APPLICATIONS OF MATRIX THEORY TO CONGRUENCE PROPERTIES OF k^{th}-ORDER F-L SEQUENCES

Chizhong Zhou
Department of Computer Science, Yueyang Normal University
Yueyang, Hunan 414000, P.R. China
e-mail: chizhongz@163.com
(Submitted November 2000-Final Revision May 2002)

1. INTRODUCTION

For convenience, we quote some notations and symbols in [7]: Let the sequence $\{w_n\}$ be defined by the recurrence relation

$$w_{n+k} = a_1 w_{n+k-1} + \cdots + a_{k-1} w_{n+1} + a_k w_n \tag{1.1}$$

and the initial conditions

$$w_0 = c_0,\ w_1 = c_1, \ldots, w_{k-1} = c_{k-1}, \tag{1.2}$$

where $a_1, \ldots, a_k$ and $c_0, \ldots, c_{k-1}$ are complex constants. Then we call $\{w_n\}$ a k^{th}-order **Fibonacci-Lucas sequence** or, simply, an **F-L sequence**, call every w_n an **F-L number**, and call

$$f(x) = x^k - a_1 x^{k-1} - \cdots - a_{k-1} x - a_k \tag{1.3}$$

the characteristic polynomial of $\{w_n\}$. A number α satisfying $f(\alpha) = 0$ is called a characteristic root of $\{w_n\}$. If $a_k \neq 0$, we may consider $\{w_n\}$ as $\{w_n\}_{-\infty}^{+\infty}$. We denote $\mathbb{Z}(a_k) = \mathbb{Z}$ for $a_k \neq 0$ or $\mathbb{Z}^+ \cup \{0\}$ for $a_k = 0$. The set of F-L sequences satisfying (1.1) is denoted by $\Omega(a_1, \ldots, a_k)$ and also by $\Omega(f(x))$. Let $\{u_n^{(i)}\}$ $(0 \le i \le k-1)$ be a sequence in $\Omega(f(x))$ with the initial conditions $u_n^{(i)} = \delta_{ni}$ for $0 \le n \le k-1$, where δ is the Kronecker function. Then we call $\{u_n^{(i)}\}$ the i^{th} **basic sequence** in $\Omega(f(x))$, and also call $\{u_n^{(k-1)}\}$ the **principal sequence** in $\Omega(f(x))$ for its importance. In [3], M. E. Waddill considered the congruence properties modulo m of the k^{th}-order F-L sequence $\{M_n\} \in \Omega(1, \ldots, 1)$ with initial conditions $M_0 = M_1 = \cdots = M_{k-3} = 0$ and $M_{k-2} = M_{k-1} = 1$. In this paper we apply matrix techniques to research the congruence properties modulo m of the general k^{th}-order F-L sequence $\{w_n\} \in \Omega(a_1, \ldots, a_k) = \Omega(f(x))$, where $a_1, \ldots, a_k \in \mathbb{Z}$. In Section 2 we give required preliminaries. By using matrix techniques, in Section 3 we discuss the congruence properties of F-L sequences and get a series of general results. In Section 4 we apply our general results to the special case of second-order F-L sequences. As examples, two more interesting theorems are given.

2. PRELIMINARIES

Let $\{w_n\} \in \Omega(a_1, \ldots, a_k) = \Omega(f(x))$. Denote $\operatorname{col} w_n = (w_{n+k-1}, w_{n+k-2}, \ldots, w_n)^T$. Then, from (1.1), we have

$$\operatorname{col} w_{n+1} = A \operatorname{col} w_n, \tag{2.1}$$

where

$$A = \begin{pmatrix} a_1 & a_2 & \cdots & a_{k-1} & a_k \\ 1 & & & & \\ & 1 & & & \\ & & \cdots & & \\ & & & 1 & \end{pmatrix} \tag{2.2}$$

is called the **associated matrix** of $\{w_n\}$, also of $f(x)$. And we also denote $\Omega(a_1, \ldots, a_k)$.by $\Omega(A)$. Note that in A the entry in the i^{th} row and j^{th} column is 0 if $i > 1$ and $i \neq j+1$.

Theorem 2.1: Let $\{w_n\} \in \Omega(A)$. Then, for $n \in \mathbb{Z}(a_k)$,

$$\text{col } w_n = A^n \text{ col } w_0. \tag{2.3}$$

For simplicity, in this paper we prove all theorems only for $\mathbb{Z}(a_k) = \mathbb{Z}$.

Proof: If $n \geq 0$, then (2.3) can be proved by induction and by using (2.1). If $n \geq 0$, again by induction and by using (2.1), we can easily verify col $w_{m+n} = A^m$ col w_n for $m \geq 0$. Taking $m=-n$ we get col $w_0 = A^{-n}$ col w_n, whence (2.3) also holds for $n < 0$. □

Theorem 2.2: Let $\{u_n^{(i)}\}$ $(i = 0, 1, \ldots, k-1)$ be the i^{th} basic sequence in $\Omega(a_1, \ldots, a_k) = \Omega(A)$. Then, for $n \in \mathbb{Z}(a_k)$,

$$A^n = (\text{col } u_n^{(k-1)}, \text{col } u_n^{(k-2)}, \ldots, \text{col } u_n^{(0)}). \tag{2.4}$$

Proof: From (2.3), the right-hand side of (2.4) is equal to (let I be the identity matrix)

$$\begin{aligned} &(A^n \text{ col } u_0^{(k-1)}, A^n \text{ col } u_0^{(k-2)}, \ldots, A^n \text{ col } u_0^{(0)}) \\ &= A^n(\text{col } u_0^{(k-1)}, \text{col } u_0^{(k-2)}, \ldots, \text{col } u_0^{(0)}) = A^n I = A^n. \quad \square \end{aligned}$$

Remark 2.3: Equation (2.4) was shown in [9] and [1]. Its equivalent form was shown as (4) in [4], where U_n is equal to $u_{n+1}^{(k-1)}$ in (2.4). It may be seen that, owing to the introduction of the basic sequences, it is more convenient to use (2.4) than to use (4) in [4].

Substituting (2.4) into (2.3) and comparing the k^{th} row on both sides, we get the following corollary which was stated in [7].

Corollary 2.4: Let $\{u_n^{(i)}\}$ $(i = 0, 1, \ldots, k-1)$ be the i^{th} basic sequence in $\Omega(a_1, \ldots, a_k) = \Omega(A)$ and let $\{w_n\} \in \Omega(A)$. Then $\{w_n\}$ can be represented uniquely as

$$w_n = \sum_{i=0}^{k-1} w_i u_n^{(i)}. \tag{2.5}$$

The following theorem gives a technique for generating F-L sequences by using the matrix other than the associated matrix. The method of proof is quoted from [9].

Theorem 2.5: Let $X_n = (x_{n1}, x_{n2}, \ldots, x_{nk})^T$ be a vector over $\mathbb{C}$ and let B be a square matrix of order k over $\mathbb{C}$. If

$$|xI - B| = f(x) = x^k - a_1 x^{k-1} - \cdots - a_{k-1}x - a_k$$

and

$$X_n = B^n X_0,$$

then, for $n \in \mathbb{Z}(a_k)$,

(1) $\{x_{nj}\}_n \in \Omega(a_1, \ldots, a_k) = \Omega(f(x))$ $(j = 1, \ldots, k)$ or, simply,

$$\{X_n\}_n \in \Omega(a_1, \ldots, a_k) = \Omega(f(x)).$$

(Naturally, we can generalize the concept of an F-L sequence to that of an F-L vector sequence.)

(2)

$$B^n = u_n^{(k-1)} B^{k-1} + u_n^{(k-2)} B^{k-2} + \cdots + u_n^{(1)} B + u_n^{(0)} I. \tag{2.6}$$

Specifically,

$$A^n = u_n^{(k-1)} A^{k-1} + u_n^{(k-2)} A^{k-2} + \cdots + u_n^{(1)} A + u_n^{(0)} I, \tag{2.7}$$

where $\{u_n^{(i)}\}$ is the i^{th} $(i = 0, \ldots, k-1)$ basic sequence in $\Omega(a_1, \ldots, a_k)$ and A is the associated matrix of $f(x)$.

Proof: By the Cayley-Hamilton Theorem, we have $B^k = a_1 B^{k-1} + \cdots + a_{k-1} B + a_k I$, whence

$$B^{n+k} = a_1 B^{n+k-1} + \cdots + a_{k-1} B^{n+1} + a_k B^n. \tag{2.8}$$

Multiplying by X_0, we obtain $X_{n+k} = a_1 X_{n+k-1} + \cdots + a_{k-1} X_{n+1} + a_k X_n$. This means that (1) holds. Denote $B^n = (b_{ij})_{1 \le i, j \le k}$. Then (2.8) implies $b_{ij}^{(n+k)} = a_1 b_{ij}^{(n+k-1)} + \cdots + a_{k-1} b_{ij}^{(n+1)} + a_k b_{ij}^{(n)}$. Therefore, $\{b_{ij}^{(n)}\}_n \in \Omega(f(x))$. By (2.5), it follows that

$$b_{ij}^{(n)} = \sum_{r=0}^{k-1} b_{ij}^{(r)} u_n^{(r)},$$

which is equivalent to (2.6). □

The following theorem is called the **Theorem of Constructing Identities (TCI)** in matrix form. TCI in polynomial form was proved in [6].

Theorem 2.6 (TCI of matrix form): Let $\Omega(a_1, \ldots, a_k) = \Omega(A)$. If

$$\sum_{i=0}^{s} d_i A^{n_i} = \sum_{j=0}^{t} e_j A^{p_j} \tag{2.9}$$

holds, where $n_i, p_j \in \mathbb{Z}(a_k)$ and $d_i, e_j \in \mathbb{C}$, $i = 0, \ldots, s$ and $j = 0, \ldots, t$, then

$$\sum_{i=0}^{s} d_i \operatorname{col} w_{n_i} = \sum_{j=0}^{t} e_j \operatorname{col} w_{p_j} \tag{2.10}$$

holds for any $\{w_n\} \in \Omega(A)$. Specifically,

$$\sum_{i=0}^{s} d_i w_{n_i} = \sum_{j=0}^{t} e_j w_{p_j} \tag{2.11}$$

holds for any $\{w_n\} \in \Omega(A)$. Conversely, if (2.11) holds for any $\{w_n\} \in \Omega(A)$, then (2.9) holds.

Proof: Multiplying (2.9) by $\operatorname{col} w_0$ and using (2.3), we get (2.10), then (2.11). Conversely, if (2.11) holds for any $\{w_n\} \in \Omega(A)$, then it holds for every basic sequence $\{u_n^{(i)}\} \in \Omega(A)$ $(i = 0, \ldots, k-1)$. By using (2.5) and (2.7), we can prove that (2.9) holds. □

The following lemma was proved in [6]. It can also be proved by using the TCI of matrix form.

Lemma 2.7: Let $\{u_n^{(i)}\}$ $(i=0,\dots,k-1)$ be the i^{th} basic sequence in $\Omega=\Omega(a_1,\dots,a_k)=\Omega(A)$ and let $\{w_n\}$ be any sequence in Ω. Then, for $m,n\in\mathbb{Z}(a_k)$,

$$w_{m+n}=\sum_{i=0}^{k-1}u_m^{(i)}w_{n+i}. \tag{2.12}$$

Remark 2.8: For convenience, we rewrite (2.12) as

$$w_{m+n}=A_m\operatorname{col}w_n, \tag{2.13}$$

where $A_m=(u_m^{(k-1)},u_m^{(k-2)},\dots,u_m^{(0)})$.

3. CONGRUENCE PROPERTIES OF F-L SEQUENCES

In the subsequent discussions we deal with the integer sequences in $\Omega(a_1,\dots,a_k)=\Omega(A)=\Omega(f(x))$, where $a_1,a_2,\dots,a_k\in\mathbb{Z}$. The Cayley-Hamilton Theorem gives

$$A^k=a_1A^{k-1}+a_2A^{k-2}+\cdots+a_{k-1}A+a_kI. \tag{3.1}$$

Let $\mathbb{M}$ be the ring of integer matrices of order k. Let $m\in\mathbb{Z}^+$, $m>1$, and let (m) be the principal ideal generated by m over $\mathbb{M}$. For $M,N\in\mathbb{M}$, define $M\equiv N \pmod m$ if $M-N\in(m)$. Let $\{w_n\}\in\Omega(A)$. If there exists $t\in\mathbb{Z}^+$ such that

$$A^t\equiv I \pmod m, \tag{3.2}$$

then we call the least positive integer t satisfying (3.2) the **order of A modulo *m*** and denote $t=\operatorname{ord}_m(A)$. If there exist integers $t>0$ and $n_0\geq 0$ such that

$$w_{n+t}\equiv w_n \pmod m \text{ iff } n\geq n_0, \tag{3.3}$$

then we call $\{w_n\}$ **periodic modulo *m*** and call the least positive integer t satisfying (3.3) the **period of $\{w_n\}$ modulo *m***, and denote $t=P(m,w_n)$. If $n_0=0$, we call $\{w_n\}$ **purely periodic**. The following lemma is obvious.

Lemma 3.1:

(1) If an integer $t>0$ satisfies (3.2), then $\operatorname{ord}_m(A)\mid t$.

(2) If an integer $t>0$ satisfies (3.3), then $P(m,w_n)\mid t$.

Lemma 3.2: Let $\Omega(a_1,\dots,a_k)=\Omega(A)$. Then $\operatorname{ord}_m(A)$ exists iff $(m,a_k)=1$.

Proof: Assume that $\operatorname{ord}_m(A)$ exists. Then (3.2) holds. Taking determinants on both of its sides and noting (2.2), we get $(-1)^{(k-1)t}a_k^t\equiv 1 \pmod m$. This implies $(m,a_k)=1$. Conversely, assume $(m,a_k)=1$. Then there exists an integer b being the inverse of $a_k \pmod m$. Whence, from (3.1), we have $Ab(A^{k-1}-a_1A^{k-2}-\cdots-a_{k-1}I)\equiv I \pmod m$. This means that there exists a matrix B which is the inverse of $A \pmod m$. Since among $I,A,\dots,A^s,\dots \pmod m$ there are at most m^{k^2} different residues, there exist $r>s\geq 0$ such that $A^r\equiv A^s \pmod m$. Multiplying by B^s, we obtain $A^{r-s}\equiv I \pmod m$, so $\operatorname{ord}_m(A)$ exists. □

Theorem 3.3: Let $\Omega=\Omega(a_1,\dots,a_k)=\Omega(A)$ and let $\{u_n\}$ be the principal sequence in Ω. If $(m,a_k)=1$, then $\{u_n\}$ is purely periodic and $P(m,u_n)=\operatorname{ord}_m(A)$.

Proof: From Lemma 3.2, $t'=\operatorname{ord}_m(A)$ exists since $(m,a_k)=1$. Then (3.2) implies that, for any $n\geq 0$, $A^{n+t'}\equiv A^n \pmod m$ holds. From TCI, for any $n\geq 0$, $u_{n+t'}\equiv u_n \pmod m$ holds. Thus,

$\{u_n\}$ is purely periodic and, by Lemma 3.1, $t = P(m, u_n) | t'$. Conversely, since any $\{w_n\} \in \Omega$ can be represented linearly by $\{u_n\}$ over the ring of integers (see [7], Lemma 2.5), the congruence $w_{n+t} \equiv w_n \pmod m$ holds for any $\{w_n\} \in \Omega$. Whence the converse of TCI implies that $A^{n+t} \equiv A^n \pmod m$ holds. Multiplying by A^{-n} (from the proof of Lemma 3.2, A^{-1} exists), we get (3.2). Thus, Lemma 3.1 implies $t' | t$. Summarizing the above, we obtain $t = t'$. □

Corollary 3.4: Let $\Omega = \Omega(a_1, \ldots, a_k) = \Omega(A)$ and let $\{u_n\}$ be the principal sequence in Ω. If $(m, a_k) = 1$, then any $\{w_n\} \in \Omega$ is purely periodic and $P(m, w_n) | P(m, u_n) = \operatorname{ord}_m(A)$.

For what sequences $\{w_n\}$ in $\Omega(A)$ besides the principal sequence will the equality $P(m, w_n) = \operatorname{ord}_m(A)$ hold? To give an answer on the sufficient condition for the question, we introduce the **Hankel matrix** and **Hankel determinant** of $\{w_n\}$, which are defined by, respectively, $H(w_n) = (\operatorname{col} w_{n+k-1}, \operatorname{col} w_{n+k-2}, \ldots, \operatorname{col} w_n)$ and $\det H(w_n)$.

Theorem 3.5: Let $\Omega = \Omega(a_1, \ldots, a_k) = \Omega(A)$. Let $\{u_n\}$ be the principal sequence in Ω and let $\{w_n\}$ be any sequence in Ω. Assume $(m, a_k) = (m, \det H(w_0)) = 1$. Then $P(m, w_n) = P(m, u_n) = \operatorname{ord}_m(A)$.

Proof: From $(m, a_k) = 1$, Theorem 3.3, and Corollary 3.4, we conclude that $\{w_n\}$ is purely periodic and $P(m, w_n) | P(m, u_n) = \operatorname{ord}_m(A)$. Thus, we need only prove that $P(m, u_n) | P(m, w_n)$. Equation (2.13) gives $w_{n+i} = A_n \operatorname{col} w_i$. Whence

$$(w_{n+k-1}, \ldots, w_{n+1}, w_n) = A_n(\operatorname{col} w_{k-1}, \ldots, \operatorname{col} w_1, \operatorname{col} w_0). \tag{3.4}$$

The equality (3.4) can be considered a system of linear equations in unknowns $u_n^{(i)}$ ($i = 0, \ldots, k-1$). The coefficient determinant of the system is $\det(\operatorname{col} w_{k-1}, \ldots, \operatorname{col} w_1, \operatorname{col} w_0) = \det H(w_0)$. Since $(m, \det H(w_0)) = 1$, we can solve $u_n = u_n^{(k-1)} \equiv b_1 w_{n+k-1} + \cdots + b_{k-1} w_1 + b_k w_0 \pmod m$. Hence, $P(m, u_n) | P(m, w_n)$. □

For more detailed consideration on the periodicity, we introduce the following concepts: Let $\{w_n\} \in \Omega(A)$. If there exists $s \in \mathbb{Z}^+$ such that

$$A^s \equiv cI \pmod m, \tag{3.5}$$

where $c \in \mathbb{Z}$ and $(m, c) = 1$, then we call the least positive integer s satisfying (3.5) the **constrained order of A modulo m**, call c a **multiplier of A modulo m**, and denote $s = \operatorname{ord}'_m(A)$. Correspondingly, if there exist integers $s > 0$ and $n_0 \geq 0$ such that

$$w_{n+s} \equiv c w_n \pmod m \ \text{ iff } n \geq n_0, \tag{3.6}$$

where c is an integer independent of n and $(m, c) = 1$, then we call the least positive integer s satisfying (3.6) the **constrained period of $\{w_n\}$ modulo m**, call c a **multiplier of $\{w_n\}$ modulo m**, and denote $s = P'(m, w_n)$. If $n_0 = 0$, we call $\{w_n\}$ **purely constrained periodic**. We point out that the definition of "constrained period" has generalized and improved the definition in [2]. Similarly to Lemma 3.1, the following lemma is obvious.

Lemma 3.6:

(1) If an integer $s > 0$ satisfies (3.5), then $\operatorname{ord}'_m(A) | s$.

(2) If an integer $s > 0$ satisfies (3.6), then $P'(m, w_n) | s$.

Clearly, if $\text{ord}_m(A)$ exists, then $\text{ord}'_m(A)$ must exist [especially in the case $c \equiv 1 \pmod{m}$]. Hence, from 3.2, we obtain

Lemma 3.7: Let $\Omega(a_1, \ldots, a_k) = \Omega(A)$. Then $\text{ord}'_m(A)$ exists iff $(m, a_k) = 1$.

By induction on j, we can easily prove

Lemma 3.8: Let s and c be the constrained period and a multiplier of $\{w_n\}$ modulo m, respectively; that is to say that (3.6) holds. Then, for $j \geq 0$ and $n \geq n_0$, we have

$$w_{n+js} \equiv c^j w_n \pmod{m}. \tag{3.7}$$

Theorem 3.9: Let $\Omega = \Omega(a_1, \ldots, a_k) = \Omega(A)$, let $\{u_n\}$ be the principal sequence in Ω, and let $\{w_n\}$ be any sequence in Ω. If $(m, a_k) = 1$, then

(1) $\{u_n\}$ and $\{w_n\}$ are purely constrained periodic and $P'(m, w_n) | P'(m, u_n) = \text{ord}'_m(A)$.

(2) u_{s+k-1}, where $s = P'(m, u_n) = \text{ord}'_m(A)$, is a multiplier of $\{u_n\} \pmod{m}$.

Proof:

(1) The proof is similar to the proofs of Theorem 3.3 and Corollary 3.4.

(2) Take $n = k-1$ in the congruence $u_{n+s} \equiv cu_n \pmod{m}$ and note that $u_{k-1} = 1$. □

Theorem 3.10: Let $\{u_n\}$ be the principal sequence in $\Omega(a_1, \ldots, a_k)$ and let $(m, a_k) = 1$. Denote $P'(m, u_n) = s$, $u_{s+k-1} = c$, and $\text{ord}_m(c) = r$. Then

(1) $P(m, u_n) = rs$.

(2) The structure of $\{u_n \pmod{m}\}$ in a period is as follows:

$$\begin{array}{llllll} 0, \ldots, 0, 1, & u_k, & u_{k+1}, & \ldots, u_{s-1}, & \\ 0, \ldots, 0, c, & cu_k, & cu_{k+1}, & \ldots, cu_{s-1}, & \pmod{m} \\ \quad \cdots \quad \cdots & \cdots & & \cdots & \\ 0, \ldots, 0, c^{r-1}, & c^{r-1}u_k, & c^{r-1}u_{k+1}, & \ldots, c^{r-1}u_{s-1}. & \end{array}$$

Proof:

(1) Let $P(m, u_n) = t$. From $u_{n+t} \equiv u_n \pmod{m}$ and Lemma 3.6, we have $s | t$. Then $t = r_1 s$. On the other hand, Theorem 3.9 implies that c is a multiplier of $\{u_n\} \pmod{m}$. Equation (3.7) implies that

$$u_{n+js} \equiv c^j u_n \pmod{m}. \tag{3.8}$$

Taking $j = \text{ord}_m(c) = r$, we have $u_{n+rs} \equiv u_n \pmod{m}$. Whence Lemma 3.1 gives $t | rs$, that is, $r_1 s | rs$. Now we need only prove that $r_1 = r$. If this were not the case, then $r_1 < r$. Let A be the associated matrix of $\{u_n\}$. Theorem 3.9 implies that $A^s \equiv c \pmod{m}$. Theorem 3.3 implies that $A^t \equiv I \pmod{m}$, that is, $A^{r_1 s} = (A^s)^{r_1} \equiv c^{r_1} I \equiv I \pmod{m}$. This contradicts $\text{ord}_m(c) = r$.

(2) In (3.8), let $j = 0, 1, \ldots, r-1$ and let $n = 0, 1, \ldots, s-1$; then we have the required result. □

Corollary 3.11: Let $\{u_n\}$ be the principal sequence in $\Omega(a_1, \ldots, a_k)$ and let $(m, a_k) = 1$. Then $P'(m, u_n)$ is the least integer s such that $s > k-1$ and

$$u_s \equiv u_{s+1} \equiv \cdots \equiv u_{s+k-2} \equiv 0 \pmod{m}. \tag{3.9}$$

As an example, we let $\{u_n\}$ be the principal sequence in $\Omega(1, 1, 1)$. By calculating, we obtain

$$\{u_n \pmod 7\} = \{0,0,1,1,2,4,0,6,3,2,4,2,1,0,3,4,\underline{0,0,4},\ldots\}.$$

Therefore, $s = P'(7, u_n) = 16$, $c = u_{s+2} \equiv 4 \pmod 7$. Since $4^2 \equiv 2$ and $4^3 \equiv 1 \pmod 7$, we obtain $r = \text{ord}_7(c) = 3$, and so $t = P(7, u_n) = rs = 48$. Furthermore, from Theorem 3.10, we can get

$$u_n \equiv 0 \pmod 7 \text{ iff } n \equiv 0, 1, 6, 13 \pmod{16},$$
$$u_n \equiv 1 \pmod 7 \text{ iff } n \equiv 2, 3, 12, 20, 25, 27, 37, 42, 47 \pmod{48},$$
$$\ldots.$$

Another application example can be found in [8]. The above numerical results can be used to verify the following theorem.

Theorem 3.12: Let $\Omega = \Omega(a_1, \ldots, a_k) = \Omega(A) = \Omega(f(x))$, let $\{u_n\}$ be the principal sequence in Ω, and let $\{w_n\}$ be any sequence in Ω. Assume that $(m, a_k) = 1$. Denote $P(m, u_n) = s$, $u_{s+k-1} = c$, and $\text{ord}_m(c) = r$.

(1) If $(m, c-1) = 1$, then, for all integers $n \ge 0$,

$$\sum_{j=0}^{r-1} w_{n+js} \equiv 0 \pmod m. \tag{3.10}$$

(2) If $(m, f(1)) = 1$, then, for $a_0 = -1$ and, for all integers $n \ge 0$,

$$\sum_{j=0}^{s-1} w_{n+j} \equiv f(1)^{-1}(c-1)\sum_{j=0}^{k-1}(a_0 + a_1 + \cdots + a_j)w_{n+k-1-j} \pmod m. \tag{3.11}$$

Specifically,

$$\sum_{j=0}^{s-1} u_{is+j} \equiv f(1)^{-1}(1-c)c^i \pmod m \quad (i \ge 0). \tag{3.12}$$

Proof:

(1) From (1) of Theorem 3.9 and (3.7), we have

$$(c-1)\sum_{j=0}^{r-1} w_{n+js} \equiv (c-1)\sum_{j=0}^{r-1} c^j w_n = (c^r - 1)w_n \equiv 0 \pmod m.$$

Then (3.10) follows from the above congruence and $(m, c-1) = 1$.

(2) From $f(A) = 0$, we have

$$\begin{aligned} -f(1)I &= f(A) - f(1)I \\ &= (A-1)((A^{k-1} + \cdots + A + I) - a_1(A^{k-2} + \cdots + A + I) - \cdots - a_{k-1}I). \end{aligned}$$

Whence, from $(m, f(1)) = 1$, we get

$$(A-I)^{-1} \equiv f(1)^{-1}\sum_{j=0}^{k-1}(a_0 + a_1 + \cdots + a_j)A^{k-1-j}.$$

On the other hand, from Theorem 3.9 and (3.5), we have

$$(A-I)(A^{s-1} + A^{s-2} + \cdots + A + I) = A^s - I \equiv (c-1)I \pmod m.$$

Whence

$$A^{s-1}+A^{s-2}+\cdots+A+I\equiv(c-1)(A-I)^{-1}$$
$$\equiv(c-1)f(1)^{-1}\sum_{j=0}^{k-1}(a_0+a_1+\cdots+a_j)A^{k-1-j}\pmod{m},$$

multiplying it by A^n, by TCI we get (3.11). □

Note: Since $(m,a_k)=1$, the inverse of A (mod m) exists, which is

$$A^{-1}\equiv a_k^{-1}(A^{k-1}-a_1A^{k-2}-\cdots-a_{k-1}I)\pmod{m}.$$

Similarly, the sequence $\{w_n \pmod{m}\}\in\Omega(A)$ can be extended to $n<0$ by using the recurrence. Under this definition, the last theorem and the subsequent theorems, which hold for $n\ge 0$, will hold for $n\in\mathbb{Z}$.

Corollary 3.13: Under the conditions of Theorem 3.12, let $t=rs$. If *(a)* $(m,c-1)=1$, or if *(b)* $m|(c-1)$ and $(m,f(1))=1$, then

$$\sum_{j=0}^{t-1}w_{n+j}\equiv\sum_{j=0}^{s-1}w_{n+j}\equiv 0\pmod{m}. \tag{3.13}$$

Proof: We have $\sum_{j=0}^{t-1}w_{n+j}=\sum_{i=0}^{s-1}\sum_{j=0}^{r-1}w_{n+i+js}$. So (3.13) is proved by using (3.10) for (a) or by using (3.11) for (b). □

Remark 3.14:

(1) If we change $P'(m,u_n)=s$ and $u_{s+k-1}=c$ so that $P'(m,w_n)=s$ and c is a multiplier of $\{w_n\}$ modulo m, respectively, then (3.10) and (3.13) still hold because (3.7) still holds. But at this time we cannot conclude that (3.11) holds.

(2) If neither conditions (a) nor (b) are fulfilled, (3.13) may not hold. For example: It is clear that $\{n\}$ is the principal sequence in $\Omega(2,-1)=\Omega(f(x))$. Thus, $f(1)=0$.

$$\{n \pmod{10}\}=\{0,1,2,3,4,5,6,7,8,9,\underline{0,1},\ldots\}$$

implies $s=10$ and $c\equiv 1$ (mod 10). Hence, neither condition (a) nor condition (b) is fulfilled. We have $0+1+2+\cdots+9\equiv 5\not\equiv 0$ (mod 10), i.e., (3.13) does not hold.

Theorem 3.15: Let $\{u_n\}$ be the principal sequence in $\Omega(a_1,\ldots,a_k)=\Omega(A)$ and $(m,a_k)=1$. Set $P'(m,u_n)=s$. Then, for $j>0$, we have

(1)

$$u_{js-1}\equiv a_k^{j-1}u_{s-1}^j\pmod{m^2}. \tag{3.14}$$

(2)

$$u_{js+d}\equiv j(a_ku_{s-1})^{j-1}u_{s+d}\pmod{m^2}\quad(0\le d\le k-2). \tag{3.15}$$

Proof: Let $\{u_n^{(i)}\}$ $(i=0,\ldots,k-1)$ be the i^{th} basic sequence in $\Omega(A)$. Clearly, $u_{n+1}^{(0)}=a_ku_n^{(k-1)}=a_ku_n$. Denote $u_{s+k-1}=c$. We shall prove the theorem by induction. For $j=1$, (3.14) and (3.15) are trivial. Assume that both (3.14) and (3.15) hold for j. We want to prove that they also hold for $j+1$.

(1) From (2.12), we have $u_{(j+1)s-1}=\sum_{i=0}^{k-1}u_{js}^{(i)}u_{s-1+i}$. Theorem 3.9 and (3.7) imply that $u_{js}^{(i)}\equiv c^ju_0=0$ and $u_{s-1+i}\equiv cu_{i-1}=0$ (mod m) for $1\le i\le k-1$. Then, by the induction hypothesis,

$$u_{(j+1)s-1} \equiv u_{js}^{(0)}u_{s-1} = a_k u_{js-1}u_{s-1} \equiv a_k(a_k^{j-1}u_{s-1}^j)u_{s-1} = a_k^j u_{s-1}^{j+1} \pmod{m^2}.$$

(2) Again from (2.12), we have $u_{(j+1)s+d} = \sum_{i=0}^{k-1} u_s^{(i)} u_{js+d+i}$. From (3.9) and the recurrence (1.1), we obtain $c = u_{s+k-1} \equiv a_k u_{s-1} \pmod m$. Whence, from (3.7), we obtain $u_{js+d+i} \equiv c^j u_{d+i} \equiv (a_k u_{s-1})^j u_{d+i} \pmod m$ and $u_s^{(i)} \equiv cu_0^{(i)} = 0 \pmod m$ for $1 \le i \le k-1$. It follows that

$$u_{(j+1)s+d} \equiv u_s^{(0)} u_{js+d} + \sum_{i=1}^{k-1} u_s^{(i)} (a_k u_{s-1})^j u_{d+i} \pmod{m^2}.$$

Since $u_d = 0$ for $0 \le d \le k-2$, the last expression can be rewritten as

$$u_{(j+1)s+d} \equiv u_s^{(0)} u_{js+d} + (a_k u_{s-1})^j \sum_{i=0}^{k-1} u_s^{(i)} u_{d+i} \pmod{m^2}.$$

Thus, by (2.12), we get

$$u_{(j+1)s+d} \equiv u_s^{(0)} u_{js+d} + (a_k u_{s-1})^j u_{s+d} \pmod{m^2}.$$

Since $u_s^{(0)} = a_k u_{s-1}$, the conclusion follows by the induction hypothesis. □

We point out that Theorem 3.12 and Corollary 3.13 have generalized Theorem 12 in [3], while Theorem 3.15 has generalized Theorem 7 in [3].

4. THE CASE OF $k = 2$

For $k = 2$, the principal sequence $u_n = u_n^{(1)}$ in $\Omega(a, b)$ satisfies $u_0 = 0$, $u_1 = 1$, and $u_{n+2} = au_{n+1} + bu_n$ for $n \ge 0$. The 0^{th} basic sequence $u_n^{(0)}$ satisfies $u_0^{(0)} = 1$, $u_1^{(0)} = 0$. and the same recurrence. We assume $b \ne 0$, since $b = 0$ is less interesting. Clearly, $u_n^{(0)} = bu_{n-1}$. The associated matrix is

$$A = \begin{pmatrix} a & b \\ 1 & 0 \end{pmatrix}.$$

Our conclusions for general k can be easily transferred to the case of $k = 2$, for example:

Theorem 2.2 gives that, for $n \in \mathbb{Z}$,

$$A^n = \begin{pmatrix} u_{n+1} & bu_n \\ u_n & bu_{n-1} \end{pmatrix}. \tag{4.1}$$

Theorem 2.5 give that, for $n \in \mathbb{Z}$,

$$A^n = u_n A + bu_{n-1} I. \tag{4.2}$$

Corollary 3.11 given that, if $(m, b) = 1$, then $P'(m, u_n)$ is the least integer s such that $s > 1$ and $u_s \equiv 0 \pmod m$.

We do not enumerate all of them. Instead, we focus our mind on obtaining more interesting conclusions. Because of limited space, as examples we give only those for Theorems 3.12 and 3.15.

Theorem 4.1: Let $\{F_n\}$ be the Fibonacci sequence, i.e., the principal sequence in $\Omega = \Omega(1, 1)$, and let $\{w_n\}$ be any sequence in Ω. Let $p > 3$ be a prime. Then, for all integer $n \in \mathbb{Z}$:

(1)

$$w_n + w_{n+p} + w_{n+2p} + w_{n+3p} \equiv 0 \pmod{F_p}. \tag{4.3}$$

(2)

$$\sum_{j=0}^{p-1} w_{n+j} \equiv (F_{p-1}-1)w_{n+1} \pmod{F_p}. \tag{4.4}$$

Proof: In Theorem 3.12, take $m=F_p$. Then, from (4.2), $A^p \equiv F_{p-1} \pmod m$, where, as is well known, $(m, F_{p-1}) = (F_p, F_{p-1}) = 1$. Lemma 3.6 implies $P'(m, F_n) = s|p$. Since $s>1$ and p is prime, we have $s=p$. And the multiplier $c \equiv F_{p-1} \equiv F_{p+1} \pmod m$ (or, it can be obtained by Theorem 3.9 directly). It is well known that

$$F_{n+1}^2 - F_{n+1}F_n - F_n^2 = (-1)^n. \tag{4.5}$$

Whence $c^2 \equiv F_{p+1}^2 \equiv (-1)^p = -1 \pmod m$. Thus, $r = \mathrm{ord}_m(c) = 4$. From Theorem 3.12:

(1) To prove (4.3), it is sufficient to prove $d = (m, c-1) = (F_p, F_{p+1}-1) = 1$. Let $p = 2q+1$ and let L_n be the n^{th} Lucas number. Then $F_p = F_{q+1}^2 + F_q^2$ and

$$\begin{aligned} F_{p+1} - 1 &= F_{q+1}L_{q+1} - 1 = F_{q+1}(F_{q+1} + 2F_q) - (-1)^q(F_{q+1}^2 - F_{q+1}F_q - F_q^2) \\ &= \begin{cases} 3F_{q+1}F_q + F_q^2 & \text{for } 2|q, \\ 2F_{q+1}^2 + F_{q+1}F_q - F_q^2 & \text{otherwise.} \end{cases} \end{aligned}$$

For even q,

$$d = (F_{q+1}^2 + F_q^2, 3F_{q+1}F_q + F_q^2) = (F_{q+1}^2 + F_q^2, F_q(3F_{q+1} + F_q)).$$

Since $(F_{q+1}^2 + F_q^2, F_{q+1}) = (F_q^2, F_{q+1}) = 1$ and, by the same reasoning, $(F_{q+1}^2 + F_q^2, F_q) = 1$, we have $d = (F_{q+1}^2 + F_q^2, 3F_{q+1} + F_q)$.

For odd q, we also have

$$\begin{aligned} d &= (F_{q+1}^2 + F_q^2, 2F_{q+1}^2 + F_{q+1}F_q - F_q^2) = (F_{q+1}^2 + F_q^2, F_{q+1}(3F_{q+1} + F_1)) \\ &= (F_{q+1}^2 + F_q^2, 3F_{q+1} + F_q). \end{aligned}$$

Thus,

$$\begin{aligned} d &= (F_{q+1}(F_{q+1} - 3F_q), 3F_{q+1} + F_q) = (F_{q+1} - 3F_q, 3F_{q+1} + F_q) \\ &= (F_{q+1} - 3F_q, 10F_q) = (F_{q+1} - 3F_q, 10) = (-L_{q-1}, 10). \end{aligned}$$

The fact that $\{L_n \pmod 5\} = \{2, 1, 3, 4, 2, 1, \ldots\}$ implies that $(L_{q-1}, 5) = 1$. And the fact that $\{L_n \pmod 2\} = \{0, 1, 1, 0, 1, 1, \ldots\}$ implies that $2|L_{q-1}$ iff $3|(q-1)$, i.e., $3|(p-3)/2$. Whence, $3|p$. This is also impossible. Hence, $d=1$.

(2) Here $f(x) = x^2 - x - 1$ and $f(1) = -1$. Whence $(m, f(1)) = 1$ holds. Hence, (4.4) holds by (3.11). □

The following theorem implies a possible generalization and an alternative proof of Theorem 3.15.

Theorem 4.2: Let $\{u_n\}$ be the principal sequence in $\Omega = \Omega(a,b) = \Omega(A)$ and $\{w_n\}$ be any sequence in Ω. Assume $(m,b)=1$. Denote $P'(m, u_n) = s$. Then, for $j>0$ and $d \ge 0$, we have

(1)

$$w_{js-1} \equiv b^{j-1}u_{s-1}^j w_1 + (bu_{s-1})^{j-1}(ju_s - au_{s-1})w_0 \pmod{m^2}. \tag{4.6}$$

(2)

$$w_{js+d} \equiv (bu_{s-1})^j w_d + j(bu_{s-1})^{j-1} u_s w_{d+1} \pmod{m^2}. \tag{4.7}$$

Proof: From (4.2), $A^s = u_s A + bu_{s-1} I$. Since $m|u_s$, we have $A^{js} = (bu_{s-1})^j I + j(bu_{s-1})^{j-1} u_s A$ $(\bmod m^2)$. Whence

$$A^{js+d} = (bu_{s-1})^j A^d + j(bu_{s-1})^{j-1} u_s A^{d+1} \pmod{m^2}. \tag{4.8}$$

If $d \ge 0$, then (4.7) follows from TCI. For $d = -1$, from $A^2 - aA - bI = 0$, we get $A(A - aI) \equiv b$ $(\bmod m^2)$. Whence $(m, b) = 1$ gives $A^{-1} \equiv b^{-1}(A - aI) \pmod{m^2}$. And (4.8) becomes $A^{js-1} = b^{j-1} u_{s-1}^j A + (bu_{s-1})^{j-1}(ju_s - au_{s-1}) I \pmod{m^2}$. Thus, (4.6) follows from TCI. □

It is easy to see that when $\{w_n\} = \{u_n\}$ and $d = 0$ the conclusions of the last theorem agree with those of Theorem 3.15.

REFERENCES

1. U. Cerruti & F. Vaccarino. "Matrices, Recurrent Sequences and Arithmetic." In *Applications of Fibonacci Numbers* **6**:53-62. Ed. G. E. Bergum et al. Dordrecht: Kluwer, 1996.
2. L. Somer. "On Even Fibonacci Pseudoprimes." In *Applications of Fibonacci Numbers* **4**: 277-88. Ed. G. E. Bergum et al. Dordrecht: Kluwer, 1991.
3. M. E. Waddill. "Properties of a k-Order Linear Recursive Sequence Modulo m." In *Applications of Fibonacci Numbers* **6**:505-19. Ed. G. E. Bergum et al. Dordrecht: Kluwer, 1996.
4. M. E. Waddill. "Using Matrix Techniques To Establish Properties of k-Order Linear Recursive Sequences." In *Applications of Fibonacci Numbers* **5**:601-15. Ed. G. E. Bergum et al. Dordrecht: Kluwer, 1993.
5. M. E. Waddill. "Using Matrix Techniques To Establish Properties of a Generalized Tribonacci Sequence." In *Applications of Fibonacci Numbers* **4**:299-308. Ed. G. E. Bergum et al. Dordrecht: Kluwer, 1991.
6. Chizhong Zhou. "Constructing Identities Involving k^{th}-Order F-L Numbers by Using the Characteristic Polynomials." In *Applications of Fibonacci Numbers* **8**:369-79. Ed. F. T. Howard. Dordrecht: Kluwer, 1999.
7. Chizhong Zhou. "A Generalization of the 'All or None' Divisibility Property." *The Fibonacci Quarterly* **35.2** (1997):129-34.
8. Chizhong Zhou. On the k^{th}-Order Derivative Sequences of Fibonacci and Lucas Polynomials." *The Fibonacci Quarterly* **34.5** (1996):394-408.
9. Chizhong Zhou. *Fibonacci-Lucas Sequences and Their Applications* (in Chinese). MR 95m:11027. Hunan: Hunan Science & Technology Press, 1993.

AMS Classification Numbers: 11B39, 11B50, 11C20, 11B37

❖❖❖