SPECIAL MULTIPLIERS OF kth-ORDER LINEAR RECURRENCES MODULO p^r

Lawrence Somer

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

e-mail: somer@cua.edu

(Submitted January 2005-Final Revision March 2006)

ABSTRACT

The author has previously generalized the concept of a multiplier of a second-order linear recurrence modulo p^r, where p is an odd prime and r is a positive integer, to that of a special multiplier of a second-order linear recurrence modulo p^r. In this paper, we will extend these results to show that infinitely many kth-order linear recurrences have special multipliers modulo p^r, where $k \geq 2$ and p is a prime, not necessarily odd.

1. INTRODUCTION

In [1], [2], and [8], Somer generalized the concept of a multiplier of a second-order linear recurrence modulo p^r, where p is an odd prime and $r \geq 1$, to that of a special multiplier of a second-order linear recurrence modulo p^r. Special multipliers modulo p^r were used in [1] to investigate the distribution of residues in second-order recurrences reduced modulo p^r. In this paper, we will extend these results to show that infinitely many kth-order linear recurrences satisfying certain conditions have special multipliers modulo p^r, where $k \geq 2$ and p is a prime, not necessarily odd. Throughout this paper, p will denote a rational prime.

2. PRELIMINARIES

Let $k \geq 2$ and let $w(a_1, a_2, \ldots, a_k) = (w)$ be a kth-order linear recurrence satisfying the recursion relation

$$w_{n+k} = a_1 w_{n+k-1} - a_2 w_{n+k-2} + \cdots + (-1)^{k+1} a_k w_n, \tag{2.1}$$

where the parameters $a_1, \ldots, a_k$ and initial terms $w_0, \ldots, w_{k-1}$ are all rational integers. We will assume throughout this paper that $w(a_1, \ldots, a_k)$ is a *regular* recurrence, that is, $w(a_1, \ldots, a_k)$ satisfies no linear recursion relation of order less than k. We will distinguish one particular recurrence, the unit sequence satisfying the recursion relation (2.1) and having initial terms $u_0 = u_1 = \cdots = u_{k-2} = 0,\ u_{k-1} = 1$.

Associated with $w(a_1, \ldots, a_k)$ is the characteristic polynomial

$$f(x) = x^k - a_1 x^{k-1} + \cdots + (-1)^k a_k = \prod_{i=1}^{t} (x - \alpha_i)^{m_1}, \tag{2.2}$$

where the distinct characteristic roots α_i appear with multiplicity m_i for $i = 1,\ 2, \ldots, t$. We let D be the discriminant of $f(x)$. We further let $\mathcal{K} = \mathbb{Q}(\alpha_1, \ldots, \alpha_t)$ be the Galois field associated with $f(x)$, i.e., the splitting field of the characteristic roots of $f(x)$, and let R be the ring of integers of $\mathcal{K}$. Note that $\alpha \in R$ for $1 \leq i \leq t$. In this paper, we will also be considering recurrences $w'(a_1, \cdots, a_k)$ satisfying the recursion relation (2.1), but having initial terms $w'_0, \ldots, w'_{k-1}$ in R and not necessarily just in $\mathbb{Z}$. We also let

$$\hat{f}(x) = \prod_{i=1}^{t}(x - \alpha_i) \tag{2.3}$$

be the square-free kernel of $f(x)$. Then the coefficients of $\hat{f}(x)$ are rational integers. We let the discriminant of $\hat{f}(x)$ be denoted by $\hat{D}$. If $t = 1$, we let $\hat{D} = 1$. We let (p) denote the principal ideal in R generated by p.

We will assume throughout this article that $a_k \neq 0$ and $gcd(a_k, p^r) = 1$. Then it is known (see [3, pp. 344-345]) that $w(a_1, \ldots, a_k)$ is purely periodic modulo p^r. The *period* $\lambda(p^r)$ of (w) modulo p^r is the least positive integer λ such that

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

for all n. Any positive integer m such that $w_{n+m} \equiv w_n \pmod{p^r}$ for all n is called a *general period* of (w) modulo p^r. Clearly, if m is a general period of (w) modulo p^r, then $\lambda(p^r)|m$.

In [3, pp. 345-355], R. D. Carmichael generalized the concept of the period $\lambda(p^r)$ of (w) modulo p^r to that of the *restricted period* $h(p^r)$ of (w) modulo p^r. He defined $h(p^r)$ to be the least positive integer h such that for some integer M, coprime to p, and for all n

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

The integer $M = M(p^r)$, defined up to congruence modulo p^r, is called the multiplier of (w) modulo p^r. Any positive integer c such that $w_{n+c} \equiv G w_n \pmod{p^r}$ for some integer G and all n is called a *general restricted period* of (w) modulo p^r, and G is called a *general multiplier* of (w) modulo p^r. If c is a general restricted period of (w) modulo p^r, then $h(p^r)|c$. It was shown in [3, pp. 345-355] that $h(p^r)|\lambda(p^r)$ and that $E(p^r) = \lambda(p^r)/h(p^r)$ is the multiplicative order in $(\mathbb{Z}/p\mathbb{Z})^*$ of the multiplier $M(p^r)$. Moreover, if $h = h(p^r)$ and $M = M(p^r)$, then, for all n,

$$w_{n+ih} \equiv M^i w_n \pmod{p^r}. \tag{2.4}$$

Thus, every general multiplier G satisfies $G \equiv M^i \pmod{p^r}$ for some i, and the general multipliers of (w) modulo p^r form a cyclic group of order $E(p^r)$ in $(\mathbb{Z}/p\mathbb{Z})^*$.

Given the prime p, we define the positive integer $e(p) = e$ as follows. If p is an odd prime, we define e to be the largest integer, if it exists, such that $h(p^e) = h(p)$. If $p = 2$, we let e be the largest integer, if it exists, such that $h(2^2) = h(2^e)$. If e does not exist, we write informally that $e = \infty$. We will give conditions shortly that show that it is usual that $e < \infty$.

As was pointed out in [1], restricted periods and multipliers may be viewed from another perspective. If $h = h(p^r)$ and $M = M(p^r)$, then for every n the sequence (w^*) defined by $w^*_m = w_{n+mh}$ satisfies the first-order recursion relation $w^*_{m+1} \equiv M w^*_m \pmod{p^r}$. Thus, the restricted period modulo p^r can be characterized as the smallest positive integer h such that for all n, the subsequence $\{w_{n+mh}\}_{m=0}^{\infty}$ satisfies the same first-order recursion relation modulo p^r.

It may occur, however, that for a fixed n, there exists a nonnegative integer $g < h$ such that the subsequence defined by $w^*_m = w_{n+mg}$ satisfies a first-order recursion relation $w^*_{m+1} \equiv M^* w^*_m \pmod{p^r}$. We will be interested in this phenomenon when $g = h(p^c)$ for some positive integer $c < r$ and $h(p^c) < h(p^r)$, where $h(p^c)$ and $h(p^r)$ are restricted periods of (w). (In this case, g becomes a restricted period when (w) is reduced modulo p^c.) Since $h(p) = h(p^2) = \cdots = h(p^e)$ when p is an odd prime and $h(p^2) = h(p^3) = \cdots = h(p^e)$ when $p = 2$, we will assume that $r > e$. This motivates the following definition.

Definition 2.1: *Let $w(a_1, \ldots, a_k)$ be a kth-order recurrence and p be a prime. For fixed integers $n \geq 0$, $r > e$, and c such that $e \leq c < r$, we call $h(p^c) = h'$ a general special restricted period of (w) with respect to w_n modulo p^r if $h(p^c) < h(p^r)$ and the sequence $w_m^* = w_{n+mh'}$ satisfies a first-order recursion relation $w_{m+1}^* \equiv M^* w_m^*$ (mod p^r) for some rational integer M^*. The integer $M^* = M^*(n, h(p^c), p^r)$ (defined up to congruence modulo p^r) is called a general special multiplier of (w) with respect to w_n modulo p^r. If c is the least positive integer greater than or equal to e such that $h(p^c)$ is a general special restricted period of (w) with respect to w_n modulo p^r, then $h(p^c)$ is called the principal special restricted period of (w) with respect to w_n modulo p^r.*

We note that if $e \leq c < r$, $h' = h(p^c)$, and $w_n \not\equiv 0 (\text{mod } p)$, then $M^*(n, h(p^c), p^r) \equiv w_{n+h'} w_n^{-1}$ (mod p^r).

Example 2.2: *Consider the Fibonacci sequence $u(1, -1)$. Here $h(3^4) = 108$ and $M(3^4) \equiv 80$ (mod 3^4). Let $h^* = h(3^2) = 12$ and $h' = h(3) = 4$. We note that if $u_i^* = u_{1+h^*i} = u_{1+12i}$, then $u_{i+1}^* \equiv 71 u_i^*$ (mod 3^4), while if $u_i' = u_{1+h'i} = u_{1+4i}$, then (u_i') does not satisfy a first-order recursion relation modulo 2^4. Hence, $h(3^2) = 12$ is the principal special restricted period of $u(1, -1)$ with respect to u_1 modulo 3^4, while*

$$M^*(1, h(3^2), 3^4) = M^*(1, 12, 81) \equiv 71 \ (mod\ 3^4)$$

is the principal special multiplier of (u) with respect to u_1(mod 3^4).

We further observe that if $h'' = h(3^3) = 36$ and $u_i'' = u_{1+h''i} = u_{1+36i}$, then $u_{i+1}'' \equiv 53$ (mod 3^4). Thus, $h(3^3) = 36$ is a nonprincipal general special restricted period of (u) with respect to u_1 (mod 3^4) and

$$M^*(1, h(3^3), 3^4) = M^*(1, 36, 81) \equiv 53 \ (mod\ 3^4)$$

is a nonprincipal general special multiplier of (u) with respect to u_1 (mod 3^4). Since $h(3^3) = 3 \cdot h(3^2)$, it follows from (2.4) that

$$M^*(1, h(3^3), 3^4) \equiv 53 \equiv [M^*(1, h(3^2), 3^4)]^3 \equiv 71^3 \ (\text{mod } 3^4).$$

Before presenting our main theorem, we will need some results and definitions concerning regular and p-regular recurrences. Given the recurrence $w(a_1, \ldots, a_k)$, we define the kth-order determinant

$$A_n(w) = \begin{vmatrix} w_n & w_{n+1} & \cdots & w_{n+k-1} \\ w_{n+1} & w_{n+2} & \cdots & w_{n+k} \\ \cdots & \cdots & \cdots & \cdots \\ w_{n+k-1} & w_{n+k} & \cdots & w_{n+2k-2} \end{vmatrix}. \tag{2.5}$$

It is known that $w(a_1, \ldots, a_k)$ is regular if and only if $A_0(w) \neq 0$. By Heymann's theorem [4, Chapter 12.12],

$$A_n(w) = a_k^n A_0(w). \tag{2.6}$$

Given the prime p, the recurrence (w) is called *p-regular* if

$$gcd(A_0(w), p) = 1. \tag{2.7}$$

We note that $w(a_1, \ldots, a_k)$ is p-regular if and only if (w), when reduced modulo p, does not satisfy a recursion relation of order less than k. Notice that by (2.6), if $w(a_1, \ldots, a_k)$ is p-regular, then $A_n(w) \not\equiv 0 \pmod p$ for all $n \geq 0$. We observe that $A_0(u) = (-1)^{k(k-1)/2}$, and thus, $u(a_1, \ldots, a_k)$ is p-regular for all primes p. If $w'(a_1, \ldots, a_k)$ is a recurrence satisfying (2.1) with initial terms $w'_0, \ldots, w'_{k-1}$ in R such that $gcd((A_0(w')), (p)) = (1)$, we say that (w') is (p)-regular, where $(A_0(w'))$ and (p) are principal ideals in R.

Let $w(a_1, \ldots, a_k)$ be p-regular and $w'(a_1, \ldots a_k)$ be any other recurrence satisfying (2.1) with initial terms $w'_0, w'_1, \ldots, w'_{k-1}$ in R and not necessarily (p)-regular. Then (2.7) together with Cramer's rule imply the existence of algebraic integers $c_0, c_1, \ldots, c_{k-1}$ in R (which are all in $\mathbb{Z}$ if $w'_0, \ldots, w'_{k-1}$ are all in $\mathbb{Z}$) such that

$$\begin{array}{ccccccccc}
c_0w_0 & + & c_1w_1 & + & \ldots & + & c_{k-1}w_{k-1} & \equiv & w'_0 \pmod{(p^r)} \\
c_0w_1 & + & c_1w_2 & + & \ldots & + & c_{k-1}w_k & \equiv & w'_1 \pmod{(p^r)} \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
c_0w_{k-1} & + & c_1w_k & + & \ldots & + & c_{k-1}w_{2k-2} & \equiv & w'_{k-1} \pmod{(p^r)}.
\end{array}$$

It now follows by the recursion relation defining both $w(a_1, \ldots, a_k)$ and $w'(a_1, \ldots, a_k)$ that for all n,

$$w'_n \equiv c_0w_n + c_1w_{n+1} + \cdots + c_{k-1}w_{n+k-1} \pmod{(p^r)}.$$

Therefore, $w'(a_1, \ldots, a_k)$ has the period, restricted period, and multiplier modulo p^r of the p-regular recurrence $w(a_1, \ldots, a_k)$ as a general period, general restricted period, and general multiplier modulo (p^r), respectively. Moreover, it follows that all p-regular recurrences have the same period, restricted period, and multiplier modulo p^r. Further, all p-regular recurrences therefore have the same value for $e(p)$.

We say that the recurrence $w(a_1, \ldots, a_k)$ is *degenerate* if α_i/α_j is a root of unity for some pair of distinct characteristic roots α_i and α_j, where $1 \leq i < j \leq t$. Let p be an odd prime. Since $u(a_1, \ldots, a_k)$ is p-regular for all odd primes p, it follows that if $w(a_1, \ldots, a_k)$ is any p-regular recurrence, then $e(p) = \infty$ if and only if $u_{h(p)+i} = 0$ for $i = 0, 1, \ldots, k-2$. By Corollary C.1 on page 38 of [5], this occurs only if $w(a_1, \ldots, a_k)$ is a degenerate sequence. (Note that $u(a_1, \ldots, a_k)$ is also then degenerate.)

The following theorem determines the value of $h(p^r)$ for p-regular recurrences $w(a_1, \ldots, a_k)$ in terms of $h(p^e)$ when $r \geq e$.

Theorem 2.3: *Let $w(a_1, \ldots, a_k)$ be a p-regular recurrence for which $e(p) < \infty$. Suppose that $r \geq e$. Then $h(p^r) = p^{r-e}h(p^e)$.*

Proof: This is proved in Theorem 1.5.18 on pages 24-25 of [6]. □

3. THE MAIN THEOREM

Theorem 3.1: *Let $k \geq 2$ and let $w(a_1, \ldots, a_k)$ be a nondegenerate regular recurrence with $a_k \neq 0$, initial terms $w_0, \ldots, w_{k-1}$ all in $\mathbb{Z}$, and distinct characteristic roots $\alpha_1, \ldots, \alpha_t$. Let the multiplicity of α_i be m_i $(1 \leq i \leq t)$ and suppose that $m_1 \leq 2$ and $m_2 = m_3 = \cdots = m_t = 1$.*

Let p be a rational prime such that $p \not| a_k A_0(w)$. If $k \geq 3$, suppose further that $p \not| \hat{D}$. Then (w) is p-regular, purely periodic modulo p^r, and $e(p) < \infty$. Suppose that $r > e$. Let $r^* = \max(\lceil r/2 \rceil, e)$. Suppose that n is a fixed nonnegative integer such that $w_n \not\equiv 0 \pmod p$.

Then $h(p^{r^*}) = h^*$ is a general special restricted period of (w) with respect to w_n modulo p^r and

$$M^*(n, h(p^{r^*}), p^r) \equiv w_{n+h^*} w_n^{-1} \pmod{p^r}$$

is a general special multiplier of (w) with respect to w_n modulo p^r.

Moreover, if $k = 2$, then $h(p^{r^*})$ is the principal special restricted period of (w) with respect to w_n modulo p^r and $M^*(n, h(p^{r^*}), p^r)$ is the principal multiplier of (w) with respect to w_n modulo p^r.

Example 3.2: *When $k \geq 3$ and $r > e$, we shall see below that while Theorem 3.1 guarantees that if $w(a_1, \ldots, a_k)$ is a p-regular recurrence and $w_n \not\equiv 0 \pmod p$, then $h(p^{r^*})$ is a general special restricted period of (w) with respect to w_n modulo p^r, it sometimes happens that $h(p^{r^*})$ might not be the principal restricted period. We will also present an example in which $h(p^{r^*})$ is the principal restricted period of (w) with respect to w_n modulo p^r.*

For both examples, we consider the 5-regular unit sequence $u(4, 1, -6)$ modulo 5^3. Then $e(5) = 1$ and $r^* = 2$. We note that $u(4, 1, -6)$ has the characteristic polynomial

$$f(x) = x^3 - 4x^2 + x + 6 = (x+1)(x-2)(x-3)$$

and that $D = \hat{D} = 144$. By Theorem 3.1, $h(5^{r^*}) = h(5^2) = 20$ is a general restricted period of (u) with respect to $u_2 \equiv 1$ modulo 5^3 and

$$M^*(2, h(5^2), 5^3) = M^*(2, 20, 125) \equiv u_{22} u_2^{-1} \equiv 51(1^{-1}) \equiv 51 \pmod{125}$$

is a general special multiplier of (u) with respect to u_2 modulo 5^3. However, by inspection, one sees that $h(5) = 4$ is the principal special restricted period with respect to u_2 modulo 5^3 and

$$M^*(3, h(5^2), 5^3) = M^*(3, 20, 125) \equiv u_{23} u_3^{-1} \equiv 4(4^{-1}) \equiv 1 \pmod{125}$$

is the principal special multiplier of (u) with respect to u_3 modulo 5^3.

From looking at numerous examples, it appears that for $k \geq 3, h(p^{r^*})$ is usually the principal special restricted period of $w(a_1, \ldots, a_k)$ with respect to w_n modulo p^r, but we have no proof of this.

4. NECESSARY LEMMAS

Before proving Theorem 3.1, we will need the following lemmas.

Lemma 4.1: *Let $w(a_1, \ldots, a_k)$ be a regular recurrence with $a_k \neq 0$ and distinct characteristic roots α_i with multiplicity m_i $(1 \leq i \leq t)$. Let*

$$b = \max_{1 \leq i \leq t} (m_i - 1).$$

Let p be a rational prime such that $p > b$ and $p \not| a_k \hat{D}$.

(a) There exist uniquely determined polynomials $f_i \in \mathcal{K}[x]$ *of degree less than* m_i $(i = 1, 2, \ldots, t)$ *such that*

$$w_n = \sum_{i=1}^{t} f_i(n)\alpha_i^n. \tag{4.1}$$

Moreover, each of the coefficients of $f_i(n)$ *can be expressed as a fraction* r_1/r_2*, where* $r_1, r_2 \in R$*, and the prime ideal* P *divides* r_2 *only if*

$$P \mid b!\alpha_1\alpha_2 \ldots \alpha_t \prod_{1 \le i < j < t} (\alpha_i - \alpha_j). \tag{4.2}$$

(b) There exist polynomials F_i *of degree less than* m_i $(1 \le i \le t)$ *with coefficients which are well-defined elements of the quotient ring* $R/(p^r)$ *such that*

$$w_n \equiv \sum_{i=1}^{t} F_i(n)\alpha_i^n \ (mod\ (p^r)). \tag{4.3}$$

(c) Let f_i *be a polynomial with coefficients in* $\mathcal{K}$ *of degree less than* m_i $(i = 1, 2, \ldots, t)$*. Let* $\{w'_n\}_{n=0}^{\infty}$ *be a sequence defined by*

$$w'_n = \sum_{i=1}^{t} f_i(n)\alpha_i^n. \tag{4.4}$$

Then (w') *satisfies the same recursion relation (2.1) as* $w(a_1, \ldots, a_k)$*.*

Proof: (a) The unique expression of (w) as given in (4.1) is proved in [5, Theorem C.1(a), pp. 33-34]. The expression of the coefficients of $f_i(n)$ as a fraction in $\mathcal{K}$ of the form r_1/r_2, where $r_1, r_2 \in R$, is determined by means of a partial fraction decomposition and by making use of the binomial theorem for negative integral exponents. By examining this proof, one sees that the only prime ideals in R which can possibly divide the denominators of the coefficients of f_i for $1 \le i \le t$ are those dividing

$$b!\alpha_1\alpha_2 \cdots \alpha_t \prod_{1 \le i < j < t} (\alpha_i - \alpha_j). \tag{4.5}$$

(b) By part (a), there exist polynomials f_i $(1 \le i \le t)$ such that

$$w_n = \sum_{i=1}^{t} f_i(n)\alpha_i^n, \tag{4.6}$$

where $deg(f_i(n)) < m_i$ and the coefficients of f_i can be expressed in the form r_1/r_2, where $r_1, r_2 \in R$ and the only prime ideals dividing r_2 are those dividing

$$b!\alpha_1\alpha_2 \cdots \alpha_t \prod_{1 \le i < j < t} (\alpha_i - \alpha_j).$$

Since $p > b,\ p \nmid a_k = \alpha_1^{m_1}\alpha_2^{m_2}\cdots\alpha_t^{m_t}$, and $p \nmid \hat{D} = \prod_{1\le i<j<t}(\alpha_i-\alpha_j)^2,\ r_2^{-1}$ exists in the quotient ring $R/(p^r)$. Reducing equation (4.6) modulo (p^r), the assertion is proved.

(c) This is proved in Theorem C.1(b) on pages 33-34 of [5]. □

Remark 4.2: *We note that in the proof of Lemma 4.1, we do not necessarily assume unique factorization in R, but we make use of the unique factorization of ideals in R as a product of prime ideals.*

In part (b) of Lemma 4.1, we talk about the coefficients of $F_i(n)$ in (4.3) being well-defined in the quotient ring $R/(p^r)$. We give an example in which the coefficients of $F_i(n)$ are not well-defined in $R/(p^r)$, and, in fact, w_n reduced modulo (p^r) cannot be expressed in the form given in congruence (4.3). Consider the Fibonacci sequence $u(1,-1)$ modulo (p^r), where $p=5$ and $r=2$. Then $\alpha_1=(1+\sqrt{5})/2,\ \alpha_2=(1-\sqrt{5})/2$, and $\alpha_1-\alpha_2=\sqrt{5}$. By the Binet formula,

$$u_n = \frac{1}{\sqrt{5}}\alpha_1^n - \frac{1}{\sqrt{5}}\alpha_2^n \tag{4.7}$$

if $\alpha_1 \ne \alpha_2$ and

$$u_n = n\alpha^{n-1} \tag{4.8}$$

if $\alpha_1=\alpha_2$. Note that

$$gcd((\alpha_1-\alpha_2),(5^2)) = gcd((\sqrt{5},(5^2)) = (\sqrt{5}) \ne (1). \tag{4.9}$$

However, $\sqrt{5}^{-1}$ is not well-defined modulo (5^2). Thus, (4.7) cannot hold as a congruence modulo (5^2), and by inspection, (4.8) is not satisfied for all n as a congruence modulo (5^2). In particular, we obtain

$$u_2 \equiv 2\alpha^1 \equiv 1+\sqrt{5} \equiv 1 \ (mod\ (25)).$$

This implies that $\sqrt{5}\equiv 0\ (mod\ (25))$, which is a contradiction. We note on the other hand that although $gcd((\alpha_1-\alpha_2),(5)) = (\sqrt{5}) \ne (1)$, we can express u_n modulo (5) by means of the congruence

$$u_n \equiv n\alpha^{n-1} \equiv n[(1+\sqrt{5})2^{-1}]^{n-1} \equiv n[(1+0)2^{-1}]^{n-1} \equiv n3^{n-1} \equiv 3^{-1}n3^n \ (mod\ (5)).$$

Lemma 4.3: *Let $w(a_1,\ldots,a_k)$ be a regular recurrence with $a_k \ne 0$ and distinct characteristic roots α_i $(i=1,2,\ldots,t)$ with multiplicity m_i as given in (2.2). Suppose that*

$$w_n = \sum_{i=1}^{t} f_i(n)\alpha_i^n \tag{4.10}$$

for some polynomials f_i, each of degree less than m_i, with coefficients in $\mathcal{K}$. Let

$$b = \max_{1\le i\le t}(m_i-1).$$

Define (w') by

$$w'_m = w_{n+cm}, \tag{4.11}$$

where n is a fixed nonzero integer and c is a fixed positive integer. Then (w') satisfies the kth-order recursion relation given by

$$w'_{m+k} = a_1^{(c)} w'_{m+k-1} - a_2^{(c)} w'_{m+k-2} + \cdots + (-1)^{k+1} a_k^{(c)} w'_m, \tag{4.12}$$

where the parameters $a_1^{(c)}, a_2^{(c)}, \ldots, a_t^{(c)}$ are all rational integers. The characteristic polynomial of (w') is given by

$$g(x) = x^k - a_1^{(c)} x^{k-1} + \cdots + (-1)^k a_k^{(c)} = \prod_{i=1}^{t} (x - \alpha_i^c)^{m_i}, \tag{4.13}$$

where the α_i's and m_i's are as given in (2.2). Moreover,

$$w'_m = \sum_{i=1}^{t} [\alpha_i^n f_i(n+cm)](\alpha_i^c)^m = \sum_{i=1}^{t} g_i(m)(\alpha_i^c)^m, \tag{4.14}$$

where the polynomials f_i are as given in (4.10). Then $deg(g_i) = deg(f_i) < m_i$ $(1 \le i \le t)$. Moreover, the coefficients of g_i can all be expressed in the form s_1/s_2, where $s_1, s_2 \in R$ and a prime ideal P divides s_2 only if

$$P \mid b!\alpha_1\alpha_2\cdots\alpha_t \prod_{1 \le i < j \le t} (\alpha_i - \alpha_j). \tag{4.15}$$

Proof: All the assertions except the last one are proved in [7]. The assertion given in (4.15) follows from (4.14) and Lemma 4.1 (a). □

Lemma 4.4: *Let $w(a_1, \ldots, a_k)$ be a p-regular recurrence such that $p \nmid a_k$ and with distinct characteristic roots $\alpha_1, \ldots, \alpha_t$. Let r^* be defined as in Theorem 3.1. Let $h^* = h(p^{r^*})$ and M^* be an integer such that $M^* \equiv M(p^{r^*})$ (mod (p^r)). Then*

$$\alpha_i^{h^*} \equiv M^* \ (mod\ (p^{r^*}))$$

for $1 \le i \le t$.

Proof: First note that for $1 \le i \le t$, the sequence $\{\alpha_i^n\}_{n=0}^{\infty}$ with terms in R satisfies the same recursion relation (2.1) as $w(a_1, \ldots, a_k)$, though it also satisfies the first-order relation

$$\alpha_i^{n+1} = \alpha_i \alpha_i^n$$

with parameter α_i in R. Thus, by our earlier discussion, $\{\alpha_i^n\}$ has $h(p^{r^*})$ as a general restricted period modulo (p^{r^*}) and M^* as a general multiplier modulo (p^{r^*}). Hence,

$$\alpha_i^{h^*} \equiv M^* \alpha_i^0 \equiv M^* \ (\text{mod } (p^{r^*}))$$

for $1 \le i \le t$. $\square$

5. PROOF OF THE MAIN THEOREM

Proof of Theorem 3.1: Since $p \not| A_0(w)$, we see that (w) is p-regular. Moreover, (w) is purely periodic modulo p^r, as $p \not| a_k$. The fact that (w) is nondegenerate guarantees that $e(p) < \infty$. We note that $r^* < r$, since $r > e$. Also, $h^* = h(p^{r^*}) < h(p^r)$ by Theorem 2.3. The result for the case in which $k = 2$ and p is an odd prime was proved in Theorem 3.5 of [1]. The proof of Theorem 3.5 of [1] carries over completely to the case in which $k = 2$ and $p = 2$ upon making use of Theorem 2.3 of this paper.

Now assume that $k \ge 3$. Let M^* be a rational integer such that $M^* \equiv w_{n+h^*} w_n^{-1} \pmod{p^r}$. By (2.2) and the hypotheses of Theorem 3.1, $w(a_1, \ldots, a_k)$ has characteristic polynomial

$$f(x) = \prod_{i=1}^{t} (x - \alpha_i)^{m_i}, \tag{5.1}$$

where $m_1 = 1$ or 2 and $m_2 = m_3 = \cdots = m_t = 1$. By Lemma 4.1 (a), there exist polynomials f_i $(i = 1, 2, \ldots, t)$ with coefficients in $\mathcal{K}$ such that

$$w_n = \sum_{i=1}^{t} f_i(n) \alpha_i^n, \tag{5.2}$$

where $deg(f_1) < m_1 \le 2$ and $deg(f_i) = 0$ for $2 \le i \le t$.

Let $\{w_m^*\}_{m=0}^{\infty}$ be the sequence defined by

$$w_m^* = w_{n+mh^*}. \tag{5.3}$$

By Lemma 4.3, (w^*) satisfies the kth-order recursion relation

$$w_{m+k}^* = a_1^{(h^*)} w_{m+k-1}^* - a_2^{(h^*)} w_{m+k-2}^* + \cdots + (-1)^{k+1} a_k^{(h^*)} w_m^* \tag{5.4}$$

with characteristic polynomial

$$G(x) = \prod_{i=1}^{t} (x - \alpha_i^{h^*})^{m_i}, \tag{5.5}$$

where the parameters $a_i^{(h^*)}$ are rational integers for $1 \le i \le t$ and the multiplicities m_i are the same as the multiplicities given in (5.1). Moreover, by (4.14),

$$w_m^* = \sum_{i=1}^{t} g_i(m) (\alpha_i^{h^*})^m, \tag{5.6}$$

where the polynomial g_i $(1 \le i \le t)$ has coefficients in $\mathcal{K}$ and has the same degree as the polynomial f_i given in (5.2). Since $w(a_1, \ldots, a_k)$ is nondegenerate, the characteristic roots $\alpha_i^{h^*}$ are distinct for $1 \le i \le t$. If $deg(g_1) = 0$, let $g_1(x) = c_1$, where $c_1 \in \mathcal{K}$. We let $g_i(x) = c_i$ $(2 \le i \le t)$, where $c_i \in \mathcal{K}$. Noting that $p \not| \, a_k \hat{D}$ and that $m_i \le 2$ for $1 \le i \le t$, it follows from Lemma 4.1 (b) and Lemma 4.3 that the coefficients of f_i and g_i are both well-defined modulo (p^r). Hence, we see that

$$w_m^* \equiv \sum_{i=1}^{t} g_i(m)(\alpha_i^{h^*})^m \ (\mathrm{mod}(p^r)), \tag{5.7}$$

where the coefficients of $g_i(m)$ can be taken to be elements of R. We note that the characteristic roots $\alpha_i^{h^*}$ $(1 \le i \le t)$ of $G(x)$ are not necessarily distinct modulo (p^r).

Let $H(x)$ be the polynomial defined by

$$H(x) = (x - \alpha_1^{h^*})^2 \text{ if } m_1 = 2 \tag{5.8}$$

and

$$H(x) = (x - M^*)^2 \text{ if } m_1 = 1. \tag{5.9}$$

Note that if $m_1 = 2$, then $\alpha_1^{h^*} \in \mathbb{Z}$, since each of the parameters $a_1^{(h^*)}, a_2^{(h^*)}, \ldots, a_k^{(h^*)}$ is in $\mathbb{Z}$. (This observation is not absolutely necessary for our proof, but we use it for convenience.) Let $w'(a_1', a_2')$ be a p-regular second-order linear recurrence having $H(x)$ as its characteristic polynomial. Then (w') satisfies the recurrence relation

$$w_{i+2}' = 2\alpha_1^{h^*} w_{i+1}' - \alpha_1^{2h^*} w_i' \tag{5.10}$$

if $m_1 = 2$ and

$$w_{i+2}' = 2M^* w_{i+1}' - (M^*)^2 w_i' \tag{5.11}$$

if $m_1 = 1$. Note that, in particular, the second-order unit sequence $u(a_1', a_2')$ is p-regular.

Our proof will proceed by first showing that the sequence $\{(M^*)^i\}_{i=0}^{\infty}$ satisfies the same second-order recursion relation modulo (p^r) as (w') does. We will next show that the kth-order recurrence (w^*) also satisfies this same second-order recursion relation modulo (p^r). We will be interested in particular in the sequence $\{(M^*)^i w_0^*\}_{i=1}^{\infty}$. This sequence satisfies the same second-order recursion relation as $\{(M^*)^i\}_{i=1}^{\infty}$ modulo (p^r), since multiples of a recurrence modulo (p^r) satisfy that same recursion relation (mod (p^r)). Using (5.3) and the definition of M^* at the beginning of Section 5, we see that

$$w_0^* = w_n \ \text{ and } \ w_1^* \equiv M^* w_0^* \ (\mathrm{mod}\ p^r). \tag{5.12}$$

Since the terms of (w^*) are all in $\mathbb{Z}$, it follows that

$$w_m^* \equiv (M^*)^m w_0^* \ (\mathrm{mod}\ p^r) \tag{5.13}$$

for all nonnegative integers m. This will imply that M^* is a general special multiplier of $w(a_1, \ldots, a_k)$ with respect to w_n modulo p^r.

To continue with our proof, we now demonstrate that

$$H(M^*) \equiv 0 \ (\text{mod } (p^r)). \tag{5.14}$$

Noting that

$$(p^{r^*})^2 \equiv 0 \ (\text{mod } p^r) \tag{5.15}$$

and that

$$\alpha_i^{h^*} \equiv M^* \ (\text{mod } (p^{r^*})) \tag{5.16}$$

for $1 \le i \le t$ by Lemma 4.4, it follows from (5.8) and (5.9) that (5.14) holds. This implies that the sequence $\{(M^*)^i\}_{i=0}^{\infty}$ satisfies the same recursion relation modulo (p^r) as $w'(a_1', a_2')$ does.

We now show that, for a fixed i, the sequence $\{c_i(\alpha_i^{h^*})^m\}_{m=0}^{\infty}$ satisfies the same second-order recursion relation modulo (p^r) as $w'(a_1', a_2')$ does. We first consider the case in which $m_i = 1$. By hypothesis, this always occurs if $2 \le i \le t$. In this case, we also treat the situation in which $i = 1$ and $m_1 = 1$. By (5.9), (5.15), and (5.16), we see that

$$H(\alpha_i^{h^*}) \equiv 0 \ (\text{mod } (p^r)) \tag{5.17}$$

if $2 \le i \le t$ or both $i = 1$ and $m_1 = 1$. Thus, $\{(\alpha_i^{h^*})^m\}_{m=0}^{\infty}$ and hence, $\{c_i(\alpha_i^{h^*})^m\}_{m=0}^{\infty}$ both satisfy the same second-order recursion relation modulo (p^r) as $w'(a_1', a_2')$ when $2 \le i \le t$ or $i = 1$ and $m_1 = 1$.

Next, we consider the remaining case in which $i = 1$ and $m_1 = 2$. Recall that $m_1 = 1$ or 2. Then by (5.8),

$$H(\alpha_1^{h^*}) = 0. \tag{5.18}$$

Thus, by Lemma 4.1 (c), (5.8), and (5.18), the sequence $\{g_1(m)(\alpha_1^{h^*})^m\}_{m=0}^{\infty}$ satisfies the same recursion relation as $w'(a_1', a_2') = w'(2\alpha_1^{h^*}, -\alpha_1^{2h^*})$ does. Reducing modulo (p^r), we see that the sequence $\{g_1(m)(\alpha_1^{h^*})^m\}_{m=0}^{\infty}$ satisfies the same recursion relation modulo (p^r) as $w'(a_1', a_2')$ does.

Noting that

$$w_m^* \equiv \sum_{i=1}^{t} g_i(m)(\alpha_i^{h^*})^m \ (\text{mod } (p^r))$$

and that linear combinations of linear recurrences all satisfying a particular recursion relation modulo (p^r) also satisfy that same recursion relation (mod (p^r)), we see that the kth-order recurrence w_m^* satisfies the same second-order recursion relation modulo (p^r) as $w'(a_1', a_2')$ does. The result now follows from our earlier discussion. □

ACKNOWLEDGMENT

I wish to thank the referee for the careful reading of the paper and suggestions which improved the paper.

REFERENCES

[1] Walter Carlip and Lawrence Somer. "Bounds for Frequencies of Residues of Regular Second-Order Recurrences Modulo p^r." *Number Theory in Progress*, Vol. 2 (Zakopane - Kościelisko, 1997), de Gruyter, Berlin, 1999, pp. 691-719.

[2] Walter Carlip and Lawrence Somer. “The Existence of Special Multipliers of Second-Order Recurrence Sequences.” *The Fibonacci Quarterly* **41.2** (2003): 156-168.

[3] R. D. Carmichael. “On Sequences of Integers Defined by Recurrence Relations.” *Quart. J. Pure Appl. Math.* **48** (1920): 343-372.

[4] L. M. Milne-Thompson. *The Calculus of Finite Differences*, Macmillan, New York, 1960.

[5] T. N. Shorey and R. Tijdman. *Exponential Diophantine Equations*, Cambridge University Press, Cambridge, 1986.

[6] Lawrence Somer. *The Divisibility and Modular Properties of kth-Order Linear Recurrences over the Ring of Integers of an Algebraic Number Field with Respect to Prime Ideals*, Ph.D. Thesis, The University of Illinois at Urbana-Champaign, 1985.

[7] Lawrence Somer. “Solution to Problem H-377.” *The Fibonacci Quarterly* **24.3** (1986): 284-285.

[8] Lawrence Somer. “Special Multipliers of Lucas Sequences Modulo p^r.” *Applications of Fibonacci Numbers*, Vol. 8, F. T. Howard (Ed.), Kluwer Academic Publishers, Dordrecht, 1999, pp. 325-336.

AMS Classification Numbers: 11B37, 11B50

✠ ✠ ✠