SECOND-ORDER LINEAR RECURRENCES HAVING ARBITRARILY LARGE DEFECT MODULO p

LAWRENCE SOMER AND MICHAL KŘÍŽEK

ABSTRACT. Let $(w) = w(a,b)$ denote the second-order linear recurrence satisfying $w_{n+2} = aw_{n+1} + bw_n$, where w_0, w_1, and a are integers, $b = \pm 1$, and $D = a^2 + 4b$ is the discriminant. We distinguish the Lucas sequences $u(a,b)$ and $v(a,b)$ with initial terms $u_0 = 0$, $u_1 = 1$, and $v_0 = 2$, $v_1 = a$, respectively. Let p be a prime. Given the recurrence $w(a,b)$, let $\delta_w(p)$, called the *defect* of $w(a,b)$ modulo p, denote the number of residues not appearing in (w) modulo p. It is known that for the recurrence $w(a,\pm 1)$, $\delta_w(p) \geq 1$ if $p > 7$ and $p \nmid D$. Given the fixed recurrence $w(a,1)$, where $w(a,1) = u(a,1)$ or $v(a,1)$, we will show that $\lim_{p\to\infty} \delta_w(p) = \infty$. Further, given the arbitrary recurrence $w(a,-1)$, we will demonstrate that $\lim_{p\to\infty} \delta_w(p) = \infty$ and $\lim_{p\to\infty} \delta_w(p)/p \geq \frac{1}{2}$. We will also prove that for the arbitrary recurrence $w(a,\pm 1)$, we have that $\limsup_{p\to\infty} \delta_w(p)/p = 1$.

1. INTRODUCTION

Given the set J of integers and a modulus p, where p is a prime, we say that J forms a *complete residue system modulo* p if for all $i \in \{0, 1, \ldots, p-1\}$ there exists $j \in J$ such that $j \equiv i \pmod{p}$. Further, J forms a *reduced residue system modulo* p if for all $i \in \{1, \ldots, p-1\}$ there exists $j \in J$ such that $j \equiv i \pmod{p}$. Sets that do not form a complete residue system modulo p are called *p-defective*. The *p-defect* of the set J, denoted by $\delta_J(p) = \delta(p)$, is the number of distinct residues modulo p not appearing in J modulo p.

In this paper, we will be concerned with the situation in which the sets J are certain second-order linear recurrence sequences. In many of these cases, we will show that $\lim_{p\to\infty} \delta_w(p) = \infty$. Throughout this paper, p will denote a prime and ε will specify an element from $\{-1, 1\}$.

Let $\mathcal{F}(a,b)$ denote the set of all recurrences $(w) = w(a,b)$ 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. The recurrence $w(a,b)$ is said to be *trivial* if $w_0 = w_1 = 0$. We distinguish two special recurrences in $\mathcal{F}(a,b)$, 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. We will be particularly interested in the case in which $b = \pm 1$. Associated with the recurrence $w(a,b)$ is the characteristic polynomial

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

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

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

and

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

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 $p \nmid b$. In particular, we assume that $b = -\alpha\beta \neq 0$.

The *period* of $w(a,b)$ modulo p, denoted by $\lambda = \lambda_w(p)$, 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 $h = h_w(p)$, is the least positive integer r such that $w_{n+r} \equiv Mw_n \pmod{p}$ for some fixed nonzero residue M modulo p. Here, $M = M_w(p)$ is called the multiplier of $w(a,b)$ modulo p. It is seen that if $h = h_w(p)$, then

$$w_{n+hi} \equiv M^i w_n \pmod{p} \tag{1.5}$$

for all $n \geq 0$. Because the LSFK $u(a,b)$ is purely periodic modulo p and has initial terms $u_0 = 0$, $u_1 = 1$, it follows 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

$$E = E_w(p) = \frac{\lambda_w(p)}{h_w(p)}.$$

Then by [7, pp. 354–355], $E_w(p)$ is the multiplicative order of $M_w(p)$ modulo p. Given the consecutive terms w_n, w_{n+1} of $w(a,b)$, the preceding term

$$w_{n-1} = \frac{w_{n+1} - aw_n}{b}$$

is uniquely determined. Thus, we will treat $\{w_n\}_{n=-\infty}^{\infty}$ as a doubly infinite sequence. Note that when $b = \pm 1$, each term of $\{w_n\}_{n=-\infty}^{\infty}$ is an integer.

Given the residue $0 \leq d \leq p-1$, we let $A_w(d)$ denote the number of times that d appears in a shortest period of (w) modulo p. We let

$$N_w(p) = \#\{d \mid 0 \leq d \leq p-1\,,\ A_w(d) > 0\}.$$

Then

$$\delta_w(p) = p - N_w(p). \tag{1.6}$$

It is clear that

$$N_w(p) \leq \lambda_w(p). \tag{1.7}$$

It follows from (1.7) that if $\lambda(p) \leq p$, then

$$\delta_w(p) = p - N_w(p) \geq p - \lambda_w(p). \tag{1.8}$$

The recurrence $w(a,b)$ with characteristic roots α and β is called *degenerate* if $\alpha\beta = 0$ or α/β is a root of unity. Given the LSFK $u(a,b)$, it follows from the Binet formulas (1.3) and (1.4) that $u_n = 0$ for $n > 0$ only if $u(a,b)$ is degenerate. Theorem 1.1 characterizes the degenerate recurrences $w(a,b)$ when $b = \pm 1$.

Theorem 1.1. *Consider the recurrence $w(a,b)$ with discriminant D and characteristic roots α and β, where $b = \pm 1$.*

(i) *$w(a,b)$ is degenerate if and only if $(a,b) = (0,1)$, $(0,-1)$, $(1,-1)$, $(-1,-1)$, $(2,-1)$, or $(-2,-1)$.*
(ii) *If $(a,b) = (0,1)$, then $w_{2n} = w_0$, $w_{2n+1} = w_1$ for $n \geq 0$.*
(iii) *If $(a,b) = (0,-1)$, then $w_{4n} = w_0$, $w_{4n+1} = w_1$, $w_{4n+2} = -w_0$, $w_{4n+3} = -w_1$ for $n \geq 0$.*
(iv) *If $(a,b) = (1,-1)$, then $w_{6n} = w_0$, $w_{6n+1} = w_1$, $w_{6n+2} = w_1 - w_0$, $w_{6n+3} = -w_0$, $w_{6n+4} = -w_1$, $w_{6n+5} = -w_1 + w_0$ for $n \geq 0$.*
(v) *If $(a,b) = (-1,-1)$, then $w_{3n} = w_0$, $w_{3n+1} = w_1$, $w_{3n+2} = -w_1 - w_0$ for $n \geq 0$.*
(vi) *If $(a,b) = (2,-1)$, then $\alpha = \beta = 1$, $D = 0$, and $w_n = nw_1 - (n-1)w_0$ for $n \geq 0$.*

(vii) *If* $(a,b)=(-2,-1)$, *then* $\alpha\beta=-1$, $D=0$, *and* $w_n=n(-1)^{n-1}w_1-(n-1)(-1)^n w_0$ *for* $n\geq 0$.

Proof. Part (i) follows from [27, p. 613]. Parts (ii)–(vii) follow by induction. □

Corollary 1.2. *Consider the nontrivial recurrence* $w(a,\pm 1)$ *with discriminant* D *and characteristic roots* α *and* β.

(i) $w(a,1)$ *is nondegenerate if and only if* $|a|\geq 1$.
(ii) $w(a,-1)$ *is nondegenerate if and only if* $|a|\geq 3$.
(iii) *If* $w(a,\pm 1)$ *is nondegenerate, then* $D>0$, D *is not a square, and* α *and* β *are real and irrational.*

Proof. Parts (i) and (ii) follow from Theorem 1.1. Part (iii) follows from parts (i) and (ii) and that the parameter $b=\pm 1$. □

We now define equivalence relations on $\mathcal{F}(a,b)$ and $\mathcal{F}(a,b)$ modulo p, respectively, where p is a fixed prime. The recurrences $w(a,b)$ and $w'(a,b)$ are said to be *equivalent* if there exist nonzero integers ℓ and m and fixed integer s such that $\ell w_n=mw'_{n+s}$ for all nonnegative integers n.

Let p be a fixed prime and let $w(a,b)$ and $w'(a,b)$ be recurrences. We say that $w'(a,b)$ is p-equivalent to $w(a,b)$ if there exist a fixed integer s and nonzero residue g modulo p such that $w'_n\equiv gw_{n+s} \pmod p$ for all $n\geq 0$.

It is evident that the following proposition holds.

Proposition 1.3. *Let* $w(a,b)$ *and* $w'(a,b)$ *be* p*-equivalent recurrences. Then,*

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

Suppose that $w(a,b)$ is nontrivial modulo p and $w'(a,b)$ is equivalent to $w(a,b)$. It is evident that $w'(a,b)$ is trivial modulo p or $w'(a,b)$ is p-equivalent to $w(a,b)$. Noting that $\delta_{w'}(p)=p-1$ if $w'(a,b)$ is trivial modulo p, we see by Proposition 1.3 that the following proposition is satisfied.

Proposition 1.4. *Suppose that* $w(a,b)$ *is nontrivial modulo* p *and* $w'(a,b)$ *is equivalent to* $w(a,b)$. *Then,*

$$\delta_{w'}(p)\geq \delta_w(p).$$

Remark 1.5. Given the recurrence $w(a,b)$, our main results will be concerned with lower bounds for $\delta_w(p)$. Thus, by Proposition 1.4, in obtaining nontrivial lower bounds for $\delta_w(p)$, we also get nontrivial lower bounds for $\delta_{w'}(p)$ whenever $w'(a,b)$ is equivalent to $w(a,b)$. Hence, for example, if $w'(a,b)$ is equivalent to $u(a,b)$, we need only find nontrivial lower bounds for $\delta_u(p)$ to obtain nontrivial lower bounds for $\delta_{w'}(p)$.

A recurrence $w(a,b)$ is called *regular modulo* p, or p*-regular* for short, if

$$\Delta(w)=w_1^2-w_0w_2=w_1^2-w_0(aw_1+bw_0)=w_1^2-aw_0w_1-bw_0^2\not\equiv 0 \pmod p. \tag{1.9}$$

Otherwise, $w(a,b)$ is called p*-irregular*. It is easy to see that $w(a,b)$ is p-irregular if and only if it satisfies a recursion relation modulo p of order less than two.

Remark 1.6. We observe by (1.9) that $\Delta(w)=0$ if and only if

$$w_1=w_0\frac{a\pm\sqrt{a^2+4b}}{2}, \tag{1.10}$$

which occurs if and only if $w_0 = 0$, in which case $w(a,b)$ is trivial, or $D = a^2 + 4b$ is a perfect square. In these cases, $w_1 = w_0\alpha$ or $w_1 = w_0\beta$, where α and β are the characteristic roots of $w(a,b)$ and are both integers. We note that $\alpha\beta = -b \neq 0$.

Lemma 1.7. *Consider the set $\mathcal{F}(a,b)$ of recurrences $w(a,b)$ with characteristic roots α and β. Suppose that $w(a,b)$ is p-irregular. Then α and β are in the field $\mathbb{Z}_p$ of integers modulo p, and the Legendre symbol $(D/p) = 0$ or 1. Let $\operatorname{ord}_p m$ denote the multiplicative order of m modulo p. Then the following holds:*

(i) *$A_w(0) \geq 1$ if and only if $w_0 \equiv 0 \pmod{p}$. In this case, (w) is the trivial recurrence modulo p and $w_n \equiv 0 \pmod{p}$ for all n.*

(ii) *Suppose that $w_0 \not\equiv 0 \pmod{p}$. Then, either $w_n \equiv \alpha^n w_0 \pmod{p}$ or $w_n \equiv \beta^n w_0 \pmod{p}$ for all $n \geq 0$. Additionally, $h_w(p) = 1$, $N_w(p) = \lambda_w(p)$, where $\lambda_w(p) = \operatorname{ord}_p\alpha$ or $\lambda_w(p) = \operatorname{ord}_p\beta$, and $\delta_w(p) = p - \lambda_w(p)$.*

This is proved in [5, pp. 694–695].

Lemma 1.8. *Suppose that $w(a,b)$ and $w'(a,b)$ are both p-regular. Then $h_w(p) = h_{w'}(p)$, $M_w(p) \equiv M_{w'}(p) \pmod{p}$, $\lambda_w(p) = \lambda_{w'}(p)$, and $E_w(p) = E_{w'}(p)$.*

This follows from the discussion in [5, p. 695].

Lemma 1.9. *Let p be a prime and let $w(a,b)$ and $w'(a,b)$ be recurrences. Then, $w'(a,b)$ is p-regular if and only if $w(a,b)$ is p-regular.*

This follows from the discussion in [5, p. 694].

Theorem 1.10. *Let $w(a,b)$ be a p-regular recurrence with discriminant D such that $p \mid D$. Then, $\delta_w(p) = 0$.*

This is proved in [4] and [28].

Remark 1.11. Consider the nondegenerate recurrence $w(a,\pm 1)$ with discriminant D. Our main result will show in many cases that $\lim_{p\to\infty} \delta_w(p) = \infty$.

Suppose that $w_0 \not\equiv 0 \pmod{p}$, $w(a,\pm 1)$ is p-irregular, and $\operatorname{ord}_p w_1/w_0 = p - 1$. Then by Lemma 1.7, $\delta_w(p) = 1$. Furthermore, by Theorem 1.10, if $p \mid D$ and $w(a,\pm 1)$ is p-regular, then $\delta_w(p) = 0$. However, by Corollary 1.2 and Remark 1.6, $D \cdot \Delta(w) \neq 0$. Thus, $D \cdot \Delta(w) \equiv 0 \pmod{p}$ for only finitely many primes p. Hence, we can assume that $p \nmid D \cdot \Delta(w)$ in establishing that

$$\lim_{p\to\infty} \delta_w(p) = \infty.$$

Shah [14] proved that for the Fibonacci sequence $\{F_n\} = u(1,1)$, $\delta(p) \geq 1$ if $p \equiv \pm 1 \pmod{10}$ or $p \equiv 13$ or $17 \pmod{20}$. Bruckner [3] proved the remaining cases that $\delta(p) \geq 1$ for $\{F_n\}$ if $p > 7$ with $p \equiv 3$ or $7 \pmod{20}$. Somer [16] partially generalized the results of Shah and Bruckner by showing for the recurrence $w(a,1)$ that $\delta_w(p) \geq 1$ if $p > 7$, $p \nmid D = a^2 + 4$, and $p \not\equiv 1$ or $9 \pmod{20}$. Schinzel [13] completely generalized the results of Shah and Bruckner by proving that for the recurrence $w(a,1)$, $\delta_w(p) \geq 1$ if $p \nmid a^2 + 4$ and $p > 7$. Li [12] also obtained Schinzel's results by extending the methods of Somer [16]. Somer [16] also proved that for the recurrence $w(a,-1)$, $\delta_w(p) \geq 1$ if $p \geq 5$ and $p \nmid D = a^2 - 4$. In Section 2, we will considerably extend these results by showing for the Lucas sequences $u(a,\pm 1)$ and $v(a,\pm 1)$, $\lim_{p\to\infty} \delta_w(p) = \infty$. Further results along these lines will also be presented in Section 2.

2. Main Results

Theorem 2.1. *Let $w(a,b)$ with discriminant D be trivial or a degenerate recurrence for which $D \neq 0$ and $b = \pm 1$. Then, either $w_0 = w_1 = 0$ or $(a,b) = (0,1)$, $(0,-1)$, $(1,-1)$, or $(-1,-1)$. Then, $\lim_{p\to\infty} \delta_w(p) = \infty$ and*

$$\lim_{p\to\infty} \frac{\delta_w(p)}{p} = 1.$$

Moreover, the following hold:

(i) *If $w(a,\pm 1)$ is trivial, then $\delta_w(p) = p-1$ for all p.*
(ii) *If $(a,b) = (0,1)$, then $p-2 \leq \delta_w(p) \leq p-1$ for $p \geq 3$.*
(iii) *If $(a,b) = (0,-1)$, then $\delta_w(p) \geq p-4$ for $p \geq 5$.*
(iv) *If $(a,b) = (1,-1)$, then $\delta_w(p) \geq p-6$ for $p \geq 7$.*
(v) *If $(a,b) = (-1,-1)$, then $\delta_w(p) \geq p-3$ for $p \geq 5$.*

This follows from Theorem 1.1 (i)–(v).

Theorem 2.2. *Let $w(a,b)$ be a nontrivial and degenerate recurrence with discriminant $D = 0$ and characteristic roots α and β, where $b = \pm 1$. Then, either $(a,b) = (2,-1)$ and $\alpha = \beta = 1$ or $(a,b) = (-2,-1)$ and $\alpha = \beta = -1$.*

(i) *Suppose that $(a,b) = (2,-1)$ and $\alpha = \beta = 1$.*
  (a) *If $w_0 = w_1$, then $\lim_{p\to\infty} \delta_w(p) = \infty$ and $\lim_{p\to\infty} \delta_w(p)/p = 1$. Moreover, $\delta_w(p) = p-1$ for all p.*
  (b) *If $w_0 \neq w_1$, then $\delta_w(p) = 0$ for all p such that $p \nmid w_1 - w_0$. In particular, $\lim_{p\to\infty} \delta_w(p) = \lim_{p\to\infty} \delta_w(p)/p = 0$.*
(ii) *Suppose that $(a,b) = (-2,-1)$ and $\alpha = \beta = -1$.*
  (a) *If $w_0 = -w_1$, then $\lim_{p\to\infty} \delta_w(p) = \infty$ and $\lim_{p\to\infty} \delta_w(p)/p = 1$. Moreover, $\delta_w(p) = p-2$ for $p \geq 3$.*
  (b) *If $w_0 \neq -w_1$, then $\delta_w(p) = 0$ for all p such that $p \nmid w_0 + w_1$. In particular, $\lim_{p\to\infty} \delta_w(p) = \lim_{p\to\infty} \delta_(p)/p = 0$.*

Proof. This follows from Theorem 1.1 (vi) and (vii) and Theorem 1.10. □

Theorem 2.3. *Let $w(a,-1)$ be a nontrivial and nondegenerate recurrence with discriminant D and characteristic roots α and β, where $|\alpha| \geq |\beta|$. Then, α and β are real, $|\alpha| > 1$, and $\beta = \alpha^{-1}$. Let $0 < \varepsilon \leq 0.4$ and $s = 168/172$. Let $n_1 = \frac{1}{s}\mathrm{e}^{2/(\varepsilon s)}$.*

(i) *$\lim_{p\to\infty} \delta_w(p) = \infty$ and $\liminf_{p\to\infty} \delta_w(p)/p \geq \frac{1}{2}$. Moreover, if $p \nmid D \cdot \Delta(w)$, then $\delta_w(p) \geq (p-3)/2$ for $p \geq 5$.*
(ii) *$\limsup_{p\to\infty} \delta_w(p)/p = 1$. Moreover, there exists a prime $p' \leq \lfloor |\alpha|^{n_1}/\sqrt{D} \rfloor$ such that $\delta_w(p')/p' \geq 1-\varepsilon$.*

Theorem 2.4. *Let $w(a,1)$ be a nontrivial and nondegenerate recurrence with discriminant D and characteristic roots α and β. Then, α and β are real, $|\alpha| > 1$, and $\beta = -\alpha^{-1}$. Let $0 < \varepsilon \leq 0.4$ and $r = 22067/22071$. Let $n_2 = \frac{1}{r}\mathrm{e}^{4/(\varepsilon r)}$.*

(i) *Let $\mathcal{A}_1 = \{p \mid p \equiv 3 \pmod 4 \text{ or } p \equiv 1 \pmod 4 \text{ and } (D/p) = -1\}$. Then,*

$$\lim_{p\in\mathcal{A}_1,\, p\to\infty} \delta_w(p) = \infty.$$

(ii) *Let $\mathcal{A}_2 = \{p \mid p \equiv 3 \pmod 4 \text{ and } (D/p) = 1\}$, where (D/p) denotes the Legendre symbol and $(D/p) = 0$ if $p \mid D$. Then,*

$$\liminf_{p\in\mathcal{A}_2,\, p\to\infty} \delta_w(p)/p \geq \frac{3}{8}.$$

Moreover, if $p \nmid \Delta(w)$, *then*

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

for $p \geq 3$ *and* $p \in \mathcal{A}_2$.

(iii) *Let* $\mathcal{A}_3 = \{p \mid p \equiv 3 \pmod 4 \text{ and } (D/p) = -1\}$. *Then,* $\liminf_{p \in \mathcal{A}_3, p \to \infty} \delta_w(p)/p \geq \frac{1}{4}$. *Moreover,*

$$\delta_w(p) \geq \begin{cases} \frac{p-3}{4}, & \text{if } p \equiv 3 \pmod 8; \\ \frac{p-7}{4}, & \text{if } p \equiv 7 \pmod 8 \end{cases}$$

for $p \geq 3$ *and* $p \in \mathcal{A}_3$.

(iv) *Let* $\mathcal{A}_4 = \{p \mid p \equiv 1 \pmod 4 \text{ and } (D/p) = -1\}$. *Let* C *be a positive integer. Then,* $\delta_w(p) \geq C$ *for* $p \in \mathcal{A}_4$ *if*

$$p > 2^{2\lfloor \frac{C+2}{2} \rfloor + 3}\left(\left\lfloor \frac{C+2}{2} \right\rfloor + 1\right) - 3 \quad \text{and} \quad p \nmid \Delta(w).$$

(v) *Let* $\mathcal{A}_5 = \{p \mid p \equiv 1 \pmod 4 \text{ and } (D/p) = 1\}$. *If* $p \in \mathcal{A}_5$, $p \geq 13$, *and* $p \nmid \Delta(w)$, *then* $\delta_w(p) \geq 5$.

(vi) $\limsup_{p \to \infty} \delta_w(p)/p = 1$. *Moreover, there exists a prime*

$$p'' \leq \left\lceil \frac{|\alpha|^{n_2}}{\sqrt{D}} \right\rceil$$

such that $\delta_w(p'')/p'' \geq 1 - \varepsilon$.

Theorem 2.5. *Let* $w(a,1)$ *be a nontrivial and nondegenerate recurrence with discriminant* D *such that* $w(a,1)$ *is equivalent to* $u(a,1)$ *or* $v(a,1)$.

(i) $\lim_{p \to \infty} \delta_w(p) = \infty$.

(ii) *Let* $\mathcal{A}_5 = \{p \mid p \equiv 1 \pmod 4 \text{ and } (D/p) = 1\}$. *Then,* $\liminf_{p \in \mathcal{A}_5, p \to \infty} \delta_w(p)/p \geq \frac{1}{2}$. *Moreover, if* $p \nmid \Delta(w)$, *then*

$$\delta_w(p) \geq \begin{cases} \frac{p-1}{2}, & \text{if } p \equiv 1 \pmod 8; \\ \frac{p-3}{2}, & \text{if } p \equiv 5 \pmod 8 \end{cases}$$

for $p \geq 13$ *and* $p \in \mathcal{A}_5$.

3. Preliminaries

In this section, we present some results and definitions that will be needed for the proofs of the main results in Section 6.

Theorem 3.1. *Let* p *be a fixed odd prime. Consider the* p*-regular recurrence* $w(a,b)$ *with discriminant* D *and characteristic roots* α *and* β. *Let* $h = h_w(p)$ *and* $\lambda = \lambda_w(p)$. *Let* P *be a prime ideal in* $\mathbb{Q}(\sqrt{D})$ *dividing* p. *If* $(D/p) = 1$, *we will identify* P *with* p.

(i) $h \mid p - (D/p)$.

(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) λ *is the least common multiple of the multiplicative orders of* α *and* β *modulo* P.

(vii) $A_w(0) \geq 1$ *if and only if* $w(a,b)$ *is* p*-equivalent to* $u(a,b)$.

Proof. Parts (i)–(v) are proven in Theorem 3.15 of [25]. Part (vi) is proved in Theorem 6 of [15]. Part (vii) is proved in Lemma 2.4 of [23]. □

Theorem 3.2. *Let* $w(a,1)$ *be a* p*-regular recurrence with discriminant* D*. Then,*

(i) $E_w(p) \in \{1, 2, 4\}$.
(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* $h_w(p) \mid 2(p+1)$.

This is proved in Theorem 3.16 of [25].

Theorem 3.3. *Let* $w(a,-1)$ *be a* p*-regular recurrence with discriminant* D*. Then,*

(i) $E_w(p) \in \{1, 2\}$.
(ii) *Suppose that* $h_w(p)$ *is odd. Then,* $E_w(p) \in \{1, 2\}$. *If* $E_w(p) = 1$, *then* $\lambda_w(p)$ *is odd. If* $E_w(p) = 2$, *then* $\lambda_w(p) \equiv 2 \pmod 4$.
(iii) *Suppose that* $h_w(p)$ *is even. Then,* $E_w(p) = 2$ *and* $\lambda_w(p) \equiv 0 \pmod 4$.
(iv) *If* $p \nmid D$, *then* $h_w(p) \mid (p - (D/p))/2$ *and* $\lambda_w(p) \mid p - (D/p)$.

This is proved in Theorem 3.17 of [25].

Theorem 3.4. *Let* $w(a,b)$ *be a* p*-regular recurrence, and let* $w'(a,b)$ *be another recurrence. Then,*

$$\lambda_{w'}(p) \mid \lambda_w(p). \tag{3.1}$$

Proof. If $w'(a,b)$ is trivial modulo p, then (3.1) is clearly satisfied. The result now follows from Theorem 3.1 (vi), Lemma 1.7, and Lemma 1.8. □

Suppose that p is an odd prime for which $h_u(a,b)$ is even and $(-b/p) = 1$. In this case, we specify a third recurrence $t(a,b)$ in the set $\mathcal{F}(a,b)$, in addition to the recurrences $u(a,b)$ and $v(a,b)$, with initial terms $t_0 = 1$ and $t_1 = b'$, where $(b')^2 \equiv -b \pmod p$ and $1 \leq b' \leq (p-1)/2$. We note that if in place of b', in the definition of $t(a,b)$, we use the square root b'' of $-b$ modulo p satisfying $(p-1)/2 < b'' \leq p-1$, then by [20, pp. 534–535], the resulting sequence is p-equivalent to $t(a,b)$.

Lemma 3.5. *Let* p *be an odd prime. Consider the recurrences* $u(a,b)$, $v(a,b)$, *and* $t(a,b)$ *modulo* p *with discriminant* D.

(i) $u(a,b)$ *is* p*-regular for all* p.
(ii) $v(a,b)$ *is* p*-regular if and only if* $p \nmid D$.
(iii) $t(a,b)$ *is* p*-regular when it is defined.*

Proof. (i) We note that

$$\Delta(u) = u_1^2 - u_0 u_2 = 1^2 - 0 \cdot a = 1,$$

and $u(a,b)$ is p-regular for all p odd.

(ii) We observe that

$$\Delta(v) = v_1^2 - v_0 v_2 = a^2 - 2(a^2 + 2b) = -a^2 - 4b = -D,$$

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

(iii) This follows from [23, p. 7]. □

Lemma 3.6. *Let p be an odd prime. Consider the recurrences $u(a,1)$, $v(a,1)$, and $t(a,1)$ modulo p with discriminant D, where $p \nmid D$. Then, $u(a,1)$, $v(a,1)$, and $t(a,1)$ are all p-regular. Let $h = h_u(p) = h_v(p) = h_t(p)$ and $M \equiv M_u(p) \equiv M_v(p) \equiv M_t(p)$ modulo p.*

(i) $u_{hi-n} \equiv (-1)^{n+1} M^i u_n \pmod{p}$ *for* $0 \le n \le hi$.
(ii) $v_{hi-n} \equiv (-1)^n M^i v_n \pmod{p}$ *for* $0 \le n \le hi$.
(iii) $u_{hi+n} \equiv (-1)^{n+1} u_{hi-n} \pmod{p}$ *for* $0 \le n \le hi$.
(iv) $v_{hi+n} \equiv (-1)^n v_{hi-n} \pmod{p}$ *for* $0 \le n \le hi$.
(v) $t_{h+1-n} \equiv (-1)^n b' M t_n \pmod{p}$ *for* $0 \le n \le h+1$.

Proof. Parts (i), (ii), and (v) follow from Lemma 5 of [20] and can be established by induction. Parts (iii) and (iv) follow from Lemmas 2.6 (ii) and 2.7 (ii) of [12]. □

Lemma 3.7. *Let $w(a,1) = u(a,1)$ or $v(a,1)$. Let p be an odd prime, and let $h = h_u(p)$. Let n and c be integers such that $0 \le n < n+c \le h$ and $w_n w_{n+c} w_{h-n} w_{h-n-c} \not\equiv 0 \pmod{p}$. Then,*

$$\frac{w_{n+c}}{w_n} \frac{w_{h-n}}{w_{h-n-c}} \equiv (-1)^c \pmod{p}.$$

Proof. This follows from Theorem 3.6 (i) and (ii). □

Lemma 3.8. *Let $w(a,b)$ be a p-regular recurrence with restricted period h modulo p. Let c be a fixed integer such that $1 \le c \le h-1$. Let*

$$R_{n,c} \equiv \frac{w_{n+c}}{w_n} \pmod{p},$$

where we let $R_{n,c} \equiv \infty \pmod{p}$ if $w_n \equiv 0 \pmod{p}$. Then, the ratios $R_{r,c}$ are distinct modulo p for $0 \le r \le h-1$. Moreover, $R_{n+h,c} \equiv R_{n,c} \pmod{p}$ for all n.

This is proved in Lemma 2 of [20].

Lemma 3.9. *Let $w(a,b)$ and $w'(a,b)$ be p-regular recurrences. Then, $h = h_w(p) = h_{w'}(p)$. Let c be an integer such that $1 \le c \le h-1$. If $w(a,b)$ and $w'(a,b)$ are p-equivalent, then the sets*

$$\left\{ \frac{w_{i+c}}{w_i} \right\}_{i=0}^{h-1} \quad \text{and} \quad \left\{ \frac{w'_{i+c}}{w'_i} \right\}_{i=0}^{h-1}$$

are identical modulo p. If $w'(a,b)$ is not p-equivalent to $w(a,b)$, then the sets

$$\left\{ \frac{w_{i+c}}{w_i} \right\}_{i=0}^{h-1} \quad \text{and} \quad \left\{ \frac{w'_{i+c}}{w'_i} \right\}_{i=0}^{h-1}$$

are disjoint modulo p.

This is proved in Lemma 3 of [20].

Lemma 3.10. *Suppose that the recurrence $t(a,1)$ is defined modulo p. Then, $p \equiv 1 \pmod{4}$ and $(D/p) = 1$.*

Proof. By the definition of $t(a,1)$, we have $(-1/p) = 1$. Then, $p \equiv 1 \pmod{4}$. Moreover, by Theorem 3.1 (iii), $h_t(p) \mid (p - (D/p))/2$. Because $h_t(p)$ is even by definition, we see that $(D/p) = 1$. □

Lemma 3.11. *Consider the recurrences $u(a,1)$, $v(a,1)$, and $t(a,1)$ with discriminant D. Let p be an odd prime such that $p \nmid D$. Then, $u(a,b)$, $v(a,b)$, and $t(a,b)$ are all p-regular and $h = h_u(p) = h_v(p) = h_t(p)$.*

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

Proof. Part (i) is proved in Lemma 2 (i) of [21], whereas part (ii) is proved in Lemma 6 (vi) of [20]. □

Lemma 3.12. *Let p be an odd prime. Let $u(a,b)$ be a LSFK with discriminant D such that $p \nmid D$ and restricted period $h = h_u(p)$. Then, $h \mid p - (D/p)$. Let*

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

(i) *There exist exactly $i(p)$ p-equivalence classes of p-regular recurrences in $\mathcal{F}(a,b)$.*
(ii) *Suppose that $i(p) = 1$ and $w(a,b)$ is p-regular. Then, $w(a,b)$ is p-equivalent to $u(a,b)$.*
(iii) *Suppose that $i(p) = 2$ and $w(a,b)$ is p-regular. Then, $A_w(0) \geq 1$ if and only if*

$$\left(\frac{\Delta(w)}{p}\right) = 1.$$

(iv) *Suppose that $i(p) = 2$ and h is odd. If $w(a,b)$ is p-regular, then $w(a,b)$ is p-equivalent to $u(a,1)$ or $v(a,1)$.*
(v) *Suppose that $i(p) = 2$, $p \equiv 1 \pmod 4$, and h is even. If $w(a,b)$ is p-regular, then $w(a,b)$ is p-equivalent to $u(a,b)$ or $t(a,b)$.*
(vi) *If $w(a,b)$ is p-regular and $w(a,b)$ is not p-equivalent to $u(a,b)$, $v(a,b)$, or $t(a,b)$, then $i(p) \geq 3$ and $h_w(p) \leq (p - (D/p))/3$.*

Proof. Part (i) is proved in Theorem 2.14 of [5], Parts (ii), (iv), and (v) follow from (i) of this lemma and from Lemma 3.11. Part (iii) follows from Theorem 1.4 of [23]. Part (vi) follows from parts (ii), (iv), and (v). □

Lemma 3.13. *Let $p \equiv 1 \pmod 4$ be a prime. Consider the Lucas sequences $u(a,1)$ and $v(a,1)$ with discriminant D such that $(D/p) = -1$. Then, $u(a,1)$ and $v(a,1)$ are p-regular, and $h = h_u(p) = h_v(p)$. Suppose that $h = (p+1)/2$. Then, the set $\{u_i u_{i-1}^{-1}\}_{i=2}^{h-1} \cup \{v_i v_{i-1}^{-1}\}_{i=1}^{h}$ form a reduced residue system modulo p.*

Proof. Because $p \nmid D$ and h is odd, we see that $u(a,1)$ and $v(a,1)$ are p-regular, $v(a,1)$ is not p-equivalent to $u(a,1)$, and $\mathcal{A}_v(0) = 0$. Moreover, by Theorem 3.1 (iv), $u_i \not\equiv 0 \pmod p$ for $1 \leq i \leq h-1$. By Lemma 3.9 and inspection, the sets $\{u_i u_{i-1}^{-1}\}_{i=2}^{h-1}$ and $\{v_i v_{i-1}^{-1}\}_{i=1}^{h}$ are disjoint modulo p and together, contain $p-1$ elements. The result now follows. □

Lemma 3.14. *Let $w(a,1) = u(a,1)$ or $v(a,1)$. Let $p \equiv 1 \pmod 4$ be a prime such that $(D/p) = -1$. Then, $h = h_w(p) \equiv 1 \pmod 2$. Moreover, $w_n \not\equiv \pm w_{n+2c} \pmod p$ for any integer n and c such that $0 \leq n < n + 2c \leq h$.*

This follows from Lemma 7 (ii) of [16], in the case in which $w(a,1) = u(a,1)$ and from Lemma 7 of [21], in the case in which $w(a,1) = v(a,1)$.

Lemma 3.15. *Let $w(a,1) = u(a,1)$ or $v(a,1)$. Let $p \equiv 1 \pmod 4$ be a prime such that $(D/p) = -1$. Then, there do not exist three integers i, j, and k such that $0 \leq i < j < k \leq h$, $w_j \equiv \pm w_i \pmod p$, and $w_k \equiv \pm w_i \pmod p$.*

Proof. Suppose that $w_j \equiv \pm w_i \pmod p$ and $w_k \equiv \pm w_i \pmod p$, where $0 \leq i < j < k \leq h$. Then by Lemma 3.14, $j - i \equiv 1 \pmod 2$ and $k - j \equiv 1 \pmod 2$. Hence, $k - i \equiv 0 \pmod 2$, which contradicts Lemma 3.14. □

Lemma 3.16. *Let $w(a,b)$ be a p-regular recurrence. Let $M \equiv M_w(p) \pmod p$, $E = E_w(p)$, $h = h_w(p)$, and $\lambda = \lambda_w(p)$.*

(i) *If $w(a,b)$ is p-equivalent to $u(a,b)$, then $N_w(p) \equiv 1 \pmod E$ and $\delta_w(p) \equiv p-1 \pmod E$.*

(ii) *If $w(a,b)$ is not p-equivalent to $u(a,b)$, then $N_w(p) \equiv 0 \pmod E$ and $\delta_w(p) \equiv p \pmod E$.*

Proof. We observe that $E = \mathrm{ord}_p M$ and $\lambda = Eh$. Consider the term w_n, where $w_n \not\equiv 0 \pmod p$ and $0 \le n \le \lambda - 1 = Eh - 1$. By (1.5), $w_{n+hi} \equiv M^i w_n$ for $i = 0, 1, \ldots, E-1$. We also observe that if $n + hi \ge \lambda = Eh$, then $w_{n+hi-\lambda} \equiv w_n \pmod p$, where $0 \le n + hi - \lambda \le \lambda - 1$. Noting that $A_w(0) \ge 1$ if and only if $w(a,b)$ is p-equivalent to $u(a,b)$, we see that $N_w(p) \equiv 1 \pmod E$, if $w(a,b)$ is p-equivalent to $u(a,b)$ and $N_w(p) \equiv 0 \pmod E$, if $w(a,b)$ is not p-equivalent to $u(a,b)$. The consequences for $\delta_w(p)$ modulo E now follow upon noting that $\delta_w(p) = p - N_w(p)$. □

Theorem 3.17. *Let $p \ge 5$, and let $w(a,1)$ be a p-regular recurrence such that $(D/p) = 1$ and $w(a,1)$ is not p-equivalent to $u(a,1)$. Then, $\lambda_w(p) \mid p-1$ and $A_w(0) = 0$. Furthermore, $\{w_0, w_1, \ldots, w_{\lambda-1}\}$ does not form a reduced residue system modulo p. In particular, $N_w(p) < p-1$ and $\delta_w(p) \ge 2$.*

This follows from Proposition 4.2 of [12]. A proof of Theorem 3.17 is given in the case of the Fibonacci sequence in Theorem 4.2 of [2].

Lemma 3.18. *Let $p \equiv 1 \pmod 4$. Let $w(a,1)$ be a p-regular recurrence such that $w(a,1)$ is not p-equivalent to $u(a,1)$, $(D/p) = 1$, $h_w(p) = (p-1)/4$, and $E_w(p) = 4$. Then, $\delta_w(p) \ge 5$.*

Proof. We observe that $\lambda = \lambda_w(p) = 4h = p - 1$. It follows, from Theorem 3.17 and Lemma 3.16, that $N_w(p) < p - 1$ and $N_w(p) \equiv 0 \pmod 4$. Thus, $N_w(p) \le p - 5$, because $p \equiv 1 \pmod 4$. Hence, $\delta_w(p) = p - N_w(p) \ge 5$. □

Lemma 3.19. *Suppose that the recurrence $t(a,1)$ is defined modulo p. Then, $p \equiv 1 \pmod 4$ and $(D/p) = 1$. Suppose further that $E = E_t(p) = 2$, $M \equiv M_t(p) \pmod p$, and $h = h_t(p) = (p-1)/2$. Then, $\delta_t(p) \equiv 1 \pmod 4$ and $\delta_t(p) \ge 5$.*

Proof. Because $t(a,1)$ is defined modulo p, it follows, from the definition of $t(a,1)$ and Lemma 3.10, that h is even, $(-1/p) = 1$, and $(D/p) = 1$. Thus, $p \equiv 1 \pmod 4$. It follows, from Lemma 3.11 (ii) and Theorem 3.1 (vii), that $A_t(0) = 0$. Because $E = 2$, $\lambda = 2h = p - 1$. Let $r^2 \equiv -1 \pmod p$, where $0 \le r \le (p-1)/2$. Then, $\mathrm{ord_p r} = 4$. We will prove that if $0 \le n \le \lambda - 1$ and $1 \le j \le 3$, then there exists an integer m such that $0 \le m \le \lambda - 1$ and $t_m \equiv r^j t_n \pmod p$. It will then follow that $N_t(p) \equiv 0 \pmod 4$. Noting that $p \equiv 1 \pmod 4$, we then see that $\delta_t(p) \equiv 1 \pmod 4$. Because $E = 2$, we observe that $M \equiv -1 \pmod p$ and $t_{n+h} \equiv -t_n \pmod p$. We now notice that

$$\{t_0, t_1, t_h, t_{h+1}\} \equiv \{1, r, -1, -r\} \pmod p.$$

Thus, we can assume that $n \notin \{0, 1, h, h+1\}$. Suppose that $2 \le n \le 1$. Then by Lemma 3.6 (v),

$$t_{h+1-n} \equiv (-1)^n M r t_n \equiv (-1)^{n+1} \pmod p,$$

$$t_{h+n} \equiv -t_n \pmod p, \quad \text{and} \quad t_{2h+1-n} \equiv -t_{h+1-n} \pmod p.$$

Similarly, if $h + 2 \le n \le \lambda - 1 = 2h - 1$, then $t_{2h+1-n} \equiv \pm r t_n \pmod p$, $t_{n-h} \equiv -t_n \pmod p$, and $t_{3h+1-n} \equiv -t_{2h+1-n} \pmod p$. It now follows that $N_t(p) \equiv 0 \pmod 4$ and $\delta_t(p) \equiv 1 \pmod 4$. By Theorem 3.17, $\delta_t(p) \ge 2$. Hence, $\delta_t(p) \ge 5$. □

Lemma 3.20. *Let $w(a,-1)$ be a p-regular recurrence that is not p-equivalent to $u(a,-1)$, $v(a,-1)$, or $t(a,-1)$. Then, $A_w(d) \le 1$ for $0 \le d \le p-1$. Moreover, $N_w(p) = \lambda_w(p)$ and $\delta_w(p) = p - \lambda_w(p)$.*

This follows from Theorem 2 (i) of [20].

Lemma 3.21. *Consider the LSFK $u(a,1)$ and the LSSK $v(a,1)$ with discriminant $D = a^2+4$. Let $D \neq 0$ and e be a fixed positive odd integer. Let $\{u'_n\}$, $\{u''_n\}$, $\{v'_n\}$, and $\{v''_n\}$ be defined by $u'_n = u_{n+e} - u_n$, $u''_n = u_{n+e} + u_n$, $v'_n = v_{n+e} - v_n$, and $v''_n = v_{n+e} + v_n$. Then, $\{u'_n\}$, $\{u''_n\}$, $\{v'_n\}$, and $\{v''_n\}$ all satisfy the same second-order recursion relation as $u(a,1)$. Moreover, the following hold:*

(i) $u_{2n} = u_n v_n$,
(ii) $(u'_n)^2 - u'_{n-1}u'_{n+1} = (-1)^n(u_{e-1} + u_{e+1}) = (-1)^n v_e$,
(iii) $(u''_n)^2 - u''_{n-1}u''_{n+1} = (-1)^{n+1} v_e$,
(iv) $(v'_n)^2 - v'_{n-1}v'_{n+1} = (-1)^{n+1}(a^2+4)v_e = (-1)^{n+1} D v_e$,
(v) $(v''_n)^2 - v''_{n-1}v''_{n+1} = (-1)^n(a^2+4)v_e = (-1)^n D v_e$.

Proof. It is evident that $\{u'_n\}$, $\{u''_n\}$, $\{v'_n\}$, and $\{v''_n\}$ all satisfy the same recursion relation as $u(a,1)$. Parts (i)–(v) follow from the Binet formulas given in (1.3). Parts (ii)–(v) also follow from the results given in [12, pp. 276, 277, and 279]. □

Lemma 3.22. *Consider the LSFK $u(a,1)$ and the LSSK $v(a,1)$ with discriminant $D = a^2+4$. Let p be a prime such that $p \equiv 1 \pmod 4$, $(D/p) = -1$, and $h = h_u(p) = (p+1)/2$. Then, $u(a,1)$ and $v(a,1)$ are p-regular and $h = h_v(p)$. Let e be an odd integer such that $1 \le e < h$. Let $\{u'_n\}$, $\{u''_n\}$, $\{v'_n\}$, and $\{v''_n\}$ be defined as in Lemma 3.21. Let $w(a,1) = \{u'_n\}$ or $\{u''_n\}$, and let $w'(a,1) = \{v'_n\}$ or $\{v''_n\}$. Then,*

(i) *$A_w(0) \ge 1$ if and only if $(v_e/p) = 1$,*
(ii) *$A_{w'}(0) \ge 1$ if and only if $(v_e/p) = -1$.*

Proof. By Lemmas 1.8 and 3.5, $u(a,1)$ and $v(a,1)$ are p-regular. We note, by Theorem 3.1 (vii), that $A_w(0) \ge 1$ if and only if $w(a,1)$ is trivial modulo p or $w(a,1)$ is p-equivalent to $u(a,1)$. Similarly, $A_{w'}(0) \ge 1$ if and only if (w') is trivial modulo p or (w') is p-equivalent to $u(a,1)$.

(i) Because $e < h \le \lambda_u(p)$, we see that (w) and (w') are nontrivial modulo p. By Lemma 3.12 (iii) and Lemma 3.21 (ii) and (iii), it follows that

$$\Big(\frac{\Delta(w)}{p}\Big) = w_1^2 - w_0 w_2 = \Big(\frac{\pm 1}{p}\Big)\Big(\frac{v_e}{p}\Big).$$

Because $p \equiv 1 \pmod 4$ and thus, $(-1/p) = 1$, we observe that (i) holds.

(ii) Similar to the proof of part (i), we see that

$$\Big(\frac{\Delta(w')}{p}\Big) = (w'_1)^2 - w'_0 w'_2 = \Big(\frac{\pm 1}{p}\Big)\Big(\frac{a^2+4}{p}\Big)\Big(\frac{v_e}{p}\Big).$$

Because $((a^2+4)/p) = -1$, it follows that part (ii) also holds. □

Lemma 3.23. *Let $u(a,-1)$ be a nondegenerate LSFK with discriminant $D = a^2 - 4$ and characteristic roots α and β, where $|\alpha| > |\beta|$. Then,*

$$|u_n| = \Big\lfloor \frac{|\alpha|^n}{\sqrt{D}} \Big\rfloor. \tag{3.2}$$

Proof. Because $u(a,-1)$ is nondegenerate, $|a| \ge \beta$, $D > 0$, α and β are real, $\alpha > 1$, $\beta = 1/\alpha$, and $|\beta| < 1$, It now follows, from the Binet formula (1.3), that (3.2) holds. □

Lemma 3.24. *Let $u(a,1)$ be a nondegenerate LSFK with discriminant $D = a^2+4$ and characteristic roots α and β, where $|\alpha| > |\beta|$. Then,*

$$|u_n| = \left\lceil \frac{|\alpha|^n}{\sqrt{D}} \right\rceil \leq |u_n| + 1. \tag{3.3}$$

Proof. Since $u(a,1)$ is nondegenerate, $|a| \geq 1$, $D > 0$, α and β are real, $|\alpha| > 1$, $\beta = -1/\alpha$, and $|\beta| < 1$. We now see, by the Binet formula (1.3), that (3.3) holds. □

Lemma 3.25. *Consider the LSFK $u(a,b)$ with discriminant $D > 0$, where $a \neq 0$. Then, $|u_n|$ is strictly increasing for $n \geq 2$.*

This is proved in Lemma 3 of [9].

Lemma 3.26. *Let $w(a,1) = u(a,1)$ or $v(a,1)$. Let $p \equiv 1 \pmod 4$ be a prime such that $(D/p) = -1$ and $h = h_w(p) = (p+1)/2$. Then, $E = E_w(p) = 4$. Let $\lambda = \lambda_w(p)$ and $M = M_w(p)$. Let A denote the number of positive odd integers $e < h$ for which there exists an integer n such that $0 \leq n < n+e \leq h$ and $w_{n+e} \equiv \pm w_n \pmod p$. Then,*

$$N_u(p) = 2(h-1-2A)+1 = p-4A, \quad \delta_u(p) = 4A, \tag{3.4}$$

whereas

$$N_v(p) = 2(h+1-2A) = p+3-4A, \quad \delta_u(p) = 4A-3. \tag{3.5}$$

Proof. Because $h = (p+1)/2$ is odd, it follows, from Theorem 3.1 (vii) and Lemma 3.11 (i), that $v(a,1)$ is not p-equivalent to $u(a,1)$ and thus, $A_v(0) = 0$. We also see, by Theorems 3.1 (iv) and 3.2 (iv), that $E = 4$ and $u_n \equiv 0 \pmod p$ if and only if $h \mid n$. Thus, we cannot have that $u_e \equiv \pm u_0$ or $u_h \equiv \pm u_{h-e} \pmod p$ for any positive integer $e < h$. We also note, by Lemma 3.14, that if $0 \leq n < n+c \leq h$ and $w_{n+c} \equiv \pm w_n \pmod p$, then c is odd. Furthermore, by Lemma 3.6 (iii) and (iv), if $0 \leq n \leq \lambda = 4h$, then there exists an integer i such that $0 \leq i \leq h$ and $w_i \equiv \pm w_n \pmod p$. Because $E = 4$, $M^2 \equiv -1 \pmod p$, and $w_{n+2h} \equiv -w_n \pmod p$ for all n. Moreover, by Lemmas 3.7 and 3.8, given a fixed positive integer $e < h$ for which there exists an integer $i \in \{0,1,\ldots,h-e\}$ such that

$$\frac{w_{i+e}}{w_i} \equiv \varepsilon \pmod p;$$

there also exists exactly one integer $j \in \{0,1,\ldots,h-e\}$ such that

$$\frac{w_{j+e}}{w_j} \equiv -\varepsilon \pmod p.$$

In particular, $j = h-i-e$. Additionally, by Lemma 3.15, given an integer $i \in \{0,1,\ldots,h\}$, there exists at most one integer $j \neq i$ such that $0 \leq j \leq h$ and $w_j \equiv \pm w_i \pmod p$. It now follows, from our above discussion, that (3.4) and (3.5) both hold. □

Lemma 3.27. *Let $w(a,1) = u(a,1)$ or $v(a,1)$. Let $p \equiv 1 \pmod 4$ be a prime such that $(D/p) = -1$ and $h = h_w(p) = (p+1)/2$ is odd. Let G_1 denote the number of positive odd integers $e < h$ such that $(v_e/p) = 1$, and let G_2 denote the number of positive odd integers $e < h$ such that $(v_e/p) = -1$. Then,*

$$\delta_u(p) = 2G_1, \tag{3.6}$$

whereas

$$\delta_v(p) = \begin{cases} 2G_2 - 3, & \text{if } p \equiv 1 \pmod 8; \\ 2G_2 - 1, & \text{if } p \equiv 5 \pmod 8. \end{cases} \tag{3.7}$$

Proof. Let B denote the number of positive odd integers e less than h for which there exists an integer n such that $0 \le n \le h-1$ and $w_{n+e} \equiv \pm w_n \pmod{p}$. Then by Lemma 3.22,

$$B = \begin{cases} G_1, & \text{if } w(a,1) = u(a,1); \\ G_2, & \text{if } w(a,1) = v(a,1). \end{cases} \tag{3.8}$$

Let A be defined as in Lemma 3.26. We will show that

$$A = \begin{cases} \frac{B}{2}, & \text{if } w(a,1) = u(a,1); \\ \frac{B}{2}, & \text{if } w(a,1) = v(a,1) \text{ and } p \equiv 1 \pmod{8}; \\ \frac{B+1}{2}, & \text{if } w(a,1) = v(a,1) \text{ and } p \equiv 5 \pmod{8}. \end{cases} \tag{3.9}$$

It will then follow, from (3.8), (3.9), (3.4), and (3.5), that (3.6) and (3.7) both hold.

Let $e < h$ be a fixed positive odd integer. First, suppose that $0 \le n < h < n+e = h+r$ and $w_{n+e} \equiv \pm w_n \pmod{p}$, where $r \ge 1$. Then by Lemma 3.6 (iii) and (iv),

$$w_n \equiv \pm w_{n+e} = w_{h+r} \equiv \pm w_{h-r} \pmod{p},$$

where $3 \le h-r \le h-1$, because $1 \le e \le h-2$. We shall find an integer $i \ne n$ such that $0 \le i \le h-1$, $w_i \equiv \pm w_n \pmod{p}$ and $|n-i| = e_1 \equiv 1 \pmod{2}$, and $1 \le e_1 < e$. We observe that $(h+r)-(h-r) = 2r$. Thus, $h-r \not\equiv n \pmod{2}$, since $h+r-n = e \equiv 1 \pmod{2}$. Hence, $|n-(h-r)| = e_1 \equiv 1 \pmod{2}$.

Now, suppose that $h > h-r > n$. Then,

$$e - e_1 = (h+r-n) - (h-r-n) = 2r > 0.$$

Next, suppose that $h > n > h-r$. Then,

$$e - e_1 = 2(h-n) > 0$$

and again $e > e_1$.

We next suppose that n is the largest integer such that $1 \le n-e < n \le h-1$ and $w_n \equiv \pm w_{n-e} \pmod{p}$. By a similar argument to that given above, we can find an integer c and an odd integer e_2 such that $1 \le i \le h-1$, $1 \le e < e_2 < h$, $i+e_2 > h$, $w_i \equiv \pm w_n \pmod{p}$, and $w_{i+e_2} \equiv \pm w_i \pmod{p}$.

We now treat the final case in which $n = 0$ or h, and

$$w_0 \equiv \varepsilon w_e \pmod{p}. \tag{3.10}$$

By Lemma 3.7, (3.10) can occur if and only if

$$w_h \equiv -\varepsilon w_{h-e} \pmod{p}. \tag{3.11}$$

By the proof of Lemma 3.26, we must then have that $w_0 w_h \not\equiv 0 \pmod{p}$ and $w(a,1) = v(a,1)$.

We now observe, by Lemmas 3.15 and 3.6 (ii), that

$$w_i \equiv \pm w_0 \pmod{p} \tag{3.12}$$

for $i \in \{0, 1, \ldots, 2h\}$ if and only if $i \in \{0, e, 2h-e, 2h\}$, whereas

$$w_i \equiv \pm w_h \pmod{p} \tag{3.13}$$

for $i \in \{0, 1, \ldots, 2h\}$ if and only if $i \in \{h-e, h, h+e\}$.

We note, by Lemma 3.13, that for each positive odd integer $e < h$, there exists an integer n such that $0 \le n \le h-1 = (p-1)/2$ and either $u_{n+e} \equiv \pm u_n \pmod{p}$ or $v_{n+e} \equiv \pm v_n \pmod{p}$. Let

$$E = \#\{e \mid 1 \le e < h,\ e \equiv 1 \pmod{2}\}.$$

By our previous discussion, $A = B/2$, if $E \equiv 0 \pmod 2$ and $A = (B+1)/2$, if $E \equiv 1 \pmod 2$.

We observe that $E = (p-1)/4$. Hence,

$$E \equiv \begin{cases} 0 \pmod 2, & \text{if } p \equiv 1 \pmod 8; \\ 1 \pmod 2, & \text{if } p \equiv 5 \pmod 8. \end{cases}$$

From our argument above, we see that (3.9) holds and the result follows. □

Lemma 3.28. *Let $v(a,1)$ be a LSSK. Let $p \equiv 1 \pmod 4$ be a prime such that $(D/p) = -1$. Let $h = h_v(p)$. Then, $(v_h/p) = 1$.*

Proof. By Theorem 3.2 (vii), $E = 4$. Thus, $M \equiv \pm\sqrt{-1} \pmod p$ and $v_h \equiv Mv_0 \equiv 2M \pmod p$. By the law of quadratic reciprocity, $(2/p) = 1$, if $p \equiv 1 \pmod 8$ and $(2/p) = -1$, if $p \equiv 5 \pmod 8$. Moreover, $(M/p) = 1$, if $p \equiv 1 \pmod 8$ and $(M/p) = -1$, if $p \equiv 5 \pmod 8$. Thus, $(v_h/p) = 1$. □

Lemma 3.29. *Let p_k denote the kth prime. Then,*

$$p_k \geq k(\ln k + \ln\ln k - 1) \tag{3.14}$$

for $k \geq 2$.

This is proved in [8].

Corollary 3.30. *For $k \geq 2$, we have*

$$p_k - 1 \geq k \ln k. \tag{3.15}$$

Proof. By examination, (3.15) holds for $2 \leq k \leq 17$. By Lemma 3.29,

$$p_k - 1 \geq k \ln k + k(\ln\ln k - 1) - 1 \text{ for } k \geq 2. \tag{3.16}$$

It suffices to prove that

$$\ln\ln k - 1 - \frac{1}{k} \geq 0 \text{ for } k \geq 18. \tag{3.17}$$

By inspection, (3.17) holds for $k = 18$. Clearly, this implies that (3.17) is also satisfied for $k \geq 18$. □

Let $w(a,b)$ be a recurrence. Then p is a *primitive prime divisor* of w_n, if $p \mid w_n$ and $p \nmid w_i$ for any i such that $0 \leq i < n$ and $w_i \neq 0$.

Theorem 3.31. *Let $u(a,b)$ be a nondegenerate LSFK for which $\gcd(a,b) = 1$ and the characteristic roots α and β are real. Then, there exist at most four indices n such that u_n has no primitive prime divisor. Moreover, each of these indices is less than or equal to 12.*

This is proved in Theorem XXI of [6].

Theorem 3.32. *Let $u(a,b)$ be a nondegenerate LSFK for which $\gcd(a,b) = 1$. Then, there exist at most nine indices n such that u_n has no primitive prime divisor. Further, each of these indices is less than or equal to 30.*

This follows from Theorem 1.4 and Tables 1 and 3 of [1].

4. The Unboundedness of $(p - (D/p))/h$

Consider the nondegenerate LSFK $u(a, b)$, where $\gcd(a, b) = 1$. Recall, by Theorem 3.1 (i), that $h_u(p) \mid p - (D/p)$. Theorem 4.1 shows that $(p - (D/p))/h_u(p)$ is unbounded as p grows arbitrarily large.

Theorem 4.1. *Let $u(a, b)$ be a nondegenerate LSFK such that $\gcd(a, b) = 1$. Then,*

$$\limsup_{p\to\infty} \frac{p - (D/p)}{h_u(p)} = \infty.$$

Proof. Let α and β be the characteristic roots of $u(a, b)$. Let

$$R = \begin{cases} 4, & \text{if } \alpha \text{ and } \beta \text{ are real;} \\ 9, & \text{if } \alpha \text{ and } \beta \text{ are imaginary.} \end{cases}$$

By Theorems 3.31 and 3.32, there exist at most R indices n for which u_n does not have a primitive prime divisor. Let $n > R$ be an arbitrary integer. It now follows that there are at least $n - R$ different primes that divide u_k for $k \in \{1, \ldots, n\}$.

Hence, there exists a prime p_m such that $h_u(p_m) \le n$ and $m \ge n - R$. By Theorem 3.29, we see that for every $n > R$,

$$\frac{p_m - (D/p)}{h(p_m)} \ge \frac{p_m - 1}{h} \ge \frac{m \ln m}{n} \ge \frac{(n - R)\ln(n - R)}{n} \tag{4.1}$$

and the theorem follows. □

Vinson [26] proved Theorem 4.1 in the case of the Fibonacci sequence. Our proof is adapted from his proof. Two further proofs of Theorem 4.1, in the case of the Fibonacci numbers, are given by [11] and [10].

Theorem 4.2. *Let $w(a, 1)$ be a nondegenerate recurrence with characteristic roots α and β, where $|\alpha| > |\beta|$. Then, α and β are real and*

$$\limsup_{p\to\infty} \frac{\delta_w(p)}{p} = 1. \tag{4.2}$$

Let $0 \le \varepsilon \le 0.4$, and let $r = 22067/22071$. Let

$$n_1 = \left\lceil \frac{1}{r} e^{4/(\varepsilon r)} \right\rceil.$$

Then, there exists a prime p' such that

$$p' \le \left\lceil \frac{|\alpha|^{n_1}}{\sqrt{D}} \right\rceil$$

and

$$\frac{\delta_w(p')}{p'} \ge 1 - \varepsilon. \tag{4.3}$$

Proof. By Theorem 4.1, we have that

$$\liminf_{p\to\infty} \frac{h_u(p)}{p} = 0. \tag{4.4}$$

We claim that this suffices to establish that (4.2) holds. Because $\lambda_u(p) \le 4h_u(p)$, by Theorem 3.2 (i) and $\lambda_w(p) \mid \lambda_u(p)$ by Theorem 3.4 and Lemma 3.5 (i), it would then follow

that $\liminf_{p\to\infty}\lambda_w(p)/p = 0$. Noting by (1.8) that $\delta_w(p) \geq p - \lambda_w(p)$, it then follows that $\limsup_{p\to\infty}\delta_w(p)/p = 1$.

We now find a prime

$$p' \leq \left\lceil \frac{|\alpha|^{n_1}}{\sqrt{D}} \right\rceil \qquad \text{and} \qquad \frac{\delta_w(p')}{p'} \geq 1 - \varepsilon.$$

It suffices to show that

$$\frac{h_w(p')}{p'} \leq \frac{\varepsilon}{4} \tag{4.5}$$

for such a prime p', because $\delta_w(p') = p' - N_w(p')$ and $N_w(p') \leq \lambda_w(p') \leq 4h_w(p')$. Moreover, (4.5) holds if and only if

$$\frac{p'}{h_w(p')} \geq \frac{4}{\varepsilon}. \tag{4.6}$$

Let $n > 4$ be an arbitrary integer. We note that $h_w(p') \mid h_u(p')$ by Theorem 3.4. We now see, by (4.1) in the proof of Theorem 4.1, that there exists $m \geq n - 4$ such that $h_u(p_m) \leq n$ and

$$\frac{p_m}{h_w(p_m)} \geq \frac{p_m}{h_u(p_m)} \geq \frac{p_m - 1}{h_u(p_m)} \geq \frac{(n-4)\ln(n-4)}{n}. \tag{4.7}$$

We wish to find n such that

$$\frac{(n-4)\ln(n-4)}{n} \geq \frac{4}{\varepsilon} \geq \frac{4}{0.4} = 10. \tag{4.8}$$

We also observe that if $n = n_1$, then

$$n_1 = \left\lceil \frac{1}{r}\mathrm{e}^{4/(\varepsilon r)} \right\rceil \geq \left\lceil \frac{1}{r}\mathrm{e}^{4/(0.4r)} \right\rceil = \left\lceil \frac{1}{r}\mathrm{e}^{10/r} \right\rceil = 22071.$$

We will show that if $n = n_1$, then (4.8) holds. We observe that

$$\frac{n_1 - 4}{n_1}\ln\Big(\frac{n_1 - 4}{n_1}n_1\Big) \geq \frac{22067}{22071}\ln\Big(\frac{22067}{22071}n_1\Big) = r\ln(rn_1). \tag{4.9}$$

We claim that

$$r\ln(rn_1) \geq \frac{4}{\varepsilon}. \tag{4.10}$$

We note that (4.10) holds if and only if

$$\mathrm{e}^{\ln(rn_1)} = rn_1 \geq \mathrm{e}^{4/(\varepsilon r)},$$

which is satisfied by the definition of n_1.

By (4.7), there exists $m > n_1 - 4$ such that $h_u(p_m) = s \leq n_1$ and

$$\frac{p_m}{h_w(p_m)} \geq \frac{p_m}{h_u(p_m)} \geq \frac{(n_1-4)\ln(n_1-4)}{n_1} \geq \frac{4}{\varepsilon}.$$

Then, $p_m \mid u_s$. Because $|u_s| \leq |u_{n_1}|$ by Lemma 3.25, we find, by Lemma 3.24, that

$$p_m \leq |u_{n_1}| \leq \left\lceil \frac{|\alpha|^{n_1}}{\sqrt{D}} \right\rceil.$$

The result follows upon letting $p' = p_m$. □

Theorem 4.3. *Let $w(a,-1)$ be a nondegenerate recurrence with characteristic roots α and β, where $|\alpha| > |\beta|$. Then, α and β are real and*

$$\limsup_{p\to\infty} \frac{\delta_w(p)}{p} = 1. \tag{4.11}$$

Let $0 \le \varepsilon \le 0.4$ and let $s = 168/172$. Let

$$n_2 = \left\lceil \frac{1}{s} \mathrm{e}^{2/(\varepsilon s)} \right\rceil.$$

Then, there exists a prime p'' such that

$$p'' \le \left\lfloor \frac{|\alpha|^{n_2}}{\sqrt{D}} \right\rfloor \qquad \text{and} \qquad \frac{\delta_w(p'')}{p''} \ge 1 - \varepsilon.$$

Proof. We observe by Theorem 3.3 (i) that $\lambda_w(p) \le 2h_w(p)$. The remainder of the proof is completely similar to that of Theorem 4.2. □

5. Values of $\delta_w(p)$ for $w(a,\pm1)$ Modulo p

Theorems 5.1–5.11 will provide lower bounds for $\delta_w(p)$, given the prime p and the p-regular sequence $w(a,\pm1)$. The proof of these theorems make use of results that provide upper bounds for $N_w(p)$. We note that $\delta_w(p) = p - N_w(p)$. In the statements of Theorems 5.1–5.11, we will accordingly frequently express $\delta_w(p)$ in the form $p - c(p)$, where $c(p)$ is an expression for $N_w(p)$. In Theorems 5.1–5.11, we let $h = h_w(p)$, $\lambda = \lambda_w(p)$, $M = M_w(p)$, $E = E_w(p)$, and the recurrence $w(a,\pm1)$ will always be considered to be nondegenerate.

In Theorems 5.1–5.3, we consider the nondegenerate recurrence $w(a,-1)$. We recall that by Theorem 3.3, $E = 1$ or 2.

Theorem 5.1. *Consider the p-regular recurrence $w(a,-1)$ such that h is odd, $E = 1$, and $p \nmid D$. Then, $h \mid (p - (D/p))/2$.*

(i) *$u(a,-1)$ is not p-equivalent to $v(a,-1)$. Moreover, if $h = (p-(D/p))/2$, then $w(a,-1)$ is p-equivalent to $u(a,-1)$ or $v(a,-1)$.*

(ii) *If $w(a,-1)$ is p-equivalent to $u(a,-1)$, then $\delta_w(p) = p - h \ge (p + (D/p))/2$.*

(iii) *If $w(a,-1)$ is p-equivalent to $v(a,-1)$, then*

$$\delta_w(p) = p - \frac{h+1}{2} \ge \frac{3p - 2 + (D/p)}{4}.$$

(iv) *Suppose that $w(a,-1)$ is not p-equivalent to $u(a,-1)$ or $v(a,-1)$. Then,*

$$h \le \frac{p - (D/p)}{4} \qquad \text{and} \qquad \delta_w(p) = p - \lambda \ge \frac{3p + (D/p)}{4}.$$

Theorem 5.2. *Consider the p-regular recurrence $w(a,-1)$ such that h is odd, $E = 2$, and $p \nmid D$. Then, $h \mid (p - (D/p))/2$.*

(i) *$u(a,-1)$ is not p-equivalent to $v(a,-1)$. Moreover, if $h = (p-(D/p))/2$, then $w(a,-1)$ is p-equivalent to $u(a,-1)$ or $v(a,-1)$.*

(ii) *If $w(a,-1)$ is p-equivalent to $u(a,-1)$, then $\delta_w(p) = p - h \ge (p + (D/p))/2$.*

(iii) *If $w(a,-1)$ is p-equivalent to $v(a,-1)$, then*

$$\delta_w(p) = p - (h+1) \ge \frac{p - 2 + (D/p)}{2}.$$

(iv) *Suppose that* $w(a,-1)$ *is not* p*-equivalent to* $u(a,-1)$ *or* $v(a,-1)$*. Then,*

$$h \le \frac{p-(D/p)}{4} \qquad \text{and} \qquad \delta_w(p) = p-\lambda = p-2h \ge \frac{p+(D/p)}{2}.$$

Theorem 5.3. *Consider the* p*-regular recurrence* $w(a,-1)$ *such that* h *is even and* $p \nmid D$*. Then,* $E=2$*,* $h \mid (p-(D/p))/2$*, and* $\lambda = 2h$*.*

(i) $v(a,-1)$ *is* p*-equivalent to* $u(a,-1)$ *and* $t(a,-1)$ *is not* p*-equivalent to* $u(a,-1)$*. Moreover, if* $h=(p-(D/p))/2$*, then* $w(a,-1)$ *is* p*-equivalent to* $u(a,-1)$ *or* $t(a,-1)$*.*

(ii) *If* $w(a,-1)$ *is* p*-equivalent to* $u(a,-1)$*, then* $\delta_w(p) = p-(h+1) \ge (p-2+(D/p))/2$*.*

(iii) *If* $w(a,-1)$ *is* p*-equivalent to* $t(a,-1)$*, then* $\delta_w(p) = p-h \ge (p+(D/p))/2$*.*

(iv) *Suppose* $w(a,-1)$ *is not* p*-equivalent to* $u(a,-1)$ *or* $t(a,-1)$*. Then,*

$$h \le \frac{p-(D/p)}{4} \qquad \text{and} \qquad \delta_w(p) = p-\lambda = p-2h \ge \frac{p+(D/p)}{2}.$$

Theorems 5.1–5.3 follow from Lemma 3.20, Theorem 7 of [18], Theorems 10–12 of [21], and Theorem 3.8 (b) of [22].

Theorem 5.4. *Let* $p \equiv 3 \pmod 4$*. Consider the* p*-regular recurrence* $w(a,1)$ *such that* $(D/p)=1$*. Then,* $E=1$*,* $\lambda = h$*,* $h \equiv 2 \pmod 4$*, and* $h \mid p-1$*, but* $h \nmid (p-1)/2$*.*

(i) *Suppose that* $h=p-1$*. Then* $w(a,1)$ *is* p*-equivalent to* $u(a,1)$*. Further,* $\delta_w(p) = (3p-1)/8$*, if* $p \equiv 3 \pmod 8$ *and* $\delta_w(p) = (3p+3)/8$*, if* $p \equiv 7 \pmod 8$*.*

(ii) *Suppose that* $w(a,1)$ *is* p*-equivalent to* $u(a,1)$ *and* $h < p-1$*. Then,* $h \le (p-1)/3$ *and* $\delta_w(p) \ge p-(3h+2)/4 \ge (3p-1)/4$*.*

(iii) *Suppose that* $w(a,1)$ *is not* p*-equivalent to* $u(a,1)$*. Then,* $h \le (p-1)/3$ *and* $\delta_w(p) \ge (2p+1)/3$*.*

Part (i) is proved in Theorem 2.7 of [25]. The remainder of Theorem 5.4 follows from (1.8) and Theorem 6 of [17].

Theorem 5.5. *Let* $p \equiv 3 \pmod 4$*. Consider the* p*-regular recurrence* $w(a,1)$ *such that* $(D/p)=-1$*. Then,* $E=2$*,* $\lambda = 2h$*,* $h \equiv 0 \pmod 4$*, and* $h \mid p+1$*, but* $h \nmid (p+1)/2$*.*

(i) *Suppose that* $h=p+1$*. Then,* $w(a,1)$ *is* p*-equivalent to* $u(a,1)$*. Moreover,* $\delta_w(p) = (p-3)/4$*, if* $p \equiv 3 \pmod 8$ *and* $\delta_w(p) = (p-7)/4$*, if* $p \equiv 7 \pmod 8$*.*

(ii) *Suppose that* $w(a,1)$ *is* p*-equivalent to* $u(a,1)$ *and* $h < p+1$*. Then,* $h \le (p+1)/3$ *and* $\delta_w(p) \ge p-(h+1) \ge (2p-4)/3$*.*

(iii) *Suppose that* $w(a,1)$ *is not* p*-equivalent to* $u(a,1)$*. Then,* $h \le (p+1)/3$ *and* $\delta_w(p) \ge p-\lambda = p-2h \ge (p-2)/3$*.*

This follows from (1.8) and Theorem 8 of [17].

In Theorems 5.6–5.8, we consider p-regular recurrences $w(a,1)$ for which $p \equiv 1 \pmod 4$ and $(D/p)=1$. In this situation, we have that E can be equal 1, 2, or 4 and all possibilities can occur. We will consider these three cases separately.

Theorem 5.6. *Let* $p \equiv 1 \pmod 4$*. Consider the* p*-regular recurrence* $w(a,1)$ *such that* $(D/p)=1$ *and* $E=1$*. Then,* $\lambda = h$*,* $h \equiv 2 \pmod 4$*, and* $h \mid (p-1)/2$*.*

(i) $v(a,1)$ *is* p*-equivalent to* $u(a,1)$ *and* $t(a,1)$ *is not* p*-equivalent to* $u(a,1)$*. Moreover, if* $h=(p-1)/2$*, then* $w(a,1)$ *is* p*-equivalent to* $u(a,1)$ *or* $t(a,1)$*.*

(ii) *If* $w(a,1)$ *is* p*-equivalent to* $u(a,1)$*, then* $\delta_w(p) \ge p-(3h+2)/4 \ge (5p-1)/8$*.*

(iii) *If* $w(a,1)$ *is* p*-equivalent to* $t(a,1)$*, then* $\delta_w(p) \ge p-\lambda \ge (p+1)/2$*.*

(iv) *Suppose that* $w(a,1)$ *is not* p*-equivalent to* $u(a,1)$ *or* $t(a,1)$*. Then,* $\lambda \le (p-1)/4$ *and* $\delta_w(p) \ge p-\lambda \ge (3p+1)/4$*.*

This follows from (1.8) and Theorem 6 of [17].

Theorem 5.7. *Let $p \equiv 1 \pmod 4$. Consider the p-regular recurrence $w(a,1)$ such that $(D/p) = 1$ and $E = 2$. Then, $\lambda = 2h$, $h \equiv 0 \pmod 4$, and $h \mid (p-1)/2$.*

(i) *$v(a,1)$ is p-equivalent to $u(a,1)$ and $t(a,1)$ is not p-equivalent to $u(a,1)$. Moreover, if $h = (p-1)/2$, then $w(a,1)$ is p-equivalent to $u(a,1)$ or $t(a,1)$.*
(ii) *If $w(a,1)$ is p-equivalent to $u(a,1)$, then $\delta_w(p) \geq p - (h+1) \geq (p-1)/2$.*
(iii) *If $w(a,1)$ is p-equivalent to $t(a,1)$ and $h = (p-1)/2$, then $\delta_w(p) \geq 5$.*
(iv) *Suppose $w(a,1)$ is p-equivalent to $t(a,1)$ and $h < (p-1)/2$ or that $w(a,1)$ is not p-equivalent to $u(a,1)$ or $t(a,1)$. Then, $h \leq (p-1)/4$ and $\delta_w(p) \geq p - \lambda = p - 2h \geq (p+1)/2$.*

Part (iii) is proved in Lemma 3.19. The remainder of Theorem 5.7 follows from (1.8) and Theorem 8 of [17].

Theorem 5.8. *Let $p \equiv 1 \pmod 4$. Consider the p-regular recurrence $w(a,1)$ such that $(D/p) = 1$ and $E = 4$. Then, $\lambda = 4h$, h is odd, and $h \mid (p-1)/4$.*

(i) *$v(a,1)$ is not p-equivalent to $u(a,1)$. Moreover, if $h = (p-1)/2$, then $w(a,1)$ is p-equivalent to $u(a,1)$ or $v(a,1)$.*
(ii) *If $w(a,1)$ is p-equivalent to $u(a,1)$, then $\delta_w(p) \geq p - (2h-1) \geq (p+3)/2$.*
(iii) *If $w(a,1)$ is p-equivalent to $v(a,1)$, then $\delta_w(p) \geq p - (2h+2) \geq (p-3)/2$.*
(iv) *Suppose that $w(a,1)$ is not p-equivalent to $u(a,1)$ or $v(a,1)$.*
  (a) *If $h = (p-1)/4$, then $p \equiv 5 \pmod 8$ and $\delta_w(p) \geq 5$.*
  (b) *If $h < (p-1)/4$, then $h \leq (p-1)/8$ and $\delta_w(p) \geq p - \lambda = p - 4h \geq (p+1)/2$.*

Part (iv) (a) is proved in Lemma 3.18. The remainder of Theorem 5.8 follows from (1.8), Theorem 10 of [17], and Theorem 9 of [21].

Theorem 5.9. *Let $p \equiv 1 \pmod 4$. Consider the p-regular recurrence $w(a,1)$ such that $(D/p) = -1$ and $h \neq (p+1)/2$. Then, $E = 4$, $\lambda = 4h$, $h \mid (p+1)/2$, and $h \leq (p+1)/6$.*

(i) *$v(a,1)$ is not p-equivalent to $u(a,1)$.*
(ii) *If $w(a,1)$ is p-equivalent to $u(a,1)$, then $\delta_w(p) \geq p - (2h-1) \geq (2p+2)/3$.*
(iii) *If $w(a,1)$ is p-equivalent to $v(a,1)$, then $\delta_w(p) \geq p - (2h+2) \geq (2p-7)/3$.*
(iv) *Suppose $w(a,1)$ is not p-equivalent to $u(a,1)$ or $v(a,1)$. Then, $\delta_w(p) \geq p - \lambda = p - 4h \geq (p-2)/3$.*

This follows from (1.8), Theorem 10 of [17], and Theorem 9 of [21].

We note, by Lemma 3.12 (ii), that if $p \equiv 1 \pmod 4$ and $w(a,1)$ is a p-regular recurrence such that $(D/p) = -1$ and $h_w(p) = (p+1)/2$, then $w(a,1)$ is p-equivalent to $u(a,1)$ or $v(a,1)$. In Theorems 5.10 and 5.11, we treat these cases separately. These theorems generalize results given by Li [12].

Theorem 5.10. *Let $p \equiv 1 \pmod 4$. Consider the p-regular recurrence $w(a,1)$ such that $w(a,1)$ is p-equivalent to $u(a,1)$, $(D/p) = -1$, and $h = h_w(p) = h_u(p) = (p+1)/2$. Consider also the LSSK $v(a,1)$. Let C be a positive integer. Then, $\delta_w(p) \geq C$ if*

$$p > 2^{2\lfloor \frac{C-1}{2} \rfloor + 3}\Big(\Big\lfloor \frac{C-1}{2} \Big\rfloor + 1\Big) - 3.$$

Proof. We can assume, without loss of generality, that $w(a,1) = u(a,1)$ by Proposition 1.4 and Remark 1.5. As in Lemma 3.27, let G_1 denote the number of positive odd integers $e < h$ such that $(v_e/p) = 1$. We will assume that $\delta_u(p) \leq C - 1$ and get a contradiction for large

enough p. Because $\delta_u(p) = 2G_1$ by Lemma 3.27, we will assume that $2G_1 \leq C - 1$, which holds if and only if

$$G_1 \leq \left\lfloor \frac{C-1}{2} \right\rfloor = C_1.$$

By Theorem 3.1 (iv) and (vii) and Lemma 3.11 (i), $v_n \not\equiv 0 \pmod{p}$ for all $n \geq 0$ and $u_n \equiv 0 \pmod{p}$ if and only if $h \mid n$. Let $s = (h+1)/2 = (p+3)/4$. We note, by Lemma 3.7, that if $1 < i < s$, then

$$(u_i u_{i-1}^{-1})(u_{h-i+1} u_{h-i}^{-1}) \equiv -1 \pmod{p} \tag{5.1}$$

and $i < h - i + 1 < h$. Moreover, by Lemma 3.7, if $1 \leq i < s$, then

$$(v_i v_{i-1}^{-1})(v_{h-i+1} v_{h-i}^{-1}) \equiv -1 \pmod{p} \tag{5.2}$$

and $i < h - i + 1 \leq h$. Since $p \equiv 1 \pmod{4}$ and thus, $(-1/p) = 1$, it follows from (5.1) and (5.2) that

$$\left(\frac{u_i u_{i-1}^{-1}}{p}\right) = \left(\frac{u_{h-i+1} u_{h-i}^{-1}}{p}\right) \tag{5.3}$$

for $1 < i < s$ and

$$\left(\frac{v_i v_{i-1}^{-1}}{p}\right) = \left(\frac{v_{h-i+1} v_{h-i}^{-1}}{p}\right) \tag{5.4}$$

for $1 < i < s$.

First, suppose that $p \equiv 1 \pmod{8}$. We note, by Lemma 3.28 and the law of quadratic reciprocity, that

$$\left(\frac{v_0}{p}\right) = \left(\frac{2}{p}\right) = \left(\frac{v_h}{p}\right) = 1. \tag{5.5}$$

We now see, by (5.4), that $(v_1/p) = (v_{h-i}/p)$. By (5.4) and induction, it follows that

$$\left(\frac{v_i}{p}\right) = \left(\frac{v_{h-i}}{p}\right) \tag{5.6}$$

for all $i \in \{0, 1, \ldots, s\}$. We note that i is odd if and only if $h - i$ is even. By assumption, there are at most $G_1 \leq C_1 = \lfloor (C-1)/2 \rfloor$ positive odd integers $e < h$ such that $(v_e/p) = 1$. Hence, there exist at most C_1 positive even integers $e < h$ such that $(v_e/p) = 1$. Therefore, among $\{v_i v_{i-1}^{-1} \mid 1 \leq i \leq h\}$, there are at most $4C_1$ quadratic nonresidues modulo p. Thus, there are at least $(p+1)/2 - 4C_1$ nonzero quadratic residues in $\{v_i v_{i-1}^{-1} \mid 1 \leq i \leq h\}$.

We note, by the proof of Lemma 3.13, that $\{u_i u_{i-1}^{-1} \mid 1 < i < h\}$ and $\{v_i v_{i-1}^{-1} \mid 1 \leq i \leq h\}$ together contain exactly $p - 1$ distinct nonzero residues modulo p, and thus, form a reduced residue system modulo p. Thus, we will get a contradiction if we find $4C_1$ nonzero quadratic residues modulo p among $\{u_i u_{i-1}^{-1} \mid 1 < i < h\}$. Therefore, by (5.3), our claim will follow if we can prove that there exist $2C_1$ integers i with $1 < i < s = (p+3)/4$ such that $u_i u_{i-1}^{-1}$ is a nonzero quadratic residue modulo p.

By Lemma 3.21 (i), $u_{2n} = u_n v_n$. Suppose that e is even and $(v_e/p) = -1$. Then, we have that $(u_{2e}/p) = -(u_e/p)$, and because e is even, it follows that there exists i with $e < i \leq 2e$ such that $(u_i/p) = (u_{i-1}/p)$. Hence, $u_i u_{i-1}^{-1}$ is a nonzero quadratic residue modulo p. Thus, our strategy is finding s large enough so that we can find $2C_1$ positive even integers $e(i)$ with $2e(i) = e(i+1)$ for $1 \leq i \leq 2C_1 - 1$ and $2e(2C_1) < s$ such that $(v_{e(i)}/p) = -1$ for all $i \in \{1, \ldots, 2C_1\}$. Because by assumption, there exist at most C_1 positive even integers e such that $(v_e/p) = 1$, we see, by the argument given by Li in [12], that the worst case is that

$$\left(\frac{v_2}{p}\right) = \left(\frac{v_4}{p}\right) = \ldots = \left(\frac{v_{2C_1}}{p}\right) = 1.$$

In this case, we can choose

$$e(1) = 2(C_1 + 1),\ e(2) = 4(C_1 + 1),\ \ldots,\ e(2C_1) = 2^{2C_1}(C_1 + 1).$$

Hence, for $s > 2^{2C_1+1}(C_1 + 1)$, we get a contradiction. Because $p = 4s - 3$, we then obtain that

$$p > 2^{2C_1+3}(C_1 + 1) - 3 = 2^{2\lfloor (C-1)/2 \rfloor + 3}\Big(\Big\lfloor \frac{C-1}{2} \Big\rfloor + 1\Big) - 3.$$

Next, suppose that $p \equiv 5 \pmod 8$. We observe, by Lemma 3.28 and the law of quadratic reciprocity, that

$$\Big(\frac{v_0}{p}\Big) = \Big(\frac{2}{p}\Big) = -1 = -\Big(\frac{v_h}{p}\Big).$$

Thus, by (5.4), $(v_1/p) = -(v_{h-i}/p)$. We now see, by (5.4) and induction, that

$$\Big(\frac{v_i}{p}\Big) = -\Big(\frac{v_{h-i}}{p}\Big) \tag{5.7}$$

for $i \in \{0, 1, \ldots, s\}$. By assumption, there are at most $G_1 \le C_1$ positive odd integers less than h such that $(v_e/p) = 1$. Hence, there exist at most C_1 positive even integers $e < h$ such that $(v_e/p) = -1$. Thus, among $\{v_i v_{i-1}^{-1} \,|\, 1 \le i \le h\}$ modulo p, there are at most $4C_1$ nonzero quadratic residues modulo p, so there are at least $(p+1)/2 - 4C_1$ quadratic nonresidues modulo p in $\{v_i v_{i-1}^{-1} \,|\, 1 \le i \le h\}$. Therefore, by the same argument as above, our claim will follow if we can prove for s large enough that $2C_1$ integers i with $1 < i < s = (p+3)/4$ such that $u_i u_i^{-1}$ is a quadratic nonresidue modulo p. Suppose that e is odd and $(v_e/p) = -1$. Then, we have that $(u_{2e}/p) = -(u_e/p)$, and it follows that there exists an integer i with $1 < i < s$ such that $(u_i/p) = -(u_{i-1}/p)$. Therefore, $u_i u_{i-1}^{-1}$ is a quadratic nonresidue modulo p. Hence, our strategy is to find s large enough so that we are able to discover $2C_1$ positive odd integers $e(i)$ with $2e(i) < e(i+1)$ for $1 \le i \le 2C_1 - 1$ and $2e(2C_1) < s$ such that $(v_{e(i)}/p) = -1$ for all $i \in \{1, \ldots, 2C_1\}$. Since, by assumption, there exist at most $2C_1$ odd integers e such that $(v_e/p) = 1$, the worst case is that

$$\Big(\frac{v_1}{p}\Big) = \Big(\frac{v_3}{p}\Big) = \cdots = \Big(\frac{v_{2C_1-1}}{p}\Big) = 1.$$

In this case, we can choose

$$e(1) = 2C_1 + 1,\ e(2) = 4C_1 + 3,\ \ldots,\ e(2C_1) = 2^{2C_1}C_1 + 2^{2C_1} - 1 < 2^{2C_1}(C_1 + 1).$$

Thus, for $s > 2^{2C_1+1}(C_1 + 1)$, we get a contradiction. Noting that $p = 4s - 3$, we also have that

$$p > 2^{2C_1+3}(C_1 + 1) - 3 = 2^{2\lfloor (C-1)/2 \rfloor + 3}\Big(\Big\lfloor \frac{C-1}{2} \Big\rfloor + 1\Big).$$

The result follows. □

Theorem 5.11. *Let $p \equiv 1 \pmod 4$. Consider the p-regular recurrence $w(a, 1)$ such that $w(a, 1)$ is p-equivalent to $v(a, 1)$, $(D/p) = -1$, and $h = h_w(p) = h_v(p) = (p+1)/2$. Consider also the LSFK $u(a, 1)$. Let C be a positive integer. Then, $\delta_w(p) \ge C$ if*

$$p > 2^{2\lfloor (C+2)/2 \rfloor + 3}\Big(\Big\lfloor \frac{C+2}{2} \Big\rfloor + 1\Big) - 3.$$

Proof. The proof of Theorem 5.11 is similar in structure to that of Theorem 5.10. Without loss of generality, we can assume that $w(a, 1) = v(a, 1)$. As in Lemma 3.27, let G_2 denote the number of positive odd integers $e < h$ such that $(v_e/p) = -1$. We will assume that $\delta_v(p) \le C - 1$ and get a contradiction for large enough p. Let $s = (h+1)/2 = (p+3)/4$.

First, suppose that $p \equiv 1 \pmod 8$. Then by Lemma 3.27, $\delta_v(p) = 2G_2 - 3 \leq C - 1$, which holds if $G_2 \leq \lfloor (C+2)/2 \rfloor = C_2$. It follows, by (5.6) in the proof of Theorem 5.10 for the case in which $p \equiv 1 \pmod 8$, that $(v_i/p) = (v_{h-i}/p)$ for all $i \in \{0, \ldots, s\}$. We observe that i is odd if and only if $h - i$ is even. By assumption, there are at most $G_2 \leq C_2$ positive odd integers $e < h$ such that $(v_e/p) = -1$. Hence, there exist at most C_2 positive even integers $e < h$ such that $(v_e/p) = -1$. Therefore, among $\{v_i v_{i-1}^{-1} \,|\, 1 \leq i \leq h\}$ there are at most $4C_2$ quadratic nonresidues modulo p. Thus, there are at least $(p+1)/2 - 4C_2$ nonzero quadratic residues modulo p in $\{v_i v_{i-1}^{-1} \,|\, 1 \leq i \leq h\}$. Therefore, by the same argument as that given in the proof of Theorem 5.10 for the case in which $p \equiv 1 \pmod 8$, our claim will follow if we can prove that for s large enough, there exist $2C_2$ integers with $1 \leq i < s = (p+3)/4$ such that $u_i u_{i-1}^{-1}$ is a nonzero quadratic residue modulo p. Suppose that e is odd and $(v_e/p) = 1$. Then, we have that $(u_{2e}/p) = (u_e/p)$, and because e is odd, it follows that there exists i with $e < i \leq 2e$ such that $(u_i/p) = (u_{i-1}/p)$. Hence, $u_i u_{i-1}^{-1}$ is a nonzero quadratic residue modulo p. Thus, our strategy is finding s large enough so that we can discover $2C_2$ positive odd integers $e(i)$ with $2e(i) < e(i+1)$ for $1 \leq i \leq 2C_2 - 1$ and $2e(C_2) < s$ such that $(v_{e(i)}/p) = 1$ for all $i \in \{1, \ldots, 2C_2\}$. Because, by assumption, there exist at most C_2 odd integers $e < h$ such that $(v_e/p) = -1$, the worst case is that

$$\Big(\frac{v_1}{p}\Big) = \Big(\frac{v_3}{p}\Big) = \cdots = \Big(\frac{v_{2C_2-1}}{p}\Big) = -1.$$

In this case, we can choose

$$e(1) = 2C_2 + 1,\ e(2) = 4C_1 + 3,\ \ldots,\ e(2C_2) = 2^{2C_2}C_2 + 2^{2C_2} - 1 < 2^{2C_2}(C_2 + 1).$$

Thus, for $s > 2^{2C_2+1}(C_2+1)$, we get a contradiction. Since $p = 4s - 3$, we also have that

$$p > 2^{2C_2+3}(C_2+1) - 3 = 2^{2\lfloor (C+2)/2 \rfloor + 3}\Big(\Big\lfloor \frac{C+2}{2} \Big\rfloor + 1\Big) - 3.$$

Finally, suppose that $p \equiv 5 \pmod 8$. Then by Lemma 3.27, $\delta_v(p) = 2G_2 - 1 \leq C - 1$ occurs if and only if $G_2 \leq \lfloor C/2 \rfloor = C_3$. It follows, by (5.7) in the proof of Theorem 5.10 for the case in which $p \equiv 5 \pmod 8$, that $(v_i/p) = -(v_{h-i}/p)$ for $0 \leq i \leq s$. By assumption, there exist at most C_3 positive integers $e < h$ such that $(v_e/p) = -1$. Hence, there exist at most C_3 positive even integers less than h such that $(v_e/p) = 1$. Thus, among $\{v_i v_{i-1}^{-1} \,|\, 1 \leq i \leq h\}$ modulo p, there are at most $4C_3$ nonzero quadratic residues modulo p. So, there are at least $(p+1)/2 - 4C_3$ quadratic nonresidues modulo p in $\{v_i v_{i-1}^{-1} \,|\, 1 \leq i \leq h\}$. Therefore, by the same argument as that given in the proof of Theorem 5.10 for the case in which $p \equiv 1 \pmod 8$, our claim will follow if we can show that there exist $2C_3$ integers i with $1 \leq i \leq s$ such that $u_i u_{i-1}^{-1}$ is a quadratic nonresidue modulo p. Suppose that e is even and $(v_e/p) = -1$. Then, we have that $(u_{2e}/p) = -(u_e/p)$, and it follows that there exists an integer i with $e < i \leq 2e$ such that $(u_i/p) = -(u_{i-1}/p)$. Therefore, $u_i u_{i-1}^{-1}$ is a quadratic nonresidue modulo p. Hence, our strategy is to find s large enough so that we are able to discover $2C_3$ positive even integers $e(i)$ with $2e(i) = e(i+1)$ for $1 \leq i \leq 2C_3 - 1$ and $2e(2C_3) < s$ such that $(v_{e(i)}/p) = -1$ for all $i \in \{1, \ldots, 2C_3\}$. The worst case is that

$$\Big(\frac{v_2}{p}\Big) = \Big(\frac{v_4}{p}\Big) = \cdots = \Big(\frac{v_{2C_3}}{p}\Big) = 1.$$

In this case, we can choose

$$e(1) = 2(C_3 + 1),\ e(2) = 4(C_3 + 1),\ \ldots,\ e(2C_3) = 2^{2C_3}(C_3 + 1).$$

Therefore, for $s > 2^{2C_3+1}(C_3+1)$, we get a contradiction. Then,

$$p = 4s - 3 > 2^{2C_3+3}(C_3+1) - 3 = 2^{2\lfloor C/2 \rfloor + 3}\Big(\Big\lfloor \frac{C}{2} \Big\rfloor + 1\Big) - 3.$$

The result follows. □

6. Proofs of the Main Results

Proof of Theorem 2.3. This follows from Theorems 5.1–5.3, and Theorems 4.1 and 4.3. □

Proof of Theorems 2.4 and 2.5. These follow from Theorems 5.4–5.11, and Theorems 4.1 and 4.2. □

7. Concluding Remarks

We now address the issue regarding why we only consider the cases in which $b = \pm 1$. Suppose that $|b| > 1$. Then by a generalization of the Artin conjecture, there exist infinitely many odd primes p such that $\frac{p-1}{2} \mid \mathrm{ord}_p(-b)$. It then follows, from Theorem 7 of [19], that for any LSFK $u(a,b)$ for which $(D/p) = -1$, we have that $E_u(p) = p-1$. In this case, we have that $u_{hi+1} \equiv M^i u_1 \equiv M^i \pmod{p}$ for $1 \le i \le p-2$. Because $\mathrm{ord}_p M = p-1$ and $u_0 = 0$, we see that $N_u(p) = p$ and $\delta_u(p) = 0$ for these primes. Hence, it would not be true that $\lim_{p\to\infty} \delta_u(p) = \infty$ as stated in Theorems 2.3 and 2.5.

Acknowledgement

This paper was supported by RVO 67985840 of the Czech Republic.

References

[1] Yu. Bilu, G. Hanrot, and P. M. Voutie, *Existence of primitive divisors of Lucas and Lehmer numbers*, J. Reine Angew. Math., **539** (2001), 75–122.
[2] O. J. Brison, *Complete Fibonacci sequences in finite fields*, The Fibonacci Quarterly, **30.4** (1992), 295–304.
[3] G. Bruckner, *Fibonacci sequence modulo a prime $p \equiv 3 \pmod 4$*, The Fibonacci Quarterly **8.3** (1970), 217–220.
[4] R. T. Bumby, *A distribution property for linear recurrence of the second order*, Proc. Amer. Math. Soc., **50** (1975), 101–106.
[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 the 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] P. Dusart, *The kth prime is greater than $k(\ln k + \ln\ln k - 1)$ for $k \ge 2$*, Math. Comp., **68** (1999), 411–415.
[9] P. Hilton, J. Pedersen, and L. Somer *On Lucasian numbers*, The Fibonacci Quarterly, **35.1** (1997), 43–47.
[10] D. Jarden, *Recurring sequences: A collection of papers*, Third edition. Riveon Lematematika, Jerusalem, 1973, 5–6.
[11] D. Jarden, *Two theorems on Fibonacci's sequence*, Amer. Math. Monthly, **53** (1946), 425–427.
[12] H.-C. Li, *Complete and reduced systems of second-order recurrences modulo p*, The Fibonacci Quarterly, **38.3** (2000), 272–281.
[13] A. Schinzel, *Special Lucas sequences including the Fibonacci sequence, modulo a prime. A Tribute to Paul Erdös*, A. Baker et al. (eds.), Cambridge Univ. Press, Cambridge, 1990, 349–357.
[14] A. P. Shah, *Fibonacci sequence modulo m*, The Fibonacci Quarterly, **6.2** (1968), 139–141.
[15] L. Somer, *The divisibility properties of primary Lucas recurrences with respect to primes*, The Fibonacci Quarterly, **18.4** (1980), 316–334.
[16] 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.), Vol. 2, 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, *Distribution of certain second-order linear recurrences modulo p. II.*, The Fibonacci Quarterly, **29.1** (1991), 72–78.
[19] 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.
[20] 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.), Vol. 5, (St. Andrew, 1992), Kluwer Acad. Publ., Dordrecht, 1993, 527–546.
[21] 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.
[22] L. Somer and W. Carlip, *Stability of second-order recurrences modulo p^r*, Int. J. Math. Math. Sci., **23** (2000), 225–241.
[23] 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.
[24] L. Somer and M. Křížek, *Identically distributed second-order linear recurrences modulo p*, The Fibonacci Quarterly, **53.4** (2015), 290–312.
[25] L. Somer and M. Křížek, *Identically distributed second-order linear recurrences modulo p, II.*, The Fibonacci Quarerly, **54.3** (2016), 217–234.
[26] J. Vinson, *A new proof of a theorem of Jarden*, Amer. Math. Monthly, **69** (1962), 534.
[27] M. Ward, *Prime divisors of second order recurring sequences*, Duke Math. J., **21** (1954), 607–614.
[28] W. A. Webb, C. T. Long, *Distribution modulo p^h of the general linear second order recurrence*, Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur., **58.8** (1975), 92–100.

MSC2020: 11B39, 11A07

Lawrence Somer, Department of Mathematics, Catholic University of America, Washington, DC 20064
Email address: somer@cua.edu

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