EASY CRITERIA TO DETERMINE IF A PRIME DIVIDES CERTAIN SECOND-ORDER RECURRENCES

LAWRENCE SOMER AND MICHAL KŘÍŽEK

ABSTRACT. Let $\mathcal{F}(a,b)$ denote the set of all second-order recurrences $w(a,b)$ satisfying the recursion relation

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

where the discriminant $D = a^2 + 4b$ and a, b, w_0, and w_1 are all integers. Let $u(a,b)$ denote the recurrence with initial terms $u_0 = 0$ and $u_1 = 1$. We say that the prime p is a divisor of $w(a,b)$ if $p \mid w_n$ for some integer $n \geq 0$. Let $z(p)$ denote the least positive integer n such that $u_n \equiv 0 \pmod{p}$. Then $z(p) \mid p - (D/p)$, where (D/p) denotes the Legendre symbol. Define the index $i(p)$ as

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

When $i(p) = 1$ or 2, we will find easy criteria to determine exactly when p is a divisor of $w(a,b)$ based on the residue class or quadratic character of $w_1^2 - aw_1w_0 - bw_0^2$ modulo p. This generalizes results of Vandervelde when $a = b = 1$.

1. INTRODUCTION

Let $\mathcal{F}(a,b)$ denote the set of all second-order recurrences $w(a,b)$ satisfying the linear recursion relation

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

with discriminant $D = a^2 + 4b$, where the parameters a and b and the initial terms w_0 and w_1 are all integers. We distinguish two particular recurrences, the Lucas sequence $(u) = u(a,b)$, and the companion Lucas sequence $(v) = v(a,b)$ in $\mathcal{F}(a,b)$ which have initial terms $u_0 = 0$, $u_1 = 1$ and $v_0 = 2$, $v_1 = a$, respectively. We say that the prime p is a divisor of $w(a,b)$ if $p \mid w_n$ for some $n \geq 0$. In this paper, we will seek easy criteria to determine if p is a divisor of the recurrence (1.1).

It is known that if $p \nmid b$ (see [3, pp. 344–345]), then $w(a,b)$ is purely periodic modulo p. For the Lucas sequence $u(a,b)$ we define the function $z(p) = z(a,b;p)$ to be the least positive integer n such that $u_n \equiv 0 \pmod{p}$. Since $u(a,b)$ is purely periodic modulo p when $p \nmid b$ and since $u_0 = 0$, we see that $z(a,b;p)$ always exists when $p \nmid b$. We have the following theorem concerning $z(p)$.

Theorem 1.1. *Let $u(a,b)$ be a Lucas sequence and p be an odd prime such that $p \nmid b$.*

(i) *$u_n \equiv 0 \pmod{p}$ if and only if $z(p) \mid n$.*
(ii) *$z(p) \mid p - (D/p)$, where (D/p) denotes the Legendre symbol and $(D/p) = 0$ when $p \mid D$.*
(iii) *If $(D/p) = 0$, then $z(p) = p$.*
(iv) *If $p \nmid D$, then $z(p) \mid (p - (D/p))/2$ if and only if $(-b/p) = 1$.*

Proof. Parts (i)–(iii) are proved in [6, pp. 422–424] and [1, pp. 314–317]. Part (iv) is proved in [6, p. 441] and [1, pp. 318–320]. □

This paper was supported by the Project RVO 67985840.

By virtue of Theorem 1.1, given any recurrence $w(a,b)$ in $\mathcal{F}(a,b)$, we can define the index $i(p)$ of the prime p to be

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

Note that if $p \mid D$ and $p \nmid b$, then $i(p) = 1$. In the next section, given the recurrence $(w) = w(a,b)$, we will define the norm $N(w)$ of (w) to be

$$w_1^2 - aw_1w_0 - bw_0^2. \tag{1.2}$$

Proposition 1.2 and Theorems 1.3 and 1.4 below provide simple necessary and sufficient conditions to determine when p is a divisor of the recurrence $w(a,b)$ based solely on the initial terms w_0, w_1, and parameters a, b. In particular, Theorems 1.3 and 1.4 will make use of $N(w) = w_1^2 - aw_1w_0 - bw_0^2$.

Proposition 1.2, which is well-known and can be proved by inspection and the use of induction, treats the cases in which $p \mid 2ab \cdot \gcd(w_0, w_1)$.

Proposition 1.2. *Let $w(a,b)$ be a recurrence and p be a prime.*

(i) *If $p \mid \gcd(w_0, w_1)$, then p is a divisor of (w) and $p \mid w_n$ for all $n \geq 0$.*
(ii) *If $p \mid \gcd(a,b)$, then p is a divisor of (w) and $p \mid w_n$ for all $n \geq 2$.*
(iii) *If $p \mid b$ and $p \nmid a$, then p is a divisor of (w) if and only if $p \mid w_0w_1$. If $p \mid w_1$, then $p \mid w_n$ for all $n \geq 1$. If $p \mid w_0$ and $p \nmid w_1$, then $p \nmid w_n$ for $n \geq 1$.*
(iv) *If $p \mid a$ and $p \nmid b$, then p is a divisor of (w) if and only if $p \mid w_0w_1$. If $p \mid w_0$ and $p \nmid w_1$, then $p \mid w_n$ if and only if $n \equiv 0 \pmod 2$. If $p \mid w_1$ and $p \nmid w_0$, then $p \mid w_n$ if and only if $n \equiv 1 \pmod 2$.*
(v) *If $p = 2$, then p is a divisor of (w) if and only if $2 \mid \gcd(a,b)$ or $2 \mid w_0w_1$ or $2 \nmid ab$.*

From here on, we assume that p is an odd prime and $p \nmid b$. When $i(p) = 1$ or 2, we can find easy criteria to determine exactly when p is a divisor of the general recurrence $w(a,b)$ based on the residue class or quadratic character of $N(w)$ modulo p. It was found by Backstrom [1, p. 313] that $i(p) = 1$ or 2 for approximately 68% of the primes $p < 5000$. The next Theorem 1.3 was proved in [5, pp. 729–731] and [4, pp. 176–178]. Theorem 1.4 generalizes Theorem 5.1 of [11], which was proved for the case $a = b = 1$.

Theorem 1.3. *Consider the set $\mathcal{F}(a,b)$. Suppose that $i(p) = 1$.*

(i) *If $(D/p) = -1$, then p is a divisor of all recurrences $w(a,b)$ in $\mathcal{F}(a,b)$.*
(ii) *If $(D/p) = 1$ or 0, then p is a divisor of $w(a,b)$ if and only if $p \mid w_0$ or $p \nmid N(w)$.*

Theorem 1.4. *Consider the set $\mathcal{F}(a,b)$. Suppose that $i(p) = 2$. Then p is a divisor of $w(a,b)$ if and only if $w_0 \equiv w_1 \equiv 0 \pmod p$ or $(N(w)/p) = 1$.*

We will prove Theorem 1.4 in Section 3.

When $w(a,b)$ is a recurrence for which $i(p) > 2$, we are unable to give an easy and general test to determine exactly when p is a divisor of $w(a,b)$ that is based on the residue class or quadratic character of $N(w)$ modulo p. However, when $i(p) > 2$ is even, we have the following necessary condition to determine the divisibility of $w(a,b)$ by p that is based on the value of $(N(w)/p)$ and is easy to apply. The proof of Theorem 1.5 will also be given in Section 3.

Theorem 1.5. *Consider the set $\mathcal{F}(a,b)$. Suppose that $i(p) > 2$ is even. If p is a divisor of $w(a,b)$, then either $w_0 \equiv w_1 \equiv 0 \pmod p$ or $(N(w)/p) = 1$.*

2. Preliminaries and Auxiliary Results

Given the recursion relation (1.1), we have the associated characteristic polynomial

$$f(x) = x^2 - ax - b \tag{2.1}$$

with characteristic roots α and β and discriminant $D = a^2 + 4b = (\alpha - \beta)^2$. If $bD \neq 0$, then we can express w_n for $n \geq 0$ in the form (see [5, p. 723])

$$w_n = \frac{A\alpha^n - B\beta^n}{\alpha - \beta}, \tag{2.2}$$

where $A = w_1 - w_0\beta$ and $B = w_1 - w_0\alpha$. In particular, for the Lucas sequence $u(a, b)$, we have the Binet formula

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}.$$

We define $N(w)$, the norm of the recurrence $(w) = w(a, b)$ by

$$N(w) = AB = w_1^2 - (\alpha + \beta)w_1w_0 + \alpha\beta w_0^2 = w_1^2 - aw_1w_0 - bw_0^2. \tag{2.3}$$

The following lemma regarding $N(w)$ is well-known (see for example [5, p. 723]). We give a short and easy proof of this lemma.

Lemma 2.1. *Consider the set $\mathcal{F}(a, b)$. Suppose that $bD \neq 0$ and that $w'(a, b)$ is a translation of $w(a, b)$ by a fixed integer j, that is, $w'_n = w_{n+j}$ for all n. Then*

$$N(w') = (-b)^j N(w). \tag{2.4}$$

Proof. We note that

$$w'_n = \frac{A'\alpha^n - B'\beta^n}{\alpha - \beta} = w_{n+j} = \frac{A\alpha^{n+j} - B\beta^{n+j}}{\alpha - \beta}.$$

Thus,

$$A' = A\alpha^j \quad \text{and} \quad B' = B\beta^j.$$

Hence,

$$N(w') = A'B' = AB(\alpha\beta)^j = (-b)^j AB = (-b)^j N(w).$$

□

The recurrence $w(a, b)$ is said to be *regular* modulo p if

$$N(w) = w_1^2 - aw_1w_0 - bw_0^2 \not\equiv 0 \pmod{p}.$$

Notice that $u(a, b)$ is always regular modulo p, since

$$N(u) = u_1^2 - au_1u_0 - bu_0^2 = 1^2 - a \cdot 1 \cdot 0 - b \cdot 0^2 = 1. \tag{2.5}$$

We note that the trivial recurrence $w(a, b)$ for which $w_0 \equiv w_1 \equiv 0 \pmod{p}$ is always irregular modulo p. We note also that the recurrence $w(a, b)$ is regular modulo p if and only if it does not satisfy a recurrence relation of order less than two. We have the following theorem regarding recurrences $w(a, b)$ that are irregular modulo p.

Theorem 2.2. *Consider the set $\mathcal{F}(a, b)$ of recurrences $w(a, b)$ with characteristic roots α and β. Suppose that $w(a, b)$ is irregular modulo p. Then both α and β are in the field $\mathbb{Z}_p$ of integers modulo p, and $(D/p) = 1$ or 0. Moreover, the following hold:*

(i) *Either $w_n \equiv \alpha^n w_0 \pmod{p}$ or $w_n \equiv \beta^n w_0 \pmod{p}$ for all $n \geq 0$.*
(ii) *The prime p is a divisor of $w(a, b)$ 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.*

This is proved in [2, pp. 694–695].

We now define an equivalence relation on $\mathcal{F}(a,b)$ modulo p. We say that $w'(a,b)$ is *equivalent* to $w(a,b)$ modulo p if and only if $w'(a,b)$ is a nonzero multiple of a translation of $w(a,b)$ modulo p, that is, $w'_n \equiv Mw_{n+j} \pmod{p}$ for all n, where $M \not\equiv 0 \pmod{p}$ is a fixed residue modulo p and j is a fixed integer. It now follows easily from the definition of a regular recurrence and from Lemma 2.1 that an equivalence class C in $\mathcal{F}(a,b)$ modulo p contains a regular recurrence modulo p if and only if all recurrences in C are regular modulo p. We call an equivalence class C in $\mathcal{F}(a,b)$ modulo p *regular* (*irregular*) modulo p if it contains a regular (irregular) recurrence modulo p.

The following theorem proved in [2, p. 698] gives the number of regular and irregular equivalence classes modulo p.

Theorem 2.3. *Consider the set $\mathcal{F}(a,b)$.*

(i) *There exist exactly $i(p)$ regular equivalence classes modulo p, each containing exactly $(p-1)z(p)$ regular recurrences modulo p.*
(ii) *If $(D/p) = -1$, then there exists no nontrivial irregular equivalence class modulo p.*
(iii) *If $(D/p) = 1$, then there exist exactly two nontrivial irregular classes modulo p, each containing $p-1$ nontrivial irregular recurrences modulo p. One of these equivalence classes contains the recurrence $w(a,b)$ with initial terms $w_0 \equiv 1$, $w_1 \equiv \alpha \pmod{p}$, and the other equivalence class contains the recurrence $w'(a,b)$ with initial terms $w'_0 \equiv 1$, $w'_1 \equiv \beta \pmod{p}$.*
(iv) *If $(D/p) = 0$, then there exists exactly one nontrivial irregular equivalence class modulo p, namely the equivalence class containing the recurrence with initial terms $w_0 \equiv 1$, $w_1 \equiv \alpha \pmod{p}$. This equivalence class contains $p-1$ nontrivial irregular recurrences modulo p.*
(v) *There exists exactly one trivial equivalence class modulo p containing the unique recurrence with initial terms $w_0 \equiv w_1 \equiv 0 \pmod{p}$.*

The next lemma shows that there is only one equivalence class in $\mathcal{F}(a,b)$ consisting of recurrences that are regular modulo p and have p as a divisor.

Lemma 2.4. *Consider the set $\mathcal{F}(a,b)$. Then the recurrence $w(a,b)$ has p as a divisor if and only if it is the trivial recurrence modulo p or it is regular modulo p and is equivalent to $u(a,b)$ modulo p.*

Proof. By Theorem 2.2, an irregular recurrence $w(a,b)$ modulo p has p as a divisor if and only if it is the trivial recurrence modulo p. Suppose that $w(a,b)$ is regular modulo p and has p as a divisor. Then $w_i \equiv 0 \pmod{p}$ for some i. If $w_{i+1} \equiv 0 \pmod{p}$ also, then by the recursion relation (1.1) defining (w) and by the fact that b is invertible modulo p, it follows that $w_n \equiv 0 \pmod{p}$ for all n, and thus (w) is the irregular trivial recurrence modulo p. Hence, $w_{i+1} \not\equiv 0 \pmod{p}$. It therefore follows that

$$w_n \equiv w_{i+1}u_{n-i} \pmod{p} \quad \text{for all } n,$$

and hence $w(a,b)$ is equivalent to $u(a,b)$ modulo p. □

Corollary 2.5 below follows immediately from Theorem 2.3 and Lemma 2.4.

Corollary 2.5. *Consider the set $\mathcal{F}(a,b)$. Then exactly $\frac{1}{i(p)}$ of the recurrences $w(a,b)$ which are regular modulo p have p as a divisor.*

The following theorem due to Catlin [4, p. 176] (see also [5, p. 729]) gives a test for p to be a divisor of the regular recurrence $w(a,b)$ modulo p.

Theorem 2.6. *The prime p is a divisor of the regular recurrence $w(a,b)$ modulo p if and only if $w_0 \equiv 0 \pmod{p}$ or $w_1 w_0^{-1} \equiv u_{r+1} u_r^{-1}$ for some r such that $1 \le r \le z(p) - 1$.*

Unfortunately, the test given in Theorem 2.6 is not quick to apply when p and $z(p)$ are both large. As stated earlier, when $i(p) = 1$ or 2, Theorems 1.3 and 1.4 give fast and easy tests to determine divisibility of $w(a,b)$ by p.

Suppose that p is a prime for which $z(a,b;p)$ 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 $1 \le b' \le (p-1)/2$. If $p \nmid D$, then we claim that both $v(a,b)$ and $t(a,b)$ are regular modulo p. We observe that

$$N(v) = v_1^2 - a v_1 v_0 - b v_0^2 = a^2 - (a)(a)(2) - b(2)^2 = -(a^2 + 4b) = -D \not\equiv 0 \pmod{p}, \quad (2.6)$$

and $v(a,b)$ is regular modulo p.

Next we note that

$$N(t) = t_1^2 - a t_1 t_0 - b t_0^2 = (b')^2 - a(b')(1) - b(1)^2 \equiv b'(2b' - a) \pmod{p}. \quad (2.7)$$

We now notice that

$$[b'(2b' - a)][b'(2b' + a)] = (b')^2(4(b')^2 - a^2) \equiv (-b)(-4b - a^2) \equiv bD \pmod{p}. \quad (2.8)$$

Since $bD \not\equiv 0 \pmod{p}$, we see by (2.7) and (2.8) that $t(a,b)$ is also regular modulo p. It follows from the results in [10, pp. 534–535] that $v(a,b)$ and $t(a,b)$ belong to distinct equivalence classes modulo p when $t(a,b)$ is defined.

Lemma 2.7. *Consider the set $\mathcal{F}(a,b)$. Let p be a prime such that $p \nmid D$. Consider the recurrences $v(a,b)$ and $t(a,b)$ in $\mathcal{F}(a,b)$.*

(i) *If $z(p)$ is odd, then $v(a,b)$ does not have p as a divisor.*
(ii) *If $z(p)$ is even and $(-b/p) = 1$, then $t(a,b)$ is defined and does not have p as a divisor.*

Proof. It was proved in [10, pp. 534–536] that $v(a,b)$ is not equivalent to $u(a,b)$ modulo p when $z(p)$ is odd and $t(a,b)$ is not equivalent to $u(a,b)$ modulo p when $z(p)$ is even and $(-b/p) = 1$. By (2.6), (2.7), and (2.8), both $v(a,b)$ and $t(a,b)$ are regular modulo p. It now follows from Lemma 2.4 that neither $v(a,b)$ nor $t(a,b)$ has p as a divisor. □

Lemma 2.8. *Consider the set $\mathcal{F}(a,b)$.*

(i) *Suppose that $p \mid D$ or $i(p)$ is even. If $w'(a,b)$ is equivalent to $w(a,b)$ modulo p, then $(N(w')/p) = (N(w)/p)$.*
(ii) *If $i(p)$ is odd, $p \nmid D$, and $w(a,b)$ is a regular recurrence modulo p, then there exists a recurrence $w'(a,b)$ such that $w'(a,b)$ is equivalent to $w(a,b)$ modulo p and $(N(w')/p) = -(N(w)/p)$.*

Proof.

(i) First suppose that $p \mid D$. Then $a^2 + 4b \equiv 0 \pmod{p}$, which implies that

$$a^2 \equiv 4(-b) \pmod{p}.$$

Since $(4/p) = 1$ and $p \nmid b$, we have that $(-b/p) = 1$. Now suppose that $i(p)$ is even. Then $p \nmid D$, since $i(p) = 1$ if $p \mid D$. It follows from Theorem 1.1 (i) and (iv) that

$(-b/p) = 1$ in this case also. Suppose that $w'(a,b)$ is equivalent to $w(a,b)$ modulo p. Then there exist a fixed nonzero residue M modulo p and fixed integer j such that

$$w'_n \equiv M w_{n+j} \pmod{p}$$

for all n. Let $w^*(a,b)$ be the recurrence such that $w^*_n = w_{n+j}$ for all n. Then by Lemma 2.1,

$$N(w') \equiv M^2(w_{j+1}^2 - a w_{j+1} w_j - b w_j^2) \equiv M^2 N(w^*) \equiv M^2(-b)^j N(w) \pmod{p}. \tag{2.9}$$

Since $(-b/p) = 1$ and $M \not\equiv 0 \pmod{p}$, it follows from (2.9) that $(N(w')/p) = (N(w)/p)$.

(ii) Now suppose that $2 \nmid i(p)$ and $p \nmid D$. Then $(-b/p) = -1$ by Theorem 1.1 (i) and (iv). Let $w(a,b)$ be a regular recurrence modulo p and define $w'(a,b)$ by $w'_n = w_{n+1}$ for all n. Then $w'(a,b)$ is equivalent to $w(a,b)$ modulo p. By Lemma 2.1, we see that

$$N(w') = -bN(w).$$

Hence, $(N(w')/p) = -(N(w)/p)$.

□

The proof of Lemma 2.8(i) generalizes an argument given in [8, p. 276] for the case in which $b = 1$.

Lemma 2.9. *Let*

$$F(x,y) = Rx^2 + Sxy + Ty^2$$

be a binary quadratic form with discriminant $D = S^2 - 4RT$, where $R, S,$ and T are integers. Assume that $p \nmid D$. Then, given any integer m there exist integers x_0, y_0 such that $F(x_0, y_0) \equiv m \pmod{p}$.

Proof. First suppose that $R \equiv T \equiv 0 \pmod{p}$. Then $S \not\equiv 0 \pmod{p}$, since $D \not\equiv 0 \pmod{p}$. Let $x_0 \equiv S^{-1}m$ and $y_0 \equiv 1 \pmod{p}$. Then

$$F(x_0, y_0) \equiv S x_0 y_0 \equiv m \pmod{p}.$$

We now assume that $R \not\equiv 0 \pmod{p}$ or $T \not\equiv 0 \pmod{p}$. Without loss of generality, we can assume that $R \not\equiv 0 \pmod{p}$. By completing the square, we obtain (see [9, p. 151])

$$4RF(x,y) = X^2 - Dy^2 = G(X,Y), \tag{2.10}$$

where $X = 2Rx + Sy$, $Y = y$. Note that

$$\begin{pmatrix} X \\ Y \end{pmatrix} = \begin{pmatrix} 2R & S \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} =: U \begin{pmatrix} x \\ y \end{pmatrix}. \tag{2.11}$$

Since $\det(U) = 2R$, we see that the upper triangular matrix U is invertible over $\mathbb{Z}_p$. Thus, as (x,y) takes on all values in $\mathbb{Z}_p \times \mathbb{Z}_p$, so does the set of ordered pairs (X,Y). Moreover, since $4R$ is also invertible modulo p, we see from (2.10) that $F(x,y)$ attains all values modulo p if and only if $G(X,Y)$ does also.

Let m_0 be an arbitrary integer. It suffices to show that there exist X_0, Y_0 such that $G(X_0, Y_0) \equiv m_0 \pmod{p}$. We now observe that there are $(p+1)/2$ distinct values of X^2 modulo p (including 0). There are also $(p+1)/2$ distinct values of $m_0 + DY^2 \pmod{p}$. Hence, by the pigeonhole principle, there exist residues X_0, Y_0 modulo p such that

$$X_0^2 \equiv m_0 + DY_0^2 \pmod{p}.$$

Thus,

$$G(X_0, Y_0) = X_0^2 - DY_0^2 \equiv m_0 \pmod{p}.$$

□

We need the following technical lemma.

Lemma 2.10. *Let a^2+4 be a prime, where a is a positive odd integer. Consider the quadratic algebraic number field $\mathbb{Q}(\sqrt{a^2+4})$. Then its fundamental unit is*

$$\varepsilon = \frac{a + \sqrt{a^2+4}}{2}.$$

Suppose that $p \equiv 1 \pmod 8$ and $(a^2+4/p) = 1$. Then $(-1/p) = 1$ and both $\mathrm{i} = \sqrt{-1}$ and $\sqrt{a^2+4}$ can be considered elements of $\mathbb{Z}_p$. Moreover, $(\varepsilon/p) = (-2 - a\mathrm{i}/p)$.

Proof. Since the Pell equation

$$x^2 - (a^2+4)y^2 = -4$$

has the solution $x = a$ and $y = 1$, it is clear that

$$\varepsilon = \frac{a + \sqrt{a^2+4}}{2}.$$

It was proved in [7, pp. 44–45] that

$$(\varepsilon/p) = (a + 2\mathrm{i}/p).$$

We note that $(\mathrm{i}/p) = 1$, since $p \equiv 1 \pmod 8$. Then

$$(\varepsilon/p) = (a + 2\mathrm{i}/p) = (\mathrm{i}/p)(a + 2\mathrm{i}/p) = (-2 + a\mathrm{i}/p).$$

Moreover,

$$(-2 + a\mathrm{i}/p)(-2 - a\mathrm{i}/p) = (a^2+4/p) = 1.$$

Hence,

$$(-2 + a\mathrm{i}/p) = (-2 - a\mathrm{i}/p) = (\varepsilon/p).$$

□

3. Proofs of the Main Theorems

To illustrate the idea of equivalence modulo p, we give a proof of Theorem 1.3.

Proof of Theorem 1.3. First suppose that $w(a,b)$ is irregular modulo p. If (w) is the trivial recurrence modulo p, then clearly p is a divisor of (w). By Theorem 2.2 (ii), an irregular recurrence (w) is the trivial recurrence modulo p if and only if $w_0 \equiv 0 \pmod p$. By Theorem 2.2 (i), if (w) is not the trivial recurrence modulo p, then p is not a divisor of (w).

Now suppose that (w) is regular modulo p. Since $i(p) = 1$, we see by Theorem 2.3 (i) that there is only one regular equivalence class modulo p. Since $u(a,b)$ is regular modulo p by (2.5), it follows that (w) is equivalent to (u) modulo p. Hence, p is a divisor of (w) by Lemma 2.4. If $(D/p) = -1$, then there are no nontrivial irregular recurrences modulo p by Theorem 2.3 (ii). Parts (i) and (ii) of Theorem 1.3 now follow. □

Proof of Theorem 1.4. We first note that $p \nmid D$, since $i(p) = 1$ if $p \mid D$ by Theorem 1.1 (iii). By Lemma 2.4, p is a divisor of $w(a,b)$ if and only if (w) is the trivial recurrence modulo p or $w(a,b)$ is regular modulo p and is in the same equivalence class as $u(a,b)$ modulo p. By

Lemma 2.8 (i) and (2.5), if the regular recurrence $w(a,b)$ is equivalent to $u(a,b)$ modulo p and thus has p as a divisor, then

$$(N(w)/p) = (N(u)/p) = (1/p) = 1.$$

Consider the binary quadratic form

$$F(x,y) = x^2 - axy - by^2.$$

Notice that for $F(x,y)$, the discriminant $D = a^2 + 4b \not\equiv 0 \pmod{p}$. Let d be a quadratic nonresidue modulo p. By Lemma 2.9, there exist integers w_0, w_1 such that if $w(a,b)$ has initial terms w_0, w_1, then

$$F(w_1, w_0) = w_1^2 - aw_1w_0 - bw_0^2 = N(w) \equiv d \pmod{p},$$

and hence,

$$(N(w)/p) = (d/p) = -1.$$

Therefore, $w(a,b)$ is regular modulo p, but is not equivalent to $u(a,b)$ modulo p, and consequently does not have p as a divisor. Since $i(p) = 2$ and thus $\mathcal{F}(a,b)$ has only two equivalence classes of regular recurrences modulo p, it follows that p is a divisor of the regular recurrence (w) if and only if $(N(w)/p) = 1$. □

Proof of Theorem 1.5. Since $i(p) > 2$, it follows from Theorem 1.1 (iii) that $p \nmid D$. We now see by Lemma 2.4 that p is a divisor of $w(a,b)$ if and only if (w) is the trivial recurrence modulo p or (w) is regular modulo p and equivalent to $u(a,b)$ modulo p. It now follows from (2.5) and Lemma 2.8 (i) that if the regular recurrence $w(a,b)$ is equivalent to $u(a,b)$ modulo p, then

$$(N(w)/p) = (N(u)/p) = 1.$$

□

Remark 3.1. We note by the argument given in the proof of Theorem 1.4 that if $i(p) > 2$ is even, then there indeed exists a regular recurrence $w(a,b)$ modulo p for which $(N(w)/p) = -1$. For this recurrence, the test presented in Theorem 1.5 successfully determines that p is not a divisor of $w(a,b)$.

In Example 3.2, Proposition 3.3, and Example 3.4, we will use the explicit recurrences $v(a,b)$ and $t(a,b)$ to show that the necessary condition given in Theorem 1.5 is not sufficient.

Example 3.2. Consider the companion Lucas sequence $v(a,b)$ and suppose that $p \nmid D$, $4 \mid i(p)$, and $z(p)$ is odd. By (2.6) and Lemma 2.7(i), $v(a,b)$ is regular modulo p and p is not a divisor of (v). We will show however that $(N(w)/p) = 1$.

Note that

$$N(v) = v_1^2 - av_1v_0 - bv_0^2 = a^2 - (a)(a)(2) - b(2^2) = -a^2 - 4b = -D.$$

First suppose that $p \equiv 1 \pmod{4}$. Since $4 \mid i(p)$, it follows that $(D/p) = 1$. Hence,

$$(N(v)/p) = (-D/p) = (-1/p)(D/p) = 1 \cdot 1 = 1.$$

Now suppose that $p = 3 \pmod{4}$. Noting that $4 \mid i(p)$, we see that $(D/p) = -1$. Then

$$(N(v)/p) = (-D/p) = (-1/p)(D/p) = (-1)(-1) = 1.$$

For the companion Lucas sequence $v(1,-2)$, we have $D = -7$ and observe that $z(p) = 17$ and $i(p) = 16$ when $p = 271$. Further, $z(p) = 19$ and $i(p) = 24$ when $p = 457$. Then

$$(N(v)/271) = (7/271) = -(271/7) = -(5/7) = 1$$

and

$$(N(v)/457) = (7/457) = (457/7) = (2/7) = 1.$$

Proposition 3.3. *Consider the set of recurrences $\mathcal{F}(a,1)$, where $D = a^2+4$ is a prime. Let p be a prime such that $p \equiv 1 \pmod 4$, $4 \mid i(p)$, and $z(p)$ is even. Then the recurrence $t(a,1)$ is defined. Moreover, $t(a,1)$ is regular modulo p and p is not a divisor of $t(a,1)$. Furthermore, $(D/p) = (N(t)/p) = 1$.*

Proof. Since $p \equiv 1 \pmod 4$, we have $(-1/p) = 1$. It now follows that $t(a,1)$ is defined, since $z(p)$ is even. By (2.7), (2.8), and Lemma 2.7 (ii), $t(a,1)$ is regular modulo p and p is not a divisor of $t(a,1)$.

Since $p \equiv 1 \pmod 4$, $4 \mid i(p)$, and $z(p)$ is even, we see that $(D/p) = 1$ and $p \equiv 1 \pmod 8$. Thus, we can consider $\mathrm{i} = \sqrt{-1}$ and both $\alpha = (a+\sqrt{D})/2$ and $\beta = (a-\sqrt{D})/2$ to be in $\mathbb{Z}_p$. We note that

$$N(t) = t_1^2 - at_1t_0 - t_0^2 = \mathrm{i}^2 - a(\mathrm{i})(1) - 1^2 = -2 - a\mathrm{i}.$$

By Lemma 2.10,

$$(\alpha/p) = \Big(\frac{a+\sqrt{a^2+4}}{2}\Big/p\Big) = (-2 - a\mathrm{i}/p).$$

Thus, we will have $(N(t)/p) = 1$ if we can show that $(\alpha/p) = 1$.

Let $k = z(p)$. Then

$$u_k \equiv 0 \equiv \frac{\alpha^k - \beta^k}{\sqrt{D}} \pmod p.$$

Noting that $p \nmid D$ and $\alpha\beta = -1$, we see that

$$0 \equiv \frac{\left(\frac{\alpha}{\beta}\right)^k - 1}{\sqrt{D}/\beta^k} \equiv (-\alpha^2)^k - 1 \pmod p.$$

As k is even, we find that

$$(-\alpha^2)^k \equiv (-1)^k\alpha^{2k} \equiv \alpha^{2k} \equiv 1 \pmod p. \tag{3.1}$$

Since $4 \mid i(p)$ and $(D/p) = 1$, we have $k \mid (p-1)/4$. Let $km = (p-1)/4$. Then by (3.1),

$$\alpha^{(p-1)/2} = (\alpha^{2k})^m \equiv 1^m \equiv 1 \pmod p.$$

Hence, $(\alpha/p) = 1$ and thus, $(N(t)/p) = 1$. □

Example 3.4. We observe in particular that for $a \equiv 1 \pmod 2$ and $1 \le a < 40$, a^2+4 is prime for $a = 1, 3, 5, 7, 13, 15, 17, 27, 33, 35,$ and 37.

We now give an example in which $a = 3$, $b = 1$, and $D = a^2+4 = 13$. Consider the prime 433. We note that $433 \equiv 1 \pmod 4$ and

$$(13/433) = (433/13) = (4/13) = 1.$$

We further observe that $z(433) = 18$ and $i(433) = 24$. We now consider the recurrence $t(3,1)$ modulo 433. By Lemma 2.7 (ii), 433 is not a divisor of $t(3,1)$. However, by the law of quadratic reciprocity,

$$\Big(\frac{N(t)}{433}\Big) = \Big(\frac{-2-3\mathrm{i}}{433}\Big) = \Big(\frac{-2-3\cdot 179}{433}\Big) = \Big(\frac{-539}{433}\Big)$$

$$= \Big(\frac{-106}{433}\Big) = \Big(\frac{-1}{433}\Big)\Big(\frac{2}{433}\Big)\Big(\frac{53}{433}\Big) = 1\cdot 1\cdot\Big(\frac{433}{53}\Big) = \Big(\frac{9}{53}\Big) = 1.$$

4. Concluding Remarks

In Theorem 2.6, we gave a necessary and sufficient test to determine if p is a divisor of the recurrence $w(a,b)$. However, this was not a quick test if both p and $z(p)$ are large. In the special cases in which $i(p) = 1$ or 2, Theorems 1.3 and 1.4 indeed provided easy criteria to tell whether p is a divisor of $w(a,b)$ or not. When $i(p) > 2$ is even, Theorem 1.5 also gave an easy necessary but not sufficient test to determine if p is a divisor of $w(a,b)$, namely if p is a divisor of $w(a,b)$, then either $w_0 \equiv w_1 \equiv 0 \pmod{p}$ or $(N(w)/p) = 1$.

When $i(p)$ is odd and $i(p) > 1$, we were unable to find even a quick and general necessary test to determine if p is a divisor of $w(a,b)$ based on either the residue class or quadratic character of $N(w)$ modulo p. The reason is that when $i(p) \geq 3$ is odd, there are $i(p) - 1$ regular equivalence classes modulo p in $\mathcal{F}(a,b)$ not having p as a divisor and also that for any regular equivalence class modulo p, there are recurrences $w(a,b)$ and $w'(a,b)$ for which $(N(w)/p) \neq (N(w')/p)$.

5. Acknowledgements

The authors would like to thank Lawrence Washington (Univ. of Maryland) and Paul Young (Univ. of Charleston) for fruitful discussions concerning Lemma 2.9. We also thank the anonymous referee for careful reading of the paper and suggestions which improved the text.

References

[1] R. Backstrom, *On the determination of the zeros of the Fibonacci sequence*, The Fibonacci Quarterly, **4.4** (1966), 313–322.
[2] W. Carlip and L. Somer, *Bounds for frequencies of residues of Lucas sequences modulo p^r*, Number Theory in Progress, Vol. 2 (Zakopane-Koscielisco, 1997), de Gruyter, Berlin, (1999), 691–719.
[3] R. D. Carmichael, *On sequences of integers defined by recurrence relations*, Quart. J. Pure Appl. Math., **48** (1920), 343-372.
[4] P. Catlin, *On the divisors of second order recurrences*, The Fibonacci Quarterly, **12.2** (1974), 175–178.
[5] R. R. Laxton, *On groups of linear recurrences I*, Duke Math. J., **36** (1969), 721–736.
[6] D. H. Lehmer, *An extended theory of Lucas' functions*, Ann. of Math., **31** (1930), 419–448.
[7] E. Lehmer, *On the quadratic character of some quadratic surds*, J. Reine Angew. Math., **250** (1971), 42–48.
[8] H.-C. Li, *Complete and reduced residue systems of second-order recurrences modulo p*, The Fibonacci Quarterly, **38.3** (2000), 272–281.
[9] I. Niven, H. S. Zuckerman, and H. L. Montgomery, *An Introduction to the Theory of Numbers*, Fifth ed., John Wiley & Sons, Inc., New York, 1991.
[10] L. Somer, *Upper bounds for frequencies of elements in second-order recurrences over a finite field*, Application of Fibonacci Numbers, Vol. 5 (St. Andrews, 1992), Kluwer Acad. Publ., Dordrecht, 1993, 527–546.
[11] S. Vandervelde, *On the divisibility of Fibonacci sequences by primes of index two*, The Fibonacci Quarterly, **50.3** (2012), 207–216.

MSC2010: 11B39, 11E16, 11R04

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