IDENTICALLY DISTRIBUTED SECOND-ORDER LINEAR RECURRENCES MODULO p, II

LAWRENCE SOMER AND MICHAL KŘÍŽEK

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 $u(a,1)$ satisfies the recursion relation $u_{n+2} = au_{n+1} + u_n$ with initial terms $u_0 = 0$ and $u_1 = 1$. Similar results are obtained for the companion Lucas sequences $v(a,1)$ and $v(a',1)$. We also explicitly determine the exact distribution of residues of $u(a,1) \pmod p$ when $u(a,1)$ has a maximal period modulo p.

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 $p \nmid b$. We will usually assume that $b = \pm 1$, which will automatically guarantee that $p \nmid b$. If $(m/p) = 1$, where (m/p) denotes the Legendre symbol, $\sqrt{m}$ modulo p will denote the residue c modulo p such that $c^2 \equiv m \pmod p$ and $0 \le c \le (p-1)/2$.

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 $n \ge 0$. 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 $n \ge 0$ 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.

The main result of the paper [21] 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, then $u(a_1, 1)$ and $u(a_2, 1)$ have the same distribution of residues modulo p. A similar result was proved for the LSSK's $v(a_1, 1)$ and $v(a_2, 1)$. With a little bit of extra effort, we can sharpen these results from [21] by also obtaining the conclusion that the actual residues modulo p occurring in $u(a_2, 1)$ are related to the residues modulo p appearing in $u(a_1, 1)$. Even more so, we will show that 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.

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 $w(a, b)$ and the LSFK $u(a, b)$. Let d be a fixed residue modulo p such that $0 \le d \le p - 1$. Let $g = \text{ord}_p(-b)$, where $\text{ord}_p(-b)$ denotes the multiplicative order of $(-b)$ modulo p. Then*

(i) $A_w(d) \le \min(2 \cdot \text{ord}_p(-b), p)$.
(ii) $A_u(0) = E_u(p) \le \min(p - 1, 2g)$ *and* $A_u(d) \le \min(g + E_u(p), 2g, p)$ *if* $d \ne 0$.
(iii) *If* $b = 1$ *then* $A_w(d) \le 4$.
(iv) *If* $b = 1$ *and* $E_u(p) = 1$*, then* $A_u(d) \le 3$.

Proof. Part (i) was proved in Theorem 3 of [12]. Part (ii) was proved in Theorem 2 of [19]. Parts (iii) and (iv) follow from parts (i) and (ii), respectively. □

We let

$$N_w(p) = \#\{d \,|\, A_w(d) > 0\}. \tag{1.4}$$

We define the set $S_w(p)$ by

$$S_w(p) = \{i \,|\, A_w(d) = i \text{ for some } d \text{ such that } 0 \le d \le p - 1\}. \tag{1.5}$$

Further, if i is a nonnegative integer, we define $B_w(i)$ by

$$B_w(i) = \#\{d \,|\, 0 \le d \le p - 1 \text{ and } A_w(d) = i\}. \tag{1.6}$$

We observe by Theorem 1.1 that

$$B_w(i) = 0 \quad \text{if } i > \min(2 \cdot \text{ord}_p b, p). \tag{1.7}$$

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 the two recurrences $w(a_1, b)$ and $w'(a_2, b)$ are identically distributed modulo p, it suffices by relation (1.7) to prove that $B_w(i) = B_{w'}(i)$ for all $i \in \{0, \dots, \ell\}$, where $\ell = \min(2 \cdot \text{ord}_p(-b), p)$. This follows, since

$$N_w(p) = \sum_{i=1}^{\ell} B_w(i) \tag{1.8}$$

and

$$S_w(p) = \{i \,|\, B_w(i) > 0\}. \tag{1.9}$$

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*

$$\begin{vmatrix} w_0 & w_1 \\ w_1 & w_2 \end{vmatrix} = w_0w_2 - w_1^2 \not\equiv 0 \pmod{p}. \tag{1.10}$$

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*

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

This is proved in [5, 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 $p \nmid D$.*
(iii) *If $w(a,b)$ is a recurrence for which $h_w(p) = 1$, then $w(a,b)$ is p-irregular.*

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 (1.10).

(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 and only if $p \nmid D$.

(iii) If $w(a,b)$ were to be p-regular, then $h_w(p) = h_u(p)$ by Theorem 1.3 and part (i) of this theorem. However, $h_u(p) \geq 2$, since $u_0 = 0$ and $u_1 = 1$. □

Theorem 1.5. *Let p be a fixed prime. Consider the p-regular recurrence $w(a,b)$ with discriminant D and characteristic roots $\alpha = (a + \sqrt{D})/2$ and $\beta = (a - \sqrt{D})/2$. Let $h = h_w(p)$ and $\lambda = \lambda_w(p)$. Let P be a prime ideal in $\mathbb{Q}(\sqrt{D})$ lying over 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 $\lambda \mid p - 1$.*
(vi) *If $p \nmid D$, then $\lambda = \text{lcm}(\text{ord}_P\alpha, \text{ord}_P\beta)$, where $\text{ord}_P\alpha$ denotes the multiplicative order of α modulo P.*

Proof. We first note that by Theorem 1.3 and Theorem 1.4 (i) and (iii), $h_w(p) > 1$, $h_w(p) = h_u(p)$, 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 [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 (vi) is proved in Theorem 6 (i) of [14] and Theorem 8.44 of [9]. □

If the p-irregular recurrence $w(a,b)$ is not the trivial recurrence modulo p, then $(D/p) = 0$ or 1 and we can consider α and β to be in $\mathbb{Z}_p$, the ring of integers modulo p.

Theorem 1.6. *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 $n \geq 0$ and $w(a,b)$ is the trivial recurrence modulo p.*
(ii) *If $w_0 \not\equiv 0 \pmod{p}$, then either $w_n \equiv \alpha^n w_0 \pmod{p}$ or $w_n \equiv \beta^n w_0 \pmod{p}$ for all $n \geq 0$.*
(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 1.7. *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*

$$w'_n \equiv cw_{n+r} \pmod{p} \quad \text{for all } n \geq 0. \tag{1.11}$$

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 (1.11) holds, then

$$A_{w'}(cd) = A_w(d) \tag{1.12}$$

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

Theorem 1.8. *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*

(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 $d \in \{0, \ldots, p-1\}$. □

Theorem 1.9. *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 1.7, 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 1.10. *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].

Theorem 1.11. *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 $m \neq 1$.*
(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 $m \neq 1$.*

(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* $m \nmid (p+1)/2$.

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

Proof. Parts (i) and (ii) follow from Theorem 12 of [15]. Parts (iii) and (iv) follow from Theorems 3 and 4 of [18]. Part (v) is proved in Theorems 3.7, 3.8, and 3.12 of [11]. □

The principal results of the paper [21] are given below.

Theorem 1.12. *Let* p *be a fixed prime. Let* $(u) = (a_1, 1)$ *and* $(u') = u(a_2, 1)$ *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 1.13. *Let* p *be a fixed prime. Let* $(v) = v(a_1, 1)$ *and* $(v') = v(a_2, 1)$ *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.

In the next section presenting the principal results of this paper in addition to the previously mentioned results refining Theorems 1.12 and 1.13, we will show that if $w(a,1)$ is a p-regular recurrence having a maximal restricted period modulo p, then we can explicitly determine the distribution of $w(a,b)$ modulo p.

2. The 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 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 not only are* (u) *and* (u') *identically distributed modulo* p, *but there exists an integer* c *such that*

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

where

$$c \equiv \begin{cases} \varepsilon\sqrt{D_1D_2^{-1}} \pmod p, & \text{if } h \equiv 2 \pmod 4; \\ \sqrt{D_1D_2^{-1}} \pmod p, & \text{if } h \not\equiv 2 \pmod 4, \end{cases}$$

for some $\varepsilon = \pm 1$.

In the case $h \not\equiv 2 \pmod 4$, *we may also choose* $c \equiv M^k\sqrt{D_1D_2^{-1}} \pmod p$, *where* k *is any integer and* M *is the multiplier* $M_u(p)$.

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 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 not only are* (v) *and* (v') *identically distributed modulo* p, *but*

$$A_{v'}(d) = A_v(d) \quad \text{for all } d \in \{0,1,\ldots,p-1\}. \tag{2.2}$$

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

$$A_{v'}(d) = A_v(M^k d) \quad \text{for all } d \in \{0,1,\ldots,p-1\}, \tag{2.3}$$

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

In Theorems 2.4, 2.6, and 2.7, we will sharpen Theorems 1.12, 1.13, 2.1, and 2.2 for p-regular recurrences having a maximal restricted period modulo p equal to $p-(D/p)$. Theorems 1.12 and 2.1 show 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 Theorems 1.13 and 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 recurrences (w) with a maximal restricted period modulo p, we will be able to explicitly determine $S_w(p)$, $N_w(p)$, and $B_w(i)$ for $i \geq 0$ given only the restricted period of (w) modulo p and also possibly the quadratic character of the discriminants of these recurrences modulo p. First, we present Proposition 2.3 which gives a relation between p-regular recurrences $w(a,b)$ having a maximal restricted period modulo p and the LSFK $u(a,b)$.

Proposition 2.3. *Let $w(a,b)$ be a p-regular recurrence with discriminant D. Suppose that $h_w(p) = p-(D/p)$. Then $w(a,b)$ is p-equivalent to $u(a,b)$. In particular,*

$$A_w(0) \geq 1. \tag{2.4}$$

Proof. By Theorem 1.10 and Theorem 1.8 (i), there exists exactly one class of regular p-equivalent recurrences. The result now follows upon application of Theorem 1.4 (i). □

Theorem 2.4. *Suppose that $w(a,1)$ is a p-regular recurrence such that $(D/p) = -1$ and $h_w(p) = p+1$. Then $p \equiv 3 \pmod 4$ and $(-D/p) = 1$. Consider the LSFK $u(a,1)$. Then $h_u(p) = h_w(p) = p+1$, $E_u(p) = E_w(p) = 2$, $M_u(p) \equiv M_w(p) \equiv -1 \pmod p$, and $\lambda_u(p) = \lambda_w(p) = 2p+2$. Moreover, there exists a nonzero residue c modulo p such that $w_n \equiv cu_{n+r} \pmod p$ for all n and some fixed integer r such that $0 \leq r \leq 2p+1$, where we can take $c \equiv 1 \pmod p$ and $r = 0$ if $w_n(a,1) \equiv u_n(a,1) \pmod p$ for all $n \geq 0$. Then the following hold:*

(i) *If $p = 3$, then $S_w(p) = \{2,3\}$ while if $p \equiv 3 \pmod 8$ and $p > 3$, then $S_w(p) = \{0,2,3,4\}$. Moreover, if $p \equiv 3 \pmod 8$ and $p \geq 3$, then*

$$N_w(p) = \frac{3p+3}{4}, \quad B_w(0) = \frac{p-3}{4}, \quad B_w(2) = \frac{p-1}{2}, \quad B_w(3) = 2, \quad B_w(4) = \frac{p-3}{4}.$$

(ii) *If $p = 7$ then $S_w(p) = \{1,2,4\}$, whereas if $p > 7$ then $S_w(p) = \{0,1,2,4\}$. Further, if $p \equiv 7 \pmod 8$ and $p \geq 7$, then*

$$N_w(p) = \frac{3p+7}{4}, \quad B_w(0) = \frac{p-7}{4}, \quad B_w(1) = 2, \quad B_w(2) = \frac{p-1}{2}, \quad B_w(4) = \frac{p+1}{4}.$$

(iii) *$A_w(d) = A_w(-d)$.*

(iv) *$A_w(d) \in \{1,3\}$* if and only if *$d \equiv \pm 2c/\sqrt{-D} \pmod p$.*

(v) *$A_w(0) = 2$.*

(vi) *If $p > 3$ and $a \equiv \pm 1 \pmod p$, then $A_w(c) = A_w(-c) = 4$.*

(vii) *If $p \equiv 3 \pmod 8$ then $A_w(2c/\sqrt{-D}) = A_w(-2c/\sqrt{-D}) = 3$.*

(viii) *If $p \equiv 7 \pmod 8$ then $A_w(2c/\sqrt{-D}) = A_w(-2c/\sqrt{-D}) = 1$.*

Proof. By Theorems 1.3, 1.4 (i), and 1.8 and by Proposition 2.3, it suffices to consider the case in which $w(a,b) = u(a,b)$. The rest of the theorem now follows from the proofs of Theorems 7 and 8 in [17]. □

Remark 2.5. It follows from Theorems 1.3, 1.4 (i), 1.10, and 1.11 (v) that if $p \equiv 3 \pmod 4$, then there exist exactly $\phi(p+1)$ parameters a, $0 \leq a \leq p-1$, such that $((a^2+4)/p) = -1$ and any p-regular recurrence $w(a,1)$ has a maximal restricted period $h_w(p) = p+1$.

Let $p = 2^q - 1$ be a Mersenne prime, where q is a prime. Then clearly $p \equiv 3 \pmod 4$. Let $w(a,1)$ be any p-regular recurrence with discriminant $D = a^2+4$ such that $(D/p) = -1$. Then by Theorem 1.5 (i) and (iii), $h_w(p) = p+1$. At present there are 49 known Mersenne primes (see [2]) with the largest being $2^{74207281} - 1$ with 22338618 digits.

Theorem 2.6. *Suppose that $w(a,1)$ is a p-regular recurrence such that $p \mid D$. Then $p \equiv 1 \pmod 4$ and $a \equiv \pm\sqrt{-4} \pmod p$. Further,*

$$h_w(p) = p, \quad E_w(p) = 4, \quad \text{and} \quad \lambda_w(p) = 4p. \tag{2.5}$$

Moreover,

$$A_w(d) = 4 \quad \textit{for all } d \in \{0, 1, \ldots, p-1\} \tag{2.6}$$

and

$$S_w(p) = \{4\}, \quad N_w(p) = p, \quad B_w(4) = p, \quad \text{and} \quad B_w(i) = 0 \quad \text{if} \quad i \neq 4. \tag{2.7}$$

Proof. The results in (2.5) follow from Theorem 1.5 (ii) and Theorem 3.11 (iv) which is given in Section 3. The results in (2.6) and (2.7) are proved in [1] and [22]. It is clear that $a \equiv \pm\sqrt{-4} \pmod p$, since $D = a^2 + 4 \equiv 0 \pmod p$. By the law of quadratic reciprocity, $p \equiv 1 \pmod 4$. □

Theorem 2.7. *Suppose that $w(a,1)$ is a p-regular recurrence such that $(D/p) = 1$ and $h_w(p) = p-1$. Then $p \equiv 3 \pmod 4$. Consider the LSFK $u(a,1)$. Then*

$$h_u(p) = h_w(p) = p-1, \quad E_u(p) = E_w(p) = 1,$$
$$M_u(p) \equiv M_w(p) \equiv 1 \pmod p, \quad \text{and} \quad \lambda_u(p) = \lambda_w(p) = p-1. \tag{2.8}$$

Furthermore, there exists a nonzero residue c modulo p such that $w_n \equiv cu_{n+r} \pmod p$ for all n and some fixed integer r such that $0 \le r \le p-2$, where we can take $c \equiv 1 \pmod p$ and $r = 0$ if $w_n(a,1) \equiv u_n(a,1) \pmod p$ for all $n \ge 0$. Then the following hold:

- (i) *If $p = 3$, then $S_w(p) = \{0,1\}$, while if $p \equiv 3 \pmod 8$ and $p > 3$, then $S_w(p) = \{0,1,2,3\}$, $N_w(p) = (5p+1)/8$, $B_w(0) = (3p-1)/8$, $B_w(1) = (3p+7)/8$, $B_w(2) = (p-3)/8$, and $B_w(3) = (p-3)/8$.*
- (ii) *If $p = 7$ then $S_w(p) = \{0,1,2\}$, while if $p \equiv 7 \pmod 8$ and $p > 7$, then $S_w(p) = \{0,1,2,3\}$. Moreover, if $p \equiv 7 \pmod 8$ and $p \ge 7$, then*

$$N_w(p) = \frac{5p-3}{8}, \quad B_w(0) = \frac{3p+3}{8}, \quad B_w(1) = \frac{3p-5}{8}, \quad B_w(2) = \frac{p+9}{8}, \quad B_w(3) = \frac{p-7}{8}.$$

- (iii) *$A_w(d) + A_w(-d) \in \{1,3\}$ if $d \equiv \pm 2c/\sqrt{D} \pmod p$.*
- (iv) *$A_w(d) + A_w(-d) \in \{0,2,4\}$ if $d \not\equiv \pm 2c/\sqrt{D} \pmod p$.*
- (v) *$A_w(0) = 1$.*
- (vi) *If $a \equiv \pm 1 \pmod p$, then $A_w(c) = 3$ and $A_w(-c) = 1$.*
- (vii) *If $A_w(d) + A_w(-d) = 4$ then $A_w(d) \in \{1,3\}$.*
- (viii) *If $p \equiv 3 \pmod 8$ then $A_w(2c/\sqrt{D}) \in \{0,1\}$ and $A_w(-2c/\sqrt{D}) = 1 - A_w(2c\sqrt{D})$.*
- (ix) *If $p \equiv 7 \pmod 8$, then $A_w(2c/\sqrt{D}) \in \{1,2\}$ and $A_w(-2c/\sqrt{D}) = 3 - A_w(2c\sqrt{D})$.*

The proof of Theorem 2.7 will be given in Section 4.

Remark 2.8. We see by Theorems 1.3, 1.4 (i), 1.10, and 1.11 (v) that if $p \equiv 3 \pmod 4$, then there exist exactly $\phi(p-1)$ parameters a, $0 \le a \le p-1$ for which $((a^2+4)/p) = 1$ and any p-regular recurrence $w(a,1)$ has a maximal restricted period modulo p equal to $p-1$. Primes q such that $2q+1$ is also prime are called Sophie Germain primes. It is easily seen that if q is an odd Sophie Gemain prime, then $2q+1 \equiv 3 \pmod 4$. Let q be an odd Sophie Germain prime and let $p = 2q+1$. Suppose that $a \not\equiv 0 \pmod p$ and $w(a,1)$ is a p-regular recurrence with discriminant $D = a^2 + 4$ such that $(D/p) = 1$. Then by Theorem 1.5 (i) and (iii), $h_w(p) = p - 1$.

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

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

According to [3], the largest known Sophie Germain prime is $18543637900515 \cdot 2^{666667} - 1$ with 200701 digits.

3. Preliminaries

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

Theorem 3.1. *Let p be a fixed prime. Let a and b be integers such that $p \nmid b$. Define the relation p-equivalence on the set of all nontrivial p-irregular recurrences $w(a, b)$ modulo p. Let $D = a^2 + 4b$. Let α and β be the characteristic roots of the characteristic polynomial*

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

Let $H(p)$ denote the number of equivalence classes.

(i) *If $(D/p) = -1$, then $H(p) = 0$.*
(ii) *If $(D/p) = 1$, then $H(p) = 2$. Moreover, the recurrence $w(a, b)$ having initial terms $w_0 \equiv 1$, $w_1 \equiv \alpha \pmod{p}$ is in one equivalence class, while the recurrence $w'(a, b)$ having initial terms $w'_0 \equiv 1$, $w'_1 \equiv \beta \pmod{p}$ is in the other equivalence class.*
(iii) *If $(D/p) = 0$, then $H(p) = 1$. Furthermore, the recurrence $w''(a, b)$ having initial terms $w''_0 \equiv 1$, $w''_1 \equiv \alpha \pmod{p}$ is in the unique equivalence class.*

This follows from Lemma 2.4 of [5].

Theorem 3.2. *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].

Theorem 3.3. *Let p be a fixed prime. Let $w(a, b)$ be a p-regular recurrence with restricted period $h = h_w(p)$ and let $w'(a, b)$ be a nontrivial recurrence modulo p (possibly p-irregular) with restricted period $h' = h_{w'}(p)$. Let c be a fixed integer such that $1 \le c \le h - 1$. Then there exist integers n_1 and n_2 such that*

$$\frac{w_{n_1+c}}{w_{n_1}} \equiv \frac{w'_{n_2+c}}{w'_{n_2}} \pmod{p}$$

if and only if $w(a, b)$ and $w'(a, b)$ are p-equivalent, where we allow the possibility that $w_{n_1+c}/w_{n_1} \equiv w'_{n_2+c}/w'_{n_2} \equiv \infty \pmod{p}$.

This follows from Lemma 3.4 of [5].

Lemma 3.4. *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 $0 \le n \le h$.*
(ii) *$v_{h-n} \equiv Mv_n/(-b)^n \pmod{p}$ for $0 \le n \le h$.*

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

Lemma 3.5. *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*

$$w_{n+2r} \not\equiv \varepsilon w_n \pmod{p} \tag{3.1}$$

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

$$w_{n+2r} \not\equiv \varepsilon w_n \pmod{p} \tag{3.2}$$

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

This follows from Lemmas 2 and 5 of [19], Lemma 7 (i) and (ii) of [16], and Lemma 7 of [20].

Proposition 3.6. *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) *$v_n^2 - Du_n^2 = 4(-b)^n$.*
(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 3.7. *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 $D' = Du_k^2(a,b)$.

Proofs of Theorem 3.7 are given in [10, pp. 189–190] and [8, p. 437].

Lemma 3.8. *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 $n \ge 0$,*
(ii) *$v_n(-a,b) = (-1)^n v_n(a,b)$ for $n \ge 0$.*
(iii) *If h_1 and h_2 are the restricted periods of $u(a,b)$ and $u(-a,b)$, respectively, then $h_1 = h_2$.*

Proof. Parts (i) and (ii) follow from the Binet formulas (1.3). Part (iii) follows from Theorem 1.5 (iv) and part (i) of this lemma. □

Lemma 3.9. *Let p be a fixed prime and let $w(a,b)$ be a p-regular recurrence. Let $M = M_w(p)$. Then*

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

This follows from the proof of Lemma 10 of [17] and Lemma 13 of [19].

Theorem 3.10. *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 3.6 (iv), $v_{h/2} \equiv 0 \pmod p$ when h is even. Then

$$v_{h/2} \equiv v_{h/2+1} \cdot u_0 \equiv v_{h/2+1} \cdot 0 \equiv 0 \pmod p \tag{3.3}$$

and

$$v_{h/2+1} \equiv v_{h/2+1} \cdot u_1 \equiv v_{h/2+1} \cdot 1 \equiv v_{h/2+1} \pmod p. \tag{3.4}$$

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

Theorem 3.11. *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 [14]. □

Lemma 3.12. *Let p be a fixed prime. Consider the recurrences $w(a,1)$ and $w'(-a,1)$, where either $w(a,1)$ and $w'(-a,1)$ are the LSFK's $u(a,1)$ and $u(-a,1)$, respectively, or they are the LSSK's $v(a,1)$ and $v(-a,1)$, respectively. Then*

$$A_{w'}(d) = A_w(d) \tag{3.5}$$

for $0 \le d \le p-1$, and $w(a,1)$ and $w'(-a,1)$ are identically distributed modulo p.

This follows from the proof of Lemma 3.18 in [21].

Lemma 3.13. *Let $u(a,1)$ be a LSFK. Suppose that $h = h_u(p) \equiv 2 \pmod 4$. Then $E_u(p) = 1$ and $M_u(p) \equiv 1 \pmod p$.*

(i) Suppose that $u_{n+2r-1} \equiv \pm u_n \pmod p$, where n and r integers such that $1 \le n < n + 2r - 1 < h/2$. Then the only values of $2s-1$ and m such that $1 \le 2s-1 \le h-1$, $1 \le m \le h-1$, $u_m \equiv \pm u_n \pmod p$, and $u_{m+2s-1}/u_m \equiv \pm 1 \pmod p$ are

$$2s - 1 = 2r - 1, \quad m = n \quad \text{or} \quad m = h - n - 2r + 1, \tag{3.6}$$

$$2s - 1 = h - 2r + 1, \quad m = n + 2r - 1 \quad \text{or} \quad m = h - n, \tag{3.7}$$

$$2s - 1 = h - 2n - 2r + 1, \quad m = n \quad \text{or} \quad m = n + 2r - 1, \tag{3.8}$$

$$2s - 1 = 2n + 2r - 1, \quad m = h - n - 2r + 1 \quad \text{or} \quad m = h - n. \tag{3.9}$$

(ii) Suppose that $u_{h/2} \equiv \pm u_n \pmod p$, where $1 \le n < h/2$ and $h/2 = n + 2r - 1$ for some positive integer r. Then the only values of $2s-1$ and m such that $1 \le 2s-1 \le h-1$, $1 \le m \le h-1$, $u_m \equiv \pm u_n \pmod p$, and $u_{m+2s-1}/u_m \equiv \pm 1 \pmod p$ are

$$2s - 1 = 2r - 1, \quad m = n \quad \text{or} \quad m = h/2, \tag{3.10}$$

$$2s - 1 = h - 2r + 1, \quad m = h/2 \quad \text{or} \quad m = h/2 + 2r - 1. \tag{3.11}$$

Proof. (i) It follows from Theorem 3.11 (ii) that $E_u(p) = 1$ and $M_u(p) \equiv 1 \pmod p$. Moreover, we see by Lemma 3.5 that if $u_e \equiv \pm u_g \pmod p$ and $u_e \equiv \pm u_n \pmod p$, where $1 \le e < g < h/2$, then $e = n$ and $g = n + 2r - 1$. It now follows from the fact that $M_u(p) \equiv 1 \pmod p$ and from Lemma 3.4 (i) that the only values for $2s - 1$ and m are the ones listed in (3.6)–(3.9).

(ii) This follows by an argument similar to that used in the proof of part (i). □

4. Proofs of the Main Theorems

Proof of Theorem 2.1. Let $h = h_u(p)$, $h_1 = h_{u'}(p)$, $\lambda = \lambda_u(p)$, and $\lambda_1 = \lambda_{u'}(p)$. By hypothesis, $(D_1/p) = (D_2/p)$, $p \nmid D_1 D_2$, and $h = h_1$. By Theorem 3.11 (i)–(iv), it then follows that $\lambda = \lambda_1$.

Let $p - (D_1/p) = 2^i m$. By Theorem 1.5,

$$h = h_1 = 2^j m_1 \tag{4.1}$$

for some j and m such that $0 \le j \le i$ and $m_1 \mid m$. Let $r = m/m_1$. By Theorem 1.11, 1.4(i), and 1.3, there exists a LSFK $(u'') = u(a_3, 1)$ and LSSK $(v'') = v(a_3, 1)$ with discriminant $D_3 = a_3^2 + 4$ such that $(D_3/p) = (D_1/p) = (D_2/p)$ and

$$h_{u''}(p) = h_{v''}(p) = 2^j m = rh = rh_1. \tag{4.2}$$

Let $\lambda_2 = \lambda_{u''}(p)$. Then by Theorem 3.11,

$$\lambda_2 = \lambda_{v''}(p) = r\lambda = r\lambda_1. \tag{4.3}$$

By (4.3) and the proof of Theorem 2.1 in [21], there exist odd integers k and ℓ such that $1 \le k, \ell \le 2^{j-1} m$ if $j \ge 1$, $1 \le k, \ell \le m - 2$ if $j = 0$,

$$\gcd(k, \lambda_2) = \gcd(\ell, \lambda_2) = r = \frac{\lambda_2}{\lambda}, \tag{4.4}$$

and

$$v_k(a_3, 1) \equiv \varepsilon_1 a_1, \quad v_\ell(a_3, 1) \equiv \varepsilon_2 a_2 \pmod p \tag{4.5}$$

for some ε_1 and $\varepsilon_2 \in \{-1, 1\}$. Then by (4.5) and Theorem 3.7,

$$u_n(\varepsilon_1 a_1, 1) \equiv u_n(v_k(a_3, 1), 1) = \frac{u_{kn}(a_3, 1)}{u_k(a_3, 1)} \pmod p \tag{4.6}$$

and

$$u_n(\varepsilon_2 a_2, 1) \equiv u_n(v_\ell(a_3, 1), 1) = \frac{u_{\ell n}(a_3, 1)}{u_\ell(a_3, 1)} \pmod p \tag{4.7}$$

for all $n \ge 0$. Since $u(a_1, 1)$ and $u(a_2, 1)$ both have periods modulo p equal to λ, it follows from Lemma 3.8 (iii) and Theorem 3.11 (i)–(iv) that $u(\varepsilon_1 a_1, 1)$ and $u(\varepsilon_2 a_2, 1)$ also have periods modulo p equal to λ. It now follows from (4.4) that the sets

$$\{kn\}_{n=1}^{\lambda} \quad \text{and} \quad \{\ell n\}_{n=1}^{\lambda} \tag{4.8}$$

contain the same sets of residues modulo λ_2. It thus follows that the sets

$$\{u_{kn}(a_3, 1)\}_{n=1}^{\lambda} \quad \text{and} \quad \{u_{\ell n}(a_3, 1)\}_{n=1}^{\lambda} \tag{4.9}$$

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 by Theorem 1.5 (iv), it follows from (4.6), (4.7), (4.9), and the fact that both $(\hat{u}) = u(\varepsilon_1 a_1, 1)$ and $(\tilde{u}) = u(\varepsilon_2 a_2, 1)$ have periods modulo p equal to λ_1 that

$$A_{\tilde{u}}(d) = A_{\hat{u}}(u''_k (u''_\ell)^{-1} d) \tag{4.10}$$

for $0 \le d \le p-1$. Since $A_{\hat{u}}(d) = A_u(d)$ and $A_{\tilde{u}}(d) = A_{u'}(d)$ for $0 \le d \le p-1$ by Lemma 3.12, we have by (4.10) that

$$A_{u'}(d) = A_u(u''_k(u''_\ell)^{-1}d) \tag{4.11}$$

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

By Proposition 3.6 (iii),

$$(v''_k)^2 - D_3(u''_k)^2 = 4(-1)^k = -4 \tag{4.12}$$

and

$$(v''_\ell)^2 - D_3(u''_\ell)^2 = 4(-1)^\ell = -4. \tag{4.13}$$

Noting that $p \nmid D_3 u''_k u''_\ell$, we see by (4.5), (4.12), and (4.13) that

$$\frac{D_3(u''_k)^2}{D_3(u''_\ell)^2} \equiv \frac{(v''_k)^2+4}{(v''_\ell)^2+4} \equiv \frac{a_1^2+4}{a_2^2+4} \equiv \frac{D_1}{D_2} \equiv \frac{(u''_k)^2}{(u''_\ell)^2} \pmod{p}. \tag{4.14}$$

Thus, by (4.14),

$$u''_k(u''_\ell)^{-1} \equiv \varepsilon\sqrt{D_1 D_2^{-1}} \pmod{p} \tag{4.15}$$

for some $\varepsilon \in \{-1, 1\}$. Therefore, by (4.11), (4.15), and Lemma 3.9,

$$A_{u'}(d) = A_u(\varepsilon\sqrt{D_1D_2^{-1}}d) = A_u(M^k\varepsilon\sqrt{D_1D_2^{-1}}d) = A_u(d) \tag{4.16}$$

for $0 \le d \le p-1$ and any integer k. We note from Theorem 3.11 (i)–(iv) that $M^k \equiv -1 \pmod{p}$ for some integer k if and only if $h \not\equiv 2 \pmod{4}$. The result now follows. □

Proof of Theorem 2.2. Since $p \nmid D_1D_2$, both $(v) = v(a_1, 1)$ and $(v') = v(a_2, 1)$ are p-regular by Theorem 1.4 (ii). Consider the LSFK's $(u) = u(a_1, 1)$ and $(u') = u(a_2, 1)$. Then by Theorem 1.3 and Theorem 1.4 (ii),

$$h_u(p) = h_v(p) \quad \text{and} \quad h_{u'}(p) = h_{v'}(p). \tag{4.17}$$

By hypothesis, $h_v(p) = h_{v'}(p)$. It now follows from Theorem 3.11 (i)–(iv) that $\lambda_v(p) = \lambda_{v'}(p)$. Let $\lambda_1 = \lambda_v(p)$. As in the proof of Theorem 2.1, let $p - (D_1/p) = 2^i m$. By Theorem 1.5

$$h_v(p) = h_{v'}(p) = 2^j m_1 \tag{4.18}$$

for some j and some m_1 such that $0 \le j \le i$ and $m_1 \mid m$. Let $r = m/m_1$. By Theorems 1.11, 1.4 (ii), and 1.3, there exists a LSSK $(v'') = v(a_3, 1)$ with discriminant $D_3 = a_3^2 + 4$ such that $(D_3/p) = (D_1/p) = (D_2/p)$ and having restricted period $h_{v''}(p)$ for which

$$h_{v''}(p) = 2^j m = r h_v(p). \tag{4.19}$$

Then by Theorem 3.11,

$$\lambda_{v''}(p) = r\lambda_v(p). \tag{4.20}$$

Let $\lambda_2 = \lambda_{v''}(p)$. By (4.20) and the proof of Theorem 2.2 in [21] there exist odd integers k and ℓ such that $1 \le k, \ell \le 2^{j-1}m$ if $j \ge 1$, $1 \le k, \ell \le m-2$ if $j = 0$,

$$\gcd(k, \lambda_2) = \gcd(\ell, \lambda_2) = r = \frac{\lambda_2}{\lambda}, \tag{4.21}$$

and

$$v_k(a_3, 1) \equiv \varepsilon_1 a_1, \quad v_\ell(a_3, 1) \equiv \varepsilon_2 a_2, \pmod{p} \tag{4.22}$$

for some $\varepsilon_1, \varepsilon_2 \in \{-1, 1\}$. Then by (4.22) and Theorem 3.7,

$$v_n(\varepsilon_1 a_1, 1) \equiv v_n(v_k(a_3, 1), 1) = v_{kn}(a_3, 1) \pmod{p} \tag{4.23}$$

and

$$v_n(\varepsilon_2 a_2, 1) \equiv v_n(v_\ell(a_3, 1), 1) = v_{\ell n}(a_3, 1) \pmod{p} \tag{4.24}$$

for all $n \geq 0$. Let $(v'') = v(a_3, 1)$, $\hat{v} = v(\varepsilon_1 a, 1)$, and $\tilde{v} = v(\varepsilon_2 a, 1)$.

Since $v(a_1, 1)$ and $v(a_2, 1)$ both have periods equal to λ, it follows from Lemma 3.8 (iii), Theorem 1.4 (ii), Theorem 1.3, and Theorem 3.11 (i)–(iv) that $v(\varepsilon_1 a_1, 1)$ and $v(\varepsilon_2 a_2, 1)$ also have periods equal to $\lambda_v(p)$. It now follows from (4.21) that the sets

$$\{kn\}_{n=1}^{\lambda} \quad \text{and} \quad \{\ell n\}_{n=1}^{\lambda} \tag{4.25}$$

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

$$\{v_{kn}(a_3, 1)\}_{n=1}^{\lambda} \quad \text{and} \quad \{v_{\ell n}(a_3, 1)\}_{n=1}^{\lambda} \tag{4.26}$$

contain the same sets of residues modulo p. Since both the LSSK's

$$v(\varepsilon_1 a_1, 1) \equiv \{v_{kn}(a_3, 1)\}_{n=0}^{\infty} \pmod{p} \tag{4.27}$$

and

$$v(\varepsilon_2 a_2, 1) \equiv \{v_{\ell n}(a_3, 1)\}_{n=0}^{\infty} \pmod{p} \tag{4.28}$$

have periods modulo p equal to λ, it follows from (4.26)–(4.28) that

$$A_{\tilde{v}}(d) = A_{\hat{v}}(d) \tag{4.29}$$

for $0 \leq d \leq p-1$. Moreover, by Lemma 3.12,

$$A_{\hat{v}}(d) = A_v(d) \quad \text{and} \quad A_{\tilde{v}}(d) = A_{v'}(d) \tag{4.30}$$

for $0 \leq d \leq p-1$. We now see from (4.29) and (4.30) that equation (2.2) holds. Equation (2.3) now follows from Lemma 3.9. □

Proof of Theorem 2.7. By Theorems 1.3, 1.4 (i), and 1.11, there exists a p-regular recurrence $w(a, 1)$ with restricted period $h_w(p) = p-1$. As in the proof of Theorem 2.4, we can assume that $w(a, 1) = u(a, 1)$, and thus, $c \equiv 1 \pmod{p}$. By Theorem 1.5 (iii), $p \equiv 3 \pmod{4}$. We note that (2.7) follows from Theorem 3.11 (ii). Moreover, by Theorem 1.5 (iv) and the fact that $E_u(p) = 1$, we see that $A_u(0) = 1$, and part (v) is established.

We now prove parts (iii), (iv), (vi), and (vii). Let $h = h_u(p) = p-1$. By Lemma 3.4 (i),

$$u_{h-n} \equiv (-1)^{n+1} u_n \pmod{n} \tag{4.31}$$

for $0 \leq n \leq h/2$. Moreover, by Lemma 3.5, if $0 \leq m < n \leq h/2$ and $m \equiv n \pmod{2}$, then

$$u_m \not\equiv \pm u_n \pmod{p}. \tag{4.32}$$

Now suppose that $1 \leq m \leq h/2$ and there does not exist an integer $n \neq m$ such that $1 \leq n \leq h/2$ and $u_n \equiv \pm u_m \pmod{p}$. If m is odd and $m \neq h/2$, then by (4.31) and the fact that $E_u(p) = 1$,

$$A(u_m) = 2 \quad \text{and} \quad A(-u_m) = 0, \tag{4.33}$$

while if $m = h/2$, then

$$A(u_m) = 1 \quad \text{and} \quad A(-u_m) = 0. \tag{4.34}$$

If m is even, then by (4.31),

$$A(u_m) = A(-u_m) = 1. \tag{4.35}$$

Next we suppose that for a given integer m such that $1 \leq m \leq h/2$, there exists an integer $n \neq m$ such that $1 \leq n \leq h/2$ and $u_n \equiv \pm u_m \pmod{p}$. By (4.32) and the pigeonhole principle, there exists exactly one such n and $n \not\equiv m \pmod{2}$. Thus, we can assume that m is odd and n is even. Then by (4.31), we find that if $1 \leq m < h/2$, then

$$A(u_m) = 3 \quad \text{and} \quad A(-u_m) = 1, \tag{4.36}$$

while if $m = h/2$, then

$$A(u_m) = 2 \quad \text{and} \quad A(-u_m) = 1, \tag{4.37}$$

We now determine $u_{h/2} \pmod p$. We observe by Theorem 1.5 (iv) and Proposition 3.6 (ii) that $u_h = u_{h/2}v_{h/2} \equiv 0 \pmod p$. Since $u_{h/2} \not\equiv 0 \pmod p$ by Proposition 1.5 (iv), we find that $v_{h/2} \equiv 0 \pmod p$. We now see by Proposition 3.6 (iii) that

$$v_{h/2}^2 - Du_{h/2}^2 \equiv 0^2 - Du_{h/2}^2 \equiv 4(-1)^{h/2} \equiv -4 \pmod p.$$

Thus, since $(D/p) = 1$, we obtain that

$$u_{h/2} \equiv 2\varepsilon/\sqrt{D} \pmod p. \tag{4.38}$$

Parts (iii), (iv), and (vii) now follow from (4.33)–(4.38). Now suppose that $a \equiv \pm 1 \pmod p$. Then $u_1 \equiv 1$ and $u_2 = a \equiv \pm 1 \pmod p$. Part (vi) now follows from (4.36).

We now prove parts (i), (ii), (viii), and (ix). We first determine $N_u(p)$. Let R be the number of even integers e such that $2 \le e \le (p-1)/2$. Let T be the number of odd integers j such that $1 \le j \le (p-1)/2$. Clearly, $R = (p-3)/4$ and $T = (p+1)/4$. Let Y be the number of odd integers m such that $m \le (p-1)/2$ and

$$u_m \equiv \pm u_e \pmod p \tag{4.39}$$

for some even integer e such that $2 \le e \le (p-1)/2$. Since $A_u(0) = 1$, we now see by (4.33)–(4.37) that

$$N_u(p) = 1 + 2R + (T - Y) = 1 + 2\Big(\frac{p-3}{4}\Big) + \frac{p+1}{4} - Y = \frac{3p-1}{4} - Y. \tag{4.40}$$

We will see later

$$Y = \begin{cases} \frac{p-3}{8}, & \text{if } p \equiv 3 \pmod 8; \\ \frac{p+1}{8}, & \text{if } p \equiv 7 \pmod 8. \end{cases} \tag{4.41}$$

This will imply by (4.40) and (4.41) that

$$N_u(p) = \begin{cases} \frac{5p+1}{8}, & \text{if } p \equiv 3 \pmod 8; \\ \frac{5p-3}{8}, & \text{if } p \equiv 7 \pmod 8), \end{cases} \tag{4.42}$$

as desired.

By Theorem 3.3 and Lemma 3.13, if there exist integers m and n such that $1 \le m < n < (p-1)/2$, $n - m$ is odd, and $u_n \equiv \pm u_m \pmod p$, then there exist exactly four odd integers ℓ such that $1 \le \ell \le p-2$ and for which there exist exactly two distinct integers n_1 and n_2 satisfying $1 \le n_1, n_2 \le p-2$,

$$u_{n_1+\ell} \equiv u_{n_1} \equiv \varepsilon u_m \pmod p \tag{4.43}$$

and

$$u_{n_2+\ell} \equiv -u_{n_1} \equiv -\varepsilon u_m \pmod p. \tag{4.44}$$

Similarly, if there exists an integer m for which $1 \le m < (p-1)/2$, $(p-1)/2 - m$ is odd, and $u_{(p-1)/2} \equiv \pm u_m \pmod p$, then there exist exactly two odd integers ℓ such that $1 \le \ell \le p-2$ and (4.43) and (4.44) hold for two distinct integers n_1 and n_2 satisfying $1 \le n_1, n_2 \le p-2$.

Let g be a fixed integer such that $1 \le g \le p-2$. Noting that $h_u(p) = p-1$, it follows from Theorem 3.2 that the $p-1$ ratios w_{n+g}/w_n are distinct modulo p for $0 \le n \le p-2$. Notice that there are $p+1$ possible values for $w_{n+g}/w_n \pmod p$ including the values 0 and ∞. Furthermore, by Theorem 1.6 (ii) and Theorem 3.1 (ii), there are two nontrivial p-irregular recurrences that are not p-equivalent to $u(a, 1)$ or to each other, namely, the recurrences

$w'(a,1)$ with initial terms $w'_0 \equiv 1$, $w'_1 \equiv \alpha \pmod p$ and $w''(a,1)$ with initial terms $w''_0 \equiv 1$, $w''_1 \equiv \beta \pmod p$. Thus, by Theorem 3.3, the ratios

$$\frac{w'_g}{w'_0} \equiv \alpha^g \pmod p \quad \text{and} \quad \frac{w''_g}{w''_0} \equiv \beta^g \pmod p \tag{4.45}$$

are distinct from each other and from the $p-1$ ratios $w_{n+g}/w_n \pmod p$, $0 \le n \le p-2$. Hence, we have exhausted all $p+1$ possible values for these ratios modulo p. Thus, for a given integer g such that $1 \le g \le p-2$ both of the residues 1 and $(-1) \pmod p$ appear among the ratios

$$\left\{\frac{u_{n+g}}{u_n}\right\}_{n=0}^{p-2}, \quad \frac{w'_g}{w'_0}, \quad \text{and} \quad \frac{w''_g}{w''_0} \quad \text{modulo } p. \tag{4.46}$$

We now determine the values of w'_g/w'_0 and $w''_g/w''_0 \pmod p$ for various integers g such that $1 \le g \le p-2$. By Theorem 1.5 (vi),

$$\lambda_u(p) = p-1 = \operatorname{lcm}(\operatorname{ord}_p\alpha, \operatorname{ord}_p\beta), \tag{4.47}$$

where we assume that $\operatorname{ord}_p\alpha \le \operatorname{ord}_p\beta$. Since $\alpha\beta = -1$, it follows from (4.47) that

$$\operatorname{ord}_p\alpha = \frac{p-1}{2}, \quad \operatorname{ord}_p\beta = p-1. \tag{4.48}$$

Hence,

$$\alpha^g \not\equiv \pm 1 \quad \text{and} \quad \beta^g \not\equiv \pm 1 \pmod p \tag{4.49}$$

if $1 \le g \le p-2$ and $g \ne (p-1)/2$, while

$$\alpha^{(p-1)/2} \equiv 1 \quad \text{and} \quad \beta^{(p-1)/2} \equiv -1 \pmod p. \tag{4.50}$$

Thus, by (4.46), (4.49), and (4.50), if ℓ is an odd integer such that $1 \le \ell \le p-2$, then there exist distinct integers n_1 and n_2 such that $0 \le n_1, n_2 \le p-2$ and

$$\frac{u_{n_1+\ell}}{u_{n_1}} \equiv 1, \quad \frac{u_{n_2+\ell}}{u_{n_2}} \equiv -1 \pmod p \tag{4.51}$$

if and only if ℓ is one of the $(p-3)/2$ odd integers for which $1 \le \ell \le p-2$ and $\ell \ne (p-1)/2$. We now observe that

$$\frac{p-3}{2} \equiv \begin{cases} 0 \pmod 4, & \text{if } p \equiv 3 \pmod 8; \\ 2 \pmod 4, & \text{if } p \equiv 7 \pmod 8). \end{cases} \tag{4.52}$$

It now follows from (4.34), (4.37), (4.38), and (4.52) that parts (viii) and (ix) both hold.

We now see from Theorem 3.2, (4.43), and (4.44) that

$$Y = \begin{cases} \frac{(p-3)/2}{4} = \frac{p-3}{8}, & \text{if } p \equiv 3 \pmod 8; \\ \frac{(p-7)/2}{4} + \frac{2}{2} = \frac{p+1}{8}, & \text{if } p \equiv 7 \pmod 8, \end{cases} \tag{4.53}$$

and the formula for $N_u(p)$ given in (4.42) indeed holds.

We now observe by Theorem 1.1 (iv) that $S_u(p) \subset \{0,1,2,3\}$. Next we determine $B_w(i)$ for $0 \le i \le 3$. First suppose that $i = 0$. Then by (4.42),

$$B_u(0) = p - N_u(p) = \begin{cases} p - \frac{5p+1}{8} = \frac{3p-1}{8} & \text{if } p \equiv 3 \pmod 8, \\ p - \frac{5p-3}{8} = \frac{3p+3}{8} & \text{if } p \equiv 7 \pmod 8. \end{cases} \tag{4.54}$$

Now we let $i = 1$. It follows from (4.34)–(4.38) and parts (v), (viii), and (ix) that

$$B_u(1) = 1 + 2(R-Y) + (Y+1) = 1 + \frac{p-3}{2} - \frac{p-3}{4} + \frac{p-3}{8} + 1 = \frac{3p+7}{8} \text{ if } p \equiv 3 \pmod 8, \tag{4.55}$$

whereas

$$B_u(1) = 1 + 2(R - Y) + Y = 1 + \frac{p-3}{2} - \frac{p+1}{4} + \frac{p+1}{8} = \frac{3p-5}{8} \text{ if } p \equiv 7 \pmod 8. \quad (4.56)$$

Further, we consider the case in which $i = 2$. Then by (4.33), (4.34), (4.37), (4.38), and parts (viii) and (ix),

$$B_u(2) = (T - Y) - 1 = \frac{p+1}{4} - \frac{p-3}{8} - 1 = \frac{p-3}{8} \text{ if } p \equiv 3 \pmod 8, \quad (4.57)$$

while

$$B_u(2) = (T - Y) + 1 = \frac{p+1}{4} - \frac{p+1}{8} + 1 = \frac{p+9}{8} \text{ if } p \equiv 7 \pmod 8. \quad (4.58)$$

Finally, we suppose that $i = 3$. Then by (4.34), (4.36), and (4.37),

$$B_u(3) = Y = \frac{p-3}{8} \text{ if } p \equiv 3 \pmod 8, \quad (4.59)$$

while

$$B_u(3) = Y - 1 = \frac{p+1}{8} - 1 = \frac{p-7}{8} \text{ if } p \equiv 7 \pmod 8. \quad (4.60)$$

Finally, we see from (4.55)–(4.60) that $S_u(p) = \{0, 1\}$ if $p = 3$, $S_u(p) = \{0, 1, 2\}$ if $p = 7$, and $S_u(p) = \{0, 1, 2, 3\}$ if $p \equiv 3 \pmod 4$ and $p > 7$.

Parts (i) and (ii) are now established and the proof is complete. □

5. Corollaries of the Main Theorems

Corollary 5.1 follows from Theorem 2.1 and 2.2 upon application of Theorem 1.8, Theorem 3.11, and (1.12).

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 $p \nmid D_1 D_2$ 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 $0 \le d \le p - 1$, and $w(a_1, 1)$ and $w'(a_2, 1)$ are identically distributed modulo p.

Corollary 5.2 below follows from Theorems 2.1 and 2.2 upon application of Theorem 1.8, Theorem 1.10, Theorem 3.10, and (1.12).

Corollary 5.2. *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 there exists a nonzero residue c modulo p such that $A_{w'}(d) = A_u(cd)$, and $w'(a_1, 1)$ is identically distributed modulo p to $u(a, 1)$. If $w'(a_1, 1)$ is p-equivalent to $v(a_1, 1)$, then there exists a nonzero residue c modulo p such that $A_{w'}(cd) = A_v(d)$, and $w'(a_1, 1)$ is identically distributed modulo p to $v(a, 1)$.

Remark 5.3. *Primes q for which $2q - 1$ is also prime are called Sophie Germain primes of the second kind. It is easily seen that if q is an odd Sophie Gemain prime, then $2q - 1 \equiv 1 \pmod 4$. Let q be an odd Sophie Germain prime and let $p = 2q - 1$. Suppose that $w(a, 1)$ is a p-regular recurrence with discriminant $D = a^2 + 4$ such that $(D/p) = -1$. Then by Theorem 1.5 (i) and (iii), $h_w(p) = (p + 1)/2$.*

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

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

The largest known Sophie Germain prime of the second kind is $129431439657 \cdot 2^{170172} + 1$ with 51238 digits according to [4].

Corollary 5.4. *Suppose that $w(a,1)$ is p-equivalent to $v(a,1)$ and that $p \mid D = a^2 + 4$. Then $w(a,1)$ is p-irregular and*

$$\lambda_w(p) = \lambda_v(p) = 4. \tag{5.1}$$

Moreover,

$$A_w(0) = 0,\ S_w(p) = \{0,1\},\ N_w(p) = \lambda_w(p) = 4,\ B_w(0) = p - 4,\ B_w(1) = 4. \tag{5.2}$$

Proof. By Theorem 1.8 it suffices to prove the result for the case in which $w(a,1) = v(a,1)$. Since $v_0 = 2$, we see by Theorem 1.6 (ii) that

$$\lambda_v(p) = \mathrm{ord}_p \alpha = \mathrm{ord}_p a/2.$$

Since $D = a^2 + 4 \equiv 0 \pmod p$, we find that $(a/2)^2 \equiv -1 \pmod p$, which implies that $\mathrm{ord}_p \alpha = \lambda_v(p) = 4$, and (5.1) holds. It now easily follows that (5.2) holds upon use of Theorem 1.6 (ii). □

Acknowledgement

We express our deep appreciation to the anonymous referee for suggestions improving and substantially shortening our paper. 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] S. Müller, *On the rank of appearance of Lucas sequences*, Applications of Fibonacci Numbers, Vol. 8, F. T. Howard (ed.), Kluwer Academic Publ., Dordrecht, 1999, 259–275.

[12] 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.

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

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

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

[16] L. Somer, *Primes having an incomplete system of residues for a class of second-order recurrences*, Applications of Fibonacci Numbers, Vol. 2, A. F. Horadam, A. N. Philippou, and G. E. Bergum (eds.), Kluwer Academic Publ., Dordrecht, 1988, 113–141.

[17] 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.

[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. 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 Acad. Publ., Dordrecht, 1996, 451–471.

[21] L. Somer and M. Křížek, *Identically distributed second-order linear recurrences modulo p*, The Fibonacci Quarterly, **53.4** (2015), 290–312.

[22] 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