fixed points of* π *are* 6^{ε} *and* $12R$*, where* $R>1$*.*

(iii) *If* $a\equiv 2 \pmod 4$*, then the only fixed points of* ρ *are* 2^iR*, where* $i\geq 0$ *and* $R\geq 1$*, whereas the only fixed points of* π *are* 2^{ε} *and* 2^jR*,* $j\geq 2$*,* $R>1$*.*

(iv) *If* $a\equiv 0 \pmod 4$*, then the only fixed points of* ρ *are* $2^{\varepsilon}R$*, where* $R\geq 1$*, whereas the only fixed points of* π *are* 2^{ε} *and* $4R$*, where* $R\geq 1$*.*

Theorem 2.3. (Fixed-point theorem for $u(a,-1)$**.)** *Let* $u(a,-1)$ *be a nondegenerate LSFK. Then the following hold:*

(i) *If* $a \equiv 5$ *or* $11 \pmod{18}$, *then the only fixed points of* ρ *are* $3^i R$, *where* $i \geq 0$ *and* $R \geq 1$, *whereas the only fixed points of* π *are* $3^i S$, $i \geq 0$, $S \geq 1$, *and* $2 \cdot 3^j ST$, $j \geq 1$, $S \geq 1$, $T > 1$.

(ii) *If* $a \equiv 7$ *or* $13 \pmod{18}$, *then the only fixed points of* ρ *are* $3^i R$, *where* $i \geq 0$ *and* $R \geq 1$, *whereas the only fixed points of* π *are* $S \geq 1$ *and* $2 \cdot 3^j ST$, *where* $j \geq 1$, $S \geq 1$, *and* $T \geq 1$.

(iii) *If* $a \equiv 17 \pmod{18}$, *then the only fixed points of* ρ *are* $3^\varepsilon R$, $R \geq 1$, *whereas the only fixed points of* π *are* $3^\varepsilon S$, $S \geq 1$, *and* $6ST$, $S \geq 1$, $T > 1$, $R \geq 1$.

(iv) *If* $a \equiv 1 \pmod{18}$, *then the only fixed points of* ρ *are* $3^\varepsilon R$, $R \geq 1$, *whereas the only fixed points of* π *are* $S \geq 1$ *and* $6ST$, *where* $S \geq 1$ *and* $T \geq 1$.

(v) *If* $a \equiv 2$ *or* $14 \pmod{36}$, *then the only fixed points of* ρ *are* $2^i 3^j R$, *where* $i \geq 0$, $j \geq 0$, $R \geq 1$, *whereas the only fixed points of* π *are* $3^j S$, $j \geq 0$, $S \geq 1$, *and* $2^i 3^j ST$, *where* $i \geq 1$, $j \geq 0$, $S \geq 1$, *and* $T \geq 1$.

(vi) *If* $a \equiv 22$ *or* $34 \pmod{36}$, *then the only fixed points of* ρ *are* $2^i 3^j R$, *where* $i \geq 0$, $j \geq 0$, $R \geq 1$, *whereas the only fixed points of* π *are* $S \geq 1$ *and* $2^i 3^j ST$, *where* $i \geq 1$, $j \geq 0$, $S \geq 1$, *and* $T \geq 1$.

(vii) *If* $a \equiv 26 \pmod{36}$, *then the only fixed points of* ρ *are* $2^i 3^\varepsilon R$, *where* $i \geq 0$ *and* $R \geq 1$, *whereas the only fixed points of* π *are* $3^\varepsilon S$, $S \geq 1$, *and* $2^i 3^\varepsilon ST$, *where* $i \geq 1$, $S \geq 1$, *and* $T \geq 1$.

(viii) *If* $a \equiv 10 \pmod{36}$, *then the only fixed points of* ρ *are* $2^i 3^\varepsilon R$, *where* $i \geq 0$ *and* $R \geq 1$, *whereas the only fixed points of* π *are* $S \geq 1$ *and* $2^i 3^\varepsilon ST$, *where* $i \geq 1$, $S \geq 1$, *and* $T \geq 1$.

(ix) *If* $a \equiv 20$ *or* $32 \pmod{36}$, *then the only fixed points of* ρ *are* $2^\varepsilon 3^j R$, *where* $j \geq 0$ *and* $R \geq 1$, *whereas the only fixed points of* π *are* $3^j S$, *where* $j \geq 1$ *and* $S \geq 1$, *and* $2^i 3^j ST$, *where* $i \in \{1, 2\}$, $j \geq 0$, $S \geq 1$, *and* $T \geq 1$.

(x) *If* $a \equiv 4$ *or* $16 \pmod{36}$, *then the only fixed points of* ρ *are* $2^\varepsilon 3^j R$, *where* $j \geq 0$ *and* $R \geq 1$, *whereas the only fixed points of* π *are* $S \geq 1$ *and* $2^i 3^j ST$, *where* $i \in \{1, 2\}$, $j \geq 0$, $S \geq 1$, *and* $T \geq 1$.

(xi) *If* $a \equiv 8 \pmod{36}$, *then the only fixed points of* ρ *are* $2^{\varepsilon_1} 3^{\varepsilon_2} R$, *where* $\varepsilon_1, \varepsilon_2 \in \{0, 1\}$ *and* $R \geq 1$, *whereas the only fixed points of* π *are* $3^\varepsilon S$, $S \geq 1$, *and* $2^i 3^\varepsilon ST$, *where* $i \in \{1, 2\}$, $S \geq 1$, *and* $T \geq 1$.

(xii) *If* $a \equiv 28 \pmod{36}$, *then the only fixed points of* ρ *are* $2^{\varepsilon_1} 3^{\varepsilon_2} R$, *where* $\varepsilon_1, \varepsilon_2 \in \{0, 1\}$, *whereas the only fixed points of* π *are* $S \geq 1$ *and* $2^i 3^\varepsilon ST$, *where* $i \in \{1, 2\}$, $S \geq 1$, *and* $T \geq 1$.

(xiii) *If* $a \equiv 3 \pmod{6}$, *then the only fixed points of* ρ *are* $6^\varepsilon R$, $R \geq 1$, *whereas the only fixed points of* π *are* $S \geq 1$ *and* $12ST$, *where* $S \geq 1$ *and* $T \geq 1$.

(xiv) *If* $a \equiv 6 \pmod{12}$, *then the only fixed points of* ρ *are* $2^i R$, *where* $i \geq 0$ *and* $R \geq 1$, *whereas the only fixed points of* π *are* $S \geq 1$ *and* $2^i ST$, *where* $i \geq 1$, $S \geq 1$, *and* $T \geq 1$.

(xv) *If* $a \equiv 0 \pmod{12}$, *then the only fixed points of* ρ *are* $2^\varepsilon R$, *where* $R \geq 1$, *whereas the only fixed points of* π *are* $S \geq 1$ *and* $2^i ST$, *where* $i \in \{1, 2\}$, $S \geq 1$, *and* $T \geq 1$.

Theorem 2.4. (Iteration theorem for $u(a, 1)$**.)** *Let* $u(a, 1)$ *be a nondegenerate LSFK and let* m *be a positive integer.*

(i) *If* $a \not\equiv 3 \pmod{6}$, *then* $\rho^\delta(m) = G_1$ *and* $\pi^\omega(m) = G_2$, *where* G_1 *is one of the fixed points of* ρ *and* G_2 *is one of the fixed points of* π *as given in Theorem 2.2.*

(ii) *If* $a \equiv 3 \pmod{6}$, *then* $\rho^{\delta+1}(m) = \rho^{\delta-1}(m) = 2R$ *and* $\rho^{\delta+2}(m) = \rho^\delta(m) = 3R$, $R \geq 1$; *or* $\rho^{\delta+1}(m) = \rho^{\delta-1}(m) = 3R$ *and* $\rho^{\delta+2}(m) = \rho^\delta(m) = 2R$, $R \geq 1$; *or* $\rho^{\delta+1}(m) = \rho^\delta(m) = 6^\varepsilon R$, $R \geq 1$. *Moreover,* $\pi^{\omega+1}(m) = \pi^{\omega-1}(m) = 2$ *and* $\pi^{\omega+2}(m) = \pi^\omega(m) = 3$;

or $\pi^{\omega+1}(m) = \pi^{\omega-1}(m) = 3$ *and* $\pi^{\omega+2}(m) = \pi^{\omega}(m) = 2$*; or* $\pi^{\omega+1}(m) = \pi^{\omega}(m) = 6^{\varepsilon}$*; or* $\pi^{\omega+1}(m) = \pi^{\omega}(m) = 12R$*,* $R > 1$*.*

Theorem 2.5. (Iteration theorem for $u(a,-1)$.) *Let $u(a,-1)$ be a nondegenerate LSFK and let m be a positive integer.*

(i) *If* $a \not\equiv 3 \pmod 6$*, then* $\rho^{\delta}(m) = G_3$ *and* $\pi^{\omega}(m) = G_4$*, where* G_3 *is one of the fixed points of* ρ *and* G_4 *is one of the fixed points of* π *as given in Theorem 2.3.*

(ii) *If* $a \equiv 3 \pmod{12}$*, then* $\rho^{\delta+1}(m) = \rho^{\delta-1}(m) = 2R$ *and* $\rho^{\delta+2}(m) = \rho^{\delta}(m) = 3R$*,* $R \geq 1$*; or* $\rho^{\delta+1}(m) = \rho^{\delta-1}(m) = 3R$ *and* $\rho^{\delta+2}(m) = \rho^{\delta}(m) = 2R$*,* $R \geq 1$*; or* $\rho^{\delta+1}(m) = \rho^{\delta}(m) = 6^{\varepsilon}R$*,* $R \geq 1$*. Further,* $\pi^{\omega+1}(m) = \pi^{\omega-1}(m) = 3S$ *and* $\pi^{\omega+2}(m) = \pi^{\omega}(m) = 4S$*,* $S \geq 1$*; or* $\pi^{\omega+1}(m) = \pi^{\omega-1}(m) = 4S$ *and* $\pi^{\omega+2}(m) = \pi^{\omega}(m) = 3S$*,* $S \geq 1$*; or* $\pi^{\omega+1}(m) = \pi^{\omega}(m) = S$*,* $S \geq 1$*; or* $\pi^{\omega+1}(m) = \pi^{\omega}(m) = 12ST$*,* $S \geq 1$*,* $T \geq 1$*.*

(iii) *If* $a \equiv 9 \pmod{12}$*, then* $\rho^{\delta+1}(m) = \rho^{\delta-1}(m) = 2R$ *and* $\rho^{\delta+2}(m) = \rho^{\delta}(m) = 3R$*,* $R \geq 1$*; or* $\rho^{\delta+1}(m) = \rho^{\delta-1}(m) = 3R$ *and* $\rho^{\delta+2}(m) = \rho^{\delta}(m) = 2R$*,* $R \geq 1$*; or* $\rho^{\delta+1}(m) = \rho^{\delta}(m) = 6^{\varepsilon}R$*,* $R \geq 1$*. Moreover,* $\pi^{\omega+1}(m) = \pi^{\omega}(m) = S$*,* $S \geq 1$*; or* $\pi^{\omega+1}(m) = \pi^{\omega}(m) = 12ST$*,* $S \geq 1$*,* $T \geq 1$*.*

3. Auxiliary Results

In this section, we provide results that will be needed for the proofs of Theorems 2.2–2.5.

Theorem 3.1. *Consider the nondegenerate LSFK $u(a,b)$. Then the following hold:*

(i) *If* $p \nmid 2b$*, then* $\rho(p) \mid p - (D/p)$*, where* (D/p) *is the Legendre symbol and* $(D/p) = 0$ *if* $p \mid D$*.*

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

(iii) *If* $p \nmid b$ *and* $(D/p) = 1$*, then* $\pi(p) \mid p - 1$*.*

(iv) *Suppose that* $p > 2$ *and* $p \nmid bD$*. If* q *is a prime and* $q \mid \rho(p)\pi(p)$*, then* $q < p$*.*

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

$$\rho(p^i) = p^{\max(i-c,0)}\rho(p) \tag{3.1}$$

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

$$\rho(2^i) = 2^{\max(i+1-d,1)}\rho(2) \tag{3.2}$$

for $i \geq 2$*.*

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

$$\pi(p^i) = p^{\max(i-e,0)}\pi(p) \tag{3.3}$$

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

$$\pi(2^i) = 2^{\max(i+1-g,1)}\pi(2) \tag{3.4}$$

for $i \geq 2$*.*

(vii) *If* $\gcd(mn, b) = 1$*, then*

$$\rho([m,n]) = [\rho(m), \rho(n)] \tag{3.5}$$

and

$$\pi([m,n]) = [\pi(m), \pi(n)], \tag{3.6}$$

where $[m,n]$ *denotes the least common multiple of the positive integers* m *and* n*.*

(viii) *If* $\gcd(mn, b) = 1$, *then*

$$\rho^i([m,n]) = [\rho^i(m), \rho^i(n)] \tag{3.7}$$

and

$$\pi^i([m,n]) = [\pi^i(m), \pi^i(n)] \tag{3.8}$$

for $i \geq 1$.

(ix) $\rho(1) = \pi(1) = 1$.

Proof. Parts (i) and (ii) are proved in [5, pp. 423 and 441]. Part (iii) is proved in [2, pp. 44–45].

(iv) By part (i), $\rho(p) \mid p \pm 1$. By (1.8) and the following discussion $\pi(p) = E(p)\rho(p)$ and $E(p) = \operatorname{ord}_p(M(p))$, where $\operatorname{ord}_p(n)$ denotes the multiplicative order of n modulo p. Hence, $E(p) \mid p - 1$. Thus, $\pi(p) \mid (p-1)(p \pm 1)$. The assertion follows.

(v) and (vi) Because $u(a,b)$ is nondegenerate, $u_n \neq 0$ for $n > 0$. It now follows from (1.6) and (1.7) that c, d, e, and g all exist. The rest of part (v) follows from Theorem X of [2], whereas the remainder of part (vi) follows from [6, pp. 619–620 and 627–628].

(vii) and (viii) We first note that if $\gcd(mn, b) = 1$, then $u(a,b)$ is purely periodic modulo mn. Parts (vii) and (viii) now follow from (1.9).

(ix) It is evident that $\rho(1) = \pi(1) = 1$. □

Theorem 3.2. *Let* $u(a,b)$ *be nondegenerate LSFK and let* $m \geq 2$ *be an integer such that* $\gcd(m,b) = 1$. *Let* $h = \operatorname{ord}_m(-b) = 2^c h'$ *and* $\rho = \rho(m) = 2^d \rho'$, *where* h' *and* ρ' *are odd integers. Let* $\pi = \pi(m)$ *and* $H = [h, \rho]$.

(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 [9].

We have the following immediate corollaries of Theorem 3.2 corresponding to the cases in which $b = \pm 1$.

Corollary 3.3. *Consider the nondegenerate LSFK* $u(a,1)$ *and let* $m \geq 2$. *Let* $E = E(m) = \pi(m)/\rho(m) = \pi/\rho$. *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* $E = 4$.

Corollary 3.4. *Consider the nondegenerate LSFK* $u(a,-1)$ *and let* $m \geq 2$. *Let* $E = E(m) = \pi(m)/\rho(m) = \pi/\rho$. *Then the following hold:*

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

(ii) *Suppose that* $m = p^i$, *where* p *is an odd prime.*
  (a) *If* $\rho \equiv 0 \pmod 2$, *then* $E = 2$.
  (b) *If* $\rho \equiv 1 \pmod 2$, *then* $E = 1$ *or* 2.

Remark 3.5. We show that both possibilities for E can occur in part (ii)(b) of Corollary 3.4. Consider the LSFK $u(3,-1)$. Then $\rho(13) = \rho(29) = 7$, whereas $\pi(13) = 14$ and $\pi(29) = 7$. Hence, $E(29) = 1$, whereas $E(13) = 2$.

Lemma 3.6. *Let $u(a,b)$ be a nondegenerate LSFK, where $b = \pm 1$ and let p be an odd prime. Let e be the largest integer such that $\rho(p^e) = \rho(p)$ and let g be the largest integer such that $\pi(p^g) = \pi(p)$. Then,*

$$e = g. \tag{3.9}$$

Proof. We note that $\rho(p^i)$ is the least positive integer r such that $u_r \equiv 0 \pmod{p^i}$, $u_{r+1} \not\equiv 0 \pmod{p^i}$, whereas $\pi(p^i)$ is the least positive integer s such that $u_s \equiv 0 \pmod{p)^i}$, $u_{s+1} \equiv 1 \pmod{p^i}$. It is now evident that $e \geq g$.

We observe by Theorem 3.1(vi) that if $\pi(p^e) \neq \pi(p)$, then

$$p \mid \frac{\pi(p^e)}{\pi(p)}. \tag{3.10}$$

However, by Corollaries 3.3 and 3.4,

$$\pi(p^e) = E(p^e)\rho(p^e) = E(p^e)\rho(p)$$

and

$$\pi(p) = E(p)\rho(p),$$

where $E(p^e) \mid 4$ and $E(p) \mid 4$. Thus,

$$\frac{\pi(p^e)}{\pi(p)} = \frac{E(p^e)}{E(p)},$$

and $p \nmid \pi(p^e)/\pi(p)$, which is a contradiction to (3.10). Hence, (3.9) holds. □

Theorem 3.7. *Let $u(a,b)$ be a nondegenerate LSFK with discriminant D. Suppose that $p \mid D$ and $p \nmid \gcd(a,b)$. We let $\nu_p(m)$ denote the largest nonnegative integer r such that $p^r \mid m$. The following hold:*

(i) *$\rho(p) = p$.*
(ii) *If $p \geq 5$, then $\rho(p^i) = p^i$ for $i \geq 1$.*
(iii) *Suppose that $p = 2$. Then $a \equiv 0 \pmod 2$. Moreover, if $a \equiv 2 \pmod 4$, then $\rho(2^i) = 2^i$ for $i \geq 1$.*
(iv) *Suppose that $p = 3$. Then, $a^2 \equiv -b \pmod 3$. Further, if $a^2 \not\equiv -b \pmod 9$, then $\rho(3^i) = 3^i$ for $i \geq 1$.*
(v) *Suppose that $p = 2$ and $\nu_2(a) = c \geq 2$. Then $\rho(2^i) = 2 \cdot 2^{\max(i-c,0)}$ for $i \geq 1$.*
(vi) *Suppose that $p = 3$ and $\nu_3(a^2 + b) = d \geq 2$. Then, $\rho(3^i) = 3 \cdot 3^{\max(i-d,0)}$.*

Proof. Parts (i), (ii), and (iv) follow from results in [1] or [8] and that $u_2 = a$ and $u_3 = a^2 + b$.

(iii) By (1.13), we note that $u_2 = a \equiv 2 \pmod 4$ and $u_4 = a(a^2 + 2b) \equiv 4 \pmod 8$. Part (iii) now follows from Theorem 3.1(v).

(v) Since $u_2 = a$, we see that $\rho(2^i) = 2$ for $1 \leq i \leq c$ and $\rho(2^{c+1}) \neq \rho(4)$. The assertion now follows from Theorem 3.1(v).

(vi) Since $u_3 = a^2 + b$, we find that $\rho(3^i) = 3$ for $1 \leq i \leq d$ and $\rho(3^{d+1}) \neq \rho(3)$. Part (vi) now follows from Theorem 3.1(v). □

Theorem 3.8. *Let $u(a,b)$ be a nondegenerate LSFK with discriminant D, where $b = \pm 1$. Suppose that $p \mid D$. If $p > 2$, let e be the largest integer such that $\rho(p^e) = \rho(p)$. 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 $p > 2$ and $a \equiv 2 \pmod p$, then*

$$\pi(p^i) = \rho(p^i) = p \cdot p^{\max(i-e,0)} \tag{3.11}$$

for $i \geq 1$. If $p > 2$ and $a \equiv -2 \pmod{p}$, then

$$\pi(p^i) = 2\rho(p^i) = 2p \cdot p^{\max(i-e,0)} \tag{3.12}$$

for $i \geq 1$.

(iii) *If $p = 2$, $b = \pm 1$, and $a \equiv 2 \pmod 4$, then $\pi(2^i) = \rho(2^i) = 2^i$ for $i \geq 1$.*

(iv) *If $b = 1$ and $p \geq 5$, then $\pi(p^i) = 4\rho(p^i) = 4p^i$ for $i \geq 1$.*

(v) *Suppose that $b = -1$. If $p \geq 5$ and $a \equiv 2 \mod p$, then $\pi(p^i) = \rho(p^i) = p^i$ for $i \geq 1$. If $p \geq 5$ and $a \equiv -2 \pmod p$, then $\rho(p^i) = p^i$ and $\pi(p^i) = 2p^i$ for $i \geq 1$.*

(vi) *If $b = 1$, $p = 2$, and $\nu_2(a) = c \geq 2$, then $\pi(2^i) = \rho(2^i) = 2 \cdot 2^{\max(i-c,0)}$ for $i \geq 1$.*

(vii) *If $b = -1$, $p = 2$, and $\nu_2(a) = c \geq 2$, then $\pi(2) = 2$ and $\pi(2^i) = 4 \cdot 2^{\max(i-1-c,0)}$ for $i \geq 2$.*

(viii) *Suppose that $b = -1$, $p = 3$, and $a \equiv \pm 2$ or $\pm 4 \pmod 9$. If $a \equiv 2$ or $5 \pmod 9$, then $\pi(3^i) = \rho(3^i) = 3^i$ for $i \geq 1$. If $a \equiv 4$ or $7 \pmod 9$, then $\pi(3^i) = 2\rho(3^i) = 2 \cdot 3^i$ for $i \geq 1$.*

(ix) *Suppose that $b = -1$, $p = 3$, and $a \equiv \pm 1 \pmod 9$. Then $|a| > 2$. Let $d = \nu_3(a^2 - 1)$. Then $d \geq 2$. If $a \equiv 8 \pmod 9$, then $\pi(3^i) = \rho(3^i) = 3 \cdot 3^{\max(i-d,0)}$ for $i \geq 1$. If $a \equiv 1 \pmod 9$, then $\pi(3^i) = 2\rho(3^i) = 6 \cdot 3^{\max(i-d,0)}$ for $i \geq 1$.*

Proof. (i) Since $D = a^2 + 4 \equiv \pmod p$, we see that $(-4/p) = 0$ or 1. Thus, $p = 2$ 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, $a \equiv \pm 2 \pmod p$. Moreover, by Theorem 3.7(i),

$$\rho(p) = p. \tag{3.13}$$

First suppose that $a \equiv 2 \pmod p$. Then by (1.2),

$$f(x) \equiv x^2 - 2x + 1 \equiv (x-1)^2 \pmod p. \tag{3.14}$$

Thus, by the Binet formula for $u(a,b)$ given in (1.4),

$$u_n \equiv n \cdot 1^{n-1} \equiv n \pmod p \tag{3.15}$$

for $n \geq 0$. Hence, by (3.13) and (3.15),

$$u_{\rho(p)+1} = u_{p+1} \equiv 1 \pmod p. \tag{3.16}$$

Thus, $\pi(p) = \rho(p) = p$. It now follows from Theorem 3.1(v) and (vi) and from equation (3.9) in Lemma 3.6 that (3.11) holds.

Now suppose that $a \equiv -2 \pmod p$. Then by (1.2),

$$f(x) \equiv x^2 + 2x + 1 \equiv (x+1)^2 \pmod p. \tag{3.17}$$

Therefore, by (1.4),

$$u_n \equiv n(-1)^{n-1} \pmod p \tag{3.18}$$

for $n \geq 0$. Consequently, by (3.13) and (3.18),

$$u_{\rho(p)+1} = u_{p+1} \equiv -1 \pmod p. \tag{3.19}$$

Hence, $\pi(p) = 2\rho(p) = 2p$. We now see, by Theorem 3.1(v) and (vi) and by (3.9), that (3.12) holds.

(iii) By Theorem 3.7(iii), $\rho(2^i) = 2^i$ for $i \geq 1$. Thus, $u_2 \equiv 2 \pmod 4$ and $u_4 \equiv 4 \pmod 8$. Moreover, by (1.13), $u_3 = a^2 + b \equiv 1 \pmod 2$ and $u_5 = u_3^2 + bu_2^2 \equiv 1 + 4b \equiv 5 \mod 8$. Hence, $\pi(2) = 2$, $\pi(4) = 4$, and $\pi(8) \neq \pi(4)$. The result now follows by Theorem 3.1(vi).

(iv) By Theorem 3.7(ii), $\rho(p^i) = p^i$ for $i \geq 1$. The result now follows from Corollary 3.3(ii)(c).

(v) This follows from Theorem 3.7(ii) and part (ii) of this theorem.

(vi) We note that $u_2 = a \equiv 2^c \pmod{2^{c+1}}$, where $c \geq 2$. Moreover, $u_3 = a^2 + 1 \equiv 1 \pmod{2^c}$. Thus, $\rho(2^c) = \rho(4) = \pi(2^c) = \pi(4) = 2$, $\rho(2^{c+1}) \neq \rho(2^c)$, and $\pi(2^{c+1}) \neq \pi(2^c)$. The result now follows from Theorem 3.1(v) and (vi).

(vii) By Theorem 3.7(v), $\rho(2^i) = 2 \cdot 2^{\max(i-c,0)}$ for $i \geq 1$. Thus, $u_2 \equiv 2^c \pmod{2)^{c+1}}$ and $u_4 \equiv 2^{c+1} \pmod{2^{c+2}}$. Moreover, by (1.13), $u_3 = a^2 - 1 \equiv -1 \pmod{2^{2c}}$ and

$$u_5 = u_3^2 - u_2^2 = (a^2-1)^2 - a^2 \equiv 1 \pmod{2^{2c}}.$$

Hence, $\pi(2) = 2$, $\pi(4) = \pi(2^{c+1}) = 4$ and $\pi(2^{c+2}) \neq \pi(2^{c+1})$. The assertion now follows from Theorem 3.1 (vi).

(viii) This follows from Theorem 3.7(iv) and part (ii) of this theorem.

(ix) We note by Theorem 1.3 that $|a| > 2$, since $u(a,-1)$ is nondegenerate. Part (ix) now follows from Theorem 3.7(vi) and part (ii) of this theorem. □

Lemmas 3.9 and 3.10 determine $\rho(p^i)$ and $\pi(p^i)$ for LSFK $u(a,\pm 1)$ when $p = 2$ or 3 and $p \nmid D$.

Lemma 3.9. *Consider the nondegenerate LSFK $u(a,1)$.*

(i) *Suppose that $a \equiv 1 \pmod 2$. Then $\rho(2) = 3$ and $\rho(2^i) = 6 \cdot 2^{\max(i-3,0)}$ for $i \geq 1$.*

(ii) *Suppose that $a \equiv \pm 1 \pmod 3$. Let $c = \nu_3(a^2+2)$. Then $c \geq 1$ and $\rho(3^i) = 4 \cdot 3^{\max(i-c,0)}$ for $i \geq 1$. Furthermore, $\pi(3^i) = 2\rho(3^i) = 8 \cdot 3^{\max(i-c,0)}$ for $i \geq 1$.*

(iii) *Suppose that $v_3(a) = d \geq 1$. Then $\rho(3^i) = \pi(3^i) = 2 \cdot 3^{\max(i-d,0)}$ for $i \geq 1$.*

Proof. (i) By (1.13), $u_1 \equiv u_2 \equiv 1 \pmod 2$, $u_3 = a^2 + 1 \equiv 2 \pmod 8$, and $u_4 = a(a^2+2) \equiv 1 \pmod 2$. Moreover,

$$u_6 = u_3 v_3 = a(a^2+1)(a^2+3) \equiv 8 \pmod{16}$$

and

$$u_7 = u_3^2 + u_4^2 = (a^2+1)^2 + (a(a^2+2))^2 \equiv 2^2 + 1 \equiv 5 \pmod 8.$$

Hence, $\rho(2) = \pi(2) = 3$, $\rho(4) = \rho(8) = 6$, and $\rho(16) \neq \rho(4)$. In addition, $\pi(4) = 6$, whereas $\pi(8) \neq \pi(4)$. Part (i) now follows from Theorem 3.1(v) and (vi).

(ii) By (1.13), $u_n \equiv 0 \pmod 3$ for $1 \leq i \leq 3$, whereas $\nu_3(u_4) = \nu_3(a(a^2+2)) = c \geq 1$. Therefore, $\rho(3^i) = 4$ for $1 \leq i \leq c$ and $\rho(3^{c+1}) \neq \rho(3)$. The assertion now follows from Theorem 3.1(v) and Corollary 3.3(ii)(b).

(iii) By (1.13), $u_1 = 1$ and $\nu_3(u_2) = \nu_3(a) = d \geq 1$. Thus, $\rho(3^i) = 2$ for $1 \leq i \leq d$ and $\rho(3^{d+1}) \neq \rho(3)$. Part (iii) now follows from Theorem 3.1(v) and Corollary 3.3(ii)(a). □

Lemma 3.10. *Consider the nondegenerate LSFK $u(a,-1)$.*

(i) *Suppose that $a \equiv 1 \pmod 2$. Let $c = \nu_2(a^2-1)$ and $d = \nu_2(a+1)$. Then c exists, $c \geq 3$, and $\rho(2^i) = 3 \cdot 2^{\max(i-c,0)}$. Moreover, d exists and $d \geq 1$. If $d = 1$, then $\pi(2) = 3$ and $\pi(2^i) = 6 \cdot 2^{\max(i-c,0)}$ for $i \geq 2$. If $d \geq 2$, then $\pi(2^i) = 3 \cdot 2^{\max(i+1-c,0)}$ for $i \geq 1$.*

(ii) *Suppose that $\nu_3(a) = e \geq 1$. Then $\rho(3^i) = 2 \cdot 3^{\max(i-e,0)}$ and $\pi(3^i) = 4 \cdot 3^{\max(i-e,0)}$ for $i \geq 1$.*

Proof. (i) We let $s \in \{0,1\}$. Since $u(a,-1)$ is nondegenerate, we have that $|a| > 2$, which implies that $c = \nu_2(a^2-1)$ exists. Noting that $a \equiv 1 \pmod 2$, we see by (1.13) that $u_1 \equiv u_2 \equiv 1 \pmod 2$ and $\nu_2(u_3) = \nu_2(a^2-1) = c \geq 3$. Hence, $\rho(2^i) = 3$ for $1 \leq i \leq c$ and $\rho(2^{c+1}) \neq \rho(4) = 3$. Therefore, $\rho(2^i) = 3 \cdot 2^{\max(i-c,0)}$ for $i \geq 1$ by Theorem 3.1(v). Moreover $\nu_2(a+1) = d \geq 1$.

Furthermore, if $d \geq 2$, then $d = c - 1$, since $a^2 - 1 = (a+1)(a-1)$. We note that

$$u_4 = -u_2 + au_3 \equiv -a + a \cdot 0 \equiv -a \pmod{2^c}.$$

Thus, $\pi(2^i) = 3$ for $1 \leq i \leq d$. Further, by (1.13),

$$u_7 = u_4^2 - u_3^2 \equiv (-a + s2^c)^2 - (2^c)^2 \equiv a^2 \equiv 1 + 2^c \mod 2^{c+1}. \tag{3.20}$$

Hence, by Theorem 3.1(vi), $\pi(2^i) = 6$ for $d+1 \leq i \leq c$, and $\pi(2^{c+1}) \neq 6$. Part (i) now follows from Theorem 3.1(vi).

(ii) Since $u_2 = a$, we see that $\nu_3(u_2) = e \geq 1$. Thus by Theorem 3.1(v) and Corollary 3.4(ii)(a), $\rho(3^i) = 2 \cdot 3^{\max(i-e,0)}$ and $\pi(3^i) = 4 \cdot 3^{\max(i-e,0)}$ for $i \geq 1$. □

Lemma 3.11. *Let $u(a,b)$ be a nondegenerate LSFK, where $b = \pm 1$. Let R, S, and T be as defined in Section 2 just after formula (2.2).*

(i) $\rho(R) = R$.
(ii) *If $b = 1$ and $R > 1$, then $\pi(R) = 4R$.*
(iii) *Suppose that $b = -1$. Then $\pi(S) = S$. Moreover, if $T > 1$, then $\pi(T) = 2T$.*

Proof. (i) We observe that $\rho(R) = R$, if $R = 1$. Suppose that $R > 1$ and $p \mid R$. Then $p \geq 5$ and $p \mid D$. It follows from Theorem 3.7(ii) that $\rho(p^i) = p^i$ for $i \geq 1$. The assertion now follows from (3.5) in Theorem 3.1.

(ii) Suppose that $p \mid R$. Then $\pi(p^i) = 4p^i$ by Theorem 3.8(iv). The result now follows from (3.6).

(iii) Suppose that $p \mid S$. Then $p \geq 5$ and $p \mid a - 2$. It now follows from Theorem 3.8(v) that $\pi(p^i) = p^i$ for $i \geq 1$. Now suppose that q is a prime and $q \mid T$. Then $q \geq 5$ and $q \mid a + 2$. We see by Theorem 3.8(v) that $\pi(q^i) = 2q^i$. The result now follows from (3.6). □

Before presenting Lemma 3.13, we define the *radical* of m, denoted by $\mathrm{rad}(m)$.

Definition 3.12. *Let m be a positive integer. Then* $\mathrm{rad}(1) = 1$ *and for $m \geq 2$,* $\mathrm{rad}(m)$ *is the squarefree integer given by*

$$\mathrm{rad}(m) = \prod_{p \mid m} p. \tag{3.21}$$

Lemma 3.13. *Let $u(a,b)$ be a nondegenerate LSFK with discriminant D, where $b = \pm 1$.*

(i) *If* $\mathrm{rad}(m) \mid 6$, *then*

$$\mathrm{rad}(\rho^i(m)\pi^i(m)) \mid 6 \quad \text{for } i \geq 1. \tag{3.22}$$

(ii) *If* $\mathrm{rad}(m) \mid D$, *then*

$$\mathrm{rad}(\rho^i(m)) \mid D \tag{3.23}$$

and

$$\mathrm{rad}(\pi^i(m)) \mid 6D \quad \text{for } i \geq 1. \tag{3.24}$$

Proof. (i) We see by Theorems 3.7 and 3.8, Lemmas 3.9 and 3.10, and Theorem 3.1(vii) and (viii) that (3.22) holds for $i = 1$. It now follows by induction that (3.22) holds for $i \geq 1$.

(ii) It follows from Theorem 3.7, Lemma 3.11(i), and induction that (3.23) holds. It further follows from Theorem 3.8, Lemma 3.11(ii), the above part (i) of this lemma, (3.6), and induction that (3.24) holds. □

Lemma 3.14. *Consider the nondegenerate LSFK $u(a, \pm 1)$ with discriminant D. Let $A > 1$ be any integer such that for each prime divisor p of A, we have that $p \geq 5$ and $p \nmid D$. Then there exists a positive integer N such that if $i \geq N$, then*

$$\mathrm{rad}(\rho^i(A)\pi^i(A)) \mid 6D. \tag{3.25}$$

Proof. Suppose that $p \geq 5$ and $p \nmid D$. We see from Theorem 3.1(iv) that if q is a prime such that $q > 3$, $q \nmid D$, and $q \mid \rho(p)\pi(p)$, then $q < p$. Now consider the prime power p^k, where $p \geq 5$, $k \geq 2$, and $p \nmid D$. Let $\sigma \geq 1$ and $\tau \geq 1$ be the largest integers such that $\rho(p^\sigma) = \rho(p)$ and $\pi(p^\tau) = \pi(p)$, respectively. Then by Theorem 3.1(v) and (vi), $\rho(p^k) = p^{\max(k-\sigma,0)}\rho(p)$ and $\pi(p^k) = p^{\max(k-\tau,0)}\pi(p)$. It thus follows from Theorem 3.1(v), (vi), and (viii) that if $i \geq \max(k+1-\sigma, 1)$ and $j \geq \max(k+1-\tau, 1)$, then $\rho^i(p^k) = \rho^i(p)$ and $\pi^j(p^k) = \pi^j(p)$.

It also follows from Lemma 3.13(i) and (ii) and from Theorem 3.1(viii) that if $\mathrm{rad}(B) \mid 6D$, then

$$\mathrm{rad}(\rho^i(B)\pi^i(B)) \mid 6D$$

for all $i \geq 1$.

Let $A = p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}$, where $p_1 < p_2 < \cdots < p_r$. Let σ_r and τ_r be the largest positive integers that $\rho(p_r^{\sigma_r}) = \rho(p_r)$ and $\pi(p_r^{\tau_r}) = \pi(p_r)$. By our above argument, we see that if $i \geq \max(k_r + 1 - \sigma_r, 1)$ and $j \geq \max(k_r + 1 - \tau_r, 1)$, then $q < p_r$ for every prime q dividing $\rho^i(p_r)\pi^j(p_r)$ for which $q \geq 5$ and $q \nmid D$. It now follows by an inductive argument that there exists a positive integer N such that (3.25) holds for all $i \geq N$. □

Corollary 3.15. *Let $u(a, \pm 1)$ be a nondegenerate LSFK and let m be a positive integer. Then there exists a positive integer N such that if $i \geq N$, then*

$$\mathrm{rad}(\rho^i(m)\pi^i(m)) \mid 6D.$$

Proof. This follows from Lemmas 3.14, 3.13, and Theorem 3.1(viii). □

Lemma 3.16. *Let $u(a, 1)$ be a nondegenerate LSFK.*

(i) *Suppose that $a \equiv \pm 1 \pmod 6$. Then 12 is a fixed point of ρ and $24R$ is a fixed point of π, where $R \geq 1$.*
(ii) *Suppose that $a \equiv 3 \pmod 6$. Then 6 is a fixed point of both ρ and π, whereas $12R$ is also a fixed point of π, where $R > 1$.*
(iii) *Suppose that $a \equiv 2 \pmod 4$. Then 2^iR is a fixed point of π, where $i \geq 2$ and $R > 1$.*
(iv) *Suppose that $a \equiv 0 \pmod 4$. Then $4R$ is a fixed point of π, where $R > 1$.*

Proof. This follows from Theorems 3.1(vii) and 3.8(iii), and Lemmas 3.9 and 3.11(ii). □

Lemma 3.17. *Let $u(a, -1)$ be a nondegenerate LSFK.*

(i) *Suppose that $a \equiv 5$ or $11 \pmod{18}$. Then $2 \cdot 3^jT$ is a fixed point of π, where $j \geq 1$ and $T > 1$.*
(ii) *Suppose that $a \equiv 7$ or $13 \pmod{18}$. Then $2 \cdot 3^jT$ is a fixed point of π, where $j \geq 1$ and $T \geq 1$.*
(iii) *Suppose that $a \equiv 17 \pmod{18}$. Then $6T$ is a fixed point of π, where $T > 1$.*
(iv) *Suppose that $a \equiv 1 \pmod{18}$. Then $6T$ is a fixed point of π, where $T \geq 1$.*
(v) *Suppose that $a \equiv \pm 2$ or $\pm 14 \pmod{36}$. Then $2^i \cdot 3^jT$ is a fixed point of π, where $i \geq 1$, $j \geq 0$, and $T \geq 1$.*
(vi) *Suppose that $a \equiv \pm 10 \pmod{36}$. Then $2^i \cdot 3^\varepsilon T$ is a fixed point of π, where $i \geq 1$ and $T \geq 1$.*
(vii) *Suppose that $a \equiv \pm 4$ or $\pm 16 \pmod{36}$. Then 2^i3^jT is a fixed point of π, where $i \in \{1, 2\}$, $j \geq 0$, and $T \geq 1$.*
(viii) *Suppose that $a \equiv \pm 8 \pmod{36}$. Then $2^i3^\varepsilon T$ is a fixed point of π, where $i \in \{1, 2\}$ and $T \geq 1$.*
(ix) *Suppose that $a \equiv 3 \pmod 6$. Then 6 is a fixed point of ρ, whereas $12T$ is a fixed point of π, where $T \geq 1$.*

(x) *Suppose that* $a \equiv 6 \pmod{12}$. *Then* $2^i T$ *is a fixed point of* π, *where* $i \geq 1$ *and* $T \geq 1$.
(xi) *Suppose that* $a \equiv 0 \pmod{12}$. *Then* $2^i T$ *is a fixed point of* π, *where* $i \in \{1, 2\}$ *and* $T \geq 1$.

Proof. This follows from Theorems 3.1(vii) and 3.8(iii), (vii), (viii), (ix), and Lemmas 3.10 and 3.11(iii). □

Lemma 3.18. *Let* $u(a, 1)$ *be a nondegenerate LSFK. Let* $c = \nu_3(a^2 + 2)$, $d = \nu_3(a)$, *and* $e = \nu_2(a)$.

(i) *If* $a \equiv 0 \pmod{2}$, *then* $\pi^j(R) = 4R$ *for* $j \geq 1$ *and* $R > 1$.
(ii) *Suppose that* $a \equiv \pm 1 \pmod{6}$. *Then* $c = \nu_3(u_4)$. *Moreover,* $c = 1$ *if* $a \equiv \pm 1$ *or* $\pm 2 \pmod{9}$, *whereas* $c \geq 2$ *if* $a \equiv \pm 4 \pmod{9}$.
  (a) *If* $j \geq \max(4, \lceil (i-4)/2 \rceil + 1)$, *then* $\rho^j(2^i) = 12$ *for* $i \geq 1$.
  (b) *If* $j \geq \max(3, i - c)$, *then* $\rho^j(3^i) = 12$ *for* $i \geq 1$.
  (c) *If* $j \geq \max(4, i - 3)$, *then* $\pi^j(2^i) = 24$ *for* $i \geq 1$.
  (d) *If* $j \geq \max(3, i - c)$, *then* $\pi^j(3^i) = 24$ *for* $i \geq 1$.
  (e) *If* $j \geq 1$, *then* $\pi^j(R) = 24R$ *for* $R > 1$.
(iii) *Suppose that* $a \equiv 3 \pmod{6}$. *Then* $d = \nu_3(u_2)$ *and* $d \geq 1$.
  (a) $\rho^{2j-1}(2) = \pi^{2j-1}(2) = 3$ *and* $\rho^{2j}(2) = \pi^{2j}(2) = 2$ *for* $j \geq 1$.
  (b) *If* $j \geq 1$ *and* $1 \leq i \leq d$, *then* $\rho^{2j-1}(3^i) = \pi^{2j-1}(3^i) = 2$ *and* $\rho^{2j}(3^i) = \pi^{2j}(3^i) = 3$.
  (c) *If* $j \geq \lceil (i-1)/2 \rceil$, *then* $\rho^j(2^i) = 6$ *for* $i \geq 2$.
  (d) *If* $j \geq i - d$, *then* $\rho^j(3^i) = \pi^j(3^i) = 6$ *for* $i \geq d + 1$.
  (e) *If* $j \geq i - 1$, *then* $\pi^j(2^i) = 6$ *for* $i \geq 2$.
  (f) *If* $j \geq 2$, *then* $\pi^j(R) = 12R$ *for* $R > 1$.
(iv) *Suppose that* $a \equiv 0 \pmod{6}$. *Then* $d = \nu_3(u_2)$ *and* $d \geq 1$. *If* $j \geq \max(i + 1 - d, 1)$, *then* $\rho^j(3^i) = \pi^j(3^i) = 2$ *for* $i \geq 1$.
(v) *Suppose that* $a \equiv \pm 2 \pmod{12}$. *Then* $c = \nu_3(u_4)$ *and* $c \geq 1$. *If* $j \geq \max(i + 1 - c, 1)$, *then* $\rho^j(3^i) = 4$ *and* $\pi^j(3^i) = 8$ *for* $i \geq 1$.
(vi) *Suppose that* $a \equiv 0 \pmod{4}$. *Then* $e = \nu_2(u_2)$ *and* $e \geq 1$. *If* $j \geq \max(i + 1 - e, 1)$, *then* $\rho^j(2^i) = \pi^j(2^i) = 2$ *for* $i \geq 1$.
(vii) *Suppose that* $a \equiv \pm 4 \pmod{12}$. *Then* $c = \nu_3(u_4)$ *and* $c \geq 1$. *If* $j \geq \max(i + 3 - c, 3)$, *then* $\rho^j(3^i) = \pi^j(3^i) = 2$ *for* $i \geq 1$.

Proof. This follows from (1.13), Theorem 3.1(viii), Theorem 3.7(v), Theorem 3.8(iii) and (vi), and Lemmas 3.9, 3.16, and 3.11(ii). □

Lemma 3.19. *Let* $u(a, -1)$ *be a nondegenerate LSFK. Suppose that* $d = \nu_3(a)$, $e = \nu_2(a)$, $g = \nu_3(a^2 - 1)$, *and* $\ell = \nu_2(a^2 - 1)$.

(i) *Suppose that* $a \equiv 0 \pmod{2}$. *Then* $\pi^j(T) = 2T$ *for* $j \geq 1$ *and* $T > 1$.
(ii) *Suppose that* $a \equiv 0 \pmod{4}$. *Then* $e = \nu_2(u_2)$ *and* $e \geq 1$.
  (a) *If* $j \geq \max(i + 1 - e, 1)$, *then* $\rho^j(2^i) = 2$ *for* $i \geq 1$.
  (b) *If* $j \geq \max(i - e, 1)$, *then* $\pi^j(2^i) = 4$ *for* $i \geq 2$.
(iii) *Suppose that* $a \equiv \pm 1 \pmod{6}$. *Then* $\ell = \nu_2(u_3)$ *and* $\ell \geq 3$.
  (a) *If* $j \geq 2$, *then* $\pi^j(T) = 6T$ *for* $T > 1$.
  (b) *If* $j \geq \max(i + 1 - \ell, 1)$, *then* $\rho^{2j}(2^i) = 3$ *for* $i \geq 1$.
(iv) *Suppose that* $a \equiv 3 \pmod{6}$. *Then* $d = \nu_3(u_2) \geq 1$ *and* $\ell = \nu_2(u_3) \geq 3$.
  (a) *If* $j \geq 3$, *then* $\pi^j(T) = 12T$ *for* $T > 1$.
  (b) $\rho^{2j-1}(2^i) = 3$ *and* $\rho^{2j}(2^i) = 2$ *for* $j \geq 1$ *and* $1 \leq i \leq \ell$.
  (c) $\rho^{2j-1}(3^i) = 2$ *and* $\rho^{2j}(3^i) = 3$ *for* $j \geq 1$ *and* $1 \leq i \leq d$.
  (d) *If* $j \geq i - \ell$, *then* $\rho^j(2^i) = 6$ *for* $i \geq \ell + 1$.

(e) *If* $j \geq i-d$, *then* $\rho^j(3^i) = 6$ *for* $i \geq d+1$.

(v) *Suppose that* $a \equiv 5$ *or* $11 \pmod{18}$. *If* $j \geq \max(i+2-\ell, 2)$, *then* $\pi^j(2^i) = 3$ *for* $i \geq 1$.

(vi) *Suppose that* $a \equiv 7$ *or* $13 \pmod{18}$. *If* $j \geq \max(i+1-\ell, 2)$, *then* $\pi^j(2^i) = 6$ *for* $i \geq 1$.

(vii) *Suppose that* $a \equiv 4$ *or* $7 \pmod{9}$. *If* $j \geq 1$, *then* $\pi^j(3^i) = 2 \cdot 3^i$ *for* $i \geq 1$.

(viii) *Suppose that* $a \equiv 8 \pmod{9}$. *Then* $g = \nu_3(u_3)$ *and* $g \geq 2$. *If* $j \geq \max(i+1-g, 1)$, *then* $\pi^j(3^i) = 3$ *for* $i \geq 1$.

(ix) *Suppose that* $a \equiv 1 \pmod{9}$. *Then* $g = \nu_3(u_3)$ *and* $g \geq 2$. *If* $j \geq \max(i+1-g, 1)$, *then* $\pi^j(3^i) = 6$ *for* $i \geq 1$.

(x) *Suppose that* $a \equiv 3 \pmod{12}$.
  (a) $\pi^{2j-1}(2^i) = 3$ *and* $\pi^{2j}(2^i) = 4$ *for* $j \geq 1$ *and* $1 \leq i \leq \ell - 1$.
  (b) $\pi^{2j-1}(3^i) = 4$ *and* $\pi^{2j}(3^i) = 3$ *for* $j \geq 1$ *and* $1 \leq i \leq d$.
  (c) *If* $j \geq \max(i-\ell, 2)$, *then* $\pi^j(2^i) = 12$ *for* $i \geq \ell$.
  (d) *If* $j \geq i-d$, *then* $\pi^j(3^i) = 12$ *for* $i \geq d+1$.

(xi) *Suppose that* $a \equiv 9 \pmod{12}$.
  (a) *If* $j \geq \max(i-\ell, 4)$, *then* $\pi^j(2^i) = 12$ *for* $i \geq 1$.
  (b) *If* $j \geq \max(i-d, 3)$, *then* $\pi^j(3^i) = 12$ *for* $i \geq 1$.

(xii) *Suppose that* $a \equiv 0 \pmod{6}$. *Then* $d = \nu_3(u_2)$ *and* $d \geq 1$. *If* $j \geq \max(i+1-d, 1)$, *then* $\rho^j(3^i) = 2$ *and* $\pi^j(3^i) = 4$ *for* $i \geq 1$.

Proof. This follows from (1.13), Theorem 3.1(viii), Theorem 3.8(iii), (vii), (viii), and (ix), and Lemmas 3.10, 3.11(iii), and 3.17. □

4. Proofs of the Main Theorems

Proof of Theorems 2.2 and 2.3. We suppose that $u(a,b)$ is a nondegenerate LSFK, where $b = \pm 1$. Let m_1 and m_2 be positive integers. It follows from Corollary 3.15, Theorem 3.1(viii) and (ix), Theorem 3.8(iii) and (vi)–(ix), Lemma 3.11 (i)–(iii), and Lemmas 3.16–3.19 that the process of integrating $\rho(m_1)$ and $\pi(m_2)$ terminates in the fixed points r_1 and r_2 if and only if r_1 and r_2 are each one of the fixed points given in Theorems 2.2 and 2.3, respectively, depending on the value of a. □

Proof of Theorem 2.4. This follows from Corollary 3.15, Theorem 3.1(viii) and (ix), Theorem 3.8(iii) and (vi), Lemma 3.11(i) and (ii), Lemma 3.18, and Theorem 2.2. □

Proof of Theorem 2.5. This follows from Corollary 3.15, Theorem 3.1(viii) and (ix), Theorem 3.8(iii) and (vii)–(ix), Lemma 3.11(i) and (iii), Lemma 3.19, and Theorem 2.3. □

Acknowledgement

We thank the anonymous referee for careful reading of the manuscript and suggestions that improved it. This paper was supported by RVO 67985840 of the Czech Republic.

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] J. D. Fulton and W.Ł. Morris, *On arithmetical functions related to the Fibonacci numbers*, Acta Arith., **XVI** (1969), 105–110.

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

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

[7] M. Ward, *Prime divisors of second order recurring sequences*, Duke Math. J., **21** (1954), 607–614.
[8] W. A. Webb, 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.
[9] O. Wyler, *On second-order recurrences*, Amer. Math. Monthly, **72** (1965), 500–506.

MSC2010: 11B39, 11A07

Lawrence Somer, Department of Mathematics, Catholic University of America, Washington, D.C. 20064, U.S.A.
E-mail address: somer@cua.edu

Michal Křížek, Institute of Mathematics, Czech Academy of Sciences, Žitná 25, CZ – 115 67 Prague 1, Czech Republic
E-mail address: krizek@math.cas.cz