IDENTICALLY DISTRIBUTED SECOND-ORDER LINEAR RECURRENCES MODULO p

LAWRENCE SOMER AND MICHAL KŘÍŽEK

Abstract. Let $w(a,-1)$ denote the second-order linear recurrence satisfying the recursion relation

$$w_{n+2} = aw_{n+1} - w_n,$$

where a and the initial terms w_0, w_1 are all integers. Let p be an odd prime. The *restricted period* $h_w(p)$ of $w(a,-1)$ modulo p is the least positive integer r such that $w_{n+r} \equiv Mw_n \pmod p$ for all $n \geq 0$ and some nonzero residue M modulo p. We distinguish two recurrences, the Lucas sequence of the first kind $u(a,-1)$ and the Lucas sequence of the second kind $v(a,-1)$, satisfying the above recursion relation and having initial terms $u_0 = 0$, $u_1 = 1$ and $v_0 = 2$, $v_1 = a$, respectively. We show that if $u(a_1,-1)$ and $u(a_2,-1)$ both have the same restricted period modulo p, or equivalently, the same period modulo p, then $u(a_1,-1)$ and $u(a_2,-1)$ have the same distribution of residues modulo p. Similar results are obtained for Lucas sequences of the second kind.

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, p will denote an odd prime unless specified otherwise, and ε will specify an element from $\{-1,1\}$. It was shown in [7, pp. 344–345] that $w(a,b)$ is purely periodic modulo p if $p \nmid b$. From here on, we assume that $p \nmid b$.

The *period* of $w(a,b)$ modulo p, denoted by $\lambda_w(p)$, is the least positive integer m such that $w_{n+m} \equiv w_n \pmod p$ for all $n \geq 0$. The *restricted period* of $w(a,b)$ modulo p, denoted by $h_w(p)$, is the least positive integer r such that $w_{n+r} \equiv Mw_n \pmod p$ for all $n \geq 0$ and some fixed nonzero residue M modulo p. Here $M = M_w(p)$ is called the *multiplier* of $w(a,b)$ modulo p. Since the LSFK $u(a,b)$ is purely periodic modulo p and has initial terms $u_0 = 0$ and $u_1 = 1$, it is easily seen that $h_u(p)$ is the least positive integer r such that $u_r \equiv 0 \pmod p$. It is proved in [7, pp. 354–355] that $h_w(p) \mid \lambda_w(p)$. Let $E_w(p) = \frac{\lambda_w(p)}{h_w(p)}$. Then by [7, pp. 354–355] $E_w(p)$ is the multiplicative order of the multiplier M modulo p.

Our main result of this paper will be 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, then $u(a_1,-1)$ and $u'(a_2,-1)$ have the same distribution of residues modulo p. We will prove a similar result for the LSSK's $v(a_1,-1)$ and $v'(a_2,-1)$.

We now define what it means for the recurrences $w(a_1,b)$ and $w'(a_2,b)$ with the same parameter b to have the same distribution of residues modulo p. Let $w(a,b)$ be a recurrence and p be a fixed prime. Given a residue d modulo p, we let $A_w(d)$ denote the number of times that d appears in a full period of (w) modulo p. We have the following theorem regarding upper bounds for $A_w(d)$.

Theorem 1.1. *Let p be a fixed prime and consider the recurrence $w(a,b)$. Let d be a fixed residue modulo p such that $0 \le d \le p-1$.*

(i) *$A_w(d) \le \min(2 \cdot \mathrm{ord}_p b, p)$, where $\mathrm{ord}_p b$ denotes the multiplicative order of b modulo p.*
(ii) *If $b = 1$ then $A_w(d) \le 2$.*
(iii) *If $b = -1$ then $A_w \le 4$.*

Proof. Part (i) was proved in Theorem 3 of [11]. Parts (ii) and (iii) follow from part (i). $\square$

We let
$$N_w(p) = \#\{d \mid A_w(d) > 0\}. \tag{1.4}$$
We define the set $S_w(p)$ by
$$S_w(p) = \{i \mid A_w(d) = i \text{ for some } d \text{ such that } 0 \le d \le p-1\}. \tag{1.5}$$
Further, if i is a nonnegative integer, we define $B_w(i)$ by
$$B_w(i) = \#\{d \mid 0 \le d \le p-1 \text{ and } A_w(d) = i\}. \tag{1.6}$$
We observe by Theorem 1.1 that
$$B_w(i) = 0 \quad \text{if } i > \min(2 \cdot \mathrm{ord}_p b, p). \tag{1.7}$$
We say that the linear recurrences $w(a_1,b)$ and $w'(a_2,b)$ have the *same distribution of residues modulo p* if $N_w(p) = N_{w'}(p)$, $S_w(p) = S_{w'}(p)$, and $B_w(i) = B_{w'}(i)$ for all $i \ge 0$. Recurrences that have the same distribution of residues modulo p are also said to be *identically distributed modulo p*.

To show that two recurrences $w(a_1,b)$ and $w'(a_2,b)$ are identically distributed modulo p, it suffices by (1.7) to show that $B_w(i) = B_{w'}(i)$ for all $i \in \{0,\ldots,\ell\}$, where $\ell = \min(2 \cdot \mathrm{ord}_p b, p)$. This follows, since
$$N_w(p) = \sum_{i=1}^{\ell} B_w(i) \tag{1.8}$$
and
$$S_w(p) = \{i \mid B_w(i) > 0\}. \tag{1.9}$$
It is also of interest that
$$\lambda_w(p) = \sum_{i=0}^{\ell} i B_w(i). \tag{1.10}$$

Example 1.2. Let $p = 17$. We show that the LSFK's $u(2,-1)$ and $u'(14,-1)$ are identically distributed modulo 17. The first 18 terms of $u(2,-1)$ and $u'(14,-1)$ are

$$\{0,\ 1,\ 2,\ 5,\ 12,\ 12,\ 2,\ 16,\ 0,\ 16,\ 15,\ 12,\ 5,\ 5,\ 15,\ 1,\ 0,\ 1\}$$

and

$$\{0,\ 1,\ 14,\ 10,\ 1,\ 7,\ 14,\ 16,\ 0,\ 16,\ 3,\ 7,\ 16,\ 10,\ 3,\ 1,\ 0,\ 1\},$$

respectively. Thus,

$$\begin{aligned} &h_u(17) = h_{u'}(17) = 8,\ \lambda_u(17) = \lambda_{u'}(17) = 16, \\ &E_u(17) = E_{u'}(17) = 2,\ \text{and } M_u(17) \equiv M_{u'}(17) = -1 \pmod{17}. \end{aligned} \tag{1.11}$$

We observe that

$$\begin{aligned} &A_u(d) = 0\ \text{ for } d \in \{3,\ 4,\ 6,\ 7,\ 8,\ 9,\ 10,\ 11,\ 13,\ 14\}, \\ &A_u(d) = 2\ \text{ for } d \in \{0,\ 1,\ 7,\ 10,\ 14\}, \\ &A_u(d) = 3\ \text{ for } d \in \{5,\ 12\}, \end{aligned}$$

while

$$\begin{aligned} &A_{u'}(d) = 0\ \text{ for } d \in \{2,\ 4,\ 5,\ 6,\ 8,\ 9,\ 11,\ 12,\ 13,\ 15\}, \\ &A_{u'}(d) = 2\ \text{ for } d \in \{0,\ 3,\ 7,\ 10,\ 14\}, \\ &A_{u'}(d) = 3\ \text{ for } d \in \{1,\ 16\}. \end{aligned}$$

Hence,

$$N_u(17) = N_{u'}(17) = 7 \quad \text{and} \quad S_u(17) = S_{u'}(17) = \{0,\ 2,\ 3\}. \tag{1.12}$$

Moreover,

$$\begin{aligned} &B_u(0) = B_{u'}(0) = 10,\ B_u(2) = B_{u'}(2) = 5,\ B_u(3) = B_{u'}(3) = 2, \\ &\text{and } B_u(i) = B_{u'}(i) = 0 \quad \text{for i} \geq 0 \text{ and i} \notin \{0,\ 2,\ 3\}. \end{aligned} \tag{1.13}$$

Therefore, $u(2, -1)$ and $u'(14, -1)$ are identically distributed modulo 17.

2. The Main Theorems

Our principal results of this paper are Theorems 2.1 and 2.2.

Theorem 2.1. *Let p be a fixed prime. Let $u(a_1, -1)$ and $u'(a_2, -1)$ be two LSFK's with discriminants $D_1 = a_1^2 + 4$ and $D_2 = a_2^2 + 4$, respectively, such that $p \nmid D_1D_2$. Suppose that $h_u(p) = h_{u'}(p)$ and $(D_1/p) = (D_2/p)$, where (D_i/p) denotes the Legendre symbol. This occurs if and only if $\lambda_u(p) = \lambda_{u'}(p)$. Then $u(a_1, -1)$ and $u'(a_2, -1)$ are identically distributed modulo p.*

Theorem 2.2. *Let p be a fixed prime. Let $v(a_1, -1)$ and $v'(a_2, -1)$ be two LSSK's with discriminants $D_1 = a_1^2 + 4$ and $D_2 = a_2^2 + 4$, respectively, such that $p \nmid D_1D_2$. Suppose that $(D_1/p) = (D_2/p)$ and that $h_v(p) = h_{v'}(p)$. This occurs if and only if $\lambda_v(p) = \lambda_{v'}(p)$. Then $v(a_1, -1)$ and $v'(a_2, -1)$ are identically distributed modulo p.*

3. Preliminaries

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

Definition 3.1. *Let p be a fixed prime. The recurrence $w(a, b)$ is said to be p-regular if*

$$\begin{vmatrix} w_0 & w_1 \\ w_1 & w_2 \end{vmatrix} = w_0w_2 - w_1^2 \not\equiv 0 \pmod{p}. \tag{3.1}$$

Otherwise, the recurrence $w(a, b)$ is called p-irregular.

Theorem 3.2. *Suppose that the recurrences $w(a, b)$ and $w'(a, b)$ are both p-regular. Then*

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

This is proved in [5, p. 695].

Consider the LSFK $u(a,b)$ when $h_u(p)$ is even and $(b/p) = 1$. We specify the recurrence $t(a,b)$ satisfying the recursion relation (1.1) and having initial terms $t_0 = 1$, $t_1 = b'$, where $(b')^2 \equiv b \pmod p$ and $0 \le b' \le (p-1)/2$. The following theorem gives results concerning the p-regularity of the distinguished recurrences $u(a,b)$, $v(a,b)$, and $t(a,b)$.

Theorem 3.3. *Let p be a fixed prime. Consider the LSFK $u(a,b)$ and the LSSK $v(a,b)$ with discriminant $D = a^2 - 4b$. Consider also the recurrence $t(a,b)$ if it is defined modulo p. Then*

(i) *$u(a,b)$ is p-regular,*
(ii) *$v(a,b)$ is p-regular if $p \nmid D$,*
(iii) *$t(a,b)$ is p-regular whenever it is defined modulo p.*

Proof. (i) We note that

$$u_0u_2 - u_1^2 = 0 \cdot a - 1^2 = -1 \not\equiv 0 \pmod p.$$

Thus, $u(a,b)$ is p-regular by (3.1).

(ii) We observe that

$$v_0v_2 - v_1^2 = 2(a^2 - 2b) - a^2 = a^2 - 4b = D.$$

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

Part (iii) is proven in [22, p. 7]. □

Theorem 3.4. *Let p be a fixed prime. Suppose that $w(a,b)$ is a p-irregular recurrence.*

(i) *If $w_0 \equiv 0 \pmod p$, then $w_n \equiv 0 \pmod p$ for $n \ge 0$.*
(ii) *If $w_0 \not\equiv 0 \pmod p$, then*

$$w_n \equiv \left(\frac{w_1}{w_0}\right)^n w_0 \pmod p \quad \text{for } n \ge 0.$$

(iii) *$h_w(p) = 1$.*

Proof. Parts (i) and (ii) are proved in [5, p. 695]. Part (iii) follows from parts (i) and (ii). □

Definition 3.5. *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*

$$w'_n \equiv cw_{n+r} \pmod p \quad \text{for all } n \ge 0. \tag{3.2}$$

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.

Theorem 3.6. *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 $n \ge 0$, where c is a fixed nonzero residue modulo p and r is a fixed integer. Then*

(i) *$w(a,b)$ and $w'(a,b)$ are either both p-regular or both p-irregular,*
(ii) *$w(a,b)$ and $w'(a,b)$ are identically distributed modulo p.*

Proof. Part (i) is proven in [5, p. 694]. Part (ii) follows from the fact that

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

for $d \in \{0, \dots, p-1\}$. □

Theorem 3.7. *Let $w(a,b)$ be a p-regular recurrence. Let e be a fixed integer such that $1 \le e \le h_w(p)-1$. Then the ratios $\frac{w_{n+e}}{w_n}$ are distinct modulo p for $0 \le n \le h_w(p)-1$, 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 [19].

Lemma 3.8. *Let p be a fixed prime. Consider the LSFK $u(a,b)$ and the LSSK $v(a,b)$. Consider also the recurrence $t(a,b)$ if it is defined. Suppose further that in the case of the LSSK $v(a,b)$ that $p \nmid D = a^2+4b$. Then $u(a,b)$, $v(a,b)$, and $t(a,b)$ are all 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* $0 \le n \le h$.
(ii) $v_{h-n} \equiv Mv_n/b^n \pmod p$ *for* $0 \le n \le h$.
(iii) $t_{h+1-n} \equiv Mb' t_n/b^n \pmod p$ *for* $0 \le n \le h+1$, *where* $(b')^2 \equiv b \pmod p$ *and* $0 \le b' \le (p-1)/2$.

This is proved in Lemma 5 of [19]. The proof is established by induction and use of the recursion relation (1.1) defining $u(a,b)$, $v(a,b)$, and $t(a,b)$.

Lemma 3.9. *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 $p \nmid D$. If h is even, then*

$$w_{n+2r} \not\equiv \varepsilon w_n \pmod p \tag{3.3}$$

for any integers n and r such that $0 \le n < n+2r \le h/2$ or $h/2 \le n < n+2r \le h$. Moreover, if h is odd, then

$$w_{n+2r} \not\equiv \varepsilon w_n \pmod p \tag{3.4}$$

for any integers n and r such that $0 \le n < n+2r \le h-1$.

Proof. Suppose that h is even and

$$w_{n+2r} \equiv \varepsilon w_n \pmod p \tag{3.5}$$

for some integers n and r such that $0 \le n < n+2r \le h/2$ or $h/2 \le n < n+2r \le h$. Then $w_n \not\equiv 0 \pmod p$, since w_{n+2r} can then be congruent to 0 modulo p only if $2r \equiv 0 \pmod h$ by the definition of h. It then follows from Lemma 3.8 (i) and (ii) that

$$\frac{w_{n+2r}}{w_n}\frac{w_{h-n}}{w_{h-n-2r}} \equiv (-1)^{2r} \equiv 1 \pmod p,$$

which implies that

$$\frac{w_{n+2r}}{w_n} \equiv \frac{w_{h-n}}{w_{h-n-2r}} \equiv \varepsilon \pmod p, \tag{3.6}$$

where $n \ne h-n-2r$, $0 \le n < h$, $0 \le h-n-2r < h$, and $2 \le 2r \le h/2$. However, (3.6) contradicts Theorem 3.7. Thus, (3.3) holds.

Now suppose that h is odd and

$$w_{n+2r} \equiv \varepsilon w_n \pmod p \tag{3.7}$$

for some n and r such that $0 \le n < n+2r \le h-1$. By the argument given above, $w \not\equiv 0 \pmod p$. It now follows from Lemma 3.8 (i) and (ii) that

$$\frac{w_{n+2r}}{w_n}\frac{w_{h-n}}{w_{h-n-2r}} \equiv (-1)^{2r} \equiv 1 \pmod p,$$

where $0 \le n \le h-2$, $1 \le h-n-2r \le h-2$, and $2 \le 2r \le h-1$. Hence,

$$\frac{w_{n+2r}}{w_n} \equiv \frac{w_{h-n}}{w_{h-n-2r}} \equiv \varepsilon \pmod p. \tag{3.8}$$

By Theorem 3.7, we must have that

$$n = h - n - 2r,$$

from which we derive that

$$2n = h - 2r,$$

which is a contradiction, since $h - 2r$ is odd. Thus, (3.4) is satisfied. □

We note that Lemma 3.9 follows from Lemmas 2 and 5 of [19], Lemma 7 (i) and (ii) of [15], and Lemma 7 of [20].

Proposition 3.10. *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) *$v_n^2 - Du_n^2 = 4b^n$.*
(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 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 3.11. *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 $D' = Du_k^2(a, b)$.

Proof. We note by the Binet formula (1.3) that

$$\frac{u_{kn}(a, b)}{u_k(a, b)} = \frac{(\alpha^{kn} - \beta^{kn})/(\alpha - \beta)}{(\alpha^k - \beta^k)/(\alpha - \beta)} = \frac{(\alpha^k)^n - (\beta^k)^n}{\alpha^k - \beta^k} \tag{3.9}$$

and

$$v_{kn}(a, b) = \alpha^{kn} + \beta^{kn} = (\alpha^k)^n + (\beta^k)^n. \tag{3.10}$$

Thus by (3.9) and (3.10)

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

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 $v'(a', b')$ both have characteristic roots. Moreover, $a' = \alpha^k + \beta^k = v_k(a, b)$ and $b' = \alpha^k \beta^k = (\alpha\beta)^k = b^k$. Furthermore, by Proposition 3.10 (iii),

$$D' = (a')^2 - 4b' = v_k^2(a, b) - 4b^k = Du_k^2(a, b).$$

□

A similar proof of Theorem 3.11 is given in [10, pp. 189–190] and [8, p. 437].

Lemma 3.12. *Consider the LSFK $u(a, b)$ and the LSSK $v(a, b)$. Then*

(i) $u'_n(-a,b) = (-1)^{n+1}u_n(a,b)$ *for* $n \geq 0$,
(ii) $v'_n(-a,b) = (-1)^n v_n(a,b)$ *for* $n \geq 0$.

Proof. Parts (i) and (ii) follow from the Binet formulas (1.3). □

Lemma 3.13. *Let* p *be a fixed prime and let* $w(a,b)$ *be a* p*-regular recurrence. Let* $M = M_w(p)$. *Then*

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

This follows from the proof of Lemma 10 of [16] and Lemma 13 of [19].

Theorem 3.14. *Let* p *be a fixed prime. Consider the recurrences* $u(a,b)$, $v(a,b)$, *and* $t(a,b)$. *Let* $h = h_u(p)$. *Then*

(i) $v(a,b)$ *is* p*-equivalent to* $u(a,b)$ *if and only if* h *is even.*
(ii) $t(a,b)$ *is not* p*-equivalent to* $u(a,b)$ *when* $t(a,b)$ *is defined.*

Proof. We prove parts (i) and (ii) together. By Proposition 3.10 (iv), $v_{h/2} \equiv 0 \pmod p$ when h is even. Then

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

and

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

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 [19] that $v(a,b)$ is not p-equivalent to $u(a,b)$ when h is odd and $t(a,b)$ is not p-equivalent to $u(a,b)$ when $t(a,b)$ is defined. □

Theorem 3.15. *Let* p *be a fixed prime. Consider the* p*-regular recurrence* $w(a,b)$. *Let* $h = h_w(p)$ *and* $\lambda = \lambda_w(p)$. *Then*

(i) $h \mid p - (D/p)$, *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) *Let* h_1 *be the restricted period modulo* p *of the LSFK* $u(a,b)$ *and* h_2 *be the restricted period modulo* p *of the LSFK* $u'(-a,b)$. *Then* $h_1 = h_2$.
(vi) *If* $(D/p) = 1$, *then* $\lambda \mid p - 1$.

Proof. We first note that by Theorem 3.2 and Theorem 3.3 (i), $h_w(p) = h_u(p)$ and $\lambda_w(p) = \lambda_u(p)$, since both $w(a,b)$ and $u(a,b)$ are p-regular. Parts (i) and (vi) are proved in [6, pp. 44–45] and [10, pp. 290, 296, 297]. Parts (ii) and (iv) are proved in [8, pp. 423–424]. Part (iii) is proved in [8, p. 441]. Part (v) follows from part (iv) and Lemma 3.12 (i). □

Theorem 3.16. *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* $E_w(p) = 4$.
(viii) *If* $(D/p) = -1$, *then* $\lambda_w(p) \mid 2(p+1)$.

Proof. By Theorem 3.3 (i), $u(a,b)$ is p-regular. It now follows from Theorem 3.2 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 [13].

We now establish part (viii). First suppose that $(D/p) = -1$ and $p \equiv 3 \pmod 4$. Then $E_w(p) = 2$ by part (vi). By Theorem 3.15 (i), $h_w(p) \mid p+1$. Thus, $\lambda_w(p) \mid 2(p+1)$.

Finally, suppose that $(D/p) = -1$ and $p \equiv 1 \pmod 4$. Then $E_w(p) = 4$ by part (vii). Moreover, $(-1/p) = 1$. It thus follows from Theorem 3.15 (iii) that $h_w(p) \mid (p+1)/2$. Consequently, $\lambda_w(p) \mid 2(p+1)$. □

Theorem 3.17. *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 and $E_w(p) = 1$.*
(iii) *If $\lambda_w(p) \equiv 2 \pmod 4$, then $h_w(p)$ is odd and $E_w(p) = 2$.*
(iv) *If $\lambda_w(p) \equiv 0 \pmod 4$, then $h_w(p)$ is even and $E_w(p) = 2$.*
(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) *$h_w(p) \mid (p-(D/p))/2$ and $\lambda_w(p) \mid p-(D/p)$.*

This follows from Theorem 3.2, Theorem 3.3 (i), and Theorem 3.15 (iii) of this paper and from Theorem 16 of [13].

Lemma 3.18. *Let p be a fixed prime and consider the LSFK $u(a,-1)$ and LSSK $v(a,-1)$. Then*

(i) *$u(a,-1)$ and $u'(-a,-1)$ are identically distributed modulo p,*
(ii) *$v(a,-1)$ and $v'(-a,-1)$ are identically distributed modulo p.*

Proof. (i) We note by Theorem 3.3 (i) that both $u(a,b)$ and $u'(a,b)$ are p-regular. By Theorem 3.15 (v), $h_u(p) = h_{u'}(p)$. It follows from Theorem 3.16 that $E_u(p) = E_{u'}(p)$, and hence, $\lambda_u(p) = \lambda_{u'}(p)$. By Lemma 3.12 (i),

$$u'_{2i+1}(-a,-1) = u_{2i+1}(a,-1) \tag{3.11}$$

and

$$u'_{2i}(-a,-1) = -u_{2i}(a,-1) \tag{3.12}$$

for $i \geq 0$.

Suppose that $h_u(p) \equiv 2 \pmod 4$. Then by Theorem 3.16 (ii), $E_u(p) = 1$, and thus $M_u(p) \equiv 1 \pmod p$. Moreover by Lemma 3.8 (i),

$$u_{2i+1} \equiv u_{h_u-2i-1} \pmod p \tag{3.13}$$

and

$$u_{2i} \equiv -u_{h_u-2i} \pmod p \tag{3.14}$$

for $0 \leq i \leq (h_u-2)/4$. It now follows from (3.11)–(3.14) that $A_u(d) = A_{u'}(d)$ for $0 \leq d \leq p-1$. Hence, $u(a,-1)$ and $u'(-a,-1)$ are identically distributed modulo p.

Now suppose that $h_u(p)$ is odd or divisible by 4. Since $M_u^2(p) \equiv -1 \pmod p$ if $h_u(p)$ is odd, and $M_u(p) \equiv -1 \pmod p$ if $h_u(p)$ is divisible by 4, it follows from Lemma 3.13 that

$$A_u(d) = A_u(-d) \quad \text{and} \quad A_{u'}(d) = A_{u'}(-d) \tag{3.15}$$

for $0 \leq d \leq p-1$. By (3.11) and (3.12),

$$A_u(d) + A_u(-d) = A_{u'}(d) + A_{u'}(-d) \tag{3.16}$$

for $0 \le d \le p-1$. Therefore, from (3.15) and (3.16), we see that $A_u(d) = A_{u'}(d)$ for $0 \le d \le p-1$. Thus, $u(a,-1)$ and $u'(-a,-1)$ are identically distributed modulo p.

(ii) By Theorem 3.6 and Theorem 3.14 (i), $u(a,-1)$ and $v(a,-1)$ are identically distributed modulo p, and $u'(-a,-1)$ and $v'(-a,-1)$ are also identically distributed modulo p if $h_u(p)$ is even and $p \nmid D$. Thus, by part (i), $v(a,-1)$ and $v'(-a,-1)$ have the same distribution of residues modulo p if $h_u(p)$ is even and $p \nmid D$.

Now suppose that $p \mid D$. Then by the proof of Theorem 3.3 (ii) both $v(a,-1)$ and $v'(-a,-1)$ are p-irregular if $p \mid D$. By inspection

$$v_0 \equiv 2,\ v_1 \equiv a,\ v_2 \equiv -2,\ v_3 \equiv -a,\ v_4 \equiv 2,\ v_5 \equiv a, \dots \pmod{p}$$

and

$$v'_0 \equiv 2,\ v'_1 \equiv -a,\ v'_2 \equiv -2,\ v'_3 \equiv a,\ v'_4 \equiv 2,\ v'_5 \equiv -a, \dots \pmod{p},$$

where $a^2 \equiv -4 \pmod{p}$, since $p \mid D = a^2+4$. Hence, $\lambda_v(p) = \lambda_{v'}(p) = 4$, and $v(a,-1)$ and $v'(-a,-1)$ are identically distributed modulo p.

Further, suppose that $p \nmid D$ and $h_u(p)$ is odd. Then both $v(a,-1)$ and $v'(-a,-1)$ are p-regular and $h_v(p) = h_{v'}(p) = h_u(p)$ is odd. Moreover, $E_v(p) = E_{v'}(p) = E_u(p) = 4$ and $M_v^2(p) \equiv M_{v'}^2(p) \equiv -1 \pmod{p}$. Further, by Lemma 3.12 (ii),

$$v'_{2i+1}(-a,-1) = -v_{2i+1}(a,-1) \tag{3.17}$$

and

$$v'_{2i}(-a,-1) = v_{2i}(a,-1) \tag{3.18}$$

for $i \ge 0$. Since $M_v^2 \equiv -1 \pmod{p}$, it follows from Lemma 3.13 that

$$A_v(d) = A_v(-d) \quad \text{and} \quad A_{v'}(d) = A_{v'}(-d) \tag{3.19}$$

for $0 \le d \le p-1$. By (3.17) and (3.18),

$$A_v(d) + A_v(-d) = A_{v'}(d) + A_{v'}(-d) \tag{3.20}$$

for $0 \le d \le p-1$. Thus, from (3.19) and (3.20), we find that $A_v(d) = A_{v'}(d)$ for $0 \le d \le p-1$. Consequently, $v(a,-1)$ and $v'(-a,-1)$ are identically distributed modulo p. □

Theorem 3.19. *Let p be a fixed prime.*

(i) *If $p \equiv 1 \pmod{4}$, then there exists a LSFK $u(a,-1)$ such that $(D/p) = 1$ and $h_u(p) = m$ if and only if $m \mid (p-1)/2$ and $m \ne 1$.*
(ii) *If $p \equiv 3 \pmod{4}$, then there exists a LSFK $u(a,-1)$ such that $(D/p) = 1$ and $h_u(p) = m$ if and only if $m \mid p-1$ and $m \nmid (p-1)/2$.*
(iii) *If $p \equiv 1 \pmod{4}$, then there exists a LSFK $u(a,-1)$ such that $(D/p) = -1$ and $h_u(p) = m$ if and only if $m \mid (p+1)/2$ and $m \ne 1$.*
(iv) *If $p \equiv 3 \pmod{4}$, then there exists a LSFK $u(a,-1)$ such that $(D/p) = -1$ and $h_u(p) = m$ if and only if $m \mid p+1$ and $m \nmid (p+1)/2$.*

Proof. Parts (i) and (ii) follow from Theorem 12 of [14]. Parts (iii) and (iv) follow from Theorems 3 and 4 of [18]. □

Theorem 3.20. *Let p be a fixed prime such that either $p = 4n+1$ or $p = 4n+3$. Consider all the possible distinct discriminants $D \equiv a^2+4$ modulo p of recurrences $w(a,-1)$, where $0 \le a \le p-1$.*

(i) *There exist exactly $n+1$ distinct discriminants D modulo p such that either $(D/p) = 0$ or $(D/p) = 1$. There exists exactly one discriminant $D \equiv a^2+4 \pmod{p}$ such that $(D/p) = 0$ if $p \equiv 1 \pmod{4}$ and no such discriminant if $p \equiv 3 \pmod{4}$.*

(ii) *There exist exactly* $(p+1)/2-(n+1)$ *distinct discriminants* $D \equiv a^2+4 \pmod p$ *such that* $(D/p) = -1$.

Proof. (i) To find all $a \in \{0, 1, \ldots, p-1\}$ such that

$$\left(\frac{a^2+4}{p}\right) = 0 \text{ or } 1,$$

all one needs to do is find all solutions to the congruence

$$x^2 - a^2 = (x+a)(x-a) \equiv 4 \pmod p. \tag{3.21}$$

There are $p-1$ sets of solutions for x and a generated by

$$x + a \equiv k,\ x - a \equiv 4/k \pmod p, \quad 1 \le k \le p-1. \tag{3.22}$$

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

$$x+a \equiv k, \quad x-a \equiv 4/k; \quad x+a \equiv 4/k, \quad x-a \equiv k;$$

$$x+a \equiv -k, \quad x-a \equiv -4/k; \quad x+a \equiv -4/k, \quad x-a \equiv -k \pmod p.$$

Since $k \not\equiv 0 \pmod p$, we find that $k \not\equiv -k$ and $4/k \not\equiv -4/k \pmod p$. However, $4/k \equiv k$ if and only if $k \equiv \pm 2 \pmod p$. Also, $-4/k \equiv k \pmod p$ if and only if $k \equiv \pm\sqrt{-4} \pmod p$. Combining these facts with the fact that $p \equiv 1 \pmod 4$ if and only if both ± 4 are quadratic residues modulo p, one finds that the number of solutions of the congruence $x^2 \equiv a^2+4 \pmod 4$ is $n+1$ if p is equal to either $4n+1$ or $4n+3$. By the above discussion, we see that there exists a discriminant $D \equiv a^2+4$ such that $D \equiv 0 \pmod p$ if and only if $p \equiv 1 \pmod 4$. Moreover, this discriminant is unique modulo p if it exists.

Part (ii) follows from the fact that there exist exactly $(p+1)/2$ distinct values of a^2+4 modulo p, which are generated by those a's for which $0 \le a \le (p-1)/2$. □

Theorem 3.20 is essentially proved in [12, p. 39].

Theorem 3.21. *Let p be a fixed prime. Let a and b be fixed integers such that $p \nmid b$. Define the relation p-equivalence on the set of all p-regular recurrences $w(a,b)$ modulo p. Let $h = h_u(a,b)$ and $D = a^2 - 4b$. Then the number of equivalence classes is equal to*

$$\frac{p-(D/p)}{h}.$$

This is proved in Theorem 2.14 of [5].

4. Proofs of the Main Theorems

Proof of Theorem 2.1. Let $h_1 = h_u(p)$, $h_2 = h_{u'}(p)$, $\lambda_1 = \lambda_u(p)$, and $\lambda_2 = \lambda_{u'}(p)$. By hypothesis, $(D_1/p) = (D_2/p)$ and

$$h_1 = h_2. \tag{4.1}$$

By Theorem 3.16 (i)–(iv), the equality (4.1) holds if and only if $E_u(p) = E_{u'}(p)$ and $\lambda_1 = \lambda_2$. We will show that $u(a_1, -1)$ and $u'(a_2, -1)$ are identically distributed modulo p. We divide the proof into four cases depending on whether $p \equiv 1$ or 3 modulo 4 and whether $(D_1/p) = (D_2/p) = 1$ or $(D_1/p) = (D_2/p) = -1$.

Case 1: $p \equiv 3 \pmod 4$ and $(D_1/p) = (D_2/p) = -1$.

Proof of Theorem 2.1 for Case 1. By Theorem 3.15 (iii) and Theorem 3.16 (vi),

$$h_1 = h_2 \equiv 0 \pmod 4, \quad h_1 \mid p+1, \quad h_1 \nmid (p+1)/2, \quad E_u(p) = E_{u'}(p) = 2,$$

and
$$\lambda_1 = \lambda_2 = 2h_1. \tag{4.2}$$

By Theorem 3.19 (iv), there exists a LSFK $u''(a_3, -1)$ with discriminant D_3 such that $(D_3/p) = -1$ and $h_3 = h_{u''}(p)$ has a maximal value of $p+1$. Let $\lambda_3 = \lambda_{u''}(p)$. Then by Theorem 3.16 (vi),
$$\lambda_3 = 2h_3 = 2(p+1).$$
By Theorem 3.20 (ii), there exist exactly $(p+1)/4$ distinct discriminants a^2+4 of LSFK's $u(a,-1)$ modulo p for which $\left(\frac{a^2+4}{p}\right) = -1$.

Now consider the LSSK $v''(a_3, -1)$. Since $p \nmid D_3$, $v''(a_3, -1)$ is p-regular by Theorem 3.3 (ii), and thus $h_{v''}(p) = h_3$. By (3.3), if i and j are odd integers such that $0 \le i < j \le h_3/2 = (p+1)/2$, then
$$v''_i(a_3, -1) \not\equiv \pm v''_j(a_3, -1) \pmod{p}. \tag{4.3}$$
Making note of Theorem 3.11, we now consider all LSFK's
$$\hat{u}(v''_{2m-1}(a_3, -1), (-1)^{2m-1}) = \hat{u}(v''_{2m-1}(a_3, -1), -1) = \left\{ \frac{u''_{(2m-1)n}(a_3, -1)}{u''_{2m-1}(a_3, -1)} \right\}_{n=0}^{\infty}, \tag{4.4}$$
where $1 \le m \le (p+1)/4$. Since $0 \le 2m-1 \le (p-1)/2$, we see by Theorem 3.15 (iv) that $u''_{2m-1}(a_3, -1) \not\equiv 0 \pmod{p}$. It now follows from (4.3) and Proposition 3.10 (iii) that the $(p+1)/4$ LSFK's in (4.4) all have distinct discriminants which are quadratic nonresidues modulo p, since
$$(v''_{2m-1}(a_3, -1))^2 + 4 = D_3 (u''_{2m-1}(a_3, -1))^2. \tag{4.5}$$
Thus, there exist some ε_1, ε_2 such that $\varepsilon_1, \varepsilon_2 \in \{-1, 1\}$ and both $\hat{u}(\varepsilon_1 a_1, -1)$ and $\tilde{u}(\varepsilon_2 a_2, -1)$ appear among the $(p+1)/4$ LSFK's in (4.4) when reduced modulo p. Let
$$r = \frac{\lambda_3}{\lambda_1}.$$
It follows from (4.2) that r is a positive odd integer. We further see from (4.4) that
$$\hat{u}(\varepsilon_1 a_1, -1) = \left\{ \frac{u''_{kn}(a_3, -1)}{u''_k(a_3, -1)} \right\}_{n=0}^{\infty} \tag{4.6}$$
and
$$\tilde{u}(\varepsilon_2 a_2, -1) = \left\{ \frac{u''_{\ell n}(a_3, -1)}{u''_\ell(a_3, -1)} \right\}_{n=0}^{\infty} \tag{4.7}$$
for all $n \ge 0$ and some odd integers k and ℓ such that $k, \ell \in \{1, \dots, (p-1)/2\}$ and
$$\gcd(k, \lambda_3) = \gcd(\ell, \lambda_3) = r. \tag{4.8}$$

We note by (4.8) that the sets
$$\{kn\}_{n=1}^{\lambda_1} \quad \text{and} \quad \{\ell n\}_{n=1}^{\lambda_1} \tag{4.9}$$
contain the same sets of residues modulo λ_3. Since $k, \ell \in \{1, \dots, (p-1)/2\}$ and $h_3 = p+1$, we see by Theorem 3.15 (iv) that both $u''_k(a_3, -1)$ and $u''_\ell(a_3, -1)$ are invertible modulo p. It now follows from (4.6), (4.7), and (4.9) that $\hat{u}(\varepsilon_1 a_1, -1)$ and $\tilde{u}(\varepsilon_2 a_2, -1)$ are identically distributed modulo p.

The result now follows upon noting by Lemma 3.18 (i) that $u(a, -1)$ and $u(-a, -1)$ are identically distributed modulo p for any integer a.

Case 2: $p \equiv 3 \pmod{4}$ and $(D_1/p) = (D_2/p) = 1$.

Proof of Theorem 2.1 for Case 2. By Theorem 3.15 (iii) and Theorem 3.16 (v),

$$h_1 = h_2 \equiv 2 \pmod 4, \quad h_1 \mid p-1, \quad h_1 \nmid (p-1)/2, \quad E_u(p) = E_{u'}(p) = 1,$$

and

$$\lambda_1 = \lambda_2 = h_1.$$

By Theorem 3.19 (ii), there exists a LSFK $u''(a_3,-1)$ with discriminant D_3 such that $(D_3/p) = 1$ and $h_3 = h_{u''}(p)$ has a maximal value of $p-1$. By Theorem 3.20 (i), there exist exactly $(p+1)/4$ distinct discriminants a^2+4 of LSFK's $u(a,-1)$ modulo p for which $\left(\frac{a^2+4}{p}\right) = 1$. We further note that by (3.3), if i and j are odd integers such that $0 \le i < j \le h_3/2 = (p-1)/2$, then

$$v''_i(a_3,-1) \not\equiv \pm v''_j(a_3,-1) \pmod p.$$

Moreover, there are exactly $(p+1)/4$ odd integers m such that $0 \le m \le (p-1)/2$. The rest of the proof is similar to that of Case 1.

Case 3: $p \equiv 1 \pmod 4$ and $(D_1/p) = (D_2/p) = -1$.

Proof of Theorem 2.1 for Case 3. By Theorem 3.15 (iii) and Theorem 3.16 (vii),

$$h_1 = h_2 \equiv 1 \pmod 2, \quad h_1 \mid (p+1)/2, \quad h_1 > 1, \quad E_u(p) = E_{u'}(p) = 4,$$

and

$$\lambda_1 = \lambda_2 = 4h.$$

By Theorem 3.19 (iii), there exists a LSFK $u''(a_3,-1)$ with discriminant D_3 such that $(D_3/p) = -1$ and $h_3 = h_{u''}(p)$ has a maximal value of $(p+1)/2$. By Theorem 3.20 (ii), there exist exactly $(p-1)/4$ distinct discriminants a^2+4 of LSFK's $u(a,-1)$ modulo p for which $\left(\frac{a^2+4}{p}\right) = -1$. We further note that by (3.4), if i and j are odd integers such that $0 \le i < j < h_3 = (p+1)/2$, then

$$v''_i(a_3,-1) \not\equiv \pm v''_j(a_3,-1) \pmod p.$$

Moreover, there are exactly $(p-1)/4$ odd integers m such that $1 \le m < (p+1)/2$. The remainder of the proof is similar to that of Case 1.

Case 4: $p \equiv 1 \pmod 4$ and $(D_1/p) = (D_2/p) = 1$.

Proof of Theorem 2.1 for Case 4. Let $p-1 = 2^\gamma m$, where $\gamma \ge 2$ and m is odd. By Theorem 3.15 (iii),

$$h_1 = h_2, \quad h_1 \mid (p-1)/2 = 2^{\gamma-1}m, \quad \text{and} \quad h_1 > 1. \tag{4.10}$$

By Theorem 3.20 (i), there exist exactly $(p-1)/4 = 2^{\gamma-2}m$ distinct discriminants a^2+4 of LSFK's $u(a,-1)$ modulo p for which $\left(\frac{a^2+4}{p}\right) = 1$.

Let $0 \le i \le \gamma-1$. By Theorem 3.19 (i), if it is not the case that $i=0$ and $m=1$, then there exists a LSFK $u''(a_3,-1)$ with discriminant D_3 such that $(D_3/p) = 1$ and $h_3 = h_{u''}(p) = 2^i m$. Let $\lambda_3 = \lambda_{u''}(p)$. First suppose that $2 \le i \le \gamma-1$. Consider the LSSK $v''(a_3,-1)$. Since $p \nmid D_3$, $v''(a_3,-1)$ is p-regular and thus $h_{v''}(p) = h_3$. Since h_3 is even, it follows from (3.3) that if k and ℓ are odd integers such that $0 \le k < \ell \le h_3/2 = 2^{i-1}m$, then

$$v''_k(a_3,-1) \not\equiv \pm v''_\ell(a_3,-1) \pmod p. \tag{4.11}$$

Taking note of Theorem 3.11, we consider all LSFK's

$$\hat{u}(v''_{2j-1}(a_3,-1),(-1)^{2j-1}) = \hat{u}(v''_{2j-1}(a_3,-1),-1) = \left\{ \frac{u''_{(2j-1)n}(a_3,-1)}{u''_{2j-1}(a_3,-1)} \right\}_{n=0}^{\infty}, \tag{4.12}$$

where $1 \leq j \leq 2^{i-2}m$. Since $0 \leq 2j-1 \leq 2^{i-1}m$, we see by Theorem 3.15 (iv) that $u''_{2j-1}(a_3,-1) \not\equiv 0 \pmod{p}$. It now follows from (4.11) and (4.5) that the $2^{i-2}m$ LSFK's in (4.12) all have distinct discriminants which are nonzero quadratic residues modulo p.

Suppose that k is an odd integer such that $1 \leq k \leq 2^{i-1}m$. Suppose further that $\gcd(k,\lambda_3) = r$. Since k is odd, then $\gcd(k,\lambda_3) = r$. It now follows that the sets $\{kn\}_{n=0}^{\infty}$ and $\{rc\}_{c=1}^{\lambda_3/r}$ have exactly the same elements modulo p. Since $u''_k(a_3,-1)$ is invertible modulo p, it follows from (4.12) that the period of $\hat{u}(v''_k(a_3,-1),-1)$ modulo p is equal to $\lambda_3/r = \lambda_4$. Then $\nu_2(\lambda_4) = \nu_2(\lambda_3)$, where $\nu_2(n) = c$ if $2^c \mid n$, but $2^{c+1} \nmid n$. Let h_4 denote the restricted period of $\hat{u}(v''_k(a_3,-1),-1)$ modulo p. Since $i \geq 2$, it follows from Theorem 3.16 (iii) that $\lambda_4 = 2h_4$ and $\lambda_3 = 2h_3$. Thus, $\nu_2(h_4) = \nu_2(h_3) = i$. We now note that in (4.12) we have generated $2^{i-2}m$ LSFK's $u(a,-1)$ with distinct discriminants a^2+4 and distinct restricted periods h modulo p such that $\left(\frac{a^2+4}{p}\right) = 1$ and $\nu_2(h) = \nu_2(h_3) = i \geq 2$.

We next suppose that $i = 1$ and that h_3 is thus equal to $2m$. Then $h_3 = \lambda_3$ by Theorem 3.16 (ii). Moreover, by (3.3), we see that (4.11) holds if k and ℓ are odd integers such that $0 \leq k < \ell \leq h_3/2 = m$. Now consider the LSFK's in (4.12), where we now take j to satisfy $1 \leq j \leq (m+1)/2$. Then $1 \leq 2j-1 \leq m$. It now follows from Theorem 3.15 (iv) that $u''_{2j-1}(a_3,-1) \not\equiv 0 \pmod{p}$ for $1 \leq 2j-1 \leq m$. By our argument above we can generate $(m+1)/2$ LSFK's $u(a,-1)$ with distinct discriminants a^2+4 and distinct discriminants a^2+4 and distinct restricted periods h modulo p such that $\left(\frac{a^2+4}{p}\right) = 1$ and $\nu_2(h) = \nu_2(h_3) = 1$.

We finally suppose that $i = 0$ and that h_3 is consequently equal to m. Then $\lambda_3 = 4h_3$ by Theorem 3.16 (iv). Furthermore, by (3.4) we find that (4.11) holds if k and ℓ are odd integers such that $0 \leq k < \ell \leq h_3 - 1 = m-1$. We now consider the LSFK's in (4.12), where we take j to satisfy $1 \leq j \leq (m-1)/2$. Then $1 \leq 2j-1 \leq m-2$. By Theorem 3.15 (iv), we see that $u''_{2j-1}(a_3,-1) \not\equiv 0 \pmod{p}$ for $1 \leq 2j-1 \leq m-2$. By our argument above, we can construct $(m-1)/2$ LSFK's $u(a,-1)$ with distinct discriminants a^2+4 and distinct restricted periods h modulo p such that $\left(\frac{a^2+4}{p}\right) = 1$ and $\nu_2(h) = \nu_2(h_3) = 0$.

Letting i vary from 0 to $\gamma - 1$, we see from our above discussion that we have generated exactly

$$\left(\frac{m-1}{2} + \frac{m+1}{2}\right) + \sum_{i=2}^{\gamma-1} 2^{i-2}m = m + m(2^{\gamma-2}-1) = 2^{\gamma-2}m$$

LSFK's $u(a,-1)$ having distinct discriminants D modulo p such that $(D/p) = 1$. Since there are exactly $2^{\gamma-2}m$ such LSFK's $u(a,-1)$ modulo p by our above discussion, it follows that $\tilde{u}(\varepsilon_1 a_1,-1)$ and $\overline{u}(\varepsilon_2 a_2,-1)$ appear among the LSFK's we have constructed above when reduced modulo p, where ε_1 and ε_2 are some elements of $\{-1,1\}$. The rest of the proof is similar to the proof of Case 1.

This completes the proof of Theorem 2.1. □

Proof of Theorem 2.2. Since $p \nmid D_1D_2$, both $v(a_1,-1)$ and $v'(a_2,-1)$ are p-regular by Theorem 3.3 (ii). Consider the LSFK's $u(a_1,-1)$ and $u'(a_2,-1)$. Then by Theorems 3.2 and 3.3 (ii),

$$h_u(p) = h_v(p) \quad \text{and} \quad h_{u'}(p) = h_{v'}(p). \tag{4.13}$$

By hypothesis, $h_v(p) = h_{v'}(p)$. Suppose that $h_v(p)$ and $h_{v'}(p)$ are both even. Then by Theorem 3.14 (i), $v(a_1,-1)$ is p-equivalent to $u(a_1,-1)$ and $v'(a_2,-1)$ is p-equivalent to $u'(a_2,-1)$. By Theorem 3.6 (ii), $v(a_1,-1)$ and $u(a_1,-1)$ are identically distributed modulo p, while $v'(a_2,-1)$ and $u'(a_2,-1)$ are also identically distributed modulo p. By Theorem 2.1, both

$u(a_1,-1)$ and $u'(a_2,-1)$ are identically distributed modulo p. Thus, $v(a_1,-1)$ and $v'(a_2,-1)$ are identically distributed modulo p.

It thus suffices to suppose that $h_v(p) = h_{v'}(p)$ is odd. We consider two cases in which $h_v(p)$ is odd and $(D_1/p) = -1$ or 1. We note that by Theorem 3.16 (iv), it then follows that $p \equiv 1 \pmod 4$. Moreover, by Theorem 3.16 (vii), if $p \equiv 1 \pmod 4$ and $(D_1/p) = -1$, then $h_v(p)$ is odd. Our proof will then complete once we prove Theorem 2.2 for the following two cases. In the first case $p \equiv 1 \pmod 4$ and $(D_1/p) = (D_2/p) = -1$. In the second case, $p \equiv 1 \pmod 4$, $(D_1/p) = (D_2/p) = 1$, and $h_v(p)$ is odd. We let $h_1 = h_v(p)$, $h_2 = h_{v'}(p)$, $\lambda_1 = \lambda_v(p)$, and $\lambda_2 = \lambda_{v'}(p)$.

<u>Case 1</u>: $p \equiv 1 \pmod 4$ and $(D_1/p) = (D_2/p) = -1$.

Proof of Theorem 2.2 for Case 1. By Theorem 3.15 (iii) and Theorem 3.16 (vii),

$$h_1 = h_2 \equiv 1 \pmod 2, \quad h_1 \mid (p+1)/2, \quad h_1 > 1, \quad E_v(p) = E_{v'}(p) = 4, \text{ and } \lambda_1 = \lambda_2 = 4h_1.$$

By Theorem 3.19 (iii), there exists a LSFK $u''(a_3,-1)$ with discriminant D_3 such that $(D_3/p) = -1$ and $h_3 = h_{u''}(p)$ has a maximal value of $(p+1)/2$. Thus, by Theorem 3.3 (ii) and Theorem 3.2, the restricted period $h_3 = h_{v''}(p)$ of $v''(a_3,-1)$ modulo p is equal to $(p+1)/2$ also, and $v''(a_3,-1)$ has the same discriminant D_3 as $u''(a_3,-1)$. By Theorem 3.20 (ii), there exist exactly $(p-1)/4$ distinct discriminants a^2+4 of LSSK's $v(a,-1)$ modulo p for which $\left(\frac{a^2+4}{p}\right) = -1$. We further observe by (3.4) that if i and j are odd integers such that $1 \le i < j < h_3/2 = (p+1)/2$, then

$$v''_i(a_3,-1) \not\equiv v''_j(a_3,-1) \pmod p. \tag{4.14}$$

Taking into account Theorem 3.11, we now consider all the LSSK's

$$\hat{v}(v''_{2m-1}(a_3,-1),(-1)^{2m-1}) = \hat{v}(v''_{2m-1}(a_3,-1),-1) = \{v''_{(2m-1)n}(a_3,-1)\}_{n=0}^{\infty}, \tag{4.15}$$

where $1 \le m \le (p-1)/4$. By (4.14) and (4.5), these $(p-1)/4$ LSSK's all have discriminants which are distinct modulo p and which are quadratic nonresidues modulo p. Thus, both $\hat{v}(\varepsilon_1 a_1,-1)$ and $\tilde{v}(\varepsilon_2 a_2,-1)$ appear among the $(p-1)/4$ LSSK's in (4.15), where ε_1 and ε_2 are elements of $\{-1,1\}$. We also note that by Lemma 3.18 (ii), $v(a,-1)$ and $v'(-a,-1)$ are identically distributed modulo p for all integers a. The rest of the proof is similar to that of the proof of Case 1 of Theorem 2.1.

<u>Case 2</u>: $p \equiv 1 \pmod 4$, $(D_1/p) = (D_2/p) = 1$, and $h_v(p)$ is odd.

Proof of Theorem 2.2 for Case 2. Let $p-1 = 2^\gamma m$, where $\gamma \ge 2$ and m is odd. By Theorem 3.15 (iii) and Theorem 3.16 (iv),

$$h_1 = h_2 \equiv 1 \pmod 2, \quad h_1 \mid (p+1)/2, \quad h_1 > 1, \quad E_v(p) = E_{v'}(p) = 4, \text{ and } \lambda_1 = \lambda_2 = 4h_1. \tag{4.16}$$

By Theorem 3.20 (i), there exist exactly $(p-1)/4 = 2^{\gamma-2}m$ distinct discriminants a^2+4 of LSSK's $v(a,-1)$ modulo p for which $\left(\frac{a^2+4}{p}\right) = -1$. By Theorem 3.19 (i), Theorem 3.3 (ii), and Theorem 3.2, it follows that if $0 \le i \le \gamma-1$ and it is not the case that $i=0$ and $m=1$, then there exists a LSSK $v''(a_3,-1)$ with discriminant D_3 such that $(D_3/p) = 1$ and $h_3 = h_{v''}(p) = 2^i m$. We also note by (3.3) that if $1 \le i \le \gamma-1$ and $1 \le 2k-1 < 2\ell-1 \le h_3/2 = 2^{i-1}m$, then

$$v''_{2k-1}(a_3,-1) \not\equiv \pm v''_{2\ell-1}(a_3,-1) \pmod p. \tag{4.17}$$

Moreover, by (3.4), (4.17) also holds if $i=0$, $m>1$, and $1 \le 2k-1 < 2\ell-1 \le h_3-1 = 2^i m-1$. Further, by Theorem 3.3 (ii), Theorem 3.2, and the argument given in the proof of Case 4 of

Theorem 2.1, we see that there are exactly $(p-1)/4 = 2^{\gamma-2}m$ LSSK's of the form

$$\hat{v}(v''_{2j-1}(a_3,-1),-1), \tag{4.18}$$

where $1 \le 2j-1 \le 2^{i-1}m$ if $1 \le i \le \gamma-1$ and $1 \le 2j-1 \le m-2$ if $i=0$ and $m > 1$. Additionally, the discriminants of those $(p-1)/4$ LSSK's are distinct nonzero quadratic residues modulo p, since

$$(v''_{2j-1}(a_3,-1))^2 + 4 = D_3(u''_{2j-1}(a_3,-1))^2$$

by Proposition 3.10 (iii). We also note by Theorem 3.3 (ii), Theorem 3.2, and the argument given in the proof of Case 4 of Theorem 2.1 that for the LSSK $\hat{v}(v''_{2j-1}(a_3,-1),-1)$ given in (4.18), we have that

$$\nu_2(h_{v''}(p)) = \nu_2(2^i m) = i.$$

The remainder of the proof now follows from arguments similar to those given in the proofs of Case 1 of Theorem 2.1 and Case 1 of this theorem.

The proof of Theorem 2.2 is now complete. □

5. Corollaries of the Main Theorems

Corollary 5.1 follows from Theorem 2.1 upon application of Theorems 3.6 and 3.2.

Corollary 5.1. *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 $p \nmid D_1D_2$ and $(D_1/p) = (D_2/p)$. Suppose that $w(a_1,-1)$ is p-equivalent to $u(a_1,-1)$ and $w'(a_2,-1)$ is p-equivalent to $u'(a_2,-1)$. Suppose further that $h_w(p) = h_{w'}(p)$. This occurs if and only if $\lambda_w(p) = \lambda_{w'}(p)$. Then $w(a_1,-1)$ and $w'(a_2,-1)$ are identically distributed modulo p.*

The above statement remains valid and follows from Theorem 2.2 if we replace u by v and u' by v'.

Corollary 5.2. *Let p be a fixed prime. Let $v(a_1,-1)$ and $v'(a_2,-1)$ be LSSK's with discriminants D_1 and D_2 such that $p \nmid D_1D_2$ and $(D_1/p) = (D_2/p)$. Suppose that $h_v(p) = h_{v'}(p)$ is even. Then $v(a_1,-1)$, $u(a_1,-1)$, $v'(a_2,-1)$, and $u'(a_2,-1)$ are all identically distributed modulo p.*

Proof. By Theorem 3.14 (i), $v(a_1,-1)$ is p-equivalent to $u(a_1,-1)$ and $v'(a_2,-1)$ is p-equivalent to $u'(a_2,-1)$. The result now follows from Corollary 5.1. □

Corollary 5.3. *Let $p \equiv 3 \pmod 4$ be a fixed prime and let $\varepsilon \in \{-1,1\}$. Then there exists a LSFK $u(a,-1)$ with discriminant D such that $(D/p) = \varepsilon$ and $h_u(p) = p-(D/p)$.*

Let $w'(a_1,-1)$ be any p-regular recurrence with discriminant D_1 such that $(D_1/p) = \varepsilon$ and $h_{w'}(p) = p-(D/p)$. Then $w'(a_1,-1)$ and $u(a,-1)$ are identically distributed modulo p.

Proof. By Theorem 3.19 (ii) and (iv), there exists a LSFK $u(a,-1)$ with discriminant D such that $(D/p) = \varepsilon$ and $h_u(p) = p-(D/p)$. We note that $u(a,-1)$ is p-regular by Theorem 3.3 (i). By Theorem 3.21, $w'(a_1,-1)$ is p-equivalent to $u'(a_1,-1)$. Since $h_{w'}(p) = p-(D/p)$, we have that $h_{u'}(p) = p-(D/p)$. By Theorem 3.6 (ii), $w'(a_1,-1)$ and $u'(a_1,-1)$ are identically distributed modulo p. By Theorem 2.1, $u'(a_1,-1)$ and $u(a,-1)$ are identically distributed modulo p. Thus, $w'(a_1,-1)$ and $u(a,-1)$ are identically distributed modulo p. □

Corollary 5.4. *Let $p \equiv 1 \pmod 4$ be a fixed prime. Then there exists a LSFK $u(a,-1)$ with discriminant D such that $(D/p) = -1$ and $h_u(p) = (p+1)/2$.*

Let $w'(a_1,-1)$ be any p-regular recurrence with discriminant D_1 such that $(D_1/p) = -1$ and $h_{w'}(p) = (p+1)/2$. Then $w'(a_1,-1)$ is p-equivalent to either $u'(a_1,-1)$ or $v'(a_1,-1)$.

If $w'(a_1,-1)$ is p-equivalent to $u'(a_1,-1)$, then $w'(a_1,-1)$ is identically distributed modulo p to $u(a,-1)$. If $w'(a_1,-1)$ is p-equivalent to $v'(a_1,-1)$, then $w'(a_1,-1)$ is identically distributed modulo p to $v(a,-1)$.

Proof. By Theorem 3.19 (iii), there exists a LSFK $u(a,-1)$ with discriminant D such that $(D/p) = -1$ and $h_u(p) = (p+1)/2$. We note that both $u(a,-1)$ and $v(a,-1)$ are p-regular by Theorem 3.3 (i) and (ii). By Theorem 3.14 (i), $v(a,-1)$ is not p-equivalent to $u(a,-1)$, and $v'(a_1,-1)$ is not p-equivalent to $u'(a_1,-1)$. By Theorem 3.21, there are exactly two equivalence classes of p-regular and p-equivalent recurrences modulo p given that $w'(a_1,-1)$ has discriminant D_1 such that $(D_1/p) = -1$ and $h_{w'}(p) = (p+1)/2$. It thus follows that $w'(a_1,-1)$ is p-equivalent to either $u'(a_1,-1)$ or $v'(a_1,-1)$. By Theorem 3.6 (ii) $w'(a_1,-1)$ is identically distributed modulo p to $u'(a_1,-1)$ if $w'(a_1,-1)$ is p-equivalent to $u'(a_1,-1)$ and $w'(a_1,-1)$ is identically distributed to $v'(a_1,-1)$ if $w'(a_1,-1)$ is p-equivalent to $v'(a_1,-1)$. By Theorems 2.1 and 2.2, $u(a,-1)$ and $u'(a_1,-1)$ are identically distributed modulo p, and $v(a,-1)$ and $v'(a_1,-1)$ are identically distributed modulo p. The result now follows. □

Primes q such that $2q+1$ is prime are called *Sophie Germain primes of the first kind*, while primes q for which $2q-1$ is prime are called *Sophie Germain primes of the second kind*. The prime p is a *Mersenne prime* if $p = 2^q - 1$ for some q, where q must be a prime.

Corollaries 5.5–5.7 restrict Theorems 2.1 and 2.2 to the cases in which the prime p has a special form, namely, $p = 2q+1$, where q is a Sophie Germain prime of the first kind, $p = 2q-1$, where q is a Sophie Germain prime of the second kind, or p is a Mersenne prime.

By inspection, we see that the first few Sophie Germain primes of the first kind are

$$2, 3, 5, 11, 23, 29, 41, 53, 83, 89, 113, 131, \ldots$$

while the few Sophie Germain primes of the second kind are

$$2, 3, 7, 19, 31, 37, 79, 97, 139, 157, 199, 211, \ldots.$$

According to [3], the largest known Sophie Germain prime of the first kind is

$$18543637900515 \cdot 2^{666667} - 1$$

with 200701 digits, while we find from [4] that the largest known Sophie Germain prime of the second kind is

$$1579755 \cdot 2^{158712} + 1$$

with 47784 digits. We note that if q is an odd Sophie Germain prime of the first kind, then $2q+1 \equiv 3 \pmod 4$, whereas if q is a Sophie Germain prime of the second kind, then $2q-1 \equiv 1 \pmod 4$.

There are 48 known Mersenne primes (see [2]) with the largest of these being

$$2^{57885161} - 1$$

with 17425170 digits. If p is a Mersenne prime, then clearly $p \equiv 3 \pmod 4$.

Corollary 5.5. *Let p be a prime such that $(p-1)/2$ is an odd Sophie Germain prime of the first kind. Then $p \equiv 3 \pmod 4$.*

Let $w'(a_1,-1)$ and $w''(a_2,-1)$ be p-regular recurrences with discriminants D_1 and D_2, respectively, such that $p \nmid a_1a_2$ and $(D_1/p) = (D_2/p) = 1$. Then $h_{w'}(p) = h_{w''}(p) = p-1$, and $w'(a_1,-1)$ and $w''(a_2,-1)$ are identically distributed modulo p.

Proof. Let $q = (p-1)/2$. Since q is odd, it follows that $p = 2q+1 \equiv 3 \pmod 4$. Let $w(a,-1)$ be any p-regular recurrence with restricted period $h = h_w(p)$ and discriminant D such that $a \not\equiv 0 \pmod p$ and $(D/p) = 1$. By Theorem 3.15 (i) and (iii),

$$h \mid p-1 \quad \text{and} \quad h \nmid (p-1)/2. \tag{5.1}$$

Since $p-1 = 2q$, it follows from (5.1) that $h = 2$ or $h = 2q = p-1$. As $u(a,-1)$ is p-regular by Theorem 3.3 (i), it follows from Theorem 3.2 that $h_u(p) = h$. If $h_u(p) = 2$, then clearly $a \equiv 0 \pmod p$, since $u_0(a,-1) = 0$ and $u_2(a,-1) = a$. However, $a \not\equiv 0 \pmod p$ by assumption. Thus,

$$h_{w'}(p) = h_{w''}(p) = p-1.$$

The result now follows from Corollary 5.3. □

Corollary 5.6. *Let p be a prime such that $(p+1)/2$ is an odd Sophie Germain prime of the second kind. Then $p \equiv 1 \pmod 4$.*

Let $u(a,-1)$ and $v(a_2,-1)$ be Lucas sequences of the first kind and second kind, respectively, with the same discriminant D such that $(D/p) = -1$. Let $w'(a_1,-1)$ be any p-regular recurrence with discriminant D_1 such that $(D_1/p) = -1$. Then $h_{w'}(p) = h_u(p) = h_v(p) = (p+1)/2$, and $w'(a_1,-1)$ is either p-equivalent to $u'(a_1,-1)$ or $v'(a_1,-1)$. If $w'(a_1,-1)$ is p-equivalent to $u'(a_1,-1)$, then $w'(a_1,-1)$ is p-equivalent to $u(a,-1)$. If $w'(a_1,-1)$ is p-equivalent to $v'(a_1,-1)$, then $w'(a_1,-1)$ is p-equivalent to $v(a,-1)$.

Proof. Let $q = (p+1)/2$. Since q is odd, it follows that $p = 2q-1 \equiv 1 \pmod 4$. Let $w'(a,-1)$ be any p-regular recurrence with restricted period $h = h_{w'}(p)$ and discriminant D such that $(D/p) = -1$. By Theorem 3.15 (iii),

$$h \mid (p+1)/2 \quad \text{and} \quad h \neq 1. \tag{5.2}$$

Since $(p+1)/2 = q$, it follows from (5.2) that $h = q$. Thus,

$$h_{w'}(p) = h_u(p) = h_v(p) = (p+1)/2.$$

The result now follows from Corollary 5.4. □

Corollary 5.7. *Let p be a Mersenne prime. Let $w'(a_1,-1)$ and $w''(a_2,-1)$ be p-regular recurrences with discriminants D_1 and D_2, respectively, such that $(D_1/p) = (D_2/p) = -1$. Then $h_{w'}(p) = h_{w''}(p) = p+1$, and $w'(a_1,-1)$ and $w''(a_2,-1)$ are identically distributed modulo p.*

Proof. Let $p = 2^q - 1$ for some prime q. Then clearly, $p \equiv 3 \pmod 4$. Let $w(a,-1)$ be a p-regular recurrence with restricted period $h = h_w(p)$ and discriminant D such that $(D/p) = -1$. By Theorem 3.15 (i) and (iii),

$$h \mid p+1 \quad \text{and} \quad h \nmid (p+1)/2. \tag{5.3}$$

Since $p+1 = 2^q$, it follows from (5.3) that $h = p+1 = 2^q$. Thus,

$$h_{w'}(p) = h_{w''}(p) = p+1.$$

The result now follows from Corollary 5.3. □

6. Recurrences Whose Distribution of Residues Are Completely Determined Modulo p

We will sharpen Theorems 2.1 and 2.2 for certain recurrences. Theorem 2.1 shows that the LSFK's $u(a_1,-1)$ and $u'(a_2,-1)$ with the same restricted periods modulo p, (or equivalently the same periods modulo p) are identically distributed modulo p if their discriminants have the same quadratic character modulo p. An analogous result was obtained in Theorem 2.2 for the LSSK's $v(a_1,-1)$ and $v'(a_2,-1)$. However, these theorems do not necessarily explicitly describe the actual distribution of residues modulo p. For certain recurrences (w) we will be able to explicitly determine $S_w(p)$, $N_w(p)$, and $B_w(i)$ for $i \geq 0$ given only the period of (w) modulo p and also possibly the quadratic character of the discriminants of these recurrences modulo p.

In some instances, we will consider the kth-order linear recurrence $w(a_1, a_2, \ldots, a_k)$, where $k \geq 1$, defined by the recursion relation

$$w_{n+k} = a_1 w_{n+k-1} - a_2 w_{n+k-2} + \cdots + (-1)^{k+1} a_k w_k. \tag{6.1}$$

We suppose from here on that $p \nmid a_k$. Then $w(a_1, \ldots, a_k)$ is purely periodic modulo p by [7, pp. 344–345]. We distinguish the kth-order unit sequence $u(a_1, a_2, \ldots, a_k)$ satisfying (6.1) and having the initial terms $u_0 = u_1 = \cdots = u_{k-2} = 0$, $u_{k-1} = 1$. Our definitions for $\lambda_w(p)$, $h_w(p)$, $E_w(p)$, $A_w(d)$, $S_w(p)$, $N_w(p)$, and $B_w(i)$ will all carry over naturally from the case in which $k = 2$ to general k.

Before presenting our results on recurrences for which the distribution of residues modulo p is completely determined, we will need the following refinement of Theorem 1.1.

Theorem 6.1. *Let p be a fixed prime and consider the recurrence $w(a,b)$. Let d be a fixed residue modulo p such that $0 \leq d \leq p-1$. Let $g = \mathrm{ord}_p b$.*

(i) *If $w(a,b)$ is not p-equivalent to $u(a,b)$, $v(a,b)$, or $t(a,b)$, then*

$$A(d) \leq g. \tag{6.2}$$

(ii) *If $w(a,b)$ is p-equivalent to $u(a,b)$, $v(a,b)$, or $t(a,b)$, then*

$$A(0) \leq E_w(p) \leq \min(p-1, 2g) \tag{6.3}$$

and

$$A(d) \leq \min(g + E_w(p), 2g, p) \tag{6.4}$$

if $d \neq 0$.

(iii) *Suppose that $w(a,b)$ is p-equivalent to $u(a,b)$, and g and $E_w(p)$ are both odd. Then*

$$A(d) \leq g. \tag{6.5}$$

(iv) *Suppose that $w(a,b)$ is p-equivalent to $t(a,b)$ and that g is even. Then*

$$A(d) \leq g. \tag{6.6}$$

This is proved in Theorem 2 of [19].

Theorems 6.2–6.6 and Theorems 6.8–6.9 show that the distribution of residues of the p-regular recurrence $w(a,1)$ is completely determined modulo p given the value of $\lambda_u(p)$ when $p \nmid D$.

Theorem 6.2. *Let p be a fixed prime. Suppose that $w(a,1)$ is p-equivalent to $u(a,1)$, $\lambda_w(p)$ is odd, and $p \nmid D$. Then*

$$E_w(p) = 1, \quad h_w(p) \mid (p - (D/p))/2, \quad \textit{and} \quad h_w(p) \neq 1.$$

Moreover,

$$S_w(p) = \{0,1\},\ N_w(p) = \lambda_w(p) = h_w(p),\ B_w(0) = p - \lambda_w(p), \quad \textit{and} \quad B_w(1) = \lambda_w(p).$$

This follows from Theorems 4 and 7 of [17] and from Theorem 3.6 of this paper.

Theorem 6.3. *Let p be a fixed prime. Suppose that $w(a,1)$ is p-equivalent to $u(a,1)$, $\lambda_w(p) \equiv 2 \pmod 4$, and $p \nmid D$. Then*

$$E_w(p) = 2, \quad h_w(p) \equiv 1 \pmod 2, \quad h_w(p) \mid (p-(D/p))/2, \quad \text{and} \quad h_w(p) \neq 1.$$

Furthermore,

$$S_w(p) = \{0,2\},\ N_w(p) = h_w(p) = \tfrac{1}{2}\lambda_w(p),\ B_w(0) = p - h_w(p), \quad \textit{and} \quad B_w(2) = h_w(p).$$

This follows from Theorems 5 and 7 of [16] and from Theorem 3.6 of this paper.

Theorem 6.4. *Let p be a fixed prime. Suppose that $w(a,1)$ is p-equivalent to $u(a,1)$, $\lambda_w(p) \equiv 0 \pmod 4$, and $p \nmid D$. Then*

$$E_w(p) = 2, \quad h_w(p) \equiv 0 \pmod 2, \quad h_w(p) \mid (p-(D/p))/2, \quad \textit{and} \quad h_w(p) \neq 1.$$

Moreover,

$$S_w(p) = \{0,1,2\},\ N_w(p) = h_w(p) + 1 = \tfrac{1}{2}\lambda_w(p) + 1,$$
$$B_w(0) = p - h_w(p) - 1,\ B_w(1) = 2,\ \text{and}\ B_w(2) = h_w(p) - 1.$$

This follows from Theorems 6 and 7 of [17] and from Theorem 3.6 of this paper.

Theorem 6.5. *Let p be a fixed prime. Suppose that $w(a,1)$ is p-equivalent to $v(a,1)$, where $\lambda_w(p)$ is odd and $p \nmid D$. Then*

$$E_w(p) = 1, \quad h_w(p) \equiv 1 \pmod 2, \quad h_w(p) \mid (p-(D/p))/2, \quad \textit{and} \quad h_w(p) \neq 1.$$

Additionally,

$$S_w(p) = \{0,1,2\},\ N_w(p) = \frac{\lambda_w(p)+1}{2},$$
$$B_w(0) = p - \frac{\lambda_w(p)+1}{2},\ B_w(1) = 1, \quad \textit{and} \quad B_w(2) = \frac{\lambda_w(p)-1}{2}.$$

This follows from Theorem 10 of [20] and from Theorem 3.6 of this paper.

Theorem 6.6. *Let p be a fixed prime. Suppose that $w(a,1)$ is p-equivalent to $v(a,1)$, where $\lambda_w(p) \equiv 2 \pmod 4$ and $p \nmid D$. Then*

$$E_w(p) = 2,\ h_w(p) \equiv 1 \pmod 2, \quad \textit{and} \quad h_w(p) \mid (p-(D/p))/2.$$

Moreover,

$$S_w(p) = \{0,1,2\},\ N_w(p) = h_w(p) + 1 = \frac{1}{2}\lambda_w(p) + 1,$$
$$B_w(0) = p - h_w(p) - 1, \quad B_w(1) = 2, \quad \textit{and} \quad B_w(2) = h_w(p) - 1.$$

This follows from Theorem 11 of [20] and from Theorem 3.6 of this paper.

Remark 6.7. It follows from Theorem 3.14 (i) that $v(a,1)$ is p-equivalent to $u(a,1)$ if $h_u(p)$ is even. This case is treated in Theorem 6.4.

Theorem 6.8. *Let p be a fixed prime. Suppose that $t(a,1)$ is defined and $w(a,1)$ is p-equivalent to $t(a,1)$, where $p \nmid D$. Then*

$$E_w(p) = 2,\ h_w(p) \equiv 0 \pmod 2, \quad \text{and} \quad h_w(p) \mid (p - (D/p))/2.$$

Further,

$$S_w(p) = \{0,2\},\ N_w(p) = h_w(p) = \lambda_w(p)/2,$$
$$B_w(0) = p - h_w(p), \quad \text{and} \quad B_w(2) = h_w(p).$$

This is proved in Theorem 3.8 (b) of [21].

Theorem 6.9. *Let p be a fixed prime. Suppose that $w(a,1)$ is p-regular and that $w(a,1)$ is not p-equivalent to $u(a,1)$, $v(a,1)$, or $t(a,1)$. Then*

$$h_w(p) \le (p-(D/p))/4, \quad h_w(p) \mid (p-(D/p))/2, \quad \text{and} \quad \lambda_w(p) \le (p-(D/p))/2. \tag{6.7}$$

Moreover,

$$S_w(p) = \{0,1\},\ N_w(p) = \lambda_w(p),\ B_w(0) = p - \lambda_w(p), \quad \text{and} \quad B_w(1) = \lambda_w(p). \tag{6.8}$$

Proof. We note that (6.7) follows from Theorems 3.15 (ii), 3.14 (i) and (ii), and Theorem 3.21. Moreover, (6.8) follows from the fact that $A_w(d) = 0$ or 1 for $0 \le d \le p-1$ by Theorem 6.1 (i). □

Theorems 6.10–6.14 consider more general recurrences than the recurrences $w(a,1)$ treated in Theorems 6.2–6.6, 6.8, and 6.9. In these theorems, as contrasted to our previous assumption, we allow the possibility that $p = 2$.

Theorem 6.10. *Let p be a fixed prime, possibly even. Let the recurrence (w) be either the first-order recurrence $w(a_1)$ defined by $w_{n+1} = a_1 w_1$, where $p \nmid a_1$ or the p-irregular second-order recurrence $w(a,b)$. Then*

$$S_w(p) = \{0,1\},\ N_w(p) = \lambda_w(p),\ B_w(0) = p - \lambda_w(p), \quad \text{and} \quad B_w(1) = \lambda_w(p).$$

Proof. This follows from the facts that $h_w(p) = 1$ and $A_w(0) = 0$ if $w_0 \not\equiv 0 \pmod p$. □

Theorem 6.11. *Let p be a fixed prime, possibly even. Consider the p-regular second-order recurrence $w(a,b)$ with discriminant D such that $p \mid D$. Then*

$$h_w(p) = p, \quad S_w(p) = \left\{\frac{\lambda_w(p)}{p}\right\}, \quad N_w(p) = p, \quad \text{and} \quad B_w\left(\frac{\lambda_w(p)}{p}\right) = p.$$

This is proved in [1] and [23].

Theorem 6.12. *Let p be a fixed prime, possibly even. Let $w(a_1,\dots,a_k)$ be p-equivalent to the kth-order unit sequence $u(a_1,\dots,a_k)$, where $k \ge 2$, $a_1 = a_2 = \cdots = a_{k-1} = 0$, $a_k = (-1)^{k+1}M$, and $p \nmid M$. Then*

$$h_w(p) = k, \quad M_u(p) \equiv M \pmod p, \quad \text{and} \quad E_w(p) = \mathrm{ord}_p M = \frac{\lambda_w(p)}{k}.$$

Moreover, the following hold:

(i) *If $k = 2$ and $M \equiv 1 \pmod p$, then*

$$N_w(p) = 2,$$
$$S_w(p) = \{1\} \quad \text{if } p = 2,$$
$$S_w(p) = \{0,1\} \quad \text{if } p > 2,$$
$$B_w(0) = p - N_w(p), \quad \text{and} \quad B_w(1) = 2.$$

(ii) *If it is not the case that* $k = 2$ *and* $M \equiv 1 \pmod{p}$, *then*

$$\begin{aligned}
N_w(p) &= \frac{\lambda_w(p)}{k} + 1, \\
S_w(p) &= \left\{0,\ 1,\ \frac{(k-1)\lambda_w(p)}{k}\right\} \quad \text{if } N_w(p) < p, \\
S_w(p) &= \left\{1,\ \frac{(k-1)\lambda_w(p)}{k}\right\} \quad \text{if } N_w(p) = p, \\
B_w(0) &= p - N_w(p), \quad B_w(1) = \frac{\lambda_w(p)}{k}, \quad \text{and} \quad B_w\left(\frac{(k-1)\lambda_w(p)}{k}\right) = 1.
\end{aligned}$$

Proof. By Theorem 3.6 (i), generalized to kth-order recurrences, it suffices to consider the case in which $w(a_1, \dots, a_k)$ is the kth-order unit sequence $u(a_1, \dots, a_k)$. By inspection, one sees that $u_n \equiv M^{i-1} \pmod{p}$ if $n = ki - 1$ for $i \geq 1$ and $u_n \equiv 0 \pmod{p}$ if $n \not\equiv -1 \pmod{k}$. The theorem now follows immediately. □

Theorem 6.13. *Let* p *be a fixed prime, possibly even. Let* $w(a_1, \dots, a_k)$ *be* p*-equivalent to the* k*th-order unit sequence* $u(a_1, \dots, a_k)$, *where* $k \geq 2$ *and* $a_i = (-1)^i$ *for* $i \in \{1, 2, \dots, k\}$. *Then*

$$h_w(p) = k + 1, \quad M_w(p) \equiv 1 \pmod{p}, \quad \text{and} \quad E_w(p) = 1.$$

Moreover, the following hold:

(i) *If* $p = 2$, *then*

$$\begin{aligned}
N_w(p) &= 2, \\
S_w(p) &= \{k-1, 2\}, \\
B_w(2) &= 2 \quad \text{if } k = 3 \\
B_w(k-1) = B_w(2) &= 1 \quad \text{if } k \neq 3.
\end{aligned}$$

(ii) *If* $p \geq 3$, *then*

$$\begin{aligned}
&N_w(p) = 3, \\
&S_w(p) = \{1, k-1\} \quad \text{if } p = 3, \\
&S_w(p) = \{0, 1, k-1\} \quad \text{if } p > 3, \\
&B_w(0) = p - 3 \quad \text{and} \quad B_w(1) = 3 \quad \text{if } k = 2, \\
&B_w(0) = p - 3, \quad B_w(1) = 2 \quad \text{and} \quad B_w(k-1) = 1 \qquad \text{if } k \geq 3.
\end{aligned}$$

Proof. It suffices to consider the case in which $w(a_1, \dots, a_k)$ is the kth-order unit sequence $u(a_1, \dots, a_k)$. By inspection, one sees that $u(a_1, \dots, a_k)$ is purely periodic with a period of $k + 1$ and that $u_0 = u_1 = \cdots = u_{k-2} = 0$, $u_{k-1} = 1$, and $u_k = -1$. The result now follows immediately. □

Theorem 6.14. *Let* p *be a fixed prime, possibly even. Let* $w(a_1, \dots, a_k)$ *be a recurrence such that* $k \geq 2$, $p \nmid a_k$, *and* $\lambda_w(p) = p^k - 1$. *Then*

$$h_w(p) = \frac{p^k - 1}{p - 1}, \quad E_w(p) = p - 1,$$
$$A_w(0) = p^{k-1} - 1, \quad \text{and} \quad A_w(d) = p^{k-1} \quad \text{if } d \not\equiv 0 \pmod{p}.$$

Moreover,

$$S_w(p) = \{p^{k-1} - 1, p^{k-1}\}, \quad N_w(p) = p,$$
$$B_w(p^{k-1} - 1) = 1, \quad \textit{and} \quad B_w(p^{k-1}) = p - 1.$$

This is proved in [9, p. 449].

Acknowledgement

The authors are indebted to the referee for careful reading and useful suggestions. 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] C. K. Caldwell, *Mersenne primes: history, theorems and lists*, `http://primes.utm.edu/mersenne/`.

[3] C. K. Caldwell, *The top twenty, Sophie Germain (p)*, `http://primes.utm.edu/top20/page.php?id=2`.

[4] C. K. Caldwell, *The top twenty, Cunningham chains (2nd kind)*, `http://primes.utm.edu/top20/page.php?id=20`.

[5] W. Carlip and L. Somer, *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, 1999, 691–719.

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

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

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

[9] R. Lidl and H. Niederreiter, *Finite fields*, Addison-Wesley, Reading, MA, 1983.

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

[11] H. Niederreiter, A. Schinzel, and L. Somer, *Maximal frequencies of elements in second-order linear recurring sequences over a finite field*, Elem. Math., **46** (1991), 139–143.

[12] L. Somer, *Fibonacci-like groups and periods of Fibonacci-like sequences*, The Fibonacci Quarterly, **15.1** (1977), 35–41.

[13] L. Somer, *The divisibility properties of primary Lucas recurrences with respect to primes*, The Fibonacci Quarterly, **18.4** (1980), 316–334.

[14] L. Somer, *Possible periods of primary Fibonacci-like sequences with respect to a fixed odd prime*, The Fibonacci Quarterly, **20.4** (1982), 311–333.

[15] L. Somer, *Primes having an incomplete system of residues for a class of second-order recurrences*, Applications of Fibonacci numbers, A. F. Horadam, A. N. Philippou, and G. E. Bergum (eds.), Kluwer Academic Publ., Dordrecht, 1988, 113–141.

[16] L. Somer, *Distribution of residues of certain second-order linear recurrences modulo p*, Applications of Fibonacci numbers, Vol. 3, G. E. Bergum, A. N. Philippou, and A. F. Horadam (eds.), Kluwer Academic Publ., Dordrecht, 1990, 311–324.

[17] L. Somer, *Distribution of certain second-order linear recurrences modulo p – II*, The Fibonacci Quarterly, **29.1** (1991), 72–78.

[18] L. Somer, *Periodicity properties of kth order linear recurrences with irreducible characteristic polynomial over a finite field*, Finite fields, coding theory and advances in communications and computing, G. L. Mullen and P. J.-S. Shiue (eds.), Marcel Dekker Inc., New York, 1993, 195–207.

[19] L. Somer, *Upper bounds for frequencies of elements in second-order recurrences over a finite field*, Applications of Fibonacci Numbers, Vol. 5, G. E. Bergum, A. N. Philippou, and A. F. Horadam (eds.), (St. Andrew, 1992), Kluwer Acad. Sci. Publ., Dordrecht, 1993, 527–546.

[20] L. Somer, *Distribution of residues of certain second-order linear recurrences modulo p – III*, Applications of Fibonacci numbers, vol. 6, G. E. Bergum, A. N. Philippou, and A. F. Horadam (eds.), Kluwer Academic Publ., Dordrecht, 1996, 451–471.

[21] L. Somer and W. Carlip, *Stability of second-order recurrences modulo p^r*, Int. J. Math. Math. Sci., **23** (2000), 225–241.

[22] L. Somer and M. Křížek, *Easy criteria to determine if a prime divides certain second-order recurrences*, The Fibonacci Quarterly, **51.1** (2013), 3–12.

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

MSC2010: 11B39, 11A07, 11A41

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

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