# $p$-STABILITY OF DEGENERATE SECOND-ORDER RECURRENCES

**Lawrence Somer**
Department of Mathematics, Catholic University of America, Washington, D.C. 20064

**Walter Carlip**
Department of Mathematics and Computer Science
University of California, Santa Barbara, California 93106
*(Submitted August 2001-Final Revision January 2002)*

## 1. INTRODUCTION

In three earlier articles, [1], [5], and [2], we examined the frequency distribution of residues, modulo powers of an odd prime $p$, of terms of second-order recurrence sequences. Two of these articles, [1] and [2], provide general bounds for the frequency distribution function of a $p$-regular second-order recurrence sequence, while the third, [5], discusses the $p$-stability of these sequences. All three articles assume throughout that the sequences under study are nondegenerate. In this article we address this omission by examining the degenerate second-order recurrences. The degenerate recurrences are no mystery: much is known about them and they are easier to handle than their nondegenerate cousins. Nonetheless, characterizing the $p$-stability of the degenerate sequences fills a gap in the literature and serves as an interesting case study.

Throughout this paper we let $\mathcal{F}(a, b)$ denote the family of all second-order linear recurrence sequences $w(a, b)$ that satisfy 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 and $p \nmid (w_0, w_1)$. We also assume that $p \nmid b$, and hence that the sequences $w(a, b) \in \mathcal{F}(a, b)$ are purely periodic. Throughout this paper, $p$ represents an odd prime.

## 2. DEGENERATE RECURRENCES

For each positive integer $r$, the *period* of a second-order recurrence sequence $w(a, b)$ modulo $p^r$, denoted $\lambda_w(p^r)$, is the least positive integer $\lambda$ such that, for all $n$

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

In general, the sequence of periods $\{\lambda_w(p^t)\}_{t=1}^{\infty}$ is well understood: it is eventually geometric after an initial constant segment (see, e.g., Theorem 2.11 of [1]). We define the parameter $f(w)$ to be the largest integer $f$ such that $\lambda_w(p^f) = \lambda_w(p)$. For some recurrence sequences $w(a, b)$, the sequence $\{\lambda_w(p^t)\}_{t=1}^{\infty}$ is constant. In this case, the parameter $f(w)$ fails to exist, and we write, informally, $f(w) = \infty$.

For each positive integer $r$, the *restricted period* of a second-order recurrence sequence $w(a, b)$ modulo $p^r$, denoted $h_w(p^r)$, is the least positive integer $h$ such that, for some integer $M$ and for all $n$,

$$w_{n+h} \equiv Mw_n \pmod{p^r}.$$

The integer $M = M_w(p^r)$, defined up to congruence modulo $p^r$, is called the *multiplier* of $w(a,b)$ modulo $p^r$. Clearly, $h_w(p^r) = 1$ if and only if $w(a,b)$ satisfies a first-order recurrence relation modulo $p^r$.

The behavior of the sequence of restricted periods $\{h_w(p^t)\}_{t=1}^{\infty}$ of a second-order recurrence $w(a,b)$ is also well understood: it is also eventually geometric after an initial constant segment (see, e.g., Theorem 2.11 of [1]). When the initial constant segment has finite length, the sequence is said to be *nondegenerate*, and we define the parameter $e(w)$ to be the largest integer $e$ such that $h_w(p^e) = h_w(p)$. For some sequences, however, the entire sequence of restricted periods $\{h(p^t)\}_{t=1}^{\infty}$ is constant. In this case the parameter $e(w)$ does not exist or, informally, $e(w) = \infty$, and the sequence is called *degenerate*.

It is easy to see that if $e(w)$ exists, then $f(w)$ also exists and $f(w) \le e(w)$. Consequently $f(w) = \infty$ only if $e(w) = \infty$.

## 3. REGULAR AND IRREGULAR RECURRENCES

The second-order recurrence sequences may be partitioned into two categories: the $p$-regular sequences, which satisfy

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

and the $p$-irregular sequences, which fail to satisfy (3.1). This classification applies to degenerate sequences as well as to their nondegenerate cousins. In this section, we examine the consequences of $p$-regularity and $p$-irregularity for degenerate sequences.

**3.1 Irregular Degenerate Recurrences**: It is an easy consequence of the definition that each $p$-irregular recurrence $w(a,b) \in \mathcal{F}(a,b)$ satisfies a first-order recurrence relation modulo $p$. In this case, $h_w(p) = 1$. If $w(a,b)$ is also degenerate, then $h_w(p^r) = h_w(p) = 1$ for all $r \ge 1$, and therefore $w(a,b)$ obeys a first order recurrence relation modulo $p^r$ for every $r \ge 1$. In fact, as we show below, the degenerate $p$-irregular sequences of $\mathcal{F}(a,b)$ are easily recognized: they are simply geometric sequences. We begin with an easy lemma.

**Lemma 3.1**: *If $w(a,b) \in \mathcal{F}(a,b)$ is $p$-irregular, then every term $w_n$ of the sequence $w(a,b)$ is relatively prime to $p$.*

**Proof**: Since $w(a,b)$ is $p$-irregular, it satifies a first-order recurrence relation modulo $p$. Thus there is an integer $\xi$ such that $p \nmid \xi$ and $w_k \equiv \xi^k w_0 \pmod{p}$ for all $k$. Since $p \nmid (w_0, w_1)$, it follows that $w_0 \not\equiv 0 \pmod{p}$, and hence $w_k \not\equiv 0 \pmod{p}$ for all $k$, as desired. □

**Theorem 3.2**: *If $w(a,b) \in \mathcal{F}(a,b)$ is both degenerate and $p$-irregular, then $w(a,b)$ itself satisfies a first-order recurrence relation.*

**Proof**: Suppose that $w(a,b)$ is both degenerate and $p$-irregular. Since $w(a,b)$ is $p$-irregular, it satisfies a first-order recurrence relation modulo $p$, and hence $h_w(p) = 1$. Since $w(a,b)$ is also degenerate, $h_w(p^r) = 1$ for all integers $r \ge 1$, and hence $w(a,b)$ satisfies a first-order relation modulo $p^r$ for each $r \ge 1$. It follows that for each $r$, there exists an integer $\xi_r$ such that, for all $k \ge 0$,

$$w_{k+1} \equiv \xi_r w_k \pmod{p^r}.$$

Therefore, for all $k \ge 0$,

$$\frac{w_{k+1}}{w_k} \equiv \frac{w_1}{w_0} \pmod{p^r},$$

and it follows that

$$w_{k+1}w_0 \equiv w_k w_1 \pmod{p^r}. \tag{3.2}$$

However, since (3.2) holds for all $r \geq 1$, we have equality

$$w_{k+1}w_0 = w_k w_1,$$

for all $k$. An easy induction argument now yields

$$w_{k+1} = \frac{w_1^{k+1}}{w_0^k}. \tag{3.3}$$

Let $q$ be a prime factor of $w_0$ and assume $q^s \parallel w_0$ and $q^s \parallel w_1$. Then (3.3) implies that $(k+1)t \geq ks$ for all $k$. Hence $t/s \geq k/(k+1)$ for all $k$, so

$$\frac{t}{s} \geq \lim_{k\to\infty} \frac{k}{k+1} = 1,$$

and therefore $t \geq s$. Since $q$ was an arbitrary prime factor of $w_0$, it follows that $w_0 \mid w_1$.

Finally, if we set $\xi = w_1/w_0$, then $\xi$ is an integer, and (3.3) yields $w_{k+1} = \xi^k w_1 = \xi^{k+1} w_0$. Consequently $w(a,b)$ is a geometric sequence, as desired. □

**3.2 Regular Degenerate Recurrences**: The $p$-regular degenerate recurrences are somewhat more complex than the $p$-irregular degenerate recurrences. In the remainder of this section we characterize the degenerate regular recurrences, their restricted periods, and their multipliers in terms of the roots $\alpha$ and $\beta$ of the characteristic polynomial $f(x) = x^2 - ax + b$ and the parameters $a$ and $b$.

A parameter associated to a $p$-regular sequence $w(a,b)$ that takes on the same value for all $p$-regular sequences in the family $\mathcal{F}(a,b)$ is known as a *global parameter* of the family $\mathcal{F}(a,b)$. It is a straightforward consequence of Cramer's rule that the period, restricted period, and multiplier are global parameters (see, e.g., [1, p. 695]). It follows that $e(w)$ is also a global parameter, and therefore the $p$-regular sequences of the family $\mathcal{F}(a,b)$ either are all degenerate or are all nondegenerate. When $w(a,b)$ is $p$-regular, we often write $\lambda_w(p^r) = \lambda(p^r),\ h_w(p^r) = h(p^r),\ M_w(p^r) = M(p^r),\ f(w) = f$, and $e(w) = e$.

The following theorem describes the periods and restricted periods of $p$-regular degenerate second-order recurrence sequences, and is the analogue for degenerate sequences of Theorem 2.11 of [1].

**Theorem 3.3**: *Suppose that the sequences of $\mathcal{F}(a,b)$ are degenerate, and let $s = \lambda(p)/h(p)$.*

(a) *If $r \geq 1$, then $h(p^r) = h(p)$.*

(b) *If $r \geq 1$ and $f = \infty$, then $\lambda(p^r) = \lambda(p)$.*

(c) *If $r \geq f$, then $\lambda(p^r) = p^{r-f}\lambda(p)$.*

(d) *If $r \geq 1$, then*

$$E(p^r) = \operatorname{ord}_{p^r}(M(p^r)) = \frac{\lambda(p^r)}{h(p^r)} = \begin{cases} \frac{\lambda(p)}{h(p)} = s & \text{if } r \leq f \text{ or } f = \infty, \\ \frac{p^{r-f}\lambda(p)}{h(p)} = p^{r-f}s & \text{if } r > f. \end{cases}$$

**Proof**: Parts (a), (b), and (c) follow from the definitions of $e$ and $f$ and well-known properties of the period of a second-order recurrence (see, e.g., [6]). Part (d) is an immediate consequence. □

The family $\mathcal{F}(a,b)$ always contains the generalized Lucas sequence $u(a,b)$, which is characterized by its initial terms $u_0 = 0$ and $u_1 = 1$. It is well known that $u(a,b)$ is always $p$-regular, and therefore the global parameter $e$ is uniquely determined by $p^e \parallel u_{h(p)}$. In particular, the $p$-regular sequences in $\mathcal{F}(a,b)$ are all degenerate if and only if $u_{h(p)} = 0$.

**Theorem 3.4**: *The $p$-regular sequences in $\mathcal{F}(a,b)$ are degenerate if and only if $\alpha/\beta$ is a primitive $m^{th}$ root of unity for some $m > 1$.*

**Proof**: The $p$-regular sequences in $\mathcal{F}(a,b)$ are degenerate if and only if $u(a,b)$ is degenerate, and this occurs precisely when $u_{h(p)} = 0$. The terms of $u(a,b)$ are determined by the Binet formula

$$u_n = \begin{cases} \frac{\alpha^n - \beta^n}{\alpha - \beta} & \text{if } \alpha \neq \beta, \\ n\alpha^{n-1} & \text{if } \alpha = \beta. \end{cases} \tag{3.4}$$

We note that if either $\alpha = 0$ or $\beta = 0$, then $b = \alpha\beta = 0$, contrary to our global hypothesis that $p \nmid b$. If $\alpha = \beta \neq 0$, then $u_n \neq 0$ for all $n \geq 1$, and $u(a,b)$ is not degenerate. Finally, if $\alpha \neq \beta$, then $u_n = 0$ if and only if $(\alpha/\beta)^n = \alpha^n/\beta^n = 1$, as desired. □

**Theorem 3.5**: *Suppose that the $p$-regular sequences in $\mathcal{F}(a,b)$ are degenerate, and choose $m$ so that $\alpha/\beta$ is a primitive $m^{th}$ root of unity. Then $m \in \{2,3,4,6\}$. Moreover, $h(p^r) = m$ and $M(p^r) \equiv u_{m+1} \pmod{p^r}$ for all $r \geq 1$. Finally, the parameters $a$ and $b$ may be characterized as follows.*

(a) *If $\alpha/\beta = -1$, then $a = 0, p \nmid b$, and $u_3 = -b \equiv M(p^r) \pmod{p^r}$ for all $r \geq 1$.*
(b) *If $\alpha/\beta$ is a primitive cube root of unity, then $p \nmid a$, $b = a^2$, and $u_4 = -a^3 \equiv M(p^r) \pmod{p^r}$ for all $r \geq 1$.*
(c) *If $\alpha/\beta$ is a primitive fourth root of unity, then $a = 2n$ and $b = 2n^2$, for some integer $n$ relatively prime to $p$, and $u_5 = -4n^4 \equiv -b^2 \equiv M(p^r) \pmod{p^r}$ for all $r \geq 1$.*
(d) *If $\alpha/\beta$ is a primitive sixth root of unity, then $p \neq 3$. Moreover, $a = 3n$ and $b = 3n^2$, for some integer $n$ relatively prime to $p$, and $u_7 = -27n^6 \equiv -b^3 \equiv M(p^r) \pmod{p^r}$ for all $r \geq 1$.*

**Proof**: By Theorem 3.4, $\alpha/\beta$ is a primitive $m^{th}$ root of unity for some $m > 1$. The Binet formula (3.4) implies that $(\alpha/\beta)^n = 1$ if and only if $u_n = 0$, and hence $m$ is the smallest positive integer such that $u_m = 0$. It follows that $h(p^r) = m$ and $M(p^r) \equiv u_{m+1} \pmod{p^r}$ for all $r \geq 1$.

Since $\alpha$ and $\beta$ are roots of a quadratic polynomial with integral coefficients, $\alpha/\beta$ lies in a quadratic extension of the rationals, and hence $m$ must be 2, 3, 4, or 6. The descriptions of $a$ and $b$ given in parts (a), (b), (c), and (d) are given in [7, p. 613] and follow from the fact that $\alpha/\beta + \beta/\alpha = (a^2 - 2b)/b$ is an integer (since it is an algebraic integer and rational), and has absolute value at most 2 (since it is the sum of two roots of unity). Computation of the multipliers $M(p^r)$ appears in [4]. □

**Lemma 3.6**: *Suppose that $w(a,b) \in \mathcal{F}(a,b)$ is both $p$-regular and degenerate and that $\alpha/\beta$ is a primitive $m^{th}$ root of unity. Then $p$ divides at most one of the terms $w_0, w_1, \ldots, w_{m-1}$.*

**Proof**: The lemma is immediate from the observation that at most one term in a restricted period of $w(a,b)$ modulo $p$ can be divisible by $p$ and, by Theorem 3.5, $h(p) = m$. □

**Remark 3.7**: If $\mathcal{F}(a,b)$ is a family of second-order recurrence sequences, then $\mathcal{F}(a,b)$ contains all translations of each recurrence in $\mathcal{F}(a,b)$. Consequently, if the $p$-regular sequences of $\mathcal{F}(a,b)$

are degenerate and $\alpha/\beta$ is a primitive $m^{th}$ root of unity as in Lemma 3.6, then we can always choose a sequence $w(a,b) \in \mathcal{F}(a,b)$ such that $p \nmid w_1 w_2 \dots w_{m-1}$.

## 4. STABILITY

The concept of *stability* generalizes the idea of *uniform distribution* of a sequence, and is useful for understanding the distribution of residues of a sequence modulo powers of a prime $p$. 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.,

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

A sequence is *uniformly distributed* modulo $m$ if $|\Omega_w(m)| = 1$, that is, if the residues $d$ modulo $m$ each appear with the same frequency in a single period of $w(a,b)$ modulo $m$. If $|\Omega_w(m)| = 2$, i.e., if the residues $d$ appear with two distinct frequencies in a single period of $w(a,b)$ modulo $m$, then $w(a,b)$ is said to be *almost uniformly distributed* modulo $m$. More generally, the cardinality of $\Omega_w(m)$ measures how far the sequence $w(a,b)$ deviates from being uniformly distributed modulo $m$.

In 1992, while investigating the Fibonacci sequence $u(1,-1)$ modulo powers of two, Eliot Jacobson [3] discovered that for some sequences $w(a,b)$, the sets $\Omega_w(p^r)$ are eventually constant as a function of $r$, and therefore these sequences $w(a,b)$ are not too far from being uniformly distributed modulo *any* power of $p$. The concept of sequence *stability modulo* $p$ arose from Jacobson's early study and describes the asymptotic structure of the sets $\Omega_w(p^r)$ for some sequences.

**Definition 4.1**: 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 $r \geq N$.

If $w(a,b)$ is $p$-stable, then 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.

In studying the distribution of frequencies of residues of a sequence $w(a,b)$ modulo $p^r$, it is often convenient to write a cycle of the sequence in an $h_w(p^r) \times E(p^r)$ array, and analyze the frequency of residues in each column of the array. To this end we define the *partial frequency distribution function* $\nu_{w,n}(d,p^r)$ as follows.

**Definition 4.2**: Let $w(a,b) \in \mathcal{F}(a,b)$ and set $h = h_w(p^r)$. We define $\nu_{w,n}(d,p^r)$, or simply $\nu_n(d,p^r)$, when $w(a,b)$ is understood, to be the number of terms $w_m$ in one period of the recurrence $w(a,b)$ modulo $p^r$ such that $w_m \equiv d \pmod{p^r}$ and $m \equiv n \pmod{h}$. In other words, $\nu_{w,n}(d,p^r)$ is the number of terms in the $n^{th}$ column of the array described above that are congruent to $d$ modulo $p^r$.

It follows immediately from the definition that

$$\nu(d,p^r) = \sum_{n=0}^{h_w(p^r)-1} \nu_n(d,p^r). \tag{4.1}$$

The next important lemma requires no revision from Lemma 4.2 of [1].

**Lemma 4.3**: *Let $w(a,b) \in \mathcal{F}(a,b)$ and set $\lambda = \lambda_w(p^r)$ and $h = h_w(p^r)$. Suppose that $p \nmid w_n$ and assume that there exists a nonnegative integer $\ell$ such that $w_{n+\ell h} \equiv d \pmod{p^r}$. Then*

$$\nu_n(d, p^r) = \frac{\lambda(p^r)/h(p^r)}{\mathrm{ord}_{p^r}(M(p^r))} = 1. \tag{4.2}$$

## 5. RESIDUE FREQUENCIES AND STABILITY OF DEGENERATE $p$-IRREGULAR SEQUENCES

In this section we compute the frequencies of residues of the degenerate $p$-irregular sequences of $\mathcal{F}(a,b)$ modulo powers of $p$, and characterize the $p$-stability of all such sequences.

**Theorem 5.1**: *Suppose that $w(a,b) \in \mathcal{F}(a,b)$ is both $p$-irregular and degenerate. Then for all $r \geq 1$,*

$$\Omega_w(p^r) = \{0, 1\}.$$

*In particular, $w(a,b)$ is $p$-stable with $\iota(w) = 1$.*

**Proof**: By Theorem 3.2, the sequence $w(a,b)$ is geometric. Thus there is an integer $\xi$, relatively prime to $p$, such that $w_k = \xi^k w_0$ for all $k \geq 0$. Since $p \nmid \xi$, the image of $\xi$ in $\boldsymbol{Z}/p^r\boldsymbol{Z}$ lies in the multiplicative group $(\boldsymbol{Z}/p^r\boldsymbol{Z})^*$ and has finite order. Let $\ell = \mathrm{ord}_{p^r}(\xi)$. Then $\lambda_w(p^r) = \ell$, and a single period of the sequence $w(a,b)$ consists of the elements $\{w_0, \xi w_0, \xi^2 w_0, \ldots, \xi^{\ell-1} w_0\}$. These are exactly the elements of the coset $\langle\xi\rangle w_0$ of the cyclic subgroup $\langle\xi\rangle$ of $(\boldsymbol{Z}/p^r\boldsymbol{Z})^*$. Since these elements are distinct, it follows that $\nu_w(\xi^i w_0, p^r) = 1$, for each $i \geq 0$. On the other hand, if $p \mid d$, then, by Lemma 3.1, $\nu_w(d, p^r) = 0$. It now follows that $\Omega_w(p^r) = \{0, 1\}$ for all $r$. It is an immediate consequence that $w(a,b)$ is $p$-stable with $\iota(w) = 1$. □

**Corollary 5.2**: *Suppose that $w(a,b) \in \mathcal{F}(a,b)$ is both $p$-irregular and degenerate. Then $w(a,b)$ is almost uniformly distributed modulo $p^r$ for all $r \geq 1$.*

## 6. RESIDUE FREQUENCY BOUNDS FOR DEGENERATE $p$-REGULAR SEQUENCES

In this section we provide bounds for the frequencies of residues, modulo powers of $p$, of the degenerate $p$-regular sequences.

**Theorem 6.1**: *Suppose that $w(a,b) \in \mathcal{F}(a,b)$ is both $p$-regular and degenerate, and either $r \leq f$ or $f$ does not exist. Then, for all residues $d$,*

$$\nu(d, p^r) \leq \nu(d, p).$$

**Proof**: Since the hypotheses imply that $\lambda(p^r) = \lambda(p)$, the theorem is immediate. □

**Theorem 6.2**: *Suppose that $w(a,b) \in \mathcal{F}(a,b)$ is both $p$-regular and degenerate, $p \nmid d$, and $r > f$. Then*

$$\nu(d, p^r) = \nu(d, p^f) \leq \nu(d, p).$$

**Proof**: Since, by definition of $f$, $\lambda(p^f) = \lambda(p)$, it is evident that $\nu(d, p^f) \leq \nu(d, p)$. Thus it suffices to show that $\nu(d, p^r) = \nu(d, p^f)$.

By Lemma 4.3, (4.1), and the fact that for a degenerate sequence $h(p^r) = h(p^f)$, it suffices to prove that $\nu_n(d, p^r) = 0$ if and only if $\nu_n(d, p^f) = 0$.

Clearly, if $\nu_n(d, p^f) = 0$, then $\nu_n(d, p^r) = 0$. To prove the converse, suppose that $\nu_n(d, p^f) > 0$. Then there is an $i$ such that $0 \le i < E(p^f)$ and $w_{n+ih} \equiv d \pmod{p^f}$. Therefore

$$w_{n+ih} \equiv d + \ell p^f \pmod{p^r}$$

for some $\ell$ satisfying $0 \le \ell < p^{r-f}$. Since $p \nmid d + \ell p^f$, the integer $d + \ell p^f$ is invertible modulo $p^r$ and we can find an integer $c$ such that $c(d + \ell p^f) \equiv 1 \pmod{p^r}$, so $cd \equiv -c\ell p^f \pmod{p^r}$. By the binomial theorem $(cd)^{p^{r-f}} \equiv 1 \pmod{p^r}$ and

$$\mathrm{ord}_{p^r}(cd) \mid p^{r-f}. \tag{6.1}$$

Now, by Theorem 3.3(d), $\mathrm{ord}_{p^r}(M(p^r)) = p^{r-f}s$. Since the unit group $(\boldsymbol{Z}/p^r\boldsymbol{Z})^*$ is cyclic, it follows that $cd \equiv M(p^r)^j \pmod{p^r}$ for some $j$. It follows that

$$w_{n+(i+j)h} \equiv M(p^r)^j w_{n+ih} \equiv cd(d + \ell p^f) \equiv d \pmod{p^r}.$$

Therefore $\nu_n(d, p^r) > 0$, as desired. □

**Theorem 6.3**: *Suppose that $w(a, b) \in \mathcal{F}(a, b)$ is both $p$-regular and degenerate, and assume that $p \mid d$. Let $m = h(p)$ and choose $c$ such that $p^c \parallel w_0 w_1 \dots w_{m-1}$, if possible. If $c > 0$ or is not defined, choose $k$ such that $0 \le k < m$ and $p \mid w_k$. Let $s = E(p), f^* = \min(r, f), t = \max(r - f^* - c, 0)$, and $d_i = M(p^r)^i w_k$ for $0 \le i < E(p^r)$.*

(a) *If $c$ is not defined or $0 < r \le c$, then* $\nu(d, p^r) = \begin{cases} p^{r-f^*}s & \text{if } p^r \mid d, \\ 0 & \text{otherwise.} \end{cases}$

(b) *If $c = 0$, then $\nu(d, p^r) = 0$ for all $r$.*

(c) *If $c > 0$ and $r > c$, then* $\nu(d, p^r) = \begin{cases} p^{r-f^*-t} & \text{if } d \equiv d_i \pmod{p^r}, \text{ for some} \\ & i \text{ satisfying } 0 \le i < p^t s, \\ 0 & \text{otherwise.} \end{cases}$

**Proof**: First note that, by Lemma 3.6, if $c > 0$ or is not defined, then the index $k$ is uniquely determined. Moreover, $p^c \parallel w_k$ when $c$ is defined and $c \neq 0$, and $w_k = 0$ when $c$ is not defined.

Suppose now that $\nu(d, p^r) \neq 0$, and choose $n$ such that $w_n \equiv d \pmod{p^r}$ and $0 \le n < \lambda(p^r)$. Since $\lambda(p^r) = h(p^r)E(p^r) = h(p)E(p^r) = mE(p^r)$, we can write $n = im + \ell$ with $0 \le i < E(p^r)$ and $0 \le \ell < m$, and therefore $w_n \equiv M(p^r)^i w_\ell \pmod{p^r}$. Since $d \equiv 0 \pmod{p}$, it follows that $M(p^r)^i w_\ell \equiv 0 \pmod{p}$, and, since $M(p^r)$ is invertible modulo $p$, Lemma 3.6 implies that $\ell = k$. Finally, we conclude that

$$d \equiv M(p^r)^i w_\ell \equiv M(p^r)^i w_k \pmod{p^r}. \tag{6.2}$$

(a) Assume that $c$ is not defined or that $0 < r \le c$. Then $w_k \equiv 0 \pmod{p^r}$, and hence $M(p^r)^i w_k \equiv 0 \pmod{p^r}$ for all $i$. Therefore, by (6.2), $d \equiv 0 \pmod{p^r}$. If $p^r \nmid d$, then we have a contradiction and conclude that $\nu(d, p^r) = 0$. On the other hand, if $p^r \mid d$, then $d \equiv M(p^r)^i w_k \equiv 0 \pmod{p^r}$ for all $i$ satisfying $0 \le i < E(p^r)$, and therefore $\nu(d, p^r) = \lambda(p^r)/h(p^r)$. The result now follows from Theorem 3.3 (d).

(b) Assume that $c = 0$. By (6.2), $M(p^r)^i w_k \equiv 0 \pmod{p}$, and it follows that $w_k \equiv 0 \pmod{p}$, a contradiction. Therefore $\nu(d, p^r) = 0$.

(c) Assume that $c > 0$ and $r > c$. Then (6.2) implies that $d \equiv d_i \equiv M(p^r)^i w_k \pmod{p^r}$ for some $i$ satisfying $0 \le i < E(p^r)$. In particular, $\nu(d, p^r) = 0$ if $d \not\equiv d_i \pmod{p^r}$ for all $i$.

Now suppose that $0 \le i < j < E(p^r)$ and write $w_k = wp^c$ with $w$ relatively prime to $p$. Then, clearly, $d_i \equiv d_j \pmod{p^r}$ if and only if $M(p^r)^i \equiv M(p^r)^j \pmod{p^{r-c}}$, or equivalently $M(p^r)^{j-i} \equiv 1 \pmod{p^{r-c}}$. It follows that the residues $d_i$ represent distinct classes modulo $p^r$ for $0 \le i < \text{ord}_{p^{r-c}}(M(p^{r-c}))$ and

$$\nu(d_i, p^r) = \frac{\text{ord}_{p^r}(M(p^r))}{\text{ord}_{p^{r-c}}(M(p^{r-c}))}.$$

By Theorem 3.3(d), we have

$$\text{ord}_{p^{r-c}}(M(p^{r-c})) = \begin{cases} s & \text{if } r < f + c, \\ p^{r-c-f}s & \text{if } f + c \le r, \end{cases}$$

and

$$\nu(d_i, p^r) = p^{r-f^*-t} = \begin{cases} \frac{s}{s} = 1 & \text{if } r < f, \\ \frac{p^{r-f}s}{s} = p^{r-f} & \text{if } f \le r < f + c, \\ \frac{p^{r-f}s}{p^{r-c-f}s} = p^c & \text{if } f + c \le r, \end{cases}$$

as desired. □

**Theorem 6.4**: *Suppose that $w(a,b) \in \mathcal{F}(a,b)$ is $p$-regular and degenerate, and that $f$ does not exist. Let $m = h = h(p)$ and $\lambda = \lambda(p)$. Then, for all $r \ge 1$, one of the following occurs*:

(a) $h(p^r) = h = 2, \lambda(p^r) = \lambda = 2, M(p^r) \equiv 1 \pmod{p^r}, a = 0,$ *and* $b = -1$;
(b) $h(p^r) = h = 2, \lambda(p^r) = \lambda = 4, M(p^r) \equiv -1 \pmod{p^r}, a = 0,$ *and* $b = 1$;
(c) $h(p^r) = h = 3, \lambda(p^r) = \lambda = 3, M(p^r) \equiv 1 \pmod{p^r}, a = -1,$ *and* $b = 1$; *or*
(d) $h(p^r) = h = 3, \lambda(p^r) = \lambda = 6, M(p^r) \equiv -1 \pmod{p^r}, a = 1,$ *and* $b = 1$.

*Moreover, for all $d$,*

$$\nu(d, p^r) = \nu(d, p^f) \le \nu(d, p).$$

**Proof**: All of the $p$-regular, degenerate second-order recurrences are listed in Theorem 3.5. Since both $f$ and $e$ fail to exist, we see that $h(p^r) = h$ and $\lambda(p^r) = \lambda$ for all $r \ge 1$. Moreover, since $f$ fails to exist exactly when $\text{ord}_{p^r}(M(p^r))$ is independent of $r$, it follows that $f$ fails to exist if and only if $u_m = 0$ and $u_{m+1} = \pm 1$. Clearly, only $m = 2, a = 0$, and $b = \pm 1$ and $m = 3, a = \pm 1$, and $b = 1$ satisfy this condition. The restricted periods $h(p^r)$ and multipliers $M(p^r)$ are given in Theorem 3.5, and the periods $\lambda(p^r)$ can be computed by $\lambda(p^r) = \text{ord}_{p^r}(M(p^r))h(p^r)$. □

## 7. STABILITY OF DEGENERATE $p$-REGULAR SEQUENCES

Finally, in this last section, we characterize the stability of degenerate $p$-regular second-order recurrence sequences. We begin by examining stability modulo $p$ when $p > 3$.

**Theorem 7.1**: *Suppose that $p > 3, w(a,b) \in \mathcal{F}(a,b)$ is both $p$-regular and degenerate, and $f$ does not exist. Define the constants $c, c_1, c_2, c_3, c_4, c_5, c_6$ by*

$$p^c \parallel w_0 w_1 \dots w_{m-1}$$

$$p^{c_1} \parallel w_1 - w_0 \quad p^{c_2} \parallel w_2 - w_0 \quad p^{c_3} \parallel w_2 - w_1$$

$$p^{c_4} \parallel w_1 + w_0 \quad p^{c_5} \parallel w_2 + w_0 \quad p^{c_6} \parallel w_2 + w_1$$

*and the constant* $t$ *by*

$$t = \begin{cases} 0 & \text{if } h = 2, a = 0, \text{ and } b = -1; \\ \max(c, c_1, c_4) & \text{if } h = 2, a = 0, b = 1, \text{ and } c, c_1, c_4 \text{ exist}; \\ \max(c_1, c_2, c_3) & \text{if } h = 3, a = -1, b = 1, \text{ and } c_1, c_2, c_3 \text{ exist}; \\ \max(c, c_2, c_4, c_6) & \text{if } h = 3, a = 1, b = 1, \text{ and } c, c_2, c_4, c_6 \text{ exist}; \\ 0 & \text{otherwise.} \end{cases}$$

*Then*

$$\Omega_w(p^r) = \begin{cases} \Omega_w(p) & \text{if } 1 \le r \le t \\ \Omega_w(p^{t+1}) & \text{if } r > t. \end{cases}$$

*In particular,* $w(a, b)$ *is* $p$*-stable with* $\iota_w(p) = t + 1$.

**Proof**: The $p$-regular and degenerate second-order recurrence sequences for which $f$ does not exist are determined in Theorem 6.4. If $w_0$ and $w_1$ are specified, one period modulo $p^r$ of each sequence described in Theorem 6.4(a), (b), (c), and (d) can be computed explicitly:

(a) $w_0, w_1, \ldots$

(b) $w_0, w_1, w_0 - w_1, \ldots$

(c) $w_0, w_1, -(w_1 + w_0), \ldots$

(d) $w_0, w_1, w_1 - w_0, -w_0, -w_1, -(w_1 - w_0), \ldots$

We inspect each case separately.

(a) Since $w(a, b)$ is $p$-regular, $w_0$ and $w_1$ are not congruent modulo $p$. It follows that $\Omega_w(p^r) = \{0, 1\}$ for all $r$, and clearly $\iota_w(p) = 1 = t + 1$.

(b) If $c$ does not exist, then either $w_0 = -w_0 = 0$ and $w_1 \not\equiv -w_1 \pmod{p}$, or $w_1 = -w_1 = 0$ and $w_0 \not\equiv -w_0 \pmod{p}$. Since $p > 3$, there are more than three possible residues, and hence $\Omega_w(p^r) = \{0, 1, 2\}$ for all $r \ge 1$. Clearly $\iota_w(p) = 1 = t + 1$.

If $c_1$ does not exist, then $w_0 = w_1$ and, since $w(a, b)$ is $p$-regular, neither $w_0$ nor $w_1$ is divisible by $p$. Consequently $\Omega_w(p^r) = \{0, 2\}$ for all $r \ge 1$. Similarly, if $c_4$ does not exist, then $w_0 = -w_1$, and neither $w_0$ nor $w_1$ is divisible by $p$. Again $\Omega_w(p^r) = \{0, 2\}$ for all $r \ge 1$. Clearly, in both cases, $\iota_w(p) = 1 = t + 1$.

Finally, suppose that $c, c_1$, and $c_4$ all exist. Then $w_0, w_1, -w_0$, and $-w_1$ are all distinct modulo $p^r$ when $r > t$. Since $p > 3$, there are at least five possible residues modulo $p^r$, and therefore $\Omega_w(p^r) = \{0, 1\}$ when $r > t$. If $1 \le r \le t$, then $2 \in \Omega_w(p^r)$, and it follows that $\iota_w(p) = t + 1$. Since $w(a, b)$ is $p$-regular, at most one of $c, c_1$, and $c_4$ is not zero. If all three are zero, then $t = 0$ and there is nothing more to show. In the remaining cases, since $p > 3$, there are more than four possible residues, so $0 \in \Omega_w(p^r)$. If either $c_1 > 0$ or $c_4 > 0$, then $c = 0$ and $\Omega_w(p^r) = \{0, 2\}$ for all $r \le t$, and, if $c > 0$, then $c_1 = c_2 = 0$ and $\Omega_w(p^r) = \{0, 1, 2\}$ for all $r \le t$.

(c) If one of $c_1, c_2$, and $c_3$ does not exist, then two of $w_0, w_1$, and $w_2$ are equal. Since $w(a, b)$ is $p$-regular, the third is not congruent to the other two modulo $p$. It follows that $\Omega_w(p^r) = \{0, 1, 2\}$ for all $r \ge 1$.

On the other hand, if $c_1, c_2$, and $c_3$ do exist, then, since $w(a, b)$ is $p$-regular, at most one of them is not zero. Thus, if $1 \le r \le t$, then $\Omega_w(p^r) = \{0, 1, 2\}$. Since $p > 3$, there are at least four possible residues, and therefore $\Omega_w(p^r) = \{0, 1\}$ when $r > t$. It follows that $\iota_w(p) = t + 1$.

(d) If $c$ does not exist, then, since $p > 3$ and there are at least 4 possible residues, it is easy to verify that $\Omega_w(p^r) = \{0, 2\}$ for all $r \ge 1$. Similarly, if one of $c_2, c_4$, or $c_6$ fails to exist, then,

since $p > 3$ and there are at least 5 possible residues, it is easy to verify that $\Omega_w(p^r) = \{0, 1, 2\}$ for all $r \geq 1$. In each case $\iota_w(p) = 1 = t + 1$.

On the other hand, if $c, c_2, c_4$, and $c_6$ all exist, then each term in one period of $w(a, b)$ is distinct modulo $p^{t+1}$, and $\Omega_w(p^r) = \{0, 1\}$ when $r > t$. If $r \leq t$, however, $2 \in \Omega_w(p^r)$ and it follows that $\iota_w(p) = t + 1$. As in the proof of (c), since $w(a, b)$ is $p$-regular, at most one of $c, c_2, c_4$, and $c_6$ is not zero. It is easy to check that if $c > 0$, then $\Omega_w(p^r) = \{0, 2\}$ for $r \leq t$ and, since $p > 3$ and there are at least five possible residues, if one of $c_2, c_4$, or $c_6$ is not zero, then $\Omega_w(p^r) = \{0, 1, 2\}$ when $r \leq t$. □

**Corollary 7.2**: *For every prime $p > 3$, there exist $p$-regular, degenerate sequences $w(a, b)$ satisfying criteria* (b), (c), *and* (d) *of Theorem 6.4 that are $p$-stable and have arbitrarily large stability index $\iota_w(p)$.*

**Proof**: Examples are easy to construct for arbitrary prime $p$.

For each positive integer $t$, the sequence $w(0, -1)$ with repeating cycle

$$1, p^t - 1, -1, -p^t + 1$$

satisfies (b) of Theorem 6.4. Clearly $\Omega_w(p^r) = \{0, 2\}$ when $r \leq t$ and $\Omega_w(p^r) = \{0, 1\}$ when $r > t$ as predicted by the proof of Theorem 7.1. Thus $w(0, 1)$ has stability index $\iota_w(p) = t + 1$. Of course, these sequences were chosen so that $c_4 = t$.

For each positive integer $t$, the sequence $w(-1, 1)$ with repeating cycle

$$1, p^t + 1, -p^t - 2$$

satisfies (c) of Theorem 7.1, and has stability index $\iota_w(p) = t + 1$.

Finally, for each positive integer $t$, the sequence $w(1, 1)$ with repeating cycle

$$p^t - 2, p^t - 1, 1, 2 - p^t, 1 - p^t, -1$$

satisfies (d) of Theorem 7.1, and has stability index $\iota_w(p) = t + 1$. □

When $p = 3$, the situation is similar, but requires additional care to handle cases in which every residue appears in a period of the sequence $w(a, b)$ modulo 3, preventing the residue frequency of zero from occurring.

**Theorem 7.3**: *Suppose that $w(a, b) \in \mathcal{F}(a, b)$ is both 3-regular and degenerate, and $f$ does not exist. Define the constants $c, c_1, c_4$ as in Theorem 7.1, and the constant $t$ by*

$$t = \begin{cases} 0 & \text{if } h = 2, a = 0, \text{ and } b = -1; \\ \max(c, c_1, c_4) & \text{if } h = 2, a = 0, b = 1, \text{ and } c, c_1, c_4 \text{ exist}; \\ 1 & \text{if } h = 2, a = 0, b = 1, \text{ and } c \text{ does not exist}; \\ 1 & \text{if } h = 3, a = -1, b = 1; \\ c & \text{if } h = 3, a = 1, b = 1, \text{ and } c \text{ exists}; \\ 1 & \text{if } h = 3, a = 1, b = 1, \text{ and } c \text{ does not exist}; \\ 0 & \text{otherwise.} \end{cases}$$

*Then for all $r > t$,*

$$\Omega_w(3^r) = \Omega_w(3^{t+1}) \neq \Omega_w(3^t).$$

*In particular, $w(a, b)$ is 3-stable with $\iota_w(p) = t + 1$.*

**Proof**: The proof is substantially the same as that for Theorem 7.1, however, one must be careful when the entire set of residues is exhausted by one period of $w(a,b)$, thereby excluding the residue frequency of zero. Again, we must examine separately the sequences with periods given by (a), (b), (c), and (d) in the proof of Theorem 7.1.

(a) The argument of Theorem 7.1 applies: $\Omega_w(3^r) = \{0,1\}$ for all $r \geq 1$.

(b) If $c$ does not exist, then either $w_0 = -w_0 = 0$ and $w_1 \not\equiv -w_1 \pmod{p}$, or $w_1 = -w_1 = 0$ and $w_0 \not\equiv -w_0 \pmod{p}$. If $r = 1$, there are only three possible residues and $\Omega_3 = \{1,2\}$. If $r > 1$, then there are more than three possible residues modulo $3^r$, and hence $\Omega_{3^r} = \{0,1,2\}$ for all $r \geq 2$.

If either $c_1$ or $c_4$ does not exist, then the argument of Theorem 7.1 applies: $\Omega_w(3^r) = \{0,2\}$ for all $r \geq 1$.

Finally, suppose that $c, c_1$, and $c_4$ all exist. Notice that it is impossible for $c, c_1$ and $c_4$ to all be zero: if neither $w_0$ nor $w_1$ is divisible by 3, then either $w_0 - w_1$ or $w_0 + w_1$ must be divisible by 3. Therefore $t \geq 1$, and $w_0, w_1, -w_0$, and $-w_1$ are distinct modulo $3^r$ when $r > t$. Clearly, there are at least five possible residues modulo $p^r$ and $\Omega_w(p^r) = \{0,1\}$ when $r > t$.

If $r \leq t$, then $2 \in \Omega_w(p^r)$, and it follows that $\iota_w(p) = t + 1$.

When $1 < r \leq t$, there are at least four possible residues modulo $3^r$. Therefore, if either $c_1 > 0$ or $c_4 > 0$, then $\Omega_w(3^r) = \{0,2\}$, and, if $c > 0$, then $\Omega_w(3^r) = \{0,1,2\}$ when $1 < r \leq t$.

Finally, if $r = 1$ and either $c_1 > 0$ or $c_4 > 0$, then $\Omega_w(3^r) = \{0,2\}$, and, if $r = 1$ and $c > 0$, then a single period exhausts the three possible residues and $\Omega_w(3) = \{1,2\}$.

(c) First, we observe that $c_1 = c_2 = c_3 = 0$, as follows. If $c_1 \neq 0$, then $w_0 \equiv w_1 \pmod{3}$, and therefore

$$w_0 w_2 - w_1^2 \equiv w_0(-(w_1 + w_0)) - w_0^2 \equiv -2w_0^2 - w_0^2 \equiv -3w_0^2 \equiv 0 \pmod{3},$$

contrary to the 3-regularity of $w(a,b)$. Similary, if $c_2 \neq 0$, then $w_0 \equiv w_2 \equiv -(w_1 + w_0) \pmod{3}$, and therefore

$$w_0 w_2 - w_1^2 \equiv w_0^2 - w_1^2 \equiv w_0^2 - (-2w_0)^2 \equiv -3w_0^2 \equiv 0 \pmod{3},$$

again contrary to the 3-regularity of $w(a,b)$. The argument that $c_3 = 0$ is similar, and we leave it to the reader to check.

Since $c_1 = c_2 = c_3 = 0$, we see that $w_0, w_1$, and $w_2$ are distinct modulo 3. Therefore one period of $w(a,b)$ modulo 3 exhausts all three possible residues and $\Omega_w(3) = \{1\}$, while $\Omega_w(3^r) = \{0,1\}$ when $r > 1$.

(d) If $c$ does not exist, then it is easy to verify that $\Omega_w(3) = \{2\}$ and $\Omega_w(3^r) = \{0,2\}$ when $r \geq 2$.

Next, we observe that $c_2 = c_4 = c_6 = 0$, as follows. If $c_2 \neq 0$, then $w_0 \equiv w_2 \equiv w_1 - w_0 \pmod{3}$, and therefore

$$w_0 w_2 - w_1^2 \equiv w_0^2 - w_1^2 \equiv w_0^2 - (2w_0)^2 \equiv -3w_0^2 \equiv 0 \pmod{3},$$

contrary to the 3-regularity of $w(a,b)$. If $c_4 \neq 0$, then $w_0 \equiv -w_1 \pmod{3}$, and therefore

$$w_0 w_2 - w_1^2 \equiv w_0(w_1 - w_0) - (-w_0)^2 \equiv -3w_0^2 \equiv 0 \pmod{3},$$

again contrary to the 3-regularity of $w(a,b)$. The argument that $c_6 = 0$ is similar, and we leave it to the reader to check.

Now suppose that $c$ does not exist. Notice that it is impossible for $c$ to be zero: if neither $w_0$ nor $w_1$ is divisible by 3, then either $w_2 = w_1 - w_0$ is divisible by 3 or $w_1 + w_0$ is divisible by 3. However, the latter condition cannot occur, since $c_4 = 0$.

It follows that $t \geq 1$, and there are at least nine possible residues modulo $3^r$ when $r > t$. Since $c, c_2, c_4$, and $c_6$ exist, the terms of $w(a,b)$ are distinct modulo $3^r$ and $\Omega_w(3^r) = \{0,1\}$ when $r > t$. Finally, since $t = c > 0$, it is easy to verify that $\Omega_w(3) = \{2\}$ and $\Omega_w(3^r) = \{0,2\}$, when $1 < r < t$. □

**Corollary 7.4**: *There exist* 3*-regular, degenerate sequences* $w(a,b)$ *satisfying criteria* (b) *and* (d) *of Theorem* 6.4 *that are* 3*-stable and have arbitrarily large stability index* $\iota_w(3)$.

**Proof**: For every positive integer $t$, the sequence with repeating cycle

$$1, 3^t - 1, -1, -3^t + 1$$

satisfies (b) of Theorem 6.4 and has stability index $\iota_w(3) = t + 1$.

For every positive integer $t$, the sequence with repeating cycle

$$3^t, 1, 1 - 3^t, -3^t, -1, -1 + 3^t$$

satisfies (d) of Theorem 6.4 and has stability index $\iota_w(3) = t + 1$. □

**Theorem 7.5**: *Suppose that* $w(a,b) \in \mathcal{F}(a,b)$ *is both* $p$*-regular and degenerate and that* $f$ *is defined. Let* $m = h(p^r)$ *for all* $r \geq 1$.

(a) *If* $p \nmid w_0 w_1 \dots w_{m-1}$, *then* $w(a,b)$ *is* $p$*-stable and* $1 \leq \iota(p) \leq f$.

(b) *If* $p^c \parallel w_0 w_1 \dots w_{m-1}$, *then* $w(a,b)$ *is* $p$*-stable and* $1 \leq \iota(p) \leq f + c$.

(c) *If* $w_0 w_1 \dots w_{m-1} = 0$, *then* $w(a,b)$ *is not* $p$*-stable.*

**Proof**: Part (a) follows immediately from Theorem 6.2 and Theorem 6.3(b), and part (b) follows from Theorem 6.2 and Theorem 6.3(c). Finally, if $w_0 w_1 \dots w_{m-1} = 0$, then Theorem 6.3(a) implies that $\nu(0, p^r)$ is unbounded as a function of $r$, and hence $w(a,b)$ is not $p$-stable. □

We conclude this section with examples of sequences satisfying conditions (a), (b), and (c) of Theorem 7.5.

**Example 7.6**: Let $p = 5, a = 57, b = 3249 = 57^2, w_0 = 1$, and $w_1 = 53$. Then one cycle of $(w)$ modulo $5^3$ is

$$1, 53, 22, 57, 21, 4, 124, 72, 103, 68, 104, 121.$$

The reader may verify that this sequence has the following properties:

- $\lambda_w(5) = \lambda_w(25) = \lambda_w(125) = 12$ and $\lambda_w(5^r) = 12 \cdot 5^{r-3}$ for $r > 3$, so $f(w) = 3$.
- $h_w(5^r) = 3$ for all $r \geq 1$, so $e(w) = \infty$ and $(w)$ is degenerate.
- $w_0 w_2 - (w_1)^2 \equiv 3 \pmod 5$, so $(w)$ is 5-regular.
- $\Omega_w(5) = \{0,3\}, \Omega_w(25) = \{0,1,2\}$, and $\Omega_w(5^r) = \{0,1\}$ for all $r \geq 3$, so $(w)$ is 5-stable with $\iota_w(5) = 3 = f(w)$.

Clearly $(w)$ satisfies the conditions of (a) of Theorem 7.5.

**Example 7.7**: Let $p = 5, a = 6, b = 18, w_0 = 1$, and $w_1 = 1$. Then one cycle of $(w)$ modulo $5^3$ is

$$1, 1, 113, 35, 51, 51, 13, 35, 101, 101, 38, 35, 26, 26, 63, 35, 76, 76, 88, 35.$$

The reader may verify that this sequence has the following properties:

- $\lambda_w(5) = \lambda_w(25) = 4$ and $\lambda_w(5^r) = 4 \cdot 5^{r-2}$ for $r > 2$, so $f(w) = 2$.

- $h_w(5^r) = 4$ for all $r \geq 1$, so $e(w) = \infty$ and $(w)$ is degenerate.
- $w_0w_2 - (w_1)^2 \equiv 2 \pmod 5$, so $(w)$ is 5-regular.
- $5^1 \parallel w_3$, so $c = 1$.
- $\Omega_w(5) = \Omega_w(25) = \{0, 1, 2\}$ and $\Omega_w(5^r) = \{0, 1, 2, 5\}$ for all $r \geq 3$, so $(w)$ is 5-stable with $\iota_w(5) = 3 = f(w) + c$.

Clearly $(w)$ satisfies the conditions of (b) of Theorem 7.5.

**Example 7.8**: Let $p = 5, a = 21, b = 147, w_0 = 125$, and $w_1 = 3$. Then one cycle of $(w)$ modulo $5^4$ has 3000 terms. The first 18 of these are

$$125, 3, 438, 7, 136, 577, 250, 431, 426, 589, 372, 604, 500, 462, 577, 453, 319, 108.$$

The reader may verify that this sequence has the following properties:

- $\lambda_w(5^r) = 24 \cdot 5^{r-1}$ for all $r \geq 1$, so $f(w) = 1$.
- $h_w(5^r) = 6$ for all $r \geq 1$, so $e(w) = \infty$ and $(w)$ is degenerate.
- $w_0w_2 - (w_1)^2 \equiv 1 \pmod 5$, so $(w)$ is 5-regular.
- $5^3 \parallel w_0$, so $c = 3$.
- $\Omega_w(5) = \{0, 4, 5\}, \Omega_w(25) = \{0, 5, 20\}, \Omega_w(125) = \{0, 5, 100\}$ and $\Omega_w(5^r) = \{0, 5, 125\}$ for all $r \geq 4$, so $(w)$ is 5-stable with $\iota_w(5) = 4 = f(w) + c$.

Clearly $(w)$ satisfies the conditions of (b) of Theorem 7.5.

**Example 7.9**: Let $p = 5, a = 6, b = 18, w_0 = 0$, and $w_1 = 3$. Then one cycle of $(w)$ modulo $5^3$ is

$$0, 3, 18, 54, 0, 28, 43, 4, 0, 53, 68, 79, 0, 78, 93, 29, 0, 103, 118, 104.$$

The reader may verify that this sequence has the following properties:

- $\lambda_w(5) = \lambda_w(25) = 4$ and $\lambda_w(5^r) = 4 \cdot 5^{r-2}$ for $r > 2$, so $f(w) = 2$.
- $h_w(5^r) = 4$ for all $r \geq 1$, so $e(w) = \infty$ and $(w)$ is degenerate.
- $w_0w_2 - (w_1)^2 \equiv 1 \pmod 5$, so $(w)$ is 5-regular.
- $\nu_w(0, 5) = \nu_w(0, 25) = 1$ and $\nu_w(0, 5^r) = 5^{r-2}$ for all $r > 2$, and therefore $5^{r-2} \in \Omega_w(p^r)$ when $r > 2$, so $(w)$ is not 5-stable.

Clearly $(w)$ satisfies the conditions of (c) of Theorem 7.5.

## 8. ACKNOWLEDGMENTS

Portions of this work were completed while the second author, Walter Carlip, was a Visiting Associate Professor at Loyola University of Chicago. He would like to thank the Loyola Department of Mathematics for their generous support.

## REFERENCES

[1] Walter Carlip and Lawrence 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, pp. 691-719.

[2] Walter Carlip and Lawrence Somer. "Bounds for Frequencies of Residues of Second-Order Recurrences Modulo $p^r$, submitted, 2001.

[3] Eliot T. Jacobson. "Distribution of the Fibonacci Numbers Mod $2^k$." *The Fibonacci Quarterly* **30.3** (1992): 211-215.

[4] Lawrence Somer. *Divisibility of Terms in Lucas Sequences by Their Subscripts.* Applications of Fibonacci Numbers, Volume 5 (St. Andrews, 1992), Kluwer Acad. Publ., Dordrecht, 1993, pp. 515-525.
[5] Lawrence Somer and Walter Carlip. "Stability of Second-Order Recurrences modulo $p^r$." *Int. J. Math. Math. Sci.* **23.4** (2000): 225-241.
[6] M. Ward. "The Arithmetical Theory of Linear Recurring Series." *Trans. Amer. Math. Soc.* **35** (1933): 600-628.
[7] Morgan Ward. "Prime Divisors of Second Order Recurring Sequences." *Duke Math. J.* **21** (1954): 607-614.

AMS Classification Numbers: 11B39, 11A25, 11A51, 11B36

✠ ✠ ✠