Internat. J. Math. & Math. Sci.
Vol. 23, No. 4 (2000) 225–241
S0161171200003240
© Hindawi Publishing Corp.

STABILITY OF SECOND-ORDER RECURRENCES MODULO p^r

LAWRENCE SOMER and WALTER CARLIP

(Received 13 April 1999)

ABSTRACT. The concept of sequence *stability* generalizes the idea of uniform distribution. A sequence is *p-stable* if the set of residue frequencies of the sequence reduced modulo p^r is eventually constant as a function of r. The authors identify and characterize the stability of second-order recurrences modulo odd primes.

Keywords and phrases. Lucas, Fibonacci, stability, uniform distribution, recurrence.

2000 Mathematics Subject Classification. Primary 11B39, 11B50; Secondary 11Y55, 11B37.

1. Introduction. Let $w(a,b) = (w)$ be a second-order linear recurrence satisfying the 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 rational integers. If m is a positive integer, then the sequence $w(a,b)$ is eventually periodic when reduced modulo m. For any residue d, we let $\nu_w(d,m)$ denote the number of times that the residue d appears in one shortest period (cycle) of the recurrence $w(a,b)$ modulo m. The function $\nu_w(d,m)$ is the *frequency distribution* function of the sequence $w(a,b)$ modulo m. Let $\Omega_w(m)$ be the image of the frequency distribution function, i.e.,

$$\Omega_w(m) = \{\nu_w(d,m) \mid d \in \mathbf{Z}\}. \tag{1.2}$$

We are concerned here with the possible values taken on by the frequency distribution function $\nu_w(d,m)$ when $m = p^r$ is a power of an odd prime.

In 1992, while investigating the Fibonacci sequence $u(1,-1)$ modulo powers of two, Eliot Jacobson [12] discovered that the frequency sets $\Omega_{u(1,-1)}(2^r)$ are eventually constant as a function of r. This observation led to the definition of sequence stability.

DEFINITION 1.1. A sequence (w) is *stable modulo p*, or simply *p-stable*, if there is a positive integer N such that $\Omega_w(p^r) = \Omega_w(p^N)$ for all $r \geq N$.

Our interest in sequence stability developed naturally from earlier study of frequency distributions of second-order recurrence sequences. In the 1970s, an extensive investigation of second-order recurrence sequences led to the complete characterization, by Bumby [1] and Webb and Long [22], of second-order recurrence sequences for which $|\Omega(m)| = 1$. The frequency distribution function of these sequences is constant and they are called *uniformly distributed.* Investigation of distributions for which $|\Omega(m)|$ is small soon followed.

In 1988 and 1989, Jacobson [10, 11] recognized that, although the Fibonacci sequence $u(1,-1)$ is not always uniformly distributed modulo p, the set $\Omega_{u(1,-1)}(p)$ is often small. He studied moduli m for which $u(1,-1)$ modulo m is *almost uniform*, i.e., $|\Omega(m)| = 2$. Conjectures proposed at the First Meeting of the Canadian Number Theory Association in Banff (1988) spurred Andrzej Schinzel [14] to classify the sets $\Omega_w(p)$ for a large class of second-order recurrences (w) and odd primes p for which $|\Omega(m)| \le 4$.

With the introduction of the concept of stability, the study of the frequency distributions of second-order recurrence sequences modulo prime powers has become much more tractable. Once a sequence is identified as p-stable, the set of allowable frequencies can, in theory, be computed with a finite computation; the frequency distributions modulo arbitrary powers of p can then be determined. In practice, as Carlip and Jacobson observed in [4], these computations may be arbitrarily long; the sets $\Omega(p^r)$ may be arbitrarily large and the constant N (the *index of stability*) required in the definition of stability also arbitrarily large.

Stability of second-order recurrences modulo two has been extensively studied by Carlip and Jacobson in [2, 3, 4, 5], while stability modulo odd primes has been examined by Carlip, Jacobson, and Somer in [6] and Carroll, Jacobson, and Somer in [9]. In recent work Carlip and Somer [7, 21] have studied the frequency distributions of second-order recurrences modulo powers of odd primes. The primary purpose of this paper is to show how the results in [7] and [21] can be applied to characterize the stability of sequences. In particular, we exhibit several classes of second-order recurrences that fail to be p-stable and provide explicit new criteria for other second-order recurrence sequences to be p-stable. In the process we extend earlier results and provide a catalogue of what is currently known about the p-stability of second-order recurrences for odd p.

2. Preliminaries and notation. We make free use of the terminology and notation of [7] and [21]. For the convenience of the reader, we provide some of the basic definitions and specialized results here.

2.1. The family $\mathscr{F}(a,b)$. Throughout this paper, we fix a prime p, usually odd, and study the p-stability of second-order recurrences from a family $\mathscr{F}(a,b)$ of second-order recurrences $w(a,b) = (w)$ that satisfy the recurrence relation

$$w_{n+2} = aw_{n+1} - bw_n, \tag{2.1}$$

for various initial terms w_0 and w_1.

If $p^m \parallel (w_0, w_1)$ for some $m \ge 1$, then $p^m \parallel (w_n, w_{n+1})$ for all $n \ge 0$. If (w'_n) is the recurrence defined by $w'_n = w_n/p^m$, then $p \nmid (w'_0, w'_1)$ and $\nu_{w'}(d, p^r) = \nu_w(p^m d, p^{r+m})$ for all $r \ge 1$. Thus, we can determine the frequency distribution function of (w) from that of (w'), and accordingly we restrict our attention to those recurrences for which $p \nmid (w_0, w_1)$.

Definition 2.1. The family $\mathscr{F}(a,b)$ consists of all second-order recurrence sequences (w) that satisfy (2.1) and $p \nmid (w_0, w_1)$.

In general, elements w_n for which $p \mid w_n$ behave quite differently from elements for which $p \nmid w_n$. We refer to elements w_n for which $p \mid w_n$ as *p-singular* elements of (w) and elements for which $p \nmid w_n$ as *p-regular* elements of (w). Analogously, we call an integer d *p-singular* if $p \mid d$ and *p-regular* if $p \nmid d$.

In addition to the constants a and b, there are other parameters associated with the family $\mathcal{F}(a,b)$ and referred to as *global parameters* of the family. These include constants associated with the *characteristic polynomial*

$$f(x) = x^2 - ax + b, \tag{2.2}$$

such as the roots α and β and the discriminant $D = D(a,b) = a^2 - 4b$. A number of our results require constraints on D, e.g., requiring that D be p-regular or a quadratic residue modulo p.

2.2. Stability and the stability index. As mentioned in the introduction, a sequence (w) is p-stable if there is a positive integer N such that $\Omega_w(p^r) = \Omega_w(p^N)$ for all $r \geq N$. In [4], Carlip and Jacobson observed that when $p = 2$, the integer N, the *generation* at which stability *begins*, may be arbitrarily large. We formalize the study of the parameter N with the following definition.

Definition 2.2. Suppose that (w) is p-stable. The smallest positive integer N such that $\Omega_w(p^r) = \Omega(p^N)$ for all $r \geq N$ is called the *index of p-stability*, or simply the *index of stability* when p is understood. The stability index of (w) is denoted by $\iota_w(p)$, or simply $\iota(p)$ when (w) is understood.

2.3. Blocks of sequences. The family $\mathcal{F}(a,b)$ is endowed with a natural equivalence relation that preserves many important properties.

Definition 2.3. The recurrence $w'(a,b)$ is a *multiple of a translation* (**mot**) of $w(a,b)$ modulo p^r if there exist integers m and c such that $p \nmid c$ and for all n

$$w'_n \equiv c w_{n+m} \pmod{p^r}. \tag{2.3}$$

The equivalence classes of the relation **mot** are called the *p^r-blocks*. If d is any integer, then $\nu_w(d,p^r) = \nu_{w'}(cd,p^r)$, and therefore for every n

$$\nu_w(w_{n+m},p^r) = \nu_{w'}(w'_n,p^r). \tag{2.4}$$

Thus, two sequences in the same block have the same *pattern* of frequencies of residues in corresponding cycles.

2.4. Periods, restricted periods, and multipliers. If the defining parameter b is p- regular, then each sequence $w(a,b)$ is purely periodic when reduced modulo p^r. We let $\lambda_w(p^r)$ denote the *period* of $w(a,b)$ modulo p^r, i.e., the least positive integer λ such that for all n

$$w_{n+\lambda} \equiv w_n \pmod{p^r}. \tag{2.5}$$

Similarly, $h_w(p^r)$ denotes the *restricted period* of $w(a,b)$ modulo p^r, i.e., the least positive integer h such that for some integer M and for all n

$$w_{n+h} \equiv M w_n \pmod{p^r}. \tag{2.6}$$

The integer $M = M_w(p^r)$, defined up to congruence modulo p^r, is called the *multiplier* of $w(a,b)$ modulo p^r. It is well known that $h_w(p^r) \mid \lambda_w(p^r)$ and that $E_w(p^r) = \lambda_w(p^r)/h_w(p^r)$ is the multiplicative order in $(\mathbf{Z}/p^r\mathbf{Z})^*$ of the multiplier $M_w(p^r)$.

2.5. Regular recurrences. In this paper, we are primarily concerned with p-regular sequences. A recurrence sequence $w(a,b)$ is *regular* modulo p, or simply p-regular, if

$$\begin{vmatrix} w_0 & w_1 \\ w_1 & w_2 \end{vmatrix} = w_0w_2 - w_1^2 \not\equiv 0 \pmod{p}. \tag{2.7}$$

It is evident that p-regularity is preserved by the equivalence relation **mot**. Thus, if a block contains a regular recurrence, then every recurrence in that block is regular and we refer to that block as a *regular block*.

If $p \mid (w_0, w_1)$, then certainly (w) is not p-regular. The second-order recurrence sequences that fail to be p-regular may be characterized as those sequences that, modulo p, satisfy a recurrence relation of order one.

A straightforward argument shows that all p-regular recurrences in $\mathcal{F}(a,b)$ have the same period, restricted period, and multiplier modulo p^r. Consequently, these may be considered to be global parameters of the family $\mathcal{F}(a,b)$, and we use the notation $\lambda(p^r)$, $h(p^r)$, and $M(p^r)$ to represent the period, restricted period, and multiplier modulo p^r of all p-regular recurrences in $\mathcal{F}(a,b)$. We make frequent use of the quotient $\lambda(p)/h(p)$, a global parameter that we now recognize as the multiplicative order of the multiplier $M(p)$ corresponding to any p-regular sequence in $\mathcal{F}(a,b)$. For notational convenience we define $s = E(p) = \lambda(p)/h(p)$.

We require Lemma 2.4, which characterizes the restricted period in terms of the characteristic roots.

Lemma 2.4. *Suppose that $p \nmid D(a,b)$ and that α and β are the roots of the characteristic polynomial $f(x) = x^2 - ax + b$. Let P be a prime ideal lying over p in $\mathbf{Q}(\alpha)$. Then $h(p^r)$ is the least integer n such that $\alpha^n \equiv \beta^n \pmod{P^r}$.*

Proof. This follows from the standard Binet formula for the regular sequence $u(a,b)$ (defined in Definition 2.5). See, e.g., [6, Lem. 2.1]. □

2.6. Some special recurrences. Three special sequences in the family $\mathcal{F}(a,b)$ play a prominent role in our study. These sequences, (u), (v), and (t), are characterized by their initial terms.

Definition 2.5. (a) The Lucas sequence of the first kind (LSFK), $u(a,b)$, is the sequence in $\mathcal{F}(a,b)$ with initial terms $u_0 = 0$ and $u_1 = 1$.

(b) The Lucas sequence of the second kind (LSSK), $v(a,b)$, is the sequence in $\mathcal{F}(a,b)$ with initial terms $v_0 = 2$ and $v_1 = a$.

(c) The recurrence $t(a,b)$, defined when p is odd, $\left(\frac{b}{p}\right) = 1$, and $u(a,b)$ has even restricted period modulo p, is the recurrence in $\mathcal{F}(a,b)$ with initial terms $t_0 = 1$ and $t_1 = \theta$, where $\theta^2 \equiv b \pmod{p}$ and $0 \le \theta \le (p-1)/2$.

If in place of θ, in the definition of $t(a,b)$, we use the square root θ' of b modulo p satisfying $(p-1)/2 \le \theta' \le p-1$, then, by [20, pp. 534–535], the resulting sequence is a **mot** of $t(a,b)$ modulo p. Moreover, the same paper shows that when $t(a,b)$ is defined, it is never a **mot** of $u(a,b)$ or of $v(a,b)$ modulo p.

We make frequent use of the fact that the recurrence $u(a,b)$ is always p-regular. It follows that $\lambda(p^r) = \lambda_u(p^r)$, $h(p^r) = h_u(p^r)$, and $M(p^r) \equiv M_u(p^r) \pmod{p^r}$. Moreover, $M(p^r) \equiv u_{h+1} \pmod{p^r}$, and $h(p^r)$ is the smallest index h such that $u_h \equiv 0 \pmod{p^r}$. Further, we note that the recurrence $v(a,b)$ is p-regular if and only if $p \nmid D(a,b)$ and that $t(a,b)$ is p-regular whenever $t(a,b)$ is defined.

We require Lemma 2.6, which relates the p-blocks containing the sequences $u(a,b)$ and $v(a,b)$.

Lemma 2.6. *The sequences $u(a,b)$ and $v(a,b)$ lie in the same p-block if and only if $h(p)$ is even.*

Proof. Clearly, $v(a,b)$ is a **mot** of $u(a,b)$ modulo p if and only if $p \mid v_m$ for some positive integer m. The lemma now follows from [8, pp. 42, 47]. □

2.7. Nondegenerate recurrences. Given a prime p, we define the global parameter e to be the largest integer, if it exists, such that $h(p^e) = h(p)$. Since $u(a,b)$ is p-regular, it follows that e is uniquely determined by $p^e \parallel u_{h(p)}$. If e does not exist, then $u_{h(p)} = 0$, and the p-regular sequences in $\mathcal{F}$ are called *degenerate*.

Similarly, f is the largest integer such that $\lambda(p^f) = \lambda(p)$. It is easy to see that if e exists, then f also exists and $f \le e$.

The parameters e and f play a critical role in the structure theory of second-order recurrence sequences. One of the outstanding open questions in the theory is whether for the family $\mathcal{F}(1,-1)$, the family that contains the Fibonacci sequence $u(1,-1)$, there exists a prime p for which $e > 1$.

In this paper, the relationship between e and f determines the subsequent analysis. If $p \nmid D$ and $\operatorname{ord}_{p^{2e}}(b) \mid p-1$, then Theorems 2.13 and 2.10 imply that $e = f$. In particular, this is true when $b = \pm 1$. On the other hand, if $e \ge 2$, then it may occur that $f < e$ or $f = e$.

2.8. Distribution theorems. Our discussion of sequence stability makes use of specialized results and notation concerning the frequency distributions of residues of second-order recurrences that appear in [7] and [21]. We list several of these key theorems here.

The principle methodology of [7] and [21] requires a subtle analysis of the ratios of certain terms of a recurrence $w(a,b)$ modulo p^r. Such ratios are well defined when the denominator is p-regular and may be viewed as embedded in the localization $\mathbf{Z}_p$ of the integers at the ideal (p). To facilitate analysis of these ratios, we make the following definition.

Definition 2.7. If (w) is a recurrence and m and n are nonnegative integers such that $p \nmid w_n$, then we define $\rho_w(n,m)$, or simply $\rho(n,m)$, to be the element $w_{n+m}/w_n \in \mathbf{Z}_p$.

We also require several special constants. We define $r^* = \max(\lceil r/2 \rceil, e)$ for use in Theorem 2.12, and, in order to handle small values of r, we define $e^* = \min(r,e)$ and $f^* = \min(r,f)$. Also, we recall that $s = E_w(p) = \lambda_w(p)/h_w(p)$ is the multiplicative order in $\mathbf{Z}/(p)$ of the multiplier $M_w(p)$.

Theorem 2.8 [7, Thm. 6.2]. *Suppose that $w(a,b) \in \mathcal{F}(a,b)$ is p-regular, $f < e$, and $p \nmid d$. Then, for all $r > f$,*

$$\nu(d,p^r) = \nu(d,p^f) \le \nu(d,p). \tag{2.8}$$

Hypothesis 2.9 [7, Hypothesis 6.3]. *There exist a p-regular recurrence $w(a,b) \in \mathcal{F}(a,b)$ and an integer n such that $\operatorname{ord}_{p^{2e}}(\rho_w(n,h(p^e))) \mid p-1$.*

Theorem 2.10 [7, Thm. 6.4]. *If Hypothesis 2.9 holds, then $e = f$ and*

$$\operatorname{ord}_{p^{2e}}(\rho_w(n,h(p^e))) = s. \tag{2.9}$$

Conversely, if $e = f$ and $(\frac{D}{p}) = -1$, then Hypothesis 2.9 holds.

Theorem 2.11 [7, Thm. 6.5]. *Let $w'(a,b) \in \mathcal{F}(a,b)$ be a p-regular recurrence satisfying the conditions of Hypothesis 2.9 and assume that $r > f$. Let $w(a,b) \in \mathcal{F}(a,b)$ and assume that $w(a,b)$ is not a* **mot** *of $w'(a,b)$ modulo p. Then, for all p-regular residues d modulo p^r,*

$$\nu(d,p^r) = \nu(d,p^f) \le \nu(d,p). \tag{2.10}$$

Theorem 2.12 [7, Thm. 6.7]. *Let $w'(a,b) \in \mathcal{F}(a,b)$ be a p-regular recurrence satisfying the conditions of Hypothesis 2.9 and assume that $r > f$. Let $w(a,b) \in \mathcal{F}(a,b)$ and assume that $w(a,b)$ is a* **mot** *of $w'(a,b)$ modulo p. Choose m maximal such that $1 \le m \le e$ and $w(a,b)$ is a* **mot** *of $w'(a,b)$ modulo p^m.*

(a) *If $r \le e+m$ or if $e = m$, then there exist at least s distinct p-regular residues d modulo p^r for which*

$$\nu_w(d,p^r) \ge p^{r-r^*}. \tag{2.11}$$

(b) *If $1 \le m < e$ and $r > e+m$, then there exist at least $p^{r-r^*-m}s$ distinct p-regular residues d modulo p^r for which*

$$\nu_w(d,p^r) \ge p^m. \tag{2.12}$$

Theorem 2.13 [7, Thm. 6.8]. *Suppose that $p \nmid D(a,b)$ and $\operatorname{ord}_{p^{2e}}(b) \mid p-1$. Then $v(a,b)$ satisfies the conditions of Hypothesis 2.9 for $n = 0$. In particular, Hypothesis 2.9 is true when $n = 0$ and $b = \pm 1$.*

Theorem 2.14 [7, Thm. 6.9]. *Suppose that $w(a,b) \in \mathcal{F}(a,b)$ is a* **mot** *of $u(a,b)$ modulo p^{e^*}. Suppose that $p \mid d$. Then*

$$\nu(d,p^r) = \begin{cases} 0 & \text{if } p^{e^*} \nmid d, \\ p^{e^*-f^*}s & \text{if } p^{e^*} \mid d. \end{cases} \tag{2.13}$$

The statement and proof of Theorem 3.3 use an integer γ whose definition first appeared in [7]. The parameter γ plays a prominent role in the statement and proof of Theorem 2.15.

Theorem 2.15 [21, Thm. 6.1]. *Suppose that $e > 1$ and that $w(a,b) \in \mathcal{F}(a,b)$ is a* **mot** *of $u(a,b)$ modulo p, but not a* **mot** *of $u(a,b)$ modulo p^{e^*}. Choose m maximal* *such that $w(a,b)$ is a* **mot** *of $u(a,b)$ modulo p^m and n minimal such that $p \mid w_n$.*

If $p \mid d$ and $\nu(d,p^r) > 0$, then $p^m \parallel d$. Furthermore,

$$\nu(d,p^r) = \begin{cases} p^{r-f^*} & \text{if } m < r \le \min(m+f,e), \\ p^m & \text{if } e-m > f \text{ and } \min(m+f,e) < r, \\ p^{e-f} & \text{if } e-m < f \text{ and } \min(m+f,e) < r. \end{cases} \tag{2.14}$$

If $e-m = f$, then

$$\operatorname{ord}_{p^{2e-2m}}\left(\frac{w_{n+h(p^e)}/p^m}{w_n/p^m}\right) = p^{\gamma} s \tag{2.15}$$

for some integer γ satisfying $0 \le \gamma \le f$, and all possibilities for γ occur. If $\gamma \ge 1$ and $r > e$, then

$$\nu(d,p^r) = p^{\min(r-f,e-\gamma)}, \tag{2.16}$$

and, if $\gamma = 0$ and $r > 2e-m$, then there exists a residue d such that $p^m \| d$ and

$$\nu(d,p^r) \ge p^{r-f-\lceil (r-2e+m)/2\rceil} = p^{r-f-\lceil (r-e-f)/2\rceil}. \tag{2.17}$$

3. Principal results. Throughout this section, we assume that $w(a,b) \in \mathcal{F}(a,b)$ is a nondegenerate, regular second-order recurrence. We fix a prime p, assumed to be odd unless otherwise noted.

3.1. Uniform distribution. We begin with the classical result on uniform distribution of second-order recurrences of Bumby [1] and Webb and Long [22]. The sequences described in this theorem are *uniformly distributed* modulo all powers of the prime p. Since the frequency s is independent of the power of p, these sequences are p-stable.

Theorem 3.1 (Bumby [1], Webb and Long [22]). *Let $w(a,b)$ be a second-order recurrence and p a prime, not necessarily odd. Assume that the following conditions hold:*

(a) $p \mid D$;
(b) $p \nmid ab$ *if* $p \ge 3$;
(c) *if* $p = 2$, *then* $a \equiv 0 \pmod 2$, $b \equiv 1 \pmod 2$, *and* $w_0 + w_1 \equiv 1 \pmod 2$;
(d) *if* $p \ge 3$, *then* $p \nmid 2w_1 - aw_0$;
(e) *if* $p = 2$ *and* $r \ge 2$, *then* $a \equiv 2 \pmod 4$, $b \equiv 1 \pmod 4$, *and* $w_0 + w_1 \equiv 1 \pmod 2$;
(f) *if* $p = 3$ *and* $r \ge 2$, *then* $a^2 \not\equiv b \pmod 9$.

Then $w(a,b)$ is p-stable, $\iota(p) = 1$, and $\Omega(p^r) = \{s\}$ for all $r \ge 1$.

Proof. All parts of this theorem are proved in [1] and [22]. □

3.2. The condition $e > f$. To a great degree, the p-stability of regular sequences in the family $\mathcal{F}(a,b)$ can be characterized by the relationship between the global parameters e and f. We recall that, in any case, $e \ge f$. In this section, we consider those two-term recurrence sequences for which $e > f$. We characterize the p-stability of most of the sequences satisfying this condition: The only sequences omitted lie in the same p^e-block as $u(a,b)$.

In the first theorem, we show that such recurrences are p-stable when they contain no p-singular terms.

Theorem 3.2. *Suppose that $e > f$. If $w(a,b)$ is* not *a* **mot** *of $u(a,b)$ modulo p, then $w(a,b)$ has no p-singular terms and is p-stable with $1 \le \iota(p) \le f$.*

Proof. Since $\mathbf{Z}/(p)$ is a field, it is clear that only one p-block contains sequences with p-singular terms. Since $u(a,b)$ certainly has p-singular terms, it follows that $w(a,b)$ has no p-singular terms.

On the other hand, by Theorem 2.8, if d is p-regular and $r \ge f$, then

$$\nu(d,p^r) = \nu(d,p^f) \le \nu(d,p). \tag{3.1}$$

Consequently, if $r \ge f$, then $\Omega_w(p^r) = \Omega_w(p^f)$, and hence $w(a,b)$ is p-stable with $\iota(p) \le f$. □

Next, we turn to recurrences that contain p-singular terms. As observed in the previous proof, these sequences lie in the same p-block as $u(a,b)$. If $w(a,b)$ is in the same p-block as $u(a,b)$, but not the same p^e-block, then there is a maximal positive integer m such that $1 \le m < e$, and $w(a,b)$ lies in the same block as $u(a,b)$ modulo p^m. In Theorem 3.3, we characterize the stability of these sequences in terms of the relation of m to $e - f$. Note, in particular, that in (d) we exhibit a class of sequences that fail to be p-stable.

Theorem 3.3. *Suppose that $e > f$. Assume that $w(a,b)$ is a* **mot** *of $u(a,b)$ modulo p but not modulo p^e, and choose m maximal such that $w(a,b)$ is a* **mot** *of $u(a,b)$ modulo p^m. If $m = e - f$, then define γ as in Theorem 2.15. Then we have the following stability criteria for $w(a,b) \in \mathcal{F}(a,b)$.*

(a) *If $m < e - f$, then $w(a,b)$ is p-stable and $\iota(p) \le m + f$.*

(b) *If $m > e - f$, then $w(a,b)$ is p-stable and $\iota(p) \le e$.*

(c) *If $m = e - f$ and $\gamma \ge 1$, then $w(a,b)$ is p-stable and $\iota(p) \le e + f - \gamma$.*

(d) *If $m = e - f$ and $\gamma = 0$, then $w(a,b)$ is not p-stable.*

Note. The definition and existence of the parameter γ that appears in (c) and (d) is a consequence of Theorem 2.15. The reader may consult [7] and [21] for additional details.

Proof. First, suppose that $p \nmid d$. Then, by Theorem 2.8,

$$\nu(d,p^r) = \nu(d,p^f) \le \nu(d,p) \tag{3.2}$$

when $r \ge f$. In particular, (3.2) holds when $r \ge m + f$, when $r \ge e$, and, since $\gamma \le f$, also when $r \ge e + f - \gamma$.

Next, suppose that $p \mid d$ and $\nu(d,p^r) > 0$. Since $e > f \ge 1$, we can easily apply Theorem 2.15 to prove (a), (b), and (c).

(a) If $m < e - f$, then Theorem 2.15 implies that

$$\nu(d,p^r) = p^m \tag{3.3}$$

when $r \ge m + f$. Clearly, (3.2) and (3.3) yield (a).

(b) If $m > e-f$, then Theorem 2.15 implies that

$$\nu(d,p^r) = p^{e-f} \tag{3.4}$$

when $r \geq e$. Now, (3.2) and (3.4) yield (b).

(c) If $m = e-f$ and $\gamma \geq 1$, then Theorem 2.15 implies that

$$\nu(d,p^r) = p^{e-\gamma} \tag{3.5}$$

when $r \geq e+f-\gamma$. In this case, (3.2) and (3.5) yield (c).

(d) Finally, assume that $m = e-f$ and $\gamma = 0$. By Theorem 2.15, if $r > 2e-m$, then there exists a residue d such that $p^m \mid d$ for which

$$\nu(d,p^r) \geq p^{r-f-\lceil (r-2e+m)/2\rceil}. \tag{3.6}$$

Clearly (3.6) implies that $\max(\Omega_w(p^r))$ is unbounded as a function of r, and hence $w(a,b)$ is not p-stable. □

3.3. The condition $e = f$. In the remainder of this paper, we consider two-term recurrence sequences for which $e = f$. These sequences have a more intricate structure and are less easy to handle than those for which $e > f$.

The two results in this section classify the stability of some of these sequences under the additional hypothesis that the discriminant D is not a quadratic residue modulo p. In particular, we identify one p^e-block whose sequences all fail to be p-stable and we show that those sequences that fail to be p-stable lie in a unique p-block.

Theorem 3.4. *Suppose that* $(\frac{D}{p}) = -1$ *and* $e = f$. *Then there exists a* p*-regular recurrence* $w'(a,b)$ *that is* not p*-stable. Furthermore, we have the following stability criteria for* $w(a,b) \in \mathcal{F}(a,b)$.

(a) *If* $w(a,b)$ *is a* **mot** *of* $w'(a,b)$ *modulo* p^e, *then* $w(a,b)$ *is* not p*-stable.*

(b) *If* $w(a,b)$ *is* not *a* **mot** *of* $w'(a,b)$ *modulo* p *and also* not *a* **mot** *of* $u(a,b)$ *modulo* p, *then* $w(a,b)$ *is* p*-stable with* $1 \leq \iota(p) \leq e$.

(c) *Suppose that* $w(a,b)$ *is* not *a* **mot** *of* $w'(a,b)$ *modulo* p, *but that* $w(a,b)$ *is a* **mot** *of* $u(a,b)$ *modulo* p. *Choose* m *maximal such that* $m \leq e$ *and* $w(a,b)$ *is a* **mot** *of* $u(a,b)$ *modulo* p^m. *Then* $w(a,b)$ *is* p*-stable with* $1 \leq \iota(p) \leq e$.

Proof. Since $(\frac{D}{p}) = -1$, Theorem 2.10 implies that there is a recurrence $w'(a,b)$ that satisfies Hypothesis 2.9. Suppose that $r \geq 2e$. By the definition of r^* given in Section 2.8, $r^* = \lceil r/2\rceil$, and $r - r^* = \lfloor r/2\rfloor \geq (r-1)/2$. Since $r > f$, Theorem 2.12(a) (with e in place of m) implies that there are at least s distinct p-regular residues d for which $\nu_w(d,p^r) \geq p^{r-r^*} \geq p^{(r-1)/2}$. In particular, $\max(\Omega_w(p^r))$ is unbounded as a function of r, and it follows that $w'(a,b)$ is not p-stable.

(a) Assume that $w(a,b)$ is in the same p^e-block as $w'(a,b)$. Then we can apply Theorem 2.12(a) (with e in place of m) in the same fashion as for $w'(a,b)$ itself, and it follows that $w(a,b)$ is not p-stable.

(b) Assume that $w(a,b)$ lies in a p-block different from those that contain $w'(a,b)$ and $u(a,b)$. As in the proof of Theorem 3.2, [7, Cor. 2.17] implies that $w(a,b)$ has no p-singular terms. But then, by Theorem 2.11, for all residues d,

$$\nu(d,p^r) = \nu(d,p^f) \leq \nu(d,p) \tag{3.7}$$

when $r \geq f = e$. It follows that $w(a,b)$ is p-stable with $1 \leq \iota(p) \leq e$.

(c) Since $w(a,b)$ lies in a different p-block than $w'(a,b)$, Theorem 2.11 implies that for all p-regular residues d,

$$\nu(d,p^r) = \nu(d,p^f) \leq \nu(d,p) \tag{3.8}$$

when $r \geq f = e$.

To handle the p-singular residues, we consider separately the cases that $m < e$ and $m = e$.

First, suppose that $m < e$. Clearly $m \geq 1$, so in this case we know that $e > 1$. Therefore, we can apply Theorem 2.15. Since $e = f$, it follows that $m > e - f$. As in the proof of Theorem 3.3(b), if d is p-singular, then

$$\nu(d,p^r) = p^{e-f} = 1 \tag{3.9}$$

when $r \geq e$. Thus, in this case, (3.8) and (3.9) imply that $w(a,b)$ is p-stable with $1 \leq \iota(p) \leq e$.

Now, suppose that $m = e$. Then, $w(a,b)$ is a **mot** of $u(a,b)$ modulo p^e and we apply Theorem 2.14. Suppose that $r \geq e$. Then, by the definitions of e^* and f^* given in Section 2.8, $e^* = e = f^*$, and hence, if d is p-singular, then

$$\nu(d,p^r) = \begin{cases} 0 & \text{if } p^e \nmid d, \\ s & \text{if } p^e \mid d. \end{cases} \tag{3.10}$$

In particular, $\nu(d,p^r)$ is independent of r. Now (3.8) and (3.10) imply that $w(a,b)$ is p-stable with $1 \leq \iota(p) \leq e$. □

In Theorem 3.5, we identify families $\mathcal{F}(a,b)$ with the property that every p-regular sequence in $\mathcal{F}(a,b)$ fails to be p-stable.

Theorem 3.5. *Suppose that $(\frac{D}{p}) = -1$, $e = 1$, and $h(p) = p+1$. Then $(\frac{b}{p}) = -1$, and every p-regular recurrence $w(a,b) \in \mathcal{F}(a,b)$ is* not *p-stable.*

Furthermore, given any integer b' such that $(\frac{b'}{p}) = -1$, there exist integers a and b with $b \equiv b' \pmod p$ such that $(\frac{D}{p}) = -1$, $h(p) = p+1$, and $e = 1$.

Proof. Since $(\frac{D}{p}) = -1$ and $h(p) = p+1$, [7, Thm. 2.14], which provides an explicit count of regular p-blocks, implies that there is only one regular p-block. Since $1 = e \geq f$, it follows that $e = f$. Consequently, Theorem 3.4 implies that this unique p-regular p-block contains a sequence that is not p-stable. Now, Theorem 3.4(a) implies that every p-regular sequence in $\mathcal{F}(a,b)$ fails to be p-stable. Finally, D. H. Lehmer [13, p. 441] has shown that if $(\frac{b}{p}) = 1$, then $h(p) \mid (p - (\frac{D}{p}))/2$. Since, by hypothesis, $h(p) = p+1$, we conclude that $(\frac{b}{p}) = -1$.

Now, suppose that $(\frac{b}{p}) = -1$. By [19, Thm. 4], there exists a p-regular recurrence $u(a,b)$ such that $(\frac{D}{p}) = -1$ and $h(p) = p+1$. If $e = 1$, we are done. Suppose instead that $e > 1$.

Let α and β be the characteristic roots of $u(a,b)$ and P a prime ideal lying over p in the algebraic number field $\mathbf{Q}(\alpha,\beta)$. Since $(\frac{D}{p}) = -1$, p is unramified. Moreover, the characteristic polynomial is irreducible over $\mathbf{Q}(\alpha,\beta)/P$ and

$$\alpha-\beta\not\equiv 0 \pmod{P}. \tag{3.11}$$

Since the Frobenius automorphism exchanges the roots α and β, we also obtain

$$\begin{aligned} \alpha^p &\equiv \beta \pmod{P} \quad \text{and} \quad p\alpha^p \equiv p\beta \pmod{P^2},\\ \beta^p &\equiv \alpha \pmod{P} \quad \text{and} \quad p\beta^p \equiv p\alpha \pmod{P^2}. \end{aligned} \tag{3.12}$$

Since $e\geq 1$, it follows that $h(p^2)=h(p)=p+1$, and hence, by Lemma 2.4,

$$\alpha^{p+1}\equiv\beta^{p+1} \pmod{P^2}. \tag{3.13}$$

Now, consider the new sequence $u(a',b')$ with characteristic roots $\alpha'=\alpha+p$ and $\beta'=\beta+p$ and satisfying

$$\begin{aligned} a' &= \alpha'+\beta' = (\alpha+p)+(\beta+p) = \alpha+\beta+2p = a+2p\equiv a \pmod{p},\\ b' &= \alpha'\beta' = (\alpha+p)(\beta+p) = \alpha\beta+(\alpha+\beta)p+p^2 = b+ap+p^2\equiv b \pmod{p}. \end{aligned} \tag{3.14}$$

Since $a\equiv a' \pmod{p}$ and $b\equiv b' \pmod{p}$, we know that $h_{u(a',b')}(p)=p+1$, and hence, by Lemma 2.4,

$$(\alpha+p)^{p+1}-(\beta+p)^{p+1}\equiv 0 \pmod{P}. \tag{3.15}$$

By the binomial theorem,

$$\begin{aligned} (\alpha+p)^{p+1} &\equiv \alpha^{p+1}+(p+1)p\alpha^p\equiv\alpha^{p+1}+p\alpha^p \pmod{P^2},\\ (\beta+p)^{p+1} &\equiv \beta^{p+1}+(p+1)p\beta^p\equiv\beta^{p+1}+p\beta^p \pmod{P^2}. \end{aligned} \tag{3.16}$$

Thus, by (3.11), (3.12), and (3.13),

$$\begin{aligned} (\alpha+p)^{p+1}-(\beta+p)^{p+1} &\equiv (\alpha^{p+1}+p\alpha^p)-(\beta^{p+1}+p\beta^p) \pmod{P^2}\\ &\equiv p\alpha^p-p\beta^p \pmod{P^2}\\ &\equiv p\beta-p\alpha \pmod{P^2}\\ &\equiv p(\beta-\alpha) \pmod{P^2}\\ &\not\equiv 0 \pmod{P^2}. \end{aligned} \tag{3.17}$$

Consequently, $h_{u(a',b')}(p^2)>h_{u(a',b')}(p)$, and hence $e=1$. It now follows that the sequence $u(a',b')$ satisfies the requirements of the theorem. □

3.4. The condition $\operatorname{ord}_{p^{2e}}(b)\mid p-1$**.** In this section, we consider sequences for which $\operatorname{ord}_{p^{2e}}(b)\mid p-1$ and $p\nmid D$. Note that, by Theorems 2.10 and 2.13, these sequences satisfy $e=f$. Thus, the sequences here specialize the condition of the previous section; however, we replace the condition $(\frac{D}{p})=-1$ with the less restrictive condition $p\nmid D$.

Theorem 3.6. *Suppose that $p\nmid D$ and $\operatorname{ord}_{p^{2e}}(b)\mid p-1$. Then $v(a,b)$ is* not *p-stable. Furthermore, we have the following stability criteria for $w(a,b)\in\mathcal{F}(a,b)$.*

(a) *If $w(a,b)$ is a* **mot** *of $v(a,b)$ modulo p^e, then $w(a,b)$ is* not *p-stable.*

(b) *If* $w(a,b)$ *is* not *a* **mot** *of* $v(a,b)$ *modulo* p *and* not *a* **mot** *of* $u(a,b)$ *modulo* p*, then* $w(a,b)$ *is* p*-stable with* $1 \le \iota(p) \le e$*.*

(c) *Suppose that* $w(a,b)$ *is* not *a* **mot** *of* $v(a,b)$ *modulo* p*, but that* $w(a,b)$ *is a* **mot** *of* $u(a,b)$ *modulo* p*. Choose* m *maximal such that* $m \le e$ *and* $w(a,b)$ *is a* **mot** *of* $u(a,b)$ *modulo* p^m*. Then* $w(a,b)$ *is* p*-stable with* $1 \le \iota(p) \le e$*.*

Note. In particular, if $p \nmid D$ and $b = \pm 1$, then each sequence $w(a,b) \in \mathcal{F}(a,b)$ satisfies the hypotheses of Theorem 3.6.

Proof. (a) By Theorem 2.13, $v(a,b)$ satisfies Hypothesis 2.9 for $n = 0$. Suppose that $r > f$. Since $w(a,b)$ is in the same p^e-block as $v(a,b)$, Theorem 2.12(a) implies that there are at least s distinct p-regular residues d modulo p^r for which

$$\nu_w(d,p^r) \ge p^{r-r^*}. \tag{3.18}$$

Clearly, this implies that $\max(\Omega_w(p^r))$ is unbounded as a function of r, and hence $w(a,b)$ is not p-stable.

(b) As in the proof of Theorem 3.2(b), since $w(a,b)$ lies in a different p-block than $u(a,b)$, the elements of $w(a,b)$ are all p-regular. As in (a), Theorem 2.13 implies that $v(a,b)$ satisfies Hypothesis 2.9 for $n = 0$. Thus, Theorem 2.11 implies that the p-regular residues d modulo p^r satisfy

$$\nu(d,p^r) = \nu(d,p^f) \le \nu(d,p) \tag{3.19}$$

when $r \ge f = e$. It follows that $w(a,b)$ is p-stable with $1 \le \iota(p) \le e$, as desired.

(c) As in (b), the p-regular residues d modulo p^r satisfy

$$\nu(d,p^r) = \nu(d,p^f) \le \nu(d,p) \tag{3.20}$$

when $r \ge f = e$.

As in the proof of Theorem 3.4, to handle the p-singular residues we consider separately the cases that $m < e$ and $m = e$.

If $m < e$, we know that $e > 1$ and can apply Theorem 2.15. Since $e = f$, p-singular residues d satisfy

$$\nu(d,p^r) = p^{e-f} = 1 \tag{3.21}$$

when $r \ge e$. It follows that $w(a,b)$ is p-stable with $1 \le \iota(p) \le e$.

If $m = e$, we appeal to Theorem 2.14. Since $w(a,b)$ is a **mot** of $u(a,b)$ modulo p^e and $e = f$, Theorem 2.14 implies that p-singular residues d satisfy

$$\nu(d,p^r) = \begin{cases} 0 & \text{if } p^e \nmid d, \\ s & \text{if } p^e \mid d, \end{cases} \tag{3.22}$$

when $r \ge e$. In either case, the frequency is independent of r, and it follows that $w(a,b)$ is p-stable with $1 \le \iota(p) \le e$. □

Corollary 3.7. *Suppose that* $p \nmid D$*, that* $\operatorname{ord}_{p^{2e}}(b) \mid p-1$*, and that* $(\frac{b}{p}) = 1$*. Then* $h(p) \mid (p - (\frac{D}{p}))/2$*, and we have the following stability criteria for* $w(a,b) \in \mathcal{F}(a,b)$*.*

(a) *If* $h(p)$ *is odd and* $w(a,b)$ *is a* **mot** *of* $u(a,b)$ *modulo* p^e*, then* $w(a,b)$ *is* p*-stable with* $1 \le \iota(p) \le e$*.*

(b) *If $h(p)$ is even and $w(a,b)$ is a* **mot** *of $t(a,b)$ modulo p, then $w(a,b)$ is p-stable with $1 \le \iota(p) \le e$.*

(c) *If $h(p) = (p - (\frac{D}{p}))/2$ and $e = 1$, then $w(a,b)$ is* not *p-stable if and only if $w(a,b)$ is a* **mot** *of $v(a,b)$ modulo p.*

(d) *If $h(p) = (p - (\frac{D}{p}))/2$, $(p - (\frac{D}{p}))/2$ is odd, and $e = 1$, then $w(a,b)$ is p-stable if and only if $w(a,b)$ is a* **mot** *of $u(a,b)$ modulo p.*

(e) *If $h(p) = (p - (\frac{D}{p}))/2$, $(p - (\frac{D}{p}))/2$ is even, and $e = 1$, then $w(a,b)$ is p-stable if and only if $w(a,b)$ is a* **mot** *of $t(a,b)$ modulo p.*

Conversely, if $\delta = \pm 1$ and b is any integer such that $\operatorname{ord}_{p^{2e}}(b) \mid p-1$ *and $(\frac{b}{p}) = 1$, then there exists an integer a and a p-regular recurrence $w(a,b)$ such that $(\frac{D}{p}) = \delta$ and $h(p) = (p - (\frac{D}{p}))/2$.*

Proof. The fact that $h(p) \mid (p - (\frac{D}{p}))/2$ is proven in [13, p. 441].

(a) By Lemma 2.6, $w(a,b)$ is not a **mot** of $v(a,b)$ modulo p. Hence (a) follows from Theorem 3.6(c).

(b) We first note that, by definition, $t(a,b)$ is defined when p is odd, $(\frac{b}{p}) = 1$, and $h(p)$ is even. Moreover, $t(a,b)$ is not a **mot** of $u(a,b)$ or of $v(a,b)$. Therefore, (b) follows from Theorem 3.6(b).

(c), (d), (e) By [7, Thm. 2.14], the number of p-regular p-blocks in $\mathcal{F}(a,b)$ is

$$T_{\text{reg}}(p) = \frac{\left(p - \left(\frac{D}{p}\right)\right)}{h(p)} = \frac{2h(p)}{h(p)} = 2. \tag{3.23}$$

One of these p-regular blocks contains the sequence $v(a,b)$. Since $e = 1$, Theorem 3.6 implies that $w(a,b)$ is not p-stable if and only if $w(a,b)$ lies in the same p-block as $v(a,b)$, and (c) follows immediately. If $h(p)$ is odd, then the other p-regular p-block contains $u(a,b)$, while if $h(p)$ is even, the other p-regular p-block contains $t(a,b)$. Thus (d) and (e) follow from (a) and (b), respectively.

To prove the partial converse, suppose that $\operatorname{ord}_{p^{2e}}(b) \mid p-1$, $(\frac{b}{p}) = 1$, and $\delta = \pm 1$. The existence of an integer a and corresponding regular second-order recurrence $w(a,b)$ such that $(\frac{D}{p}) = \delta$ and $h(p) = (p - (\frac{D}{p}))/2$ follows from [16, Thm. 12(i)] and [19, Thm. 4]. □

3.5. The condition $b = \pm 1$. In this section, we sketch more detailed results in the case that $b = \pm 1$. These sequences have particular historical interest. Of course, the Fibonacci sequence itself belongs to the family $\mathcal{F}(1,-1)$. These are the sequences studied by Schinzel in the quintessential work [14], by Somer in [15, 17, 18, 20], and by Jacobson, Carroll, and Somer in [9].

In two theorems, dealing with $b = 1$ and $b = -1$ in turn, we describe the stability of sequences that belong to the same p^e-blocks as $u(a,b)$, $v(a,b)$, and $t(a,b)$. Since $b = \pm 1$, it is clear that $\operatorname{ord}_{p^{2e}}(b) \mid p-1$. Since we also assume that $p \nmid D$ in this section, the theorems here specialize those in the previous section. In particular, as in the previous section, each family $\mathcal{F}(a,b)$ studied here satisfies $e = f$.

Theorem 3.8. *Suppose that $b = 1$ and $p \nmid D$.*

(a) *If $h(p)$ is odd and $w(a,b)$ is a* **mot** *of $u(a,b)$ modulo p^e, then $w(a,b)$ is p-stable* *and* $\iota(p) = 1$. *Furthermore, either* $\lambda(p) \equiv 1 \pmod 2$ *or* $\lambda(p) \equiv 2 \pmod 4$, *and, for all* $r \geq 1$,

$$\Omega(p^r) = \begin{cases} \{0,1\} & \text{if } \lambda(p) \equiv 1 \pmod 2, \\ \{0,2\} & \text{if } \lambda(p) \equiv 2 \pmod 4. \end{cases} \tag{3.24}$$

(b) *If* $h(p)$ *is even and* $w(a,b)$ *is a* **mot** *of* $t(a,1)$ *modulo* p^e, *then* $w(a,b)$ *is* p*-stable and* $\iota(p) = 1$. *Furthermore,* $\lambda(p) \equiv 0 \pmod 4$ *and* $\Omega(p^r) = \{0,2\}$ *for all* $r \geq 1$.

(c) *If* $w(a,b)$ *is a* **mot** *of* $v(a,b)$ *modulo* p^e, *then* $w(a,b)$ *is* not p*-stable.*

Proof. (a) Since $w(a,b)$ is a **mot** of $u(a,b)$ modulo p^e, [7, Cor. 2.15] implies that $w(a,b)$ is a **mot** of $u(a,b)$ modulo p^r for all $r \geq e$. Therefore, $w(a,b)$ is a **mot** of $u(a,b)$ modulo p^r for all $r \geq 1$. Since two sequences in the same p^r-block have the same residue frequencies, we may assume that $w(a,b) = u(a,b)$.

By hypothesis, $h(p)$ is odd, so Lemma 2.6 implies that $w(a,b)$ is not a **mot** of $v(a,b)$ modulo p. Thus, by Theorem 3.6(c), $w(a,b)$ is p-stable with $1 \leq \iota(p) \leq e$.

From [15, Thm. 16], we see that $\lambda(p) \equiv 1 \pmod 2$ or $\lambda(p) \equiv 2 \pmod 4$ and

$$s = \begin{cases} 2 & \text{when } \lambda(p) \equiv 1 \pmod 2, \\ 1 & \text{when } \lambda(p) \equiv 2 \pmod 4. \end{cases} \tag{3.25}$$

In the case that $\lambda(p) \equiv 1 \pmod 2$, [18, Thm. 4] shows that $\Omega(p) = \{0,1\}$. Since, as previously observed, $e = f$, Theorem 2.14 implies that if $r \geq e$, then the p-singular residues d satisfy

$$\nu(d,p^r) = \begin{cases} 0 & \text{if } p^e \nmid d, \\ s = 1 & \text{if } p^e \mid d. \end{cases} \tag{3.26}$$

On the other hand, by Theorem 2.11, if $r \geq e$, then the p-regular residues d satisfy

$$\nu(d,p^r) = \nu(d,p^f) \leq \nu(d,p). \tag{3.27}$$

Clearly, (3.26) and (3.27) imply that $\Omega(p^r) = \{0,1\}$ when $r \geq e = f$. On the other hand, if $r \leq f$, then $\lambda(p^r) = \lambda(p^f)$ and it is clear that $\nu(d,p) \geq \nu(d,p^r)$. It follows that $\Omega(p^r) = \{0,1\}$ for all $r \geq 1$. In particular, $\iota(p) = 1$.

In the case that $\lambda(p) \equiv 2 \pmod 4$, [18, Thm. 5] shows that $\Omega_u(p) = \{0,2\}$. As before, Theorem 2.14 implies that if $r \geq e$, then the p-singular residues d satisfy

$$\nu(d,p^r) = \begin{cases} 0 & \text{if } p^e \nmid d, \\ s = 2 & \text{if } p^e \mid d. \end{cases} \tag{3.28}$$

On the other hand, the p-regular residues d continue to satisfy (3.27). Moreover, the same symmetry argument used to prove [18, Thm. 5] shows that 1 cannot occur as $\nu(d,p^r)$ for a p-regular residue d. It now follows from (3.28) and (3.27) that $\Omega(p^r) = \{0,2\}$ when $r \geq e$, and, as in the previous paragraph, $\Omega(p^r) = \{0,2\}$ for all $r \geq 1$. Once again, we also conclude that $\iota(p) = 1$.

(b) Since $w(a,b)$ is a **mot** of $t(a,b)$ modulo p^e, [7, Cor. 2.15] implies that $w(a,b)$ is a **mot** of $t(a,b)$ modulo p^r for all $r \geq e$. Therefore $w(a,b)$ is a **mot** of $t(a,b)$ modulo

p^r for all $r \geq 1$. Since two sequences in the same p^r-block have the same residue frequencies, we may assume that $w(a,b) = t(a,b)$.

By hypothesis, $h(p)$ is even and $w(a,b)$ is a **mot** of $t(a,b)$ modulo p. Consequently, Corollary 3.7(b) implies that $w(a,b)$ is p-stable with $1 \leq \iota(p) \leq e$.

By [18, Thm. 3(ii)], $\lambda(p) \equiv 0 \pmod 4$. By using the technique of [18, Thms. 4-6] together with the symmetry properties of $t(a,b)$ given in [20, Lem. 5], it is easy to see that $s = 2$ for this sequence, $\Omega(p) = \{0,2\}$, and that 1 cannot occur as $\nu(d,p^r)$ for a p-regular residue d. The argument can now be completed as in (a).

(c) This follows immediately from Theorem 3.6(a). □

Theorem 3.9. *Suppose that $b = -1$ and $p \nmid D$.*

(a) *If $h(p)$ is odd and $w(a,b)$ is a* **mot** *of $u(a,b)$ modulo p^e, then $w(a,b)$ is p-stable. Furthermore, $p \equiv 1 \pmod 4$ and*

1. *if $p = 5$ and $e = 1$, then $\iota(p) = 1$, and $\Omega(p^r) = \{2,4\}$ for all $r \geq 1$;*
2. *if $p = 5$ and $e > 1$, then $\iota(p) = 2$, and $\Omega(p) = \{2,4\}$ and $\Omega(p^r) = \{0,2,4\}$ for all $r \geq 2$;*
3. *if $p > 5$, then $\iota(p) = 1$, and $\Omega(p^r) = \{0,2,4\}$ for all $r \geq 1$.*

(b) *If $h(p)$ is even, $p \equiv 1 \pmod 4$, and $w(a,b)$ is a* **mot** *of $t(a,b)$ modulo p, then $w(a,b)$ is p-stable and $1 \leq \iota(p) \leq e$. Furthermore, $\Omega(p^r) = \{0,1\}$, $\{0,1,2\}$, or $\{0,2\}$ for all $r \geq 1$.*

(c) *If $w(a,b)$ is a* **mot** *of $v(a,b)$ modulo p^e, then $w(a,b)$ is* not *p-stable.*

Proof. (a) Since $w(a,b)$ is a **mot** of $u(a,b)$ modulo p^e and $u(a,b)$ is p-regular, [7, Cor. 2.15] implies that $w(a,b)$ is a **mot** of $u(a,b)$ for all $r \geq e$. It follows that $w(a,b)$ is a **mot** of $u(a,b)$ for all $r \geq 1$, and we may assume that $w(a,b) = u(a,b)$.

By [23, Thm. 4], $h(p^r)$ is odd if and only if both $\lambda(p^r) \equiv 4 \pmod 8$ and $E(p^r) = 4$. In particular, since $h(p)$ is odd, $s = 4$. Moreover, [15, Lem. 3] implies that $p \equiv 1 \pmod 4$. Now, by Euler's criterion, $(\frac{-1}{p}) = 1$, and we can apply Corollary 3.7(a) to conclude that $w(a,b)$ is p-stable with $1 \leq \iota(p) \leq e$. If $r \geq 1$, the same methods used to prove [17, Thm. 9] can be used to show that $\nu(d,p) = 2$ or $\nu(d,p) = 4$ when $\nu(d,p^r) \neq 0$.

Now, suppose that $p = 5$ and $e = 1$. Then $\iota(5) = 1$, and an explicit computation shows that $h(5)$ is odd if and only if $a \equiv 2 \pmod 5$ or $a \equiv 3 \pmod 5$. In both cases $\lambda(5) = 12$ and $\Omega(5) = \{2,4\}$.

Next, suppose that $p = 5$ and $e > 1$, and let $e^* = \min(r,e)$. By Theorem 2.14, if d is p-singular, then, for all r,

$$\nu(d,p^r) = \begin{cases} 0 & \text{if } p^{e^*} \nmid d, \\ s = 4 & \text{if } p^{e^*} \mid d. \end{cases} \tag{3.29}$$

In particular, when $r \geq 2$, we obtain $\nu(p,p^r) = 0$ and $\nu(0,p^r) = 4$.

Since, by Lemma 2.6, $u(a,b)$ is not a **mot** of $v(a,b)$, we can also apply Theorem 2.11. Thus, for p-regular residues d,

$$\nu(d,p^r) = \nu(d,p^f) \leq \nu(d,p) \tag{3.30}$$

when $r \geq f = e$. Since $\nu(1,5) = 2$, it follows that $2 \in \Omega(p^r)$ for all $r \geq 1$. Now, $\Omega(p^r) = \{0,2,4\}$ when $r \geq 2$. Since $\Omega(5) = \{2,4\}$ whenever $h(5)$ is odd, we conclude that $\iota(p) = 2$.

Finally, suppose that $p > 5$. Since $p \equiv 1 \pmod 4$, we know that $p > 7$, and the result is proven in [9].

(b) As in (a), we may assume that $w(a,b) = t(a,b)$. Since $p \equiv 1 \pmod 4$, Euler's criterion implies that $(\frac{-1}{p}) = 1$. Hence, by Corollary 3.7(b), $w(a,b)$ is stable, with $1 \le \iota(p) \le e$. Using the symmetry properties for $t(a,b)$ modulo p given in [20, Lem. 5] and employing methods similar to those used in the proofs of [17, Thms. 5, 7, and 9], we can show that $\Omega(p) = \{0,1\}$, $\{0,1,2\}$, or $\{0,2\}$. Finally, if $r \le f = e$, then $\nu(d,p) \ge \nu(d,p^r)$. It follows that $\Omega(p^r) = \{0,1\}$, $\{0,1,2\}$, or $\{0,2\}$ for all $r \ge 1$.

(c) This follows immediately from Theorem 3.6(a). □

References

[1] R. T. Bumby, *A distribution property for linear recurrence of the second order*, Proc. Amer. Math. Soc. **50** (1975), 101–106. MR 51 5475. Zbl 318.10006.

[2] W. Carlip and E. Jacobson, *A criterion for stability of two-term recurrence sequences modulo* 2^k, Finite Fields Appl. **2** (1996), no. 4, 369–406. MR 97h:11012. Zbl 924.11007.

[3] ———, *On the stability of certain Lucas sequences modulo* 2^k, Fibonacci Quart. **34** (1996), no. 4, 298–305. MR 97c:11026. Zbl 866.11009.

[4] ———, *Unbounded stability of two-term recurrence sequences modulo* 2^k, Acta Arith. **74** (1996), no. 4, 329–346. MR 97b:11021. Zbl 838.11009.

[5] ———, *Stability of two-terms recurrence sequences with even parameter*, Finite Fields Appl. **3** (1997), no. 1, 70–83. MR 98b:11014. Zbl 905.11011.

[6] W. Carlip, E. Jacobson, and L. Somer, *A criterion for stability of two-term recurrence sequences modulo odd primes*, Application of Fibonacci Numbers (G. E. Bergum et al., ed.), vol. 7, Kluwer Acad. Publ., Dordrecht, 1998, Proceedings of the 7th international research conference on Fibonacci numbers and their applications, Graz, Austria, July 15–19, 1996, pp. 49–60. CMP 1 638 430. Zbl 921.11012.

[7] W. Carlip and L. Somer, *Bounds for frequencies of residues of regular second order recurrences modulo* p^r, Number Theory in Progress (Kálmán Győry, Henryk Iwaniec, and Jerzy Urbanowicz, eds.), Walter de Gruyter, Berlin, 1999, Proceedings of the International Conference on Number Theory held in Honor of the 60th Birthday of Andrzej Schinzel (Zakopane, Poland, 1997), pp. 691–719. CMP 1 689 539. Zbl 990.56684.

[8] R. D. Carmichael, *On the numerical factors of the arithmetic forms* $\alpha^n \pm \beta^n$, Ann. of Math. (2) **15** (1913–1914), no. 1/4, 30–70.

[9] D. Carroll, E. Jacobson, and L. Somer, *Distribution of two-term recurrence sequences mod* p^e, Fibonacci Quart. **32** (1994), no. 3, 260–265. MR 95f:11010. Zbl 809.11011.

[10] E. Jacobson, *Almost uniform distribution of the Fibonacci sequence*, Fibonacci Quart. **27** (1989), no. 4, 335–337. MR 90h:11015. Zbl 681.10005.

[11] ———, *A brief survey on distribution questions for second order linear recurrences*, Number Theory (Banff, AB, 1988) (Berlin), de Gruyter, 1990, pp. 249–254. MR 92e:11015. Zbl 694.10012.

[12] ———, *Distribution of the Fibonacci numbers mod* 2^k, Fibonacci Quart. **30** (1992), no. 3, 211–215. MR 93f:11014. Zbl 760.11007.

[13] D. H. Lehmer, *An extended theory of Lucas' functions*, Ann. of Math. (2) **31** (1930), no. 3, 419–448.

[14] A. Schinzel, *Special Lucas sequences, including the Fibonacci sequence, modulo a prime*, A Tribute to Paul Erdős (Cambridge), Cambridge Univ. Press, 1990, pp. 349–357. MR 92f:11029. Zbl 716.11009.

[15] L. Somer, *The divisibility properties of primary Lucas recurrences with respect to primes*, Fibonacci Quart. **18** (1980), no. 4, 316–334. MR 82g:10023. Zbl 441.10007.

[16] ______, *Possible periods of primary Fibonacci-like sequences with respect to a fixed odd prime*, Fibonacci Quart. **20** (1982), no. 4, 311–333. MR 84g:10022. Zbl 498.10010.

[17] ______, *Distribution of residues of certain second-order linear recurrences modulo p*, Applications of Fibonacci Numbers (Dordrecht) (G. E. Bergum et al., ed.), vol. 3, Kluwer Acad. Publ., 1990, Proceedings of the Third International Conference on Fibonacci Numbers and their Applications held at the University of Pisa, Pisa, July 25–29, 1988, pp. 311–324. MR 92j:11019. Zbl 722.11008.

[18] ______, *Distribution of residues of certain second-order linear recurrences modulo p–II*, Fibonacci Quart. **29** (1991), no. 1, 72–78. MR 92k:11016. Zbl 728.11010.

[19] ______, *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 (Las Vegas, NV, 1991) (New York), Lecture Notes in Pure and Appl. Math., vol. 141, Dekker, 1993, pp. 195–207. MR 94c:11014. Zbl 790.11013.

[20] ______, *Upper bounds for frequencies of elements in second-order recurrences over a finite field*, Applications of Fibonacci Numbers (Dordrecht) (G. E. Bergum et al., ed.), vol. 5, Kluwer Acad. Publ., 1993, Proceedings of the Fifth International Conference on Fibonacci Numbers and their Applications held at the University of St. Andrews, St. Andrews, July 20–24, 1992, pp. 527–546. MR 95c:11021. Zbl 805.11022.

[21] L. Somer and W. Carlip, *Bounds for frequencies of residues of second order recurrences modulo p^r*, preprint.

[22] W. A. Webb and C. T. Long, *Distribution modulo p^h of the general linear second order recurrence*, Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (8) **58** (1975), no. 2, 92–100. MR 54 7396. Zbl 325.10008.

[23] O. Wyler, *On second-order recurrences*, Amer. Math. Monthly **72** (1965), 500–506. MR 35#6641. Zbl 151.02503.

Somer: Department of Mathematics, Catholic University of America, Washington, DC 20064, USA

Carlip: Department of Mathematics, Duke University, Durham, North Carolina 27708, USA