LINEAR RECURSIVE SEQUENCES AND POWERS OF MATRICES

Zhi-Hong Sun

Department of Mathematics, Huaiyin Teachers College, Huaiyin, Jiangsu 223001, P.R. China
E-mail: hyzhsun@public.hy.js.cn

(*Submitted July 1999-Final Revision November 1999*)

1. INTRODUCTION

In this paper we study the properties of linear recursive sequences and give some applications to matrices.

For $a_1, a_2 \in \mathbb{Z}$, the corresponding Lucas sequence $\{u_n\}$ is given by $u_0 = 0$, $u_1 = 1$, and $u_{n+1} + a_1 u_n + a_2 u_{n-1} = 0$ $(n \geq 1)$. Such series have very interesting properties and applications, and have been studied in great detail by Lucas and later writers (cf. [2], [4], [6], [10]).

The general linear recursive sequences $\{u_n\}$ is defined by $u_n + a_1 u_{n-1} + \cdots + a_m u_{n-m} = 0$ $(n \geq 0)$. Since Dickson [2], many mathematicians have been devoted to the study of the theory of linear recursive sequences. More recently, linear recursive sequences in finite fields have often been considered; for references, one may consult [3], [5], [7], [8], [11], [12], [13], [16], [17], and [18].

In this paper we extend the Lucas series to general linear recursive sequences by defining $\{u_n(a_1, \ldots, a_m)\}$ as follows:

$$\begin{gathered} u_{1-m} = \cdots = u_{-1} = 0, \ u_0 = 1, \\ u_n + a_1 u_{n-1} + \cdots + a_m u_{n-m} = 0 \quad (n = 0, \pm 1, \pm 2, \ldots), \end{gathered} \tag{1.1}$$

where $m \geq 2$ and $a_m \neq 0$.

We mention that sequences like (1.1) have been studied by Somer in [12] and [13], and by Wagner in [15].

In Section 2 we obtain various expressions for $\{u_n(a_1, \ldots, a_m)\}$. For example,

$$\begin{aligned} u_n(a_1, \ldots, a_m) &= \sum_{k_1 + 2k_2 + \cdots + mk_m = n} \frac{(k_1 + \cdots + k_m)!}{k_1! \cdots k_m!} (-1)^{k_1 + \cdots + k_m} a_1^{k_1} \cdots a_m^{k_m} \\ &= \sum_{i=1}^{m} \frac{\lambda_i^{n+m-1}}{\prod_{j \neq i} (\lambda_i - \lambda_j)} \quad (n = 0, 1, 2, \ldots), \end{aligned}$$

where $\lambda_1, \ldots, \lambda_m$ are all distinct roots of the equation $x^m + a_1 x^{m-1} + \cdots + a_m = 0$.

The purpose of Section 3 is to give the formula for the powers of a square matrix and further properties of $\{u_n(a_1, \ldots, a_m)\}$. The main result is that

$$A^n = \sum_{r=0}^{m-1} \left(\sum_{s=r}^{m-1} a_{s-r} u_{n-s} \right) A^r, \tag{1.2}$$

where $u_n = u_n(a_1, \ldots, a_m)$ $(n = 0, \pm 1, \pm 2, \ldots)$ and A is an $m \times m$ matrix with the characteristic polynomial $a_0 x^m + a_1 x^{m-1} + \cdots + a_m$ $(a_0 = 1)$.

Formula (1.2) is a generalization of the Hamilton-Cayley theorem, and it provides a simple method of calculating the powers of a square matrix.

Let $\lambda_1, \ldots, \lambda_m$ be the roots of the equation $x^m + a_1 x^{m-1} + \cdots + a_m = 0$, $u_n = u_n(a_1, \ldots, a_m)$, and $s_n = \lambda_1^n + \cdots + \lambda_m^n$ $(n = 1, 2, 3, \ldots)$. In Sections 2 and 3 we also show that

$$\sum_{k=1}^{n} s_k u_{n-k} = n u_n \quad \text{and} \quad s_n = -\sum_{k=1}^{m} k a_k u_{n-k}. \tag{1.3}$$

We establish the following identity in Section 4:

$$u_{kn+l} = \sum_{k_0+k_1+\cdots+k_{m-1}=k} \frac{k!}{k_0!k_1!\cdots k_{m-1}!} \prod_{r=0}^{m-1} \left(\sum_{s=r}^{m-1} a_{s-r} u_{n-s} \right)^{k_r} u_{\substack{m-1 \\ \sum_{r=0} rk_r+l}}, \tag{1.4}$$

where $u_r = u_r(a_1, \ldots, a_m)$ and $a_0 = 1$.

For later convenience, we use the following notations throughout this paper: $\mathbb{Z}$ denotes the set of integers; $\mathbb{Z}^+$ denotes the set of positive integers; $|A|$ denotes the determinant of A; and $\{u_n(a_1, \ldots, a_m)\}$ denotes the sequence defined by (1.1).

2. EXPRESSIONS FOR $\{u_n(a_1, \ldots, a_m)\}$

In this section we establish some formulas for $\{u_n(a_1, \ldots, a_m)\}$.

Lemma 2.1: Let $a_1, \ldots, a_m$ be complex numbers with $a_m \neq 0$. For any $n \in \mathbb{Z}$, we have

$$u_n(a_1, \ldots, a_m) = -\frac{1}{a_m} u_{-n-m}\left(\frac{a_{m-1}}{a_m}, \ldots, \frac{a_1}{a_m}, \frac{1}{a_m} \right).$$

Proof: Let

$$v_n = u_n\left(\frac{a_{m-1}}{a_m}, \ldots, \frac{a_1}{a_m}, \frac{1}{a_m} \right) \quad \text{and} \quad u_n = -\frac{1}{a_m} v_{-n-m}.$$

Since $v_{1-m} = \cdots = v_{-1} = 0$, $v_{-m} = -a_m v_0 = -a_m$, we see that $u_{1-m} = \cdots = u_{-1} = 0$, $u_0 = 1$. Also,

$$\begin{aligned} &u_n + a_1 u_{n-1} + \cdots + a_m u_{n-m} \\ &= -\left(\frac{1}{a_m} v_{-n-m} + \frac{a_1}{a_m} v_{-n-m+1} + \cdots + \frac{a_{m-1}}{a_m} v_{-n-1} + v_{-n} \right) \\ &= 0 \quad (n = 0, \pm 1, \pm 2, \ldots). \end{aligned}$$

Thus, $u_n = u_n(a_1, \ldots, a_m)$ for any $n \in \mathbb{Z}$.

Theorem 2.1: Let $a_1, \ldots, a_m$ be complex numbers with $a_m \neq 0$. Then the generating functions of $\{u_n(a_1, \ldots, a_m)\}$ and $\{u_{-n}(a_1, \ldots, a_m)\}$ are given by

$$\sum_{n=0}^{\infty} u_n(a_1, \ldots, a_m) x^n = \frac{1}{1 + a_1 x + \cdots + a_m x^m}$$

and

$$\sum_{n=0}^{\infty} u_{-n}(a_1, \ldots, a_m) x^n = 1 - \frac{x^m}{x^m + a_1 x^{m-1} + \cdots + a_m}.$$

Proof: Let $u_n = u_n(a_1, \ldots, a_m)$, $a_0 = 1$, and $a_k = 0$ for $k > m$. Then

$$\left(\sum_{n=0}^{\infty} u_n x^n \right)\left(\sum_{k=0}^{m} a_k x^k \right) = \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} a_k u_{n-k} \right) x^n.$$

Observe that $a_{m+1} = \cdots = a_n = 0$ for $n > m$ and that $u_{n-m} = \cdots = u_{-1} = 0$ for $n \in \{1, 2, \ldots, m-1\}$. So we have

$$\sum_{k=0}^{n} a_k u_{n-k} = \sum_{k=0}^{m} a_k u_{n-k} = 0 \quad \text{for } n = 1, 2, 3, \ldots,$$

and therefore,

$$\left(\sum_{n=0}^{\infty} u_n x^n\right)\left(\sum_{k=0}^{m} a_k x^k\right) = a_0 u_0 = 1.$$

It then follows that

$$\sum_{n=0}^{\infty} u_n x^n = \frac{1}{1 + a_1 x + \cdots + a_m x^m}.$$

From the above and Lemma 2.1, we see that

$$\begin{aligned}
\sum_{n=1}^{\infty} u_{-n} x^n &= -\frac{1}{a_m} \sum_{n=m}^{\infty} u_{n-m}\left(\frac{a_{m-1}}{a_m}, \ldots, \frac{a_1}{a_m}, \frac{1}{a_m}\right) x^n \\
&= -\frac{1}{a_m} x^m \sum_{k=0}^{\infty} u_k \left(\frac{a_{m-1}}{a_m}, \ldots, \frac{a_1}{a_m}, \frac{1}{a_m}\right) x^k \\
&= -\frac{x^m}{a_m} \cdot \frac{1}{1 + \frac{a_{m-1}}{a_m} x + \cdots + \frac{1}{a_m} x^m} \\
&= -\frac{x^m}{x^m + a_1 x^{m-1} + \cdots + a_m}.
\end{aligned}$$

This completes the proof.

Corollary 2.1: Let $a_0 = b_0 = 1$ and $(\sum_{n=0}^{\infty} a_n x^n)(\sum_{n=0}^{\infty} b_n x^n) = 1$. For $m = 1, 2, 3, \ldots$, we have $b_m = u_m(a_1, \ldots, a_m)$.

Proof: Since the coefficient of x^m in $(1 + a_1 x + \cdots + a_m x^m + \cdots)^{-1}$ is the same as the coefficient of x^m in $(1 + a_1 x + \cdots + a_m x^m)^{-1}$, by using Theorem 2.1 we get $b_m = u_m(a_1, \ldots, a_m)$. This completes the proof.

We remark that Corollary 2.1 gives a simple method of calculating $\{b_n\}$.

Theorem 2.2: Let $a_1, \ldots, a_m$ be complex numbers with $a_m \neq 0$ and

$$x^m + a_1 x^{m-1} + \cdots + a_{m-1} x + a_m = \prod_{i=1}^{m} (x - \lambda_i).$$

(a) For $n = 0, 1, 2, \ldots$, we have

$$\begin{aligned}
u_n(a_1, \ldots, a_m) &= \sum_{k_1 + k_2 + \cdots + k_m = n} \lambda_1^{k_1} \lambda_2^{k_2} \cdots \lambda_m^{k_m} \\
&= \sum_{k_1 + 2k_2 + \cdots + mk_m = n} \frac{(k_1 + \cdots + k_m)!}{k_1! \cdots k_m!} (-1)^{k_1 + \cdots + k_m} a_1^{k_1} \cdots a_m^{k_m}.
\end{aligned}$$

(b) For $n=m, m+1, m+2, \ldots$, we have

$$u_{-n}(a_1,\ldots,a_m) = -\frac{1}{a_m}\sum_{k_1+\cdots+k_m=n-m}\frac{1}{\lambda_1^{k_1}\cdots\lambda_m^{k_m}}$$
$$= \sum_{k_1+2k_2+\cdots+mk_m=n-m}\frac{(k_1+\cdots+k_m)!}{k_1!\cdots k_m!}\left(-\frac{1}{a_m}\right)^{k_1+\cdots+k_m+1} a_1^{k_{m-1}}\cdots a_{m-1}^{k_1}.$$

Proof: Since $1+a_1x+\cdots+a_mx^m=(1-\lambda_1x)\cdots(1-\lambda_mx)$, by Theorem 2.1, we have

$$\sum_{n=0}^{\infty}u_n(a_1,\ldots,a_m)x^n = \prod_{i=1}^{m}\frac{1}{1-\lambda_ix} = \prod_{i=1}^{m}\left(\sum_{k=0}^{\infty}\lambda_i^kx^k\right)$$
$$= \sum_{n=0}^{\infty}\left(\sum_{k_1+\cdots+k_m=n}\lambda_1^{k_1}\cdots\lambda_m^{k_m}\right)x^n.$$

This implies

$$u_n(a_1,\ldots,a_m) = \sum_{k_1+k_2+\cdots+k_m=n}\lambda_1^{k_1}\lambda_2^{k_2}\cdots\lambda_m^{k_m}.$$

From Theorem 2.1 and the multinomial theorem, we see that

$$\sum_{n=0}^{\infty}u_n(a_1,\ldots,a_m)x^n = \frac{1}{1+a_1x+\cdots+a_mx^m} = \sum_{r=0}^{\infty}(-1)^r(a_1x+\cdots+a_mx^m)^r$$
$$= \sum_{r=0}^{\infty}(-1)^r\sum_{n=0}^{\infty}\left(\sum_{\substack{k_1+2k_2+\cdots+mk_m=n\\ k_1+\cdots+k_m=r}}\frac{r!}{k_1!\cdots k_m!}a_1^{k_1}\cdots a_m^{k_m}\right)x^n$$
$$= \sum_{n=0}^{\infty}\left(\sum_{k_1+2k_2+\cdots+mk_m=n}\frac{(k_1+\cdots+k_m)!}{k_1!\cdots k_m!}(-1)^{k_1+\cdots+k_m}a_1^{k_1}\cdots a_m^{k_m}\right)x^n.$$

Thus,

$$u_n(a_1,\ldots,a_m) = \sum_{k_1+2k_2+\cdots+mk_m=n}\frac{(k_1+\cdots+k_m)!}{k_1!\cdots k_m!}(-1)^{k_1+\cdots+k_m}a_1^{k_1}\cdots a_m^{k_m}.$$

This proves part (a).

Now consider part (b). It follows from Theorem 2.1 that

$$\sum_{n=m}^{\infty}u_{-n}(a_1,\ldots,a_m)x^n = -x^m\frac{1}{(x-\lambda_1)}\cdots\frac{1}{(x-\lambda_m)}$$
$$= \frac{(-1)^{m-1}x^m}{\lambda_1\cdots\lambda_m}\cdot\frac{1}{\left(1-\frac{x}{\lambda_1}\right)}\cdots\frac{1}{\left(1-\frac{x}{\lambda_m}\right)} = -\frac{x^m}{a_m}\prod_{i=1}^{m}\left(\sum_{k=0}^{\infty}\left(\frac{x}{\lambda_i}\right)^k\right)$$
$$= -\frac{1}{a_m}\sum_{n=m}^{\infty}\left(\sum_{k_1+\cdots+k_m=n-m}\left(\frac{1}{\lambda_1}\right)^{k_1}\cdots\left(\frac{1}{\lambda_m}\right)^{k_m}\right)x^n.$$

Therefore, we have

$$u_{-n}(a_1, \dots, a_m) = -\frac{1}{a_m} \sum_{k_1+\cdots+k_m=n-m} \frac{1}{\lambda_1^{k_1}\cdots\lambda_m^{k_m}} \quad \text{for } n \ge m.$$

By Lemma 2.1 and part (a),

$$\begin{aligned} u_{-n}(a_1, \dots, a_m) &= -\frac{1}{a_m} u_{n-m}\left(\frac{a_{m-1}}{a_m}, \dots, \frac{a_1}{a_m}, \frac{1}{a_m}\right) \\ &= -\frac{1}{a_m} \sum_{k_1+2k_2+\cdots+mk_m=n-m} \frac{(k_1+\cdots+k_m)!}{k_1!\cdots k_m!}(-1)^{k_1+\cdots+k_m}\left(\frac{a_{m-1}}{a_m}\right)^{k_1}\cdots\left(\frac{1}{a_m}\right)^{k_m}. \end{aligned}$$

Hence, the proof is complete.

Remark 2.1: Let $x^m + a_1x^{m-1} + \cdots + a_m = (x-\lambda_1)\cdots(x-\lambda_m)$. If $\{u_n(a_1, \dots, a_m)\}$ is given by its generating function, by Theorem 2.2(a) we have

$$u_n(a_1, \dots, a_m) = \sum_{k_1+k_2+\cdots+k_m=n} \lambda_1^{k_1}\lambda_2^{k_2}\cdots\lambda_m^{k_m} \quad (n \ge 0), \tag{2.1}$$

as was found by Wagner [15].

Suppose $a_0 = 1$ and $a_k = 0$ for $k \notin \{0, 1, \dots, m\}$. Using Theorem 2.1 and Cramer's rule, one can prove the following facts:

(a) For $n = 1, 2, 3, \dots,$ we have

$$u_n(a_1, \dots, a_m) = (-1)^n \begin{vmatrix} a_1 & a_2 & \cdots & a_n \\ a_0 & a_1 & \cdots & a_{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ a_{2-n} & a_{3-n} & \cdots & a_1 \end{vmatrix}. \tag{2.2}$$

(b) For $n = m+1, m+2, \dots,$ we have

$$u_{-n}(a_1, \dots, a_m) = \left(-\frac{1}{a_m}\right)^{n-m+1} \begin{vmatrix} a_{m-1} & a_{m-2} & \cdots & a_{2m-n} \\ a_m & a_{m-1} & \cdots & a_{2m-n+1} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n-2} & a_{n-3} & \cdots & a_{m-1} \end{vmatrix}. \tag{2.3}$$

Here, (a) is well known (see [9]) when $\{u_n(a_1, \dots, a_m)\}$ is given by its generating function.

Theorem 2.3: Let $a_1, \dots, a_m$ be complex numbers with $a_m \ne 0$, and $\lambda_1, \lambda_2, \dots, \lambda_m$ be the distinct roots of the equation $x^m + a_1x^{m-1} + \cdots + a_m = 0$. For any integer n, we have

$$u_n(a_1, \dots, a_m) = \sum_{i=1}^{m} \frac{\lambda_i^{n+m-1}}{\prod_{\substack{j=1 \\ j\ne i}}^{m}(\lambda_i - \lambda_j)}.$$

Proof: Consider the following system of m linear equations in m unknowns $x_1, x_2, \dots, x_m$:

$$\begin{aligned} &x_1 + x_2 + \cdots + x_m = 0 \\ &\lambda_1x_1 + \lambda_2x_2 + \cdots + \lambda_mx_m = 0 \\ &\cdots \\ &\lambda_1^{m-2}x_1 + \lambda_2^{m-2}x_2 + \cdots + \lambda_m^{m-2}x_m = 0 \\ &\lambda_1^{m-1}x_1 + \lambda_2^{m-1}x_2 + \cdots + \lambda_m^{m-1}x_m = 1. \end{aligned} \tag{2.4}$$

Since (2.4) is equivalent to

$$\begin{pmatrix} 1 & 1 & \cdots & 1 \\ \lambda_1 & \lambda_2 & \cdots & \lambda_m \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_1^{m-2} & \lambda_2^{m-2} & \cdots & \lambda_m^{m-2} \\ \lambda_1^{m-1} & \lambda_2^{m-1} & \cdots & \lambda_m^{m-1} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_{m-1} \\ x_m \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix},$$

by the solution of Vandermonde's determinants and Cramer's rule, we obtain

$$x_i = \frac{1}{\prod\limits_{r>s}(\lambda_r - \lambda_s)} \begin{vmatrix} 1 & \cdots & 1 & 0 & 1 & \cdots & 1 \\ \lambda_1 & \cdots & \lambda_{i-1} & 0 & \lambda_{i+1} & \cdots & \lambda_m \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \lambda_1^{m-1} & \cdots & \lambda_{i-1}^{m-1} & 1 & \lambda_{i+1}^{m-1} & \cdots & \lambda_m^{m-1} \end{vmatrix}$$

$$= \frac{(-1)^{m+i}}{\prod\limits_{r>s}(\lambda_r - \lambda_s)} \begin{vmatrix} 1 & \cdots & 1 & 1 & \cdots & 1 \\ \lambda_1 & \cdots & \lambda_{i-1} & \lambda_{i+1} & \cdots & \lambda_m \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \lambda_1^{m-2} & \cdots & \lambda_{i-1}^{m-2} & \lambda_{i+1}^{m-2} & \cdots & \lambda_m^{m-2} \end{vmatrix}$$

$$= \frac{(-1)^{m+i}}{\prod\limits_{r>s}(\lambda_r - \lambda_s)} \prod_{\substack{r>s \\ r,\, s\neq i}}(\lambda_r - \lambda_s) = \frac{1}{\prod\limits_{j\neq i}(\lambda_i - \lambda_j)} \quad (i = 1, 2, \ldots, m).$$

For $n \in \mathbb{Z}$, set

$$u_n = \sum_{i=1}^{m} \frac{\lambda_i^{n+m-1}}{\prod\limits_{j\neq i}(\lambda_i - \lambda_j)}.$$

From the above, we see that $u_{1-m} = \cdots = u_{-1} = 0,\ u_0 = 1$. Also,

$$u_n + a_1 u_{n-1} + \cdots + a_m u_{n-m} = \sum_{i=1}^{m} \frac{\lambda_i^{n-1}}{\prod\limits_{j\neq i}(\lambda_i - \lambda_j)} (\lambda_i^m + a_1 \lambda_i^{m-1} + \cdots + a_m)$$

$$= 0 \quad (n = 0, \pm 1, \pm 2, \ldots).$$

Thus, $u_n = u_n(a_1, \ldots, a_m)$ for $n = 0, \pm 1, \pm 2, \ldots$. This completes the proof.

For example, let $\{S(n, m)\}$ be the Stirling numbers of the second kind given by

$$x^n = \sum_{m=0}^{n} S(n, m) x(x-1)\cdots(x-m+1).$$

It is well known (see [1]) that

$$S(n, m) = \frac{1}{m!} \sum_{i=0}^{m} \binom{m}{i} (-1)^{m-i} i^n = \sum_{i=1}^{m} \frac{i^{n-1}}{\prod\limits_{\substack{j=1 \\ j\neq i}}^{m} (i - j)} \quad \text{for } n \geq m \geq 1.$$

Thus, for $n \geq m \geq 1$, $S(n, m) = u_{n-m}(a_1, \ldots, a_m)$, where $a_1, \ldots, a_m$ are determined by $(x-1)(x-2)\cdots(x-m) = x^m + a_1 x^{m-1} + \cdots a_m$. From this, we may extend the Stirling numbers of the second kind by defining $S(n, m) = u_{n-m}(a_1, \ldots, a_m)$ for any $n \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$.

Remark 2.2: Suppose that the equation $x^m + a_1x^{m-1} + \cdots + a_m = 0$ has distinct nonzero roots λ_1, ..., λ_m, and that $\{U_n\}$ satisfies the recurrence relation $U_n + a_1U_{n-1} + \cdots + a_mU_{n-m} = 0$ $(n \geq m)$. It is well known (see [1]) that there are m constants $c_1, \ldots, c_m$ such that $U_n = c_1\lambda_1^n + c_2\lambda_2^n + \cdots + c_m\lambda_m^n$ for every $n = 0, 1, 2, \ldots$.

If $a_m \neq 0$ and $x^m + a_1x^{m-1} + \cdots + a_m = (x-\lambda_1)^{n_1} \cdots (x-\lambda_r)^{n_r}$, where $\lambda_1, \ldots, \lambda_r$ are all distinct, then using Theorem 2.1 we can prove that

$$u_n(a_1, \ldots, a_m) = \frac{1}{a_m}\sum_{i=1}^{r}\sum_{j=0}^{n_i-1}\binom{n_i - j - 1 + n}{n}(-1)^{n_i-j}\frac{f_i^{(j)}\left(\frac{1}{\lambda_i}\right)}{j!}\lambda_i^{n+n_i-j} \quad (n \geq 0), \tag{2.5}$$

where

$$f_i(x) = \prod_{\substack{s=1 \\ s\neq i}}^{r}\left(x - \frac{1}{\lambda_s}\right)^{-n_s} \quad \text{and} \quad f_i^{(j)}(x) = \frac{d^j f_i(x)}{dx^j}.$$

Theorem 2.4: Let $a_1, \ldots, a_m$ be complex numbers with $a_m \neq 0$, $x^m + a_1x^{m-1} + \cdots + a_m = (x-\lambda_1)\cdots(x-\lambda_m)$, $s_n = \lambda_1^n + \lambda_2^n + \cdots + \lambda_m^n$ and $u_n = u_n(a_1, \ldots, a_m)$. For $n = 1, 2, 3, \ldots$, we have

$$\sum_{k=1}^{n} s_k u_{n-k} = nu_n \quad \text{and} \quad \sum_{k=1}^{n} s_{-k}u_{k-n-m} = nu_{-n-m}.$$

Proof: Since

$$\sum_{n=0}^{\infty} u_n x^n = \frac{1}{1 + a_1x + \cdots + a_mx^m} = (1-\lambda_1x)^{-1}(1-\lambda_2x)^{-1}\cdots(1-\lambda_mx)^{-1},$$

we have

$$\log\sum_{n=0}^{\infty}u_nx^n = -\sum_{i=1}^{m}\log(1-\lambda_ix) = \sum_{i=1}^{m}\sum_{n=1}^{\infty}\frac{\lambda_i^nx^n}{n} = \sum_{n=1}^{\infty}\frac{s_nx^n}{n}.$$

By differentiating the expansion, we get

$$\frac{\sum_{n=1}^{\infty} nu_nx^{n-1}}{\sum_{n=0}^{\infty} u_nx^n} = \sum_{n=1}^{\infty} s_nx^{n-1}.$$

That is,

$$\left(\sum_{n=1}^{\infty} s_nx^n\right)\left(\sum_{n=0}^{\infty} u_nx^n\right) = \sum_{n=1}^{\infty} nu_nx^n.$$

Comparing the coefficients of x^n on both sides gives

$$\sum_{k=1}^{n} s_k u_{n-k} = nu_n.$$

To complete the proof, by the above and Lemma 2.1 one can easily derive

$$\sum_{k=1}^{n} s_{-k}u_{k-n-m} = nu_{-n-m}.$$

3. THE FORMULA FOR THE POWERS OF A SQUARE MATRIX

This section is devoted to giving a formula for the powers of a square matrix. First, we derive an explicit formula for companion matrices and then give a formula for arbitrary square matrices.

Theorem 3.1: Let $a_1, \ldots, a_m$ be complex numbers with $a_m \neq 0$, $n \in \mathbb{Z}$, and $u_n = u_n(a_1, \ldots, a_m)$. Then

$$\begin{pmatrix} 0 & & & & -a_m \\ 1 & 0 & & & -a_{m-1} \\ & 1 & \ddots & & \vdots \\ & & \ddots & 0 & -a_2 \\ & & & 1 & -a_1 \end{pmatrix}^n = \begin{pmatrix} 1 & a_1 & a_2 & \cdots & a_{m-1} \\ & 1 & a_1 & \cdots & a_{m-2} \\ & & \ddots & \ddots & \vdots \\ & & & \ddots & a_1 \\ & & & & 1 \end{pmatrix} \begin{pmatrix} u_n & u_{n+1} & \cdots & u_{n+m-1} \\ u_{n-1} & u_n & \cdots & u_{n+m-2} \\ \vdots & \vdots & \ddots & \vdots \\ u_{n-m+1} & u_{n-m+2} & \cdots & u_n \end{pmatrix}.$$

Proof: Let

$$A = \begin{pmatrix} 0 & & & & -a_m \\ 1 & 0 & & & -a_{m-1} \\ & 1 & \ddots & & \vdots \\ & & \ddots & 0 & -a_2 \\ & & & 1 & -a_1 \end{pmatrix}, \quad D = \begin{pmatrix} 1 & a_1 & a_2 & \cdots & a_{m-1} \\ & 1 & a_1 & \cdots & a_{m-2} \\ & & \ddots & \ddots & \vdots \\ & & & \ddots & a_1 \\ & & & & 1 \end{pmatrix},$$

and

$$M_n = \begin{pmatrix} u_n & u_{n+1} & \cdots & u_{n+m-1} \\ u_{n-1} & u_n & \cdots & u_{n+m-2} \\ \vdots & \vdots & \ddots & \vdots \\ u_{n-m+1} & u_{n-m+2} & \cdots & u_n \end{pmatrix}.$$

Since $u_{1-m} = \cdots = u_{-1} = 0$ and $u_0 = 1$, we see that $DM_0 = A^0$.

Clearly, $M_k A = M_{k+1}$ for any $k \in \mathbb{Z}$. Therefore, for $n = 1, 2, 3, \ldots$, we have

$$M_n = M_{n-1}A = M_{n-2}A^2 = \cdots = M_0 A^n$$

and

$$M_{-n} = M_{-n+1}A^{-1} = M_{-n+2}A^{-2} = \cdots = M_0 A^{-n}.$$

From this, it follows that

$$DM_n = DM_0 A^n = A^n \quad \text{and} \quad DM_{-n} = DM_0 A^{-n} = A^{-n},$$

which proves the theorem.

Remark 3.1: Let $\{u_n(a_1, \ldots, a_m)\}$ be given by its generating function. For $n \geq 0$, the result of Theorem 3.1 is known (see [9]).

Corollary 3.1: Let $a_1, \ldots, a_m$ be complex numbers with $a_m \neq 0$, $n \in \mathbb{Z}$, and $u_n = u_n(a_1, \ldots, a_m)$. Then

$$\begin{vmatrix} u_n & u_{n+1} & \cdots & u_{n+m-1} \\ u_{n-1} & u_n & \cdots & u_{n+m-2} \\ \vdots & \vdots & \ddots & \vdots \\ u_{n-m+1} & u_{n-m+2} & \cdots & u_n \end{vmatrix} = (-1)^{mn} a_m^n.$$

Proof: Let A, D, and M_n be the matrices as in the proof of Theorem 3.1. It is clear that $|A| = (-1)^m a_m$ and $|D| = 1$. Thus, taking the determinant of both sides of the identity $A^n = DM_n$ gives the result.

Clearly, Corollary 3.1 is a vast generalization of the known fact that $F_n^2 - F_{n-1}F_{n+1} = (-1)^{n-1}$, where $\{F_n\}$ is the Fibonacci sequence.

Corollary 3.2: Let $a_1, \ldots, a_m$ be complex numbers with $a_m \neq 0$, $x^m + a_1 x^{m-1} + \cdots + a_m = (x-\lambda_1)\cdots(x-\lambda_m)$, $n \in \mathbb{Z}$, $u_n = u_n(a_1, \ldots, a_m)$, and $s_n = \lambda_1^n + \lambda_2^n + \cdots + \lambda_m^n$. Then

$$s_n = -\sum_{k=1}^{m} k a_k u_{n-k}.$$

Proof: Suppose that A is the companion matrix in Theorem 3.1. Then $x^m + a_1 x^{m-1} + \cdots + a_m$ is the characteristic polynomial of A and hence $\lambda_1, \ldots, \lambda_m$ are the eigenvalues of A. From matrix theory, we know that the eigenvalues of A^n are $\lambda_1^n, \lambda_2^n, \ldots, \lambda_m^n$. Denote the trace of the matrix C by tr(C). Then, by the above and Theorem 3.1,

$$\begin{aligned} s_n &= \lambda_1^n + \lambda_2^n + \cdots + \lambda_m^n = \operatorname{tr}(A^n) = \operatorname{tr}(DM_n) \\ &= \sum_{i=1}^{m}\left(\sum_{k=0}^{m-i} a_k u_{n-k}\right) = \sum_{k=0}^{m-1}(m-k)a_k u_{n-k} \\ &= -m a_m u_{n-m} - \sum_{k=0}^{m-1} k a_k u_{n-k} = -\sum_{k=1}^{m} k a_k u_{n-k}. \end{aligned}$$

This proves the corollary.

Theorem 3.2: Let A be an $m \times m$ matrix with the characteristic polynomial $\chi_A(x) = a_0 x^m + a_1 x^{m-1} + \cdots + a_m$, $a_m \neq 0$, $n \in \mathbb{Z}$, and $u_n = u_n(a_1, \ldots, a_m)$. Then

$$A^n = \sum_{r=0}^{m-1}\left(\sum_{s=r}^{m-1} a_{s-r} u_{n-s}\right) A^r.$$

Proof: For $n \in \mathbb{Z}$ and arbitrary numbers $v_0, \ldots, v_{m-1}$, set

$$v_n^* = \sum_{s=0}^{m-1}\left(\sum_{r=0}^{s} a_{s-r} v_r\right) u_{n-s}.$$

Then

$$\sum_{k=0}^{m} a_k v_{n-k}^* = \sum_{s=0}^{m-1}\left(\sum_{r=0}^{s} a_{s-r} v_r\right) \sum_{k=0}^{m} a_k u_{n-s-k} = 0 \quad (n = 0, \pm 1, \pm 2, \ldots). \tag{3.1}$$

Since $a_0 = 1$ and $u_{-1} = \cdots = u_{1-m} = 0$, we see that

$$\begin{aligned} v_n^* &= \sum_{s=0}^{n}\left(\sum_{r=0}^{s} a_{s-r} v_r\right) u_{n-s} = \sum_{r=0}^{n}\left(\sum_{s=r}^{n} a_{s-r} u_{n-s}\right) v_r = v_n + \sum_{r=0}^{n-1}\left(\sum_{s=r}^{n} a_{s-r} u_{n-s}\right) v_r \\ &= v_n + \sum_{r=0}^{n-1}\left(\sum_{s=r}^{m+r} a_{s-r} u_{n-s}\right) v_r = v_n \quad (n = 0, 1, \ldots, m-1). \end{aligned} \tag{3.2}$$

Hence, $\{v_n^*\}$ is uniquely determined by (3.1) and (3.2).

From the Hamilton-Cayley theorem, we know that $A^m + a_1 A^{m-1} + \cdots + a_m I = O$, where I is the $m \times m$ unit matrix and O is the $m \times m$ zero matrix. So, for $n \in \mathbb{Z}$, $A^n + a_1 A^{n-1} + \cdots + a_m A^{n-m} = O$. If we set $A^n = (a_{ij}^{(n)})_{m \times m}$, then

$$a_{ij}^{(n)} + a_1 a_{ij}^{(n-1)} + \cdots + a_m a_{ij}^{(n-m)} = 0 \quad (n = 0, \pm 1, \pm 2, \ldots).$$

Applying the above result, we get

$$a_{ij}^{(n)} = \sum_{s=0}^{m-1}\left(\sum_{r=0}^{s} a_{s-r} a_{ij}^{(r)}\right) u_{n-s} = \sum_{r=0}^{m-1}\left(\sum_{s=r}^{m-1} a_{s-r} u_{n-s}\right) a_{ij}^{(r)} \quad (i, j = 1, 2, \ldots, m).$$

Hence,

$$A^n = \sum_{r=0}^{m-1}\left(\sum_{s=r}^{m-1} a_{s-r} u_{n-s}\right) A^r.$$

The proof is now complete.

Since $u_{1-m} = \cdots = u_{-1} = 0$ and $u_0 = 1$, we see that $a_0 u_{m-r} + \cdots + a_{m-1-r} u_1 = -a_{m-r}$ if $0 \le r \le m-1$. Thus, the Hamilton-Cayley theorem is a special result of Theorem 3.2 in the case $n = m$.

We remark that the result of Theorem 3.2 provides a very simple method of calculating the powers of a square matrix.

Corollary 3.3: Let p be an odd prime, $a, b, c, d \in \mathbb{Z}$, $p \nmid ad - bc$, $\Delta = (a-d)^2 + 4bc$. Then

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{p - (\frac{\Delta}{p})} \equiv \begin{cases} I & (\bmod p) \quad \text{if } (\frac{\Delta}{p}) = 1, \\ \frac{a+d}{2} I & (\bmod p) \quad \text{if } (\frac{\Delta}{p}) = 0, \\ (ad - bc) I & (\bmod p) \quad \text{if } (\frac{\Delta}{p}) = -1,. \end{cases}$$

where I is the 2×2 identity matrix and $(\frac{\cdot}{p})$ denotes the Legendre symbol.

Proof: Let $u_{-1} = 0$, $u_0 = 1$, and $u_{n+1} = (a+d)u_n - (ad-bc)u_{n-1}$ $(n = 0, 1, 2, \ldots)$. Then $u_n = u_n(-a-d, ad-bc)$. Since the characteristic polynomial of $(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix})$ is $x^2 - (a+d)x + ad - bc$, using Theorem 3.2 we see that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^n = u_{n-1}\begin{pmatrix} a & b \\ c & d \end{pmatrix} + (u_n - (a+d)u_{n-1})\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} u_n - du_{n-1} & bu_{n-1} \\ cu_{n-1} & u_n - au_{n-1} \end{pmatrix}. \tag{3.3}$$

Clearly, $\Delta = (a+d)^2 - 4(ad - bc)$. Thus, by [10, pp. 46-47],

$$u_{p-1-(\frac{\Delta}{p})} \equiv 0 \ (\bmod p), \quad u_{p-1} \equiv \left(\frac{\Delta}{p}\right) (\bmod p).$$

Putting the above together yields

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{p-(\frac{\Delta}{p})} \equiv u_{p-(\frac{\Delta}{p})} I \ (\bmod p).$$

If $(\frac{\Delta}{p}) = 1$ then $u_{p-(\frac{\Delta}{p})} = u_{p-1} \equiv (\frac{\Delta}{p}) = 1$ (mod p). If $(\frac{\Delta}{p}) = -1$, then $u_{p-1} \equiv -1$ (mod p) and $u_p \equiv 0$ (mod p). Thus, $u_{p-(\frac{\Delta}{p})} = u_{p+1} = (a+d)u_p - (ad-bc)u_{p-1} \equiv ad - bc$ (mod p).

If $\left(\frac{\Delta}{p}\right)=0$, then $p\mid\Delta$. Using Fermat's little theorem, we see that

$$u_{p-(\frac{\Delta}{p})}=u_p=\frac{1}{\sqrt{\Delta}}\left\{\left(\frac{a+d+\sqrt{\Delta}}{2}\right)^{p+1}-\left(\frac{a+d-\sqrt{\Delta}}{2}\right)^{p+1}\right\}$$

$$=\frac{2}{2^{p+1}}\sum_{2\nmid k}\binom{p+1}{k}(a+d)^{p+1-k}(\sqrt{\Delta})^{k-1}$$

$$\equiv\frac{2}{2^{p+1}}(p+1)(a+d)^p\equiv\frac{a+d}{2}\pmod{p}.$$

Combining the above produces the desired result.

4. AN IDENTITY FOR $\{u_n(a_1,\ldots,a_m)\}$

Using Theorems 3.1 and 3.2, one can prove the following identity.

Theorem 4.1: Let $a_1,\ldots,a_m$ be complex numbers with $a_m\neq 0$, $a_0=1$, and $u_n=u_n(a_1,\ldots,a_m)$. Then, for $n,l\in\mathbb{Z}$ and $k\in\mathbb{Z}^+$, we have

$$u_{kn+l}=\sum_{k_0+k_1+\cdots+k_{m-1}=k}\frac{k!}{k_0!k_1!\cdots k_{m-1}!}\prod_{r=0}^{m-1}\left(\sum_{s=r}^{m-1}a_{s-r}u_{n-s}\right)^{k_r}u_{\sum_{r=0}^{m-1}rk_r+l}.$$

Proof: Let A, D, and M_n denote the matrices as in the proof of Theorem 3.1. It is clear that the characteristic polynomial of A is $x^m+a_1x^{m-1}+\cdots+a_m$. So, by Theorem 3.2,

$$A^n=\sum_{r=0}^{m-1}\left(\sum_{s=r}^{m-1}a_{s-r}u_{n-s}\right)A^r.$$

From this and the multinomial theorem for square matrices, it follows that

$$A^{kn+l}=\left(\sum_{r=0}^{m-1}\left(\sum_{s=r}^{m-1}a_{s-r}u_{n-s}\right)A^r\right)^k A^l$$

$$=\sum_{k_0+k_1+\cdots+k_{m-1}=k}\frac{k!}{k_0!k_1!\cdots k_{m-1}!}\prod_{r=0}^{m-1}\left(\sum_{s=r}^{m-1}a_{s-r}u_{n-s}\right)^{k_r}A^{\sum_{r=0}^{m-1}rk_r+l}.$$

Multiplying both sides on the left by D^{-1} and then applying Theorem 3.1, we see that

$$M_{kn+l}=\sum_{k_0+k_1+\cdots+k_{m-1}=k}\frac{k!}{k_0!k_1!\cdots k_{m-1}!}\prod_{r=0}^{m-1}\left(\sum_{s=r}^{m-1}a_{s-r}u_{n-s}\right)^{k_r}M_{\sum_{r=0}^{m-1}rk_r+l}.$$

Now, comparing the elements in row 1 and column 1 of the matrices on both sides yields the result.

Corollary 4.1: Let a_1 and a_2 be complex numbers with $a_2\neq 0$. If $\{U_r\}$ is the Lucas sequence given by $U_0=0$, $U_1=1$, and $U_r+a_1U_{r-1}+a_2U_{r-2}=0$ $(r=0,\pm1,\pm2,\ldots)$, then

$$U_{kn+l}=\sum_{i=0}^{k}\binom{k}{i}(-a_2U_{n-1})^{k-i}U_n^iU_{l+i},\tag{4.1}$$

where $n,l\in\mathbb{Z}$ and $k\in\mathbb{Z}^+$.

Proof: Note that $U_r = u_{r-1}(a_1, a_2)$. By taking $m = 2$ in Theorem 4.1 and then replacing l by $l-1$, we obtain the result.

Remark 4.1: When $n, l \geq 0$ and $a_1 = a_2 = -1$, the result of Corollary 4.1 was established by my brother Zhi-Wei Sun [14]. (In the case $l = 0$, the result is due to Siebeck [2, p. 394].) Here I give the following general identity,

$$U_s^k U'_{kn+l} = \sum_{i=0}^{k} \binom{k}{i} U_n^i (-a_2^s U_{n-s})^{k-i} U'_{l+is}, \tag{4.2}$$

where $\{U'_r\}$ satisfies the recurrence relation $U'_r + a_1 U'_{r-1} + a_2 U'_{r-2} = 0$ $(n = 0, \pm 1, \pm 2, \ldots)$. This can be proved easily by using the relation $U'_r = U'_1 U_r - a_2 U'_0 U_{r-1}$ and the known formula

$$U_r = \frac{1}{\sqrt{a_1^2 - 4a_2}} \left\{ \left(\frac{-a_1 + \sqrt{a_1^2 - 4a_2}}{2} \right)^r - \left(\frac{-a_1 - \sqrt{a_1^2 - 4a_2}}{2} \right)^r \right\}.$$

Corollary 4.2: Let $a_1, \ldots, a_m$ be complex numbers with $a_m \neq 0$, $a_0 = 1$, and $u_n = u_n(a_1, \ldots, a_m)$. For n, $l \in \mathbb{Z}$, we have

$$u_{n+l} = \sum_{r=0}^{m-1} \left(\sum_{s=r}^{m-1} a_{s-r} u_{n-s} \right) u_{r+l}.$$

Proof: Putting $k = 1$ in Theorem 4.1 yields the result.

Corollary 4.3: Let p be a prime, $a_1, \ldots, a_m \in \mathbb{Z}$, $p \nmid a_m$, $l, n \in \mathbb{Z}$, $a_0 = 1$, and $u_n = u_n(a_1, \ldots, a_m)$. Then

$$u_{np+l} \equiv \sum_{r=0}^{m-1} \sum_{s=r}^{m-1} a_{s-r} u_{n-s} u_{rp+l} \pmod{p}.$$

Proof: If $k_0 + \cdots + k_{m-1} = p$, then

$$\frac{p!}{k_0! \cdots k_{m-1}!} \equiv \begin{cases} 1 \pmod{p} & \text{if } p = k_r, \text{ for some } r \in \{0, \ldots, m-1\}, \\ 0 \pmod{p} & \text{otherwise.} \end{cases}$$

This, together with Theorem 4.1 and Fermat's little theorem, gives

$$\begin{aligned} u_{np+l} &\equiv \sum_{r=0}^{m-1} \left(\sum_{s=r}^{m-1} a_{s-r} u_{n-s} \right)^p u_{rp+l} \\ &\equiv \sum_{r=0}^{m-1} \sum_{s=r}^{m-1} a_{s-r} u_{n-s} u_{rp+l} \pmod{p}, \end{aligned}$$

which is the result.

REFERENCES

1. R. A. Brualdi. *Introductory Combinatorics*, pp. 99-125. New York, Oxford, Amsterdam: Elsevier North-Holland, Inc., and North-Holland Publishing Company, 1977.
2. L. E. Dickson. *History of the Theory of Numbers*. Vol. I, Ch. XVII. New York: Chelsea, 1952.
3. H. T. Engstrom. "Periodicity in Sequences Defined by Linear Recurrence Relations." *Proc. Nat. Acad. Sci. U.S.A.* **16** (1930):663-65.

4. D. H. Lehmer. *Annals of Math.* **31.2** (1930):419-48.
5. R. Lidl & H. Niederreiter. *Finite Fields*, pp. 394-469. London and Amsterdam: Addison-Wesley, 1983.
6. E. Lucas. "Théorie des fonctions numériques simplement périodiques." *Amer. J. Math.* **1** (1878):184-240.
7. W. Mantel. "Residues of Recurring Series." (Dutch) *Nieuw Arch. Wisk.* **1** (1894):172-84.
8. M. d'Ocagne. "Mémoire sur les suites réecurrentes." *J. de l'Ecole Polytechnique* **64** (1894): 151-224.
9. G. Pólya & G. Szegö. *Problems and Theorems in Analysis.* Vol. II, Ch. VII, 11.1, 32. New York: Springer-Verlag, 1972.
10. P. Ribenboim. *The Book of Prime Number Records.* 2nd ed., pp. 44-50. Berlin: Springer-Verlag World Publishing Corp., 1989.
11. E. S. Selmer. *Linear Recurrence Relations over Finite Fields.* University of Bergen, 1966.
12. L. Somer. "Periodicity Properties of k^{th}-Order Linear Recurrences Whose Characteristic Polynomial Splits Completely over a Finite Field *I*." In *Finite Fields: Theory, Applications, and Algorithms*, pp. 327-339. MR95k:11018. Las Vegas, Nevada, 1993.
13. L. Somer. *Finite Fields and Applications*, pp. 333-347. MR97m:11022. Glasgow, 1995.
14. Z. W. Sun. "Reduction of Unknowns in Diophantine Representations." *Science in China* (Ser. A) **35** (1992):1-13.
15. C. G. Wagner. "Generalized Stirling and Lah Numbers." *Discrete Mathematics* **160** (1996): 199-218.
16. M. Ward. "Some Arithmetical Properties of Sequences Satisfying a Linear Recursion Relation." *Ann. of Math.* **32** (1931):734-38.
17. M. Ward. "The Arithmetical Theory of Linear Recurring Series." *Trans. Amer. Math. Soc.* **35** (1933):600-28.
18. N. Zierler. "Linear Recurring Sequences." *J. Soc. Indust. Appl. Math.* **7** (1959):31-48.

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

❖❖❖

F_{81839} Is Prime

David Broadhurst and Bouk de Water have recently proved that F_{81839} is prime.