THE EXISTENCE OF SPECIAL MULTIPLIERS OF SECOND-ORDER RECURRENCE SEQUENCES

Walter Carlip
Department of Mathematics and Computer Science
Loyola University of Chicago, Chicago, Illinois 60626

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

(Submitted February 2001)

1. INTRODUCTION

One approach to the study of the distributions of residues of second-order recurrence sequences (w_n) modulo powers of a prime p is to identify and examine subsequences $w_t^* = w_{n+tm}$, that are themselves first-order recurrence sequences. In particular, the *restricted period*, $h = h(p^r)$, and the *multiplier*, $M = M(p^r)$, satisfy $w_{n+th} \equiv M^t w_n \pmod{p^r}$ for all t and all n, and are independent of the initial terms of the sequence (see, e.g., [1]). In [1], we generalized the notion of the restricted period and multiplier to that of the *special restricted period* and *special multiplier*. Theorem 3.5 of [1] shows that if the sequence w is p-regular for an odd prime p, r is sufficiently large, and w_n is not divisible by p, then $w_{n+th(p^{r^*})} \equiv (M^*(n,p^r))^t w_n$ $\pmod{p^r}$ for all t, where $r^* = \lceil r/2 \rceil$, and the integer $M^*(n,p^r)$, which is defined up to congruence modulo p^r and depends upon n, is called the *special multiplier of w with respect to n.*

In this article, we examine the residues d that actually occur as special multipliers of a second-order recurrence sequence. We show that if there exists a p-regular sequence satisfying a given second-order recursion and r is sufficiently large, then every conceivable special multiplier actually exists modulo p^r. Since the special multiplier $M^*(n,p^r)$ must satisfy the congruence

$$M^*(n,p^r) \equiv M(p^{r^*}) \pmod{p^{r^*}},$$

this amounts to showing that if $d \equiv M(p^{r^*}) \pmod{p^{r^*}}$, then there exists a sequence w that satisfies the given recursion, and an index n, such that d actually occurs as the special multiplier $M^*(n,p^r)$ of that sequence.

The proof of the theorem is broken into three cases depending upon whether $\left(\frac{D}{p}\right) = -1$, 1, or 0, where D is the discriminant of the sequence w.

2. PRELIMINARIES

We employ the standard notation of [1]. In particular, $w(a,b)$ represents a second-order sequence that satisfies the recursion

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

and, for a given odd prime $p, \mathcal{F}(a,b)$ denotes the family of sequences (w) that satisfy (2.1) and for which $p \not| (w_0, w_1)$. We let $\lambda_w(p^r)$ denote the *period* of $w(a,b)$ modulo p^r, i.e., the least positive integer λ such that for all n

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

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

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

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. Since they are critical to the present study, we also remind the reader of the definitions of the *special restricted period* and *special multipliers* of a sequence $w \in \mathcal{F}(a,b)$.

Definition 2.1: For fixed n and r, let $h_w^*(n,p^r)$ be the least integer m of the set $\{ h_w(p^c) \mid 1 \leq c \leq r \}$ for which the sequence $w_t^* = w_{n+tm}$ satisfies a first-order recurrence relation $w_{t+1}^* \equiv M^* w_t^* \pmod{p^r}$ for some integer M^*. The integer $h^* = h_w^*(n,p^r)$ is called the *special restricted period* and $M^* = M_w^*(n,p^r)$ (defined up to congruence modulo p^r) the *special multiplier* with respect to w_n modulo p^r.

Finally, we let $f(x) = x^2 - ax + b$ be the *characteristic polynomial* of (w) and $D = D(a,b) = a^2 - 4b$ the *discriminant* of (w).

In general, when studying recursive sequences $w(a,b)$ modulo powers of a prime p, elements w_n for which $p \mid w_n$ behave quite differently from elements for which $p \not| w_n$. It is convenient to refer to a term w_n for which $p \not| w_n$ as *p-regular* and a term w_n for which $p \mid w_n$ as *p-singular*. Analogously, we call an integer d p-singular if $p \mid d$ and p-regular if $p \not| d$.

The sequences of $\mathcal{F}(a,b)$ are partitioned into equivalence classes, usually called *m-blocks*, by the equivalence relation **mot**, which relates two sequences if one is equivalent modulo m to a multiple of a translation of the other. We are interested here in p^r-blocks, where p is an odd prime.

A recurrence $w(a,b)$ is *p-regular* if $w_0w_2 - w_1^2 \not\equiv 0 \pmod{p}$, and *p-irregular* (or simply *irregular*, if the prime p is evident) otherwise. It is well known that either every sequence in a block of $\mathcal{F}(a,b)$ is p-regular, or none of them are, and hence, the blocks of $\mathcal{F}(a,b)$ are divided into p-regular and p-irregular blocks. It is also easy to see that all p-regular sequences in $\mathcal{F}(a,b)$ have the same period, restricted period, and multiplier. Consequently, the period, restricted period, and multiplier of a regular sequence in $\mathcal{F}(a,b)$ are independent of the initial terms of the sequence, and are *global parameters* of the family $\mathcal{F}(a,b)$. We denote these global parameters by $\lambda(p^r)$, $h(p^r)$, and $M(p^r)$, respectively. If $u(a,b) \in \mathcal{F}(a,b)$ denotes the generalized Fibonacci sequence, i.e., the sequence in $\mathcal{F}(a,b)$ with initial terms 0 and 1, then $u(a,b)$ is p-regular and therefore can be used to determine the global parameters of $\mathcal{F}(a,b)$. In particular, $h(p^r) = h_u(p^r)$.

For most second-order sequences $w(a,b)$, the restricted period modulo p^{r+1} is p times the restricted period of $w(a,b)$ modulo p^r when the exponent r is sufficiently large. The precise value of r that constitutes *sufficiently large* in this sense is denoted by the critical parameter $e(w)$, as defined below.

Definition 2.2: If $w(a,b) \in \mathcal{F}(a,b)$, then we define $e = e(w)$ to be the largest integer, if it exists, such that $h_w(p^e) = h_w(p)$.

The period of a second-order recurrence manifests a similar behavior and we define the corresponding parameter $f(w)$.

Definintion 2.3: If $w(a,b) \in \mathcal{F}(a,b)$, then we define $f = f(w)$ to be the largest integer, if it exists, such that $\lambda_w(p^f) = \lambda_w(p)$.

The sequence $w(a,b)$ is said to be *nondegenerate* if the parameter $e(w)$ exists, and *degenerate* otherwise. If w is p-regular and $e(w)$ does not exist, then $h_u(p) = 0$, and all of the p-regular sequences in $\mathcal{F}(a,b)$ are degenerate. Our main theorem, Theorem 5.1, concerns families $\mathcal{F}(a,b)$ that contain a nondegenerate p-regular sequence. It follows that all of the p-regular sequences examined in this paper are nondegenerate.

On the other hand, we must take into account degenerate p-irregular sequences in $\mathcal{F}(a,b)$. For notational convenience we adopt the convention that $e(w) = \infty$ when w is degenerate, and consider the statement $r < e(w)$ to be true when $e(w) = \infty$. Note that a degenerate p-irregular second-order recurrence satisfies a first-order recurrence modulo p^r for all positive integers r.

The restricted periods of p-regular sequences are given by the following important theorem.

Theorem 2.4 (Theorem 2.11 of [1]): *Suppose that $w(a,b) \in \mathcal{F}(a,b)$ is p-regular and that $e = e(w)$ and $f = f(w)$ both exist. Let $e^* = \min(r,e)$, $f^* = \min(r,f)$, and $s = \lambda(p)/h(p)$. Then, for all positive integers r,*

$$h(p^r) = p^{r-e^*}h(p^e) \tag{2.2}$$

$$\lambda(p^r) = p^{r-f^*}\lambda(p^f) \quad \textit{and} \tag{2.3}$$

$$E(p^r) = \operatorname{ord}_{p^r}(M(p^r)) = \frac{\lambda(p^r)}{h(p^r)} = \frac{p^{r-f^*}\lambda(p)}{p^{r-e^*}h(p)} = p^{e^*-f^*}s. \tag{2.4}$$

The following theorem is analogue for p-irregular sequences. We note that both Theorem 2.5 and Corollary 2.6 remain true in the case that w is degenerate.

Theorem 2.5: *Let $w(a,b) \in \mathcal{F}(a,b)$ be a p-irregular recurrence and set $h'(p^r) = h_w(p^r)$, $e = e(u)$, and $e' = e(w)$. Let $\hat{r} = \max(r - e', 0)$. Then*

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

Theorem 2.5 has an important corollary that we require below.

Corollary 2.6: *If w, $w' \in \mathcal{F}(a,b)$ are p-irregular and satisfy $e(w) = e(w')$, then $h_w(p^r) = h_{w'}(p^r)$.*

Proof: It is clear from Theorem 2.5 that the restricted period depends only on $e(w)$ and the global parameters $h(p)$ and e.

The ratios of terms of recurrences (w) modulo p^r are closely related to multipliers and play a key role in our study. If a, b, c, and d are integers, with $p \not| b$ and $p \not| d$, then the quotients a/b and c/d may be viewed as elements of $\mathbf{Z}_p$, the localization of the integers at the prime ideal (p). It is then natural to define

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

In [1], the notation $\rho_w(n,m)$ was introduced to represent the ratio of elements w_{n+m} and w_n of a second-order recurrence sequence (w) when w_n was not divisible by p. We extend that notation to include the situation when the p-power dividing w_n does not exceed the p-power dividing w_{n+m}.

Definition 2.7: If $w(a,b) \in \mathcal{F}(a,b)$ and m and n are nonnegative integers such that $p^k \parallel w_n$ and $p^k \parallel w_{n+m}$, then we define $\rho(n,m) = \rho_w(n,m)$ to be the element $(w_{n+m}/p^k)/(w_n/p^k) \in \mathbf{Z}_p$.

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

$$M_w(p^r) \equiv \rho(n, h_w(p^r)) \pmod{p^r},$$
$$M_w^*(p^r) \equiv \rho(n, h_w^*(p^r)) \pmod{p^r}.$$

To make it convenient to refer to elements congruent to ratios modulo p^r, we introduce the mapping $\pi_r : \mathbf{Z}_p \to \mathbf{Z}/p^r\mathbf{Z}$, the canonical extension to $\mathbf{Z}_p$ of the quotient map $\pi : \mathbf{Z} \to \mathbf{Z}/p'\mathbf{Z}$.

We require the following three basic lemmas from [1] in our analysis below.

Lemma 2.8 (Lemma 3.3 of [1]): *Let $w(a,b) \in \mathcal{F}(a,b)$ 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 $h(p^\ell) \mid c$ 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 $\ell + m \geq r$. In particular, if w_i and w_j are p-regular, then $\rho_w(i,c) \equiv \rho_w(j,c)$ $\pmod{p^r}$ *if and only if $\ell + m \geq r$.*

Lemma 2.9 (Lemma 3.4) of [1]): *Let $w(a,b) \in \mathcal{F}(a,b)$ and $w'(a,b) \in \mathcal{F}(a,b)$ and fix a positive integer c. Let ℓ be the largest integer such that $h(p^\ell) \mid c$ and assume that $\ell < r$. If, for integers n and i,*

$$w'_{n+c}w_{n+i} - w_{n+i+c}w'_n \equiv 0 \quad (mod\ p^r), \tag{2.5}$$

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

Conversely, if $w'(a,b)$ is a **mot** *of $w(a,b)$ modulo $p^{r-\ell}$, then there exists an i such that (2.5) holds for all n.*

Lemma 2.10 (Lemma 2.13 of [1]): *Let $\mathcal{B}$ be a p^r-block of $\mathcal{F}(a,b)$ containing the sequence w. Then, up to congruence modulo p^r, $\mathcal{B}$ contains $p^{r-1}(p-1)h_w(p^r)$ distinct sequences.*

Finally, we require two tools to "lift" roots modulo p of the characteristic polynomial to roots modulo higher powers of p. When $\left(\frac{D}{p}\right) = 1$, the characteristic polynomial $f(x)$ has *nonsingular* roots, that is, roots that are not simultaneously roots of $f'(x)$. In this situation, each of the roots modulo p lifts to a unique root modulo each higher power of p. The required lifting theorem is Hensel's lemma, which we state here for reference.

Theorem 2.11 (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 [2]. □

When $\left(\frac{D}{p}\right) = 0$, the characteristic polynomial $f(x)$ has only one *singular* root modulo p, that is, the single root of $f(x)$ modulo p is simultaneously a root of $f'(x)$. In this case, the lifting of roots is governed by the following theorem.

Theorem 2.12: *Suppose that $f(x)$ is a polynomial with integral coefficients. If $f(m) \equiv 0 \pmod{p^i}$ and $f'(m) \equiv 0 \pmod{p}$, then $f(m+tp^i) \equiv f(m) \pmod{p^{i+1}}$. Furthermore, one of the following occurs*:

(a) *Each of the p distinct residues $m+tp^i \pmod{p^{i+1}}$, for $0 \leq t < p$, satisfy $f(m+tp^i) \equiv 0 \pmod{p^{i+1}}$.*

(b) *None of the residues $m+tp^i \pmod{p^{i+1}}$, for $0 \leq t < p$, satisfy $f(m+tp^i) \equiv 0 \pmod{p^{i+1}}$.*

Proof: See p. 88 of [2]. □

The lifting of singular roots of a polynomial $f(x)$ is more complicated than that of nonsingular roots and is best described by the *modulo p root tree of $f(x)$*.

Definition 2.13: The *modulo p root tree* of $f(x)$ is a tree whose nodes at the k-th level are labelled by the roots of $f(x)$ modulo p^k. The nodes at level $k+1$ are connected to the nodes at level k corresponding to the roots from which they are lifted. A *terminal* node of the root tree at the k-th level corresponds to a root modulo p^k that does not lift to a root modulo p^{k+1}.

For use below, we denote by n_k the number of *nonterminal* nodes of the modulo p root tree of $f(x)$ at the k-th level. In other words, $f(x)$ has exactly n_k roots modulo p^k that lift to roots modulo p^{k+1}.

The root tree may be finite or infinite: in the first case, all the nodes at some level of the root tree are terminal; in the second case, one of the roots modulo p lifts to a root modulo p^k for all k. The polynomials that concern us in this paper, the quadratic characteristic polynomials $f(x) = x^2 - ax + b$, have at most one singular root when $\left(\frac{D}{p}\right) = 0$, and consequently the root tree is connected with a single base node. We illustrate the root tree with two examples.

Example 2.14: Let $f(x) = x^2 - x - 1$, the characteristic polynomial of the Fibonacci family $\mathcal{F}(1,-1)$. Since $D = a^2 - 4b = 1 + 4 = 5 \equiv 0 \pmod{5}$, we see that $\left(\frac{D}{5}\right) = 0$ and $f(x)$ has a unique, singular root modulo 5, namely $m = 3$. However, since $f(3) = 5 \not\equiv 0 \pmod{25}$, this root does not lift to any root of $f(x)$ modulo 25. It follows that the root tree of $f(x)$ modulo 5 consists of only the base node.

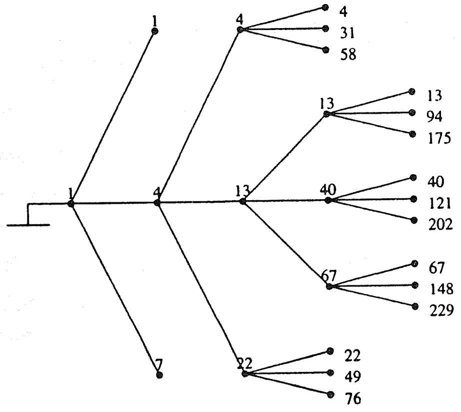

FIGURE 1. The Modulo 3 Root Tree of $f(x) = x^2 + x + 61$

Example 2.15: Let $f(x) = x^2+x+61$, the characteristic polynomial of the family $\mathcal{F}(-1,61)$. Since $D = 1-244 = -243 \equiv 0 \pmod 3$, we see that $f(x)$ has a unique singular root modulo 3, namely $m = 1$. Since $f(1) = 63 \equiv 0 \pmod 9$, Theorem 2.12 implies that the root 1 lifts to three distinct roots modulo 9, namely 1, 4, and 7. Thus the root tree of $f(x)$ modulo 3 has three nodes on the second level.

Since $f(1) = 63 \not\equiv 0 \pmod{27}$ and $f(7) = 117 \not\equiv 0 \pmod{27}$, neither 1 nor 7 lifts to a root of $f(x)$ modulo 27. However, $f(4) = 81 \equiv 0 \pmod{27}$, so Theorem 2.12 implies that the root 4 lifts to three roots of $f(x)$ modulo 27, namely 4, 13, and 22. We conclude that the root tree of $f(x)$ modulo 3 has three nodes on the third level.

Next, we observe that $f(4) \equiv f(13) \equiv f(22) \equiv 0 \pmod{81}$, so each of these roots lifts to three roots modulo 81. Clearly the root 4 lifts to 4, 31, and 58; 13 lifts to 13, 40, and 67; and 22 lifts to 22, 49, and 76. Therefore the root tree of $f(x)$ modulo 3 has nine nodes on the fourth level.

To compute the fifth level of the root tree, we observe that $f(x) \not\equiv 0 \pmod{243}$ when $x \in \{4, 31, 58, 22, 49, 76\}$ while $f(x) \equiv 0 \pmod{243}$ when $x \in \{13, 40, 67\}$. Therefore the roots 13, 40, and 67 each lift to three roots modulo 243, namely 13, 94, 175, 40, 121, 202, 67, 148, and 229. Thus the fifth level of the root tree has nine nodes.

Finally, it is easy to check that none of the nine roots of $f(x)$ modulo 243 lifts to a root modulo 729. Thus the root tree of $f(x)$ modulo 3 is finite with five levels. (See Figure 1.)

3. p-REGULAR BLOCKS

Our analysis of special multipliers requries a careful accounting of the number of p^r-blocks in $\mathcal{F}(a,b)$ having certain properties. For p-regular blocks, this accounting was performed in [1].

Theorem 3.1 (Corollary 2.17 of [1]): *Let $T_{\text{sing}}(p^r)$ and $T_{\text{reg}}(p^r)$ denote, respectively, the number of p-regular blocks in $\mathcal{F}(a,b)$ with and without p-singular terms. Then*

$$T_{\text{sing}}(p^r) = \frac{p^{r-1}h(p)}{h(p^r)} \quad \textit{and} \quad T_{\text{reg}}(p^r) = \frac{p^{r-1}(p - \left(\frac{D}{p}\right) - h(p))}{h(p^r)}. \tag{3.1}$$

4. p-IRREGULAR BLOCKS

Counting the number of p-irregular blocks in $\mathcal{F}(a,b)$ is somewhat more complicated, and requires examination of several cases. Note that the p-irregular sequences w in this section may be degenerate, in which case $e(w) = \infty$. By convention, the assertion that $e(w) > r$ includes the possibility that $e(w) = \infty$.

Lemma 4.1: *If $w \in \mathcal{F}(a,b)$ is p-irregular and $r \le e(w)$, then w lies in the same p^r-block as a sequence in $\mathcal{F}(a,b)$ that has initial terms 1, γ, where γ is congruent modulo p^r to a root of the characteristic polynomial $f(x) = x^2 - ax + b$.*

Proof: Since w is p-irregular and $r \le e(w)$, the sequence w is first-order modulo p^r. Moreover, since $w \in \mathcal{F}(a,b)$, we know that $p \not| (w_0, w_1)$, and therefore $p \not| w_0$. Choose ζ and $\gamma \in \mathbf{Z}$ to satisfy $\zeta \equiv w_0^{-1} \pmod{p^r}$ and $\gamma \equiv w_0^{-1}w_1 \pmod{p^r}$. Then the multiple ζw of the sequence w is first-order modulo p^r, satisfies the recurrence relation (2.1), and has initial terms 1, γ. It follows that $\gamma^2 \equiv a\gamma - b \pmod{p^r}$, and we see that $f(\gamma) \equiv 0 \pmod{p^r}$, as desired. □

Theorem 4.2: *Suppose $\mathcal{B}$ is a p-irregular p^r-block of $\mathcal{F}(a,b)$ and w, $w' \in \mathcal{B}$. Then either $e(w) = e(w') < r$ or $e(w)$, $e(w') \geq r$.*

Proof: First suppose that w, $w' \in \mathcal{B} \subseteq \mathcal{F}(a,b)$ and $r \leq e(w)$. Since $r \leq e(w)$ and w is p-irregular, it follows that w satisfies a first-order recurrence modulo p^r. Since w' lies in the same p^r-block as w, and, obviously, any multiple of a translation of a first-order recurrence is also a first-order recurrence, it is clear that w' is also first-order modulo p^r, and hence $r \leq e(w')$.

Next, suppose that w, $w' \in \mathcal{B} \subseteq \mathcal{F}$ and $r > e(w)$. Without loss of generality, we may assume that $e(w') \geq e(w)$. If $e(w') \geq r$, then w' is a first-order recurrence modulo p^r, and, since w belongs to the same p^r-block, w must also be first-order modulo p^r. But then $e(w) \geq r$, a contradiction. Thus, $r > e(w') \geq e(w)$.

Since $r > e(w')$, it is now clear that w and w' belong to the same $p^{e(w')}$-block. By definition of $e(w')$ and the fact that w' is p-irregular, we know that w' is first-order modulo $p^{e(w')}$. Therefore w is also first-order modulo $p^{e(w')}$, and hence $e(w) \geq e(w')$. We now conclude that $e(w) = e(w')$, as desired. □

The next two theorems provide an accounting of p-irregular p^r-blocks when $\left(\frac{D}{p}\right) = 1$, making extensive use of Hensel's lemma.

Theorem 4.3: *If $\left(\frac{D}{p}\right) = 1$, then there are exactly two distinct p-irregular p^r-blocks in $\mathcal{F}(a,b)$ that contain a sequence w with the property that $r \leq e_w$.*

Proof: Since $\left(\frac{D}{p}\right) = 1$, the characteristic polynomial $f(x) = x^2 - ax + b$ has two distinct roots in $\mathbf{Z}/p\mathbf{Z}$. Suppose that α, $\beta \in \mathbf{Z}$ project onto these distinct roots. It is easy to verify that $f'(\alpha) \not\equiv 0 \pmod{p}$ and $f'(\beta) \not\equiv 0 \pmod{p}$, as otherwise $\alpha \equiv \beta \equiv a/2 \pmod{p}$, and the roots are not distinct. By Hensel's lemma, applied repeatedly, the polynomial $f(x)$ has exactly two distinct roots modulo p^r. If we suppose now that α and $\beta \in \mathbf{Z}$ were chosen to project onto these distinct roots modulo p^r, then the two sequences w_α and w_β that satisfy the recursion (2.1) and have initial terms 1, α and 1, β, respectively, are p-irregular and first-order modulo p^r. Hence $e(w_\alpha) \geq r$ and $e(w_\beta) \geq r$. Moreover, it is clear that w_α and w_β lie in different p^r-blocks.

Conversely, if w is p-irregular with $e(w) \geq r$, then, by Lemma 4.1, w lies in the same p^r-block as w_α or (w_β), as desired. □

Theorem 4.4: *If $\left(\frac{D}{p}\right) = 1$ and $k < r$, then there are exactly $2p^{r-k-1}(p-1)/h_w(p^r)$ distinct p-irregular p^r-blocks in $\mathcal{F}(a,b)$ that contain a sequence w with the property that $e_w = k$.*

Proof: First we note that, by Corollary 2.6, $h_w(p^r)$ is independent of the choice of the sequence w.

Next, we count the number of sequences, up to congruence modulo p^r, in the set

$$\Omega_k = \{w \in \mathcal{F}(a,b) \mid w \text{ is } p\text{-irregular, } e(w) = k, \text{ and } w_0 \equiv 1 \pmod{p^r}\}.$$

If $w \in \Omega_k$, then w is first-order modulo p^k, but is *not* first order modulo p^{k+1}. Consequently, if $f(x) = x^2 - ax + b$ is the characteristic polynomial of w and $w_1 = \gamma$, then

$$f(\gamma) \equiv 0 \pmod{p^k} \quad \text{and} \tag{4.1}$$

$$f(\gamma) \not\equiv 0 \pmod{p^{k+1}}. \tag{4.2}$$

Since $\left(\frac{D}{p}\right) = 1$, the polynomial $f(x)$ has two distinct roots modulo p. By Hensel's lemma, there are exactly two residues modulo p^k that satisfy (4.1), and, again by Hensel's lemma, exactly $2(p-1)$ residues modulo p^{k+1} that satisfy both (4.1) and (4.2). It follows that there are $2p^{r-(k+1)}(p-1)$ residues modulo p^r that satisfy both (4.1) and (4.2).

On the other hand, if $w \in \mathcal{F}(a,b)$ has initial terms $1, \gamma$, where γ is congruent modulo p^r to one of the $2p^{r-(k+1)}(p-1)$ residues that satisfy both (4.1) and (4.2), then w satisfies (2.1) and is first-order modulo p^k, but is not first order modulo p^{k+1}. Thus $e(w) = k$ and $w \in \Omega_k$. It follows that Ω_k contains exactly $2p^{r-(k+1)}(p-1)$ sequences that are distinct modulo p^r.

Since the initial term w_0 of a p-irregular sequence in $\mathcal{F}(a,b)$ is invertible, it is clear that each p-irregular sequence in $\mathcal{F}(a,b)$ for which $e(w) = k$ is equivalent modulo p^r to one of the sequences in Ω_k. Moreover, the $\phi(p^r)$ multiples by an invertible element of $\mathbb{Z}/p^r\mathbb{Z}$ of each of the $2p^{r-(k+1)}(p-1)$ sequences in Ω_k are distinct modulo p^r. Thus there are exactly $2\phi(p^r)p^{r-(k+1)}(p-1) = 2p^{2r-k-2}(p-1)^2$ p-irregular sequences $w \in \mathcal{F}(a,b)$ that are distinct modulo p^r and satisfy $e(w) = k$.

Finally, by Lemma 2.10 and Corollary 2.6, every p^r-block of $\mathcal{F}(a,b)$ that contains a sequence w that is p-irregular and satisfies $e(w) = k$ contains $p^{r-1}(p-1)h_w(p^r)$ distinct sequences modulo p^r, and hence there are $2p^{r-(k+1)}(p-1)/h_w(p^r)$ such p^r-blocks. □

Finally, we examine the situation when $\left(\frac{D}{p}\right) = 0$. Again, our objective is to count the number of p-irregular p^r-blocks and the primary technique is to lift the roots of the characteristic polynomial. In this situation, however, the roots are singular, and the primary tool is Theorem 2.12 rather than Hensel's lemma.

As in the analysis when $\left(\frac{D}{p}\right) = 1$, we wish to count separately the p-irregular blocks that which contain a sequence w for which $e_w < r$ and those that which contain a sequence w for which $r \le e_w$. However, the computation here depends heavily on the parameters a and b. Consequently, our results will depend upon the structure of the modulo p root tree of the characteristic polynomial $f(x) = x^2 - ax + b$. In particular, the next two results depend upon the number of nonterminal nodes n_k at the k-th level of the root tree.

Theorem 4.5: *If $\left(\frac{D}{p}\right) = 0$ and n_{r-1} is the number of nonterminal nodes at level $r-1$ of the modulo p root tree of $f(x) = x^2 - ax + b$, then there are exactly pn_{r-1} distinct p-irregular p^r-blocks in $\mathcal{F}(a,b)$ that contain a sequence w with the property that $r \le e_w$.*

Proof: As in the proof of Theorem 4.3, the p-irregular p^r-blocks that contain a sequence w for which $r \le e_w$ correspond to the sequences w_α that satisfy the recursion (2.1) and have initial terms $1, \alpha$, where $\alpha \in \mathbb{Z}$ projects onto a root of $f(x)$ modulo p^r. The roots of $f(x)$ modulo p^r correspond to the nodes at the r-th level of the modulo p root tree.

By Theorem 2.12 each root of $f(x)$ modulo p^{r-1} either fails to lift to any root modulo p^r, or lifts to p distinct roots modulo p^r. By definition of n_{r-1}, the characteristic polynomial

$f(x)$ has exactly n_{r-1} roots modulo p^{r-1} that lift to roots modulo p^r. It follows that there are exactly pn_{r-1} distinct roots of $f(x)$ modulo p^r, and consequently, there are exactly pn_{r-1} distinct p-irregular p^r-blocks that contain a sequence w for which $r \leq e_w$. □

Theorem 4.6: *Suppose that* $\left(\frac{D}{p}\right) = 0$ *and* $k < r$. *Let* n_k *denote the number of nonterminal nodes at the* k*-th level of the modulo* p *root tree of* $f(x) = x^2 - ax + b$. *Then the number of distinct* p*-irregular* p^r*-blocks in* $\mathcal{F}(a,b)$ *that contain a sequence* w *with the property that* $e_w = k$ *is exactly*

(a) $(1-n_1)p^{r-1}/h_w(p^r)$, *if* $k = 1$, *and*

(b) $(pn_{k-1} - n_k)p^{r-k}/h_w(p^r)$, *if* $1 < k < r$.

Proof: As in the proof of Theorem 4.4, we first observe that, by Corollary 2.6, $h_w(p^r)$ is independent of the choice of the sequence w.

For each $k < r$, we let

$$\Omega_k = \{w \in \mathcal{F}(a,b) \mid w \text{ is } p\text{-irregular}, \ e(w) = k, \ \text{and } w_0 \equiv 1 \pmod{p^r}\}.$$

As in the proof of Theorem 4.4, if $w \in \Omega_k$, then w is first-order modulo p^k, but is *not* first order modulo p^{k+1}. Consequently, if $f(x) = x^2 - ax + b$ is the characteristic polynomial of w and $w_1 = \gamma$, then

$$f(\gamma) \equiv 0 \pmod{p^k} \quad \text{and} \tag{4.3}$$

$$f(\gamma) \not\equiv 0 \pmod{p^{k+1}}. \tag{4.4}$$

Therefore, γ corresponds to a node on level k of the modulo p root tree of $f(x)$, but not on level $k+1$, i.e., a terminal node on the k-th level of the root tree.

Suppose that $k = 1$. We know that there is a unique node at the first level of the root tree, corresponding to the unique root modulo p of the characteristic polynomial $f(x)$. Since n_1, which must be either 0 or 1, is the number of nodes that lift, there remain $(1 - n_1)$ terminal nodes, that is, $(1 - n_1)$ roots modulo p that satisfy both (4.3) and (4.4). It follows that there are $(1-n_1)p^{r-1}$ residues modulo p^r that satisfy both (4.3) and (4.4), and hence $|\Omega_1| = (1-n_1)p^{r-1}$.

Now suppose that $1 < k < r$. By Theorem 2.12 there are pn_{k-1} nodes at the k-th level of the modulo p root tree, and n_k of these lift. It follows that the k-th level of the root tree contains $(pn_{k-1} - n_k)$ terminal nodes. These nodes correspond to roots γ of $f(x)$ modulo p^k that satisfy both (4.3) and (4.4). Therefore there are $(pn_{k-1} - n_k)p^{r-k}$ distinct residues modulo p^r that satisfy both (4.3) and (4.4), and hence $|\Omega_k| = (pn_{k-1} - n_k)p^{r-k}$.

Since the initial term w_0 of a p-irregular sequence in $\mathcal{F}(a,b)$ is invertible, it is clear that each p-irregular sequence in $\mathcal{F}(a,b)$ for which $e(w) = k$ is equivalent modulo p^r to one of the sequences in Ω_k. Moreover, the $\phi(p^r)$ multiples by an invertible element of $\mathbf{Z}/p^r\mathbf{Z}$ of each of the sequences in Ω_k are distinct modulo p^r. Thus there are exactly $\phi(p^r)|\Omega_k \mid p$-irregular sequences $w \in \mathcal{F}(a,b)$ that are distinct modulo p^r and satisfy $e(w) = k$.

Finally, by Lemma 2.10 and Corollary 2.6, every p^r-block of $\mathcal{F}(a,b)$ that contains a sequence w that is p-irregular and satisfies $e(w) = k$ contains $p^{r-1}(p-1)h_w(p^r) = \phi(p^r)h_w(p^r)$ distinct sequences modulo p^r, and hence there are $|\Omega_k|/h_w(p^r)$ such p^r-blocks.

By substituting in the computed values of $|\Omega_k|$ for $k = 1$ and $1 < k < r$, we obtain the conclusion of the theorem. □

5. THE MAIN THEOREM

Theorem 5.1: *Suppose that $\mathcal{F}(a,b)$ contains a nondegenerate p-regular sequence and $r > e$. Let d be a nonnegative integer such that $d \equiv M(p^{r^*}) \pmod{p^{r^*}}$. Then there exists a recurrence $w(a,b) \in \mathcal{F}(a,b)$ and an index n such that $0 \leq n < h(p^{r-r^*})$ and*

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

Proof: If $w(a,b) \in \mathcal{F}(a,b)$, then for each p-regular term w_n, the ratio $\rho_w(n,h^*)$ satisfies

$$\rho_w(n,h^*) \equiv M(p^{r^*}) \pmod{p^{r^*}}.$$

There are exactly p^{r-r^*} residues t modulo p^r with the property that $t \equiv d \pmod{p^{r^*}}$. Consequently, if we can show that the residues $\pi_r(\rho_w(n,h^*)) \in \mathbb{Z}/p^r\mathbb{Z}$, corresponding to the ratios $\rho_w(n,h^*)$ arising from every p-regular term w_n of every sequence $w(a,b) \in \mathcal{F}(a,b)$, account for p^{r-r^*} distinct residues modulo p^r, then one ratio must satisfy the required congruence $\rho_w(n,h^*) \equiv d \pmod{p^r}$. To this end, we carefully enumerate the distinct residues modulo p^r that appear as ratios $\rho_w(n,h^*) (\bmod\ p^r)$ for sequences $w(a,b) \in \mathcal{F}$.

First observe that, by Lemma 2.8, the ratios $\rho_w(n,h^*)$ are distinct modulo p^r for $0 \leq n < h(p^{r-r^*})$. Second, by Lemma 2.9,

$$\{\pi_r(\rho_w(n,h^*)) \mid 0 \leq n < (p^{r-r^*})\} = \{\pi_r(\rho_{w'}(n,h^*)) \mid 0 \leq n < h(p^{r-r^*})\}$$

when w and w' lie in the same block modulo p^{r-r^*}, while

$$\{\pi_r(\rho_w(n,h^*)) \mid 0 \leq n < (p^{r-r^*})\} \cap \{\pi_r(\rho_{w'}(n,h^*)) \mid 0 \leq n < h(p^{r-r^*})\} = \phi$$

when $w(a,b)$ and $w'(a,b)$ lie in different blocks modulo p^{r-r^*}. Thus we may narrow our analysis to one sequence from each p^{r-r^*}-block of $\mathcal{F}(a,b)$.

If $w(a,b)$ contains no p-singular elements, then the ratios $\{\rho_w(n,h^*) \mid 0 \leq n < h(p^{r-r^*})\}$ account for $h(p^{r-r^*})$ distinct residues modulo p^r. On the other hand, suppose that $w(a,b)$ contains p-singular terms. Clearly every cycle in the same block as $w(a,b)$ has the same number of p-singular terms, and without loss of generality, we may assume that w_0 is p-singular. Then w_m is p-singular if and only if $h(p) \mid m$. Consequently, one restricted period of $w(a,b)$ contains $h(p^{r-r^*})/h(p)$ p-singular terms and $h(p^{r-r^*}) - h(p^{r-r^*})/h(p)$ p-regular terms. As noted above, these p regular terms w_m give rise to distinct ratios $\rho_w(m,h^*)$ modulo p^r, and hence the block of $w(a,b)$ contributes $h(p^{r-r^*}) - h(p^{r-r^*})/h(p)$ ratios modulo p^r.

We can now apply Theorem 3.1 to count the distinct special multipliers that arise from sequences in the p-regular p^{r-r^*}-blocks of $\mathcal{F}(a,b)$. The number of distinct ratios $\rho_w(n,h^*)$ modulo p^r is:

$$\begin{aligned} &T_{\text{reg}}(p^{r-r^*}) \cdot h(p^{r-r^*}) + T_{\text{sing}}(p^{r-r^*}) \cdot \left(h(p^{r-r^*}) - \frac{h(p^{r-r^*})}{h(p)}\right) \\ &\qquad = \left(T_{\text{reg}}(p^{r-r^*}) + T_{\text{sing}}(p^{r-r^*})\right) h(p^{r-r^*}) - T_{\text{sing}}(p^{r-r^*}) - \left(\frac{h(p^{r-r^*})}{h(p)}\right) \qquad (5.1) \\ &\qquad = p^{r-r^*-1}\left(p - \left(\frac{D}{p}\right)\right) - p^{r-r^*-1}. \end{aligned}$$

To complete the proof, we count the number of distinct special multipliers that arise from sequences in the p-irregular p^{r-r^*}-blocks. We break the analysis into three cases corresponding to $\left(\frac{D}{p}\right) = -1, 1$, and 0.

Case 1: $\left(\frac{D}{p}\right) = -1$.

If $\left(\frac{D}{p}\right) = -1$, (5.1) yields p^{r-r^*} distinct ratios, and the argument is complete.

Case 2: $\left(\frac{D}{p}\right) = 1$.

Assume that $\left(\frac{D}{p}\right) = 1$. Then (5.1) yields $p^{r-r^*} - 2p^{r-r^*-1}$ distinct ratios arising from the p-regular p^{r-r^*}-blocks. To complete the argument, we counnt the distinct ratios arising from sequences in the p-irregular p^{r-r^*}-blocks.

If $\mathcal{B}$ is a p-irregular p^{r-r^*}-block of $\mathcal{F}(a,b)$ that contains a sequence w for which $e(w) \geq r - r^*$ then, by Theorem 2.5, $h_w(p^{r-r^*}) = 1$ and the block $\mathcal{B}$ contributes only one additional ratio, $\rho(0,1)$. Since, by Theorem 4.3, there are exactly two such blocks, these blocks contribute two additional ratios.

If $\mathcal{B}$ is a p^{r-r^*}-block containing a sequence w for which $e(w) = k < r - r^*$, then w contributes $h_w(p^{r-r^*})$ additional ratios. By Theorem 4.4, there are exactly $2p^{r-r^*-k-1}(p-1)/h_w(p^{r-r^*})$ such p^{r-r^*}-blocks, and therefore these blocks contribute

$$\frac{2p^{r-r^*-k-1}(p-1)}{h_w(p^{r-r^*})} \cdot h_w(p^{r-r^*}) = 2p^{r-r^*-k-1}(p-1)$$

additional ratios. If we sum over all possible values of k, i.e., $1 \leq k < r - r^*$, we obtain

$$\begin{aligned}\sum_{k=1}^{r-r^*-1} 2p^{r-r^*-k-1}(p-1) &= 2(p-1)\sum_{k=1}^{r-r^*-1} p^{r-r^*-1-k} \\ &= 2(p-1)\frac{p^{r-r^*-1}-1}{p-1} = 2p^{r-r^*-1} - 2 \qquad (5.2)\end{aligned}$$

additional ratios.

Combining the new ratios obtained from the p-irregular p^{r-r^*}-blocks with those obtained from the p-regular p^{r-r^*}-blocks yields $p^{r-r^*} - 2p^{r-r^*-1} + 2p^{r-r^*-1} - 2 + 2 = p^{r-r^*}$ ratios, as desired.

Case 3: $\left(\frac{D}{p}\right) = 0$.

Assume that $\left(\frac{D}{p}\right) = 0$. Then (5.1) yields $p^{r-r^*} - p^{r-r^*-1}$ distinct ratios arising from the p-regular p^{r-r^*}-blocks. As in the previous case, we complete the argument by counting the distinct ratios arising from sequences in the p-irregular p^{r-r^*}-blocks.

As usual, for each k satisfying $1 \leq k \leq r$, let n_k represent the number of nonterminal nodes at the k-th level of the modulo p root tree of the characteristic polynomial $f(x) = x^2 - ax + b$.

If $\mathcal{B}$ is a p-irregular p^{r-r^*}-block of $\mathcal{F}(a,b)$ that contains a sequence w for which $e(w) \geq r - r^*$ then, by Theorem 2.5, $h_w p^{(r-r^*)} = 1$ and the block $\mathcal{B}$ contributes only one additional ratio, $\rho(0,1)$. Since, by Theorem 4.5, there are exactly pn_{r-r^*-1} such blocks, these blocks contribute pn_{r-r^*-1} ratios.

If $\mathcal{B}$ is a p-irregular p^{r-r^*}-block that contains a sequence w for which $e(w) = k < r - r^*$, then w contributes $h_w p^{(r-r^*)}$ additional ratios. Theorem 4.6 implies that there are exactly $(1-n_1)p^{r-r^*-1}/h_w(p^{r-r^*})$ such p^{r-r^*}-blocks when $k = 1$ and $(pn_{k-1} - n_k)p^{r-r^*-k}/h_w(p^{r-r^*})$ such p^{r-r^*}-blocks when $1 < k < r - r^*$. Therefore the number of additional ratios contributed by these blocks is

$$\frac{(1-n_1)p^{r-r^*-1}}{h_w(p^{r-r^*})} \cdot h_w(p^{r-r^*}) = p(1-n_1)p^{r-r^*-1}, \qquad \text{when } k = 1$$

$$\frac{(pn_{k-1} - n_k)p^{r-r^*-k}}{h_w(p^{r-r^*})} \cdot h_w(p^{r-r^*}) = (pn_{k-1} - n_k)p^{r-r^*-k}, \qquad \text{when } k > 1.$$

If we sum over all possible values of k, i.e., $1 \leq k < r - r^*$, we obtain a simple telescoping sum:

$$\begin{aligned}(1-n_1)p^{r-r^*-1} &+ \sum_{k=2}^{r-r^*-1} (pn_{k-1} - n_k)p^{r-r^*-k} \\ &= (1-n_1)p^{r-r^*-1} + (pn_1 - n_2)p^{r-r^*-2} + \cdots + (pn_{r-r^*-2} - n_{r-r^*-1})p \\ &= p^{r-r^*-1} - pn_{r-r^*-1}.\end{aligned}$$

Adding the count of new ratios obtained from the p irregular p^{r-r^*}-blocks to that obtained from the p-regular p^{r-r^*}-blocks yields $p^{r-r^*} - p^{r-r^*-1} + pn_{r-r^*-1} + p^{r-r^*-1} - pn_{r-r^*-1} = p^{r-r^*}$ ratios, as desired. □

ACKNOWLEDGMENTS

Portions of this work were completed while the second author, Walter Carlip, was a visiting Scholar at the University of Chicago. He would like to thank the University of Chicago 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] Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery. *An Introduction to the Theory of Numbers*. Fifth edition, John Wiley & Sons Inc., New York, 1991.

AMS Classification Numbers: 11B39, 11B50, 11A07, 11B37

✠✠✠