The Fibonacci Quarterly 2003 (41,1): 41-47

ON LACUNARY RECURRENCES

Paul Thomas Young
Dept. of Mathematics, University of Charleston, Charleston, SC 29424
e-mail: paul@math.cofc.edu
(*Submitted November 2000*)

1. INTRODUCTION

Let $\{a_n\}_{n=-\infty}^{\infty}$ be a sequence which satisfies a linear recurrence of order $k+1$. We are herein concerned with the lacunary subsequences $\{a_{mn+b}\}_{n=-\infty}^{\infty}$, where m and b are fixed integers, so called because they consist of the terms from $\{a_n\}$ with *lacunae*, or gaps, of length m between them. In [5], [2], and [3] it has been shown that, for any m and b, the subsequences $\{a_{mn+b}\}$ also satisfy a linear recurrence of order $k+1$. In this note we shall express the coefficients of this recurrence in terms of generalized Dickson polynomials, by means of their functional equations, and present some applications of this description. As corollaries to our main theorem we give generalizations, to prime power moduli, of the known result ([5], Theorem 4) that whenever p is prime, the subsequences $\{a_{p^r n+b}\}_{n=0}^{\infty}$ satisfy the same linear recurrence modulo p as is satisfied by $\{a_n\}$. We conclude with an analog of Howard's tribonacci identity ([3], Theorem 3.1) for tetranacci sequences.

2. THE MAIN RESULT

Let our sequence $\{a_n\}$ satisfy a linear recurrence of order $k+1$, say

$$a_{n+k} = x_1 a_{n+k-1} - x_2 a_{n+k-2} + \cdots - (-1)^k x_k a_n + (-1)^k a a_{n-1}, \tag{2.1}$$

where a is a unit in some integral domain R and $x_1, x_2, \ldots, x_k$ are indeterminates over R. (By use of evaluation homomorphisms $R[x_1, \ldots, x_k] \to R$, one may also regard $x_1, x_2, \ldots, x_k$ as elements of R). If we are given some initial conditions, say $a_0, a_1, \ldots, a_k \in R[x_1, \ldots, x_k]$, then the recurrence (2.1) may be used to define a_n for all integers n, and for any integer b we have a formal power series identity

$$\sum_{n=0}^{\infty} a_{n+b} T^n = \frac{Q(T)}{P(T)} \tag{2.2}$$

in the formal power series ring $R[x_1, x_2, \ldots, x_k][\![T]\!]$, where

$$P(T) = 1 - x_1 T + x_2 T^2 + \cdots + (-1)^k x_k T^k - (-1)^k a T^{k+1} \tag{2.3}$$

is the characteristic polynomial of the recurrence (2.1) and $Q(T)$ is some polynomial of degree at most k.

Now let K be the quotient field of the polynomial ring $R[x_1, x_2, \ldots, x_k]$. Then over some finite extension field L of K the polynomial $P(T)$ splits into the product

$$P(T) = \prod_{j=0}^{k} (1 - \alpha_j T). \tag{2.4}$$

It follows that $x_j = \sigma_j(\alpha_0, \ldots, \alpha_k)$ for $1 \le j \le k$ and $a = \sigma_{k+1}(\alpha_0, \ldots, \alpha_k)$, where σ_j denotes the j^{th} elementary symmetric function in $k+1$ indeterminates.

For $1 \le i \le k$, let $P^{(i)}(T)$ be the polynomial in $R[x_1, \ldots, x_k][T]$ of degree $l = \binom{k+1}{i}$ with constant term 1 whose reciprocal roots are all products of the form $\alpha_{j_1} \ldots \alpha_{j_i}$, where $0 \le j_1 < \cdots < j_i \le k$. The coefficients of $P^{(i)}$ are symmetric functions of $\alpha_0, \ldots, \alpha_k$, and therefore there are polynomials $y_{j,i}$ in $R[x_1, \ldots, x_k]$ such that

$$P^{(i)}(T) = 1 - y_{1,i}T + y_{2,i}T^2 + \cdots + (-1)^l y_{l,i}T^l, \tag{2.5}$$

with $y_{1,i} = x_i$ and $y_{l,i} = a^i$. The generalized Dickson polynomials $D_m^{(i)}$ (over R) are then defined for $m > 0$ by the expansion

$$\frac{dP^{(i)}}{P^{(i)}} = -\sum_{m=1}^{\infty} D_m^{(i)}(x_1, \ldots, x_k, a)T^m \frac{dT}{T} \tag{2.6}$$

in $R[x_1, \ldots, x_k][[T]]$ (cf. [6], eq. (1.6)). The usual Dickson polynomials $D_m(x, a)$ are obtained in this way from $P(T) = 1 - xT + aT^2$ with $i = k = 1$, and if R is a finite field then this definition of generalized Dickson polynomials agrees with that given in [4]. From the generating form (2.6), we may derive for $m > 0$ the functional equations (cf. [6], eq. 2.5))

$$D_m^{(i)}(x_1, \ldots, x_k, a) = \sigma_i(\alpha_0^m, \ldots, \alpha_k^m) \quad (1 \le i \le k) \tag{2.7}$$

and the identity $a^m = \alpha_0^m \alpha_1^m \ldots \alpha_k^m$. These relations may be used to define the polynomials $D_m^{(i)}(x_1, \ldots, x_k, a) \in R[x_1, \ldots, x_k]$ for all integers m; specifically, we have

$$D_0^{(i)}(x_1, \ldots, x_k, a) = \binom{k+1}{i} \tag{2.8}$$

for $m = 0$, and for any integer m we have

$$D_m^{(i)}(x_1, \ldots, x_k, a) = a^m D_{-m}^{(j)}(x_1, \ldots, x_k, a), \tag{2.9}$$

where $i + j = k + 1$. With this definition, the polynomial $D_m^{(i)}$ is a polynomial of total degree $|m|$ in $R[x_1, \ldots, x_k]$ for every integer m. Now we are ready to state the main theorem.

Theorem 1: Let $\{a_n\}$ satisfy the linear recurrence (2.1) in $R[x_1, \ldots, x_k]$. Then, for any integers m and b, the lacunary subsequence $\{a_{mn+b}\}$ in $R[x_1, \ldots, x_k]$ satisfies the recurrence

$$a_{km+b} = \left(\sum_{i=1}^{k} (-1)^{i-1} D_m^{(i)}(x_1, \ldots, x_k, a) a_{(k-i)m+b} \right) + (-1)^k a^m a_{b-m}.$$

Proof: Let m and b be given. If $m = 0$, the statement of the theorem reduces to the very well-known identity

$$\sum_{i=0}^{k+1} (-1)^i \binom{k+1}{i} = 0 \tag{2.10}$$

by (2.8). Assuming the theorem is true for m, it follows also for $-m$ by (2.9); therefore, it suffices to assume m is positive. Consider the generating function (2.2) for the sequence $\{a_{n+b}\}$. Define the linear operator φ on $R[x_1, \ldots, x_k][[T]]$ by

$$\varphi f(T) = \frac{1}{m}(f(T) + f(\theta T) + f(\theta^2 T) + \cdots + f(\theta^{m-1} T)) \tag{2.11}$$

where θ is a primitive m^{th} root of unity in some finite extension of K. Since

$$\varphi(T^j) = \begin{cases} T^j, & \text{if } m \text{ divides } j, \\ 0, & \text{otherwise,} \end{cases} \tag{2.12}$$

we have

$$\varphi\left(\sum_{n=0}^{\infty} a_{n+b} T^n\right) = \sum_{n=0}^{\infty} a_{mn+b} T^{mn}, \tag{2.13}$$

which is the generating function for our lacunary subsequence.

By virtue of the factorization (2.4), we have a partial fraction decomposition

$$\frac{Q(T)}{P(T)} = \sum_{i=0}^{k} \frac{c_i}{(1-\alpha_i T)^{e_i}}, \tag{2.14}$$

valid as a power series identity in the subring $R[x_1, \ldots, x_k][\![T]\!]$ of $L[\![T]\!]$, where the exponents are defined by setting e_i equal to 1 plus the number of α_j with $\alpha_j = \alpha_i$ and $j < i$ (so, e.g., all e_i are 1 if and only if all α_i are distinct). Then we compute in $L(\theta)[\![T]\!]$

$$\begin{aligned} \varphi\left(\frac{Q(T)}{P(T)}\right) &= \frac{1}{m}\sum_{j=0}^{m-1}\sum_{i=0}^{k}\frac{c_i}{(1-\alpha_i\theta^j T)^{e_i}} = \frac{1}{m}\sum_{i=0}^{k}\sum_{j=0}^{m-1}\frac{c_i}{(1-\alpha_i\theta^j T)^{e_i}} \\ &= \frac{1}{m}\sum_{i=0}^{k}\frac{Q_i(T^m)}{(1-\alpha_i^m T^m)^{e_i}} = \frac{\tilde{Q}(T^m)}{\tilde{P}(T^m)}, \end{aligned} \tag{2.15}$$

with each Q_i a polynomial of degree less than e_i, and $\tilde{Q}$ therefore a polynomial of degree at most k. It follows by comparison with (2.13) that $\tilde{P}$ is the characteristic polynomial for the recurrent sequence $\{a_{mn+b}\}$, where $\tilde{P}(T^m) = \prod_{i=0}^{k}(1-\alpha_i^m T^m)$. If we write

$$\tilde{P}(T) = 1 - y_1 T + y_2 T^2 + \cdots + (-1)^k y_k T^k - (-1)^k y_{k+1} T^{k+1}, \tag{2.16}$$

then we have $y_i = \sigma_i(\alpha_0^m, \ldots, \alpha_k^m)$ for $1 \le i \le k$ and $y_{k+1} = \alpha_0^m \alpha_1^m \ldots \alpha_k^m$. Hence, by the functional equations (2.7), we have $y_i = D_m^{(i)}(x_1, \ldots, x_k, a)$ for $1 \le i \le k$ and $y_{k+1} = a^m$, giving the result.

Remarks: In Theorem 1 we have assumed a is a unit in R; however, this assumption is needed only to ensure that a_n and $D_n^{(i)}$ are elements of R when n is negative. The recurrence given in the theorem remains valid in $R[x_1, \ldots, x_k]$ if a is an arbitrary element of R (even if $a = 0$), or in $R[x_1, \ldots, x_k, a]$ if a is regarded as an indeterminate over R, provided $b \ge m \ge 0$. It is equally valid for arbitrary integers m and b if interpreted as a recurrence in the Laurent ring $R[x_1, \ldots, x_k, a, a^{-1}]$.

3. CONGRUENCES FOR LACUNARY RECURRENCES

It is known ([5], Theorem 4) that, if $\{a_n\}_{n=0}^{\infty}$ is a linearly recurrent sequence in $\mathbb{Z}$ and p is prime, then the subsequence $\{a_{p^r n+b}\}_{n=0}^{\infty}$ satisfies the same linear recurrence modulo p as is satisfied by $\{a_n\}$. Theorem 1 and results of [6] give rise to some generalizations of this result.

Corollary 2: Let $\{a_n\}_{n=0}^{\infty}$ satisfy a linear recurrence

$$a_{n+k} = x_1 a_{n+k-1} - x_2 a_{n+k-2} + \cdots - (-1)^k x_k a_n + (-1)^k a\, a_{n-1}$$

in $R[x_1, \ldots, x_k, a]$, and let $\{a'_n\}_{n=0}^{\infty}$ satisfy the linear recurrence

$$a'_{n+k} = x_1^p a'_{n+k-1} - x_2^p a'_{n+k-2} + \cdots - (-1)^k x_p^k a'_n + (-1)^k a^p a'_{n-1}$$

in $R[x_1, \ldots, x_k, a]$. Then for any prime p and any positive integers b, d, m, and r, the two lacunary subsequences $\{a_{mp^r n+b}\}_{n=0}^{\infty}$ and $\{a'_{mp^{r-1}n+d}\}_{n=0}^{\infty}$ in $R[x_1, \ldots, x_k, a]$ satisfy the same recurrence modulo $p^r R[x_1, \ldots, x_k, a]$.

Proof: In Theorem 2 of [6], we showed that the differential form (2.6) is an invariant differential on the multiplicative formal group law over the polynomial ring $R[x_1, \ldots, x_k, a]$, from which one may deduce the congruences

$$D^{(i)}_{mp^r}(x_1, \ldots, x_k, a) \equiv D^{(i)}_{mp^{r-1}}(x_1^p, \ldots, x_k^p, a^p) \pmod{p^r R[x_1, \ldots, x_k, a]} \tag{3.1}$$

in $R[x_1, \ldots, x_k, a]$. Since $a^{mp^r} = (a^p)^{mp^{r-1}}$, the corollary then follows from Theorem 1 and the observation that the left members of the congruences (3.1) are the coefficients of the recurrence for $\{a_{mp^r n+b}\}$ and the right members of the congruences (3.1) are the coefficients of the recurrence for $\{a'_{mp^{r-1}n+d}\}$.

Taking $m = r = 1$ in the above Corollary 2 yields a polynomial congruence which implies Theorem 3 of [5] and the main result of [1]. We now consider another generalization.

Corollary 3: Let $\{a_n\}_{n=0}^{\infty}$ satisfy the linear recurrence

$$a_{n+k} = x_1 a_{n+k-1} - x_2 a_{n+k-2} + \cdots - (-1)^k x_k a_n + (-1)^k a\, a_{n-1}$$

in $\mathbb{Z}$. Then, for any prime p and any positive integers b, d, m, and r, the two lacunary subsequences $\{a_{mp^r n+b}\}_{n=0}^{\infty}$ and $\{a_{mp^{r-1}n+d}\}_{n=0}^{\infty}$ in $\mathbb{Z}$ satisfy the same recurrence modulo p^r.

Proof: In Theorem 3 of [6], we showed that, for any integers $x_1, \ldots, x_k, a$, the differential form (2.6) is an invariant differential on the multiplicative formal group law over $\mathbb{Z}$, from which one may deduce the congruences

$$D^{(i)}_{mp^r}(x_1, \ldots, x_k, a) \equiv D^{(i)}_{mp^{r-1}}(x_1, \ldots, x_k, a) \pmod{p^r \mathbb{Z}} \tag{3.2}$$

for any integers $x_1, \ldots, x_k, a$. Since $a^{mp^r} \equiv a^{mp^{r-1}} \pmod{p^r}$, the corollary then follows from Theorem 1 and the observation that the left members of the congruences (3.2) are the coefficients of the recurrence for $\{a_{mp^r n+b}\}$ and the right members of the congruences (3.2) are the coefficients of the recurrence for $\{a_{mp^{r-1}n+d}\}$.

The $r = 1$ case of this theorem contains the result of [1] and Theorems 3 and 4 of [5]. To illustrate the general case, consider the example of the tribonacci sequence $\{P_n\}$ defined by the recurrence

$$P_{n+2} = P_{n+1} + P_n + P_{n-1} \tag{3.3}$$

with P_0, P_1, P_2 arbitrary integers. As a special case of Theorem 1, we have Howard's general formula (see [3], eq. (3.6)) for the lacunary subsequences $\{P_{mn+b}\}$ which implies, for example,

$$P_{n+4} = 3P_{n+2} + P_n + P_{n-2}, \tag{3.4}$$

$$P_{n+8} = 11P_{n+4} + 5P_n + P_{n-4}, \tag{3.5}$$

$$P_{n+16} = 131P_{n+8} - 3P_n + P_{n-8}, \tag{3.6}$$

$$P_{n+32} = 17155P_{n+16} + 253P_n + P_{n-16}. \tag{3.7}$$

We observe that the recurrence coefficients in (3.3) and (3.4) agree modulo 2, while those in (3.4) and (3.5) agree modulo 2^2, those in (3.5) and (3.6) agree modulo 2^3, and those in (3.6) and (3.7) agree modulo 2^4, as predicted by Corollary 3 for $p = 2$. For $p = 3$ one has

$$P_{n+6} = 7P_{n+3} - 5P_n + P_{n-3}, \tag{3.8}$$

$$P_{n+18} = 241P_{n+9} - 23P_n + P_{n-9}, \tag{3.9}$$

$$P_{n+54} = 13980895P_{n+27} + 4459P_n + P_{n-27}, \tag{3.10}$$

with the recurrence coefficients in (3.3) and (3.8) agreeing modulo 3, those in (3.8) and (3.9) agreeing modulo 3^2, and those in (3.9) and (3.10) agreeing modulo 3^3. Once more,

$$P_{n+10} = 21P_{n+5} + P_n + P_{n-5}, \tag{3.11}$$

$$P_{n+50} = 4132721P_{n+25} + 2201P_n + P_{n-25}, \tag{3.12}$$

with the recurrence coefficients in (3.3) and (3.11) agreeing modulo 5, and those in (3.11) and (3.12) agreeing modulo 5^2.

The system of congruences (3.2) implies that $\{D^{(i)}_{mp^r}(x_1, \ldots, x_k, a)\}_{r=0}^{\infty}$ is a Cauchy sequence in the ring $\mathbb{Z}_p$ of p-adic integers for fixed $x_1, \ldots, x_2$, a, m, i, and any prime p, and therefore converges p-adically to some limit $H^{(i)}_m$. Combining Theorem 1 with the complete statement of Theorem 3 in [6] therefore allows a p-adic restatement of Corollary 3.

Corollary 3 (alternate version): Let $\{a_n\}_{n=0}^{\infty}$ satisfy the linear recurrence

$$a_{n+k} = x_1 a_{n+k-1} - x_2 a_{n+k-2} + \cdots - (-1)^k x_k a_n + (-1)^k a\, a_{n-1}$$

in $\mathbb{Z}$ and let p be any prime. Then, for any positive integer m, there exist algebraic integers $H^{(1)}_m$, $\ldots$, $H^{(k)}_m$, A_m in $\mathbb{Z}_p$, which depend only on $x_1, \ldots, x_k, a \pmod p$, such that the lacunary subsequences $\{b_n\} = \{a_{mp^r n+d}\}$ satisfy

$$b_{n+k} \equiv H^{(1)}_m b_{n+k-1} - H^{(2)}_m b_{n+k-2} + \cdots - (-1)^k H^{(k)}_m b_n + (-1)^k A_m b_{n-1} \pmod{p^{r+1}\mathbb{Z}_p}$$

for all nonnegative integers r and d.

This version of the corollary says that associated to any integral linear recurrent sequence $\{a_n\}_{n=0}^{\infty}$ there is, for each positive integer m and each prime p, a *single* recurrence (with p-adic coefficients) that is satisfied modulo $p^{r+1}\mathbb{Z}_p$ by *every* lacunary subsequence $\{a_{mp^r n+d}\}_{n=0}^{\infty}$. As an illustration of the idea, from (3.7), we note that the recurrence

$$b_{n+2} = 17155b_{n+1} + 253b_n + b_{n-1} \tag{3.13}$$

is satisfied modulo 2^{r+1} by $\{b_n\} = \{P_{2^r n+d}\}$ for $r = 0, 1, 2, 3, 4$; analogous examples of this type for lacunary subsequences of $\{P_n\}$ are given by (3.10) for $p = 3$ and $r = 0, 1, 2, 3$, and by (3.12) for $p = 5$ and $r = 0, 1, 2$. A natural question to ask is: When will the "universal" p-adic recurrences of the corollary, which hold for all r, actually have integer coefficients?

This question may be answered to some extent in the case of second-order recurrences ($k = 1$) using the results of [7], where systems of congruences

$$D^{(1)}_{mp^r}(x, a) \equiv B \pmod{p^{r+1}} \tag{3.14}$$

for integer values of B were classified. In particular, combining Theorem 1 of the present paper with Theorem 1 of [7] yields the following corollary.

Corollary 4: Let $\{a_n\}_{n=0}^{\infty}$ satisfy the second-order linear recurrence

$$a_{n+1} = xa_n - a\,a_{n-1}$$

for integers x and a. Then, for every prime p, there exists an integer m and integers H_m and A_m such that the recurrence

$$b_{n+1} = H_m b_n - A_m b_{n-1}$$

is satisfied modulo p^{r+1} by the lacunary subsequence $\{b_n\} = \{a_{mp^r n+d}\}$ for all nonnegative integers r and d. Furthermore, $H_m \in \{-2, -1, 0, 1, 2\}$ and $A_m \in \{-1, 0, 1\}$.

The means for determining the integers m, H_m, and A_m are outlined in the corollary to Theorem 2 of [7]. A few examples involving the Fibonacci sequence $\{F_n\}$ are:

$$F_{n+m\cdot 2^r} \equiv -F_n - F_{n-m\cdot 2^r} \pmod{2^{r+1}} \text{ if } 3 \nmid m; \tag{3.15}$$

$$F_{n+m\cdot 2^r} \equiv 2F_n - F_{n-m\cdot 2^r} \pmod{2^{r+1}} \text{ if } 3 \mid m; \tag{3.16}$$

$$F_{n+m\cdot 3^r} \equiv -F_{n-m\cdot 3^r} \pmod{3^{r+1}} \text{ if } m \equiv \pm 2 \pmod 8; \tag{3.17}$$

$$F_{n+m\cdot 5^r} \equiv -2F_n - F_{n-m\cdot 5^r} \pmod{5^{r+1}} \text{ if } m \equiv 2 \pmod 4; \tag{3.18}$$

$$F_{n+m\cdot 7^r} \equiv -F_{n-m\cdot 7^r} \pmod{7^{r+1}} \text{ if } m \equiv \pm 4 \pmod{16}. \tag{3.19}$$

4. TETRANACCI SEQUENCES

In Theorem 2.1 of [3], Howard showed that if $\{a_n\}$ satisfies the recurrence (2.1) over $\mathbb{C}$ then, for any integers m and b, the lacunary subsequence $\{a_{mn+b}\}$ satisfies the recurrence

$$a_{km+b} = \sum_{j=1}^{k+1} (-1)^{j-1} c_{m,jm} a_{(k-j)m+b}, \tag{4.1}$$

where the numbers $c_{m,jm}$ are independent of the initial conditions $a_0, a_1, \ldots, a_k$, and are defined by a certain generating function. The identity $c_{m,(k+1)m} = a^m$ was shown in Lemma 2.2 of [3]; the result of Theorem 1 above shows that $c_{m,jm} = D_m^{(j)}(x_1, \ldots, x_k, a)$ for $1 \le j \le k$. In the tribonacci case ($k = 2$), Howard showed (see Lemma 3.2 of [3]) that $c_{m,m} = D_m$ and $c_{m,2m} = a^m D_{-m}$, where $D_m = D_m^{(1)}(x_1, x_2, a)$. This produces the beautiful identity (cf. [3], eq. (1.5))

$$a_{n+2m} = D_m a_{n+m} - a^m D_{-m} a_n + a^m a_{n-m}, \tag{4.2}$$

which is valid for all integers m and n; observe that $\{a_m\}$ and $\{D_m\}$ satisfy the *same* third-order recurrence. We remark that the two identities of Lemma 3.2 in [3] are generalized to arbitrary k by (2.9) and Theorem 1; specifically, we have

$$c_{m,m} = D_m \quad \text{and} \quad c_{m,km} = a^m D_{-m}, \tag{4.3}$$

where $D_m = D_m^{(1)}(x_1, \ldots, x_k, a)$. In the tetranacci case ($k = 3$), equation (4.3) expresses all but the central coefficient $c_{m,2m}$ in terms of a and D_m. Whereas $\{a_m\}$ and $\{D_m\}$ both satisfy the same fourth-order recurrence, this central coefficient $\{c_{m,2m}\}$ unfortunately satisfies a recurrence of

order $\binom{4}{2} = 6$. This suggests that perhaps there is no general simple analog of (4.2) for recurrences whose order exceeds three. However, by means of the functional equations (2.7), one may easily verify that $c_{m,2m} = D_m^{(2)}(x_1, \ldots, x_k, a) = (D_m^2 - D_{2m})/2$ over any integral domain R of characteristic not equal to 2. Therefore, we may state the following analog of Theorem 3.1 in [3] for tetranacci sequences.

Theorem 5: Let $\{a_n\}$ satisfy the linear recurrence

$$a_{n+3} = x_1 a_{n+2} - x_2 a_{n+1} + x_3 a_n - a\, a_{n-1}$$

in $R[x_1, x_2, x_3]$, where the characteristic of the integral domain R is different from 2 and a is a unit in R. Then, for any integers m and n, we have the identity

$$a_{n+3m} = D_m a_{n+2m} - \frac{1}{2}(D_m^2 - D_{2m})a_{n+m} + a^m D_{-m} a_n - a^m a_{n-m}$$

in $R[x_1, x_2, x_3]$, where $D_m = D_m^{(1)}(x_1, x_2, x_3, a)$.

REFERENCES

1. H. T. Freitag & G. M. Phillips. "A Congruence Relation for a Linear Recursive Sequence of Arbitrary Order." In *Applications of Fibonacci Numbers* **1**:39-44. Ed. G. E. Bergum et al. Dordrecht: Kluwer, 1988.
2. F. T. Howard. "Generalizations of a Fibonacci Identity." In *Applications of Fibonacci Numbers* **8**:201-11. Ed. F. T. Howard. Dordrecht: Kluwer, 1999.
3. F. T. Howard. "A Tribonacci Identity." *The Fibonacci Quarterly* **39.4** (2001):352-57.
4. R. Lidl & H. Niederreiter. "Finite Fields." *Encyclopedia of Mathematics and Its Applications* **20**. Reading, MA: Addison-Wesley, 1983.
5. L. Somer. "Congruence Relations for k^{th}-Order Linear Recurrences." *The Fibonacci Quarterly* **27.1** (1989):25-31.
6. P. T. Young. "Congruences for Generalised Dickson Polynomials." In *Applications of Finite Fields*. IMA Conference Series, Vol. 59, pp. 33-46. Ed. D. Gollman. Oxford: Oxford University Press, 1996.
7. P. T. Young. "On a Class of Congruences for Lucas Sequences." In *Applications of Fibonacci Numbers* **6**:537-44. Ed. G. E. Bergum et al. Dordrecht: Kluwer, 1996.

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

❖❖❖