Notes on Number Theory and Discrete Mathematics
Print ISSN 1310–5132, Online ISSN 2367–8275
2024, Volume 30, Number 1, 47–66
DOI: 10.7546/nntdm.2024.30.1.47-66

Second-order linear recurrences with identically distributed residues modulo p^e

Lawrence Somer[1] **and Michal Křížek**[2]

[1] Department of Mathematics, Catholic University of America
Washington, D.C. 20064, United States
e-mail: somer@cua.edu

[2] Institute of Mathematics, Czech Academy of Sciences
Žitná 25, CZ – 115 67 Prague 1, Czech Republic
e-mail: krizek@math.cas.cz

Received: 8 September 2023 **Revised:** 21 February 2024
Accepted: 23 February 2024 **Online First:** 27 February 2024

Abstract: Let p be an odd prime and let $u(a,-1)$ and $u(a',-1)$ be two Lucas sequences whose discriminants have the same nonzero quadratic character modulo p and whose periods modulo p are equal. We prove that there is then an integer c such that for all $d \in \mathbb{Z}_p$, the frequency with which d appears in a full period of $u(a,-1) \pmod p$ is the same frequency as cd appears in $u(a',-1) \pmod p$. Here $u(a,b)$ satisfies the recursion relation $u_{n+2} = au_{n+1} + bu_n$ with initial terms $u_0 = 0$ and $u_1 = 1$. Similar results are obtained for the companion Lucas sequences $v(a,-1)$ and $v(a',-1)$. This paper extends analogous statements for Lucas sequences of the form $u(a,1) \pmod p$ given in a previous article. We further generalize our results by showing for a certain class of primes p that if $e > 1$, $b = \pm 1$, and $u(a,b)$ and $u(a',b)$ are Lucas sequences with the same period modulo p, then there exists an integer c such that for all residues $d \pmod{p^e}$, the frequency with which d appears in $u(a,b) \pmod{p^e}$ is the same frequency as cd appears in $u(a',b) \pmod{p^e}$.

Keywords: Lucas sequences, Discriminant, Primes, Second-order recurrence.
2020 Mathematics Subject Classification: 11B39, 11A07, 11A41.

1 Introduction

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

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

where the parameters a and b and the initial terms w_0 and w_1 are all integers. We distinguish two special recurrences, the Lucas sequence of the first kind (LSFK) $u(a, b)$ and the Lucas sequence of the second kind (LSSK) $v(a, b)$ with initial terms $u_0 = 0$, $u_1 = 1$ and $v_0 = 2$, $v_1 = a$, respectively. Associated with the linear recurrence $w(a, b)$ is the characteristic polynomial $f(x)$ defined by

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

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

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \quad v_n = \alpha^n + \beta^n. \tag{1.3}$$

Throughout this paper, m will denote a positive integer, p will denote an odd prime unless specified otherwise, and ε will specify an element from $\{-1, 1\}$. It was shown in Carmichael [3, pp. 344–345] that $w(a, b)$ is purely periodic modulo m if $\gcd(b, m) = 1$. From here on, we assume that $\gcd(b, m) = 1$. We will usually assume that $b = \pm 1$, which will automatically guarantee that $\gcd(b, m) = 1$. If $(r/p) = 1$, where (r/p) denotes the Legendre symbol, $\sqrt{r}$ modulo p will denote the residue c modulo p such that $c^2 \equiv r \pmod{p}$ and $0 \leq c \leq (p-1)/2$.

The *period* of $w(a, b)$ modulo m, denoted by $\lambda_w(m)$, is the least positive integer c such that $w_{n+c} \equiv w_n \pmod{m}$ for all $n \geq 0$. The *restricted period* of $w(a, b)$ modulo m, denoted by $h_w(m)$, is the least positive integer r such that $w_{n+r} \equiv Mw_n \pmod{m}$ for all $n \geq 0$ and some fixed residue M modulo m such that $\gcd(M, m) = 1$. Here $M = M_w(m)$ is called the *multiplier* of $w(a, b)$ modulo m. Since the LSFK $u(a, b)$ is purely periodic modulo m and has initial terms $u_0 = 0$ and $u_1 = 1$, it is easily seen that $h_u(m)$ is the least positive integer r such that $u_r \equiv 0 \pmod{m}$. It is proved in Carmichael [3, pp. 354–355] that $h_w(m) \mid \lambda_w(m)$. Let $E_w(p) = \frac{\lambda_w(m)}{h_w(m)}$. Then by Carmichael [3, pp. 354–355], $E_w(m)$ is the multiplicative order of the multiplier M modulo m.

The main result of the paper Somer & Křížek [20] was to prove that if p is a fixed prime and $u(a_1, 1)$ and $u(a_2, 1)$ are two LSFK's with the same restricted period modulo p, or equivalently the same period modulo p, then the residues appearing in $u(a_2, 1)$ are fixed multiples of the residues appearing in $u(a_1, 1)$ modulo p. Even more so, it was shown that if $v(a_1, 1)$ and $v(a_2, 1)$ are two LSSK's with the same restricted period modulo p, then the residues modulo p appearing in $v(a_2, 1)$ are exactly the same as the residues appearing in $v(a_1, 1)$ modulo p. The results of Somer & Křížek [20] extend those in Somer & Křížek [19].

In this paper, we will prove similar results for the Lucas sequences $u(a, -1)$ and $v(a, -1)$ modulo p. Furthermore, we will extend these results to $u(a, \pm 1)$ modulo prime powers for a certain class of primes.

Given a residue d modulo m, we let $A_w(d, m)$ denote the number of times that d appears in a minimal period of (w) modulo m. If the modulus m is clearly specified, we frequently simply

write only $A_w(d)$ rather than $A_w(d, m)$. We have the following theorem regarding upper bounds for $A_w(d, p)$.

Theorem 1.1. *Let p be a fixed prime and consider the recurrence $w(a, b)$ and the LSFK $u(a, b)$. Let d be a fixed residue modulo p such that $0 \leq d \leq p-1$. Let $g = \mathrm{ord}_p(-b)$, where $\mathrm{ord}_p(-b)$ denotes the multiplicative order of $(-b)$ modulo p.*

(i) $A_w(d) \leq \min(2 \cdot \mathrm{ord}_p(-b), p)$.

(ii) $A_u(0) = E_u(p) \leq \min(p-1, 2g)$ *and* $A_u(d) \leq \min(g + E_u(p), 2g, p)$ *if* $d \neq 0$.

(iii) If $b = 1$ *then* $A_w(d) \leq 4$.

(iv) If $b = 1$ *and* $E_u(p) = 1$, *then* $A_u(d) \leq 3$.

(v) If $b = -1$ *then* $A_w(d) \leq 2$.

Proof. Part (i) was proved in Theorem 3 of Niederreiter et al. [9]. Part (ii) was proved in Theorem 2 of Somer [17]. Parts (iii) and (v) follow from parts (i) and (ii), respectively. □

Before proceeding further, we will need the following results and definitions.

Definition 1.2. *Let p be a fixed prime. The recurrence $w(a, b)$ is said to be p-regular if*

$$\begin{vmatrix} w_0 & w_1 \\ w_1 & w_2 \end{vmatrix} = w_0 w_2 - w_1^2 \not\equiv 0 \pmod{p}. \tag{1.4}$$

Otherwise, the recurrence $w(a, b)$ is called p-irregular. The p-irregular recurrence in which $w_n \equiv 0 \pmod{p}$ for all $n \geq 0$ is called the trivial recurrence modulo p.

The recurrence $w(a, b)$ is p-irregular if and only if it satisfies a recursion relation modulo p of order less than two.

Theorem 1.3. *Suppose that the recurrences $w(a, b)$ and $w'(a, b)$ are both p-regular. Then*

$$\lambda_w(p) = \lambda_{w'}(p),\ h_w(p) = h_{w'}(p),\ E_w(p) = E_{w'}(p), \quad \textit{and} \quad M_w(p) \equiv M_{u'}(p) \pmod{p}.$$

This is proved in Carlip & Somer [1, p. 695].

Theorem 1.4. *Let p be a fixed prime. Consider the LSFK $u(a, b)$ and the LSSK $v(a, b)$ with discriminant $D = a^2 + 4b$. Then*

(i) $u(a, b)$ is p-regular,

(ii) $v(a, b)$ is p-regular if and only if $p \nmid D$.

Proof. (i) We note that

$$u_0 u_2 - u_1^2 = 0 \cdot a - 1^2 = -1 \not\equiv 0 \pmod{p}.$$

Thus, $u(a, b)$ is p-regular by (1.4).
(ii) We observe that

$$v_0 v_2 - v_1^2 = 2(a^2 + 2b) - a^2 = a^2 + 4b = D.$$

Thus, $v(a, b)$ is p-regular if and only if $p \nmid D$. □

Theorem 1.5. *Let p be a fixed prime. Consider the p-regular recurrence $w(a,b)$ with discriminant D. Let $h = h_w(p)$ and $\lambda = \lambda_w(p)$. Then*

(i) $h > 1$ *and* $h \mid p - (D/p)$, *where* $(D/p) = 0$ *if* $p \mid D$.

(ii) If $(D/p) = 0$, *then* $h = p$.

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

(iv) If $w(a,b) = u(a,b)$, *then* $u_n \equiv 0 \pmod{p}$ *if and only if* $h \mid n$.

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

Proof. We first note that by Theorem 1.3 and Theorem 1.4 (i) and (iii), we have $h_w(p) > 1$, $h_w(p) = h_u(p)$, and $\lambda_w(p) = \lambda_u(p)$, since both $w(a,b)$ and $u(a,b)$ are p-regular. Parts (i) and (v) are proved in Carmichael [2, pp. 44–45] and Lucas [6, pp. 290, 296, 297]. Parts (ii) and (iv) are proved in Lehmer [5, pp. 423–424]. Part (iii) is proved in Lehmer [5, p. 441]. □

Theorem 1.6. *Let $w(a,1)$ be a p-regular recurrence with discriminant D. Then*

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

(ii) $E_w(p) = 1$ *if and only if* $h_w(p) \equiv 2 \pmod{4}$. *Moreover, if* $E_w(p) = 1$, *then* $(D/p) = 1$.

(iii) $E_w(p) = 2$ *if and only if* $h_w(p) \equiv 0 \pmod{4}$. *Moreover, if* $E_w(p) = 2$, *then* $(D/p) = (-1/p)$.

(iv) $E_w(p) = 4$ *if and only if* $h_w(p)$ *is odd. Moreover, if* $E_w(p) = 4$ *then* $p \equiv 1 \pmod{4}$.

(v) If $p \equiv 3 \pmod{4}$ *and* $(D/p) = 1$, *then* $h_w(p) \equiv 2 \pmod{4}$ *and* $E_w(p) = 1$.

(vi) If $p \equiv 3 \pmod{4}$ *and* $(D/p) = -1$, *then* $h_w(p) \equiv 0 \pmod{4}$ *and* $E_w(p) = 2$.

(vii) If $p \equiv 1 \pmod{4}$ *and* $(D/p) = -1$, *then* $h_w(p)$ *is odd and* $E_w(p) = 4$.

Proof. By Theorem 1.4 (i), $u(a,b)$ is p-regular. It now follows from Theorem 1.3 that $h_w(p) = h_u(p)$ and $\lambda_w(p) = \lambda_u(p)$. Parts (i)–(vii) now follow from Lemma 3 and Theorem 13 of Somer [12]. □

Theorem 1.7. *Let $w(a,-1)$ be a p-regular recurrence with discriminant D. Then*

(i) $E_w(p) = 1$ *or* 2.

(ii) If $\lambda_w(p)$ *is odd, then* $h_w(p)$ *is odd,* $E_w(p) = 1$, *and* $M_w(p) \equiv 1 \pmod{p}$.

(iii) If $\lambda_w(p) \equiv 2 \pmod{4}$, *then* $h_w(p)$ *is odd,* $E_w(p) = 2$, *and* $M_w(p) \equiv -1 \pmod{p}$.

(iv) If $\lambda_w(p) \equiv 0 \pmod{4}$, *then* $h_w(p)$ *is even,* $E_w(p) = 2$, *and* $M_w(p) \equiv -1 \pmod{p}$.

(v) If $\left(\frac{2-a}{p}\right) = -1$ *and* $\left(\frac{2+a}{p}\right) = 1$, *then* $\lambda_w(p)$ *is odd.*

(vi) If $\left(\frac{2-a}{p}\right) = 1$ *and* $\left(\frac{2+a}{p}\right) = -1$, *then* $\lambda_w(p) \equiv 2 \pmod{4}$.

(vii) If $\left(\frac{2-a}{p}\right) = \left(\frac{2+a}{p}\right) = -1$, *then* $\lambda_w(p) \equiv 0 \pmod{4}$.

(viii) If $p \nmid D$, *then* $h_w(p) \mid (p - (D/p))/2$ *and* $\lambda_w(p) \mid p - (D/p)$.

The proof follows from Theorem 1.4 (i), Theorem 1.3, and Theorem 1.5 (iii) of this paper and from Theorem 16 of Somer [12].

Definition 1.8. *Let p be a fixed prime. The recurrences $w(a,b)$ and $w'(a,b)$ are p-equivalent if $w'(a,b)$ is a nonzero multiple of a translation of $w(a,b)$ modulo p, that is, there exists a nonzero residue c and a fixed integer r such that*

$$w'_n \equiv cw_{n+r} \pmod{p} \quad \text{for all } n \geq 0. \tag{1.5}$$

It is clear that p-equivalence is indeed an equivalence relation on the set of recurrences $w(a,b)$ modulo p, since c is invertible modulo p. It is also evident that if $w'(a,b)$ is p-equivalent to $w(a,b)$ and (1.5) holds, then

$$A_{w'}(cd) = A_w(d) \tag{1.6}$$

for $0 \leq d \leq p-1$.

Theorem 1.9. *Suppose that $w(a,b)$ and $w'(a,b)$ are p-equivalent recurrences such that $w'_n \equiv cw_{n+r} \pmod{p}$ for all $n \geq 0$, where c is a fixed nonzero residue modulo p and r is a fixed integer. Then $w(a,b)$ and $w'(a,b)$ are either both p-regular or both p-irregular.*

This is proven in Carlip & Somer [1, p. 694].

Theorem 1.10. *Let $w(a,b)$ be a p-regular recurrence. Then $w(a,b)$ is p-equivalent to $u(a,b)$ if and only if $w_n \equiv 0 \pmod{p}$ for some $n \geq 0$.*

Proof. This follows from the fact that $u_0 \equiv 0 \pmod{p}$, from Definition 1.8, from Theorem 1.4 (i), and from the fact that if $c \not\equiv 0 \pmod{p}$, then $cm \equiv 0 \pmod{p}$ if and only if $m \equiv 0 \pmod{p}$. □

Theorem 1.11. *Let p be a fixed prime and let $\varepsilon \in \{-1, 1\}$.*

(i) If $p \equiv 1 \pmod{4}$, then there exists a LSFK $u(a,1)$ such that $(D/p) = \varepsilon$ and $h_u(p) = r$ if and only if $r \mid (p-\varepsilon)/2$ and $r \neq 1$.

(ii) If $p \equiv 3 \pmod{4}$, then there exists a LSFK $u(a,1)$ such that $h_u(p) = r$ if and only if $r \mid p+\varepsilon$ and $r \nmid (p-\varepsilon)/2$.

(iii) There exists a LSFK $u(a,-1)$ such that $(D/p) = \varepsilon$ and $h_u(p) = r$ if and only if $r \mid (p-\varepsilon)/2$ and $r \neq 1$.

(iv) Let $p > 3$. Then there exists a LSFK $u(a,-1)$ such that $(D/p) = \varepsilon$ and $\lambda_u(p) = p - \varepsilon$.

(v) If there exists a LSFK $u(a,\varepsilon_1)$ such that $(D/p) = \varepsilon$ and $h_u(p) = r$, where $\varepsilon_1 \in \{-1,1\}$, then there exist exactly $\phi(r)$ such LSFK's, where $\phi(r)$ denotes Euler's totient function and $0 \leq a \leq p-1$.

Proof. Parts (i)–(iii) follow from Theorem 12 of Somer [13]. and Theorems 3 and 4 of Somer [16]. Part (iv) follows from Theorem 11 of Somer [13] and Theorems 1 and 2 of Somer [16]. Part (v) is proved in Theorems 3.7, 3.8, and 3.12 of Müller [8]. □

The principal results of the paper Somer & Křížek [20] are given in Theorems 1.12 and 1.13.

Theorem 1.12. *Let p be an odd prime. Suppose that $(u) = u(a_1, 1)$ and $(u') = u(a_2, 1)$ both have the same restricted period $h = h_u(p)$ and that the associated respective discriminants D_1 and D_2 both have the same nonzero quadratic character modulo p. Then (u) and (u') have the same period modulo p and there exists an integer c such that*

$$A_{u'}(d) = A_u(cd) \quad \forall d \in \{0, 1, \ldots, p-1\},$$

where

$$c \equiv \begin{cases} \varepsilon\sqrt{D_2 D_1^{-1}} \pmod{p} & \text{if } h \equiv 2 \pmod{4} \\ \sqrt{D_2 D_1^{-1}} \pmod{p} & \text{if } h \not\equiv 2 \pmod{4} \end{cases}$$

for some $\varepsilon = \pm 1$.

In the case $h \not\equiv 2 \pmod 4$, we may also choose $c \equiv M^k\sqrt{D_2 D_1^{-1}} \pmod p$, where k is any integer and M is the multiplier $M_u(p)$.

Theorem 1.13. *Let p be an odd prime. Suppose that $(v) = v(a_1, 1)$ and $(v') = v(a_2, 1)$ both have the same restricted period $h = h_v(p)$ and that the associated respective discriminants D_1 and D_2 both have the same nonzero quadratic character modulo p. Then (v) and (v') have the same period modulo p and*

$$A_{v'}(d) = A_v(d) \quad \forall d \in \{0, 1, \ldots, p-1\}.$$

Moreover, in the case $h \not\equiv 2 \pmod 4$ we also have that

$$A_{v'}(d) = A_v(M^k d) \quad \forall d \in \{0, 1, \ldots, p-1\},$$

where k is any integer and M is the multiplier $M_v(p)$.

The example below illustrates Theorems 1.12 and 1.13 for particular cases.

Example 1.14. Let $p = 11$. Consider the LSFK's $(u) = u(4, 1)$ and $(u') = u(1, 1)$ and the LSSK's $(v) = v(4, 1)$ and $(v') = v(1, 1)$ modulo 11. The first 12 terms of $u(4, 1)$, $u(1, 1)$, $v(4, 1)$, and $v(1, 1)$ modulo 11 are:

$$\begin{aligned} u(4,1):&\ \{0,1,4,6,6,8,5,6,7,1,0,1\},\\ u(1,1):&\ \{0,1,1,2,3,5,8,2,10,1,0,1\},\\ v(4,1):&\ \{2,4,7,10,3,0,3,1,7,7,2,4\},\\ v(1,1):&\ \{2,1,3,4,7,0,7,7,3,10,2,1\}. \end{aligned}$$

Thus, the restricted period and periods modulo 11 of all these four sequences are equal to $10 \equiv 2 \pmod 4$, and each recurrence has the same multiplier $M \equiv 1 \pmod{11}$. We observe that $u(4, 1)$ and $v(4, 1)$ both have the discriminant $D_1 = 20$, while $u(1, 1)$ and $v(1, 1)$ each has the discriminant $D_2 = 5$. Moreover,

$$\left(\frac{D_1}{11}\right) = \left(\frac{9}{11}\right) = \left(\frac{D_2}{11}\right) = \left(\frac{5}{11}\right) = 1.$$

Further, we let $c \equiv \sqrt{D_2/D_1} \pmod{11}$. Then

$$c \equiv \sqrt{\frac{5}{9}} \equiv \sqrt{3} \equiv 5 \pmod{11}.$$

By inspection, we see that indeed

$$A_{u'}(d) = A_u(6d) = A_u(-cd)$$

and

$$A_{v'}(d) = A(d)$$

for all $d \in \{0, 1, 2, \ldots, 10\}$.

In the next section we present the principal results of this paper.

2 Main theorems

Theorem 2.1. *Let p be an odd prime. Suppose that $(u) = u(a_1, -1)$ and $(u') = u(a_2, -1)$ both have the same period $\lambda = \lambda_u(p)$ and that the associated respective discriminants D_1 and D_2 both have the same nonzero quadratic character modulo p. Then there exists an integer c such that*

$$A_{u'}(d) = A_u(cd) \quad \forall d \in \{0, 1, \ldots, p-1\}, \tag{2.1}$$

where

$$c \equiv \begin{cases} \varepsilon\sqrt{D_2 D_1^{-1}} \pmod{p} & \text{if } \lambda \text{ is odd} \\ \sqrt{D_2 D_1^{-1}} \pmod{p} & \text{if } \lambda \text{ is even} \end{cases}$$

for some $\varepsilon = \pm 1$.

In the case λ is even, we may also choose

$$c \equiv -\sqrt{D_2 D_1^{-1}} \pmod{p}. \tag{2.2}$$

Theorem 2.2. *Let p be an odd prime. Suppose that $(v) = v(a_1, -1)$ and $(v') = v(a_2, -1)$ both have the same period $\lambda = \lambda_v(p)$ and that the associated respective discriminants D_1 and D_2 both have the same nonzero quadratic character modulo p. Then*

$$A_{v'}(d) = A_v(d) \quad \forall d \in \{0, 1, \ldots, p-1\}. \tag{2.3}$$

Moreover, in the case for which λ is even, we also have that

$$A_{v'}(d) = A_v(-d) \quad \forall d \in \{0, 1, \ldots, p-1\}. \tag{2.4}$$

Theorems 2.1 and 2.2 will be proved in Section 4.

Example 2.3. Let $p = 17$. Consider the LSFK's $(u) = u(4, -1)$ and $(u') = (10, -1)$ and the LSSK's $(v) = v(4, -1)$ and $(v') = v(10, -1)$ modulo 17. The first 20 terms of $u(4, -1)$, $u(10, -1)$, $v(4, -1)$, and $v(10, -1)$ modulo 17 are:

$$\begin{aligned}
u(4,-1):&\ \{0,1,4,15,5,5,15,4,1,0,-1,-4,-15,-5,-5,-15,-4,-1,0,1\},\\
u(10,-1):&\ \{0,1,10,14,11,11,14,10,1,0,-1,-10,-14,-11,-11,-14,-10,-1,0,1\},\\
v(4,-1):&\ \{2,4,14,1,7,10,16,3,13,15,13,3,16,10,7,1,14,4,2,4\},\\
v(10,-1):&\ \{2,10,13,1,14,3,16,4,7,15,7,4,16,3,14,1,13,10,2,10\}.
\end{aligned}$$

Therefore, for all four of these recurrences, the restricted periods modulo 17 are each equal to 9, the periods modulo 17 are all equal to $18 \equiv 0 \pmod 2$, and $M \equiv -1 \pmod{17}$. Moreover, $u(4,-1)$ and $v(4,-1)$ both have the discriminant $D_1 = 12$, whereas $u(10,-1)$ and $v(10,-1)$ each has the discriminat $D_2 = 96$. We observe that

$$\left(\frac{D_1}{17}\right) = \left(\frac{12}{17}\right) = \left(\frac{D_2}{17}\right) = \left(\frac{11}{17}\right) = -1.$$

Further, we let $c \equiv \sqrt{D_2/D_1} \pmod{17}$. Then

$$c \equiv \sqrt{\frac{11}{12}} \equiv \sqrt{8} \equiv 5 \pmod{17}.$$

By examination, we find that

$$A_{u'}(d) = A_u(5d) = A_u(12d) = A_u(cd) = A_u(-cd)$$

and

$$A_{v'}(d) = A_v(d) = A_v(-d)$$

for all $d \in \{0, 1, 2, \ldots, 16\}$ as required by Theorems 2.1 and 2.2.

Corollary 2.4 below follows from Theorems 2.1 and 2.2 upon application of Theorem 1.7, Theorem 1.9, and (1.6).

Corollary 2.4. *Let p be a fixed prime. Let $w(a_1,1)$ and $w'(a_2,1)$ be recurrences with discriminants $D_1 = a_1^2 + 4$ and $D_2 = a_2^2 + 4$, respectively, such that $p \nmid D_1 D_2$ and $(D_1/p) = (D_2/p)$. Suppose that either $w(a_1,1)$ is p-equivalent to $u(a_1,1)$ and $w'(a_2,1)$ is p-equivalent to $u(a_2,1)$, or it is the case that $w(a,1)$ is p-equivalent to $v(a_1,1)$ and $w'(a_2,1)$ is p-equivalent to $v(a_2,1)$.*

Suppose further that $h_w(p) = h_{w'}(p)$. This occurs if and only if $\lambda_w(p) = \lambda_{w'}(p)$. Then there exists a nonzero residue c modulo p such that $A_{w'}(d) = A_w(cd)$ for $0 \le d \le p-1$.

In Theorems 2.5 and 2.6, we extend Theorems 1.12 and 2.1 to prime powers for a certain class of primes.

Theorem 2.5. *Let $\varepsilon \in \{-1, 1\}$ and p be an odd prime. Consider the LSFK's $(u) = u(a_1,1)$ and $(u') = u(a_2,1)$ with restricted periods $h = h_u(p)$ and $h_1 = h_{u'}(p)$ and respective discriminants D_1 and D_2. Suppose that $(D_1/p) = (D_2/p) = \varepsilon$ and*

$$h = h_u(p) = h_{u'}(p) \equiv 1 \pmod 2. \tag{2.5}$$

Then

$$p \equiv 1 \pmod 4 \tag{2.6}$$

and

$$\lambda = \lambda_u(p) = \lambda_{u'}(p) = 4h. \tag{2.7}$$

Suppose further that

$$h_u(p) \ne h_u(p^2) \quad \text{and} \quad h_{u'}(p) \ne h_{u'}(p^2). \tag{2.8}$$

Then

$$\lambda_u(p) \ne \lambda_u(p^2) \quad \text{and} \quad \lambda_{u'}(p) \ne \lambda_{u'}(p^2). \tag{2.9}$$

Let $e > 1$. Then

$$h_u(p^e) = h_{u'}(p^e), \quad \lambda_u(p^e) = \lambda_{u'}(p^e), \tag{2.10}$$

and

$$E_u(p^e) = E_{u'}(p^e) = E_u(p) = 4. \tag{2.11}$$

Denote $M_u(p^e)$ by M. Let

$$c \equiv \sqrt{D_2 D_1^{-1}} \pmod{p}, \tag{2.12}$$

where $c \in \{1, 2, \ldots, (p-1)/2\}$. Suppose that $c_1 \in \{1, 2, \ldots, p^e - 1\}$ and

$$c_1 \equiv c \pmod{p}. \tag{2.13}$$

Then

$$A_{u'}(d, p^e) = A_u(M^i c_1 d, p^e) \quad \forall d \in \{0, 1, \ldots, p^e - 1\} \tag{2.14}$$

and for $i \in \{0, 1, 2, 3\}$.

Theorem 2.6. *Let $\varepsilon \in \{-1, 1\}$ and p be an odd prime. Consider the LSFK's $(u) = u(a_1, -1)$ and $(u') = u(a_2, -1)$ with periods $\lambda = \lambda_u(p)$ and $\lambda_1 = \lambda_{u'}(p)$ and respective discriminants D_1 and D_2. Suppose that $(D_1/p) = (D_2/p) = \varepsilon$ and*

$$\lambda = \lambda_u(p) = \lambda_{u'}(p) \not\equiv 0 \pmod{4}. \tag{2.15}$$

Then

$$h = h_u(p) = h_{u'}(p) \equiv 1 \pmod{2}. \tag{2.16}$$

Suppose further that

$$h_u(p) \neq h_u(p^2) \quad \text{and} \quad h_{u'}(p) \neq h_{u'}(p^2). \tag{2.17}$$

Then

$$\lambda_u(p) \neq \lambda_u(p^2) \quad \text{and} \quad \lambda_{u'}(p) \neq \lambda_{u'}(p^2). \tag{2.18}$$

Let $e > 1$. Then

$$h_u(p^e) = h_{u'}(p^e), \quad \lambda_u(p^e) = \lambda_{u'}(p^e) \tag{2.19}$$

and

$$E_u(p^e) = E_{u'}(p^e) = E_u(p) = 1 \quad \text{or } 2. \tag{2.20}$$

Let

$$c \equiv \sqrt{D_2 D_1^{-1}} \pmod{p}, \tag{2.21}$$

where $c \in \{1, 2, \ldots, (p-1)/2\}$. Suppose that $c_1 \in \{1, 2, \ldots, p^e - 1\}$ and

$$c_1 \equiv c \pmod{p}. \tag{2.22}$$

Then

$$A_{u'}(d, p^e) = A_u(\varepsilon_1 c_1 d, p^e) \quad \forall d \in \{0, 1, \ldots, p^e - 1\} \tag{2.23}$$

for some $\varepsilon_1 \in \{-1, 1\}$ if λ is odd, while

$$A_u(d, p^e) = A_u(c_1 d, p^e) \quad \forall d \in \{0, 1, \ldots, p^e - 1\} \tag{2.24}$$

if $\lambda \equiv 2 \pmod{4}$. Moreover, in the latter case we also have that

$$A_{u'}(d, p^e) = A_u(-c_1 d, p^e) \quad \forall d \in \{0, 1, \ldots, p^e - 1\}. \tag{2.25}$$

Theorems 2.5 and 2.6 are proved in Section 4.

Remark 2.7. In Theorems 2.5 and 2.6, we required that for the LSFK's $(u) = u(a, \varepsilon)$ and $(u') = u(a_2, \varepsilon)$, we have that $h_u(p) = h_{u'}(p)$ is odd and

$$h_u(p) \neq h_u(p^2), \quad h_{u'} \neq h_{u'}(p^2).$$

We show that these are reasonable assumptions. We first demonstrate that if the prime p is large, then indeed there exist many parameters a for which $u(a, \varepsilon)$ modulo p has a fixed odd restricted period, where we take $p \equiv 1 \pmod 4$ if $\varepsilon = 1$. Suppose $p \equiv 1 \pmod 4$. Then by Theorem 1.11 (v), there exist $\phi((p+1)/2)$ parameters a modulo p such that for the LSFK $u(a, 1)$

$$h_u(p) = \frac{p+1}{2} \equiv 1 \pmod 2.$$

Moreover, suppose that $p \equiv \delta \pmod 4$, where $\delta \in \{-1, 1\}$. Again, by Theorem 1.11 (v), there exist $\phi((p+\delta)/2)$ parameters a modulo p such that for the LSFK $u(a, -1)$,

$$h_u(p) = \frac{p+\delta}{2} \equiv 1 \pmod 2.$$

It appears that for a given LSFK $(u) = u(a, \varepsilon)$, primes p for which $h_u(p) = h_u(p^2)$ are exceedingly rare. For example, consider the case in which $(u) = u(1, 1) = \{F_n\}_{n=0}^{\infty}$, the Fibonacci sequence, and $h_u(p) = h_u(p^2)$. Such primes are called *Wall–Sun–Sun primes* or *Fibonacci–Wieferich primes*. An equivalent criterion for p to be a Wall–Sun–Sun prime is that (see PrimeGrid [10])

$$p^2 \mid F_{p-(5/p)}.$$

By McIntosh & Roettger [7], there are no Wall–Sun–Sun primes p for $p < 2 \cdot 10^{14}$. The online usergroup PrimeGrid has an ongoing project to search for Wall–Sun–Sun primes. As of the writing of this paper, it has been found by this project that there are no Wall–Sun–Sun primes for $p < 1.9 \cdot 10^{17}$ (see PrimeGrid [10]).

3 Auxiliary results

Before proving our main theorems, we will need the following results.

Theorem 3.1. *Let $w(a, b)$ be a p-regular recurrence. Let e be a fixed integer such that $1 \leq e \leq h_w(p) - 1$. Then the ratios $\frac{w_{n+e}}{w_n}$ are distinct modulo p for $0 \leq n \leq h_w(p) - 1$, where we denote the ratio $\frac{w_{n+e}}{w_n} \pmod p$ by ∞ if $w_n \equiv 0 \pmod p$.*

This is proved in Lemma 2 of Somer [17].

Lemma 3.2. *Let p be a fixed prime. Consider the LSFK $u(a, b)$ and the LSSK $v(a, b)$. Suppose further that in the case of the LSSK $v(a, b)$ that $p \nmid D = a^2 + 4b$. Then $u(a, b)$ and $v(a, b)$ are both p-regular and have common restricted period h and multiplier M modulo p. Moreover, the following hold:*

(i) $u_{h-n} \equiv -Mu_n/(-b)^n \pmod p$ *for* $0 \leq n \leq h$.

(ii) $v_{h-n} \equiv Mv_n/(-b)^n \pmod p$ *for* $0 \leq n \leq h$.

This is proved in Lemma 5 of Somer [17]. The proof is established by induction and use of the recursion relation (1.1) defining $u(a,b)$ and $v(a,b)$.

Lemma 3.3. *Let p be a fixed prime. Let $w(a,-1)$ be either the LSFK $u(a,-1)$ or the LSSK $v(a,-1)$, and let $h = h_w(p)$, where $p \nmid D$. Then*

$$w_{n+r} \not\equiv \varepsilon w_n \pmod{p} \tag{3.1}$$

for any integers n and r such that $0 \le n < n+r \le h/2$ or $h/2 \le n < n+r \le h$.

This follows from Lemma 4 of Somer [15] and Lemma 8 of Somer [18].

Proposition 3.4. *Consider the LSFK $u(a,b)$ and the LSSK $v(a,b)$ with discriminant $D = a^2 - 4b \neq 0$. Let p be a fixed prime and let $h = h_u(p)$.*

(i) If $m \mid n$, then $u_m \mid u_n$.

(ii) $u_{2n} = u_n v_n$.

(iii) $v_n^2 - D u_n^2 = 4(-b)^n$.

(iv) If h is even, then $v_{h/2} \equiv 0 \pmod{p}$.

Proof. Parts (i)–(iii) follow from the Binet formulas (1.3). We now establish part (iv). Suppose that h is even. Then h is the least positive integer n such that $u_n \equiv 0 \pmod{p}$. Hence, by part (ii),

$$u_h = u_{h/2} v_{h/2} \equiv 0 \pmod{p},$$

where $u_{h/2} \not\equiv 0 \pmod{p}$. Therefore, $v_{h/2} \equiv 0 \pmod{p}$. □

Theorem 3.5. *Let k be a fixed positive integer. Consider the LSFK $u(a,b)$ and LSSK $v(a,b)$, where $b \neq 0$, with characteristic roots α and β and discriminant $D = a^2 + 4b \neq 0$. Suppose that $u_k(a,b) \neq 0$. Then*

$$\left\{ \frac{u_{kn}(a,b)}{u_k(a,b)} \right\}_{n=0}^{\infty}$$

is a LSFK $u(a',b')$ and $\{v_{kn}(a,b)\}_{n=0}^{\infty}$ is a LSSK $v(a',b')$, where $u(a',b')$ and $v(a',b')$ have characteristic roots α^k and β^k, parameters $a' = v_k(a,b)$ and $b' = -(-b)^k$, and discriminant $D' = D u_k^2(a,b)$.

Proofs of Theorem 3.5 are given in Lucas [6, pp. 189–190] and Lehmer [5, p. 437].

Lemma 3.6. *Let p be a fixed prime and let $w(a,b)$ be a p-regular recurrence. Let $M = M_w(p^e)$, where $e \ge 1$. Then*

$$A_w(d,p^e) = A_w(M^j d, p^e) \quad \text{for } 1 \le j \le E_w(p^e) - 1.$$

This follows from the proof of Lemma 10 of Somer [14] and Lemma 13 of Somer [17].

Lemma 3.7. *Let $p > 2$ be a fixed prime. Consider all the possible discriminants $D \equiv a^2 - 4$ modulo p of recurrences $w(a,-1)$, where $0 \le a \le p-1$.*

(i) $\left(\frac{a^2-4}{p}\right) = 0$ if and only if $a \equiv \pm 2 \pmod{p}$.

(ii) There exist exactly $n = \lfloor \frac{p}{4} \rfloor$ *discriminants* $D \equiv a^2 - 4$ *modulo* p *such that* $\left(\frac{D}{p}\right) = 1$*, where either* $p = 4n + 1$ *or* $p = 4n + 3$*.*

(iii) There exist exactly $\frac{p-1}{2} - \lfloor \frac{p}{4} \rfloor = \lceil \frac{p-1}{4} \rceil$ *discriminants* $D \equiv a^2 - 4$ *modulo* p *such that* $\left(\frac{D}{p}\right) = -1$*.*

Proof. It is immediate that (i) holds. We now consider all the $(p-1)/2$ possible discriminants $D \equiv a^2 - 4 \pmod{p}$ such that $\left(\frac{D}{p}\right) = \pm 1$. First suppose that $\left(\frac{D}{p}\right) = 1$. To find all $a \in \{0, 1, \ldots, p-1\}$ such that $\left(\frac{a^2-4}{p}\right) = 1$, all one needs to do is determine all solutions to the congruence

$$a^2 - x^2 = (a + x)(a - x) \equiv 4 \pmod{p},$$

where we exclude the solutions $(a, x) \equiv (2, 0)$ or $(-2, 0) \pmod{p}$. There are $p - 3$ sets of solutions for a and x generated by

$$a + x \equiv k, \quad a - x \equiv 4/k \pmod{p}, \quad k \in \{1, 2, \ldots, p-1\} \setminus \{2, p-2\}.$$

In general, four sets of solutions lead to the same a^2 and x^2 modulo p for a fixed k:

$$\begin{aligned} &a + x \equiv k,\ a - x \equiv 4/k; && a + x \equiv 4/k,\ a - x \equiv k; \\ &a + x \equiv -k,\ a - x \equiv -4/k; && a + x \equiv -4/k,\ a - x \equiv -k \pmod{p}. \end{aligned}$$

Since $k \not\equiv 0 \pmod{p}$, we find that $k \not\equiv -k \pmod{p}$. Clearly, $4/k \not\equiv -4/k \pmod{p}$. However, $4/k \equiv k \pmod{p}$ if and only if $k \equiv \pm 2 \pmod{p}$, which has been excluded. Also, $-4/k \equiv k \pmod{p}$ if and only if $k \equiv \pm\sqrt{-4} \pmod{p}$, which can occur if and only if $p \equiv 1 \pmod{4}$. One now finds from these observations that the number of solutions of the congruence $x^2 \equiv a^2 - 4 \pmod{p}$, where $x^2 \not\equiv 0 \pmod{p}$, is equal to $n = \lfloor \frac{p}{4} \rfloor$ if p is equal to either $4n + 1$ or $4n + 3$. Thus, part (ii) holds.

It now follows that the number of discriminants $D \equiv a^2 - 4 \pmod{p}$ for which $\left(\frac{D}{p}\right) = -1$ is equal to $\frac{p-1}{2} - \lfloor \frac{p}{4} \rfloor = \lceil \frac{p-1}{4} \rceil$. □

Lemma 3.7 is essentially proved in Somer [11, p. 39].

Lemma 3.8. *Let* $\varepsilon \in \{-1, 1\}$ *and let* $p > 3$*. Let* $(u) = u(a, -1)$ *be a LSFK with discriminant* D *such that* $(D/p) = \varepsilon$*. Then there exists a LSFK* $(u') = u(a_1, -1)$ *with discriminant* D_1 *such that*

$$\left(\frac{D_1}{p}\right) = \left(\frac{D}{p}\right) = \varepsilon \tag{3.2}$$

and

$$\lambda' = \lambda_{u'}(p) = p - \varepsilon. \tag{3.3}$$

Let $h' = h_{u'}(p)$*. Then*

$$h' = \frac{p - \varepsilon}{2}. \tag{3.4}$$

Let $(v') = v(a_1, -1)$*. Then*

$$\lambda_{v'}(p) = \lambda' \quad \text{and} \quad h_{v'}(p) = h'. \tag{3.5}$$

Moreover, there exists an integer $j \in \{1, 2, \ldots, h' - 1\}$ *such that*

$$v_j(a_1, -1) \equiv a \pmod{p}. \tag{3.6}$$

Proof. By Theorem 1.11 (iv), there exists a LSFK $(u') = u(a_1, -1)$ with discriminant D_1 such that $(D_1/p) = (D/p) = \varepsilon$ and $\lambda' = \lambda_{u'}(p) = p - \varepsilon$. Since $p - \varepsilon$ is even, it then follows from Theorem 1.7 (iii) and (iv) that

$$h' = h_{u'}(p) = \frac{p - \varepsilon}{2}.$$

Let $(v') = v(a_1, -1)$. By Theorem 1.4 (ii), Theorem 1.3, and (3.2)–(3.4), we see that (v') is p-regular,

$$\lambda_{v'}(p) = \lambda' = p - \varepsilon \tag{3.7}$$

and

$$h_{v'}(p) = h' = \frac{p - \varepsilon}{2}. \tag{3.8}$$

We observe from Lemma 3.3 that

$$v_k(a_1, -1) \not\equiv \pm v_\ell(a_1, -1) \pmod{p} \tag{3.9}$$

for $1 \leq k < \ell \leq \lfloor h'/2 \rfloor$. By examining the four cases in which $\varepsilon = \pm 1$ and $p \equiv \pm 1 \pmod 4$, we see from (3.8) that

$$\lfloor h'/2 \rfloor = \lfloor p/4 \rfloor \tag{3.10}$$

if $(D/p) = \varepsilon = 1$ and

$$\lfloor h'/2 \rfloor = \lceil (p-1)/4 \rceil \tag{3.11}$$

if $(D/p) = \varepsilon = -1$, whether $p \equiv 1 \pmod 4$ or $p \equiv -1 \pmod 4$.

We note by Proposition 3.4 (iii) and Theorem 1.5 (iv) that

$$v_n^2(a_1, -1) - 4 = D_1 u_n^2(a_1, -1) \tag{3.12}$$

and

$$u_n(a_1, -1) \not\equiv 0 \pmod{p} \tag{3.13}$$

for $1 \leq n \leq \lfloor h'/2 \rfloor$. Thus,

$$\Big(\frac{v_n^2(a_1, -1) - 4}{p}\Big) = \Big(\frac{D_1}{p}\Big) = \Big(\frac{D}{p}\Big) = \varepsilon \tag{3.14}$$

for $1 \leq n \leq \lfloor h'/2 \rfloor$. We now see from (3.9)–(3.14) and Lemma 3.7 that the $\lfloor h'/2 \rfloor$ expressions

$$v_n^2(a_1, -1) - 4, \tag{3.15}$$

where $1 \leq n \leq \lfloor h'/2 \rfloor$ exhaust all the possible values of $c^2 - 4$ modulo p, given that $\varepsilon = \Big(\frac{c^2-4}{p}\Big)$. Noting that

$$\Big(\frac{D}{p}\Big) = \Big(\frac{a^2 - 4}{p}\Big) = \varepsilon,$$

we obtain that there exists an integer i, $1 \leq i \leq \lfloor h'/2 \rfloor$, such that

$$v_i(a_1, -1) \equiv \varepsilon_1 a \pmod{p} \tag{3.16}$$

for some $\varepsilon_1 \in \{-1, 1\}$. Since $\lambda_{v'}(p) = p - \varepsilon$ is even, we see from Theorem 1.7 (iii) and (iv) that $M_{v'}(p) \equiv -1 \pmod p$. Therefore, by Lemma 3.2 (ii),

$$v_{h'-i}(a_1, -1) \equiv -v_i(a_1, -1) \equiv -\varepsilon_1 a \pmod{p}. \tag{3.17}$$

Thus, by (3.14) and (3.15), there exists an integer j, $1 \leq j \leq h' - 1$, such that

$$v_j(a_1, -1) \equiv a \pmod{p}. \qquad \square$$

Theorem 3.9. *Let p be a fixed prime. Consider the recurrences $u(a,b)$ and $v(a,b)$. Let $h = h_u(p)$. Then $v(a,b)$ is p-equivalent to $u(a,b)$ if and only if h is even.*

Proof. By Proposition 3.4 (iv), $v_{h/2} \equiv 0 \pmod{p}$ when h is even. Then

$$v_{h/2} \equiv v_{h/2+1} \cdot u_0 \equiv v_{h/2+1} \cdot 0 \equiv 0 \pmod{p} \tag{3.18}$$

and

$$v_{h/2+1} \equiv v_{h/2+1} \cdot u_1 \equiv v_{h/2+1} \cdot 1 \equiv v_{h/2+1} \pmod{p}. \tag{3.19}$$

Since $v(a,b)$ is nontrivial modulo p, it now follows by the recursion relation (1.1) defining both $u(a,b)$ and $v(a,b)$ that $v(a,b)$ is p-equivalent to $u(a,b)$ when h is even. It is proved in Lemma 6 of Somer [17] that $v(a,b)$ is not p-equivalent to $u(a,b)$ when h is odd. $\square$

Theorem 3.10. *Let $e > 1$, $\varepsilon \in \{-1, 1\}$, and p be an odd prime. Consider the p-regular recurrence $w(a,\varepsilon)$. Suppose that $h_w(p^2) \neq h_w(p)$. Then the following hold:*

(i) $\lambda_w(p^2) \neq \lambda_w(p)$.

(ii) $h_w(p^e) = p^{e-1} h_w(p)$.

(iii) $\lambda_w(p^e) = p^{e-1} \lambda_w(p)$.

(iv) $E_w(p^e) = E_w(p)$.

Proof. Part (i) follows from the discussion in Carlip & Somer [1, p. 697]. Part (ii) is proved in Carmichael [2, p. 42] and part (iii) is proved in Ward [21, pp. 619–620]. Part (iv) follows from parts (ii) and (iii). $\square$

Theorem 3.11. *Let $e > 1$, $\varepsilon \in \{-1, 1\}$, and p be an odd prime. Consider the p-regular recurrence $w(a,\varepsilon)$ with discriminant D. Suppose that $p \nmid D$ and $h_w(p^2) \neq h_w(p)$. Suppose further that $w(a,\varepsilon)$ is not p-equivalent to $v(a,\varepsilon)$ modulo p. Then*

$$A_w(d, p^e) = A_w(d, p) \quad \forall d \in \{0, 1, \ldots, p^e - 1\}. \tag{3.20}$$

This follows from Theorem 3.10 (i) of this paper and from Theorems 6.5, 6.8, and 6.9 of Carlip & Somer [1].

Remark 3.12. Theorem 3.11 was proved in Carroll et al. [4] for the case in which $w(a,\varepsilon) = u(a,1)$ and $h_u(p) \equiv 1 \pmod{2}$.

4 Proofs of the main theorems

Proof of Theorem 2.1. Let $\lambda = \lambda_u(p)$ and $\lambda_1 = \lambda_{u'}(p)$. By hypothesis, $(D_1/p) = (D_2/p) = \varepsilon_1$, where $\varepsilon_1 \in \{-1, 1\}$, and $\lambda = \lambda_1$. First suppose that $p = 3$. We notice that for the LSFK $u(a_1, -1)$ modulo 3, we have $D \equiv 0 \pmod 3$ if $a_1 \equiv \pm 1 \pmod 3$, while $(D/3) = 1$ if $a_1 \equiv 0 \pmod 3$. Thus, there is only one LSFK $u(a_1, -1)$ modulo 3 for which

$$\Big(\frac{D}{3}\Big) = \Big(\frac{a_1^2 - 4}{3}\Big) = \pm 1,$$

and the theorem holds trivially in this case.

We now assume that $p > 3$. By Lemma 3.8, there exists a LSFK $(u'') = u(a_3, -1)$ with discriminant D_3 such that

$$\Big(\frac{D_3}{p}\Big) = \Big(\frac{D_1}{p}\Big) = \Big(\frac{D_2}{p}\Big) = \varepsilon_1, \tag{4.1}$$

$$\lambda_2 = \lambda_{u''}(p) = p - \varepsilon_1, \tag{4.2}$$

and

$$h_2 = h_{u''}(p) = \frac{p - \varepsilon_1}{2}. \tag{4.3}$$

By Theorem 1.7 (viii), $\lambda \mid \lambda_2$. Let

$$r = \frac{\lambda_2}{\lambda}. \tag{4.4}$$

Let $(v'') = v(a_3, -1)$. Then by Lemma 3.8,

$$\lambda_{v''}(p) = \lambda_2 \quad \text{and} \quad h_{v''}(p) = h_2, \tag{4.5}$$

and there exist unequal integers k, ℓ such that $1 \le k, \ell \le h_2 - 1$ and

$$v_k(a_3, -1) \equiv a_1, \quad v_\ell(a_3, -1) \equiv a_2 \pmod p. \tag{4.6}$$

Then by Theorem 3.5, we see that

$$u_n(a_1, -1) \equiv u_n(v_k(a_3, -1), -1) = \frac{u_{kn}(a_3, -1)}{u_k(a_3, -1)} \pmod p, \tag{4.7}$$

$$u_n(a_2, -1) \equiv u_n(v_\ell(a_3, -1), -1) = \frac{u_{\ell n}(a_3, -1)}{u_\ell(a_3, -1)} \pmod p \tag{4.8}$$

for all $n \ge 0$. We note that by Theorem 1.5 (iv), $u_k(a_3, -1)u_\ell(a_3, -1) \not\equiv 0 \pmod p$. Since $u(a_1, -1)$ and $u(a_2, -1)$ both have periods modulo p equal to λ and since $u(a_3, -1)$ has a period modulo p equal to λ_2, it follows from (4.4) and from the last equalities in (4.7) and (4.8) that

$$\gcd(k, \lambda_2) = \gcd(\ell, \lambda_2) = r = \frac{\lambda_2}{\lambda_1}. \tag{4.9}$$

It now follows from (4.9) that the sets

$$\{kn\}_{n=1}^{\lambda} \quad \text{and} \quad \{\ell n\}_{n=1}^{\lambda} \tag{4.10}$$

contain the same sets of residues modulo λ_2.

It thus follows that

$$\{u_{kn}(a_3,-1)\}_{n=1}^{\lambda} \quad \text{and} \quad \{u_{\ell n}(a_3,-1)\}_{n=1}^{\lambda} \tag{4.11}$$

contain the same sets of residues modulo p. Let $u_k'' = u_k(a_3,-1)$, $u_\ell'' = u_\ell(a_3,-1)$, $v_k'' = v_k(a_3,-1)$, and $v_\ell'' = v_\ell(a_3,-1)$, Noting that u_k'' and u_ℓ'' are both invertible modulo p, it follows from (4.7), (4.8), (4.11), and the fact that both $(u) = u(a_1,-1)$ and $(u') = u(a_2,-1)$ have periods modulo p equal to λ that

$$A_{u'}(d) = A_u(u_\ell''(u_k'')^{-1}d) \quad \forall d \in \{0,1,\dots,p-1\}. \tag{4.12}$$

By Proposition 3.4 (iii),

$$(v_k'')^2 - D_3(u_k'')^2 = 4 \tag{4.13}$$

and

$$(v_\ell'')^2 - D_3(u_\ell'')^2 = 4. \tag{4.14}$$

Noting that $p \nmid D_3u_k''u_\ell''$, we see by (4.6), (4.13), and (4.14) that

$$\frac{D_3(u_\ell'')^2}{D_3(u_k'')^2} = \frac{(v_\ell'')^2-4}{(v_k'')^2-4} \equiv \frac{a_2^2-4}{a_1^2-4} \equiv \frac{D_2}{D_1} \equiv \frac{(u_\ell'')^2}{(u_k'')^2} \pmod{p}. \tag{4.15}$$

Thus, by (4.15),

$$u_\ell''(u_k'')^{-1} \equiv \varepsilon\sqrt{D_2D_1^{-1}} \pmod{p} \tag{4.16}$$

for some $\varepsilon \in \{-1,1\}$. Hence, by (4.12) and (4.16), we see that if λ is odd, then

$$A_{u'}(d) = A_u(\varepsilon\sqrt{D_2D_1^{-1}}d) \quad \forall d \in \{0,1,\dots,p-1\}. \tag{4.17}$$

Now suppose that λ is even. Then by Theorem 1.7 (iii) and (iv),

$$M_u(p) \equiv M_{u'}(p) \equiv -1 \pmod{p}. \tag{4.18}$$

It now follows from Lemma 3.6 and (4.18) that

$$A_{u'}(d) = A_u(\sqrt{D_2D_1^{-1}}d) = A_u(\sqrt{-D_2D_1^{-1}}d) \quad \forall d \in \{0,1,\dots,p-1\} \tag{4.19}$$

when λ is even. The proof is now complete. □

Proof of Theorem 2.2. Let $\lambda = \lambda_v(p)$ and $\lambda_1 = \lambda_{v'}(p)$. By hypothesis, $(D_1/p) = (D_2/p) = \varepsilon_1$, where $\varepsilon_1 \in \{-1,1\}$, and $\lambda = \lambda_1$. First suppose that $p = 3$. As in the proof of Theorem 2.1, there is a LSSK $v(a_1,-1)$ with discriminant D such that $(D/3) = \pm 1$ if and only if $a_1 \equiv 0 \pmod 3$. Thus, the theorem holds trivially in this case.

We now assume that $p > 3$. By Lemma 3.8, there exists a LSSK $(v'') = v(a_3,-1)$ with discriminant D_3 such that

$$\Big(\frac{D_3}{p}\Big) = \Big(\frac{D_1}{p}\Big) = \Big(\frac{D_2}{p}\Big) = \varepsilon_1, \tag{4.20}$$

$$\lambda_2 = \lambda_{u''}(p) = p - \varepsilon_1, \tag{4.21}$$

and

$$h_2 = h_{u''}(p) = \frac{p - \varepsilon_1}{2}. \tag{4.22}$$

We note that by Theorem 1.4 (ii), $v(a_1, -1)$, $v(a_2, -1)$, and $v(a_3, -1)$ are all p-regular. Moreover, by Theorem 1.7 (viii), $\lambda \mid \lambda_2$. Let

$$r = \frac{\lambda_2}{\lambda}. \tag{4.23}$$

By Lemma 3.8, there exist unequal integers k, ℓ such that $1 \leq k, \ell \leq h_2 - 1$ and

$$v_k(a_3, -1) \equiv a_1, \quad v_\ell(a_3, -1) \equiv a_2 \pmod{p}. \tag{4.24}$$

Hence, by (4.24) and Theorem 3.5, we see that

$$v_n(a_1, -1) \equiv v_n(v_k(a_3, -1), -1) = v_{kn}(a_3, -1) \pmod{p} \tag{4.25}$$

and

$$v_n(a_2, -1) \equiv v_n(v_\ell(a_3, -1), -1) = v_{\ell n}(a_3, -1) \pmod{p} \tag{4.26}$$

for all $n \geq 0$. Since $v(a_1, -1)$ and $v(a_2, -1)$ both have periods modulo p equal to λ and since $v(a_3, -1)$ has a period modulo p equal to λ_2, it follows from the last equalities in (4.25) and (4.26) and from (4.23) that

$$\gcd(k, \lambda_2) = \gcd(\ell, \lambda_2) = r = \frac{\lambda_2}{\lambda}. \tag{4.27}$$

We see by (4.27) that the sets

$$\{kn\}_{n=1}^{\lambda} \quad \text{and} \quad \{\ell n\}_{n=1}^{\lambda} \tag{4.28}$$

contain the same sets of residues modulo λ_2. Therefore, it follows that the sets

$$\{v_{kn}(a_3, -1)\}_{n=1}^{\lambda} \quad \text{and} \quad \{v_{\ell n}(a_3, -1)\}_{n=1}^{\lambda} \tag{4.29}$$

contain the same sets of residues modulo p. It now follows from (4.25), (4.26), (4.29), and the fact that both $(v) = v(a_1, -1)$ and $(v') = v(a_2, -1)$ have periods modulo p equal to λ that

$$A_{v'}(d) = A_v(d) \quad \forall d \in \{0, 1, \ldots, p-1\}. \tag{4.30}$$

Now suppose that λ is even. Then by Theorem 1.7 (iii) and (iv),

$$M_v(p) \equiv M_{v'}(p) \equiv -1 \pmod{p}. \tag{4.31}$$

It now follows from Lemma 3.6, (4.30), and (4.31) that when λ is even, we also have that

$$A_{v'}(d) = A_v(-d) \quad \forall d \in \{0, 1, \ldots, p-1\}, \tag{4.32}$$

as desired. □

Proof of Theorem 2.5. We note that (2.6) and (2.7) follow from the hypothesis given in (2.5) and from Theorem 1.6 (iv). Moreover, (2.9)–(2.11) follow from the hypothesis given in (2.8), Theorem 1.6 (iv), and Theorem 3.10. Let $d \in \{0, 1, \ldots, p^e - 1\}$. Since $h = h_u(p)$ is odd, we see by Theorem 1.12 that

$$A_{u'}(d, p) = A_u(cd, p), \tag{4.33}$$

where $c \equiv \sqrt{D_2 D_1^{-1}} \pmod{p}$ and $c \in \{0, 1, \dots, (p-1)/2\}$. It now follows from the fact that h is odd and from Theorem 3.9 that $(u) = u(a_1, 1)$ is not p-equivalent to $v(a_1, 1)$ and $(u') = u(a_2, 1)$ is not p-equivalent to $v(a_2, 1)$. It then follows from Theorem 3.11 that

$$A_{u'}(d, p^e) = A_{u'}(d, p) \tag{4.34}$$

and

$$A_u(c_1 d, p^e) = A_u(cd, p), \tag{4.35}$$

where $c_1 \in \{0, 1, \dots, p^e - 1\}$ and $c_1 \equiv c \pmod{p}$. Thus, by (4.33)–(4.35),

$$A_{u'}(d, p^e) = A_u(c_1 d, p^e). \tag{4.36}$$

Let $M = M_u(p^e)$. We now see from Theorem 1.6 (iv), Lemma 3.6, and (2.11) that

$$\operatorname{ord}_{p^e} M = 4 \tag{4.37}$$

and

$$A_u(M^i c_1 d.p^e) = A_u(c_1 d, p^e) \tag{4.38}$$

for $i \in \{0, 1, 2, 3\}$, where $\operatorname{ord}_{p^e} M$ denotes the multiplicative order of M modulo p^e. It now follows from (4.36)–(4.38) that (2.14) holds, and the theorem follows. □

Proof of Theorem 2.6. We observe that (2.16) follows from the hypothesis given in (2.15) and from Theorem 1.7 (ii) and (iii). Furthermore, (2.18)–(2.20) follow from the hypothesis given in (2.17) and from Theorem 3.10. Let $d \in \{0, 1, \dots, p^e - 1\}$. Now we see by Theorem 2.1 that

$$A_{u'}(d, p) = A_u(\varepsilon_1 cd, p) \quad \text{if} \quad \lambda \equiv 1 \pmod{2} \tag{4.39}$$

for some $\varepsilon_1 \in \{1, -1\}$ and

$$A_{u'}(d, p) = A_u(cd, p) \quad \text{if} \quad \lambda \equiv 2 \pmod{4}, \tag{4.40}$$

where $c \in \{0, 1, \dots, (p-1)/2\}$ and $c \equiv \sqrt{D_2 D_1^{-1}} \pmod{p}$. Since $h = h_u(p)$ is odd by (2.16), we find by Theorem 3.9 that $u(a_1, -1)$ is not p-equivalent to $v(a_1, -1)$ and $(u') = u(a_2, -1)$ is not p-equivalent to $v(a_2, -1)$. It now follows from Theorem 3.11 that

$$A_{u'}(d, p^e) = A_{u'}(d, p), \tag{4.41}$$

$$A_u(\varepsilon_1 c_1 d, p^e) = A_u(\varepsilon_1 cd, p), \tag{4.42}$$

and

$$A_u(c_1 d, p^e) = A_u(cd, p), \tag{4.43}$$

where $c_1 \in \{0, 1, \dots, p^e - 1\}$ and $c_1 \equiv c \pmod{p}$. Therefore, by (4.39)–(4.43),

$$A_{u'}(d, p^e) = A_u(\varepsilon_1 c_1 d, p^e) \quad \text{if} \quad \lambda \equiv 1 \pmod{2} \tag{4.44}$$

and

$$A_{u'}(d, p^e) = A_u(c_1 d, p^e) \quad \text{if} \quad \lambda \equiv 2 \pmod{4}. \tag{4.45}$$

If $\lambda \equiv 2 \pmod 4$, let $M = M_u(p^e)$. Then by Theorem 1.7 (iii) and Lemma 3.6,

$$M \equiv -1 \pmod{p^e} \tag{4.46}$$

and

$$A_u(-c_1 d, p^e) = A_u(c_1 d, p^e) \quad \text{if} \quad \lambda \equiv 2 \pmod 4. \tag{4.47}$$

It now follows from (4.45) and (4.47) that (2.25) holds, and the theorem follows. □

Acknowledgements

This paper was supported by the Czech Academy of Sciences (RVO 67985840) and grant no. 24-10586S of GAČR.

References

[1] Carlip, W., & Somer, L. (1999). Bounds for frequencies of residues of regular second-order recurrences modulo p^r. *Number Theory in Progress*, Vol. 2, (Zakopane-Kościelisko, 1997), de Gruyter, Berlin, 691–719.

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

[3] Carmichael, R. D. (1920). On sequences of integers defined by recurrence relations. *The Quarterly Journal of Pure and Applied Mathematics*, 48, 343–372.

[4] Carroll, D., Jacobson, E., & Somer, L. (1994). Distribution of two-term recurrence sequences mod p^e. *The Fibonacci Quarterly*, 32, 260–265.

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

[6] Lucas, E. (1878). Théorie des fonctions numériques simplement périodiques. *American Journal of Mathematics*, 1, 184–240, 289–321.

[7] McIntosh, R. J., & Roettger, E. L. (2007). A search for Fibonacci–Wieferich and Wolstenholme primes. *Mathematics of Computation*, 76, 2087–2094.

[8] Müller, S., (1999). On the rank of appearance of Lucas sequences. In Howard, F. T. (Ed.), *Applications of Fibonacci Numbers*, Vol. 8 (pp. 259–275). Kluwer Academic Publishers, Dordrecht.

[9] Niederreiter, H., Schinzel, A., & Somer, L. (1991). Maximal frequencies of elements in second-order linear recurring sequences over a finite field. *Elemente der Mathematik*, 46, 139–143.

[10] PrimeGrid. *Welcome to PrimeGrid PRPNET: Wall–Sun–Sun Prime Search*. Available online at: `http://www.primegrid.com/forum_thread.php?id=9436`.

[11] Somer, L. (1977). Fibonacci-like groups and periods of Fibonacci-like sequences. *The Fibonacci Quarterly*, 15, 35–41.

[12] Somer, L. (1980). The divisibility properties of primary Lucas recurrences with respect to primes. *The Fibonacci Quarterly*, 18, 316–334.

[13] Somer, L. (1982). Possible periods of primary Fibonacci-like sequences with respect to a fixed odd prime. *The Fibonacci Quarterly*, 20, 311–333.

[14] Somer, L. (1990). Distribution of residues of certain second-order linear recurrences modulo p. In Bergum, G. E., Philippou, A. N., & Horadam, A. F. (Eds.), *Applications of Fibonacci Numbers, Vol. 3* (pp. 311–324). Kluwer Academic Publishers, Dordrecht.

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

[16] Somer, L. (1993). Periodicity properties of kth order linear recurrences with irreducible characteristic polynomial over a finite field. In Mullen, G. L., & Shiue, P. J.-S. (Eds.), *Finite Fields, Coding Theory and Advances in Communications and Computing* (pp. 195–207). Marcel Dekker Inc., New York.

[17] Somer, L. (1993). Upper bounds for frequencies of elements in second-order recurrences over a finite field. In Bergum, G. E., Philippou, A. N., & Horadam, A. F. (Eds.), *Applications of Fibonacci Numbers, Vol. 5* (pp. 527–546). St. Andrews, 1992, Kluwer Academic Publishers, Dordrecht.

[18] Somer, L. (1996). Distribution of residues of certain second-order linear recurrences modulo p – III. In Bergum, G. E., Philippou, A. N., & Horadam, A. F. (Eds.), *Applications of Fibonacci Numbers, Vol. 6* (pp. 451–471). Kluwer Academic Publishers, Dordrecht.

[19] Somer, L., & Křížek, M. (2015). Identically distributed second-order linear recurrences modulo p. *The Fibonacci Quarterly*, 53, 290–312.

[20] Somer, L., & Křížek, M. (2016). Identically distributed second-order linear recurrences modulo p, II. *The Fibonacci Quarterly*, 54, 217–234.

[21] Ward, M. (1933). The arithmetical theory of linear recurring series. *Transactions of the American Mathematical Society*, 35, 600–628.