CONGRUENCE RELATIONS FOR k^{th}-ORDER LINEAR RECURRENCES

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

(Submitted January 1987)

1. Introduction

Let k be a positive integer and let $\{T_n\}_{n=0}^{\infty}$ be a k^{th}-order integral linear recurrence defined by

$$T_{n+k} = a_1T_{n+k-1} + a_2T_{n+k-2} + \cdots + a_kT_n \tag{1}$$

with arbitrary initial terms $T_0, T_1, \ldots, T_{k-1}$. Associated with the recursion relation (1) is the characteristic polynomial

$$f(x) = x^k - a_1x^{k-1} - \cdots - a_{k-1}x - a_k \tag{2}$$

with characteristic roots $r_1, r_2, \ldots, r_k$. We will seek subsequences of $\{T_n\}$ such that the recursion relation (1) is also satisfied as a congruence modulo some integer m. Specifically, we will endeavor to find positive integers d and n such that

$$T_{n+kd} \equiv a_1T_{n+(k-1)d} + a_2T_{n+(k-2)d} + \cdots + a_{k-1}T_{n+d} + a_kT_n \pmod{m} \tag{3}$$

for all nonnegative integers n. This investigation was suggested by Freitag [2] and by Freitag and Phillips [3] and [4], and will generalize the results of these papers.

Two approaches will be taken in satisfying congruence (3). In the first approach, given a fixed modulus m we will seek to find integers d such that (3) is satisfied. Along these lines, Freitag [2] proved the following theorem:

Theorem 1: Let $\{F_n\}$ as usual denote the Fibonacci sequence. Then

$$F_{n+2d} \equiv F_{n+d} + F_n \pmod{10} \tag{4}$$

for all nonnegative integers n if and only if $d \equiv 1$ or $5 \pmod{12}$.□

The second approach will be to take the integer d from among the integers appearing in a specified sequence such as the sequence of primes and then find moduli m, depending on d, such that congruence (3) is satisfied. Corresponding to this approach, Freitag and Phillips proved Theorems 2 and 3 in [3] and [4], respectively.

Theorem 2: Let $\{T_n\}$ be a second-order recurrence defined by

$$T_{n+2} = a_1T_{n+1} + a_2T_n.$$

Then, if p is a prime greater than 3,

$$T_{n+2p} \equiv a_1T_{n+p} + a_2T_n \pmod{2p}$$

for all nonnegative integers n.□

Theorem 3: Let $\{T_n\}$ be a k^{th}-order recurrence with distinct characteristic roots satisfying

$$T_{n+k} = a_1T_{n+k-1} + a_2T_{n+k-2} + \cdots + a_kT_n.$$

Then, if p is a prime,

$$T_{n+kp} \equiv a_1 T_{n+(k-1)p} + a_2 T_{n+(k-2)p} + \cdots + a_{k-1} T_{n+p} + a_k T_n \pmod{p}$$

for all nonnegative integers n.□

2. Definitions and Known Results

We will need the following definitions and lemmas to continue.

Lemma 1: Let $\{T_n\}$ be a k^{th}-order linear recurrence with distinct characteristic roots $r_1, r_2, \ldots, r_m$. Then

$$T_n = \sum_{i=1}^{m} (c_i^{(0)} + c_i^{(1)} n + \cdots + c_i^{(s_i-1)} n^{s_i-1}) r_i^n,$$

where the $c_i^{(j)}$ are complex constants and s_i is the multiplicity of the root r_i.

Proof: This is a classical result in the theory of finite differences (see, for example, Milne-Thomson [5, Ch. XIII]).□

Definition 1: The primary linear recurrence $\{V_n\}_{n=0}^{\infty}$ is the recurrence satisfying (1) and defined by

$$V_n = r_1^n + r_2^n + \cdots + r_k^n,$$

where $r_1, r_2, \ldots, r_k$ are the zeros of the characteristic polynomial (2). If any characteristic root $r_i = 0$, we define r_i^0 to be 1.

Lemma 2: Suppose $\{T_n\}$ is a k^{th}-order linear recurrence satisfying

$$T_{n+k} = a_1 T_{n+k-1} + a_2 T_{n+k-2} + \cdots + a_k T_n.$$

Suppose m is a positive integer such that $(a_k, m) = 1$. Then $\{T_n\}$ is purely periodic modulo m.

Proof: This is proved by Carmichael [1, p. 344].□

Lemma 3: Let $\{T_n\}$ be a k^{th}-order integral linear recurrence with characteristic roots $r_1, r_2, \ldots, r_k$. Let h be a fixed positive integer, and let q be a fixed nonnegative integer. Then the sequence

$$\{S_n\}_{n=0}^{\infty} = \{T_{hn+q}\}_{n=0}^{\infty}$$

also satisfies a linear integral recursion relation

$$S_{n+k} = a_1^{(h)} S_{n+k-1} + a_2^{(h)} S_{n+k-2} + \cdots + a_k^{(h)} S_n, \tag{5}$$

where $a_1^{(h)}, a_2^{(h)}, \ldots, a_k^{(h)}$ are integral constants dependent on h but not on q. Further, if j is a fixed integer such that $1 \le j \le k$, then

$$a_j^{(h)} = \sum (-1)^j r_{i_1}^h r_{i_2}^h \cdots r_{i_j}^h, \tag{6}$$

where one sums over all indices $i_1, i_2, \ldots, i_j$ such that

$$1 \le i_1 < i_2 < \cdots < i_j \le k.$$

Proof: This is proved in [6].□

3. Main Results

We now present our principal theorems.

Theorem 4: Let $\{T_n\}$ be a k^{th}-order recurrence defined by

$$T_{n+k} = a_1T_{n+k-1} + a_2T_{n+k-2} + \cdots + a_kT_n.$$

Let p be a prime. Then for all nonnegative integers b,

$$T_{n+kp^b} \equiv a_1T_{n+(k-1)p^b} + a_2T_{n+(k-2)p^b} + \cdots + a_{k-1}T_{n+p^b} + a_kT_n \pmod{p},$$

where n is any nonnegative integer.

Proof: Let $r_1, r_2, \ldots, r_m$ be the distinct characteristic roots of $\{T_n\}$. Let R denote the integers of the algebraic number field $Q(r_1, r_2, \ldots, r_m)$, where Q denotes the rational numbers. Let Z denote the rational integers. Let P be a prime ideal of R dividing p. Let σ be the Frobenius automorphism of the finite field R/P having Z/p as a fixed field. Then σ is defined by $\sigma(x) = x^p$. Then, for any nonnegative integer b, σ^b, defined by $\sigma^b(x) = x^{p^b}$, is also an automorphism of R/P fixing Z/p.

Now, for $1 \le i \le m$,

$$r_i^k = a_1r_i^{k-1} + a_2r_i^{k-2} + \cdots + a_{k-1}r_i + a_k. \tag{7}$$

Applying σ^b to equation (7), we have, for $1 \le i \le m$,

$$\begin{aligned}\sigma^b(r_i^k) &\equiv r_i^{kp^b} \equiv \sigma^b(a_1r_i^{k-1} + a_2r_i^{k-2} + \cdots + a_k) \equiv \sum_{j=1}^{k} a_j\sigma^b(r_i^{k-j}) \\ &\equiv \sum_{j=1}^{k} a_jr_i^{(k-j)p^b} \pmod{P}.\end{aligned} \tag{8}$$

By (8), (1), and Lemma 1, we have

$$\begin{aligned}T_{n+kp^b} &= \sum_{i=1}^{m}\left[\left(c_i^{(0)} + c_i^{(1)}n + \cdots + c_i^{(m_i-1)}n^{m_i-1}\right)r_i^n\right]r_i^{kp^b} \\ &\equiv \sum_{i=1}^{m}\left[\left(c_i^{(0)} + c_i^{(1)}n + \cdots + c_i^{(m_i-1)}n^{m_i-1}\right)r_i^n\right]\sum_{j=1}^{k}a_jr_i^{(k-j)p^b} \\ &\equiv \sum_{j=1}^{k}a_j\sum_{i=1}^{m}\left(c_i^{(0)} + c_i^{(1)}n + \cdots + c_i^{(m_i-1)}n^{m_i-1}\right)r_i^{n+(k-j)p^b} \\ &\equiv \sum_{j=1}^{k}a_jT_{n+(k-j)p^b} \pmod{P}.\end{aligned} \tag{9}$$

Since the first and last terms of (9) are rational integers, we have

$$T_{n+kp^b} \equiv \sum_{j=1}^{k}a_jT_{n+(k-j)p^b} \pmod{p}. \square$$

Remark: We note that Theorem 4 is a generalization of Theorem 3.

Theorem 5: Let $\{T_n\}$ be a k^{th}-order recurrence defined by

$$T_{n+k} = a_1T_{n+k-1} + a_2T_{n+k-2} + \cdots + a_kT_n.$$

Let c be a fixed positive integer such that $(c, a_k) = 1$. Then there exists a fixed modulus g such that if $h \equiv 1 \pmod{g}$, then

$$T_{n+kh} \equiv a_1T_{n+(k-1)h} + a_2T_{n+(k-2)h} + \cdots + a_{k-1}T_{n+h} + a_kT_n \pmod{c},$$

where n is any nonnegative integer.

Proof: If h is any positive integer, then by (5) and (6),

$$T_{n+kh} = a_1^{(h)} T_{n+(k-1)h} + a_2^{(h)} T_{n+(k-2)h} + \cdots + a_k^{(h)} T_n, \tag{10}$$

where, for $1 \le j \le k$,

$$a_j^{(h)} = \sum (-1)^{j+1} r_{i_1}^h r_{i_2}^h \ldots r_{i_j}^h, \tag{11}$$

where one sums over all indices $i_1, i_2, \ldots, i_j$ such that

$$1 \le i_1 < i_2 < \cdots < i_j \le k.$$

Let $n_j = \binom{k}{j}$. Let $1 \le j \le k$ be a fixed integer and let $t_1^{(j)}, t_2^{(j)}, \ldots, t_{n_j}^{(j)}$ denote the $\binom{k}{j}$ algebraic integers $(-1)^{j+1} r_{i_1} r_{i_2} \ldots r_{i_j}$, where these represent all the $\binom{k}{j}$ products taken j at a time of the characteristic roots $r_1, r_2, \ldots, r_k$ of $\{T_n\}$. By the theory of symmetric polynomials, for a fixed integer j such that $1 \le j \le k$, the n_j algebraic integers $t_1^{(j)}, t_2^{(j)}, \ldots, t_{n_j}^{(j)}$ are the roots, possibly with repetitions, of a monic polynomial of degree n_j with rational integral coefficients.

Let $\{V_n^{(j)}\}$, defined by

$$V_n^{(j)} = (t_1^{(j)})^n + (t_2^{(j)})^n + \cdots + (t_{n_j}^{(j)})^n$$

be the primary linear recurrence with characteristic roots $t_1^{(j)}, t_2^{(j)}, \ldots, t_{n_j}^{(j)}$. Since $(a_k, c) = 1$, it follows by Lemma 2 that $\{V_n^{(j)}\}$ is purely periodic modulo c. Let d_j denote the period modulo c of $\{V_n^{(j)}\}$ for $1 \le j \le k$. Let g be the least common multiple of $d_1, d_2, \ldots, d_k$. Since by (11),

$$V_1^{(j)} = a_j^{(1)} = a_j,$$

it follows that if $h \equiv 1 \pmod{g}$, then

$$a_j^{(h)} = V_h^{(j)} \equiv V_1^{(j)} = a_j \pmod{c}. \tag{12}$$

The result now follows by (10).□

Corollary: Let $\{T_n\}$ be a k^{th}-order linear recurrence defined by

$$T_{n+k} = a_1 T_{n+k-1} + a_2 T_{n+k-2} + \cdots + a_k T_n.$$

Let p be a fixed prime such that $p \nmid a_k$. Then there exists a fixed modulus g such that if $h \equiv p^b \pmod{g}$, where b is any nonnegative integer, then

$$T_{n+kh} \equiv a_1 T_{n+(k-1)h} + a_2 T_{n+(k-2)h} + \cdots + a_k T_n \pmod{p},$$

where n is any nonnegative integer.

Proof: Let $\{V_n\}$ be any primary linear recurrence with characteristic roots $r_1, r_2, \ldots, r_k$. Then

$$V_{p^b} = r_1^{p^b} + r_2^{p^b} + \cdots + r_k^{p^b} \equiv (r_1 + r_2 + \cdots + r_k)^{p^b} = (V_1)^{p^b} \equiv V_1 \pmod{p}.$$

Let the primary linear recurrences $\{V_n^{(j)}\}$ and the integers $a_j^{(h)}$, where $1 \le j \le k$, be defined as in the proof of Theorem 5. Choose the modulus g in the same manner as in the proof of Theorem 5, letting $p = c$. Then

$$V_{p^b}^{(j)} \equiv V_h^{(j)} \pmod{g}$$

and

$$a_j^{(h)} = V_h^{(j)} \equiv V_{p^b}^{(j)} \equiv V_1^{(j)} = a_j \pmod{p}$$

for all j such that $1 \le j \le k$. The proof now follows by (10).□

Remark 1: Note that if p is a fixed prime, the corollary to Theorem 5 is a strengthening of Theorem 4.

Remark 2: Theorem 1 follows from the corollary to Theorem 5. By the proof of this corollary, it can be shown that if $d \equiv 1$ or 5 (mod 12), then

$$F_{n+2d} \equiv F_{n+d} + F_n \pmod 5. \tag{13}$$

Similarly, it can be shown that if $d \equiv 1$ or 2 (mod 3), then

$$F_{n+2d} \equiv F_{n+d} + F_n \pmod 2. \tag{14}$$

It thus follows that if $d \equiv 1$ or 5 (mod 12), then (14) holds. Since 2 and 5 are relatively prime, it follows from (13)-(14) that if $d \equiv 1$ or 5 (mod 12), then congruence (4) holds. This proves the necessity of Theorem 1. The sufficiency of Theorem 1 follows from the fact that $\{F_n\}$ has a period modulo 10 equal to 60. Examining (4) for all integral values of d between 1 and 60 establishes the result.

Theorem 6: Let $\{T_n\}$ be a k^{th}-order linear recurrence defined by

$$T_{n+k} = a_1T_{n+k-1} + a_2T_{n+k-2} + \cdots + a_kT_n.$$

Let c be a fixed positive integer such that $(c, a_k) = 1$. Then for all nonnegative integers b, there exists an infinite number of primes p of positive density in the set of primes such that

$$T_{n+kp^b} \equiv a_1T_{n+(k-1)p^b} + a_2T_{n+(k-2)p^b} + \cdots + a_{k-1}T_{n+p^b} + a_kT_n \pmod{cp}, \tag{15}$$

where n is any nonnegative integer. Furthermore, there exists a fixed modulus g such that if $p \equiv 1 \pmod g$, then congruence (15) is satisfied.

Proof: By Theorem 4, the congruence (15) is satisfied modulo p for any prime p. Given the integer c, we choose the modulus g in the same manner as in the proof of Theorem 5. By Dirichlet's theorem on the infinitude of primes in arithmetic progressions, there exists an infinite number of primes p such that $p \equiv 1 \pmod g$. Further, the density of such primes is $1/\phi(g)$, where ϕ denotes Euler's totient function. By Theorem 5, congruence (15) is also satisfied modulo c, since p^b is also congruent to 1 modulo g for any nonnegative integer b. Since we can also assume that $(p, c) = 1$, it follows that (15) is satisfied modulo cp.□

Corollary 1: Let $\{T_n\}$ be a k^{th}-order linear recurrence defined by

$$T_{n+k} = a_1T_{n+k-1} + a_2T_{n+k-2} + \cdots + a_kT_n.$$

Let c be a fixed prime such that $c \nmid a_k$. Then for all nonnegative integers b, there exists an infinite number of primes p of positive density in the set of primes such that

$$T_{n+kp^b} \equiv a_1T_{n+(k-1)p^b} + a_2T_{n+(k-2)p^b} + \cdots + a_{k-1}T_{n+p^b} + a_kT_n \pmod{cp}, \tag{16}$$

where n is any nonnegative integer. Furthermore, there exists a fixed modulus g such that if the prime $p \equiv c^b \pmod g$, where b is any nonnegative integer, then congruence (16) is satisfied.

Proof: This follows by the corollary to Theorem 5 and the proof of Theorem 6.

Corollary 2: Let $\{T_n\}$ be a second-order linear recurrence defined by

$$T_{n+2} = a_1 T_{n+1} + a_2 T_n.$$

Then for all primes $p > 3$ and for all nonnegative integers b,

$$T_{n+2p^b} \equiv a_1 T_{n+p^b} + a_2 T_n \pmod{2p}, \tag{17}$$

where n is any nonnegative integer.

Proof: Let $p > 3$ be a prime. By Theorem 4, congruence (17) holds modulo p for all n. We will show that (17) also holds modulo 2 for all n. The corollary will then follow since $(2, p) = 1$.

First, suppose that $2|a_2$. Considering the characteristic polynomial $f(x)$ of $\{T_n\}$ modulo 2, we have

$$f(x) = x^2 - a_1 x - a_2 \equiv x(x - a_1) \pmod{2}.$$

Hence, the characteristic roots of $\{T_n\}$ modulo 2 are $r_1 \equiv a_1 \pmod{2}$ and $r_2 \equiv 0 \pmod{2}$. As in the proof of Theorem 5, we have that if h is any nonnegative integer, then

$$T_{n+2h} = a_1^{(h)} T_{n+h} + a_2^{(h)} T_n, \tag{18}$$

where $a_1^{(h)}$ and $a_2^{(h)}$ are defined as in equation (11). Constructing the primary linear recurrences $\{V_n^{(1)}\}$ and $\{V_n^{(2)}\}$ as in the proof of Theorem 5, we observe that

$$V_n^{(1)} \equiv a_1 \pmod{2} \tag{19}$$

for all $n \geq 1$ and

$$V_n^{(2)} \equiv a_2 \equiv 0 \pmod{2} \tag{20}$$

for all $n \geq 1$. By (12) and (18)-(20), we see that for $j = 1$ or 2,

$$a_j^{(h)} = V_h^{(j)} \equiv a_j \pmod{2} \tag{21}$$

for all positive integers h. Letting $h = p^b$, equation (18) and congruence (21) lead to the congruence

$$T_{n+2p^b} \equiv a_1 T_{n+p^b} + a_2 T_n \pmod{2},$$

which is what we wanted to show.

Now, suppose that $2 \nmid a_2$. Constructing the primary recurrences $\{V_n^{(1)}\}$ and $\{V_n^{(2)}\}$ as in the proof of Theorem 5, we see that $\{V_n^{(1)}\}$ and $\{V_n^{(2)}\}$ are each purely periodic modulo 2 by Lemma 2. Further, one can easily determine that the period of the second-order recurrence $\{V_n^{(1)}\}$ modulo 2 is either 2 or 3, and the period of the first-order recurrence $\{V_n^{(2)}\}$ modulo 2 is 1. It thus follows that if we determine the modulus g, as in the proof of Theorem 5, then $g = 2$ or 3. By Theorem 5, if $g = 2$ and p is a prime such that $p \equiv 1 \pmod{2}$, then congruence (17) holds modulo 2. By the corollary to Theorem 5, if $g = 3$ and p is a prime such that $p \equiv 1$ or $2 \pmod{3}$, then the congruence (17) again holds modulo 2. Since for any $p > 3$, $p \equiv 1 \pmod{2}$ and $p \equiv 1$ or $2 \pmod{3}$, the result now follows. □

Remark: Note that Corollary 2 to Theorem 6 generalizes Theorem 2.

References

1. R. D. Carmichael. "On Sequences of Integers Defined by Recurrence Relations." *Quart. J. Pure Appl. Math.* *48* (1920):343-372.

2. H. T. Freitag. "A Property of Unit Digits of Fibonacci Numbers." *Fibonacci Numbers and Their Applications*. Edited by A. N. Philippou, G. E. Bergum, & A. F. Horadam. Dordrecht, Holland: D. Reidel, 1986, pp. 39-41.
3. H. T. Freitag & G. M. Phillips. "A Congruence Relation for Certain Recursive Sequences." *Fibonacci Quarterly 24.4* (1986):332-335.
4. H. T. Freitag & G. M. Phillips. "A Congruence Relation for a Linear Recursive Sequence of Arbitrary Order." *Applications of Fibonacci Numbers*. Edited by A. N. Philippou, A. F. Horadam, & G. E. Bergum. Dordrecht, Holland: Kluwer Academic Publishers, 1988, pp. 39-44.
5. L. M. Milne-Thomson. *The Calculus of Finite Differences*. London: Macmillan, 1960.
6. L. Somer. Solution to Problem H-377. *Fibonacci Quarterly 24.3* (1986):284-285.

*****

REFEREES

In addition to the members of the Board of Directors and our Assistant Editors, the following mathematicians, engineers, and physicists have assisted **THE FIBONACCI QUARTERLY** by refereeing papers during the past year. Their special efforts are sincerely appreciated, and we apologize for any names that have inadvertently been overlooked or misspelled.

AKRITAS, A. G.
University of Kansas
ANDERSON, Sabra
University of Minnesota-Duluth
ANDO, Shiro
Hosei University
ANDREWS, George E.
Pennsylvania State University
BACKSTROM, Robert P.
GYMEA, New South Wales
BALTUS, Christopher
SUNY College at Oswego
BENNETT, Larry F.
South Dakota State University
BERNDT, Bruce C.
University of Illinois
BERZSENYI, George
Rose-Hulman
BEZUSZKA, Stanley J.
Boston College
BOLLINGER, Richard C.
Pennsylvania State University-Erie
BRESSOUD, David M.
Pennsylvania State University
BRUCE, Ian
St. Peter's Collegiate School
BUMBY, Richard T.
Rutgers University
BURKE, John
Gonzaga University
BURTON, David M.
University of New Hampshire
CACOULLOS, T.
University of Athens
CAMPBELL, Colin
University of St. Andrews
CANTOR, David G.
University of California at LA
CAPOCELLI, Renato M.
University' di Salerno
CASTELLANOS, Dario
Valencia, Venezuela
CHANG, Derek
California State University at LA
CHARALAMBIDES, Ch. A.
University of Athens
CHURCH, C. A.
University of North Carolina-Greensboro
COHEN, M. E.
California State University-Fresno
COHN, J. H. E.
Royal Holloway College
COOPER, Curtis
Central Missouri State University
CREELY, Joseph W.
Vincetown, New Jersey
DAVIS, Philip J.
Brown University
DEARDEN, Bruce
University of North Dakota
deBRUIN, Marcel G.
University of Amsterdam
DeLEON, M. J.
Florida Atlantic University
DENCE, Thomas P.
Ashland College
DEO, Narsingh
University of Central Florida
DEUFLHARD, Peter J.
Berlin, Germany
DEVANEY, Robert L.
Boston University
DODD, Fred
University of South Alabama
DOWNEY, Peter J.
The University of Arizona
DUDLEY, Underwood
DePauw University
ECKERT, Ernest J.
University of South Carolina-Aiken
ENNEKING, Eugene A.
Portland State University
EWELL, John A.
Northern Illinois University
FARRELL, E. J.
University of the West Indies
FILASETA, Michael
University of South Carolina
FRAENKEL, Aviezri S.
Weizmann Institute of Science
FUCHS, Eduard
University of J. E. Purkyne
GALL, Lisl
University of Minnesota-Minneapolis
GALLIAN, Joseph A.
University of Minnesota-Duluth
GORDON, Basil
University of California-LA
GUY, Richard
University of Calgary
HARBORTH, Heiko
Braunschweig, West Germany
HARRIS, V. C.
San Diego, California
HAUKKANEN, Pentti
University of Tampere
HAYES, David F.
San Jose State University