BOUNDS FOR FREQUENCIES OF RESIDUES OF SECOND-ORDER RECURRENCES MODULO p^r

Walter Carlip, Lancaster, Lawrence Somer, Washington D.C.

(Received January 10, 2006)

Abstract. The authors examine the frequency distribution of second-order recurrence sequences that are not p-regular, for an odd prime p, and apply their results to compute bounds for the frequencies of p-singular elements of p-regular second-order recurrences modulo powers of the prime p. The authors' results have application to the p-stability of second-order recurrence sequences.

Keywords: Lucas, Fibonacci, stability, uniform distribution, recurrence

MSC 2000: 11B37, 11A25, 11A51, 11B39

1. Introduction

In [9] and [12], H. Niederreiter, A. Schinzel, and L. Somer obtained results concerning the number of times elements of a finite field appear in a shortest period of a second-order linear recurrence over that finite field. One can specialize their results to the residues of a second-order linear recurrence modulo a prime. In [2], we generalized these results to regular second-order recurrences modulo powers of an odd prime. That paper was concerned primarily with *p-regular* second-order recurrences, i.e., recurrences that do not satisfy a recurrence relation of order less than two when reduced modulo p. The analysis in [2] required examination of certain subsequences of the original sequence that arise as columns of a rectangular array constructed from one period of the sequence modulo a power of the prime p. When studying the distribution of p-singular terms (i.e., terms that are divisible by p) of certain classes of p-regular sequences, regularity of these subsequences played an important role in our proofs. In some instances, however, the subsequences that arise fail to be p-regular, and the analysis becomes more complicated. The purpose of this paper, which may be viewed as a continuation of [2], is to analyze the distribution of residues, modulo powers of an odd prime p, of second-order sequences that fail to be p-regular, and to apply this analysis to certain subsequences of p-regular sequences. The results here are critical to complete the analysis of the frequency distribution of the p-singular terms of p-regular sequences, as well as being interesting in their own right. A preliminary version of our main result, Theorem 6.1, was announced, but not proved, in [2] and is applied to the study of sequence stability in [13].

2. Preliminaries and notation

Throughout this paper we are concerned with the distribution, modulo powers of a fixed odd prime p, of second-order recurrence sequences $w(a,b) = (w)$ that satisfy the relation

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

where the parameters a and b and the initial terms w_0 and w_1 are all rational integers. In this section we introduce the basic notation and definitions we require for our study.

2.1. The family $\mathscr{F}(a,b)$. If $w(a,b)$ satisfies (2.1) and $p^m \parallel (w_0, w_1)$ for some $m \geqslant 1$, then it is easy to see that $p^m \parallel (w_n, w_{n+1})$ for all $n \geqslant 0$. It follows that the new sequence (w'), defined by $w'_n = w_n/p^m$, satisfies the same recurrence relation (2.1) and has the property that $p \nmid (w'_0, w'_1)$. Moreover, for any $r \geqslant m$, the frequency distribution of $w(a,b)$ modulo p^r can readily be determined from the frequency distribution of $w'(a,b)$ modulo p^{r-m}. Consequently, we lose no generality by restricting our attention to sequences $w(a,b)$ for which $p \nmid (w_0, w_1)$, and we make the following definition.

Definition 2.1. Denote by $\mathscr{F}(a,b)$ the family of second-order recurrence sequences $w(a,b)$ that satisfy (2.1) and for which $p \nmid (w_0, w_1)$.

In the analysis of distributions of terms of second-order recurrences modulo powers of a prime p, there are significant differences in the behavior of terms that are divisible by p and terms that are relatively prime to p. Following the convention introduced in [2], we refer to terms w_n for which $p \nmid w_n$ as *p-regular* terms and to terms w_n for which $p \mid w_n$ as *p-singular* terms.

2.2. Periods, restricted periods, and multipliers. It is well known that if $p \nmid b$, then each sequence $w(a,b) \in \mathscr{F}(a,b)$ is purely periodic modulo p^r for all $r \geqslant 1$. We assume throughout this paper that $p \nmid b$, and adopt the notation for the *period* and *restricted period* of $w(a,b)$ from [2].

Definition 2.2. The *period* of $w(a,b)$ modulo p^r, denoted $\lambda_w(p^r)$, is the least positive integer λ such that, for all $n \geqslant 0$,

$$w_{n+\lambda} \equiv w_n \pmod{p^r}. \tag{2.2}$$

Any positive integer λ, not necessarily the smallest, that satisfies (2.2) is called a *general period* of $w(a,b)$.

Similarly, the *restricted period* of $w(a,b)$ modulo p^r, denoted $h_w(p^r)$, is the least positive integer h such that, for some integer M and all $n \geqslant 0$,

$$w_{n+h} \equiv M w_n \pmod{p^r}. \tag{2.3}$$

The integer $M = M_w(p^r)$ is called the *multiplier* of $w(a,b)$ modulo p^r, and is defined up to congruence modulo p^r. Again, any positive integer h, not necessarily the smallest, that satisfies (2.3) is called a *general restricted period* and the corresponding integer M a *general multiplier* of $w(a,b)$.

It is well known that $h_w(p^r) \mid \lambda_w(p^r)$ and that the multiplicative order of the multiplier $M_w(p^r)$, modulo p^r, is given by

$$E_w(p^r) = \operatorname{ord}_{p^r}(M_w(p^r)) = \lambda_w(p^r)/h_w(p^r). \tag{2.4}$$

Furthermore, if $M = M_w(p^r)$ and $h = h_w(p^r)$, then, for all nonnegative integers i and n,

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

We also require the notion of the *special restricted period* and *special multiplier* with respect to w_n modulo p^r, introduced in [2].

Definition 2.3. Let $w(a,b) \in \mathscr{F}(a,b)$. The *special restricted period* with respect to w_n modulo p^r, denoted $h_w^*(n,p^r)$, is the smallest restricted period $h^* = h_w(p^c)$ with the property that the subsequence $w_t^* = w_{n+th^*}$ satisfies a first-order recurrence $w_{t+1}^* \equiv M^* w_t \pmod{p^r}$. The integer $M^* = M_w^*(n,p^r)$ is called the *special multiplier* with respect to w_n modulo p^r. We denote by r_n^* the smallest positive integer such that $h_w^*(n,p^r) = h_w(p^{r_n^*})$. Since r_n^* is usually independent of the index n, the subscript is often omitted.

2.3. Frequency distribution functions. Following the notation of [2] we introduce the *(total) frequency distribution function* $\nu(d,p^r)$, the *(ordinary) partial distribution function* $\nu_n(d,p^r)$, and the *(special) partial distribution function* $\nu_n^*(d,p^r)$.

Definition 2.4. Let $w(a,b) \in \mathscr{F}(a,b)$ and, as usual, assume that $p \nmid b$ so that $w(a,b)$ is purely periodic. Set $\lambda = \lambda_w(p^r)$ and $h = h_w(p^r)$. Then we define

$$\nu_w(d,p^r) = \left|\{\, m;\ w_m \equiv d \,(\operatorname{mod} p^r) \text{ and } 0 \leqslant m < \lambda \,\}\right| \quad \text{and}$$
$$\nu_{w,n}(d,p^r) = \left|\{\, m;\ w_m \equiv d \,(\operatorname{mod} p^r),\ m \equiv n \,(\operatorname{mod} h), \text{ and } 0 \leqslant m < \lambda \,\}\right|.$$

When the recurrence $w(a,b)$ is evident, we simplify the notation to $\nu(d,p^r) = \nu_w(d,p^r)$ and $\nu_n(d,p^r) = \nu_{w,n}(d,p^r)$.

Several observations are apropos here. It is evident from (2.4) that a single cycle of the sequence $w(a,b)$ modulo p^r can be written in an $E_w(p^r) \times h_w(p^r)$ array, and the partial frequency $\nu_n(d,p^r)$ represents the number times the residue d occurs in the n^{th} column of the array. It is an easy consequence of these observations that

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

Moreover, we have the following proposition, which appears as Lemma 4.2 in [2].

Proposition 2.5. *Let $w(a,b) \in \mathscr{F}(a,b)$ and suppose that w_n is p-regular. Assume that there exists a nonnegative integer l such that $w_{n+lh} \equiv d \ (\operatorname{mod} p^r)$. Then*

$$\nu_{w,n}(d,p^r) = \frac{\lambda_w(p^r)/h_w(p^r)}{\operatorname{ord}_{p^r}(M_w(p^r))} = 1.$$

The definition of the special partial distribution function $\nu_n^*(d,p^r)$ is similar to that of the partial distribution function $\nu_{w,n}(d,p^r)$, but requires some additional finesse.

Definition 2.6. Let $w(a,b) \in \mathscr{F}(a,b)$ and, as usual, assume that $p \nmid b$ so that $w(a,b)$ is purely periodic. Set $\lambda = \lambda_w(p^r)$ and $h^* = h_w^*(l,p^r)$ for some l such that w_l is p-regular. Then we define

$$\nu_{w,n}^*(d,p^r) = \left|\{\, m;\ w_m \equiv d \,(\operatorname{mod} p^r),\ m \equiv n \,(\operatorname{mod} h^*), \text{ and } 0 \leqslant m < \lambda \,\}\right|.$$

As usual, when the recurrence $w(a,b)$ is evident, we write $\nu_n^*(d,p^r) = \nu_{w,n}^*(d,p^r)$.

Again, a few remarks are in order to justify this definition. First, note that it follows from the definition of $h_w^*(l,p^r)$ that $h_w^*(l,p^r) = h_w(p^c)$ for some integer $c \leqslant r$. Consequently $h_w^*(l,p^r) \mid h_w(p^r)$, and hence $h_w^*(l,p^r) \mid \lambda_w(p^r)$. If we now define

$$E_{w,n}^*(p^r) = \lambda_w(p^r)/h_w^*(l,p^r) = \lambda_w(p^r)/h_w(p^{r_i^*}), \tag{2.6}$$

then we can write a single cycle of the sequence $w(a,b)$ modulo p^r in an $E^*_{w,n}(p^r) \times h_w(p^{r^*_l})$ array. The partial frequency $\nu^*_{w,n}(d,p^r)$ then represents the number of times the residue d occurs in the n^{th} column of the array. As with the ordinary partial distribution function, the total partial distribution function can be written in terms of the special partial distribution function:

$$\nu(d,p^r) = \sum_{n=0}^{h^*_w(l,p^r)-1} \nu^*_n(d,p^r) = \sum_{n=0}^{h_w(p^{r^*_l})-1} \nu^*_n(d,p^r). \tag{2.7}$$

We observe that the definition of $\nu^*_{w,n}(d,p^r)$ appears to depend upon the choice of the integer l. Fortunately, this is not so. In Theorem 3.5 of [2], it is shown for one class of second-order recurrences, the p-regular recurrences, that the special restricted period $h^*_w(l,p^r)$ with respect to a p-regular term w_l is independent of l. In Theorem 4.6, below, we generalize this result to the complementary class of recurrences, the irregular recurrences. Thus, in all cases it is safe to drop the subscript and write $r^*_l = r^*$.

An analogue of Proposition 2.5 holds for the special partial distribution function and is essential in our analysis. We postpone the statement and proof of this analogue to §4.

A key classical result on frequency distributions of second-order recurrence sequences is the characterization of uniformly distributed sequences due to R. T. Bumby [1], and W. A. Webb and C. T. Long [15], which we state only for odd primes.

Theorem 2.7 (Bumby, Webb, and Long). *Let $w(a,b)$ be a second-order recurrence and p an odd prime. If $w(a,b)$ is uniformly distributed modulo p^r, then $\nu_w(d,p^r) = \lambda_w(p^r)/p^r = E(p^r)$ for all d. Moreover, $w(a,b)$ is uniformly distributed modulo p^r if and only if the following conditions are satisfied:*

(a) $p \mid D$;
(b) $p \nmid ab$;
(c) $p \nmid 2w_1 - aw_0$;
(d) *if* $p = 3$ *and* $r \geqslant 2$, *then* $a^2 \not\equiv b \pmod 9$.

If conditions (a)–(d) *hold, then $w(a,b)$ is p-regular, $e = f = 1$, and, for all r, $E(p^r) = E(p)$ and $E(p^r) \mid 2 \cdot \mathrm{ord}_p(b)$.*

Proof. All parts of the theorem are proven in [1] and [15] except for the assertion that $E(p^r) \mid 2 \cdot \mathrm{ord}_p(b)$, which follows from Lemma 4 of [12]. □

2.4. Blocks. It is customary to partition the family $\mathscr{F}(a,b)$ of second-order recurrences into equivalence classes, called p^r*-blocks*, arising from the equivalence relation mot defined as follows.

Definition 2.8. Suppose that $w(a,b)$, $w'(a,b) \in \mathscr{F}(a,b)$. Then $w'(a,b)$ 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,

$$w'_n \equiv c w_{n+m} \pmod{p^r}. \tag{2.8}$$

It is easy to see that mot is an equivalence relation (see, e.g., §2.1 of [2]) and that, if (2.8) occurs, then for all n,

$$\nu_w(w_{n+m}, p^r) = \nu_{w'}(w'_n, p^r). \tag{2.9}$$

In particular, the frequency distribution function of $w'(a,b)$ can be completely determined from that of $w(a,b)$.

It is a consequence of the definition that two sequences that lie in the same p^r-block have identical invariants. Thus, for example, if $w(a,b)$ and $w'(a,b)$ lie in the same p^r-block, then both sequences have the same period, restricted period, and special restricted periods modulo p^r.

2.5. Regular recurrences and blocks. One class of second-order recurrence sequences, the regular recurrence sequences, plays a prominent role in the theory. We define a recurrence (w) satisfying (2.1) to be p-regular if

$$\begin{vmatrix} w_0 & w_1 \\ w_1 & w_2 \end{vmatrix} = w_0 w_2 - w_1^2 \not\equiv 0 \pmod{p}. \tag{2.10}$$

We refer to sequences in the family $\mathscr{F}(a,b)$ that fail to be p-regular, as *p-irregular*, or simply *irregular*, when the prime p is evident.

As we noted in [2], Heymann's theorem [7, Chapter 12.12], implies that

$$\begin{vmatrix} w_n & w_{n+1} \\ w_{n+1} & w_{n+2} \end{vmatrix} = b^n \begin{vmatrix} w_0 & w_1 \\ w_1 & w_2 \end{vmatrix},$$

and hence, if (w') is a mot of (w), then (w') is p-regular if and only if (w) is p-regular. It follows that the sequences in a given block are either all p-regular or all p-irregular, and we are justified in referring to the block as a *p-regular block* or a *p-irregular block*.

We also note that if $w(a,b) \in \mathscr{F}(a,b)$ is p-regular and $w'(a,b) \in \mathscr{F}(a,b)$ is any other recurrence, then Cramer's rule implies that there exist integers c_1 and c_2 such that

$$w'_n \equiv c_1 w_n + c_2 w_{n+1} \pmod{p^r} \tag{2.11}$$

(see, e.g., §2.3 of [2]). It follows that the p-regular recurrences in $\mathscr{F}(a,b)$ have the same period, restricted period, and multiplier modulo p^r. We refer to a parameter that is constant on the set of p-regular sequences in the family $\mathscr{F}(a,b)$ as a *global parameter* of the family. We customarily drop the explicit mention of the sequence in the notation for $\lambda(p^r)$, $h(p^r)$, and $M(p^r)$ when referring to the global parameter.

We frequently use two particular sequences in the family $\mathscr{F}(a,b)$, the *generalized Fibonacci sequence* $u(a,b)$ and the *generalized Lucas sequence* $v(a,b)$, which are determined by their initial terms: $u_0 = 0$, $u_1 = 1$, $v_0 = 2$, and $v_1 = a$. Of particular utility is the fact that $u(a,b)$ is *always* p-regular, and consequently the global parameters λ, h, e, and f may be computed using $u(a,b)$. In particular, $h(p^r) = h_u(p^r)$ and may be characterized as the least integer h such that $p^r \mid u_h$.

2.6. The parameters e and f. The period and restricted period of a p-regular sequence modulo any power of p can be expressed in terms of the period and restricted period modulo p and two fundamental parameters, e and f, associated with the family $\mathscr{F}(a,b)$ and introduced in [2]. In [2], these parameters are discussed only for p-regular sequences, but the concept is a general one.

Definition 2.9. Let $w(a,b) \in \mathscr{F}(a,b)$. We define $e = e(w)$ to be the largest integer, if it exists, such that $h_w(p^e) = h_w(p)$. Similarly, we define $f = f(w)$ to be the largest integer, if it exists, such that $\lambda_w(p^f) = \lambda_w(p)$.

In studying the frequency distribution of a sequence modulo a particular power p^r of the odd prime p, it is often necessary to consider cases that depend upon the relationship of r to both e and f. To simplify the notation in these cases we set

$$e^* = \min(r,e) \quad \text{and} \quad f^* = \min(r,f).$$

The critical result on periods and restricted periods modulo prime powers is the following theorem.

Theorem 2.10. *Suppose that $w(a,b) \in \mathscr{F}(a,b)$ is p-regular and that $e = e(w)$ and $f = f(w)$ both exist. Let $s = \lambda(p)/h(p)$. Then, for all positive integers r,*

$$h(p^r) = p^{r-e^*} h(p^e) \tag{2.12}$$

$$\lambda(p^r) = p^{r-f^*} \lambda(p^f) \quad \textit{and} \tag{2.13}$$

$$E(p^r) = \operatorname{ord}_{p^r}(M(p^r)) = \frac{\lambda(p^r)}{h(p^r)} = \frac{p^{r-f^*}\lambda(p)}{p^{r-e^*}h(p)} = p^{e^*-f^*} s. \tag{2.14}$$

P r o o f. See, e.g., Theorem 2.11 of [2]. □

2.7. Ratios. The ratios of terms of recurrences (w) modulo p^r are closely related to multipliers and play a key role in our study. As usual, we follow the notation and conventions of [2].

If a, b, c, and d are integers, with $p \nmid b$ and $p \nmid d$, then the quotients a/b and c/d may be viewed as elements of $\mathbb{Z}_p$, the localization of the integers at the prime ideal (p). It is then natural to define, for each positive integer r,

$$a/b \equiv c/d \pmod{p^r} \quad \text{if and only if} \quad ad - bc \equiv 0 \pmod{p^r}.$$

In [2], the notation $\varrho_w(n, m)$ was introduced to represent the ratio of elements w_{n+m} and w_n of a second-order recurrence sequence (w) when w_n is p-regular. We extend that notation here to include the situation when the p-power dividing w_n does not exceed the p-power dividing w_{n+m}.

Definition 2.11. If $w(a, b) \in \mathscr{F}(a, b)$ and m and n are nonnegative integers such that $p^k \parallel w_n$ and $p^k \mid w_{n+m}$, then we define $\varrho(n, m) = \varrho_w(n, m)$ to be the element $(w_{n+m}/p^k)/(w_n/p^k) \in \mathbb{Z}_p$.

In this notation it is immediate that if $p^k \parallel w_n$, then

$$w_{n+m} \equiv \varrho(n, m) w_n \pmod{p^{r-k}}.$$

In particular, if w_n is p-regular, then the multiplier and special multiplier modulo p^r can be expressed in terms of ratios:

$$\begin{aligned} M_w(p^r) &\equiv \varrho_w(n, h_w(p^r)) \pmod{p^r}, \\ M_w^*(n, p^r) &\equiv \varrho_w(n, h_w^*(n, p^r)) \pmod{p^r}. \end{aligned}$$

2.8. Quoted results. We require several basic results from [2] concerning second-order recurrences. We list them here for reference.

Proposition 2.12. *Suppose that $w(a, b)$ is p-regular.*
(a) *For all p, $h(p) \mid p - (\frac{D}{p})$.*
(b) *If $p \nmid D$, then $h(p) \mid \frac{1}{2}(p - (\frac{D}{p}))$ if and only if $(\frac{b}{p}) = 1$.*
(c) *If $(\frac{D}{p}) = 1$, then $\lambda(p) \mid p - 1$.*

Proof. Parts (a) and (c) are proven in [3, pp. 44–45] and [6, pp. 290, 296, 297]. Part (b) is proven in [4, p. 441]. $\square$

Proposition 2.13. *Let $w(a,b) \in \mathscr{F}(a,b)$ and fix a positive integer c. Let i and j be two integers such that $i < j$. Let l be the largest integer (possibly zero) such that $h(p^l) \mid c$ and m the largest integer (possibly zero) such that $h_w(p^m) \mid j-i$. Then*

$$w_{i+c}w_j - w_{j+c}w_i \equiv 0 \pmod{p^r}$$

if and only if $l + m \geqslant r$. In particular, if w_i and w_j are p-regular, then $\varrho_w(i,c) \equiv \varrho_w(j,c) \pmod{p^r}$ if and only if $l+m \geqslant r$.

Proof. This is Lemma 3.3 of [2]. □

Proposition 2.14. *Let $w(a,b) \in \mathscr{F}(a,b)$ and $w'(a,b) \in \mathscr{F}(a,b)$ and fix a positive integer c. Let l be the largest integer such that $h(p^l) \mid c$ and assume that $l < r$. If, for integers n and i,*

$$w'_{n+c}w_{n+i} - w_{n+i+c}w'_n \equiv 0 \pmod{p^r}, \tag{2.15}$$

then $w'(a,b)$ is a mot *of $w(a,b)$ modulo p^{r-l}.*

Conversely, if $w'(a,b)$ is a mot *of $w(a,b)$ modulo p^{r-l}, then there exists an i such that* (2.15) *holds for all n.*

Proof. This is Lemma 3.4 of [2]. □

Finally, we need the following result, which determines the number sequences in a p-regular p^r-block of $\mathscr{F}(a,b)$.

Proposition 2.15. *Let $\mathscr{B}$ be a p^r-block of $\mathscr{F}(a,b)$ containing the p-regular sequence $w(a,b)$ and the cycle $S = (w_0, w_1, \ldots, w_{\lambda-1})$. Then the block $\mathscr{B}$ contains $p^{r-1}(p-1)h_w(p^r)$ distinct second-order recurrences and $p^{r-1}(p-1)/E_w(p^r)$ distinct cycles.*

Proof. This is Lemma 2.13 of [2]. □

3. Number theoretic results

In this section we offer several number theoretic results that we require in the proofs below. We begin with two basic propositions from [2].

Proposition 3.1. *Let d be an integer such that $p \nmid d$ and suppose there exists a largest positive integer m such that $\operatorname{ord}_{p^m}(d) = \operatorname{ord}_p(d)$. If $r \geqslant m$, then $\operatorname{ord}_{p^r}(d) = p^{r-m} \operatorname{ord}_{p^m}(d)$.*

Proof. This is Lemma 2.18 of [2]. See also [14, pp. 619–620] and [5] for proofs. $\square$

Proposition 3.2. *Suppose that $r \geqslant 4$ and $\operatorname{ord}_{p^r}(d) = p^n t$, with $n \geqslant 3$ and $t \mid p-1$. Let $c = d^p + ip^{r-1}$. Then $\operatorname{ord}_{p^r}(c) = \operatorname{ord}_{p^r}(d^p) = (1/p)\operatorname{ord}_{p^r}(d)$.*

Proof. This is Lemma 2.19 of [2]. $\square$

We apply Hensel's lemma below, and state here the version we need.

Theorem 3.3 (Hensel's lemma). *Suppose that $f(x)$ is a polynomial with integral coefficients. If $f(m) \equiv 0 \pmod{p^i}$ and $f'(m) \not\equiv 0 \pmod{p}$, then there is a unique t, modulo p, such that $f(m + tp^i) \equiv 0 \pmod{p^{i+1}}$.*

Proof. See Theorem 2.23, p. 87 of [10]. $\square$

Finally, we require an analysis of the multiplicative orders of certain elements of $(\mathbb{Z}/p^{2t}\mathbb{Z})^*$.

Proposition 3.4. *Suppose that t is a positive integer and $M \in (\mathbb{Z}/p^{2t}\mathbb{Z})^*$ satisfies $\operatorname{ord}_{p^t}(M) = s$, where $s \mid p-1$. Let*

$$\Gamma = \{\, k \in \mathbb{Z}/p^{2t}\mathbb{Z};\ k \equiv M \pmod{p^t} \ \text{ and } \ k \not\equiv M \pmod{p^{t+1}} \,\}.$$

Then Γ contains $(p-2)p^{t-1}$ residues k that satisfy $\operatorname{ord}_{p^{2t}}(k) = p^t s$, one residue k that satisfies $\operatorname{ord}_{p^{2t}}(k) = s$ and, for each c such that $1 \leqslant c \leqslant t-1$, $(p-1)p^{c-1}$ residues k that satisfy $\operatorname{ord}_{p^{2t}}(k) = p^c s$.

Proof. Let $f(x) = x^s - 1$. By hypothesis, $f(M) \equiv 0 \pmod{p^t}$ and, clearly, $f'(M) \not\equiv 0 \pmod{p}$, so, by Hensel's lemma (Theorem 3.3), there is a unique residue α_1, modulo p, such that $f(M + \alpha_1 p^t) \equiv 0 \pmod{p^{t+1}}$. Consequently, if ξ is congruent to neither 0 nor α_1, modulo p, then $f(M + \xi p^t) \not\equiv 0 \pmod{p^{t+1}}$. Since it is clear that $f(M + \xi p^t) \equiv 0 \pmod{p^t}$, it follows from Proposition 3.1 that the $p-2$ residues $M + \xi p^t$ have order ps, modulo p^{t+1}. Moreover, Proposition 3.1 now implies that the $(p-2)p^{t-1}$ residues in Γ that reduce to the residues $M + \xi p^t$, modulo p^{t+1}, have order $p^t s$ modulo p^{2t}, as desired.

Suppose that $c = t-1$. Since $f(M + \alpha_1 p^t) \equiv 0 \pmod{p^{t+1}}$, Hensel's lemma implies that there is a unique residue α_2, modulo p, such that $f(M + \alpha_1 p^t + \alpha_2 p^{t+1}) \equiv 0 \pmod{p^{t+2}}$. Now, if ξ is not congruent to α_2 modulo p, then $f(M + \alpha_1 p^t + \xi p^{t+1}) \not\equiv 0$

$\pmod{p^{t+2}}$ and it follows from Proposition 3.1 that the $p-1$ residues $M+\alpha_1 p^t+\xi p^{t+1}$ satisfy $\operatorname{ord}_{p^{t+2}}(M+\alpha_1 p^t+\xi p^{t+1}) = ps$. These residues lift to $(p-1)p^{t-2}$ residues in Γ that have order $p^{t-1}s = p^c s$, modulo p^{2t}.

Clearly, this argument can be repeated for each $c = t-2, t-3, \ldots, 1$ to construct, $(p-1)p^{c-1}$ residues k that satisfy $\operatorname{ord}_{p^{2t}}(k) = p^c s$. Moreover, after the final application of Hensel's lemma, we have constructed an element $M + \alpha_1 p^t + \alpha_2 p^{t+1} + \ldots + \alpha_t p^{2t-1}$ that has order s, as desired. □

4. Irregular recurrences

In order to prove our main theorem, Theorem 6.1, we extend the analysis of p-regular sequences in [2] to second-order recurrences that fail to be p-regular. The main distinguishing characteristic of p-irregular second-order recurrences is that they satisfy a first-order recurrence relation modulo p.

Theorem 4.1. *Let $w(a,b)$ be a second-order recurrence and $f(x) = x^2 - ax + b$ its characteristic polynomial. Then $w(a,b)$ is not p-regular if and only if there exists an integer α with the property that $f(\alpha) \equiv 0 \pmod{p}$ and, for all $n \geqslant 0$,*

$$w_n \equiv w_0 \alpha^n \pmod{p}. \tag{4.1}$$

Proof. Clearly, if (4.1) is true, then $w_0 w_2 - w_1^2 \equiv w_0^2\alpha^2 - w_0^2\alpha^2 \equiv 0 \pmod{p}$, and hence $w(a,b)$ is not p-regular.

Conversely, suppose that $w(a,b)$ is not p-regular. By (2.10), $w_0 \equiv 0 \pmod{p}$ if and only if $w_1 \equiv 0 \pmod{p}$, and (4.1) is trivial. Suppose that $w_0 \not\equiv 0 \pmod{p}$. Then w_0 is invertible, modulo p, and we can find an integer α such that $\alpha \equiv w_1 w_0^{-1} \pmod{p}$. It follows that $w_1 \equiv \alpha w_0 \pmod{p}$ and, since $w(a,b)$ is not p-regular,

$$w_2 \equiv w_1^2 w_0^{-1} \equiv \alpha w_1 \equiv \alpha^2 w_0 \pmod{p}.$$

Equation (4.1) now follows by induction. Finally, we must verify that $f(\alpha) \equiv 0 \pmod{p}$. Since w_0 is invertible modulo p,

$$\begin{aligned}
\alpha^2 - a\alpha + b &\equiv w_2 w_0^{-1} - a w_1 w_0^{-1} + b \pmod{p}\\
&\equiv (a w_1 - b w_0) w_0^{-1} - a w_1 w_0^{-1} + b \pmod{p}\\
&\equiv 0 \pmod{p},
\end{aligned}$$

as desired. □

Corollary 4.2. *If $w(a,b) \in \mathscr{F}(a,b)$ is not p-regular, then every element w_n of the sequence $w(a,b)$ is p-regular.*

P r o o f. Let $n \geqslant 0$. By Theorem 4.1, $w_n \equiv w_0\alpha^n \pmod{p}$. Since $w(a,b) \in \mathscr{F}(a,b)$, we know that $w_0 \not\equiv 0 \pmod{p}$, and since $\alpha \in (\mathbb{Z}/p\mathbb{Z})^*$, it follows that $\alpha^n \not\equiv 0 \pmod{p}$. Therefore, $w_n \not\equiv 0 \pmod{p}$, as desired. □

Irregular sequences differ from regular sequences in another important way. As mentioned above, certain parameters, such as the period, $\lambda(p^r)$, and the restricted period, $h(p^r)$, are identified as global parameters, because they are identical for all p-regular sequences in the family $\mathscr{F}(a,b)$. It is common, however, for these parameters to take on *different* values for irregular sequences. Thus each irregular sequence $w(a,b)$ has, in essence, two copies of each parameter associated with it, e.g., its own period, $\lambda_w(p^r)$, and the global period parameter, $\lambda(p^r) = \lambda_u(p^r)$. In fact, $\lambda_u(p^r)$ is a general period of $w(a,b)$. Some care must be taken to avoid confusing the two parameters when dealing with irregular sequences. In the next propositions we consider the ramifications of this observation for the parameters e, f, λ, and h.

For the remainder of this section, we apply the following general hypothesis.

Hypothesis 4.3. *Suppose that $w(a,b) \in \mathscr{F}(a,b)$ is p-irregular and $r \geqslant 1$. Fix the following notation:*

$$\begin{aligned} \lambda = \lambda(p^r) &= \lambda_u(p^r), & \lambda' &= \lambda'(p^r) = \lambda_w(p^r), \\ h = h(p^r) &= h_u(p^r), & h' &= h'(p^r) = h_w(p^r), \\ f &= f(u), & f' &= f(w), \\ e &= e(u), & e' &= e(w). \end{aligned}$$

As observed in [2], λ, h, e and f are global parameters, so they attain the same values for all p-regular sequences $w(a,b)$. However, for p-irregular sequences these values may differ, and, in fact, have a somewhat different interpretation and significance. We begin with a general observation about the relationship between h and h' and between λ and λ'.

Proposition 4.4. *Assume Hypothesis 4.3. Then $\lambda'(p^r) \mid \lambda(p^r)$ and $h'(p^r) \mid h(p^r)$.*

P r o o f. It is an immediate consequence of (2.11), with $u(a,b)$ in place of $w(a,b)$ and $w(a,b)$ in place of $w'(a,b)$, that $\lambda_u(p^r)$ is a general period of $w(a,b)$. Therefore $\lambda_w(p^r) \mid \lambda_u(p^r)$. Similarly, $h_u(p^r)$ is a general restricted period of $w(a,b)$, and hence $h_w(p^r) \mid h_u(p^r)$. □

Next, we take up the restricted period $h'(p^r) = h_w(p^r)$ and the parameter $e' = e(w)$ for an irregular sequence. If $w(a,b)$ is not p-regular, then Theorem 4.1 implies that $h'(p) = 1$. It follows that $h'(p^r) = 1$ if and only if $1 \leqslant r \leqslant e'$, and therefore e' represents the highest power of p modulo which $w(a,b)$ satisfies a first-order recurrence. The following theorem completely identifies the restricted periods of irregular second-order recurrences and is an analogue for irregular recurrences of the first part of Theorem 2.10.

Theorem 4.5. *Assume Hypothesis* 4.3. *Let* $\hat{r} = \max(r - e', 0)$. *Then*

$$h'(p^r) = h_w(p^r) = h(p^{\hat{r}}) = \begin{cases} 1 & \text{if } r \leqslant e', \\ h(p^{r-e'}) = h(p^e) = h(p) & \text{if } e' < r < e' + e, \\ h(p^{r-e'}) = p^{r-e-e'} h(p) & \text{if } e' + e \leqslant r. \end{cases}$$

Remark. If $w(a,b)$ is p-regular, then Theorem 4.5 reduces to (2.12) by setting $e' = 0$.

Proof. The fact that $h'(p^r) = 1$ if and only if $r \leqslant e'$ follows immediately from Theorem 4.1 and the definition of e'.

To prove the rest of the theorem, we suppose that $r > e'$, and apply Proposition 2.13.

First note that by Corollary 4.2, w_i is p-regular for every i. Moreover, since h' is the least integer such that $w_{i+h'} \equiv M w_i \pmod{p^r}$ for all i and constant multiplier M, it is also the least integer such that

$$\varrho_w(i, h') \equiv \varrho_w(i+1, h') \pmod{p^r}$$

for all i.

Let $c = h(p^{r-e'}) = h(p^{\hat{r}})$ and let l be the largest integer such that $h(p^l) \mid c$. By (2.12), it is clear that $l = \max(\hat{r}, e)$. Furthermore, as observed above, e' is the largest integer such that $h'(p^{e'}) \mid (i+1) - i$. Consequently, by Proposition 2.13,

$$\varrho_{w'}(i, c) \equiv \varrho_{w'}(i+1, c) \pmod{p^r} \tag{4.2}$$

if and only if $r \leqslant l + e'$. In particular, if $r - e' < e$, then (4.2) holds if and only if $r < e + e'$, and if $r - e' \geqslant e$, then (4.2) holds for all r.

Now, suppose that $c < h(p^{r-e'})$, and again let l be the largest integer such that $h(p^l) \mid c$. This time (2.12) implies that $l = 0$ when $r - e' \leqslant e$, and $l < r - e'$ when $r - e' > e$. By Proposition 2.13, we conclude that (4.2) is true if and only if $r \leqslant l + e'$. Thus, if $r - e' \leqslant e$, then (4.2) holds if and only if $r \leqslant e'$. But we have assumed that

$r > e'$, so, in fact, (4.2) never holds. Similarly, if $r - e' > e$, then (4.2) holds if and only if $r \leqslant l + e' < r - e' + e' = r$. Again, (4.2) never holds.

We can now conclude that $c = h(p^{\hat{r}})$ is the smallest integer such that (4.2) holds, and therefore $h'(p^r) = h(p^{\hat{r}})$. The remaining conclusions of the theorem now follow from (2.12). □

We can apply a similar argument to compute the *special* restricted periods $h^*_w(n, p^r)$ for an irregular recurrence $w(a, b)$ in the family $\mathscr{F}(a, b)$.

Theorem 4.6. *Assume Hypothesis* 4.3. *Let* $r^* = \max(\lceil \frac{1}{2}(r - e') \rceil, 0)$. *Then*

$$h^*_w(n, p^r) = h(p^{r^*}) = \begin{cases} 1 & \text{if } r \leqslant e', \\ h(p^e) = h(p) & \text{if } e' < r \leqslant 2e + e', \\ p^{r^* - e} h(p) & \text{if } 2e + e' < r. \end{cases}$$

Remark. If $w(a, b)$ is p-regular, then Theorem 4.6 reduces to Theorem 3.5 of [2] by setting $e' = 0$.

Proof. The fact that $h^*_w(n, p^r) = 1$ when $1 \leqslant r \leqslant e'$ follows immediately from Theorem 4.1 and the definitions of the special restricted period $h^*_w(n, p^r)$ and of e'.

Suppose now that $r > e'$. Choose an integer l such that $e' + e \leqslant l$ and set $m = h'(p^l)$. Let $w^*_t = w_{n+tm}$. We wish to determine the smallest value of l for which the sequence (w^*) satisfies a first-order recurrence modulo p^r.

Since, by Corollary 4.2, each element of the sequence $w(a, b)$ is p-regular, all element ratios exist and, for each t,

$$w^*_{t+1} \equiv \varrho_w(n + tm, m) w^*_t \pmod{p^r}.$$

Therefore (w^*) satisfies a first-order recurrence modulo p^r if and only if

$$\varrho_w(n + tm, m) \equiv \varrho_w(n + (t + 1)m, m) \pmod{p^r} \tag{4.3}$$

for all t.

We apply Proposition 2.13 with $c = m$, $i = n + tm$, and $j = n + (t + 1)m$. Clearly, $j - i = m$. Since $l \geqslant e + e'$, Theorem 4.5 implies that

$$h'(p^l) = h(p^{l-e'}) = p^{l-e-e'} h(p).$$

Moreover, Theorem 4.5 shows that l is the largest integer such that $h'(p^l) \mid j - i$, and also that $l - e'$ is the largest integer such that $h(p^{l-e'}) \mid m$.

Proposition 2.13 now implies that (4.3) holds if and only if $l + l - e' \geqslant r$, i.e., if $l \geqslant \frac{1}{2}(r + e')$. Thus, the smallest value of l for which (w^*) satisfies a first-order recurrence modulo p^r is $l = \lceil \frac{1}{2}(r + e') \rceil$. By Theorem 4.5, the special restricted period is

$$h_w^*(n, p^r) = h'(p^{\lceil (r+e')/2 \rceil}) = h(p^{\lceil (r+e')/2 \rceil - e'}) = h(p^{\lceil (r-e')/2 \rceil}) = h(p^{r^*}),$$

as desired. The final conclusion now follows from (2.12) and the observation that $r^* \leqslant e$ if and only if $r \leqslant 2e + e'$. □

Next we offer the promised analogue of Proposition 2.5 for the special partial distribution function.

Proposition 4.7. *Assume Hypothesis* 4.3. *Let* $h^* = h_w^*(n, p^r)$, *and suppose that there exists a nonnegative integer* l *such that* $w_{n+lh^*} \equiv d \pmod{p^r}$. *Define* r^* *by*

$$r^* = \max(\lceil \tfrac{1}{2}(r - e') \rceil, 0).$$

Then

$$\nu_{w,n}^*(d, p^r) = \frac{\lambda_w(p^r)/h_w(p^{r^*})}{\operatorname{ord}_{p^r}(\varrho_w(n, h^*))} = \frac{\lambda_w(p^r)/h_w(p^{r^*})}{\operatorname{ord}_{p^r}(M_w^*(n, p^r))}. \tag{4.4}$$

P r o o f. Theorem 4.6 shows that the special restricted period $h_w^*(n, p^r)$ is independent of n and

$$h_w^*(n, p^r) = h(p^{r^*}).$$

Therefore, by the definition of $\nu_{w,n}^*(d, p^r)$, we must count the number of indices i such that $w_{n+ih^*} \equiv d \pmod{p^r}$ and $0 \leqslant i < \lambda_w(p^r)/h_w^*(n, p^r) = E_{w,n}^*(p^r)$.

By Corollary 4.2, every element of $w(a, b)$ is p-regular, and hence all element ratios are well defined. By (2.5), for all i,

$$w_{n+ih^*} \equiv \varrho_w(n, h^*)^i w_n \pmod{p^r}. \tag{4.5}$$

In particular,

$$\varrho_w(n, h^*)^l w_n \equiv d \pmod{p^r}.$$

Moreover, if $t = \operatorname{ord}_{p^r}(\varrho_w(n, h^*))$, then (4.5) implies that $w_{n+ih^*} \equiv w_{n+lh^*} \pmod{p^r}$ if and only if $i \equiv l \pmod{t}$. On the other hand,

$$w_n \equiv w_{n+\lambda_w(p^r)} \equiv w_{n+E_{w,n}^*(p^r)h^*} \equiv \varrho_w(n, h^*)^{E_{w,n}^*(p^r)} w_n \pmod{p^r},$$

so $t \mid E_{w,n}^*(p^r)$. It follows that the number of indices i such that $w_{n+ih^*} \equiv d \pmod{p^r}$ and $0 \leqslant i < E_{w,n}^*(p^r)$ is exactly $E_{w,n}^*(p^r)/t = E_{w,n}^*(p^r)/\operatorname{ord}_{p^r}(\varrho_w(n, h^*))$, and the first equality follows. The remainder of the proposition follows from the observation that $\varrho_w(n, h^*) \equiv M_w^*(n, p^r) \pmod{p^r}$. □

We require the following proposition, which is an analogue for p-irregular sequences of Lemma 3.7 of [2].

Proposition 4.8. *Assume Hypothesis* 4.3. *If* $r \geqslant e + e'$, *then for some integer* k,

$$\begin{aligned}(4.6)\qquad \varrho_w(n, h'(p^{r+1})) &= \varrho_w(n, ph'(p^r)) \\ &\equiv (\varrho_w(n, h'(p^r)))^p (\operatorname{mod} p^{2r-e'+1})\end{aligned}$$

$$\begin{aligned}(4.7)\qquad \varrho_w(n, h'(p^{r+1})) &= \varrho_w(n, ph'(p^r)) \\ &\equiv (\varrho_w(n, h'(p^r)))^p + kp^{2r-e'+1} (\operatorname{mod} p^{2r-e'+2}).\end{aligned}$$

P r o o f. Since $r \geqslant e + e'$, Theorem 4.5 implies that $h'(p^{r+1}) = ph'(p^r)$ and the first equalities in (4.6) and (4.7) follow immediately. From the definition of $\varrho_w(n, ph'(p^r))$ it is clear that

$$\begin{aligned}(4.8)\qquad \varrho_w(n, ph'(p^r)) &= \varrho_w(n, h'(p^r))\varrho_w(n + h'(p^r), h'(p^r)) \\ &\times \varrho_w(n + 2h'(p^r), h'(p^r)) \ldots \varrho_w(n + (p-1)h'(p^r), h'(p^r)).\end{aligned}$$

□

We apply Proposition 2.13, with $c = h'(p^r)$, and $ih'(p^r)$ and $jh'(p^r)$ in place of i and j for $0 \leqslant i < j < p$. Since $r \geqslant e + e'$, Theorem 4.5 implies that that $r - e'$ is the largest integer such that $h(p^{r-e'}) \mid h'(p^r)$ and r is the largest integer such that $h'(p^r) \mid (j-i)h'(p^r)$. Consequently, Proposition 2.13 implies, for $0 \leqslant i < p$, that the ratios $\varrho_w(n + ih'(p^r), h'(p^r))$ are all equivalent modulo $p^{2r-e'}$ and distinct modulo $p^{2r-e'+1}$. It follows that we can find a complete residue system $k_0, k_1, \ldots, k_{p-1}$, modulo p, with the property that, for each i,

$$(4.9)\qquad \varrho_w(n + ih'(p^r), h'(p^r)) \equiv \varrho_w(n, h'(p^r)) + k_i p^{2r-e'} \ (\operatorname{mod} p^{2r-e'+1}).$$

Since $k_0 + k_1 + \ldots + k_{p-1} \equiv 0 + 1 + \ldots + (p-1) \equiv 0 \ (\operatorname{mod} p)$ and $p^{2r-e'+1} \mid (p^{2r-e'})^i$ for $i \geqslant 2$, (4.8) and (4.9) imply that

$$\begin{aligned}\varrho_w(n, ph'(p^r)) &\equiv (\varrho_w(n, h'(p^r)) + k_0 p^{2r-e'})(\varrho_w(n, h'(p^r)) + k_1 p^{2r-e'}) \\ &\qquad \ldots (\varrho_w(n, h'(p^r)) + k_{p-1} p^{2r-e'}) \\ &\equiv (\varrho_w(n, h'(p^r)))^p + \varrho_w(n, h'(p^r))^{p-1}(k_0 + k_1 + \ldots + k_{p-1})p^{2r-e'} \\ &\equiv (\varrho_w(n, h'(p^r)))^p \ (\operatorname{mod} p^{2r-e'+1}),\end{aligned}$$

as desired. This proves (4.6), and (4.7) follows immediately. □

In §5 we require a slight generalization of Proposition 4.8 for sequences with the special property that $e = 1$ and $h(p^e) = h(p) = p$. With these additional hypotheses, Proposition 4.8 can be extended to include all $r \geqslant e'$.

Proposition 4.9. *Assume Hypothesis* 4.3 *and suppose that* $e = 1$ *and* $h(p^e) = h(p) = p$. *Then for each* $r \geqslant e'$, *there exists an integer* k *such that* (4.6) *and* (4.7) *are true. In particular,*

$$\varrho_w(n, h'(p^{e'+1})) = \varrho_w(n,p) \equiv (\varrho_w(n,1))^p \pmod{p^{e'+1}}, \tag{4.10}$$

$$\varrho_w(n, h'(p^{e'+1})) = \varrho_w(n,p) \equiv (\varrho_w(n,1))^p + kp^{e'+1} \pmod{p^{e'+2}}, \tag{4.11}$$

and for all $l \geqslant 1$,

$$\varrho_w(n, h'(p^{e'+l})) = \varrho_w(n,p^l) \equiv (\varrho_w(n,p^{l-1}))^p \pmod{p^{e'+2l-1}}. \tag{4.12}$$

Proof. Since $e = 1$, if $r \geqslant e' + 1$ the result is simply that of Proposition 4.8. Therefore, we must only prove the result for $r = e'$. Since Theorem 4.5 implies that $h'(p^{e'+1}) = h(p) = p = ph'(p^{e'})$, (4.6) and (4.7) simplify to (4.10) and (4.11) when $r = e'$. Furthermore, the first equalities in (4.10) and (4.11) follow immediately. With the additional hypotheses of this proposition and taking $r = e'$, (4.8) now becomes

$$\varrho_w(n,p) = \varrho_w(n,1)\varrho_w(n+1,1)\varrho_w(n+2,1)\ldots\varrho_w(n+(p-1),1). \tag{4.13}$$

Again we apply Proposition 2.13, this time with $c = 1$, and with $0 \leqslant i \leqslant j < p$ as in the proof of Proposition 4.8. Clearly 0 is the largest integer such that $h(p^0) \mid 1$ and e' is the largest integer such that $h'(p^{e'}) \mid (j-i)$. Thus Proposition 2.13 implies that the ratios $\varrho_w(n+i,1)$, for $0 \leqslant i < p$, are congruent modulo $p^{e'}$ and distinct modulo $p^{e'+1}$. Once again we can find a complete residue system $k_0, k_1, \ldots, k_{p-1}$ modulo p such that, for each i,

$$\varrho_w((n+i),1) \equiv \varrho_w(n,1) + k_i p^{e'} \pmod{p^{e'+1}}, \tag{4.14}$$

and we obtain

$$\begin{aligned}\varrho_w(n,p) &\equiv (\varrho_w(n,1) + k_0p^{e'})(\varrho_w(n,1) + k_1p^{e'})\ldots(\varrho_w(n,1) + k_{p-1}p^{e'})\\ &\equiv (\varrho_w(n,1))^p + \varrho_w(n,1)^{p-1}(k_0 + k_1 + \ldots + k_{p-1})p^{e'}\\ &\equiv (\varrho_w(n,1))^p \pmod{p^{e'+1}},\end{aligned}$$

as desired. This proves (4.10), and (4.11) follows immediately. The final observation, (4.12), follows from (4.6) with $e' + l$ in place of $r + 1$. □

The next two propositions concern the orders of the special multipliers $M^*_w(n,p^r)$ and are used to evaluate (4.4) for particular sequences.

Proposition 4.10. *Assume Hypothesis* 4.3. *Suppose* $\operatorname{ord}_{p^{2e+e'}}(\varrho_w(n,h(p^e))) = p^c s$, *where* $p \nmid s$ *and* $1 \leqslant c < 2e+e'$. *Then*

$$\operatorname{ord}_{p^r}(M_w^*(n,p^r)) = \begin{cases} s & \text{if } e' < r \leqslant 2e+e'-c, \\ p^{r-(2e+e'-c)}s & \text{if } 2e+e'-c < r \leqslant 2e+e', \\ p^{c+\lfloor (r-(2e+e'))/2 \rfloor} s & \text{if } 2e+e' < r. \end{cases}$$

Proof. Suppose that $e' < r \leqslant 2e+e'$. Then Theorem 4.6 implies that $h_w^*(n,p^r) = h(p^{r^*}) = h(p^e)$, and Proposition 3.1 yields

$$\begin{aligned} \operatorname{ord}_{p^r}(M_w^*(n,p^r)) &= \operatorname{ord}_{p^r}(\varrho_w(n,h(p^{r^*}))) \\ &= \begin{cases} s & \text{if } e' < r \leqslant 2e+e'-c, \\ p^{r-(2e+e'-c)}s & \text{if } 2e+e'-c < r \leqslant 2e+e'. \end{cases} \end{aligned}$$

Suppose that $r = 2e+e'+1$. Then $r^* = \max(\lceil \frac{1}{2}(2e+1) \rceil, 0) = e+1$. Therefore Theorem 4.5, Theorem 4.6, and Proposition 4.8 yield

$$\begin{aligned} \operatorname{ord}_{p^r}(M_w^*(n,p^r)) &= \operatorname{ord}_{p^{2e+e'+1}}(\varrho_w(n,h(p^{r^*}))) \\ &= \operatorname{ord}_{p^{2e+e'+1}}(\varrho_w(n,h'(p^{r^*+e'}))) \\ &= \operatorname{ord}_{p^{2e+e'+1}}(\varrho_w(n,h'(p^{e+e'+1}))) \\ &= \operatorname{ord}_{p^{2e+e'+1}}(\varrho_w(n,h'(p^{e+e'}))^p) \\ &= \operatorname{ord}_{p^{2e+e'}}(\varrho_w(n,h'(p^{e+e'}))) \\ &= p^c s. \end{aligned}$$

Now, suppose that $r = 2e+e'+2$. Then $r^* = \max(\frac{1}{2}(2e+2), 0) = e+1$. Therefore Theorem 4.5, Theorem 4.6, Proposition 4.8, and Proposition 3.2 yield

$$\begin{aligned} \operatorname{ord}_{p^r}(M_w^*(n,p^r)) &= \operatorname{ord}_{p^{2e+e'+2}}(\varrho_w(n,h(p^{r^*}))) \\ &= \operatorname{ord}_{p^{2e+e'+2}}(\varrho_w(n,h'(p^{r^*+e'}))) \\ &= \operatorname{ord}_{p^{2e+e'+2}}(\varrho_w(n,h'(p^{e+e'+1}))) \\ &= \operatorname{ord}_{p^{2e+e'+2}}(\varrho_w(n,h'(p^{e+e'}))^p + kp^{2e+e'+1}) \\ &= (1/p)\operatorname{ord}_{p^{2e+e'+2}}(\varrho_w(n,h'(p^{e+e'}))) \\ &= p^{c+1}s. \end{aligned}$$

The proposition may now be completed by induction. $\square$

Once again, we need a slight generalization for the case that $e = 1$ and $h(p^e) = h(p) = p$.

Proposition 4.11. *Assume Hypothesis* 4.3 *and suppose that* $e = 1$ *and* $h(p^e) = p$. *Suppose that* $\operatorname{ord}_{p^{e'}}(\varrho_w(n,1)) = p^c s$, *where* $p \nmid s$ *and* $1 \leqslant c < e'$. *Then*

$$\operatorname{ord}_{p^r}(M_w^*(n,p^r)) = \begin{cases} s & \text{if } 1 \leqslant r \leqslant e' - c, \\ p^{r-(e'-c)} s & \text{if } e' - c < r \leqslant e', \\ p^{c + \lfloor (r-e')/2 \rfloor} s & \text{if } e' < r. \end{cases}$$

Proof. Suppose that $r \leqslant e'$. Then Proposition 3.1 implies that

$$\operatorname{ord}_{p^r}(M_w^*(n,p^r)) = \operatorname{ord}_{p^r}(\varrho_w(n,1)) = \begin{cases} s & \text{if } r \leqslant e' - c, \\ p^{r-(e'-c)} s & \text{if } e' - c < r \leqslant e'. \end{cases}$$

Suppose that $r = e' + 1$. Then $r^* = \max(\lceil \frac{1}{2} \rceil, 0) = 1$, and Proposition 4.9 yields

$$\begin{aligned} \operatorname{ord}_{p^r}(M_w^*(n,p^r)) &= \operatorname{ord}_{p^{e'+1}}(\varrho_w(n,h(p))) \\ &= \operatorname{ord}_{p^{e'+1}}(\varrho_w(n,p)) \\ &= \operatorname{ord}_{p^{e'+1}}(\varrho_w(n,1)^p) \\ &= p^c s. \end{aligned} \tag{4.15}$$

Now, suppose that $r = e'+2$. Then $r^* = \max(\frac{2}{2}, 0) = 1$. Therefore Proposition 4.9 and Proposition 3.2 imply that

$$\begin{aligned} \operatorname{ord}_{p^r}(M_w^*(n,p^r)) &= \operatorname{ord}_{p^{e'+2}}(\varrho_w(n,h(p))) \\ &= \operatorname{ord}_{p^{e'+2}}(\varrho_w(n,p)) \\ &= \operatorname{ord}_{p^{e'+2}}(\varrho_w(n,1)^p + kp^{e'+1}) \\ &= (1/p)\operatorname{ord}_{p^{e'+2}}(\varrho_w(n,1)) \\ &= p^{c+1} s. \end{aligned}$$

The proposition can be completed by using Proposition 4.10 with $c + 1$ in place of c. □

In our analysis, we also require the following two propositions concerning the orders of element ratios under the special hypotheses that $e = 1$ and $h(p^e) = h(p) = p$.

Proposition 4.12. *Assume Hypothesis* 4.3 *and suppose that* $e = 1$ *and* $h(p^e) = p$. *Suppose that* $\operatorname{ord}_{p^{e'}}(\varrho_w(n,1)) = p^c s$, *where* $p \nmid s$ *and* $1 \leqslant c < e'$, *and let* $l \geqslant 0$. *Then*

$$\operatorname{ord}_{p^r}(\varrho_w(n, h'(p^{l+e'}))) = \begin{cases} s & \text{if } r \leqslant l - c + e', \\ p^{c+r-e'-l} s & \text{if } l - c + e' < r. \end{cases}$$

Proof. We first show, by induction on l, that

$$\operatorname{ord}_{p^{l+e'}}(\varrho_w(n, h'(p^{l+e'}))) = p^c s. \tag{4.16}$$

If $l = 0$, then $h'(p^{l+e'}) = h'(p^{e'}) = h'(p) = 1$, and (4.16) reduces to the hypothesis. If $l = 1$, the result follows from (4.10), as shown in (4.15). By way of induction, assume that (4.16) is true for some $l \geqslant 0$. Then, by Proposition 4.9 and Proposition 3.1,

$$\begin{aligned} \operatorname{ord}_{p^{l+1+e'}}(\varrho_w(n, h'(p^{l+e'+1}))) &= \operatorname{ord}_{p^{l+1+e'}}(\varrho_w(n, h'(p^{l+e'}))^p) \\ &= p \operatorname{ord}_{p^{l+e'}}(\varrho_w(n, h'(p^{l+e'}))^p) \\ &= p^c s, \end{aligned}$$

as desired. By induction, we now conclude that (4.16) is true for all $l \geqslant 0$.

The remainder of the theorem now follows from Proposition 3.1. □

Proposition 4.13. *Assume Hypothesis* 4.3 *and suppose that* $e = 1$ *and* $h(p^e) = p$. *Assume as well that* $\operatorname{ord}_{p^{e'}}(\varrho_w(n,1)) = p^c s$, *where* $p \nmid s$ *and* $1 \leqslant c < e'$. *Let* $h^* = h^*_w(n, p^r)$ *and suppose that* $0 \leqslant n < k < h^*$ *and* $p^l \parallel (k-n)$. *Write* $k - n = p^l t$. *Then*

$$\operatorname{ord}_{p^r}(\varrho_w(n, k-n))) = \begin{cases} \gcd(s,t) & \text{if } r \leqslant l - c + e' \\ p^{c+r-e'-l} \gcd(s,t) & \text{if } l - c + e' < r < l + e'. \end{cases}$$

Proof. By Proposition 4.12, Theorem 2.10, and the hypotheses,

$$h'(p^{l+e'}) = h(p^l) = p^{l-e} h(p) = p^{l-1} p = p^l.$$

It follows that $(k-n) = th'(p^{l+e'})$, and therefore $\varrho_w(n, k-n) = \varrho_w(n, th'(p^{l+e'})) \equiv \varrho_w(n, h'(p^{l+e'}))^t \pmod{p^{l+e'}}$. It follows that

$$\operatorname{ord}_{p^r}(\varrho_w(n, k-n))) = \gcd(\operatorname{ord}_{p^r}(\varrho_w(n, h'(p^{l+e'}))), t),$$

and the proposition now follows from Proposition 4.12. □

The final two propositions of this section are used to show, in certain instances, that only one of the terms in the summation (2.7), which we use to compute residue frequencies, is nonzero.

Proposition 4.14. *Assume Hypothesis* 4.3 *and suppose that* $e = 1$ *and* $h(p^e) = p$. *Assume as well that* $\operatorname{ord}_{p^{e'}}(\varrho_w(n, 1)) = p^c s$, *where* $p \nmid s$ *and* $1 \leqslant c < e'$. *Let* $h^* = h_w^*(n, p^r)$ *and suppose that* $0 \leqslant n < k < h^*$ *and* $0 \leqslant i \leqslant j < E_{w,n}^*(p^r)$. *If* $r \geqslant e'$ *then*

$$w_{n+ih^*} \not\equiv w_{k+jh^*} \pmod{p^r}.$$

Proof. Suppose otherwise. Then

$$w_{n+ih^*} \equiv w_{k+jh^*} \pmod{p^r}.$$

From the definitions of $M_w^*(n, p^r)$ and $M_w^*(k, p^r)$, we know that

$$\begin{aligned} w_{n+ih^*} &\equiv (M_w^*(n, p^r))^i w_n \pmod{p^r}, \\ w_{k+jh^*} &\equiv (M_w^*(k, p^r))^j w_k \pmod{p^r}, \end{aligned}$$

and hence

$$(M_w^*(n, p^r))^i w_n \equiv (M_w^*(k, p^r))^j w_k \pmod{p^r}.$$

It follows that

$$\varrho_w(n, k-n)(M_w^*(n, p^r))^i \equiv (M_w^*(k, p^r))^j \pmod{p^r}. \tag{4.17}$$

To obtain a contradiction we now apply Proposition 4.11 and Proposition 4.13 to compute the orders of $M_w^*(n, p^r)$, $M_w^*(k, p^r)$, and $\varrho_w(n, k-n)$.

By Proposition 4.11,

$$\operatorname{ord}_{p^r}(M_w^*(n, p^r)) = \operatorname{ord}_{p^r}(M_w^*(k, p^r)) = p^{c+\lfloor (r-e')/2 \rfloor} s.$$

If we set $p^l \parallel k - n$, then, since $1 \leqslant k - n < h^*$, Theorem 4.6 and the hypotheses imply that

$$0 \leqslant l < r^* = \lceil \tfrac{1}{2}(r - e') \rceil.$$

Moreover, by Proposition 4.13,

$$\operatorname{ord}_{p^r}(\varrho_w(n, k-n)) = p^{c+r-e'-l} t,$$

for some integer t such that $p \nmid t$.

By raising both sides of (4.17) to the power $p^{c+\lfloor (r-e')/2 \rfloor} s$, we obtain

$$\varrho_w(n, k-n)^{p^{c+\lfloor (r-e')/2 \rfloor} s} \equiv 1 \pmod{p^r},$$

and therefore $p^{c+r-e'-l} \mid p^{c+\lfloor (r-e')/2 \rfloor}$. But $c + r - e' - l > c + r - e' - \lceil \frac{1}{2}(r - e') \rceil = c + \lfloor \frac{1}{2}(r - e') \rfloor$, a contradiction. □

Proposition 4.15. *Assume Hypothesis* 4.3 *and suppose that* $e = 1$ *and* $h(p^e) = p$. *Assume as well that* $\operatorname{ord}_{p^{e'}}(\varrho_w(n,1)) = p^c s$, *where* $p \nmid s$ *and* $1 \leqslant c < e'$. *Suppose that* $r \geqslant e'$ *and set* $h^* = h^*_w(l, p^r))$, *for some* $l \geqslant 0$.

If $\nu(d, p^r) \neq 0$, *then there is a unique index* n, *with* $0 \leqslant n < h^*$, *for which* $\nu^*_n(d, p^r) \neq 0$. *In particular, the summation* (2.7) *has at most a single nonzero term.*

Proof. Suppose otherwise. Then there exist integers n and k such that $0 \leqslant n < k < h^*_w(l, p^r))$ and $\nu^*_n(d, p^r) \neq 0$ and $\nu^*_k(d, p^r) \neq 0$. But then we can find i and j, with $0 \leqslant i \leqslant j < E^*_{w,n}(p^r)$, satisfying $w_{n+ih^*} \equiv w_{k+jh^*} \equiv d \pmod{p^r}$. This contradicts Proposition 4.14. $\square$

5. Subsequences

The main theorem of this paper, Theorem 6.1, concerns the frequency distribution of p-singular elements of a p-regular second-order recurrence $w(a, b)$. It turns out that these p-singular elements lie in a subsequence of $w(a, b)$ and this subsequence is itself a second-order recurrence. In this section we set the stage for the proof by examining the structure of this subsequence of p-singular terms of $w(a, b)$.

Suppose that $w(a, b) \in \mathscr{F}(a, b)$ has p-singular terms. Then (w) is multiple of a translation of the generalized Fibonacci sequence $u(a, b)$ modulo p, i.e., $w(a, b)$ lies in the same p-block as $u(a, b)$. Since $u(a, b)$ is p-regular, this forces $w(a, b)$ to be p-regular as well. If $w(a, b)$ is a multiple of a translation of $u(a, b)$ modulo p^e, then, by Corollary 2.15 of [2], $w(a, b)$ is a multiple of a translation of $u(a, b)$ modulo p^r for all $r \geqslant e$, and the frequency distribution of its p-singular terms is determined by Theorem 6.9 of [2].

Our goal in §6 is to characterize the distribution frequencies of p-singular elements in the remaining case, when $w(a, b)$ lies in the same p-block as $u(a, b)$, but not in the same p^e-block. Note that this condition requires $e > 1$. If $w(a, b)$ is such a sequence, then there exists a maximum integer m with the property that $w(a, b)$ lies in the same p^m-block as $u(a, b)$. In the following proposition, we prove that the p-singular elements of $w(a, b)$ all lie in a subsequence of $w(a, b)$ arising from subscripts in arithmetic progression, and that all of the p-singular terms of $w(a, b)$ are exactly divisible by p^m.

Proposition 5.1. *Suppose that* $e > 1$ *and that* $w(a, b) \in \mathscr{F}(a, b)$ *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 choose* k *minimal such that* $p \mid w_k$. *Then the* p*-singular terms of* $w(a, b)$ *have the following properties.*

(a) *The p-singular terms of (w) form the subsequence $w_n^* = w_{k+nh(p)}$.*
(b) *If $p \mid d$ and $\nu(d, p^r) > 0$ for some $r > m$, then $p^m \parallel d$. Furthermore, $m < e$.*

P r o o f. (a) Since $u(a,b) \in \mathscr{F}(a,b)$ is p-regular, $u_l \equiv 0 \pmod p$ if and only if $h(p) \mid l$, i.e., $l = nh(p)$ for some n. Since $w(a,b)$ is a mot of $u(a,b)$ modulo p and $p \mid w_k$, we can find a p-regular integer c such that, for all l, $w_l \equiv cu_{l-k} \pmod p$. Consequently, $w_l \equiv 0 \pmod p$ if and only if $u_{l-k} \equiv 0 \pmod p$, i.e., if and only if $l = k + nh(p)$.

(b) Since $w(a,b)$ is a mot of $u(a,b)$ modulo p^m, it follows that $w(a,b)$ is p-regular and therefore that $w_n^* = w_{k+nh(p)} \equiv M^n w_k \pmod{p^m}$, where M is an integer that is congruent, modulo p^m, to the multiplier $M_w(p^m)$. Moreover, $w_n^* \equiv 0 \pmod{p^m}$ for some n, and since M^n is invertible modulo p^m, it follows that $w_n^* \equiv 0 \pmod{p^m}$ for all n. On the other hand, since $w(a,b)$ is not a mot of $u(a,b)$ modulo p^{m+1}, no term of $w(a,b)$ is divisible by p^{m+1}. We now conclude that $p^m \parallel w_n^*$ for all n, and the first statement of (b) follows immediately. The fact that $m < e$ follows from the hypothesis that $w(a,b)$ is not a mot of $u(a,b)$ modulo p^e. □

The next well-known proposition shows that subsequences of second-order recurrence sequences arising from arithmetic subsequences of the indices are also second-order recurrence sequences, though in general they do not belong to $\mathscr{F}(a,b)$.

Proposition 5.2. *Let $w(a,b)$ be any second-order recurrence sequence and define (w') by $w'_n = w_{cn+m}$, where c is a fixed positive integer and m a fixed nonnegative integer. Then, for all n,*

$$w'_{n+2} = v_c w'_{n+1} - b^c w'_n.$$

Furthermore, if α and β are the characteristic roots of (w), then (w') has characteristic roots α^c and β^c.

P r o o f. This is Lemma 2.10 of [2], and is proven in [8] and [11] for the general k^{th}-order recurrence, where $k \geqslant 2$. □

The remainder of this section is devoted to a study of the situation described in Proposition 5.1, and in particular to an analysis of the structure of the subsequence $w^*(a,b)$ of p-singular terms of $w(a,b)$ and the computation of its structural parameters. To avoid needless repetition, we state the following hypothesis.

Hypothesis 5.3. *Suppose that $w(a,b) \in \mathscr{F}(a,b)$ is a* mot *of $u(a,b)$ modulo p, but not a* mot *of $u(a,b)$ modulo p^e. Let α and β be the roots of the characteristic polynomial of $w(a,b)$ and $D(a,b) = a^2 - 4b$ its discriminant. Replacing $w(a,b)$ with a translation, if necessary, assume that $p^m \parallel w_0$.*

Let $w^*_n = w_{nh(p)}$ be the subsequence of p-singular terms of (w) and $w'_n = w^*_n/p^m = w_{nh(p)}/p^m$ the sequence of p-regular parts of the p-singular terms of $w_n(a,b)$. Define $a' = v_{h_w(p)}$ and $b' = b^{h_w(p)}$. Let $u'_n = u_{nh_u(p)}/p^{e(u)}$. Finally, for each positive integer r, fix the following notation:

$$\begin{array}{ccc} \lambda(p^r) = \lambda_w(p^r), & \lambda'(p^r) = \lambda_{u'}(p^r), & \lambda''(p^r) = \lambda_{w'}(p^r), \\ h(p^r) = h_w(p^r), & h'(p^r) = h_{u'}(p^r), & h''(p^r) = h_{w'}(p^r), \\ e = e(w), & e' = e(u'), & e'' = e(w'). \end{array}$$

Proposition 5.4. *Assume Hypothesis* 5.3. *Then $w'_n \in \mathscr{F}(a',b')$ is a second-order recurrence satisfying*

$$w'_{n+2} = a'w'_{n+1} - b'w'_n, \tag{5.1}$$

and the discriminant $D' = D(a',b')$ is p-singular.

Proof. Equation (5.1) is an immediate consequence of Proposition 5.2. Let $D = D(a,b)$ and $h = h_w(p)$. By Lemma 2.9 of [2] and the definition of the discriminant,

$$D' = D(a',b') = (a')^2 - 4b' = v_h^2 - 4b^h = Du_h^2.$$

Since $p \mid u_h$, it follows that D' is p-singular. $\square$

Proposition 5.5. *Assume Hypothesis* 5.3. *Then the sequence (u') is p-regular and obeys the same recurrence relation as (w'), that is, $(u') \in \mathscr{F}(a',b')$. Moreover, $e' = e(u') = 1$ and $h'(p) = h_{u'}(p) = p$.*

Proof. The fact that (u') satisfies the same recurrence as (w') and $(u') \in \mathscr{F}(a',b')$ follows directly from Proposition 5.2.

We wish to apply Theorem 2.7. As in the proof of Proposition 5.4, (u') has p-singular discriminant $D' = D(a',b') = Du_h^2$. Moreover, since $a' = v_{h_w(p)}$ and $b' = b^{h_w(p)}$, we know that $p \nmid a'b'$. Also, $u'_0 = u_0/p^e = 0$, while $u'_1 = u_{h(p)}/p^e$. Since $p^e \parallel u_{h(p)}$, it follows that $p \nmid u'_1$, and consequently $p \nmid 2u'_1 - a'u'_0$. Finally, if $p = 3$, then $v^2_{h(p)} - b^{h(p)} \equiv 3b^{h(p)} \not\equiv 0 \pmod 9$. Therefore (u') satisfies the hypotheses of Theorem 2.7, and it follows that (u') is p-regular and $e' = e(u') = 1$.

Finally, Proposition 2.12 implies that $h_{u'}(p) \mid p - (\frac{D'}{p})$. Since $D' = Du_h^2$ and $p \mid u_h$, it follows that $(\frac{D'}{p}) = 0$, and hence $h_{u'}(p) \mid p$. Since (u') is p-regular, Theorem 4.1 implies that $h_{u'}(p) \neq 1$, and therefore $h_{u'}(p) = p$, as desired. $\square$

Proposition 5.6. *Assume Hypothesis* 5.3. *Then* $\lambda_{w^*}(p^r) = \lambda_{w'}(p^{r-m}) = \lambda''(p^{r-m})$. *Furthermore,* $\lambda''(p^{r-m})$ *divides* $\lambda(p^r)/h(p)$.

P r o o f. The fact that $\lambda_{w^*}(p^r) = \lambda_{w'}(p^{r-m})$ follows from the evident equivalence, for all $\lambda \geqslant 0$, of the following three statements:

$$\begin{aligned} w_n^* &\equiv w_{n+\lambda}^* \pmod{p^r}, \\ p^m w_n' &\equiv p^m w_{n+\lambda}' \pmod{p^r}, \\ w_n' &\equiv w_{n+\lambda}' \pmod{p^{r-m}}. \end{aligned}$$

It is also clear that $\lambda(p^r)/h(p)$ is a general period of (w^*). Therefore $\lambda_{w^*}(p^r)$, and consequently $\lambda''(p^{r-m})$ as well, divides $\lambda(p^r)/h(p)$. $\square$

In practice, it may happen that one period of $w(a,b)$ includes several cycles of the subsequence $w_{nh(p)}$ that is used to define $w'(a',b')$. It is convenient to keep track of the number of cycles that occur, and we do so with the following definition.

Definition 5.7. Assume Hypothesis 5.3. Define $\delta = \delta_w(p^r)$, the *discrepancy* of $w(a,b)$, to be the number of cycles of $w_n^* = w_{nh(p)}$ occurring within a single cycle of $w(a,b)$ modulo p^r.

Proposition 5.8. *Assume Hypothesis* 5.3. *Then* $\lambda(p^r)/h(p) = \delta\lambda''(p^{r-m})$.

P r o o f. The proposition follows immediately from Proposition 5.6 and the definition of the discrepancy $\delta_w(p^r)$. $\square$

Proposition 5.9. *Assume Hypothesis* 5.3 *and suppose that* $p^m \parallel d$ *and* $\nu_w(p^r) \neq 0$ *for some* $r > m$. *Then* $\nu_w(d, p^r) = \delta\nu_{w'}(d/p^m, p^{r-m})$.

P r o o f. Suppose that $w_k \equiv d \pmod{p^r}$ with $0 \leqslant k < \lambda_w(p^r)$. Then, by Proposition 5.1, $k \equiv 0 \pmod{h(p)}$, and therefore, by Proposition 5.8, $w_k = w_{nh(p)} = w_n^*$ for some n such that $0 \leqslant n < \lambda(p^r)/\lambda(p) = \delta\lambda''(p^{r-m})$. It follows that $\nu_w(d,p^r) = \delta\nu_{w^*}(d,p^r)$, and the proposition follows from the observation that $w_n^* \equiv d \pmod{p^r}$ if and only if $w_n' \equiv d/p^m \pmod{p^{r-m}}$. $\square$

In the next theorem, we express the restricted period $h_{w'}(p^r)$ in terms of the parameters e and m of the original sequence $w(a,b)$. One consequence of this computation is that $h_{w'}(p) = 1$, from which it follows that (w') is p-irregular and subject to the analysis given in §4.

Proposition 5.10. *Assume Hypothesis* 5.3. *Then* $e'' = 2e - 2m$ *and*

$$h''(p^r) = h_{w'}(p^r) = \begin{cases} 1 & \text{if } r \leqslant 2e-2m, \\ p^{r-2e+2m} & \text{if } 2e-2m < r. \end{cases} \tag{5.2}$$

Proof. Let $h = h(p)$. We apply Proposition 2.13 to $w(a,b)$ with $c = h$, and with $i = nh$ and $j = (n+1)h$, for arbitrary n. Since e is the largest integer such that $h(p^e) \mid h$, the parameter e takes the place of both l and m in Proposition 2.13, and hence, for all n, the following congruences are true if and only if $r \leqslant 2e$:

$$\begin{aligned} w_{nh+h}w_{(n+1)h} - w_{(n+1)h+h}w_{nh} &\equiv 0 \pmod{p^r}, \\ p^{2m}w'_{n+1}w'_{n+1} - p^{2m}w'_{n+2}w'_n &\equiv 0 \pmod{p^r}, \\ w'_{n+1}w'_{n+1} - w'_{n+2}w'_n &\equiv 0 \pmod{p^{r-2m}}. \end{aligned}$$

Since, by Proposition 5.1, the terms of w' are p-regular, it follows that, for all n,

$$\varrho_{w'}(n,1) \equiv \varrho_{w'}(n+1,1) \pmod{p^{2e-2m}},$$

while, also for all n,

$$\varrho_{w'}(n,1) \not\equiv \varrho_{w'}(n+1,1) \pmod{p^{2e-2m+1}}.$$

We can now conclude that $h''(p^r) = 1$ when $r \leqslant 2e-2m$ and $h''(p^r) > 1$ when $r > 2e-2m$. This proves the first part of (5.2), as well as the assertion that $e'' = 2e-2m$. Moreover, since Proposition 5.1 (b) implies that $2e-2m > 0$, we see that $h_{w'}(p) = 1$, and therefore (w') is p-irregular.

To complete the theorem, we apply Theorem 4.5 and Proposition 5.5. By Proposition 5.5, we know that $e' = 1$ and $h'(p) = p$. Therefore, by Theorem 4.5, we have

$$h''(p^r) = h_{w'}(p^r) = \begin{cases} 1 & \text{if } r \leqslant e'', \\ h'(p^{r-e''}) = h'(p^{e'}) = h'(p) & \text{if } e'' < r < e''+e', \text{ and} \\ h'(p^{r-e''}) = p^{r-e'-e''}h'(p) & \text{if } e''+e' \leqslant r, \end{cases}$$

and hence

$$h''(p^r) = h_{w'}(p^r) = \begin{cases} 1 & \text{if } r \leqslant 2e-2m, \\ h'(p^{r-2e+2m}) = p^{r-2e+2m} & \text{if } 2e-2m < r, \end{cases}$$

as desired. □

The irregularity of the sequence (w'), which we use implicitly throughout the remainder of the paper, is sufficiently important to single out in the following corollary.

Corollary 5.11. *Assume Hypothesis* 5.3. *Then the sequence* (w') *is* p*-irregular.*

Having computed the restricted period $h_{w'}(p^r)$, we turn to the special restricted periods $h^*_{w'}(n, p^r)$.

Proposition 5.12. *Assume Hypothesis* 5.3, *and let* $r^* = \max(\lceil \frac{1}{2}(r-2e+2m)\rceil, 0)$. *Then*

$$h^*_{w'}(n, p^r) = p^{r^*} = \begin{cases} 1 & \text{if } r \leqslant 2e-2m, \\ p^{\lceil (r-2e+2m)/2 \rceil} & \text{if } 2e-2m < r. \end{cases} \tag{5.3}$$

P r o o f. We apply Theorem 4.6, Proposition 5.5, and Proposition 5.10. By Proposition 5.10, $e'' = 2e-2m$ and, by Proposition 5.5, $e' = e(u') = 1$ and $h'(p) = p$. Therefore Proposition 5.5 and Theorem 4.6 imply that

$$h^*_{w'}(n, p^r) = h'(p^{r^*}) = \begin{cases} 1 & \text{if } r \leqslant 2e-2m, \text{ and} \\ p^{r^*} & \text{if } 2e-2m < r, \end{cases}$$

as desired. □

Proposition 5.13. *Assume Hypothesis* 5.3. *Suppose that* $\operatorname{ord}_{p^{2e-2m}}(\varrho_{w'}(0,1)) = p^c s$, *where* $p \nmid s$ *and* $1 \leqslant c < 2e-2m$. *Then*

$$\operatorname{ord}_{p^{r-m}}(M^*_{w'}(n, p^{r-m})) = \begin{cases} s & \text{if } m < r \leqslant 2e-m-c, \\ p^{(r-2e+m+c)} s & \text{if } 2e-m-c < r \leqslant 2e-m, \\ p^{c+\lfloor (r-2e+m)/2 \rfloor} s & \text{if } 2e-m < r. \end{cases}$$

P r o o f. Since, by Proposition 5.10, $e'' = 2e-2m$, Theorem 4.1 implies that $\varrho_{w'}(n,1) \equiv \varrho_{w'}(0,1)$ for all n. Thus, the proposition follows directly from Proposition 4.11, Proposition 5.10, and Proposition 5.5. □

The next two propositions are somewhat technical in nature and are used in §6 to demonstrate the existence of residues with frequencies that are unbounded as a function of the power of the modulus p^r.

Proposition 5.14. *Assume Hypothesis* 5.3. *Suppose that* $\operatorname{ord}_{p^{2e-2m}}(\varrho_{w'}(0,1)) = s$, *where* $p \nmid s$. *Then there exists a corresponding integer* n *with* $0 \leqslant n < h(p^r)$ *such that*

$$\operatorname{ord}_{p^{2r-2m}}(\varrho_w(nh(p), h(p^r))) = s.$$

Proof. If $r \leqslant e$, then $h(p^r) = h(p)$. Since $p^m \parallel w_{kh(p)}$ for all k, it follows that $\varrho_{w'}(0,1) = \varrho_w(0, h(p))$, and hence the hypotheses, together with Proposition 3.1, imply that

$$s = \operatorname{ord}_{p^{2e-2m}}(\varrho_{w'}(0,1)) = \operatorname{ord}_{p^{2r-2m}}(\varrho_{w'}(0,1)) = \operatorname{ord}_{p^{2r-2m}}(\varrho_w(0, h(p))),$$

thus verifying the proposition with $n = 0$.

To prove the proposition for $r > e$, we proceed by induction. To this end, fix $r \geqslant e$ and assume the conclusion of the proposition is true for this r. In particular, there is an integer n such that $\operatorname{ord}_{p^{2r-2m}}(\varrho_w(nh(p), h(p^r)) = s$. To complete the induction we show that $\operatorname{ord}_{p^{2(r+1)-2m}}(\varrho_w(nh(p) + ih(p^r), h(p^{r+1}))) = s$ for some integer i.

Since $r \geqslant e$, Theorem 2.10 implies that $h(p^{r+1}) = ph(p^r)$. For $0 \leqslant i < j < p$, we see that r is the largest integer such that $h_w(p^r) \mid (j-i)h(p^r)$, while $r+1$ is the largest integer such that $h(p^{r+1}) \mid ph(p^r)$. Consequently Proposition 2.13 implies, for $0 \leqslant i < j < p$, that

$$\begin{aligned} &w_{nh(p)+ih(p^r)+h(p^{r+1})} w_{nh(p)+jh(p^r)} \\ &\qquad - w_{nh(p)+jh(p^r)+h(p^{r+1})} w_{nh(p)+ih(p^r)} \equiv 0 \pmod{p^l} \end{aligned} \tag{5.4}$$

if and only if $2r + 1 \geqslant l$. Since $p^m \parallel w_{kh(p)}$ for all k, (5.4) is equivalent to

$$\varrho_w(nh(p) + ih(p^r), h(p^{r+1})) \equiv \varrho_w(nh(p) + jh(p^r), h(p^{r+1})) \pmod{p^{l-2m}}$$

if and only if $2r + 1 \geqslant l$, and it follows that, for $0 \leqslant i < p$, the residues $\varrho_w(nh(p) + ih(p^r), h(p^{r+1}))$ are mutually congruent modulo $p^{2r-2m+1}$ and pairwise incongruent modulo $p^{2r-2m+2}$.

In order to apply Proposition 4.9, we express the previous observations in terms of the p-irregular subsequence (w'). By Theorem 2.10, we see that

$$\varrho_{w'}(n + ih(p^r)/h(p), p^{r+1-e}) \equiv \varrho_{w'}(n, p^{r+1-e}) \pmod{p^{2r-2m+1}}$$

for $0 \leqslant i < p$, while

$$\varrho_{w'}(n + ih(p^r)/h(p), p^{r+1-e}) \not\equiv \varrho_{w'}(n + jh(p^r)/h(p), p^{r+1-e}) \pmod{p^{2r-2m+2}},$$

for $0 \leqslant i < j < p$.

By Proposition 5.5 and Proposition 5.10, we know that $e' = e(u') = 1$ and $h'(p) = h_{u'}(p) = p$, so Proposition 4.9, along with the observation that $e'' = 2e - 2m$, implies that

$$\begin{aligned} \varrho_{w'}(n + ih(p^r)/h(p), p^{r+1-e})) &\equiv \varrho_{w'}(n, p^{r+1-e}) \\ &\equiv \varrho_{w'}(n, p^{r-e})^p \pmod{p^{2r-2m+1}}, \end{aligned}$$

and therefore

$$\begin{aligned} \varrho_w(nh(p) + ih(p^r), h(p^{r+1})) &\equiv \varrho_w(nh(p), h(p^{r+1})) \\ &\equiv \varrho_w(nh(p), h(p^r))^p \pmod{p^{2r-2m+1}}. \end{aligned}$$

Raising both sides to the power p, it follows that

$$\varrho_w(nh(p) + ih(p^r), h(p^{r+1}))^p \equiv \varrho_w(nh(p), h(p^r))^{p^2} \pmod{p^{2r-2m+2}}. \tag{5.5}$$

Since, by our induction hypothesis, $\mathrm{ord}_{p^{2r-2m}}(\varrho_w(nh(p), h(p^r))) = s$, it follows that $\mathrm{ord}_{p^{2r-2m+2}}(\varrho_w(nh(p), h(p^r)))^{p^2}) = s$, and hence $\mathrm{ord}_{p^{2r-2m+2}}(\varrho_w(nh(p) + ih(p^r, h(p^{r+1})))^p) = s$ or ps for each i. However, these residues constitute all p distinct solutions to the congruence $x^p \equiv \varrho_w(nh(p), h(p^r))^{p^2} \pmod{p^{2r+2}}$, and it follows from the structure of $(\mathbb{Z}/p^{2r+2}\mathbb{Z})^*$ that exactly one of them has order s. $\square$

Proposition 5.15. *Assume Hypothesis* 5.3. *Suppose that* $\mathrm{ord}_{p^{2e-2m}}(\varrho_{w'}(0,1)) = s$, *where* $p \nmid s$, *and that* $r - m \geqslant 2e - 2m$. *Then there exists a corresponding integer* n *with* $0 \leqslant n < h(p^r)$ *such that*

$$\mathrm{ord}_{p^{r-m}}(\varrho_{w'}(n, h^*_{w'}(n, p^{r-m}))) = s.$$

Proof. Let $(r-m)^* = \max(\lceil \frac{1}{2}(r - m - (2e - 2m))\rceil, 0) = \lceil \frac{1}{2}(r - 2e + m)\rceil$. We apply Proposition 5.14 with $\hat{r} = (r-m)^* + e$ in place of r. Clearly,

$$2\hat{r} - 2m = 2(r-m)^* + 2e - 2m = \begin{cases} r - m & \text{if } r - m \text{ is even, and} \\ r - m + 1 & \text{if } r - m \text{ is odd.} \end{cases}$$

Moreover, by Theorem 2.10,

$$h(p^{\hat{r}}) = h(p^{(r-m)^* + e}) = p^{(r-m)^*} h(p).$$

Finally, since $p^m \parallel w_{kh(p)}$ for all k, Proposition 5.12 implies that

$$\varrho_w(nh(p), p^{(r-m)^*} h(p))) = \varrho_{w'}(n, p^{(r-m)^*}))) = \varrho_{w'}(n, h^*_{w'}(n, p^{r-m}))).$$

Therefore, if $r - m$ is even, the conclusion of Proposition 5.14 is

$$\operatorname{ord}_{p^{r-m}}(\varrho_{w'}(n, h^*_{w'}(n, p^{r-m}))) = s,$$

as desired. On the other hand, if $r - m$ is odd, the conclusion is

$$\operatorname{ord}_{p^{r-m+1}}(\varrho_{w'}(n, h^*_{w'}(n, p^{r-m}))) = s,$$

and we apply Proposition 3.1 to obtain the desired result. □

Proposition 5.16. *Assume Hypothesis* 5.3. *If* $e - m < f$, *then*

$$\begin{aligned} \operatorname{ord}_{p^{e-m}}(\varrho_{w'}(0,1)) &= s \\ \operatorname{ord}_{p^{e-m+1}}(\varrho_{w'}(0,1)) &= ps, \end{aligned}$$

and, if $f < e - m$, *then*

$$\operatorname{ord}_{p^{e-m}}(\varrho_{w'}(0,1)) = p^{(e-m)-f}s.$$

Proof. Let $h = h_w(p) = h_w(p^e)$, and suppose that $0 \leqslant M < p^{e+1}$ satisfies $w_{h+1} \equiv M w_1 \pmod{p^{e+1}}$. Then clearly

$$M \equiv M(p^e) \pmod{p^e}, \tag{5.6}$$

and hence

$$\begin{aligned} w_h &\equiv M w_0 \pmod{p^e} \quad \text{and} \\ w_{h+1} &\equiv M w_1 \pmod{p^e}. \end{aligned}$$

If it is also true that $w_h \equiv M w_0 \pmod{p^{e+1}}$, then an easy induction argument shows that $w_{h+i} \equiv M w_i \pmod{p^{e+1}}$ for all i, contrary to the maximality of e. Therefore $w_h \not\equiv M w_0 \pmod{p^{e+1}}$. Suppose, then, that $0 \leqslant K < p^{e+1}$ satisfies $w_h \equiv K w_0 \pmod{p^{e+1}}$. Then $K w_0 \equiv M w_0 \pmod{p^e}$ and, since $p^m \parallel w_0$, it follows that $K \equiv M + l p^{e-m} \pmod{p^{e-m+1}}$, for some integer l that is relatively prime to p. Since $p^m \parallel w_0$ and $p^m \parallel w_h$, it follows that

$$\begin{aligned} w'_1 &\equiv M w'_0 \pmod{p^{e-m}} \quad \text{and} \\ w'_1 &\equiv (M + l p^{e-m}) w'_0 \pmod{p^{e-m+1}}, \end{aligned}$$

and therefore

$$
\begin{aligned}
&\varrho_{w'}(0,1) \equiv M \pmod{p^{e-m}} \quad \text{and} \\
&\varrho_{w'}(0,1) \equiv (M + lp^{e-m}) \pmod{p^{e-m+1}}.
\end{aligned} \tag{5.7}
$$

Now suppose that $e - m < f$. Then $h(p^{e-m}) = h(p^{e-m+1}) = h(p^e)$ and, since $e - m + 1 \leqslant f$, Theorem 2.10 and (5.6) yield

$$
\begin{aligned}
\operatorname{ord}_{p^{e-m}}(M) &= \operatorname{ord}_{p^{e-m}}(M(p)) = s, \text{ and} \\
\operatorname{ord}_{p^{e-m+1}}(M) &= \operatorname{ord}_{p^{e-m+1}}(M(p)) = s.
\end{aligned}
$$

The binomial theorem now yields

$$
\begin{aligned}
(M + lp^{e-m})^s &\equiv M^s + sM^{s-1}lp^{e-m} \pmod{p^{e-m+1}} \\
&\equiv 1 + sM^{s-1}lp^{e-m} \pmod{p^{e-m+1}},
\end{aligned}
$$

and hence, by Proposition 3.1,

$$
\operatorname{ord}_{p^{e-m+1}}(\varrho_{w'}(0,1)) = ps,
$$

as desired.

Now suppose that $f < e - m$. Again $h(p^{e-m}) = h(p^e)$ and, by Theorem 2.10 and (5.6),

$$
\operatorname{ord}_{p^{e-m}}(\varrho_{w'}(0,1)) = \operatorname{ord}_{p^{e-m}}(M) = \operatorname{ord}_{p^{e-m}}(M(p)) = p^{(e-m)-f}s,
$$

as desired. □

Proposition 5.17. *Assume Hypothesis* 5.3. *If* $e - m < f$, *then*

$$
\operatorname{ord}_{p^{r-m}}(\varrho_{w'}(0,1)) = \begin{cases} s & \text{if } r \leqslant e, \\ p^{r-e}s & \text{if } e < r, \end{cases} \tag{5.8}
$$

and if $f < e - m$, *then*

$$
\operatorname{ord}_{p^{r-m}}(\varrho_{w'}(0,1)) = \begin{cases} s & \text{if } r \leqslant m + f, \\ p^{r-m-f}s & \text{if } m + f < r. \end{cases} \tag{5.9}
$$

Proof. Both equations (5.8) and (5.9) follow immediately from Proposition 5.16 and Proposition 3.1. □

Proposition 5.18. *Assume Hypothesis* 5.3. *Then*

$$\operatorname{ord}_{p^{2e-2m}}(\varrho_{w'}(0,1)) = p^c s, \tag{5.10}$$

for some c that satisfies $0 \leqslant c \leqslant 2e-2m-f$. Moreover, for each such integer c, there is a p-regular sequence $w_c(a,b) \in \mathscr{F}(a,b)$ for which $\operatorname{ord}_{p^{2e-2m}}(\varrho_{w'_c}(0,1)) = p^c s$.

P r o o f. Since $p^m \parallel w_0$ and $p^m \parallel w_{h(p)}$, it follows that $\varrho_{w'}(0,1) = \varrho_w(0,h(p))$. Thus, Theorem 2.10 yields

$$\operatorname{ord}_{p^f}(\varrho_{w'}(0,1)) = \operatorname{ord}_{p^f}(\varrho_w(0,h(p))) = \operatorname{ord}_{p^f}(M(p^f)) = s.$$

Now choose $k \geqslant f$ maximal such that $\operatorname{ord}_{p^k}(\varrho_w(0,h(p))) = s$. If $2e-2m \leqslant k$, then (5.10) is true with $c = 0$. Otherwise, Proposition 3.1 implies that

$$\operatorname{ord}_{p^{2e-2m}}(\varrho_{w'}(0,1)) = \operatorname{ord}_{p^{2e-2m}}(\varrho_w(0,h(p))) = p^{2e-2m-k}s,$$

and (5.10) is true with $c = 2e-2m-k$. Clearly in both cases $0 \leqslant c \leqslant 2e-2m-f$.

To prove the converse, let $\mathscr{F}_m(a,b) \subseteq \mathscr{F}(a,b)$ be the subset of p-regular sequences $w(a,b) \in \mathscr{F}(a,b)$ for which $p^m \parallel w_n$, for some n, and set

$$\Omega = \{\, k \in \mathbb{Z}/p^{2e-2m}\mathbb{Z};\ k \equiv \varrho_{w'}(0,1) \pmod{p^{2e-2m}} \text{ for some } w(a,b) \in \mathscr{F}_m(a,b) \,\}$$
$$\Gamma = \{\, k \in \mathbb{Z}/p^{2e-2m}\mathbb{Z};\ k \equiv M(p^e) \pmod{p^{e-m}} \text{ and } k \not\equiv M(p^e) \pmod{p^{e-m+1}} \,\}.$$

We claim that $\Omega = \Gamma$.

To begin, we apply an argument, similar to that used in Proposition 5.16 to obtain (5.7), to show that $\Omega \subseteq \Gamma$. Suppose that $k \in \Omega$, and choose w such that $k \equiv \varrho_{w'}(0,1) \pmod{p^{2e-2m}}$. Let $h = h_w(p) = h_w(p^e)$, and let M be an integer that satisfies

$$w_{h+1} \equiv M w_1 \pmod{p^{e+1}}. \tag{5.11}$$

Then $w_{h+1} \equiv M w_1 \pmod{p^e}$ and, certainly, $w_{h+1} \equiv M(p^e) w_1 \pmod{p^e}$, so

$$M \equiv M(p^e) \pmod{p^e}.$$

Since $k \in \Omega$ and $e \geqslant m+1$,

$$k \equiv \varrho_{w'}(0,1) \pmod{p^{e-m+1}}.$$

Since $p^m \parallel w_0$ and $p^m \parallel w_h$, we obtain the following congruences:

$$\begin{aligned} w_h &\equiv kw_0 \pmod{p^{e+1}} \\ w_h &\equiv kw_0 \pmod{p^e}, \end{aligned}$$

and therefore

$$k \equiv M(p^e) \ (\operatorname{mod} p^{e-m}).$$

It now follows as well that

$$k \equiv M \ (\operatorname{mod} p^{e-m}).$$

On the other hand, if

$$\begin{aligned} k &\equiv M(p^e) \pmod{p^{e-m+1}} \\ &\equiv M \pmod{p^{e-m+1}}, \end{aligned}$$

then $kw_0 \equiv Mw_0 \ (\operatorname{mod} p^{e+1})$, and hence

$$w_h \equiv Mw_0 \ (\operatorname{mod} p^{e+1}). \tag{5.12}$$

However, (5.11) and (5.12), together with an easy induction argument, contradict the minimality of e. Hence $k \not\equiv M(p^e) \ (\operatorname{mod} p^{e-m+1})$, and $k \in \Gamma$, as desired.

To complete the proof that $\Omega = \Gamma$, we show that $|\Omega| = |\Gamma|$. It is an easy exercise to verify that $|\Gamma| = \varphi(p^{e-m})$.

Now, if $w(a,b)$ and $x(a,b)$ are sequences in $\mathscr{F}_m(a,b)$ and $h = h(p)$, then the following statements are equivalent:

$$\begin{aligned} \varrho_{w'}(0,1) &\equiv \varrho_{x'}(0,1) \pmod{p^{2e-2m}}, \\ w_0'x_1' - x_0'w_1' &\equiv 0 \pmod{p^{2e-2m}}, \\ w_0x_h - x_0w_h &\equiv 0 \pmod{p^{2e}}. \end{aligned}$$

By Proposition 2.14, this last statement is true if and only if $w(a,b)$ and $x(a,b)$ lie in the same p^e-block. It follows that $|\Omega|$ is equal to the number $T_m(p^e)$ of p-regular p^e-blocks of $\mathscr{F}(a,b)$ that contain a sequence $w(a,b)$ for which $p^m \parallel w_n$, for some n. We can determine $T_m(p^e)$ by enumerating the sequences in $\mathscr{F}_m(a,b)$ and applying Proposition 2.15. Each sequence $w(a,b) \in \mathscr{F}_m(a,b)$ is determined by a pair of consecutive terms (w_n, w_{n+1}), with $p^m \parallel w_n$, $p \nmid w_{n+1}$, and $0 \leqslant n < h(p)$. Since there are $\varphi(p^{e-m})$ integers w_n such that $p^m \parallel w_n$ and $0 \leqslant w_n < p^e$, and $\varphi(p^e)$

integers w_{n+1} such that $p \nmid w_{n+1}$ and $0 \leqslant w_{n+1} < p^e$, it follows that $|\mathscr{F}_m(a,b)| = \varphi(p^{e-m})\varphi(p^e)h(p)$. Proposition 2.15 now implies that

$$T_m(p^e) = \frac{\varphi(p^{e-m})\varphi(p^e)h(p)}{\varphi(p^e)h(p)} = \varphi(p^{e-m}). \tag{5.13}$$

We can now conclude that $|\Omega| = |\Gamma|$, and hence $\Omega = \Gamma$, as claimed above.

The rest of the theorem now follows from Proposition 3.4. □

6. Bounds for frequency distributions for regular recurrences

In this final section, we prove our main theorem, Theorem 6.1, which describes the distribution of frequencies modulo p^r of p-singular terms of a p-regular second-order recurrence that lies in the same p-block as the generalized Fibonacci sequence $u(a,b)$, but not in the same p^e-block. This result, together with the previously published results in [2], provide a precise description of the frequency distribution functions of p-regular second-order recurrences in terms of the global parameters e and f.

Theorem 6.1. *Suppose that $e > 1$ and that $w(a,b) \in \mathscr{F}(a,b)$ 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,

$$\nu(d,p^r) = \begin{cases} p^{r-f^*} & \text{if } m < r \leqslant \min(m+f,e), \\ p^m & \text{if } e-m > f \text{ and } \min(m+f,e) < r, \text{ and} \\ p^{e-f} & \text{if } e-m < f \text{ and } \min(m+f,e) < r. \end{cases} \tag{6.1}$$

If $e - m = f$, then

$$\operatorname{ord}_{p^{2e-2m}}\left(\frac{w_{n+h(p^e)}}{p^m}\Big/\frac{w_n}{p^m}\right) = p^\gamma s \tag{6.2}$$

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

$$\nu(d,p^r) = p^{\min(r-f,e-\gamma)}, \tag{6.3}$$

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

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

P r o o f. Suppose that $w(a,b)$ satisfies the hypotheses of the theorem and that d is divisible by p and satisfies $\nu_w(d,p^r) > 0$. The fact that $p^m \parallel d$ follows from Proposition 5.1. Moreover, by (2.9), we lose no generality by replacing $w(a,b)$ with a translation, and hence we can assume that $w(a,b)$ satisfies Hypothesis 5.3. By Proposition 5.9, if we set $d' = d/p^m$, we obtain

$$\nu_w(d,p^r) = \delta\nu_{w'}(d/p^m, p^{r-m}) = \delta\nu_{w'}(d', p^{r-m}). \tag{6.4}$$

We now set $(r-m)^* = \max(\lceil\frac{1}{2}(r+m-2e)\rceil, 0)$ and apply, in turn, Proposition 5.9, (2.7), Proposition 4.7, Proposition 5.8, and Theorem 2.10 to the p-irregular sequence $w'(a',b')$ to obtain

$$\begin{aligned} \nu_w(d,p^r) &= \delta\nu_{w'}(d',p^{r-m}) \\ &= \delta \sum_{n=0}^{h^*_{w'}(l,p^{r-m})-1} \nu^*_{w',n}(d',p^{r-m}) = \delta \sum_{n\in\Omega} \frac{\lambda_{w'}(p^{r-m})/h_{w'}(p^{(r-m)^*})}{\operatorname{ord}_{p^{r-m}}(M^*_{w'}(n,p^{r-m}))} \\ &= \sum_{n\in\Omega} \frac{\lambda(p^r)/h(p)h''(p^{(r-m)^*})}{\operatorname{ord}_{p^{r-m}}(M^*_{w'}(n,p^{r-m}))} = \sum_{n\in\Omega} \frac{p^{r-f^*}s/h''(p^{(r-m)^*})}{\operatorname{ord}_{p^{r-m}}(M^*_{w'}(n,p^{r-m}))}, \end{aligned} \tag{6.5}$$

where $\Omega = \{\, n;\ 0 \leqslant n < h^*_{w'}(p^{r-m}) \text{ and } \nu^*_{w',n}(d',p^{r-m}) \neq 0 \,\}$.

We complete the theorem by applying (6.5) in several cases corresponding to the parts of (6.1).

C a s e 1. $m < r \leqslant \min(m+f, e)$.

Since $m < e$, the hypothesis that $r \leqslant e$ implies that $r < 2e - m$, and hence $(r-m)^* = \max(\lceil\frac{1}{2}(r+m-2e)\rceil, 0) = 0$. Therefore, by Proposition 5.12, $h^*_{w'}(n,p^{r-m}) = h_{w'}(p^{(r-m)^*}) = h''(p^{(r-m)^*}) = 1$. It follows that the summation (2.7) has only a single term, corresponding to $n = 0$. Moreover, since $h^*_{w'}(n,p^{r-m}) = 1$, we also see that $M^*_{w'}(0,p^{r-m}) \equiv \varrho_{w'}(0,1) \pmod{p^{r-m}}$. Since $p^m \parallel w_0$ and $p^m \parallel w_{h(p)}$, it follows that $\varrho_{w'}(0,1) = \varrho_w(0,h(p))$ and, since $r - m \leqslant f$, Theorem 2.10 shows that $\operatorname{ord}_{p^{r-m}}(\varrho_w(0,h(p))) = s$. Therefore, (6.5) yields

$$\nu_w(d,p^{r-m}) = \frac{p^{r-f^*}s}{s} = p^{r-f^*}.$$

C a s e 2. $e - m > f$ and $\min(m+f, e) < r$.

First, note that since $e - m > f$, we know that $e > m + f$, and hence the second hypothesis reduces to $m + f < r$.

Suppose as well that $r \leqslant 2e-m$. Then, as in Case 1, $(r-m)^* = 0$, $h''(p^{(r-m)^*}) = 1$, and the summation (2.7) has only a single term, corresponding to $n = 0$. As before,

$M^*_{w'}(0, p^{r-m}) \equiv \varrho_{w'}(0,1) \pmod{p^{r-m}}$, but now $e - m > f$ and $m + f < r$, so Proposition 5.17 implies that $\mathrm{ord}_{p^{r-m}}(\varrho_{w'}(0,1)) = p^{r-m-f}s$. Therefore, (6.5) yields

$$\nu_w(d, p^{r-m}) = \frac{p^{r-f^*}s}{p^{r-m-f}s} = p^m.$$

Now suppose that $2e - m < r$. Then $h''(p^{(r-m)^*}) > 1$. We claim, however, that the summation (6.5) still has has only one nonzero term. This follows immediately from Proposition 4.15 once we establish the hypothesis that $\mathrm{ord}_{p^{e''}}(\varrho_{w'}(0,1)) = p^c s$, where $p \nmid s$ and $1 \leqslant c < e''$.

But we know that $e'' = 2e - 2m = 2(e - m) > f$, so $e'' + m > f + m$. Therefore, Proposition 5.17 implies that $\mathrm{ord}_{p^{e''}}(\varrho_{w'}(0,1)) = p^{e''-f}s$. Consequently, setting $c = e'' - f > 0$, we have established the hypotheses of Proposition 4.15. Therefore the summation (6.5) reduces to

$$\nu_w(d, p^r) = \frac{p^{r-f^*}s/h''(p^{(r-m)^*})}{\mathrm{ord}_{p^{r-m}}(M^*_{w'}(n, p^{r-m}))}, \tag{6.6}$$

where the index n is chosen so that $\nu^*_{w',k}(d', p^{r-m}) \neq 0$.

Now, Proposition 5.12 implies that $h''(p^{(r-m)^*}) = p^{\lceil (r-2e+m)/2 \rceil}$ and Proposition 5.13 implies that $\mathrm{ord}_{p^{r-m}}(M^*_{w'}(n, p^{r-m})) = p^{c+\lfloor (r-2e+m)/2 \rfloor}s$. Finally, (6.6) yields

$$\begin{aligned}\nu_w(d, p^r) &= \frac{p^{r-f^*}s/h''(p^{(r-m)^*})}{\mathrm{ord}_{p^{r-m}}(M^*_{w'}(n, p^{r-m}))} = \frac{p^{r-f^*}s/p^{\lceil (r-2e+m)/2 \rceil}}{p^{c+\lfloor (r-2e+m)/2 \rfloor}s} \\ &= p^{r-f-\lceil (r-2e+m)/2 \rceil - c - \lfloor (r-2e+m)/2 \rfloor} = p^{2e-m-f-c} = p^m,\end{aligned}$$

as desired.

Case 3. $e - m < f$ and $\min(m + f, e) < r$.

In this case, note that since $e - m \leqslant f$, we know that $e \leqslant m + f$, and hence the second hypothesis reduces to $e < r$.

As in Case 2, we first consider the situation when $r \leqslant 2e - m$. Once again $(r - m)^* = 0$, $h''(p^{(r-m)^*}) = 1$, and the summation (2.7) has only a single term, corresponding to $n = 0$. As in both previous cases, $M^*_{w'}(0, p^{r-m}) \equiv \varrho_{w'}(0,1) \pmod{p^{r-m}}$, and this time $e - m \leqslant f$ and $e < r$, so Proposition 5.17 implies that $\mathrm{ord}_{p^{r-m}}(\varrho_{w'}(0,1)) = p^{r-e}s$. Therefore, (6.5) yields

$$\nu_w(d, p^{r-m}) = \frac{p^{r-f^*}s}{p^{r-e}s} = p^{e-f}.$$

Now suppose that $2e - m < r$. Then $h''(p^{(r-m)^*}) > 1$, but again we claim that the summation (6.5) has only one nonzero term. Again, this follows from

Proposition 4.15 once we establish the hypothesis that $\operatorname{ord}_{p^{e''}}(\varrho_{w'}(0,1)) = p^c s$, where $p \nmid s$ and $1 \leqslant c < e''$.

In this case, since $m < e$, we see that $e'' + m = 2e - m \geqslant e$, so Proposition 5.17 implies that $\operatorname{ord}_{p^{e''}}(\varrho_{w'}(0,1)) = p^{e''+m-e}s = p^{e-m}s$.

Thus, we have established the remaining hypothesis of Proposition 4.15, with $c = e - m > 0$, and can proceed to evaluate (6.6). Once again, Proposition 5.12 implies that $h''(p^{(r-m)^*}) = p^{\lceil (r-2e+m)/2\rceil}$, and Proposition 5.13 implies that $\operatorname{ord}_{p^{r-m}}(M^*_{w'}(n, p^{r-m})) = p^{c+\lfloor (r-2e+m)/2\rfloor}s$. Thus, (6.6) yields

$$\begin{aligned}\nu_w(d, p^r) &= \frac{p^{r-f^*}s/h''(p^{(r-m)^*})}{\operatorname{ord}_{p^{r-m}}(M^*_{w'}(n, p^{r-m}))} = \frac{p^{r-f^*}s/p^{\lceil (r-2e+m)/2\rceil}}{p^{c+\lfloor (r-2e+m)/2\rfloor}s} \\ &= p^{r-f-\lceil (r-2e+m)/2\rceil - c - \lfloor (r-2e+m)/2\rfloor} = p^{2e-m-f-c} = p^{e-f},\end{aligned}$$

as desired.

The remaining two cases, those for which $e - m = f$, require the construction of the parameter γ. The existence of γ and of sequences $w(a,b) \in \mathscr{F}(a,b)$ that satisfy the hypotheses of the theorem and for which γ takes on each of the values $0 \leqslant \gamma \leqslant f$ is proven in Proposition 5.18, once the observation is made that $2e - 2m - f = f$.

Case 4. $e - m = f$, $r > e$, and $\gamma \geqslant 1$.

As in the previous cases, we start by assuming $r \leqslant 2e - m$. Then $(r-m)^* = 0$, $h''(p^{(r-m)^*}) = 1$, and the summation (2.7) has only a single term, corresponding to $n = 0$. As before, $M^*_{w'}(0, p^{r-m}) \equiv \varrho_{w'}(0,1) \pmod{p^{r-m}}$. By (6.2) and Proposition 3.1, and the observation that $(r-m)-(2e-2m)+\gamma = r-2e+m+\gamma = r-e-f+\gamma$, we obtain

$$\operatorname{ord}_{p^{r-m}}(\varrho_{w'}(0,1)) = \begin{cases} s & \text{if } r \leqslant 2e - m - \gamma, \text{ and} \\ p^{r-e-f+\gamma}s & \text{if } 2e - m - \gamma < r. \end{cases}$$

Therefore, (6.5) yields

$$\nu_w(d, p^{r-m}) = \begin{cases} \dfrac{p^{r-f^*}s}{s} = p^{r-f} & \text{if } r \leqslant 2e - m - \gamma, \text{ and} \\ \dfrac{p^{r-f^*}s}{p^{r-e-f+\gamma}} = p^{e-\gamma} & \text{if } 2e - m - \gamma < r. \end{cases} \tag{6.7}$$

Now, $r \leqslant 2e - m - \gamma$ is equivalent to $r - f \leqslant 2e - m - \gamma - f = e - \gamma$, so (6.3) follows from (6.7).

Now suppose that $2e - m < r$. Then $h''(p^{(r-m)^*}) > 1$. However, setting $c = \gamma > 0$, we see that all the hypotheses of Proposition 4.15 are true, and therefore the summation (6.5) has only one nonzero term. As usual, we must evaluate (6.6).

As in the previous cases, Proposition 5.12 implies $h''(p^{(r-m)^*}) = p^{\lceil (r-2e+m)/2\rceil}$, and Proposition 5.13 implies that

$$\mathrm{ord}_{p^{r-m}}(M^*_{w'}(n, p^{r-m})) = p^{c+\lfloor (r-2e+m)/2\rfloor} s = p^{\gamma+\lfloor (r-2e+m)/2\rfloor} s.$$

Thus, (6.6) yields

$$\nu_w(d, p^r) = \frac{p^{r-f^*} s / h''(p^{(r-m)^*})}{\mathrm{ord}_{p^{r-m}}(M^*_{w'}(n, p^{r-m}))} = p^{2e-m-f-\gamma} = p^{e-\gamma}.$$

Since $r > 2e - m > 2e - m - \gamma$, we know that $r - f > e - \gamma$, and (6.3) follows immediately.

Case 5. $e - m = f$, $r > 2e - m$, and $\gamma = 0$.

By Proposition 5.15, we can find n with $0 \leqslant n < h(p^r)$ such that

$$\mathrm{ord}_{p^{r-m}}(M^*_{w'}(n, p^{r-m})) = \mathrm{ord}_{p^{r-m}}(\varrho_{w'}(n, h^*_{w'}(n, p^{r-m}))) = s. \tag{6.8}$$

If we now choose d such that $d \equiv w_{nh(p)}$, then Proposition 5.1 implies that $p^m \parallel d$ and, clearly, $\nu^*_{w',n}(d', p^{r-m}) \neq 0$.

By hypothesis, $r > 2e - m$, and therefore $h''(p^{(r-m)^*}) > 1$. Since $\gamma = 0$, we are unable to apply Proposition 4.15 and return instead to (6.5). By our choice of d in the previous paragraph, we know that Ω is not empty, and we can rewrite (6.6) as an inequality:

$$\nu_w(d, p^r) \geqslant \frac{p^{r-f^*} s / h''(p^{(r-m)^*})}{\mathrm{ord}_{p^{r-m}}(M^*_{w'}(n, p^{r-m}))}. \tag{6.9}$$

We now proceed as in the previous cases. Since Proposition 5.12 implies that $h''(p^{(r-m)^*}) = p^{\lceil (r-2e+m)/2\rceil}$, (6.9) and (6.8) yield

$$\begin{aligned}\nu_w(d, p^r) &\geqslant \frac{p^{r-f^*} s / h''(p^{(r-m)^*})}{\mathrm{ord}_{p^{r-m}}(M^*_{w'}(n, p^{r-m}))} = \frac{p^{r-f} s / p^{\lceil (r-2e+m)/2\rceil}}{s} \\ &= p^{r-f-\lceil (r-2e+m)/2\rceil} = p^{r-f-\lceil (r-e-f)/2\rceil},\end{aligned}$$

as desired. $\square$

References

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

[2] *Walter Carlip, 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.

[3] *R. D. Carmichael*: On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$. Ann. Math. *15* (1913/14), 30–70.

[4] *D. H. Lehmer*: An extended theory of Lucas' functions. Ann. of Math. *31* (1930), 419–448.

[5] *William J. LeVeque*: Fundamentals of Number Theory. Dover Publications Inc., Mineola, NY, 1996, Reprint of the 1977 original.

[6] *E. Lucas*: Théorie des fonctions numériques simplement périodiques. Amer. J. Math. *1* (1878), 184–240, 289–321.

[7] *L. M. Milne-Thompson*: The Calculus of Finite Differences. Macmillan, London, 1951.

[8] *H. Niederreiter*: A simple and general approach to the decimation of feedback shift-register sequences. Problems Control Inform. Theory/Problemy Upravlen. Teor. Inform. *17* (1988), 327–331.

[9] *H. Niederreiter, A. Schinzel, L. Somer*: Maximal frequencies of elements in second-order linear recurring sequences over a finite field. Elem. Math. *46* (1991), 139–143.

[10] *Ivan Niven, Herbert S. Zuckerman, Hugh L. Montgomery*: An Introduction to the Theory of Numbers, fifth ed. John Wiley & Sons Inc., New York, 1991.

[11] *Lawrence Somer*: Solution to problem H-377. Fibonacci Quart. *24* (1986), 284–285.

[12] *Lawrence Somer*: Upper Bounds for Frequencies of Elements in Second-Order Recurrences Over a Finite Field. Applications of Fibonacci numbers, Vol. 5 (St. Andrews, 1992), Kluwer Acad. Publ., Dordrecht, 1993, pp. 527–546.

[13] *Lawrence Somer, Walter Carlip*: Stability of second-order recurrences modulo p^r. Int. J. Math. Math. Sci. *23* (2000), 225–241.

[14] *Morgan Ward*: The arithmetical theory of linear recurring series. Trans. Amer. Math. Soc. *35* (1933), 600–628.

[15] *William A. Webb, Calvin T. Long*: Distribution modulo p^h of the general linear second order recurrence. Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. *58* (1975), 92–100.

Authors' addresses: *Walter Carlip*, Department of Mathematics, Franklin & Marshall College, Lancaster, Pennsylvania 17604, USA; mailing address: 408 Harvard Street, Vestal, New York 13850, USA, e-mail: `c3ar@math.uchicago.edu`; *Lawrence Somer*, Department of Mathematics, Catholic University of America, Washington D. C. 20064, USA, e-mail: `somer@cua.edu`.