GENERATING FUNCTIONS OF LINEAR DIVISIBILITY SEQUENCES

CLARK KIMBERLING
University of Evansville, Evansville, IN 47702

1. INTRODUCTION

A *k*th-order divisibility sequence is introduced in Hall [3] as a sequence of rational integers $u_0, u_1, u_2, \ldots, u_n, \ldots$ satisfying a linear recurrence relation

(1) $$u_{n+k} = a_1u_{n+k-1} + \cdots + a_ku_n,$$

where the a's are rational integers, and u_m divides u_n whenever m divides n, for all positive integers m and n.

Some examples follow: 0, 1, 2, 4, 8, ... is a first-order divisibility sequence, while 0, 1, 2, 3, 4, ... is a second-order divisibility sequence. Another second-order divisibility sequence is the Fibonacci sequence

$$0, 1, 1, 2, 3, 5, 8, \ldots,$$

whole recurrence relation is

$$u_{n+2} = u_{n+1} + u_n.$$

If this recurrence relation is generalized to

$$u_{n+2} = xu_{n+1} + yu_n,$$

where x and y are indeterminates, the sequence resulting from the initial terms $u_0 = 0$ and $u_1 = 1$ is the sequence of Fibonacci polynomials. Like the numerical Fibonacci sequence, these polynomials satisfy the divisibility property $u_m|u_n$ (in the ring $I[x, y]$ of polynomials in x and y with integer coefficients) whenever $m|n$. Unlike the Fibonacci numbers, however, the polynomial is irreducible (in $I[x, y]$) whenever the index m is irreducible in I. Thus, the divisibility properties of the more general sequence differ from those of the numerical sequence.

This example and others lead us to extend the coverage of the term *k*th-order divisibility sequence to include sequences for which any number of the a's in (1) and any number of the initial terms $u_0, u_1, \ldots, u_{k-1}$ are indeterminates. The resulting sequence may then be a sequence of integers, but it may, instead, be a sequence of polynomials in one or more indeterminates $x_1, \ldots, x_p$. In this case, our discussion of divisibility properties refers to arithmetic in the ring $I[x_1, \ldots, x_p]$.

When a divisibility sequence is to be discussed without reference to its recurrence order, we call it a linear divisibility sequence. Thus, a distinction is made between the sequences at hand and nonlinear divisibility sequences, such as the elliptic divisibility sequences studied by Ward [7], [8].

The only known linear divisibility sequences are resultant sequences and their divisors, as defined below. Our purpose in this paper is to discuss generating functions of such sequences. Suppose

$$X(t) = \prod_{i=1}^{p}(t - x_i) \quad \text{and} \quad Y(t) = \prod_{j=1}^{q}(t - y_j)$$

are polynomials with integer coefficients; here, any number of the roots x_i and y_j may be indeterminates. A resultant sequence $\{u_n\}$, $n = 0, 1, \ldots,$ is a sequence of the form

$$u_n = \prod_{j=1}^{q} \prod_{i=1}^{p} \frac{x_i^n - y_j^n}{x_i - y_j}. \tag{2}$$

Thus, $u_n = R_n/R_1$, where $R_n = R_n(X, Y)$ is the resultant of the polynomials

$$\prod_{i=1}^{p} (t - x_i^n) \quad \text{and} \quad \prod_{j=1}^{q} (t - y_j^n).$$

A divisor of a resultant sequence $\{u_n\}$ is a linear divisibility sequence $\{v_n\}$, $n = 0, 1, \ldots$, such that $v_n | u_n$ for $n = 1, 2, \ldots$.

Ward proved in [5] that every resultant sequence is a linear divisibility sequence, and conjectured repeatedly that every linear divisibility sequence is a divisor of a resultant sequence. No proof of this conjecture seems to be known or imminent, even in the case that all the roots are indeterminates!

Before continuing directly toward an investigation of generating functions, we pose another problem, closely related to Ward's conjecture. For (not necessarily distinct) algebraic integers ξ and ζ, let F be the smallest normal field containing both ξ and ζ. Define

$$v_n = \prod_{S} \frac{\xi^n - \zeta^n}{\xi - \zeta}, \quad n = 0, 1, \ldots, \tag{3}$$

the product being taken over all automotphisms S of F. Then the terms v_n are rational integers and the sequence $\{v_n\}$ a linear divisibility sequence. We call this the linear divisibility sequence belonging to ξ, ζ. Suppose now that $\{u_n\}$ is a numerical resultant sequence and that $\{v_n\}$ is a divisor of $\{u_n\}$. Suppose, further, that $u_n = v_n = 1$ and $\{v_n\}$ has no divisors of its own except $(0, 1, 1, \ldots)$ and $\{v_n\}$. Must $\{v_n\}$ be a linear divisibility sequence belonging to some pair of algebraic integers appearing in (2)?

2. RECIPROCAL POLYNOMIALS

Suppose $A \neq 0$. A polynomial

$$H(t) = h_0 + h_1 t + \cdots + h_{2k} t^{2k}$$

of even degree $2k$ is an A-reciprocal polynomial of the first kind if

$$h_{2k-q} = A^{k-q} h_q \quad \text{for } q = 0, 1, \ldots, k,$$

and an A-reciprocal polynomial of the second kind if

$$h_{2k-q} = -A^{k-q} h_q \quad \text{for } q = 0, 1, \ldots, k.$$

In both cases, the roots of $H(t)$ occur in pairs whose product is A; conversely, any polynomial with this property is an A-reciprocal polynomial. A discussion may be found in Burnside and Panton [2, pp. 63-64].

Suppose

$$f = f(t) = \sum_{i=0}^{2k} f_i t^i \quad \text{and} \quad g = g(t) = \sum_{j=0}^{2k} g_j t^j,$$

and write

$$[\alpha, \beta] = \begin{cases} g_\alpha f_\beta - f_\alpha g_\beta & \text{for } \max\{\alpha, \beta\} \leq 2k \\ 0 & \text{otherwise.} \end{cases}$$

Clearly $[\beta, \alpha] = -[\alpha, \beta]$.

Lemma 1a: Suppose

$$0 \le \alpha \le 2k \quad \text{and} \quad 0 \le \beta \le 2k.$$

If f and g are A-reciprocal polynomials of the first kind, then

$$[\alpha, \beta] = A^{\alpha+\beta-2k}[2k - \alpha, 2k - \beta].$$

Proof:

$$\begin{aligned}[\alpha, \beta] &= g_\alpha f_\beta - f_\alpha g_\beta \\ &= g_{k+q} f_{k+q'} - f_{k+q} g_{k+q'} \\ &= A^q g_{k-q} A^{q'} f_{k-q'} - A^q f_{k-q} A^{q'} g_{k-q'} \\ &= A^{q+q'}[k - q, k - q'] \\ &= A^{\alpha+\beta-2k}[2k - \alpha, 2k - \beta].\end{aligned}$$

Theorem 1a: Suppose

$$F(t) = f_0 + f_1 t + \cdots + f_{2k} t^{2k}$$

and

$$G(t) = g_0 + g_1 t + \cdots + g_{2k} t^{2k}$$

are polynomials of degree $2k > 0$. Let

$$H(t) = F(t)G'(t) - G(t)F'(t) = h_0 + h_1 t + \cdots + h_{4k-1} t^{4k-1}.$$

Suppose $F(t)$ and $G(t)$ are A-reciprocal polynomials of the first kind:

$$f_{k+q} = A^q f_{k-q} \quad \text{and} \quad g_{k+q} = A^q g_{k-q} \quad \text{for } q = 0, 1, \ldots, k.$$

Then $h_{2k-1} = h_{4k-1} = 0$, and $H(t)$ is an A-reciprocal polynomial of the second kind:

$$h_{2k-1+q} = -A^q h_{2k-1-q}, \quad q = 0, 1, \ldots, 2k - 1.$$

Proof:

$$\begin{aligned}H(t) &= \left(\sum_{i=0}^{2k} f_i t^i\right)\left(\sum_{i=0}^{2k-1} (i + 1) g_{i+1} t^i\right) - \left(\sum_{i=0}^{2k} g_i t^i\right)\left(\sum_{i=0}^{2k-1} (i + 1) f_{i+1} t^i\right) \\ &= \sum_{j=0}^{4k-1} t^j \sum_{i=0}^{j} (i + 1)[i + 1, j - i].\end{aligned}$$

Thus, for $q = 0, 1, \ldots, 2k - 1$, we find, after some simplification,

$$h_{2k-1-q} = \sum_{i=0}^{s} (2k - q - 2i)[2k - q - i, i].$$

where

$$s = (2k - q - 2)/2 \text{ for even } q \text{ and } (2k - q - 1)/2 \text{ for odd } q.$$

On the other hand,

$$\begin{aligned}h_{2k-1+q} &= \sum_{i=0}^{2k} (q + 2k - i)[q + 2k - i, i] \\ &= \sum_{i=q}^{2k} (q + 2k - i)[q + 2k - i, i]\end{aligned}$$

(continued)

$$= \sum_{i=0}^{2k-q}(2k - i)[2k - i, q + i]$$

$$= \sum_{i=0}^{s}(2k - q - 2i)[2k - i, q + i]$$

$$= -A^q\sum_{i=0}^{s}(2k - q - 2i)[2k - q - i, i],$$

by Lemma 1a, but this equals $-A^q h_{2k-1-q}$, as desired. In particular, for $q = 0$, we find $h_{2k-1} = -h_{2k-1}$, so that $h_{2k-1} = 0$. That $h_{4k-1} = 0$ follows directly from the definition of $H(t)$.

Lemma 1b: Suppose $0 \leq \alpha \leq 2k$ and $0 \leq \beta \leq 2k$. Suppose f and g satisfy

$$g_{k+q} = A^q f_{k-q} \quad \text{for } q = -k, \ldots, 0, \ldots, k.$$

Then

$$[\alpha, \beta] = -A^{\alpha+\beta-2k}[2k - \alpha, 2k - \beta].$$

Proof:

$$\begin{aligned}[\alpha, \beta] &= g_\alpha f_\beta - f_\alpha g_\beta \\ &= g_{k+q}f_{k+q'} - f_{k+q}g_{k+q'} \\ &= A^{q+q}(f_{k-q}g_{k-q'} - g_{k-q}f_{k-q'}) \\ &= -A^{\alpha+\beta-2k}[2k - \alpha, 2k - \beta].\end{aligned}$$

Theorem 1b: Suppose $F(t)$, $G(t)$, and $H(t)$ are as in Theorem 1a, but that for some $A \neq 0$,

$$g_{k+q} = A^q f_{k-q} \quad \text{for } q = -k, \ldots, 0, \ldots, k.$$

Then $h_{4k-1} = 0$, and $H(t)$ is an A-reciprocal polynomial of the first kind:

$$h_{2k-1+q} = A^q h_{2k-1-q} \quad \text{for } q = 0, 1, \ldots, 2k - 1.$$

Proof: The proof is so similar to that of Theorem 1a that it is omitted.

3. GENERATING FUNCTIONS

Suppose $m \geq 1$ and $x_1, \ldots, x_m, y_1, \ldots, y_m$ are (not necessarily distinct) indeterminates. Write

$$X(t) = \prod_{i=1}^{m}(t - x_i) = t^m - X_1t^{m-1} + \cdots + (-1)^m X_m,$$

$$Y(t) = \prod_{i=1}^{m}(t - y_i) = t^m - Y_1t^{m-1} + \cdots + (-1)^m Y_m,$$

$$\sigma_0 = 1,\ \sigma_1 = \sum\frac{y_i}{x_i},\ \sigma_2 = \sum\frac{y_{i_1}y_{i_2}}{x_{i_1}x_{i_2}},\ \ldots,\ \sigma_m = \frac{y_1 \ldots y_m}{x_1 \ldots x_m}.$$

Then $\displaystyle\prod_{i=1}^{m}(x_i - y_i) = X_m\left(1 - \frac{y_1}{x_1}\right)\left(1 - \frac{y_2}{x_2}\right) \cdots \left(1 - \frac{y_m}{x_m}\right)$

$$= X_m(1 - \sigma_1 + \sigma_2 - \cdots + (-1)^m\sigma_m)$$

(continued)

$$(4) \qquad = \begin{cases} X_m + X_m\sigma_2 + \cdots + X_m\sigma_{m-1} - (X_m\sigma_1 + \cdots + X_m\sigma_m), \text{ odd } m \\ X_m + X_m\sigma_2 + \cdots + X_m\sigma_m - (X_m\sigma_1 + \cdots + X_m\sigma_{m-1}), \text{ even } m. \end{cases}$$

The right side of (4) consists of 2^m terms of the form

$$\pm y_{i_1} y_{i_2} \cdots y_{i_k} x_{i_{k+1}} \cdots x_{i_m}.$$

Let P be the set of those terms having positive coefficient (i.e., an even number of y's) and N the set of those having negative coefficient. In the set $P \cup N$, define a mapping

$$\phi(y_{i_1} y_{i_2} \cdots y_{i_k} x_{i_{k+1}} \cdots x_{i_m}) = y_{i_{k+1}} \cdots y_{i_m} x_{i_1} x_{i_2} \cdots x_{i_k}.$$

If m is odd, ϕ is a one-to-one correspondence between P and N; if m is even, ϕ defines a one-to-one correspondence between P and P, and also between N and N. For each element z of $P \cup N$, we have $z\phi(z) = X_m Y_m$.

At this point, we introduce some more notation. Write

$$x = (x_1, \ldots, x_m),\ y = (y_1, \ldots, y_m),\ \mathcal{A} = (X_m\sigma_0, X_m\sigma_1, \ldots, X_m\sigma_m),$$

$$U_n(x, y) = \sum_{i=1}^{m} (x_i^n - y_i^n),\ n = 0, 1, \ldots,$$

$$(5) \qquad \mathcal{F}_n(x, y) = \frac{1}{2}[U_n(x, y) + U_n(x, -y)] = \sum_{\gamma \varepsilon P} \gamma^n,$$

$$(6) \qquad \mathcal{G}_n(x, y) = \frac{1}{2}[U_n(x, y) - U\ (x, -y)] = \sum_{\gamma \varepsilon N} \delta^n.$$

We index the γ's and δ's in any order, as

$$\gamma_1, \gamma_2, \ldots, \gamma_{2k} \quad \text{and} \quad \delta_1, \delta_2, \ldots, \delta_{2k},$$

where $2k = 2^{m-1}$.

Theorem 2: The sequence $\{u_n\}$ defined by

$$u_n = \frac{U_n}{U_1} = \sum_{i=1}^{m} \frac{x_i^n - y_i^n}{x_i - y_i},\ m \geq 1;\ n = 0, 1, \ldots,$$

is a 2^m-order linear divisibility sequence with generating function

$$(7) \qquad \frac{t}{U_1}\left[\frac{G'(t)}{G(t)} - \frac{F'(t)}{F(t)}\right] = \frac{tH(t)}{F(t)G(t)},$$

where $F(t)G(t)$ is an X_mY_m-reciprocal polynomial of the first kind, lying in $I[\mathcal{A}, t]$ with degree 2^m in t, and $H(t)$ is an X_mY_m-reciprocal polynomial of the first or second kind, depending on whether m is even or odd, lying in $I[\mathcal{A}, t]$ with degree $2^m - 2$ in t.

Proof: Equation (5) shows that the sum

$$s_n = \sum_{\gamma \varepsilon P} \gamma^n$$

is a binary symmetric function (as in Bôcher [1, p. 255]) of the pairs

$$(x_1, y_1), \ldots, (x_m, y_m),$$

namely $X_m\sigma_0$, $X_m\sigma_1$, ..., $X_m\sigma_m$. Since these (ordinary) homogeneous power sums s_n of the γ's thus lie in $I[\mathcal{A}]$, the (ordinary) elementary symmetric functions of the γ's also lie in $I[\mathcal{A}]$. The same is true for the elementary symmetric functions of the δ's. Therefore, the polynomials

$$(8) \qquad F(t) = \prod_{i=1}^{2k}(1 - \gamma_i t) \quad \text{and} \quad G(t) = \prod_{j=1}^{2k}(1 - \delta_j t)$$

lie in $I[\mathcal{A}, t]$.

Suppose m is even. Then $F(t)$ is an X_mY_m-reciprocal polynomial of the first kind, since each γ_i is accompanied in $F(t)$ by $\phi(\gamma_i) = X_mY_m\gamma_i^{-1}$. The same is true for $G(t)$. On the other hand, if m is odd, then each γ_i in $F(t)$ equals $X_mY_m\phi(\delta_j) = X_mY_m\gamma_i^{-1}$ for some δ_j in $G(t)$, and conversely for each δ_i in $G(t)$. Thus, $F(t)$ and $G(t)$ are related as in Theorem 1b. In both cases, even m and odd m, the product $F(t)G(t)$ is therefore an X_mY_m-reciprocal polynomial of the first kind.

Since $\{\mathcal{F}_n(x, y)\}$ and $\{\mathcal{G}_n(x, y)\}$ are sequences of power sums, we have

$$\sum_{n=0}^{\infty} U_n(x, y)t^n = \sum_{n=0}^{\infty}\mathcal{F}_n(x, y)t^n - \sum_{n=0}^{\infty}\mathcal{G}_n(x, y)t^n = \frac{-F'(t)}{F(t)} - \frac{-G'(t)}{G(t)},$$

and (7) follows. Theorems 1a and 1b now apply to the polynomial

$$H(t) = \frac{1}{U_1(x, y)}[F(t)G'(t) - G(t)F'(t)],$$

and the proof of Theorem 2 is finished.

In Theorem 2, the coefficients of the polynomials $H(t)$ and $F(t)G(t)$ lie in $I[\mathcal{A}]$; that is, they themselves are polynomials in the indeterminates $X_m\sigma_0$, $X_m\sigma_1$, ..., $X_m\sigma_m = Y_m$. Of special interest is the possibility that these coefficients lie, *a fortiori*, in the ring

$$I^* = I[X_1, \ldots, X_m, Y_1, \ldots, Y_m]$$

[or a suitable modification of this ring, as in Theorem 2a below; just so that the coefficients in question are polynomials in the coefficients of the underlying polynomials $X(t)$ and $Y(t)$]. If repetition of x_i's and y_i's is allowed, then all these coefficients can possibly lie in I^*. We investigate two such cases in the next section: resultant sequences and certain divisors of resultant sequences which we call Vandermonde sequences. Under the additional hypothesis $X_m = Y_m = 1$, we are able to prove another symmetric property of $H(t)$ and $F(t)G(t)$: as functions of $(X_1, \ldots, X_{m-1}, Y_1, \ldots, Y_{m-1})$, each of their coefficients remains unaltered under the substitution

$$X_i \to X_{m-i},\ Y_i \to Y_{m-i},\quad i = 1, \ldots, m - 1.$$

4. RESULTANT SEQUENCES AND VANDERMONDE SEQUENCES

Theorem 2a: Suppose $p \geq 1$, $q \geq 1$, and $p + q \geq 3$. Suppose

$$(2) \qquad u_n = \prod_{j=1}^{q}\prod_{i=1}^{p}\frac{x_i^n - y_j^n}{x_i - y_j}, \quad n = 0, 1, \ldots,$$

where

$$(9) \qquad X(t) = \prod_{i=1}^{p}(t - x_i) = t^p - X_1t^{p-1} + X_2t^{p-2} - \cdots + (-1)^pX_p,$$

$$(10) \qquad Y(t) = \prod_{j=1}^{q}(t - y_j) = t^q - Y_1t^{q-1} + Y_2t^{q-2} - \cdots + (-1)^qY_q,$$

and

$$I^* = I[X_1, \ldots, X_p, Y_1, \ldots, Y_q].$$

Then, $\{u_n\}$ is a 2^{pq}-order linear divisibility sequence with generating function

$$\frac{t}{R_1}\left[\frac{G'(t)}{G(t)} - \frac{F'(t)}{F(t)}\right] = \frac{tH(t)}{F(t)G(t)},$$

where

$$R_1 = \prod_{j=1}^{q}\prod_{i=1}^{p}(x_i - y_j)$$

is the resultant of $X(t)$ and $Y(t)$, $F(t)G(t)$ is an $X_p^qY_q^p$-reciprocal polynomial of the first kind, lying in $I^*[t]$ with degree 2^{pq} in t, and $H(t)$ is an $X_p^qY_q^p$-reciprocal polynomial of the first or second kind, depending on whether p is even or odd, lying in $I^*[t]$ with degree $2^{pq} - 2$ in t.

Proof: Put $m = pq$, $\alpha_k = x_i$ for $iq - q + 1 \leq k \leq iq$; $i = 1, \ldots, p$, and $\beta_k = y_j$ for $k = \ell q + j$; $\ell = 0, 1, \ldots, p - 1$; $j = 1, \ldots, q$. Then, Theorem 2 applies, where the pairs (x_k, y_k) of Theorem 2 are the pairs (α_k, β_k) of the present discussion. All that remains to be seen is that the coefficients of $H(t)$and $F(t)G(t)$ lie in I^* and that the dependence of $H(t)$ for first or second kind reciprocity rests on the parity of p alone.

For the latter, we refer to the proof of Theorem 2: Equation (5) shows that for even p, each γ_i occurs in $F(t)$ along with $\phi(\gamma_i) = X_p^qY_q^p\gamma_i^{-1}$. This makes $F(t)$ an $X_p^qY_q^p$-reciprocal polynomial of the first kind, and similarly for $G(t)$. For odd p, we find $F(t)$ and $G(t)$ related as in Theorem 1b, and the argument is finished as in the proof of Theorem 2.

Equation (5) also shows that the sum

$$s_n = \sum_{\gamma \in P}\gamma^n$$

is symmetric in $x_1, \ldots, x_p$ and symmetric in $y_1, \ldots, y_q$, since $\mathcal{F}_n(x, y)$, where $(x, y) = (\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_m)$, is a sum of two resultants, each symmetric in $x_1, \ldots, x_p$ and symmetric in $y_1, \ldots, y_q$. Thus, s_n is a polynomial in the elementary symmetric functions of $x_1, \ldots, x_p$ and of $y_1, \ldots, y_q$, namely, the coefficients $X_1, \ldots, X_p$ and $Y_1, \ldots, Y_q$. Each s_n therefore lies in I^*, so that the elementary symmetric functions of the γ's also lie in I^*. The same is true for the elementary symmetric functions of the δ's. Therefore, $F(t)$, $G(t)$, and $H(t)$ all lie in $I^*[t]$.

Theorem 3a: Suppose the generating function $\frac{tH(t)}{F(t)G(t)}$ in Theorem 2a is written out as

$$(11) \qquad \frac{t(h_0 + h_1t + \cdots + h_{4k-2}t^{4k-2})}{w_0 + w_1t + \cdots + w_{4k}t^{4k}},$$

where $k = 2^{pq-2}$. Then the coefficients h_i and w_i, regarded as functions of $X_0, \ldots, X_p, Y_0, \ldots, Y_q$, where $X_0 = Y_0 = 1$, satisfy

$$\begin{aligned}(12)\qquad & h_i(1, X_{p-1}, \ldots, X_1, 1, 1, Y_{q-1}, \ldots, Y_1, 1)\\ &= h_i(1, X_1, \ldots, X_{p-1}, 1, 1, Y_1, \ldots, Y_{q-1}, 1),\\ &\qquad\qquad i = 0, 1, \ldots, 4k-2,\end{aligned}$$

$$\begin{aligned}(13)\qquad & w_i(1, X_{p-1}, \ldots, X_1, 1, 1, Y_{q-1}, \ldots, Y_1, 1)\\ &= w_i(1, X_1, \ldots, X_{p-1}, 1, 1, Y_1, \ldots, Y_{q-1}, 1),\\ &\qquad\qquad i = 0, 1, \ldots, 4k.\end{aligned}$$

Proof: Write $x = (x_1, \ldots, x_p)$ and $y = (y_1, \ldots, y_p)$, and consider the effect of the operation of reciprocation,

$$x_i \to x_i^{-1},\ i = 1, 2, \ldots, p \quad\text{and}\quad y_j \to y_j^{-1},\ j = 1, 2, \ldots, q,$$

on the sequence $\{u_n(x, y)\}$ and its generating function. The series belonging to this sequence is transformed into

$$(14)\qquad X_p^q Y_q^p[0 + t' + u_2(x, y)t'^2 + u_3(x, y)t'^3 + \cdots],$$

where $t' = t/X_p^q Y_q^p$, and we may write its generating function as

$$(15)\qquad \frac{t(h_0' + h_1't + \cdots + h_{4k-2}'t^{4k-2})}{w_0' + w_1't + \cdots + w_{4k}'t^{4k}},$$

where the h_i' and w_i' are functions of $X_0, \ldots, X_p, Y_0, \ldots, Y_q$. To solve for the h_i' and w_i', note that reciprocation transforms the polynomials (9) and (10) into

$$\frac{(-1)^p}{X_p}[X_0 - X_1t + X_2t^2 - \cdots + (-1)^pX_pt^p]$$

and

$$\frac{(-1)^q}{Y_q}[Y_0 - Y_1t + Y_2t^2 - \cdots + (-1)^qY_qt^q].$$

Therefore

$$(16)\qquad h_i' = h_i\left(\frac{X_p}{X_p}, \frac{X_{p-1}}{X_p}, \ldots, \frac{X_0}{X_p}, \frac{Y_q}{Y_q}, \ldots, \frac{Y_0}{Y_q}\right),\ i = 0, 1, \ldots, 4k-2$$

and

$$(17)\qquad w_i' = w_i\left(\frac{X_p}{X_p}, \frac{X_{p-1}}{X_p}, \ldots, \frac{X_0}{X_p}, \frac{Y_q}{Y_q}, \ldots, \frac{Y_0}{Y_q}\right),\ i = 0, 1, \ldots, 4k.$$

If we replace t by $t' = t/X_p^qY_q^p$ in (11) and multiply the resulting rational function by $X_p^qY_q^p$, the series expansion is (14). Thus, (11), as modified, equals (15). Since the degrees of the denominators are equal and $w_0' = w_0 = 1$, we equate denominators and we equate numerators. This gives equal coefficients: $h_i' = h_i$ and $w_i' = w_i$. Equations (16) and (17) now complete the proof of a more general set of equations than we set out to prove. Clearly, for

$$X_p = Y_q = 1,$$

these equations reduce to (12) and (13).

Theorem 2b: For $p \geq 3$, suppose

$$u_n = \prod_{1 \leq i < j \leq p} \frac{x_i^n - x_j^n}{x_i - x_j}, \quad n = 0, 1, \ldots,$$

where

$$\prod_{i=1}^{p} (t - x_i) = t^p - X_1 t^{p-1} + X_2 t^{p-2} - \cdots + (-1)^p X_p, \tag{9}$$

and

$$I^* = I[X_1, \ldots, X_p].$$

Then $\{u_n\}$ is a $p!$-order linear divisibility sequence with generating function

$$\frac{t}{V_1}\left[\frac{G'(t)}{G(t)} - \frac{F'(t)}{F(t)}\right] = \frac{tH(t)}{F(t)G(t)},$$

where

$$V_1 = \prod_{1 \leq i < j \leq p} (x_i - x_j),$$

$F(t)G(t)$ is an X_p^{p-1}-reciprocal polynomial of the first kind, lying in $I^*[t]$ with degree $p!$ in t, and $H(t)$ is an X_p^{p-1}-reciprocal polynomial of the first kind, lying in $I^*[t]$ with degree $p! - 2$ in t.

Proof: As is well known, V_1 is the Vandermonde determinant:

$$\begin{vmatrix} 1 & 1 & \ldots & 1 \\ x_1 & x_2 & \ldots & x_p \\ x_1^2 & x_2^2 & \ldots & x_p^2 \\ \vdots & & & \vdots \\ x_1^{p-1} & x_2^{p-1} & \ldots & x_p^{p-1} \end{vmatrix} = (-1)^k \sum x_1^{i_1} x_2^{i_2} \ldots x_p^{i_p},$$

where $\{i_1, i_2, \ldots, i_p\} = \{0, 1, \ldots, p - 1\} = \mathcal{I}$ and

$$k_\sigma = \begin{cases} 0 & \text{if } \sigma \text{ is an even permutation of } \mathcal{I} \\ 1 & \text{if } \sigma \text{ is an odd permutation of } \mathcal{I}. \end{cases}$$

Half of these $p!$ summands have $k_\sigma = 0$ and the other half, $k_\sigma = 1$. If $p > 3$, then $p!/2$ is even, and each summand $z = x_1^{i_1} x_2^{i_2} \ldots x_p^{i_p}$ with $k_\sigma = 0$ is matched with a summand $X_p^{p-1} z^{-1}$, also with $k_\sigma = 0$; if z has $k_\sigma = 1$, so has $X_p^{p-1} z^{-1}$. The situation is much the same as in the proof of Theorem 2, with one essential difference. Here, the functions $X_p\sigma_0, X_p\sigma_1, \ldots, X_p\sigma_p$, where for each

i it is understood that y_i is the x_j appearing with x_i in the product

$$\prod_{i<j} (x_i - x_j),$$

are not symmetric in $x_1, \ldots, x_p$. This is a consequence of the fact that V_1 is not symmetric in $x_1, \ldots, x_p$ [unlike the discriminant V_1^2 of $X(t)$]. We may proceed by dealing directly with the symmetric *quotients*

$$u_n(x) = \frac{x_i^n - x_j^n}{x_i - x_j}$$

rather than the asymmetric products $\prod(x_i^n - x_j^n)$: put

$$\mathcal{F}_n(x) = \frac{1}{2}[u_n(x) + u_n(-x)]$$

and

$$\mathcal{G}_n(x) = \frac{1}{2}[u_n(x) - u_n(-x)].$$

The proof for $p > 3$ now follows that of Theorems 2 and 2a so closely that we omit further details.

Consider now the case $p = 3$: for z with $k_\sigma = 0$, we have $X_3^2 z^{-1}$ with $k_\sigma = 1$, and conversely. The polynomials

$$F(t) = (1 - x_1^2 x_2 t)(1 - x_1 x_3^2 t)(1 - x_2^2 x_3 t)$$

and

$$G(t) = (1 - x_1^2 x_3 t)(1 - x_1 x_2^2 t)(1 - x_2 x_3^2 t)$$

are not covered by Theorems 1a and b, since they are of odd degree. Although these theorems can easily be extended to odd-degree polynomials, we choose to defer the case $p = 3$ to the third example in Section 5, where the generating function $tH(t)/F(t)G(t)$ is fully displayed.

Theorem 3b: Suppose the generating function $tH(t)/F(t)G(t)$ in Theorem 2b is written out as

$$\frac{t(h_0 + h_1 t + \cdots + h_{k-2} t^{k-2})}{w_0 + w_1 t + \cdots + w_k t^k},$$

where $k = p!$. Then the coefficients h_i and w_i, regarded as functions of X_0, $\ldots$, X_p (where $X_0 = 1$) satisfy

(12′) $$h_i(1, X_{p-1}, \ldots, X_1, 1) = h_i(1, X_1, \ldots, X_{p-1}, 1),\quad i = 0, 1, \ldots, k-2,$$

and

(13′) $$w_i(1, X_{p-1}, \ldots, X_1, 1) = w_i(1, X_1, \ldots, X_{p-1}, 1),\quad i = 0, 1, \ldots, k.$$

Proof: The proof is so similar to that of Theorem 3a that we omit it here.

4. REDUCTION OF RECURRENCE ORDER

The definition of *kth-order divisibility sequence* in terms of (1) does not preclude a given kth-order sequence from being a jth-order sequence for some $j < k$. However, a linear recurrence sequence must be of some *least* recurrence order, and so the following questions arise:

1. When are the recurrence orders of the sequences of §3, as reported, already least possible?
2. When the recurrence order is reducible to a least value k, so that the generating function $tH(t)/F(t)G(t)$ is reducible to a quotient $th(t)/f(t)g(t)$ whose denominator is a polynomial of degree k, then what symmetric properties remain with this reduced generating function?

Clearly, the least recurrence order of a sequence is k if and only if the polynomials $h(t)$ and $f(t)g(t)$ have no common linear factor.

First, we consider the possibilities for common linear factors in case all the x_i's and y_j's are, as in §3, indeterminates. We can then use this information in case some or all of the x_i's and y_j's are algebraic integers.

Possibilities for reduction of generating functions in Theorems 2, 2a, and 2b

1. $H(t)$ has no linear factors in common with $F(t)G(t)$.
2. $F(t)$ and $G(t)$ have a common linear factor.
3. $F(t)$ or $G(t)$ has a repeated linear factor.
4. $H(t)$ has a linear factor in common with $F(t)G(t)$ which is neither a common linear factor of $F(t)$ and $G(t)$ nor a repeated linear factor of $F(t)$ or $G(t)$.

For the general sequences of Theorem 2 and the Vandermonde sequences of Theorem 2b, the second and third possibilities clearly do not occur, since we are dealing with distinct inteterminates. We conjecture that the fourth possibility does not occur for these sequences or for the resultant sequences, either.

For the resultant sequences of Theorem 2a, the second possibility still cannot occur, for, appealing to α's and β's as in the proof of Theorem 2a, the linear divisors of $F(t)$ are all of the form $1 - BAt$ where B is a product of an even number of β's, hence has even weight in the y-indeterminates; on the other hand, the linear divisors of $G(t)$ all involve odd weights in the y-indeterminates.

However, for resultant sequences, the third possibility does occur. It would be difficult to obtain a general classification of occurrences of repeated linear factors within $F(t)$ or $G(t)$, but to acquire some knowledge of such occurrence, we put $p = q = 4$ and seek repeated linear factors: as in the proof of Theorem 2a, we have

$$\begin{array}{llll}
x_1 = \alpha_1 = \alpha_2 = \alpha_3 = \alpha_4 & \qquad & y_1 = \beta_1 = \beta_5 = \beta_9 = \beta_{13} \\
x_2 = \alpha_5 = \alpha_6 = \alpha_7 = \alpha_8 & \qquad & y_2 = \beta_2 = \beta_6 = \beta_{10} = \beta_{14} \\
x_3 = \alpha_9 = \alpha_{10} = \alpha_{11} = \alpha_{12} & \qquad & y_3 = \beta_3 = \beta_7 = \beta_{11} = \beta_{15} \\
x_4 = \alpha_{13} = \alpha_{14} = \alpha_{15} = \alpha_{16} & \qquad & y_4 = \beta_4 = \beta_8 = \beta_{12} = \beta_{16}
\end{array}$$

The linear factor $1 - y_1y_2x_1^3x_2^3x_3^4x_4^4t$ occurs both as

$$1 - \beta_1\beta_6\alpha_2\alpha_3\alpha_4\alpha_5\alpha_7 \ldots \alpha_{16}t$$

and as

$$1 - \beta_2\beta_5\alpha_1\alpha_3\alpha_4\alpha_6 \ldots \alpha_{16}t.$$

To account for such repetitions, consider the 4 x 4 rectangular array:

	y_1	y_2	y_3	y_4
x_1	1	2	3	4
x_2	5	6	7	8
x_3	9	10	11	12
x_4	13	14	15	16

The sub-array involving 1, 2, 5, 6 corresponds in an obvious way to the equations $\beta_1\beta_6 = \beta_2\beta_5$ and $\alpha_1\alpha_6 = \alpha_2\alpha_5$. Any such occurrence of $\beta_i\beta_j = \beta_\ell\beta_k$ and $\alpha_i\alpha_j = \alpha_\ell\alpha_k$, where $i \neq \ell$, corresponds to a repeated linear factor of $F(t)$ with y-weight 2. The array contains 36 rectangular sub-arrays, each corresponding to a repeated linear factor. A moment's reflection now indicates that there are many more than 36 repeated linear factors of $G(t)$ having y-weight 3, and so on. Since $F'(t)$ and $F(t)$ have a common linear factor whenever $F(t)$ has a repeated linear factor [or the same for $G'(t)$ and $G(t)$], and since

$$H(t) = [F(t)G'(t) - G(t)F'(t)]/R_1,$$

we conclude that the order of recurrence 2^{pq} reported in Theorem 2a can be reduced considerably.

Since $H(t)$ and $F(t)G(t)$ are P-reciprocal polynomials for some P, each linear factor $1 - rt$ of $H(t)$ occurs with $1 - Pr^{-1}t$, and the same pairing occurs in $F(t)G(t)$. For the remainder of this section, we restrict our attention to all the sequences considered in §3 *except* the Vandermonde sequence in the special case $p = 3$. Therefore, in the cases under consideration not only the degree of the denominator, but also that of the numerator, of each generating function, before any possible reductions, is an even positive integer. Accordingly, in the case $1 - rt = 1 - Pr^{-1}t$, this factor occurs an *even* number of times. This remains true in the cases under consideration if any number of the symbols $x_1, \ldots, y_1, \ldots$ represent algebraic integers rather than indeterminates. We summarize and extend these considerations in the following two theorems.

Theorem 4a: For the sequences $\{u_n\}$ of Theorem 2, Theorem 2a, and Theorem 2b (except for $p = 3$), wherein any number of the x_i's and y_i's may be algebraic integers, the least recurrence order k is an even positive integer. The generating function $th(t)/f(t)g(t)$, where $H(t)$ and $F(t)G(t)$ are P-reciprocal polynomials, reduces, by cancellation of common linear factors, to a rational function $th(t)/f(t)g(t)$, where $h(t)|H(t)$, $f(t)|F(t)$, and $g(t)|G(t)$. Moreover, $f(t)g(t)$ is a P-reciprocal polynomial with degree k in t, and $h(t)$ is a P-reciprocal polynomial with degree $k - 2$ in t. The coefficients of these two polynomials lie in $I[\mathcal{A}]$ for the general sequences of Theorem 2, and in I^* for the resultant and Vandermonde sequences of Theorems 2a and 2b.

Proof: All these claims follow easily from the cited theorems, together with the fact that each linear factor $1 - rt$ of $H(t)$ cancels along with another factor, $1 - Pr^{-1}t$. After all such pairs cancel, the remaining linear factors of $h(t)$ and of $f(t)g(t)$ still occur in pairs of the form $1 - rt$, $1 - Pr^{-1}t$, so that we still have P-reciprocal polynomials.

Theorem 4b: The symmetry property for coefficients indicated by (12), (13), (12'), and (13') hold for the coefficients of the reduced polynomials $h(t)$ and $f(t)g(t)$ of Theorem 4a.

Proof: The proof is so similar to that of Theorem 3a that we omit it here.

5. EXAMPLES

Example 1: First, we write out the polynomials $F(t)$, $G(t)$, and $H(t)$ which appear in the generating function of the resultant sequence obtained from

$$X(t) = (t - x_1)(t - x_2)(t - x_3) = t^3 - at^2 + bt - c \quad\text{and}\quad Y(t) = t - d:$$

$$F(t) = 1 - (c + ad^2)t + d^2(ac + bd^2)t^2 - cd^4(b + d^2)t^3 + c^2d^6t^4,$$

$$G(t) = 1 - d(b + d^2)t + d^2(ac + bd^2)t^2 - cd^4(c + ad^2)t^3 + c^2d^6t^4,$$

$$H(t) = 1 - d^2(ac + 3cd + bd^2)t^2 + 2cd^3(c + bd + ad^2 + d^3)t^3 - cd^5(ac + 3cd + bd^2)t^4 + c^3d^9t^6.$$

In accord with Theorems 2a and 3a, $H(t)$ is a cd^3-reciprocal polynomial of the first kind, and a and b are interchangeable within each of the coefficients in case $c = d = 1$. Similar observations hold for the product $F(t)G(t)$.

If $c = d = 1$ and $a = b$, then the resultant $R = c + ad^2 - (bd + d^3)$ of $X(t)$ and $Y(t)$ vanishes, and $F(t) = G(t)$ has the root 1 in common with $H(t)$. In this case, the expression

$$\frac{(x_1^n - 1^n)(x_2^n - 1^n)(1^n - 1^n)}{(x_1 - 1)(x_2 - 1)(1 - 1)}$$

formally equals

$$n\frac{(x_1^n - 1)(x_2^n - 1)}{(x_1 - 1)(x_2 - 1)}$$

which generates a sequence of recurrence order less than 8. Nevertheless, this sequence is formally generated by $tH(t)/F(t)G(t)$.

Putting $-a = b = c = d = 1$, we obtain an 8th-order divisibility sequence:

$$0,\ 1,\ 2,\ 1,\ 8,\ 11,\ 14,\ 34,\ 64,\ 109,\ 242,\ \ldots\ .$$

Example 2: Here we examine a divisor of a resultant sequence. Suppose

$$F(t) = (t - x_1)(t - x_2) = t^2 - at - b$$

and

$$G(t) = (t - y_1)(t - y_2) = t^2 - ct - d.$$

Let

$$A_n = (-1)^n(b^n + d^n) \quad\text{and}\quad \Delta^2 = (a^2 + 4b)(c^2 + 4d),$$

and let

$$L_n = x_1^n + x_2^n, \quad \overline{L}_n = y_1^n + y_2^n$$

and

$$F_n = \frac{x_1^n - x_2^n}{x_1 - x_2}, \quad \overline{F}_n = \frac{y_1^n - y_2^n}{y_1 - y_2}, \quad n = 0,\ 1,\ \ldots\ .$$

Each of the latter four expressions is a polynomial in a and b or c and d. The polynomials $L_n = L_n(a, b)$ and $\overline{L}_n(c, d)$ are often called Lucas polynomials, and the polynomials $F_n = F_n(a, b)$ and $\overline{F}_n = \overline{F}_n(c, d)$ are the Fibonacci polynomials mentioned in §1.

The resultant $R_n(F, G)$ of the polynomials $F_n(t) = (t - x_1^n)(t - x_2^n)$ and $G_n(t) = (t - y_1^n)(t - y_2^n)$ can be written as

$$R_n(a,\ b,\ c,\ d) = \frac{1}{4}(L_n\overline{L}_n - 2A_n + \Delta F_n\overline{F}_n)(L_n\overline{L}_n - 2A_n - \Delta F_n\overline{F}_n),$$

since

$$L_n\overline{L}_n - 2A_n + \Delta F_n\overline{F}_n = -2(x_1^n - y_2^n)(x_2^n - y_1^n)$$

and

$$L_n\overline{L}_n - 2A_n - \Delta F_n\overline{F}_n = -2(x_1^n - y_1^n)(x_2^n - y_2^n).$$

Thus, if $(a^2 + 4b)(c^2 + 4d)$ is a perfect square, the sequence with nth term

$$v_n = \frac{L_n\overline{L}_n - 2A_n + \Delta F_n\overline{F}_n}{L_1\overline{L}_1 - 2A_1 + \Delta F_1\overline{F}_1}$$

is a divisor of the resultant sequence

$$\{u_n\} = \{R_n/R_1\}.$$

Writing $D = x_1y_1 + x_2y_2$, we find that the quotient

$$\text{(18)}\qquad \frac{1 - bdt^2}{1 + (b + d - D)t + (2bd - bD - dD)t^2 + bd(b + d - D)t^3 + b^2d^2t^4}$$

is a generating function for the sequence $\{v_n\}$.

If we put $D = x$, $-b - d = y$, and $-bd = z$, then the sequence $\{v_n\}$ is the same as the sequence $\{\ell_n(x,\ y,\ z)\}$ discussed in detail in [4]. This is a 4th-order divisibility sequence (for which 4 is the least possible order), and as a polynomial in x, we find for $n \geq 2$ the following factorization in terms of linear factors:

$$\ell_n(x,\ 2\alpha,\ -\alpha^2 - \beta^2) = \prod_{k=0}^{n-1}(x - 2\alpha\cos 2k\pi/n - 2\beta\sin 2k\pi/n).$$

It seems likely that *every* 4th-order divisibility sequence with $u_0 = 0$ and $u_1 = 1$ is generated by (18) for some choice of b, d, and D. We point out that 3rd-order divisibility sequences are characterized in Hall [3].

Example 3: Here we examine a Vandermonde sequence. Let

$$X(t) = (t - \alpha)(t - \beta)(t - \gamma) = t^3 - At^2 + Bt - C.$$

The Vandermonde sequence whose nth term is

$$\text{(19)}\qquad \frac{\alpha^n - \beta^n}{\alpha - \beta}\cdot\frac{\alpha^n - \gamma^n}{\alpha - \gamma}\cdot\frac{\beta^n - \gamma^n}{\beta - \gamma},\quad n = 0,\ 1,\ \ldots,$$

has a generating function

$$\frac{t[1 + 2Ct + C(3C - AB)t^2 + 2C^3t^3 + C^4t^4]}{\begin{array}{c}1 + (3C - AB)t + [B^3 + C(A^3 - 5AB + 6C)]t^2 + C[B(2B^2 - A^2B) + C(7C + 2A^3 - 6AB)]t^3\\ + C^2[B^3 + C(A^3 - 5AB + 6C)]t^4 + C^4(3C - AB)t^5 + C^6t^6\end{array}}$$

The first six terms are as follows:

$$u_0 = 0,\quad u_1 = 1,\quad u_2 = AB - C,\quad u_3 = A^2B^2 - B^3 - CA^3$$

$$u_4 = C^3 + 2A^3C^2 - 5ABC^2 + 2B^3C + 3A^2B^2C - 2A^4BC + A^3B^3 - 2AB^4$$

$$\begin{aligned}u_5 = -C^4 + A^3C^3 + 8ABC^3 + B^3C^2 + A^4BC^2 - 15A^2B^2C^2 - 3A^2B^5 - 3A^5B^2C\\ + AB^4C + 8A^3B^3C + A^6C^2 + A^4B^4 + B^6.\end{aligned}$$

For $C = 1$, note that *all* the terms of the sequence are symmetric in A and B, in accord with Theorem 3b.

As a special case, put $A^3 = x$, $B = 0$, and $C = C$. The generating function is then

$$\frac{t(C^2t^2 + Ct + 1)^2}{(C^2t^2 + Ct + 1)^3 + Cx(Ct + 1)^2t^2},$$

and it is easily seen that the numerator and denominator have a common root if and only if $x = 0$, in which case the sequence degenerates to a Fibonacci sequence. Thus, except for $x = 0$, this Vandermonde sequence is of recurrence order 6 and not of any lesser order.

For $A^3 = x$, $B = 0$, $C = 1$, the first nine terms are:

$$u_0 = 0,\quad u_1 = 1,\quad u_2 = -1,\quad u_3 = -x,\quad u_4 = 2x + 1,\quad u_5 = x^2 + x - 1,$$
$$u_6 = -3x^2 - 8x,\quad u_7 = -x^3 - x^2 + 9x + 1,\quad u_8 = 4x^3 + 18x^2 + 6x - 1.$$

It is not difficult to prove that the nth term

$$u_n = u_n(x)$$

of this sequence factors as follows:

$$u_n(x) = (-1)^{n+1}\prod_{k=1}^{\left[\frac{n-1}{2}\right]}[-4x\cos^2 k\pi/n - (4\cos^2 4\pi/n - 1)^3].$$

We conjecture that $u_n(x)$ is irreducible in $I[x]$ if and only if n is a prime positive integer.

Finally, we list some terms of the numerical 6th-order divisibility sequence $\{u_n(-1)\}$ and remark that

$$|u_n(-1)| \le F_n \quad (= \text{the } n\text{th Fibonacci number}),$$

for $1 \le n \le 100$ and perhaps for all positive integers n.

0, 1, -1, 1, -1, -1, 5, -8, 7, 1, -19, 43, -55, 27, 64, -211, 343, -307, -85, 911,

$$u_{20} = -1919 = -19 \cdot 101, \qquad u_{22} = -989 = -43 \cdot 23$$
$$u_{23} = -3151 = -23 \cdot 137, \qquad u_{25} = -15049 = -101 \cdot 149$$
$$u_{27} = 5671 = 53 \cdot 107, \qquad u_{54} = -989617855 = 174505u_{27}.$$

REFERENCES

1. Maxime Bôcher. *Higher Algebra.* New York: Macmillan, 1931.
2. William S. Burnside & Arthur W. Panton. *The Theory of Equations*, Vol. 1. New York: Dover, 1960 (1912).
3. Marshall Hall. "Divisibility Sequences of Third Order." *Amer. J. Math.* 58 (1936):577-584.
4. Clark Kimberling. "Divisibility Properties of Recurrent Sequences." *The Fibonacci Quarterly* 14, No. 4 (1976):369-376.
5. Morgan Ward. "Linear Divisibility Sequences." *Trans. AMS* 41 (1937): 276-286.
6. Morgan Ward. "Arithmetical Properties of Sequences in Rings." *Annals of Math.* 39 (1938):210-219.

7. Morgan Ward. "The Law of Apparition of Primes in a Lucasian Sequence." *Trans. AMS* 44 (1948):68-86.
8. Morgan Ward. "Memoir on Elliptic Divisibility Sequences." *Amer. J. Math.* 70 (1948):31-74.
9. Morgan Ward. "The Law of Repetition of Primes in an Elliptic Divisibility Sequence." *Duke Math. J.* 15 (1948):941-946.

*****

LOCAL PERMUTATION POLYNOMIALS IN THREE VARIABLES OVER Z_p

GARY L. MULLEN
The Pennsylvania State University, Sharon, PA 16146

1. INTRODUCTION

If p is a prime, let Z_p denote the integers modulo p and Z_p^* the set of nonzero elements of Z_p. It is well known that every function from $Z_p \times Z_p \times Z_p$ into Z_p can be represented as a polynomial of degree < p in each variable. We say that a polynomial $f(x_1, x_2, x_3)$ with coefficients in Z_p is a *local permutation polynomial* in three variables over Z_p if $f(x_1, a, b)$, $f(c, x_2, d)$, and $f(e, f, x_3)$ are permutations in x_1, x_2, and x_3, respectively, for all a, b, c, d, e, $f \in Z_p$. A general theory of local permutation polynomials in n variables will be discussed in a subsequent paper.

In an earlier paper [2], we considered polynomials in two variables over Z_p and found necessary and sufficient conditions on the coefficients of a polynomial in order that it represents a local permutation polynomial in two variables over Z_p. The number of Latin squares of order p was thus equal to the number of sets of coefficients satisfying the conditions given in [2]. In this paper, we consider polynomials in three variables over Z_p and again determine necessary and sufficient conditions on the coefficients of a polynomial in order that it represents a local permutation polynomial in three variables over Z_p.

As in [1], a *Latin cube of order* n is defined as an $n \times n \times n$ cube consisting of n rows, n columns, and n levels in which the numbers 0, 1, ..., $n - 1$ are entered so that each number occurs exactly once in each row, column, and level. Clearly the number of Latin cubes of order p equals the number of local permutation polynomials in three variables over Z_p. We say that a Latin cube is *reduced* if row one, column one, and level one are in the form 0, 1, ..., $n - 1$. The number of reduced Latin cubes of order p will equal the number of sets of coefficients satisfying the set of conditions given in Section 2.

In Section 3, we use our theory to show that there is only one reduced local permutation polynomial in three variables over Z_3 and, thus, there is precisely one reduced Latin cube of order three.

2. A NECESSARY AND SUFFICIENT CONDITION

Clearly, the only local permutation polynomials in three variables over Z_p are $x_1 + x_2 + x_3$ and $x_1 + x_2 + x_3 + 1$, so that we may assume p to be an odd prime. We will make use of the following well-known formula:

$$\sum_{j=1}^{p-1} j^k = \begin{cases} 0 & \text{if } k \not\equiv 0 \pmod{p-1} \\ -1 & \text{if } k \equiv 0 \pmod{p-1}. \end{cases} \tag{2.1}$$

Suppose

$$f(x_1, x_2, x_3) = \sum_{m=0}^{p-1} \sum_{n=0}^{p-1} \sum_{r=0}^{p-1} a_{mnr} x_1^m x_2^n x_3^r$$

is a local permutation polynomial over Z_p. We assume that $f(x_1, x_2, x_3)$ is in reduced form so that for $t = 0, 1, \ldots, p-1$ we have

$$f(t, 0, 0) = f(0, t, 0) = f(0, 0, t) = t.$$

Thus, the corresponding Latin cube is reduced so that row one, column one, and level one are in the form $0, 1, \ldots, p-1$. If we write out the above equations and use the fact that the coefficient matrix is the Vandermonde matrix whose determinant is nonzero, we have the condition

$$a_{t00} = a_{0t0} = a_{00t} = \begin{cases} 0 & \text{if } t = 0, 2, 3, \ldots, p-1 \\ 1 & \text{if } t = 1. \end{cases} \tag{C1}$$

It is well known that no permutation over Z_p can have degree $p-1$. By considering the polynomials $f(0, n, x_3)$ for $n = 0, 1, \ldots, p-1$, one can show that $a_{0,n,p-1} = 0$ for $n = 0, 1, \ldots, p-1$. Proceeding in a similar manner, we find that

$$\left.\begin{aligned} a_{0,t,p-1} &= a_{t,0,p-1} = 0 \\ a_{0,p-1,t} &= a_{t,p-1,0} = 0 \\ a_{p-1,t,0} &= a_{p-1,0,t} = 0 \end{aligned}\right\} \text{ for } t = 0, 1, \ldots, p-1. \tag{C2}$$

Let

$$f(i, j, x_3) = \sum_{m=0}^{p-1} \sum_{n=0}^{p-1} \sum_{r=0}^{p-1} a_{mnr} i^m j^n x_3^r, \text{ for } 1 \le i, j \le p-1$$

and consider the coefficient of x_3^{p-1}. Using the fact that no permutation over Z_p can have degree $p-1$, we see that

$$\sum_{m=0}^{p-1} \sum_{n=0}^{p-1} a_{m,n,p-1} i^m j^n = 0, \text{ for } 1 \le i, j \le p-1. \tag{C3}$$

Similarly, one can show that

$$\sum_{m=0}^{p-1} \sum_{r=0}^{p-1} a_{m,p-1,r} i^m k^n = 0, \text{ for } 1 \le i, k \le p-1. \tag{C4}$$

and

$$\sum_{n=0}^{p-1} \sum_{r=0}^{p-1} a_{p-1,n,r} j^n k^n = 0, \text{ for } 1 \le j, k \le p-1. \tag{C5}$$

We note that the above conditions correspond to conditions (C1) and (C1′) of [2].

Let $f(i, j, k) = \ell(i, j, k)$ for $0 \le i, j, k \le p-1$. Suppose $i = 0$ so that

$$f(0, j, k) = \sum_{n=0}^{p-1} \sum_{r=0}^{p-1} a_{0nr} j^n k^r.$$

Let $\ell'(0, j, k) = f(0, j, k) - \ell(0, 0, 0)$. Fix j and write out the $p-1$

equations for $k = 1, \ldots, p - 1$. For fixed j, $\{\ell'(0, j, k)\}$ runs through the elements of Z_p^*. If we raise each of the equations to the ℓth power, sum by columns using (2.1), we obtain for each $j = 1, \ldots, p - 1$,

$$\text{(C6)} \qquad \sum \prod_{r=1}^{p-1} \prod_{n=0}^{p-1} \frac{\ell! a_{0nr}^{i_{0nr}} j^{\Sigma n}}{i_{0nr}!} = \begin{cases} 0 & \text{if } \ell = 2, \ldots, p-2 \\ 1 & \text{if } \ell = p-1, \end{cases}$$

where the sum is over all i_{0nr} such that

$$\text{(2.2)} \qquad 0 \le i_{0nr} \le \ell$$

$$\text{(2.3)} \qquad \sum_{r=1}^{p-1} \sum_{n=0}^{p-1} i_{0nr} = \ell$$

$$\text{(2.4)} \qquad \sum_{r=1}^{p-1} \sum_{n=0}^{p-1} r i_{0nr} \equiv 0 \pmod{p-1}.$$

In the condition (C6), Σn is understood to mean the sum, counting multiplicities, of all second subscripts of the a_{0nr}'s which appear in a given term.

Similarly, if we fix k and write out the $p - 1$ equations for $j = 1, \ldots, p - 1$, raise each equation to the ℓth power, sum by columns using (2.1), we obtain for each $k = 1, \ldots, p - 1$,

$$\text{(C7)} \qquad \sum \prod_{n=1}^{p-1} \prod_{r=0}^{p-1} \frac{\ell! a_{0nr}^{i_{0nr}} k^{\Sigma r}}{i_{0nr}!} = \begin{cases} 0 & \text{if } \ell = 2, \ldots, p-2 \\ 1 & \text{if } \ell = p-1, \end{cases}$$

where the sum is over all i_{0nr} such that

$$\text{(2.5)} \qquad 0 \le i_{0nr} \le \ell$$

$$\text{(2.6)} \qquad \sum_{n=1}^{p-1} \sum_{r=0}^{p-1} i_{0nr} = \ell$$

$$\text{(2.7)} \qquad \sum_{n=1}^{p-1} \sum_{r=0}^{p-1} n i_{0nr} \equiv 0 \pmod{p-1}.$$

We observe that we can obtain the condition (C7) from the condition (C6) as follows. In (C6), (2.2), (2.3), and (2.4), let $n = r$, $r = n$, and $j = k$. After making these substitutions, replace the subscripts $0rn$ by $0nr$ to obtain (C7).

Along the same line, let $j = 0$ and $\ell'(i, 0, k) = f(i, 0, k) - \ell(0, 0, 0)$. If i is fixed, then for each $i = 1, \ldots, p - 1$, we obtain

$$\text{(C8)} \qquad \sum \prod_{r=1}^{p-1} \prod_{m=0}^{p-1} \frac{\ell! a_{m0r}^{i_{m0r}} i^{\Sigma m}}{i_{m0r}!} = \begin{cases} 0 & \text{if } \ell = 2, \ldots, p-2 \\ 1 & \text{if } \ell = p-1, \end{cases}$$

where the sum is over all i_{m0r} such that

$$\text{(2.8)} \qquad 0 \le i_{m0r} \le \ell$$

$$\sum_{r=1}^{p-1} \sum_{m=0}^{p-1} i_{m0r} = \ell \tag{2.9}$$

$$\sum_{r=1}^{p-1} \sum_{m=0}^{p-1} r i_{m0r} \equiv 0 \pmod{p - 1}. \tag{2.10}$$

If $j = 0$ and k is fixed, then for each $k = 1, \ldots, p - 1$ we obtain a set of conditions (C9) which can be obtained from the condition (C8) as follows. In (C8), (2.8), (2.9), and (2.10), let $m = r$, $r = m$, and $i = k$. After making these substitutions, replace the subscripts $r0m$ by $m0r$ to obtain (C9).

Finally, if $k = 0$, then for $i = 1, \ldots, p - 1$, we obtain .

$$\sum \prod_{n=1}^{p-1} \prod_{m=0}^{p-1} \frac{\ell ! a_{mn0}^{i_{mn0}} i^{i_{mn0} \cdot \Sigma m}}{i_{mn0}!} = \begin{cases} 0 & \text{if } \ell = 2, \ldots, p - 2 \\ 1 & \text{if } \ell = p - 1, \end{cases} \tag{C10}$$

where the sum is over all i_{mn0} such that

$$0 \leq i_{mn0} \leq \ell \tag{2.11}$$

$$\sum_{n=1}^{p-1} \sum_{m=0}^{p-1} i_{mn0} = \ell \tag{2.12}$$

$$\sum_{n=1}^{p-1} \sum_{m=0}^{p-1} n i_{mn0} \equiv 0 \pmod{p - 1}. \tag{2.13}$$

If $k = 0$, then for $j = 1, \ldots, p - 1$ we obtain a set of conditions (C11) which can be obtained from (C10) as follows. In (C10), (2.11), (2.12), and (2.13), let $m = n$, $n = m$, and $i = j$. After making these substitutions, replace the subscripts $nm0$ by $mn0$ to obtain (C11).

Thus, we have six sets of conditions involving coefficients where at least one subscript on the coefficient is zero. These conditions correspond to the conditions (C2) and (C2′) of [2].

We will now consider the general case where $ijk > 0$. Let $f(i, j, k) = \ell(i, j, k)$ and suppose $\ell'(i, j, k) = f(i, j, k) - \ell(i, j, 0)$ for fixed i and j. The set $\{\ell'(i, j, k)\}$ for $k = 1, \ldots, p - 1$ constitutes all of Z_p^*. Raising each of the equations to the ℓth power, summing by columns using (2.1), we obtain for each $1 \leq i, j \leq p - 1$,

$$\sum \prod_{r=1}^{p-1} \prod_{m=0}^{p-1} \prod_{n=0}^{p-1} \frac{\ell ! a_{mnr}^{i_{mnr}} i^{i_{mnr} \cdot \Sigma m} j^{i_{mnr} \cdot \Sigma n}}{i_{mnr}!} = \begin{cases} 0 & \text{if } \ell = 2, \ldots, p - 2 \\ 1 & \text{if } \ell = p - 1, \end{cases} \tag{C12}$$

where the sum is over all i_{mnr} such that

$$0 \leq i_{mnr} \leq \ell \tag{2.14}$$

$$\sum_{r=1}^{p-1} \sum_{m=0}^{p-1} \sum_{n=0}^{p-1} i_{mnr} = \ell \tag{2.15}$$

$$\sum_{r=1}^{p-1} \sum_{m=0}^{p-1} \sum_{n=0}^{p-1} r i_{mnr} \equiv 0 \pmod{p - 1}. \tag{2.16}$$

Fixing i and k and proceeding as above for each $1 \leq i, k \leq p - 1$, we obtain a set of conditions (C13) which can be obtained from (C12) as follows. In (C12), (2.14), (2.15), and (2.16), let $n = r$, $r = n$, and $j = k$. After making these substitutions, replace the subscripts mrn by mnr to obtain (C13).

Finally, fixing j and k and proceeding as above, for each $1 \leq j, k \leq p - 1$, we obtain a set of conditions (C14) which can be obtained from (C12) as follows. In (C12), (2.14), (2.15), and (2.16), let $m = r$, $r = m$, and $i = k$. After making these substitutions, replace subscripts rnm by mnr to obtain (C14).

We observe that the conditions (C12), (C13), and (C14) correspond to the conditions (C3) and (C3′) of [2]. We note that the set of conditions (C1), ..., (C14) actually involves a total of

$$9p + 3(p - 1)^2 + 6(p - 1)(p - 2) + 3(p - 1)^2(p - 2) = 3p^3 - 3p^2 + 9$$

conditions. Further, it should be noted that some of the above conditions may be simplified by making substitutions from (C1) and (C2). However, we will not make these substitutions at the present time.

We now proceed to show that, if the coefficients of a polynomial $f(x_1, x_2, x_3)$ satisfy the above conditions, then $f(x_1, x_2, x_3)$ is a local permutation polynomial over Z_p. Suppose the coefficients of $f(x_1, x_2, x_3)$ satisfy the conditions (C1), ..., (C14). For each fixed $0 \leq i, j \leq p - 1$, let $t_{ijk} = f(i, j, k) - f(i, j, 0)$ for $k = 1, \ldots, p - 1$. The above conditions imply that for fixed i and j the t_{ijk} satisfy

$$(2.17) \qquad \sum_{k=1}^{p-1} t_{ijk}^{\ell} = \begin{cases} 0 & \text{if } \ell = 1, \ldots, p - 2 \\ -1 & \text{if } \ell = p - 1. \end{cases}$$

Let V be the matrix

$$V = \begin{bmatrix} 1 & \ldots & 1 \\ t_{ij1} & \ldots & t_{i,j,p-1} \\ \vdots & & \vdots \\ t_{ij1}^{p-2} & \ldots & t_{i,j,p-1}^{p-2} \end{bmatrix}.$$

Using (2.17), we see that

$$\det(V^2) = \det(V)\det(V^t) = \det \begin{bmatrix} -1 & 0 & \ldots & 0 & 0 \\ 0 & 0 & \ldots & 0 & -1 \\ 0 & 0 & \ldots & -1 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & -1 & \ldots & 0 & 0 \end{bmatrix} = \pm 1.$$

Since $\det(V)$ is the Vandermonde determinant, we have for fixed i and j,

$$\det(V) = \prod_{k_1 > k_2} (t_{ijk_1} - t_{ijk_2}) \neq 0,$$

so that the t_{ijk} are distinct for $k = 1, \ldots, p - 1$. Hence, for fixed i and j, $f(i, j, 0)$ and $f(i, j, k) = t_{ijk} + f(i, j, 0)$ for $k = 1, \ldots, p - 1$ constitute all of Z_p.

If $0 \leq i, k \leq p - 1$ are fixed, let $s_{ijk} = f(i, j, k) - f(i, 0, k)$ for $j = 1, \ldots, p - 1$. Proceeding as above, $f(i, 0, k)$ and $f(i, j, k) = s_{ijk} + f(i, 0, k)$ are distinct for $j = 1, \ldots, p - 1$ and thus constitute all of Z_p.

Similarly, if $0 \leq j$, $k \leq p - 1$ are fixed, let $u_{ijk} = f(i, j, k) - f(0, j, k)$ for $i = 1, \ldots, p - 1$. Hence, $f(0, j, k)$ and $f(i, j, k) = u_{ijk} + f(0, j, k)$ are distinct for $i = 1, \ldots, p - 1$ and thus constitute all of Z_p.

We have now proven the following.

Theorem 1: If $f(x_1, x_2, x_3)$ is a polynomial over Z_p, p an odd prime, then f is a reduced local permutation polynomial over Z_p if and only if the coefficients of f satisfy (C1), ..., (C14).

Corollary 2: The number of reduced Latin cubes of order p an odd prime equals the number of sets of coefficients $\{a_{mnr}\}$ satisfying the above conditions.

3. ILLUSTRATIONS

As a simple illustration of the above theory, we determine all reduced local permutation polynomials in three variables over Z_3. Let

$$f(x_1, x_2, x_3) = \sum_{m=0}^{2} \sum_{n=0}^{2} \sum_{r=0}^{2} a_{mnr} x_1^m x_2^n x_3^r. \tag{3.1}$$

The corresponding Latin cube will be in reduced form, so that row one, column one, and level one are in the form 0, 1, and 2. From (C1), we see that

$$\begin{aligned} a_{000} &= 0 \\ a_{100} = a_{010} = a_{001} &= 1 \\ a_{200} = a_{020} = a_{002} &= 0. \end{aligned} \tag{3.2}$$

From (C2), we see that

$$\begin{aligned} a_{012} = a_{102} = a_{021} = a_{120} = a_{210} = a_{201} &= 0 \\ a_{022} = a_{202} = a_{022} = a_{220} = a_{202} = a_{220} &= 0. \end{aligned} \tag{3.3}$$

We have thus uniquely determined 16 coefficients from the conditions (C1) and (C2).

From (C3), we obtain, after some simplification,

$$\begin{aligned} a_{112} + a_{122} + a_{212} + a_{222} &= 0 \\ 2a_{112} + a_{122} + 2a_{212} + a_{222} &= 0 \\ 2a_{112} + 2a_{122} + a_{212} + a_{222} &= 0 \\ a_{112} + 2a_{122} + 2a_{212} + a_{222} &= 0, \end{aligned} \tag{3.4}$$

so that $a_{112} = a_{122} = a_{212} = a_{222} = 0$.

From (C4), we obtain, after some simplification,

$$\begin{aligned} a_{121} + a_{221} &= 0 \\ 2a_{121} + 2a_{221} &= 0 \\ 2a_{121} + a_{221} &= 0 \\ a_{121} + 2a_{221} &= 0, \end{aligned} \tag{3.5}$$

so that $a_{121} = a_{221} = 0$. Using (C5), after some simplification, we see that $a_{211} = 0$.

From (C6), with $j = 1$, we have, after some simplification,

$$a_{001}^2 + a_{011}^2 + 2a_{001}a_{011} = 1. \tag{3.6}$$

If $j = 2$ in (C6), we obtain

$$a_{001}^2 + a_{011}^2 + a_{001}a_{011} = 1. \tag{3.7}$$

Using (3.6) and (3.7) along with the fact that $a_{001} = 1$, we see that $a_{011} = 0$.

Since all the variables in (C7) have already been uniquely determined, we proceed to (C8), where we obtain

$$a_{001}^2 + a_{101}^2 + 2a_{001}a_{101} = 1 \tag{3.8}$$

and

$$a_{001}^2 + a_{101}^2 + a_{001}a_{101} = 1, \tag{3.9}$$

so that $a_{101} = 0$.

From (C10), we obtain

$$a_{010}^2 + a_{110}^2 + 2a_{010}a_{110} = 1 \tag{3.10}$$

and

$$a_{010}^2 + a_{110}^2 + a_{010}a_{110} = 1, \tag{3.11}$$

so that $a_{110} = 0$.

From (C12), we obtain, after simplification,

$$a_{111}^2 + 2a_{111} = 0 \tag{3.12}$$

and

$$a_{111}^2 + a_{111} = 0, \tag{3.13}$$

so that $a_{111} = 0$.

We have now uniquely determined all 27 coefficients in (3.1). Thus,

$$f(x_1, x_2, x_3) = x_1 + x_2 + x_3$$

is the only reduced local permutation polynomial in three variables over Z_3 and, hence, there is precisely one reduced Latin cube of order three. If we list the cube in terms of the three Latin squares of order three which form its different levels, we can list the only reduced Latin cube of order three as

012	120	201
120	201	012
201	012	120.

REFERENCES

1. J. Arkin and E. G. Straus. "Latin k-cubes." *The Fibonacci Quarterly* 12 (1974):288-292.
2. G. L. Mullen. "Local Permutation Polynomials over Z_p." *The Fibonacci Quarterly* 18 (1980):104-108.

*****

SOME COMBINATORIAL IDENTITIES

MORDECHAI LEWIN
Israel Institute of Technology, Haifa

In this paper, we wish to derive some combinatorial identities (partly known, partly apparently new) by combining well-known recurrence relations with known forms for characteristic polynomials of paths and cycles (i.e., of their adjacency matrices). We also obtain some extensions of known results.

Define $P_0 = 1$, $P_1 = x$. For $n > 1$, define

$$P_n = P_n(x) = xP_{n-1} - P_{n-2}. \tag{1}$$

This recurrence relation has been investigated by Liebestruth [5] (see also [2, v. I, p. 402]). The formula for P_n is given as

$$P_n = \sum_{k=0} (-1)^k \binom{n-k}{k} x^{n-2k} \tag{2}$$

for every nonnegative integer n.

The following Fibonacci polynomial is treated in [8].

$$F_0(x) = 0,\ F_1(x) = 1,\ F_n(x) = xF_{n-1}(x) + F_{n-2}(x)$$

(see also [4]). The polynomial P_n is hence essentially a Fibonacci polynomial. As such (2) appears as a problem in [7]. The connection between the polynomial P_n and F_n is easily seen to be

$$P_n(x) = i^n F_{n+1}(-ix), \tag{3}$$

where i is the imaginary unit.

By postulating $P_{-1} = 0$, and in general

$$P_{-n} = -P_{n-2} \tag{4}$$

for all positive integers n, P_n turns out to be a polynomial for every integer n. It is easy to check that both (1) and (4) are valid for all integral n.

Using (1) and the induction principle, we can show that, for $n \geq 0$, we have

$$x^n = \sum_{k=0} \binom{n-1}{k} P_{n-2k}. \tag{5}$$

Let t be any positive integer. Writing $x = P_1$, (1) may be written as

$$P_1 P_t = P_{t+1} + P_{t-1}. \tag{6}$$

Now let t be any positive integer ≥ 2. It is easily checked that

$$P_2 P_t = P_{t+2} + P_t + P_{t-2}. \tag{7}$$

We shall now show that (6) and (7) are special cases of the general formula expressed by

Theorem 1: For any nonnegative integers s and t we have

$$P_s P_t = \sum_{k=0}^{s} P_{t+s-2k}.$$

We first prove Theorem 1 for the case $0 \leq s \leq t$. For $s = 0, 1, 2$, the theorem is already established. Let it hold for all $0 \leq s' < s$ and for all $t \geq s'$. Consider s, t such that $2 < s \leq t$. Using (1), we have

$$\begin{aligned} P_s P_t &= (xP_{s-1} - P_{s-2})P_t = xP_{s-1}P_t - P_{s-2}P_t \\ &= x\sum_{k=0}^{s-1} P_{s+t-1-2k} - \sum_{k=0}^{s-2} P_{s+t-2-2k} \\ &= \sum_{k=0}^{s-1} P_{s+t-2k} + \sum_{k=0}^{s-1} P_{s+t-2-2k} - \sum_{k=0}^{s-2} P_{s+t-2-2k} = \sum_{k=0}^{s} P_{s+t-2k}. \end{aligned}$$

This proves the theorem for $0 \le s \le t$.

The right-hand side of Theorem 1 appears at first sight not to be symmetric with respect to s and t. We show it to be symmetric. We first prove the simple

Lemma 1:

$$\sum_{k=1}^{n} P_{n-2k} = 0.$$

Proof: Take the terms in pairs symmetric with respect to their positions in the series. We then have

$$\sum_{k=1} P_{n-2k} = \sum_{j=1}^{[n/2]} (P_{n-2j} + P_{-(n-2j)-2}) = 0,$$

which proves the lemma.

Now let $s > t$. Put $n = s - t$ and apply Lemma 1. Then

$$\sum_{k=1}^{s-t} P_{s-t-2k} = 0. \tag{8}$$

Equality (8) together with that part of Theorem 1 already proved yield

$$\begin{aligned} P_s P_t &= \sum_{k=0}^{t} P_{s+t-2k} = \sum_{k=0}^{t} P_{s+t-2k} + \sum_{k=1}^{s-t} P_{s-t-2k} \\ &= \sum_{k=0}^{t} P_{s+t-2k} + \sum_{k=t+1}^{s} P_{s-t-2(k-t)} = \sum_{k=0}^{s} P_{s+t-2k}, \end{aligned}$$

which proves the theorem for all nonnegative integers s and t.

The following are some special cases of Theorem 1.

$$P_n^2 = \sum_{k=0}^{n} P_{2k}, \tag{9}$$

$$P_n P_{n+1} = \sum_{k=0}^{n} P_{2k+1}. \tag{10}$$

Both (9) and (10) appear in [2, p. 403].

We now have

Theorem 2: Let m and n be arbitrary integers. Then

$$P_n^2 - P_{n-m}P_{n+m} = P_{m-1}^2.$$

Proof: *Case 1.* $0 \le m \le n$. By using Theorem 1 for $s = n - m$, $t = n + m$, we get

$$P_{n-m}P_{n+m} = \sum_{k=0}^{n-m} P_{2(n-k)} = \sum_{k=m}^{n} P_{2k}. \tag{11}$$

Putting $m = 0$ in (11) yields (9). Subtracting (11) from (9) yields

$$P_n^2 - P_{n-m}P_{n+m} = \sum_{k=m}^{m-1} P_{2k}.$$

Using (9) again we obtain Theorem 2. This settles Case 1.

Case 2. $0 \leq n < m$.

Subcase 2.1.—$n + 1 > m - 1$. Since $n + 1 \leq m$, it follows that $m - 1 = n$. Then $n - m = -1$, and the theorem holds.

Subcase 2.2.—$n + 1 \leq m - 1$. Then, using (4), we may write

$$\begin{aligned} P^2_{m-1} + P_{n-m}P_{n+m} &= P^2_{m-1} - P_{m-n-2}P_{n+m} \\ &= P^2_{m-1} - P_{m-1-(n+1)}P_{m-1+(n+1)} = P^2_n. \end{aligned}$$

The last equality follows by applying Case 1 to $n + 1$ and $m - 1$. This completes Case 2.

The remaining cases are settled by applying similar arguments.

Corollary 1: For all integral n, we have

$$P^2_n - P_{n-1}P_{n+1} = 1.$$

Proof: Put $m = 1$ in Theorem 2.

Writing (1) again we have $xP_n = P_{n+1} + P_{n-1}$. Then,

$$x^2P_n = x(P_{n+1} + P_{n-1}) = P_{n+2} + 2P_n + P_{n-2}.$$

By induction, it is easy to show that for all positive integers r we have

$$x^rP_n = \sum_{k=0} \binom{r}{n} P_{n+r-2k}.$$

Then,

$$\begin{aligned} P_sP_t &= \sum_{q=0} (-1)^q \binom{s-q}{q} x^{s-2q}P_t \\ &= \sum_{q=0} (-1)^q \binom{s-q}{q} \left\{ \sum_{k=0} \binom{s-2q}{k} P_{t+s-2(q+k)} \right\}. \end{aligned} \tag{12}$$

Now let $q + k = m$ be constant. Equating corresponding terms of Theorem 1 and (12) we obtain, after replacing s by n,

Theorem 3: Let m, n be nonnegative integers such that $m \leq n$. Then,

$$\sum_{k=0}^{\min(m,\, n-m)} (-1)^k \binom{n-k}{k} \binom{n-2k}{m-k} = 1.$$

Corollary 2: For any nonnegative integer n, we have

$$\sum_{k=0}^{n} (-1)^k \frac{(2n-k)!}{k!((n-k)!)^2} = 1.$$

Proof: Put $n = 2m$ in Theorem 3 and replace m by n.

For nonnegative n, the polynomial $P_n(x)$ is known to be the characteristic polynomial of a simple path of length n (number of vertices in the path) [1, p. 75].

Let $C_n(x)$ be the characteristic polynomial of an n-cycle. In [6, p. 159], the following close relationship between $C_n(x)$ and $P_n(x)$ is given for $n \geq 3$:

$$C_n = C_n(x) = P_n - P_{n-2} - 2. \tag{13}$$

Using (4), we may write (13) as

$$C_n = P_n + P_{-n} - 2. \tag{14}$$

In a regular graph G, the order of regularity r is an eigenvalue of G. Therefore, we have $C_n(2) = 0$. Using (13), we obtain

$$P_n(2) = P_{n-2}(2) + 2 \tag{15}$$

for $n \geq 3$. Since $P_0(2) = 1$, $P_1(2) = 2$, $P_2(2) = 3$, it follows that for $n \geq 0$ we have

$$P_n(2) = n + 1. \tag{16}$$

This is a result in [3, 1.72].

Using (14), it is easily checked that both (15) and (16) are valid for all integral n.

Using the known expression for P_n, [6], we obtain

$$\begin{aligned} P_n &= \sum_{k=0} (-1)^k \binom{n-k}{k} x^{n-2k} = \prod_{j=1}^{n} (x - 2\cos(\pi j/(n+1))) \\ &= x^h \prod_{j=1}^{[n/2]} (x^2 - 4\cos^2(\pi j/(n+1))), \end{aligned} \tag{17}$$

where $h = n - 2[n/2]$, [8].

For positive n, (16) and (17) together imply

$$2^n \prod_{j=1}^{n} (1 - \cos(\pi j/(n+1))) = n + 1. \tag{18}$$

Taking the factors of the left-hand side in pairs, we get

Theorem 4: Let n be an integer > 1. Then,

$$\prod_{k=1}^{[n/2]} \sin(\pi k/(n+1)) = (n+1)^{\frac{1}{2}} 2^{-n/2}.$$

Theorem 4 and the left-hand side of (17) together yield

$$\prod_{k=1}^{[n/2]} \sin^2(\pi k/(n+1)) = (n+1)2^{-2} = \sum_{k=0} \left(-\frac{1}{4}\right)^k \binom{n-k}{k}. \tag{19}$$

Put $x = 0$ in (17) and let n be even and positive.

Put $n = 2m$. We then have

$$P_n(0) = (-1)^m = (-1)^m 2^n \prod_{k=1}^{m} \cos^2(\pi k/(n+1)),$$

yielding

Theorem 5: $\displaystyle\prod_{k=1}^{m} \cos(\pi k/(2m+1)) = 2^{-m}.$

Now put $x = 2i$. It then follows from (17) that

$$2^n i^n \sum_{k=0} 4^{-k} \binom{n-k}{k} = 2^n \prod_{j=1}^{n} (i - \cos(\pi j/(n+1))).$$

Again taking the factors in pairs and cancelling out, we get

(20)
$$\sum_{k=0} \binom{n-k}{k} 4^{-k} = \prod_{j=1}^{[n/2]} (1 + \cos^2(\pi j/(n+1))).$$

By setting $x = i$ in (17), we get

$$P_n(i) = i^n \sum_{k=0} \binom{n-k}{k} = \prod_{j=1}^{n} (i - 2\cos(\pi j/(n+1))).$$

Taking the factors in pairs yields

(21)
$$\sum_{k=0} \binom{n-k}{k} = \prod_{j=1}^{[n/2]} (1 + 4\cos^2(\pi j/(n+1))).$$

Using (3), it follows that

(22)
$$P_n(i) = i^n F_{n+1}(1) = i^n f_{n+1},$$

where f_n is the nth term of the Fibonacci sequence

$$f_0 = 0,\ f_1 = 1,\ f_2 = 1,\ f_n = f_{n-1} + f_{n-2}.$$

Combining (21) and (22), we get

(23)
$$f_{n+1} = \prod_{j=1}^{[n/2]} (1 + 4\cos^2(\pi j/(n+1))).$$

Theorem 1 and (22) together yield, for $s \leq t$,

(24)
$$f_s f_t = \sum_{k=0}^{s-1} (-1)^k f_{s+t-1-2k}.$$

A considerable number of identities and results on Fibonacci numbers may be derived from repeatedly using (24).

Let $\textcircled{Y}_n$ be the Y-graph mentioned in [6, p. 162] and let $Y_n = Y_n(x)$ be its characteristic polynomial. It follows from [6] that

(25)
$$Y_n = x(P_{n-1} - P_{n-3}) = P_n - P_{n-4}.$$

We then have

$$Y_n(2) = P_n(2) - P_{n-4}(2) = 4.$$

Using the expression for Y_n in [6], we get

(26)
$$Y_n = x \prod_{j=1}^{n-1} (x - 2\cos(\pi(2j-1)/2(n-1))).$$

Combining (25) and (26), we get, after setting $x = 2$,

$$2^n \prod_{j=1}^{[(n-1)/2]} (1 - \cos^2(\pi(2j-1)/2(n-1))) = 4.$$

Writing n instead of $n - 1$, we get

$$\prod_{j=1}^{[n/2]} (1 - \cos^2(\pi(2j-1)/2n)) = 2^{1-n},$$

and finally,

$$\prod_{j=1}^{[n/2]} \sin(\pi(2j - 1)/2n) = 2^{-\frac{1}{2}(n-1)}. \tag{27}$$

REFERENCES

1. L. Collatz and U. Sinogowitz. "Spektren endlicher Grafen." *Abh. Math. Sem. Univ. Hamburg* 21 (1957):63-77.
2. L. E. Dickson. *History of the Theory of Numbers.* I. N.Y.: Chelsea, 1952.
3. H. W. Gould. *Combinatorial Identities.* Morgantown, W. Va.: Henry W. Gould, 1972.
4. V. E. Hoggatt, Jr., and M. Bicknell. "Roots of Fibonacci Polynomials." *The Fibonacci Quarterly* 11 (1973):271-274.
5. L. Liebestruth. "Beitrag zur Zahlentheorie." *Progr.*, Zerbst, 1888.
6. A. J. Schwenk. "Computing the Characteristic Polynomial of a Graph." In "Graphs and Combinatorics." *Lecture Notes Math.* 406 (1974):153-172.
7. M. N. S. Swamy. Problem B-74. *The Fibonacci Quarterly* 3 (1965):236.
8. W. A. Webb and E. A. Parberry. "Divisibility Properties of Fibonacci Polynomials." *The Fibonacci Quarterly* 7 (1969):457-463.

*****

ADDITIVE PARTITIONS OF THE POSITIVE INTEGERS

V. E. HOGGATT, JR.
San Jose State University, San Jose, CA 95192

1. INTRODUCTION

In July 1976, David L. Silverman (now deceased) discovered the following theorem.

Theorem 1: There exist sets A and B whose disjoint union is the set of positive integers so that no two distinct elements of either set have a Fibonacci number for their sum. Such a partition of the positive integers is *unique.*

Detailed studies by Alladi, Erdös, and Hoggatt [1] and, most recently, by Evans [7] further broaden the area.

The Fibonacci numbers are specified as $F_1 = 1$, $F_2 = 1$, and, for all integral n, $F_{n+2} = F_{n+1} + F_n$.

Lemma: F_{3m} is even, and F_{3m+1} and F_{3m+2} are odd.

The proof of the lemma is very straightforward.

Let us start to make such a partition into sets A and B. Now, 1 and 2 cannot be in the same set, since $1 = F_2$ and $2 = F_3$ add up to $3 = F_4$. Also, 3 and 2 cannot be in the same set, because $2 + 3 = 5 = F_5$.

$$A = \{1, 3, 6, 8, 9, 11, \ldots\};$$

$$B = \{2, 4, 5, 7, 10, 12, 13, \ldots\}.$$

If we were to proceed, we would find that there is but one choice for each integer. We also note, from $F_{n+2} = F_{n+1} + F_n$, that F_{2n} belongs in set

A, and F_{2n+1} belongs in set B for all $n \geq 1$. Thus, all the positive Fibonacci numbers F_m $(m > 1)$ have their positions uniquely determined.

Proof of Theorem 1: The earlier discussion establishes the *inductive basis*.

> *Inductive Assumption*: All the positive integers in $\{1, 2, 3, \ldots, F_k\}$ have their places in sets A and B determined subject to the constraint that no two distinct members of either set have any Fibonacci number as their sum.

Note that $F_{k-1} - i$ and $F_k + i$ must lie in opposite sets, and this yields a unique placement of the integers x, $F_k < x < F_{k+1}$. By the inductive hypothesis, no two integers x and y lying in the interval $1 \leq x, y \leq F_k$ which are in the same set add up to a Fibonacci number; thus, we have constructed and extended sets A and B so that this goes to F_{k+1}, except we now must show that no x, y such that

$$F_{k-1} < x < F_k \quad \text{and} \quad F_k < y < F_{k+1}$$

can lie in the same set and have a Fibonacci number for their sum. Actually, such x and y yield

$$F_{k+1} < x + y < F_{k+2},$$

and there is no Fibonacci number in that interval. We now determine whether x and y both lying between F_k and F_{k+1} can be in the same set and add up to a Fibonacci number. Let

$$x = F_k + i \quad \text{and} \quad y = F_k + j, \quad 0 < i, j < F_{k-1},$$

so that

$$\begin{aligned} 2F_k &< x + y < 2F_{k+1} \\ 2F_k &< 2F_k + i + j < 2F_{k+1}. \end{aligned}$$

The only Fibonacci number in that interval is F_{k+2}, and thus $i + j = F_{k-1}$.

From the fact that $F_k + i$ and $F_{k-1} - i$ lie in opposite sets *and* $F_k + j$ and $F_{k-1} - j$ lie in opposite sets, then if $F_k + i$ and $F_k + j$ were in the same set, so would be $F_{k-1} - i$ and $F_{k-1} - j$, but if $i + j = F_{k-1}$, then the sum of $(F_{k-1} - i)$ and $(F_{k-1} - j)$ is F_{k-1}, which violates the inductive hypothesis. Thus, no two distinct positive integers x and y, $x, y \leq F_{k+1}$, lie in the same set and sum to a Fibonacci number.

By the principle of mathematical induction, we have shown the *existence* and *uniqueness* of the additive partition of the positive integers into two sets such that no two distinct members of the same set add up to a Fibonacci number. This concludes the proof of the theorem.

Theorem 2: For every positive integer N not equal to a Fibonacci number, there exist two distinct Fibonacci numbers F_m and F_n such that the system

$$\begin{aligned} a + b &= N \\ b + c &= F_m \\ a + c &= F_n \end{aligned}$$

has solutions with a, b, and c positive integers,

$$a = \frac{N + F_n - F_m}{2}, \quad b = \frac{N + F_m - F_n}{2}, \quad c = \frac{F_m + F_n - N}{2}.$$

Comments: The sum of $F_m + F_n + N$ is even. The numbers N, F_n, and F_m must satisfy the triangle inequalities

$$\begin{aligned} N + F_n &> F_m, \\ N + F_m &> F_n, \\ F_m + F_n &> N. \end{aligned}$$

Proof: The proof will be presented for six cases. Recall that F_{3m} is even and F_{3m+1} with F_{3m+2} are odd.

Case 1: N even, $F_{3k} < N < F_{3k+1}$.

$$\begin{aligned} F_{3k-1} + F_{3k+1} &> N \\ F_{3k+1} + N &> F_{3k-1} \\ F_{3k-1} + N &> F_{3k+1} \end{aligned}$$

Case 2: N odd, $F_{3k} < N < F_{3k+1}$.

$$\begin{aligned} F_{3k+1} + N &> F_{3k} \\ F_{3k} + N &> F_{3k+1} \\ F_{3k+1} + F_{3k} &> N \end{aligned}$$

Case 3: N even, $F_{3k-1} < N < F_{3k}$.

$$\begin{aligned} F_{3k+1} + N &> F_{3k-1} \\ F_{3k-1} + N &> F_{3k+1} \\ F_{3k+1} + F_{3k-1} &> N \end{aligned}$$

Case 4: N odd, $F_{3k-1} < N < F_{3k}$.

$$\begin{aligned} F_{3k-1} + N &> F_{3k} \\ F_{3k} + N &> F_{3k-1} \\ F_{3k} + F_{3k-1} &> N \end{aligned}$$

Case 5: N even, $F_{3k+1} < N < F_{3k+2}$.

$$\begin{aligned} F_{3k+1} + N &> F_{3k+2} \\ F_{3k+2} + N &> F_{3k-1} \\ F_{3k+2} + F_{3k} &> N \end{aligned}$$

Case 6: N odd, $F_{3k+1} < N < F_{3k+2}$.

$$\begin{aligned} F_{3k} + N &> F_{3k+2} \\ F_{3k+2} + N &> F_{3k} \\ F_{3k+2} + F_{3k} &> N \end{aligned}$$

From the direct theorem, a and c lie in opposite sets and b and c lie in opposite sets; hence, a and b lie in the same set.

Corollary 1: In each of the six cases above, it is a fact that

$$a - b = F_m - F_n,$$

which is always a Fibonacci number (Sarsfield [5]).

Corollary 2: F_{2m} and F_{2n} never add to a Fibonacci number, nor do F_{2m+1} and F_{2n+1} for $n \neq m \neq 0$.

2. EXTENSIONS OF PARTITION RESULTS

In this section, we shall use Zeckendorf's theorem to prove and extend the results cited in [3].

Zeckendorf's theorem states that every positive integer has a unique representation using distinct Fibonacci numbers $F_2, F_3, \ldots, F_n, \ldots,$ if no two consecutive Fibonacci numbers are to be used in the representation.

Theorem 1: The Fibonacci numbers additively partition the Fibonacci numbers *uniquely*.

Proof: Since $F_m + F_n = F_p$ if and only if $p = m + 2 = n + 1$, $m, n > 1$, by Zeckendorf's theorem, let set A_1 contain F_{2n+1} and set A_2 contain F_{2n+2}, $n \geq 1$. No two distinct members of A_1 and no two distinct members of A_2 can sum to a Fibonacci number by Zeckendorf's theorem.

Theorem 2: The Lucas numbers additively partition the Lucas numbers *uniquely*.

Proof: Similar to the proof of Theorem 1, since the Lucas numbers enjoy a Zeckendorf theorem (see Hoggatt [6]).

Theorem 3: The Lucas numbers additively partition the Fibonacci numbers *uniquely*.

Discussion: Let $A_1 = \{1, 5, 8, 34, 55, \ldots\}$

$$= \{F_2, F_5, F_6, F_9, F_{10}, \ldots\}$$

$$= \{F_2, F_{4n+1}, F_{4n+2}\}_{n=1}^{\infty},$$

and $A_2 = \{F_3, F_4, F_{4n+3}, F_{4n+4}\}_{n=1}^{\infty}$.

The proof is omitted.

Theorem 4: The union of the Fibonacci numbers and Lucas numbers additively partition the Fibonacci numbers uniquely into three sets—A_1, A_2, and A_3—such that no two distinct members of the same set sum to a Lucas number and no two distinct members of the same set sum to a Fibonacci number.

Proof: From $L_n = F_{n+1} + F_{n-1}$, we see that Zeckendorf's theorem guarantees a unique representation for each L_n in terms of Fibonacci numbers.

Let A_1 contain F_{3n-1}, A_2 contain F_{3n}, and A_3 contain F_{3n+1} for $n > 1$. No two consecutive Fibonacci numbers can belong to the same set because they would sum to a Fibonacci number, and no two alternating subscripted Fibonacci numbers can belong to the same set because they would sum to a Lucas number; therefore, the above partitioning must obtain.

Theorem 5: The union of the sequences $\{F_i + F_{i+j}\}_{n=2}^{\infty}$, $j = 1, 2, \ldots, k$, partitions the Fibonacci numbers uniquely into k sets so that no two members of the same set add up to a member of the union sequences.

Theorem 6: The sequence $\{5F_n\}$ uniquely partitions the Lucas numbers.

Discussion: Let $A_1 = \{2, L_{4n-1}, L_{4n}\}_{n=1}^{\infty}$, and

$$A_2 = \{1, 3, L_{4n+1}, L_{4n+2}\}_{n=1}^{\infty}.$$

The proof is omitted.

There are clearly many more results which could be stated but we now now leave Fibonacci and Lucas numbers and go to the Tribonacci numbers

$$T_1 = T_2 = 1, T_3 = 2, \ldots, T_{n+3} = T_{n+2} + T_{n+1} + T_n, (n \geq 1).$$

3. TRIBONACCI ADDITIVE PARTITION OF THE POSITIVE INTEGERS

Let

$$T_1 = T_2 = 1, T_3 = 2,$$

and

$$T_{n+3} = T_{n+2} + T_{n+1} + T_n$$

for all $n \geq 1$. Below, we shall show that the set $\{3, T_n\}_{n=2}^{\infty} = R$ induces an additive partition of the positive integers uniquely into two sets A_1 and A_2 such that no two distinct members of A_1 and no two distinct members of A_2 add up to a member of R, and, further, every $n \notin R$ can be so represented.

Since $T_{n+3} = T_{n+2} + T_{n+1} + T_n$, it is clear that T_{n+2} and $T_{n+1} + T_n$ are in opposite sets, and so say $T_2 = 1$ is in set A_1 and $T_3 = 2$ is in A_2 since we wish to avoid 3. Now, $T_3 + T_4$ must also be in A_2 since $T_2 + T_3 + T_4 = T_5$. Thus, T_{3n+1} and T_{3n+2} are in A_1 and T_{3n} is in A_2, $T_{3n-1} + T_{3n}$ and $T_{3n+1} + T_{3n}$ are in A_2 and $T_{3n+1} + T_{3n+2}$ is in A_1. This is easily established by induction.

If $T_{3n+1} + T_{3n+2}$ is in A_1, then T_{3n+3} and T_{3n} are in A_2. Since $T_{3n-1} + T_{3n}$ and $T_{3n+1} + T_{3n}$ are in A_2, then T_{3n-2} and T_{3n+1} with T_{3n-1} and T_{3n+2} are all in A_1. This places all the Tribonacci numbers.

Since T_{3n+1} is in A_1, then $T_{3n+2} + T_{3n+3}$ is in A_2. Thus, since T_{3n+2} is in A_1, then $T_{3n+3} + T_{3n+4}$ is in A_2, and T_{3n+5} is in A_1. This completes the induction.

Now that all the Tribonacci numbers are placed in sets A_1 and A_2, we place the positive integers in sets A_1 and A_2.

It is clear that $(T_n - i)$ and i are in opposite sets, except when $i = T_n/2$. From $T_{n+4} = T_{n+3} + T_{n+2} + T_{n+1}$, we get

$$T_{n+4} + T_n = T_{n+3} + (T_{n+2} + T_{n+1} + T_n) = 2T_{n+3}.$$

Thus, generally,

$$T_{n+4}/2 + T_n/2 = T_{n+3}.$$

Since T_{4n-1} and T_{4n} are even, and T_{4n+1} and T_{4n+2} are odd, we get two different sets. $T_{4n}/2$ and $T_{4n+4}/2$ must lie in opposite sets because their sum is T_{4n+3}. Also, $T_{4n-1}/2$ and $T_{4n+3}/2$ must lie in opposite sets because their sum is T_{4n+2}. $T_4/2 = 2$ is in set A_2, and $T_8/2 = 22$ is in A_1. Thus, $T_{8n}/2$ is in A_2, and $T_{8n+4}/2$ is in A_1. $T_3/2 = 1$ is in A_1, and $T_7/2 = 12$ is in A_2; thus, $T_{8n+3}/2$ is in A_1, and $T_{8n+7}/2$ is in A_2. So, by induction, the placement for all integers $i = T_n/2$ is complete.

The use of 3 in set R forced us to put 1 in A_1 and 2 in A_2 as an initial choice. Now, all T_n and $T_n/2$ have been placed. Since $(T_n - i)$ and i are in opposite sets except when $i = T_n/2$, we can specify the unique placement of the other positive integers.

This establishes the uniqueness of the bisection. Each T_n, each $T_n + T_{n+1}$, and each $T_n/2$ an integer is uniquely placed.

Next, consider $n \notin R$, $n \neq T_n + T_{n+1}$. Then

$$\left.\begin{aligned} a + b &= n \\ b + c &= T_s \\ c + a &= T_t \end{aligned}\right\}$$

is solvable provided that $(n + T_s + T_t)$ is even and

$$\left.\begin{aligned} T_s + T_t - n &> 0 \\ T_s + n - T_t &> 0 \\ T_t + n - T_s &> 0 \end{aligned}\right\}$$

Lemma: For every $n \notin R$ and $n \neq T_n + T_{n+1}$ there exist two Tribonacci numbers T_s and T_t such that $T_s + T_t + n$ is even, and

$$\left.\begin{aligned} T_s + T_t - n &> 0 \\ T_s + n - T_t &> 0 \\ T_t + n - T_s &> 0 \end{aligned}\right\}$$

Proof: There are several cases. Let $T_t < n < T_{t+1}$ where T_t and T_{t+1} are both even; then, if n is even, we are in business. If n is odd, then

$$T_t < n < T_{t+1} < T_{t+2}$$

where T_t and T_{t+1} are even and T_{t+2} is odd, and $n \neq T_{t-1} + T_t$, then either T_{t-1}, n, T_t or T_{t+1}, n, T_{t+2} will do the job.

Next, let $T_t < n < T_{t+1}$ where T_t is odd and T_{t+1} is even. If n is odd, we are in business. If n is even, T_{t+1}, n, T_{t+2} or T_t, n, T_{t-1} will do the job except when $n = T_{t-1} + T_t$.

Finally, let $T_t < n < T_{t+1}$ where T_t and T_{t+1} are odd. If n is even, we are in business; if n is odd, then n, T_{t+1}, T_{t+2} or T_{t-1}, n, T_t will do the job except when $n = T_t + T_{t+1}$.

Thus, if $n \neq T_r$ and $n \neq T_t + T_{t-1}$, the system of equations

$$\left.\begin{aligned} a + b &= n \\ b + c &= T_t \\ c + a &= T_s \end{aligned}\right\}$$

is solvable in positive integers. Note that c and a cannot be in the same set, nor can b and c be in the same set. Therefore, a and b are in the same set, so that n is so representable.

We now show that $n = T_t + T_{t-1}$ are representable in the same side on which they appear as the sum of two integers, and take the cases for

$$n = T_t + T_{t-1}.$$

Earlier we noted that T_{3n+1} and T_{3n+2} are in A_1 and $T_{3n+1} + T_{3n+2}$ is in A_1, so that $T_{3n+1} + T_{3n+2}$ is representable as the sum of two elements. We now look at $6 = 5 + 1$.

As we said, $T_{3n+1} + T_{3n+2}$, $T_{3n} + T_{3n+1}$, $T_{3n+4} + T_{3n+5}$, and $T_{3n+3} + T_{3n+4}$ lie in A_2. Look at

$$T_{3n+5} + T_{3n+4} - (T_{3n+4} + T_{3n+3}) = T_{3n+5} - T_{3n+3}.$$

This is in set A_2, because T_{3n+3} is in A_1. Thus, since $(T_{3n+4} + T_{3n+3})$ and $(T_{3n+5} - T_{3n+3})$ are both in A_2, $T_{3n+5} + T_{3n+4}$ has a representation as the sum of two elements from set A_2.

Next, consider

$$\begin{aligned} &T_{3n+4} + T_{3n+3} - (T_{3n+1} + T_{3n}) \\ &= T_{3n+4} + T_{3n+3} + T_{3n+2} - (T_{3n+2} + T_{3n+1} + T_{3n}) \\ &= T_{3n+5} - T_{3n+3}, \end{aligned}$$

which we have seen to lie in A_2, so that

$$(T_{3n+5} - T_{3n+3}) + (T_{3n+1} + T_{3n}) = T_{3n+4} + T_{3n+3}$$

is the sum of two integers from A_2, since both are in A_2. This completes the proof.

If $n \neq T_m$ or $n \neq T_s + T_{s+1}$, then n has a representation as the sum of two elements from the same set. If $n = T_s + T_{s+1}$, then if $n = T_{3m+1} + T_{3m+2}$, both T_{3m+1} and T_{3m+2} appear in A_1, and n has a representation as the sum of two elements from A_1. If $n = T_{3m+2} + T_{3m+3}$ or $n = T_{3m} + T_{3m+1}$, then each has a sum of two elements from A_2.

REFERENCES

1. K. Alladi, P. Erdös, and V. E. Hoggatt, Jr. "On Additive Partitions of Integers." *Discrete Mathematics* 22 (1978):201-211.
2. Robert E. F. Higgins. "Additive Partitions of the Positive Integers." Unpublished Master's thesis, San Jose State University, August 1978.
3. V. E. Hoggatt, Jr. "Additive Partitions I." *The Fibonacci Quarterly* 15, No. 2 (1977):166.
4. V. E. Hoggatt, Jr. "Additive Partitions II." *The Fibonacci Quarterly* 15, No. 2 (1977):182.
5. Richard Sarsfield, private communication.
6. V. E. Hoggatt, Jr. *Fibonacci and Lucas Numbers*. Boston: Houghton-Mifflin Publishing Company, 1969. Theorem VII, p. 76.
7. R. Evans. "On Additive Partitions of Alladi, Erdös, and Hoggatt." To appear.

*****

THE NUMBER OF MORE OR LESS "REGULAR" PERMUTATIONS

G. KREWERAS
Institut de Statistique, Paris, France

Let us call S_{m+1} the set of all permutations of the integers $\{1, 2, \ldots, m+1\}$. Any permutation α from S_{m+1} may be decomposed into b blocks $B_1, B_2, \ldots, B_b$ defined by the following property: each block consists of integers increasing unit by unit, and no longer block has the same property.

<u>*Example*</u>: $m = 8$, $\alpha = 314562897$; there are $b = 6$ blocks:

$$B_1 = 3,\ B_2 = 1,\ B_3 = 456,\ B_4 = 2,\ B_5 = 89,\ B_6 = 7.$$

The lengths of the blocks form a b-composition q of $m + 1$ (see [1]); in the above example, $q = (1, 1, 3, 1, 2, 1)$.

If $\alpha(i)$ is the ith integer in α, $\alpha(i)$ and $\alpha(i+1)$ belong to the same block iff $\alpha(i+1) = \alpha(i) + 1$; let us call the number of i's satisfying this condition the regularity r of α. Obviously $b + r = m + 1$, so that b and r are equivalent descriptive parameters of α. The greatest possible regularity is $r = m$; it occurs iff α is the identical permutation. The smallest possible regularity is $r = 0$; it occurs iff $q = (1, 1, 1, \ldots, 1)$; we shall call the corresponding permutations "irregular permutations," and look for their number. More generally, we shall call $U(m, r)$ the subset of S_{m+1} consisting of the permutations of regularity r, and $u(m, r)$ the cardinality of $U(m, r)$. We know already that $u(m, m) = 1$ and that

$$\sum_{r=0}^{m} u(m, r) = (m+1)! \tag{1}$$

Setting $u(m, 0) = u$, we shall first show that

$$u(m, r) = \binom{m}{r} u_{m-r}. \tag{2}$$

Let us start from a permutation α of regularity r, i.e., of $b = m - r + 1$ blocks. Besides their order of appearance in α, there is an "order of increasing values" of the blocks; in that order, the smallest block in the above example is 1 ($=B_2$), then comes 2 ($=B_4$), then 3 ($=B_1$), then 456 ($=B_3$), then 7 ($=B_6$), and finally, 89 ($=B_5$). If we relabel the blocks according to their place in the latter order, and if we list them by order of appearance in α, we obtain a permutation p of $\{1, 2, \ldots, b\}$; in the above example, $p = (314265)$.

Necessarily, this permutation p is an irregular one, since, if it had two consecutive integers at two consecutive places, it would mean that the corresponding blocks in α could be merged into a single block, which is contradictory with the definition of the "blocks."

Let us start now from the pair (p, q), where p is any irregular permutation of $\{1, 2, \ldots, m - r + 1\}$ and q is any $(m - r + 1)$-composition of $m + 1$:

$$p = (p_1, p_2, \ldots, p_b),$$
$$q = (q_1, q_2, \ldots, q_b).$$

If $p_i = p(i) = 1$, transform p by replacing p_i by a block $(123 \ldots q_i)$; if $p(j) = 2$, replace p_j by a block $(q_i + 1, q_i + 2, \ldots, q_i + q_j)$, and so on, until p is finally transformed into a permutation α of $\{1, 2, \ldots, m + 1\}$.

This procedure defines in fact a $(1-1)$-correspondence between the set $U(m, r)$ and the set of pairs (p, q) consisting of an irregular permutation p of $\{1, 2, \ldots, m - r + 1\}$ and a $(m - r + 1)$-composition q of $m + 1$. Since it is well known that the number of u-compositions of v is $\binom{v-1}{u-1}$, we can conclude that

$$u(m, r) = u_{m-r}\binom{m}{m-r},$$

which proves (2).

Inverting (1) after replacement of $u(m, r)$ by its expression (2), we obtain

$$u = \sum_{r=0}^{m} (-1)^r \binom{m}{r} (m + 1 - r)!,$$

which may be written

$$u_m = \Delta^m 1!. \tag{3}$$

This enables us to calculate u_m for moderate values of m:

$m =$ 0	1	2	3	4	5	6	...
$u_m =$ 1	1	3	11	53	309	2119	...

For larger values of m, it is convenient to use recursion formulas with positive terms only, which will be connected with a closer investigation of irregular permutations.

If we start from one of the u_m permutations belonging to $U(m,\ 0)$, say α, and if we delete $m+1$ in α, the remaining permutation β of $\{1, 2, \ldots, m\}$ may be irregular or not, and, in fact, will be of regularity either 0 or 1. Conversely, the whole set $U(m,\ 0)$ can be reconstructed by the reinsertion of integer $m+1$ either at some suitable place of an irregular permutation β or at the only suitable place of a permutation β of regularity 1.

If β is irregular, there are $m+1$ conceivable places for insertion of integer $m+1$, but one and only one of them, namely the place immediately after integer m, is not suitable. The number of corresponding possibilities is thus mu_{m-1}.

If β is of regularity 1, the number of possibilities for β is given by formula (2), substituting $m-1$ for m and 1 for r, which yields $(m-1)u_{m-2}$; integer $m+1$ must then be inserted between the only two consecutive integers of β.

Finally,

$$u_m = mu_{m-1} + (m-1)u_{m-2}, \tag{4}$$

which provides an easier calculation of the sequence.

A numerical table of $u(m,\ r)$ is readily formed from the knowledge of u_m and formula (2):

	$r =$ 0	1	2	3	4
$m =$ 0	1				
1	1	1			
2	3	2	1		
3	11	9	3	1	
4	55	44	18	4	1

The following properties are easy to verify:

(1°) Column $r = 1$ consists of the "rencontres" numbers (see [2]). The numbers of columns 0 and 1 appear in [3], but without reference to their enumerative meaning.

(2°) The Blissard generating function [2] of column 0,

$$y(x) = \sum_{m=0}^{+\infty} u_m \frac{x^m}{m!},$$

satisfies the differential equation

$$y'\,(1-x) = y(1+x),$$

since (4) may be written

$$u_{m+1} - mu_m = u_m + mu_{m-1}.$$

Elementary integration yields

$$y = y_0 = e^{-x}(1-x)^{-2}.$$

(3°) The Blissard generating function y_r of column r is given by use of (2):

$$\sum_m \binom{m}{r} u_{m-r}\frac{x^m}{m!} = \frac{x^r}{r!}\sum_m u_{m-r}\frac{x^{m-r}}{(m-r)!},$$

so that

$$y_r = e^{-x}(1-x)^{-2}x^r/r!.$$

(4°) The sum $\sum_{r=0}^{+\infty} y_r$ is $(1-x)^{-2} = 1 + 2x + 3x^2 + \cdots$, which confirms that the coefficient of $x^m/m!$ is $(m+1)!$.

(5°) According to (3), the ratio $u_m/(m+1)!$ is equal to

$$1 - \binom{m}{1}\frac{1}{m+1} + \binom{m}{2}\frac{1}{(m+1)m} - \cdots + (-1)^r\binom{m}{r}\frac{1}{(m+1)_r} + \cdots$$

As m increases, with fixed r, the general term of this sum tends toward $(-1)^r/r!$; it follows that the sum itself tends toward e^{-1}, which is the limiting proportion of irregular permutations.

(6°) Using (2), it appears that

$$\frac{u(m,r)}{(m+1)!} = \frac{u_{m-r}}{(m-r+1)!}\cdot\frac{m-r+1}{r!(m+1)}.$$

As m increases, the second member tends toward $e^{-1}/r!$. The latter result means that, if a permutation is chosen at random in S_{m+1} and if m increases, the limiting probability distribution of its regularity is a Poisson distribution with mean 1.

REFERENCES

1. L. Comtet. *Analyse Combinatoire*. Paris: P.U.F., 1970. I:132.
2. J. Riordan. *An Introduction to Combinatorial Analysis*, pp. 65 and 19-20. New York, 1958.
3. M. Rumney & E. J. F. Primrose. *The Mathematical Gazette* 52 (1968):381.

*****

STAR POLYGONS, PASCAL'S TRIANGLE, AND FIBONACCI NUMBERS

AARON B. BUDGOR
Lawrence Livermore Laboratory, U.C., Livermore, CA 94550

In recent years, there has been some flurry of excitement over the relationship between the complexity of a graph, i.e., the number of distinct spanning trees in a graph, and the Fibonacci and Lucas numbers [1, 2]. In this note, I shall demonstrate a relationship, although incomplete, between the Fibonacci numbers and the star polygons. My hope is to spur further research into the connection between nonplanar graphs and their enumeration from number theory.

The star n-polygon $\left\{\begin{matrix} n \\ d \end{matrix}\right\}$, one of the simplest of these nonplanar graphs, is constructed by placing n points equidistantly on the perimeter of a circle and then connecting every dth point such that

$$n/d \text{ is relatively prime and } n \neq n - d \neq 1.$$

The last condition effectively removes the class of all regular polygons.

The group structure of such polygons is clear; it is related to the partition of unity in which this partition is prime. Therefore, it does not come as any surprise that a symmetry relation for the star n-polygon $\left\{\begin{matrix} n \\ d \end{matrix}\right\}$ is

$$\left\{\begin{matrix} n \\ d \end{matrix}\right\} = \left\{\begin{matrix} n \\ n - d \end{matrix}\right\}. \tag{1}$$

This fact was brought to my attention by Ms Dianne Olvera.

It then intrigued me to discern whether the symbolic symmetry exhibited by (1) could be generated by a somewhat similar number-theoretic symmetry, that produced by Pascal's triangle; row-wise, the combinatorial symmetry

$$\binom{\gamma}{\beta} = \binom{\gamma}{\gamma - \beta} \tag{2}$$

exists.

At first glance, the similarity between (1) and (2) appears to be only cosmetic, since there are absolutely no restrictions on the values of the positive integers γ and β as long as $\gamma > \beta$. Secondly, there seems to be no numerical congruence between (1) and (2).

On the other hand, if one were to examine the Fibonacci numbers F_n generated by summing entries along the diagonals of Pascal's triangle, an algorithm can be constructed that will produce all the possible star n-polygons excluding a sparse set. The procedure is as follows.

Algorithm: The symmetry relation $\left\{\begin{matrix} n \\ d \end{matrix}\right\} = \left\{\begin{matrix} n \\ n - d \end{matrix}\right\}$ for star n-polygons results from partitioning any number or sum of numbers in the sum of some Fibonacci sequence equalling n around its relatively prime divisors.

Example 1: The star pentagons (pentagrams) $\left\{\begin{matrix} 5 \\ 2 \end{matrix}\right\} = \left\{\begin{matrix} 5 \\ 3 \end{matrix}\right\}$ are generated by summing the Fibonacci numbers $F_3 + F_4 = 5$. Since its prime divisors are 2 and 3, respectively, partitioning 5 around 2 yields the star pentagon $\left\{\begin{matrix} 5 \\ 2 \end{matrix}\right\} = \left\{\begin{matrix} 5 \\ 3 \end{matrix}\right\}$.

Example 2: The star heptagons $\left\{\begin{matrix} 7 \\ 5 \end{matrix}\right\} = \left\{\begin{matrix} 7 \\ 2 \end{matrix}\right\}$ and $\left\{\begin{matrix} 7 \\ 3 \end{matrix}\right\} = \left\{\begin{matrix} 7 \\ 4 \end{matrix}\right\}$ are generated by summing the Fibonacci numbers $F_1 + F_2 + F_3 + F_4 = 1 + 1 + 2 + 3 = 7$. Partitioning the sum around 3 produces $\left\{\begin{matrix} 7 \\ 3 \end{matrix}\right\} = \left\{\begin{matrix} 7 \\ 4 \end{matrix}\right\}$. The reader can quickly convince himself or herself that partitions around various alternative sums of this sequence which are relatively prime to 7 do not generate any other possibilities.

Example 3: Star nonagons are obtainable by summing the sequences

$$F_1 + F_4 + F_5 = 1 + 3 + 5 = 9$$

and

$$F_1 + F_2 + F_3 + F_5 = 1 + 1 + 2 + 5 = 9.$$

The former yields, upon partitioning around the sum $F_1 + F_4$, the star nonagons $\left\{ {9 \atop 4} \right\} = \left\{ {9 \atop 5} \right\}$, while the latter yields, upon partitioning around the sum $F_1 + F_2 + F_3$ or around F_3, the previous star nonagon or $\left\{ {9 \atop 2} \right\} = \left\{ {9 \atop 7} \right\}$.

I have examined all the possible star nonagons for all n inclusive of 21. When $n = 13$ and 21, this algorithm breaks down and will not produce $\left\{ {13 \atop 6} \right\}$, $\left\{ {21 \atop 4} \right\}$, and $\left\{ {21 \atop 10} \right\}$. For larger values of n, other discrepancies will appear (n need not be a Fibonacci number), but always much fewer in number than the star n-gons that are generated.

It therefore appears that the Fibonacci sequence on its own cannot exhaustively generate all star n-gons. The basic reason for this nonisomorphism is that the Fibonacci numbers are related to the combinatorics of spanning trees, the combinatorics of planar graphs, not of nonplanar graphs.

REFERENCES

1. A. J. W. Hilton. "Spanning Trees and Fibonacci and Lucas Numbers." *The Fibonacci Quarterly* 12 (October 1974):259-262.
2. K. R. Rebman. "The Sequence 1 5 16 45 121 320 ... in Combinatorics." *The Fibonacci Quarterly* 13 (February 1975):51-55.

*****

A CONVERGENCE PROOF ABOUT AN INTEGRAL SEQUENCE

MASAJI YAMADA
Ibaraki University, Naka-Narusawa, Hitachi, Japan

ABSTRACT

The major theorem proven in this paper is that every positive integer necessarily converges to 1 by a finite number of iterations of the process such that, if an odd number is given, multiply by 3 and add 1; if an even number if given, divide by 2.

The first step is to show an infinite sequence generated by that iterative process is recursive. For the sake of that object, an integral variable x with $(\ell + 1)$ bits is decomposed into $(\ell + 1)$ variables $a_0, a_1, \ldots, a_\ell$, each of which is a binary variable. Then, rth iteration, starting from x, has a correspondence with a fixed polynomial of $a_0, \ldots, a_\ell$, say

$$f_r(a_0, \ldots, a_\ell),$$

no matter what value x takes. Since the number of distinct f_r's is finite in the sense of normalization, the common f_r must appear after some iterations. In the circumstances, the sequence must be recursive.

The second step is to show that a recursive segment in that sequence is (1, 2) or (2, 1). For that object, the subsequences with length 3 of that segment are classified into twelve types concerned with the middle elements modulo 12. The connectability in the segment with length 5 or larger, and the constancy of the values at the head of each segment, specify the types of subsequences, found impossible, as well as with lengths 1, 3, and 4. The only possible segment is that with length 2, like (1, 2) or (2, 1).

1. INTRODUCTION

An iterative process illustrated in Figure 1* is conjectured to necessarily converge to 1 with a finite number of iterations whenever its initial value is a positive integer. It seems, however, that no proof is yet found (see [1]).

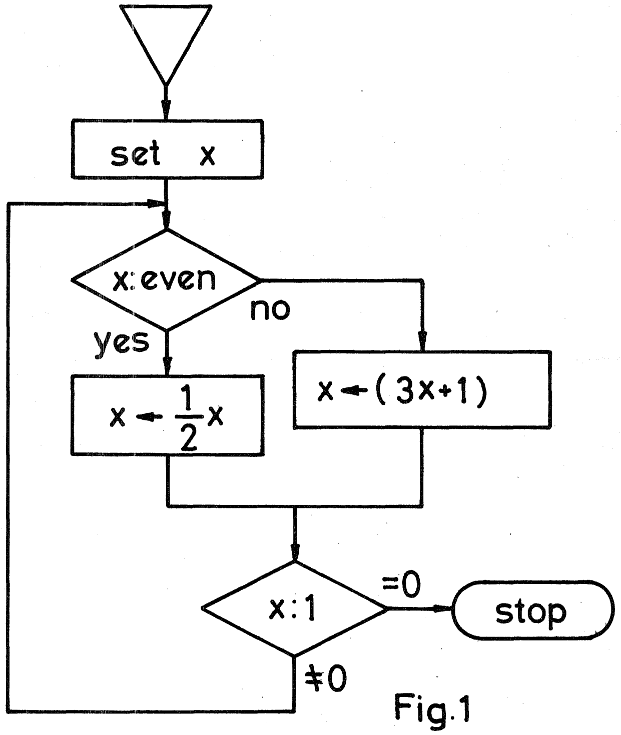


Fig.1

It is the main object to prove the truth of this conjecture.

By preliminary considerations, we easily find:

1. This iterative process is always feasible and not stopped without a reason before it attains 1.

2. If we eliminate the stopping operation after we gain 1, the sequence will be followed by a recursive sequence such as (4, 2, 1, 4, 2, 1, ...).

3. Since $(3x + 1)$ yields as an even number for odd x, then twice running on the odd side path would not occur in succession.

2. NOTATIONS AND DEFINITIONS; STATEMENT OF THE PROBLEM

ℓ is a fixed number, $\ell \in Z^+$.

a_i, $i = 0, 1, 2, \ldots, \ell$ are binary (integral) variables in the range of [0, 1] and $a_0 + a_1 + \cdots + a_\ell \neq 0$.

x is a variable such that $x = 2^\ell a_0 + 2^{\ell+1} a_1 + \cdots + a_\ell$.

$\{F(a_0, a_1, \ldots, a_\ell)\}$, or $\{F(a)\}$, for short, is a set of $F(a_0, a_1, \ldots, a_\ell)$'s, the polynomials with integral coefficients about $a_0, a_1, \ldots, a_\ell$, including a polynomial with *0*th order.

*[*AMS (MOS) Subject Classifications* (1970). Primary 10A35,10L99,68A40.

$F_\mu(a_0, a_1, \ldots, a_\ell)$, or $F_\mu(a)$, is an element of $\{F(a)\}$ composed of the the terms about the combinations of $1, a_0, \ldots, a_\ell$, as:

$$F_\mu(a) = c + c_0a_0 + c_1a_1 + \cdots + c_{01}a_0a_1 + \cdots + c_{01\ldots\ell}a_0a_1 \ldots a_\ell,$$

where $c, c_0, \ldots, c_{01\ldots\ell} \varepsilon \{0, 1\}$.

$P[F(a)]$ is a binary function about some $F(a)$ whose value is assigned as 1 or 0 according to the parity (odd or even) of the values of $F(a)$.

$AF(a)$ is the transformation of $F(a)$, where

$$AF(a) = \tfrac{1}{2}F(a) + [F(a) + \tfrac{1}{2}]P[F(a)].$$

Then, we can embed the original problem into the following:

Let ℓ be artitrarily given. Let x_0 be an arbitrary number, where

$$x_0 \; \varepsilon \; \{1, 2, 3, \ldots, 2^{\ell+1} - 1\}.$$

Then,

(i) *every x_r, $r = 1, 2, 3, \ldots$ is a positive integer, where*

$$x \;\; = \tfrac{1}{2}(3x_{r-1} + 1) \text{ for odd } x_{r-1};\; x_r = \tfrac{1}{2}x_{r-1} \text{ for even } x_{r-1},$$

and

(ii) *an infinite sequence $(x_0, x_1, \ldots)$—referred to as the S-sequence—has a recursive segment $(1, 2)$.*

3. PROCEDURES OF THE PROOF

The process of the proof is roughly classified into two stages:

1. A sequence $S{:}(x_0, x_1, \ldots)$ must necessarily have a subsequence with periodicity.

2. This periodical subsequence must necessarily have a recursive segment as $(1, 2)$.

4. PROOF OF PERIODICITY

Lemma 1: *Let a_i^*, $i = 0, 1, \ldots, \ell$ be some fixed numbers,*

$$a_i^* \; \varepsilon \; \{0, 1\} \text{ and } a_0^* + a_1^* + \cdots + a_\ell^* \neq 0.$$

If $a_i = a_i^*$, then $x = x_0$, where

$$x_0 = 2^\ell a_0^* + 2^{\ell-1}a^* + \cdots + a_\ell^* \text{ and } x_0 \; \varepsilon \; \{1, 2, \ldots, 2^{\ell+1} - 1\}.$$

Conversely, let x_0 be a fixed number,

$$x_0 \; \varepsilon \; \{1, 2, \ldots, 2^{\ell+1} - 1\}.$$

If $x = x_0$, then $a_i = a_i^*$, $i = 0, 1, \ldots, \ell$, where

$$a_0^* = \left[\frac{x_0}{2^\ell}\right], \; a_j^* = \left[\frac{x_0}{2^{\ell-j}}\right] - 2\left[\frac{x_0}{2^{\ell-j+1}}\right], \; j \; \varepsilon \; [1, \ell],$$

and

$$a_i^* \; \varepsilon \; \{0, 1\} \text{ with } a_0^* + \cdots + a_\ell^* \neq 0.$$

Proof: Obvious.

Corollary 1-1: $a_i^\nu = a_i^\nu$ *and* $P(a_i) = a_i$, $i = 0, 1, \ldots, \ell$, for $^\forall\nu \; \varepsilon \; Z^+$.

Proof: It is obvious, since the statement does hold for arbitrary values a_i of a_i, $i = 0, 1, \ldots, \ell$.

Lemma 2: $\{F_\mu(a)\} \subseteq \{F(a)\}$.

$\{F_\mu(a)\}$ is a finite set with 2^K elements, where $K = 2^{\ell+1}$.

$\{F_\mu(a)\}$ is an ordered set with $\mu = 2^{K-1}c + 2^{K-2}c_0 + \cdots + c_{01\ldots\ell}$.

Proof: It is obvious, since K is the total number of the coefficients

$$c,\ c_0,\ c_1,\ \ldots,\ c_{01\ldots\ell},$$

that is,

$$K = 1 + \binom{\ell+1}{1} + \binom{\ell+1}{2} + \cdots + \binom{\ell+1}{\ell+1} = 2^{\ell+1}.$$

Corollary 2-1: *There exists some $F_\mu(a)$ for each $F(a)$, $F(a) \in \{F(a)\}$, which satisfies*

$$F_\mu(a) \equiv F(a) \pmod 2.$$

Proof: Obvious from the definition and Corollary 1-1.

Lemma 3: $P[F(a)] \in \{F(a)\}$.

Proof: Let $a = a^*$ be simultaneous equations $a_i = a_i^*$, $i = 0, 1, \ldots, \ell$, where each a_i^* is a fixed number with value 1 or 0.

Let $F_\mu(a) \equiv F(a) \pmod 2$ for an arbitrarily given $F(a)$ from Corollary 2-1. Then, it holds for the following congruence with fixed μ:

$$F_\mu(a^*) \equiv F(a^*) \pmod 2 \text{ for any values } a^* \in a.$$

Then, the following equalities must be satisfied:

$$\begin{aligned} 1 - (-1)^{F_\mu(a^*)} &= 1 - (-1)^{F(a^*)} \\ &= [1 - (-1)][1 + (-1) + (-1)^2 + \cdots + (-1)^{F(a^*)-1}] \\ &= 2, \text{ if } F(a^*) \text{ is odd,} \\ &= 0, \text{ if } F(a^*) \text{ is even.} \end{aligned}$$

Hence,

$$2P[F(a^*)] = 1 - (-1)^{F_\mu(a^*)}.$$

Now, since $F_\mu(a)$ is congruent to such a polynomial as

$$F_\mu(a) \equiv \alpha + \alpha_0 a_0 + \alpha_1 a_1 + \cdots + \alpha_{01} a_0 a_1 + \cdots \pmod 2,$$

where

$$\alpha,\ \alpha_0\ \ldots \in \{0, 1\} \quad \text{and} \quad \alpha \equiv c,\ \alpha_0 \equiv c_0\ \ldots \pmod 2,$$

we obtain

$$\begin{aligned} (-1)^{F_\mu(a^*)} &= (-1)^{\alpha + \alpha_0 a_0^* + \alpha_1 a_1^* + \cdots} \\ &= (-1)^\alpha (-1)^{\alpha_0 a_0^*} \cdot (-1)^{\alpha_1 a_1^*} \times \cdots \\ &= (-1)^\alpha [1 - 2P(\alpha_0 a_0^*)][1 - 2P(\alpha_1 a_1^*)] \times \ldots . \end{aligned}$$

Since

$$P(\alpha_0 a_0^*) = \alpha_0 a_0^*,\ P(\alpha_1 a_1^*) = \alpha_1 a_1^*,\ \ldots,$$

then

$$(-1)^{F_\mu(a^*)} = (-1)^\alpha (1 - 2\alpha_0 a_0^*)(1 - 2\alpha_1 a_1^*) \times \ldots,$$

so that

$$2P[F(a^*)] = 1 - (-1)^\alpha (1 - 2\alpha_0 a_0^*)(1 - 2\alpha_1 a_1^*) \times \ldots .$$

If we expand the righthand side as a polynomial of a_0^*, a_1^*, ..., then we would find that every coefficient is an even number.

Hence, we obtain the result that $P[F(a^*)]$ can be described as a fixed polynomial of a^*, a^*, ..., a_ℓ^* with integral coefficients for any values a^* of a, which is nothing but the statement of the present lemma.

Corollary 3-1:

$$P[F(a)] = P[F(a)^\nu] = \{P[F(a)]\}^\rho = \tfrac{1}{2}P\{F(a) + P[F(a)]\}, \text{ for } \forall\nu,\ \rho \in Z^+.$$

Proof: Obvious.

Lemma 4: *Let* $A^{r+1}x = A(A^r x)$, *if* $A^r x \in \{F(a)\}$, *where* $r \in \{Z^+, 0\}$. *Then,*

$$A^r x \in \{F(a)\} \text{ for every } r.$$

Proof: When $r = 0$.

Obviously, $x \in \{F(a)\}$ from the definition.

When $r \geqq 1$.

Suppose $A^{r-1}x \in \{F(a)\}$ and $P(A^{r-1}x) \in \{F(a)\}$ for some r. Let $F(a) = A^{r-1}x$ for some $F(a) \in \{F(a)\}$. Then we obtain from the definition,

$$A^r x = \tfrac{1}{2}F(a) + [F(a) + \tfrac{1}{2}]P[F(a)].$$

Since $F(a) \equiv P[F(a)] \pmod 2$ for every value of a, then we obtain

$$\tfrac{1}{2}[F(a) + P\{F(a)\}] \in \{F(a)\} \quad \text{and} \quad A^r x \in \{F(a)\}.$$

By virtue of the last lemma, we also obtain

$$P(A^r x) \in \{F(a)\}.$$

Hence, we induce that if

$$A^{r-1}x \in \{F(a)\} \quad \text{and} \quad P(A^{r-1}x) \in \{F(a)\},$$

then

$$A^r x \in \{F(a)\} \quad \text{and} \quad P(A^r x) \in \{F(a)\}.$$

Consequently, by the use of mathematical induction, we can justify the statement, since it is the truth for $r = 0$.

Lemma 5: $A^{r+1}x = \tfrac{1}{2}A^r x + (A^r x + \tfrac{1}{2})P(A^r x)$, $r = 0, 1, 2, \ldots$, *where*

$$A^{r+1}x = A(A^r x).$$

Proof: Obvious from the last lemma.

Lemma 6: *Suppose that* x *and* a *have one-to-one correspondence in the way of Lemma 1. Then, there exists a function* $f_r(a) \in \{F_\mu(a)\}$ *which satisfies for any values of* x:

$$A^r x \equiv f_r(a) \pmod 2,$$

where $r \in \{Z^+, 0\}$.

Proof: Lemma 4 shows that $A^r x$ yields a polynomial of $a_0, a_1, \ldots, a_\ell$ with integral coefficients.

Since $a_i^\nu = a_i$, for $\forall i$, $\forall \nu$ from Corollary 1-1, we can normalize $A^r x$ in the following way:

$$A^r x = \beta + \beta_0 a_0 + \cdots + \beta_{01\ldots\ell} a_0 a_1 \ldots a_\ell,$$

where $\beta, \beta_0 \ldots \in Z$. Here, the number of terms reduces to 2^ℓ or less.

The equation yields a congruence, modulo 2, such that $A^r x$ is congruent to a polynomial of $a_0, a_1, \ldots, a_\ell$ with coefficients 1, which is nothing but an element of the set $\{F_\mu(a)\}$.

Lemma 7: (i) *Let* y *be some fixed number, where* $y \in \{1, 2, \ldots, (2^{\ell'} - 1)\}$, *then* $A^r y \not\equiv 0 \pmod 3$ *for* $r \geqq \ell$, *where* $\ell' = \ell + 1$.

(ii) *Let* $y \in Z^+$ *and* $y \not\equiv 0 \pmod 3$. *Then,* $A^r y \not\equiv 0 \pmod 3$ *for* $r \geq 1$.

(iii) *Let* $y_1, y_2 \in Z^+$ *and let* $y_1 \not\equiv 0 \pmod 3$ *and* $y_2 \not\equiv 0 \pmod 3$. *If* $y_1 \equiv y_2 \pmod 4$, *then* $Ay_1 \equiv Ay_2 \not\equiv 0 \pmod 6$.

Proof: (i) Suppose $A^r y$ is a multiple of 3 for some nonnegative integer r. Then, every $A^{r-1}y$, $A^{r-2}y$, ..., y must be an even number, because an odd number causes a number not divisible by 3 at the next step. Hence, $2^r \cdot 3|y$. Since $y < 2^{\ell} \cdot 3$, then $A^r y$ is not a multiple of 3 for $r \geqq \ell$, contradicting the hypothesis.

(ii) Obvious, because $3\nmid y$ does not cause $3|Ay$.

(iii) If we construct a sequence (y_1, Ay_1, A^2y_1) or (y_2, Ay_2, A^2y_2), the sequence yields one of four types, according as the increasement or decreasement of values, illustrated as follows:

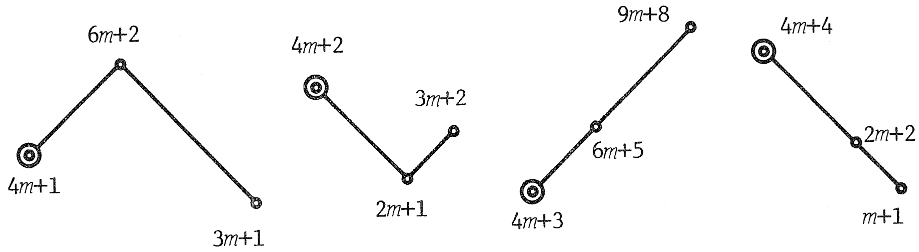


Fig.2

From the proposition, we find that (y_1, Ay_1, A^2y_1) and (y_2, Ay_2, A^2y_2) belong to a common type.

On the other hand, a sequence (y_1, Ay_1, A^2y_1) or (y_2, Ay_2, A^2y_2) can be classified about the middle element modulo 6 as follows:

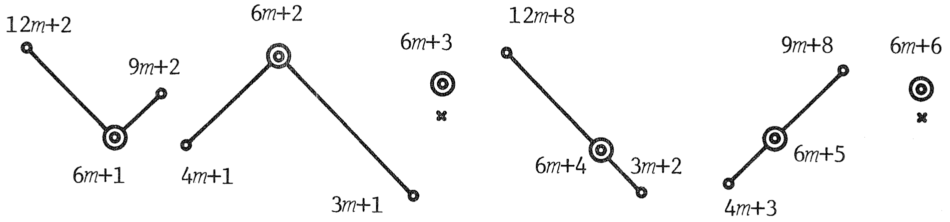


Fig.3

Since $3\nmid y_i$ and since $3\nmid Ay_i$ from (ii), where $i = 1, 2$, the types $(6m + 3)$ and $6m$ would not occur. Then, the types of Figure 2 have one-to-one correspondence with the types of Figure 3. Hence, the statement is justified.

Lemma 8: *Suppose that x and a have one-to-one correspondence in the way of Lemma 1. Suppose that $A^r x \equiv f_r(a) \pmod 2$ for some $f_r(a) \in \{F_\mu(a)\}$ at each $r \in \{0, 1, 2, ...\}$. Suppose that there exist some positive integers s and t larger than or equal to ℓ, for which $f_s(a) = f_t(a)$. Then,*

$$A^s x = A^t x \text{ for every value of } x.$$

Proof: Let $x_s = A^s x|_{x=x_0}$ and $x_t = A^t x|_{x=x_0}$ for some fixed value x_0 in the range of x and let $a_0^*, a_1^*, \ldots, a_\ell^*$ or a^*, for short, have a one-to-one correspondence with x_0, as in Lemma 1. Suppose $x_s \neq x_t$, for a while, and let $x_s < x_t$. We obtain, from the propositions,

$$x_s = f_s(a^*) + (\text{an even number}),$$
$$x_t = f_t(a^*) + (\text{an odd number}),$$

which reduce to

$$x_s = f(a^*) + 2S,$$
$$x_t = f(a^*) + 2T,$$

where $f(a^*) = f_s(a^*) = f_t(a^*)$ and $S < T$. That is, $x_s \equiv x_t \pmod 2$. Moreover, since $s, t \geqq \ell$, we find $3 \nmid x_s$ and $3 \nmid x_t$ from the last lemma.

First, let us deal with $2A^s x$ and $2A^t x$. Since $A^s x, A^t x \in \{F(a)\}$, then $2A^s x, 2A^t x \in \{F(a)\}$; besides $P(2A^s x) = P(2A^t x) = 0$. Therefore, $A(2A^s x)$ and $A(2A^t x)$ can be defined. Since

$$A(2A^s x)|_{x=x_0} = A(2x_s) = x_s$$

as well as

$$A(2A^t x)|_{x=x} = A(2x_t) = x_t,$$

and since $2x_s \equiv 2x_t \pmod 4$ with $3 \nmid x_s x_t$, we obtain, from the last lemma,

$$A(2x_s) \equiv A(2x_t) \pmod 6, \text{ so that } x_s \equiv x_t \pmod 3.$$

That is, $S \equiv T \pmod 3$.

Now let us again deal with $A^s x$ and $A^t x$. Let $y_1 = \frac{1}{3}(2x_s + x_t)$. Then.

$$y_1 = f(a^*) + 2S + \tfrac{2}{3}(T - S).$$

Hence, y_1 is an integer with $P(y_1) = P[f(a^*)]$, and $x_s < y_1 < x_t$.

Let $y_2 = \frac{1}{3}(x_s + 2x_t)$. Then, we obtain analogously

$$y_2 = f(a^*) + 2T + \tfrac{2}{3}(S - T) \text{ and } y_2 \in Z^+,\ P(y_2) = P[f(a^*)],\ x_s < y_2 < x_t.$$

(i) When $y_1 \not\equiv y_2 \pmod 3$:

There exists y_1 or y_2 not a multiple of 3, so that at least one of Ay_1 and Ay_2 is not divisible by 3.

(ii) When $y_1 \equiv y_2 \pmod 3$:

Then,

$$2S + \tfrac{2}{3}(T - S) \equiv 2T + \tfrac{2}{3}(S - T) \pmod 3,$$

which reduces to $T \equiv S \pmod 9$.

On the other hand, we can calculate as follows:

$$Ay_1 - Ax_s = \tfrac{1}{3}(T - S)\{1 - 2P[f(a^*)]\}.$$

Thus, $Ay_1 \equiv Ax_s \pmod 3$. Since Ax_s is not divisible by 3 for $3 \nmid x_s$, then

$$Ay_1 \not\equiv 0 \pmod 3.$$

Consequently, we can always find a number y_i, $i = 1$ or 2, which satisfies

$$\begin{cases} y_i = f(a^*) + (\text{an even number}), \\ x_s < y_i < x_t \text{ and} \\ Ay_i \not\equiv 0 \pmod 3. \end{cases}$$

Next let us replace a pair (x_s, x_t) with another pair (x_s, y_i) and repeat the calculations above. Then, we would obtain, analogously, some number y_i' which satisfies

$$\begin{cases} y_i' = f(a^*) + (\text{an even number}), \\ Ay_i' \not\equiv 0 \pmod 3, \text{ and} \\ x_s < y_i' < y_i. \end{cases}$$

Since this procedure can be continued infinitely, we obtain an infinite sequence of numbers y_i, y_i', y_i'', ..., which satisfies

$$x_s < \cdots < y_i'' < y_i' < y_i < x_t.$$

It is impossible in reality, because all of y_i, y_i', ..., are integers. Hence, we must conclude that $x_s = x_t$, contradicting the hypothesis in this proof.

Theorem 1: *An infinite sequence, $S:(x_0, x_1, x_2, \ldots)$, $\forall x_0 \in Z^+$, $x_r = A^r x_0$, is a recursive sequence.*

Proof: Lemmas 6 and 2 show that an upper limit of the number of the distinct $f_r(a)$'s is the total number of elements of the finite set $\{F_\mu(a)\}$ like 2^K. That is, the number of the distinct $f_r(a)$'s is finite.

On the other hand, since a sequence $(x_0, x_1, \ldots)$ is infinite, there exists at least one pair (x_s, x_t) which satisfies $f_s(a) = f_t(a)$ along with $s, t \geqq \ell$. For that reason, we obtain from the preceding lemmas

$$x_s = x_t.$$

Then, $x_{s+1} = x_{t+1}$, $x_{s+2} = x_{t+2}$, ..., so that the sequence is recursive. In addition, the length of a recursive segment is limited within the number of the distinct $f_r(a)$'s, like 2^K.

[NOTE: This theorem may be extended to the case of $x_0 \in Z^-$, by slight modifications.]

5. PROOF ABOUT THE LENGTH OF A PERIOD

Lemma 9: *Suppose that $S:(x_0, x_1, \ldots, x_{s+1}, \ldots, x_t, \ldots)$, where*

$$x_r = A^r x|_{x=x_0} \text{ for } x_0 \in \{1, 2, \ldots, 2^{\ell+1} - 1\}$$

is an infinite sequence with recursive segment $S_p:(x_{s+1}, \ldots, x_t)$.

(i) *Let M_j, $j \in \{1, 2, 3, 4\}$ be the total number of elements in an S_p with value congruent to j modulo 4. Then, $M_1 = M_2$.*

(ii) *Let N_k, $k \in \{1, 2, \ldots, 12\}$ be the total number of elements in an S_p with value congruent to k modulo 12. Then,*

$$N_1 = N_2 \text{ and } N_3 = N_5 = N_6 = N_7 = N_8 = N_9 = N_{10} = N_{12} = 0.$$

Proof: (i) If we construct sequences U_3's$(x_r, Ax|_{x=x_r}, A^2x|_{x=x_r})$ for each element x_r of an S_p, the number of U_3's is equal to the total number of elements of an S_p, that is, $M_1 + M_2 + M_3 + M_4$. Besides, every U_3 is a subsequence of S. As we saw in Lemma 7, U_3's are classified into four-types like Figure 2. It is easily recognized that the number of each type coincides with M_1, M_2, M_3, and M_4, respectively.

On the other hand, concerning the middle elements, U_3's can be classified into six-types modulo 6 as illustrated in Figure 3. In this place, we should like to omit $6m + 3$ and $6m$, since these would not appear as a recursive element. Then, we can also recognize that the number of each type coincides with M_2, M_1, 0, M_4, M_3, and 0, respectively.

Hence, we obtain the following contrast.

M_1: total number of type $(4m + 1)$ = total number of type $(6m + 2)$,
M_2: total number of type $(4m + 2)$ = total number of type $(6m + 1)$,
M_3: total number of type $(4m + 3)$ = total number of type $(6m + 5)$,
M_4: total number of type $(4m + 4)$ = total number of type $(6m + 4)$.

Then, we can calculate the total number of the odd types in two ways: one is based on the types modulo 4 and the other is based on the types modulo 6. The result is $M_1 + M_3 = M_2 + M_3$. Hence, $M_1 = M_2$.

(ii) Let us subdivide the types of the above table modulo 12. For instance, the type $(4m+1)$ is subdivided into the types $(12m + 1)$, $(12m + 5)$, and $(12m + 9)$. Then, we can reconstruct the above table as follows:

$$M_1:\ \left.\begin{array}{r}\text{total number of types}\\(12m+1)\\(12m+5)\\(12m+9)\end{array}\right\}=\left\{\begin{array}{r}\text{total number of types}\\(12m+2)\\(12m+8)\\ \end{array}\right.$$

$$M_2:\ \left.\begin{array}{r}\text{total number of types}\\(12m+2)\\(12m+6)\\(12m+10)\end{array}\right\}=\left\{\begin{array}{r}\text{total number of types}\\(12m+1)\\(12m+7)\\ \end{array}\right.$$

$$M_3:\ \left.\begin{array}{r}\text{total number of types}\\(12m+3)\\(12m+7)\\(12m+11)\end{array}\right\}=\left\{\begin{array}{r}\text{total number of types}\\(12m+5)\\(12m+11)\\ \end{array}\right.$$

$$M_4:\ \left.\begin{array}{r}\text{total number of types}\\(12m+4)\\(12m+8)\\(12m+12)\end{array}\right\}=\left\{\begin{array}{r}\text{total number of types}\\(12m+4)\\(12m+10)\\ \end{array}\right.$$

If we omit the types with a multiple of 3 for the reason stated, and calculate in two ways, we obtain the following relations:

$$M_1 = N_1 + N_5 = N_2 + N_8,\ M_2 = N_2 + N_{10} = N_1 + N_7,$$
$$M_3 = N_{11} = N_5 + N_{11},\ M_4 = N_4 + N_8 = N_4 + N_{10}.$$

Besides, we obtain, from (i),

$$M_1 = M_2.$$

Then, they reduce to the following relations:

$$N_1 = N_2,\ N_3 = N_5 = N_6 = N_7 = N_8 = N_9 = N_{10} = N_{12} = 0.$$

Lemma 10: *Suppose that*

$$S:(x_0,\ x_1,\ \ldots),\ x_0 \in \{1,\ 2,\ \ldots,\ (2^{\ell+1} - 1)\},\ x_r = A^r x|_{x=x_0}$$

is an infinite sequence with recursive segment $S_p:(x_{s+1}, \ldots, x_t)$. *Let* p *be the length of an irreducible* S_p. *Then* $p \neq 1,\ 3,\ 4$.

Proof: Since each element of S_p shows the value increasing or decreasing, according as the preceder is odd or even, then possible S_p must necessarily involve an odd element as well as an even element.

Now, let us assume, without loss of generality, that the first element of S_p is an odd number. Here $p \neq 1$, for if not, a segment would cause the value to increase. Hence, the cases to be examined are those for $p = 3$ and $p = 4$.

Let $x_{s+1} = 2R + 1$. Since $x_{s+1} \in Z^+$, then $R \in \{Z^+, 0\}$. Moreover, we obtain $x_{s+2} = 3R + 2$.

(i) When $p = 3$:

The cases examined are classified into four types according to the parities of x_{s+2} and x_{s+3}. Then, we can calculate x_{s+4} as a function of R.

Since $x_{s+1} = x_{s+4}$ and $R \varepsilon \{Z^+, 0\}$ must be simultaneously satisfied, we have a criterion for the existence of a recursive segment.

The result is as follows:

x_{s+2}	x_{s+3}	x_{s+4}	$x_{s+1} = x_{s+4}$	$R \varepsilon \{Z^+, 0\}$?
odd	odd	$(27R + 23)/4$	$19R + 22 = 0$	no
odd	even	$(9R + 7)/4$	$R + 3 = 0$	no
even	odd	$(9R + 8)/4$	$R + 4 = 0$	no
even	even	$(3R + 2)/4$	$5R + 2 = 0$	no

Hence, any recursive segment with length 3 does not exist.

(ii) When $p = 4$:

Analogously, we examine the simultaneous compliance of

$$x_{s+1} = x_{s+4} \neq x_{s+2} \quad \text{and} \quad R \varepsilon \{Z^+, 0\}.$$

x_{s+2}	x_{s+3}	x_{s+4}	x_{s+5}	$x_{s+1} = x_{s+5}$	$R \varepsilon \{Z^+, 0\}$?
odd	odd	odd	$(81R + 73)/8$	$R + 1 = 0$	no
odd	odd	even	$(27R + 23)/8$	$11R + 15 = 0$	no
odd	even	odd	$(27R + 25)/8$	$11R + 17 = 0$	no
even	odd	odd	$(27R + 28)/8$	$11R + 20 = 0$	no
odd	even	even	$(9R + 7)/8$	$7R + 1 = 0$	no
*even	odd	even	$(9R + 8)/8$	$R = 0$	yes
even	even	odd	$(9R + 10)/8$	$7R = 2$	no
even	even	even	$(3R + 2)/8$	$13R + 6 = 0$	no

In the above table, the asterisk marks the case of $x_{s+3} = \frac{1}{2}(3R+2)$. Since $x_{s+1} \neq x_{s+3}$ is required for an irreducible segment, then $R \neq 0$, which contradicts $x_{s+1} = x_{s+5}$.

After all, there exists no irreducible S_p with $p = 4$.

Theorem 2: *Suppose that*

$$S:(x_0, x_1, \ldots), \; x_0 \; \varepsilon \; \{1, 2, \ldots, (2^{\ell+1} - 1)\}, \; x_r = A^r x|_{x=x_0}$$

is a recursive sequence. Then, an irreducible segment of recursion, S_p *is* (1, 2) *or* (2, 1).

Proof: Since p, the length of an S_p, is not equal to 1, 3 or 4, as we saw, then the bases to be examined are limited to those of $p \geqq 5$ and $p = 2$.

(i) When $p \geqq 5$:

If we construct sequences U_4's:$(x_r, Ax|_{x=x_r}, A^2x|_{x=x_r}, A^3x|_{x=x_r})$ for each element x_r of an S_p, the number of U_4's is equal to the total number of elements of an S_p. Besides, every U_4 is a subsequence of S. As in Lemma 8, U_4's can be classified into 12-types about the second elements modulo 12 as follows.

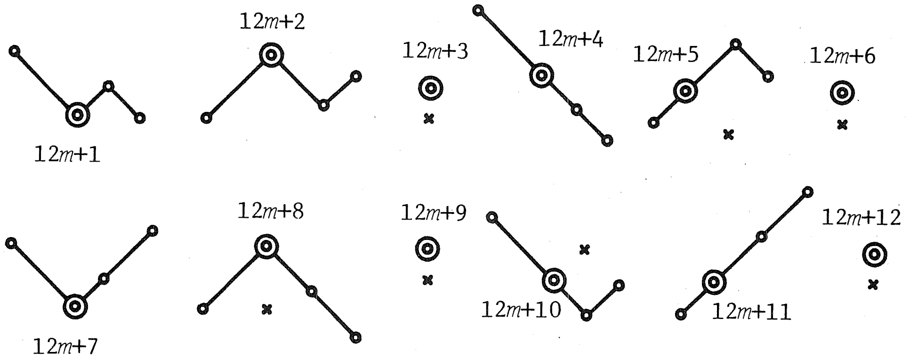


Fig.4

Since each number of type $(12m + k)$, $k \in \{1, 2, \ldots, 12\}$ coincides to the N_k stated in Lemma 8, the types $(12m + k)$, $k = 3, 5, 6, 7, 8, 9, 10, 12$ do not exist, in reality.

Now, let us construct U_5's:$(x_r, Ax|_{x=x_r}, \ldots, A^4x|_{x=x_r})$. Since every U_4 is a subsequence of S and since $p \geqq 5$, then any U_5 involves at least one combination of two U_4's such that the second, third, and fourth elements of the first U_4 overlap to the first, second, and third elements of the second U_4, respectively.

Hence, we obtain the possible combinations:

$$N_1 \to N_2;\ N_2 \to N_1;\ N_4 \to N_4;\ N_{11} \to N_{11}.$$

Since each of the latter two would not cause a recursive segment, the former two only may exist. Consequently, successive elements of S_p show the alternative increasing or decreasing of values, if it exists. In general, however, a sequence like (odd, even, odd, even, odd, ...) causes a decrease of value in the global sense, except the sequence (1, 2, 1, 2, 1, ...).

Hence, it is impossible to construct S_p with $p \geqq 5$.

(ii) When $p = 2$:

Obviously, the only S_p:(1, 2) exists, if the first element is odd.

Theorem 3: There exists an infinite sequence $(x_0, x_1, \ldots)$ generated by a recursion formula:

$$x_{r+1} = \tfrac{1}{2}(3x_r + 1),\ \textit{if } x_r \textit{ is odd};\ x_{r+1.} = \tfrac{1}{2}x_r,\ \textit{if } x_r \textit{ is even},$$

where x_0 is arbitrarily given in Z^+.

This sequence necessarily has an element with value 1 in a finite position less than or equal to $M = 2^K + \ell$, $K = 2^{\ell+1}$ from the top of the sequence, where $K > x_0$.

Proof: Obvious from Theorems 1 and 2.

Complement: An infinite sequence $(x_0, x_1, \ldots)$ with the recursion formula like Theorem 3 starting from an arbitrary x_0 in Z^- is a recursive sequence.

Proof: Left to the reader.

6. CONCLUSION

We have proven a number-theoretical problem about a sequence, which is a computer-oriented type, but cannot be solved by any computer approach.

REFERENCE

1. J. Nievergelt, J. C. Farrar, & E. M. Reingold. *Computer Approaches to Mathematical Problems.* New Jersey: Prentice-Hall, 1074. Ch. 5.3.3.

*****

WEIGHTED STIRLING NUMBERS OF THE FIRST AND SECOND KIND—II

L. CARLITZ
Duke University, Durham, NC 27706

1. INTRODUCTION

The Stirling numbers of the first and second kind can be defined by

$$(1.1)\qquad (x)_n \equiv x(x+1)\cdots(x+n-1) = \sum_{k=0}^{n} S_1(n, k)x^k,$$

and

$$(1.2)\qquad x^n = \sum_{k=0}^{n} S(n, k)x\cdot(x-1)\cdots(x-k+1),$$

respectively. In [6], the writer has defined *weighted* Stirling numbers of the first and second kind, $\overline{S}_1(n, k, \lambda)$ and $\overline{S}(n, k, \lambda)$, by making use of certain combinatorial properties of $S_1(n, k)$ and $S(n, k)$. Numerous properties of the generalized quantities were obtained.

The results are somewhat simpler for the related functions:

$$(1.3)\qquad \begin{cases} R_1(n, k, \lambda) = \overline{S}_1(n, k+1, \lambda) + S_1(n, k) \\ R(n, k, \lambda) = \overline{S}(n, k+1, \lambda) + S(n, k). \end{cases}$$

In particular, the latter satisfy the recurrences,

$$(1.4)\qquad \begin{cases} R_1(n, k, \lambda) = R_1(n, k-1, \lambda) + (n+\lambda)R_1(n, k, \lambda) \\ R(n, k, \lambda) = R(n, k-1, \lambda) + (k+\lambda)R(n, k, \lambda), \end{cases}$$

and the orthogonality relations

$$(1.5)\qquad \begin{aligned} &\sum_{j=0}^{n} R(n, j, \lambda)\cdot(-1)^{j-k}R_1(j, k, \lambda) \\ &\quad = \sum_{j=0}^{n} (-1)^{n-j}R_1(n, j, \lambda)R(j, k, \lambda) = \begin{cases} 1 & (n = k) \\ 0 & (n \neq k). \end{cases} \end{aligned}$$

We have also the generating functions

$$(1.6)\qquad \sum_{n=0}^{\infty} \frac{x^n}{n!} \sum_{k=0}^{n} R_1(n, k, \lambda)y^k = (1-x)^{-\lambda-y},$$

$$\sum_{n=0}^{\infty} \frac{x^n}{n!} \sum_{k=0}^{n} R(n,\ k,\ \lambda) y^k = e^{\lambda x} \exp\{y(e^x - 1)\}, \tag{1.7}$$

and the explicit formula

$$R(n,\ k,\ \lambda) = \frac{1}{k!} \sum_{j=0}^{k} (-1)^{k-j} \binom{k}{j} (j + \lambda)^n. \tag{1.8}$$

Moreover, corresponding to (1.1) and (1.2), we have

$$(\lambda + y)^n = \sum_{k=0}^{n} R_1(n,\ k,\ \lambda) y^k \tag{1.9}$$

and

$$y^n = \sum_{k=0}^{n} (-1)^{n-k} R(n,\ k,\ \lambda)(y + \lambda)_k. \tag{1.10}$$

It is well known that the numbers $S_1(n,\ n-k)$, $S(n,\ n-k)$ are polynomials in n of degree $2k$. In [4] it is proved that

$$\left\{ \begin{aligned} S_1(n,\ n-k) &= \sum_{j=1}^{k} B_1(k,\ j) \binom{n+j-1}{2k} \\ S(n,\ n-k) &= \sum_{j=1}^{n} B(k,\ j) \binom{n+j-1}{2k} \end{aligned} \right. \quad (k \geq 1), \tag{1.11}$$

where $B_1(k,\ j)$, $B(k,\ j)$ are independent of n, and

$$B_1(k,\ j) = B(k,\ k - j + 1), \quad (1 \leq j \leq k). \tag{1.12}$$

The representations (1.11) are applied in [4] to give new proofs of the known relations

$$\left\{ \begin{aligned} S(n,\ n-k) &= \sum_{t=0}^{k} \binom{k+n}{k-t} \binom{k-n}{k+t} S_1(k+t,\ t) \\ S_1(n,\ n-k) &= \sum_{t=0}^{k} \binom{k+n}{k-t} \binom{k-n}{k+t} S(k+t,\ t). \end{aligned} \right. \tag{1.13}$$

For references to (1.13), see [2], [7].

One of the principal objectives of the present paper is to generalize (1.11). The generalized functions $R_1(n,\ n-k,\ \lambda)$, $R(n,\ n-k,\ \lambda)$ are also polynomials in n of degree $2k$. We show that

$$\left\{ \begin{aligned} R_1(n,\ n-k,\ \lambda) &= \sum_{j=0}^{k} B_1(k,\ j,\ \lambda) \binom{n+j}{2k} \\ R(n,\ n-k,\ \lambda) &= \sum_{j=0}^{k} B(k,\ j,\ \lambda) \binom{n+j}{2k} \end{aligned} \right. \tag{1.14}$$

where $B_1(k,\ j,\ \lambda)$, $B(k,\ j,\ \lambda)$ are independent of n, and

$$B_1(k,\ j,\ \lambda) = B(k,\ k-j,\ 1-\lambda), \quad (0 \leq j \leq k). \tag{1.15}$$

As an application of (1.14) and (1.15), it is proved that

$$(1.16)\quad \begin{cases} R(n,\ n-k,\ \lambda) = \displaystyle\sum_{t=0}^{k} \binom{k+n+1}{k-t}\binom{k-n-1}{k+t} R_1(k+t,\ t,\ 1-\lambda) \\ R_1(n,\ n-k,\ \lambda) = \displaystyle\sum_{t=0}^{k} \binom{k+n+1}{k-t}\binom{k-n-1}{k+t} R(k+t,\ t,\ 1-\lambda). \end{cases}$$

For $\lambda = 1$, (1.16) reduces to (1.13) with n replaced by $n + 1$; for $\lambda = 0$, we apparently get new results.

In the next place, we show that

$$(1.17)\quad \begin{cases} R(n,\ n-k,\ \lambda) = \dbinom{n}{k} B_k^{(-n+k)}(\lambda) \\ R(n,\ n-k,\ \lambda) = \dbinom{k-n-1}{k} B_k^{(n+1)}(1-\lambda), \end{cases}$$

where $B_k^{(k)}(\lambda)$ is the Bernoulli polynomial of higher order defined by [8, Ch. 6]:

$$\sum_{n=0}^{\infty} B_k^{(k)}(\lambda)\frac{u^k}{k!} = \left(\frac{u}{e^u - 1}\right)^z e^{\lambda u}.$$

We remark that (1.17) can be used to give a simple proof of (1.16). For the special case of Stirling numbers, see [2].

It is easily verified that, for $\lambda = 0$ and 1, (1.17) reduces to well-known representations [8, Ch. 6] of $S(n,\ n-k)$ and $S_1(n,\ n-k)$.

In view of the formulas (for notation and references see [3]),

$$(1.18)\quad \begin{cases} S(n,\ n-k) = \displaystyle\sum_{j=0}^{k-1} S'(k,\ j)\binom{n}{2k-j} \\ S_1(n,\ n-k) = \displaystyle\sum_{j=0}^{k} S'(k,\ j)\binom{n}{2k-j}, \end{cases}$$

it is of interest to define coefficients $R'(k, j, \lambda)$ and $R_1'(k, j, \lambda)$ by means of

$$(1.19)\quad \begin{cases} R(n,\ n-k,\ \lambda) = \displaystyle\sum_{j=0}^{\lambda} R'(k,\ j,\ \lambda)\binom{n}{2k-j} \\ R_1(n,\ n-k,\ \lambda) = \displaystyle\sum_{j=0}^{\lambda} R_1'(k,\ j,\ \lambda)\binom{n}{2k-j}. \end{cases}$$

Each coefficient is a polynomial in λ of degree $2k$ and has properties generalizing those of $S'(k,\ j)$ and $S_1'(k,\ j)$.

Finally (§9), we derive a number of relations similar to (1.16), connecting the various functions defined above. For example, we have

$$(1.20)\quad \begin{cases} R_1(n,\ n-k,\ \lambda) = \displaystyle\sum_{j=0}^{k} (-1)^{k-j}\binom{n+j}{k+j} R'(k,\ k-j,\ 1-\lambda) \\ R(n,\ n-k,\ \lambda) = \displaystyle\sum_{j=0}^{k} (-1)^{k-j}\binom{n+j}{k+j} R_1'(k,\ k-j,\ 1-\lambda) \end{cases}$$

and

$$(1.21)\qquad \begin{cases} R_1'(n, k, \lambda) = \sum_{t=0}^{k} (-1)^t \binom{n-t}{k-t} R'(n, t, 1-\lambda) \\ R'(n, k, \lambda) = \sum_{t=0}^{k} (-1)^t \binom{n-t}{k-t} R_1'(n, t, 1-\lambda). \end{cases}$$

In the proofs, we make use of the relations (1.15).

2. REPRESENTATIONS OF $R(n, n - k, \lambda)$

As a special case of a more general result proved in [5], if $f(x)$ is an arbitrary polynomial of degree $\leq m$, then there is a *unique* representation in the form

$$(2.1)\qquad f(x) = \sum_{j=0}^{m-1} a_j \binom{x+j}{m},$$

where the a are independent of x. Thus, since $R(n, n - k, \lambda)$ is a polynomial in n of degree $2k$, we may put, for $k \geq 1$,

$$(2.2)\qquad R(n, n-k, \lambda) = \sum_{j=0}^{2k} B(k, j, \lambda) \binom{n+j}{2k},$$

where the coefficients $B(k, j, \lambda)$ are independent of n.

By (1.4), we have, for $k > 1$,

$$(2.3)\qquad R(n+1, n-k+1, \lambda) = (n-k+1+\lambda)R(n, n-k+1, \lambda) + R(n, n-k, \lambda).$$

Thus, (2.2) yields

$$\sum_{j=0}^{2k} B(k, j, \lambda)\binom{n+j}{2k-1} = (n-k+1+\lambda)\sum_{j=0}^{2k-2} B(k-1, j, \lambda)\binom{n+j}{2k-2}.$$

Since

$$n - k + 1 + \lambda = (n + j - 2k + 2) + (k - j - 1 + \lambda),$$

we get

$$\sum_j B(k, j, \lambda)\binom{n+j}{2k-1} = \sum_j (2k-1)B(k-1, j, \lambda)\binom{n+j}{2k-1} + \sum_j (k-j-1+\lambda)B(k-1, j, \lambda)\left\{\binom{n+j+1}{2k-1}\binom{n+j}{2k-1}\right\}.$$

It follows that

$$(2.4)\qquad B(k, j, \lambda) = (k+j-\lambda)B(k-1, j, \lambda) + (k-j+\lambda)B(k-1, j-1, \lambda).$$

We shall now compute the first few values of $B(k, j, \lambda)$. To begin with we have the following values of $R(n, n - k, \lambda)$. Clearly, $R(n, n, \lambda) = 1$. Then, by (2.3), with $k = 1$, we have

$$R(n+1, n, \lambda) - R(n, n-1, \lambda) = n + \lambda.$$

It follows that

$$(2.5)\qquad R(n, n-1, \lambda) = \binom{n}{2} + n\lambda.$$

Next, taking $k = 2$ in (2.3),

$$R(n + 1, n - 1, \lambda) - R(n, n - 2, \lambda) = (n - 1 + \lambda)R(n, n - 1, \lambda),$$

we find that

$$R(n, n - 2, \lambda) = 3\binom{n}{4} + \binom{n}{3} + 3\binom{n}{3}\lambda + \binom{n}{2}\lambda^2, \quad (n \geq 2). \tag{2.6}$$

A little computation gives the following table of values:

$B(k, j, \lambda)$

j k	0	1	2	3
0	1			
1	$1 - \lambda$	λ		
2	$(1 - \lambda)_2$	$1 + 3\lambda - 2\lambda^2$	λ^2	
3	$(1 - \lambda)_3$	$8 + 7\lambda - 12\lambda^2 + 3\lambda^3$	$1 + 4\lambda + 6\lambda^2 - 3\lambda^3$	λ^3

The last line was computed by using the recurrence (2.4).

Note that the sum of the entries in each row above is independent of λ. This is in fact true generally. By (2.2), this is equivalent to saying that the coefficient of the highest power of λ in $R(n, n - k, \lambda)$ is independent of λ. To prove this, put

$$R(n, n - k, \lambda) = a\, n^{2k} + a'n^{2k-1} + \cdots .$$

Then

$$\begin{aligned} R(n + 1, n - k + 1, \lambda) - R(n, n - k, \lambda) &= a_k((n + 1)^{2k} - n^{2k}) + a_k'((n + 1)^{2k-1} - n^{2k-1}) + \cdots \\ &= 2ka_k n^{2k-1} + \cdots . \end{aligned}$$

Thus, by (2.3), $2ka_k = a_{k-1}$. Since $a_1 = \frac{1}{2}$, we get

$$a_k = \frac{1}{2k(2k - 2) \ldots 2} = \frac{1}{2^k k!} .$$

Therefore,

$$\sum_{j=0}^{k} B(k, j, \lambda) = \frac{(2k)!}{2^k k!} = 1.3.5 \ldots (2k - 1). \tag{2.7}$$

This can also be proved by induction using (2.4).

However, the significant result implied by the table together with the recurrence (2.4) is that

$$B(k, j, \lambda) = 0, \quad (j > k). \tag{2.8}$$

Hence, (2.2) reduces to

$$R(n, n - k, \lambda) = \sum_{j=0}^{k} B(k, j, \lambda)\binom{n + j}{2k}. \tag{2.9}$$

It follows from (2.9) that the *polynomial* $R(n, n - k, \lambda)$ vanishes for $0 \leq n < k$.

Incidentally, we have anticipated (2.9) in the upper limit of summation in (2.7).

3. REPRESENTATION OF $R_1(n, n - k, \lambda)$

Since $R_1(n, n - k, \lambda)$ is a polynomial in n of degree $2k$, we may put, for $k \geq 1$,

$$R_1(n, n - k, \lambda) = \sum_{j=0}^{2k} B_1(k, j, \lambda)\binom{n + j}{2k}, \tag{3.1}$$

where $B_1(k, j, \lambda)$ is independent of n.

By (1.4) we have, for $k > 1$,

$$R_1(n+1, n-k+1, \lambda) = (n+\lambda)R_1(n, n-k+1, \lambda) + R_1(n, n-k, \lambda). \tag{3.2}$$

Thus, by (3.1), we get

$$\begin{aligned}\sum_{j=0}^{2k} B_1(k, j, \lambda)\binom{n+j}{2k - 1} &= (n + \lambda)\sum_{j=0}^{2k-2} B_1(k - 1, j, \lambda)\binom{n+j}{2k - 2}\\ &= \sum_j (2k - 1)B_1(k - 1, j, \lambda)\binom{n + j}{2k - 1}\\ &+ \sum_j (2k - j - 2 + \lambda)B_1(k - 1, j, \lambda)\left\{\binom{n + j + 1}{2k - 1} - \binom{n + j}{2k - 1}\right\}.\end{aligned}$$

It follows that

$$\begin{aligned}B_1(k, j, \lambda) = (j + 1 - \lambda)&B_1(k - 1, j, \lambda)\\ &+ (2k - j - 1 + \lambda)B_1(k - 1, j - 1, \lambda).\end{aligned} \tag{3.3}$$

As in the previous section, we shall compute the first few values of $B_1(k, j, \lambda)$.

To begin with, we have $R_1(n, n, \lambda) = 1$. Then by (3.2), with $k = 1$, we have

$$R_1(n + 1, n, \lambda) - R_1(n, n - 1, \lambda) = n + \lambda,$$

so that

$$R_1(n, n - 1, \lambda) = \binom{n}{2} + n. \tag{3.4}$$

Next, taking $k = 2$ in (3.2),

$$R_1(n + 1, n - 1, \lambda) - R_1(n, n - 2, \lambda) = (n + \lambda)R_1(n, n - 1, \lambda).$$

It follows that

$$R_1(n, n - 2, \lambda) = 3\binom{n}{4} + 2\binom{n}{3} + \left\{3\binom{n}{3} + \binom{n}{2}\right\}\lambda + \binom{n}{2}\lambda^2, \quad (n \geq 2). \tag{3.5}$$

A little computation gives the following table of values:

$B_1(k,\ j,\ \lambda)$

$k \backslash j$	0	1	2	3
0	1			
1	$1 - \lambda$	λ		
2	$(1 - \lambda)^2$	$2 + \lambda - 2\lambda^2$	$(\lambda)_2$	
3	$(1 - \lambda)^3$	$8 - 7\lambda - 3\lambda^2 + 3\lambda^3$	$6 + 8\lambda - 3\lambda^2 - 3\lambda^3$	$(\lambda)_3$

Exactly as above, we find that

$$\sum_{j=0}^{k} B_1(k,\ j,\ \lambda) = \frac{(2k)!}{2^k k!} = 1.3.4\ \ldots\ (2k - 1). \tag{3.6}$$

This can also be proved by induction using (3.3). Moreover,

$$B_1(k,\ j,\ \lambda) = 0, \qquad (j > k), \tag{3.7}$$

so that (3.1) becomes

$$R_1(n,\ n - k,\ \lambda) = \sum_{j=0}^{k} B_1(k,\ j,\ \lambda)\binom{n + j}{2k}. \tag{3.8}$$

Thus, the *polynomial* $R_1(n,\ n - k,\ \lambda)$ vanishes for $0 \le n < k$.

4. RELATION OF $B_1(k,\ j,\ \lambda)$ TO $B(k,\ j,\ \lambda)$

In (2.4) replace j by $k - j$ and we get

$$\begin{aligned} B(k,\ k - j,\ \lambda) &= (2k - j - \lambda)B(k - 1,\ k - j,\ \lambda) \\ &\quad + (j + \lambda)B(k - 1,\ k - j - 1,\ \lambda). \end{aligned} \tag{4.1}$$

Put

$$\overline{B}(k,\ j,\ \lambda) = B(k - j,\ \lambda).$$

Then (4.1) becomes

$$\begin{aligned} \overline{B}(k,\ j,\ \lambda) &= (2k - j - \lambda)\overline{B}(k - 1,\ j - 1,\ \lambda) \\ &\quad + (j + \lambda)\overline{B}(k - 1,\ j,\ \lambda). \end{aligned} \tag{4.2}$$

Comparison of (4.2) with (3.3) gives

$$B_1(k,\ j,\ \lambda) = \overline{B}(k,\ j,\ 1 - \lambda),$$

and therefore

$$B_1(k,\ j,\ \lambda) = B(k,\ k - j,\ 1 - \lambda). \tag{4.3}$$

In particular,

$$\begin{cases} B_1(k,\ 0,\ \lambda) = B(k,\ k,\ 1 - \lambda) = (1 - \lambda)^k \\ B_1(k,\ k,\ \lambda) = B(k,\ 0,\ 1 - \lambda) = (\lambda)_k. \end{cases} \tag{4.4}$$

We recall that

$$R(n,\ k,\ 0) = S(n,\ k),\ R(n,\ k,\ 1) = S(n + 1,\ k + 1) \tag{4.5}$$

and

(4.6) $R_1(n, k, 0) = S_1(n, k),\ R_1(n, k, 1) = S_1(n + 1, k + 1).$

In (2.9), take $\lambda = 0$. Then, by (1.11) and (4.5) with k replaced by $n - k$,

$$\sum_{j=0}^{k} B(k, j, 0)\binom{n + j}{2k} = \sum_{j=1}^{k} B(k, j)\binom{n + j - 1}{2k}.$$

It follows that

(4.7) $B(k, j, 0) = B(k, j + 1), \quad (0 \le j < k);\ B(k, k, 0) = 0.$

Similarly, taking $\lambda = 1$ in (2.9), we get

$$\sum_{j=0}^{k} B(k, j, 1)\binom{n + j}{2k} = \sum_{j=1}^{k} B(k, j)\binom{n + j}{2k}.$$

Thus

(4.8) $B(k, j, 1) = B(k, j), \quad (1 \le j \le k);\ B(k, 0, 1) = 0.$

Next, take $\lambda = 0$ in (3.8), and we get

$$\sum_{j=0}^{k} B_1(k, j, 0)\binom{n + j}{2k} = \sum_{j=1}^{k} B(k, j)\binom{n + j - 1}{2k}.$$

This gives

(4.9) $B_1(k, j, 0) = B_1(k, j + 1), \quad (0 \le j < k);\ B_1(k, k, 0) = 0.$

Similarly, we find that

(4.10) $B_1(k, j, 1) = B_1(k, j), \quad (1 \le j \le k);\ B_1(k, 0, 1) = 0.$

It is easily verified that (4.9) and (4.10) are in agreement with (4.4). Moreover, for $\lambda = 0$, (4.3) reduces to

$$B_1(k, j, 0) = B(k, k - j, 1);$$

by (4.8) and (4.9), this becomes

$$B_1(k, j + 1) = B(k, k - j),$$

which is correct. For $\lambda = 1$, (4.3) reduces to

$$B_1(k, j, 1) = B(k, k - j, 0);$$

by (4.7) and (4.10), this becomes

$$B_1(k, j) = B(k, k - j + 1)$$

as expected.

5. THE COEFFICIENTS $B(k, j, \lambda);\ B_1(k, j, \lambda)$

It is evident from the recurrences (2.4) and (3.3) that $B(k, j, \lambda)$ and $B_1(k, j, \lambda)$ are polynomials of degree $\le k$ in λ with integral coefficients. Moreover, they are related by (4.3). Put

(5.1) $$f_k(\lambda, x) = \sum_{j=0}^{k} B(k, j, \lambda)x^j$$

and

$$f_{1,k}(\lambda, x) = \sum_{j=0}^{k} B_1(k, j, \lambda)x^j. \tag{5.2}$$

By (4.3), we have

$$f_{1,k}(\lambda, x) = x^k f_k\left(1 - \lambda, \frac{1}{x}\right). \tag{5.3}$$

By (2.7) and (3.6),

$$f_k(\lambda, 1) = f_{1,k}(\lambda, 1) = \frac{(2k)!}{2^k k!}. \tag{5.4}$$

In the next place, by (2.4), (5.1) becomes

$$f_k(\lambda, x) = \sum_{j=0}^{k} \{(k + j - \lambda)B(k - 1, j, \lambda) + (k - j + \lambda)B(k - 1, j - 1, \lambda)\}x^j.$$

Since

$$\sum_{j=0}^{k} (k + j - \lambda)B(k - 1, j, \lambda)x^j = (k - \lambda + xD)f_{k-1}(\lambda, x)$$

and

$$\sum_{j=0}^{k} (k - j + \lambda)B(k - 1, j - 1, \lambda)x^j = x\sum_{j=0}^{k-1} (k - j - 1 + \lambda)B(k - 1, j, \lambda)x^j$$

$$= x(k - 1 + \lambda - xD)f_{k-1}(\lambda, x),$$

where $D \equiv d/dx$, it follows that

$$f_k(\lambda, x) = \{k - \lambda + (k - 1 + \lambda)x + x(1 - x)D\}f_{k-1}(\lambda, x). \tag{5.5}$$

The corresponding formula for $f_{1,k}(\lambda, x)$ is

$$f_{1,k}(\lambda, x) = \{1 - \lambda + (2k - 2 + \lambda)x + x(1 - x)D\}f_{1,k-1}(\lambda, x). \tag{5.6}$$

Let E denote the familiar operator defined by $Ef(n) = f(n + 1)$. Then, by (2.9) and (5.1), we have

$$R(n, n - k, \lambda) = f_k(\lambda, E)\binom{n}{2k}. \tag{5.7}$$

Similarly, by (3.8) and (5.2),

$$R_1(n, n - k, \lambda) = f_{1,k}(\lambda, E)\binom{n}{2k}. \tag{5.8}$$

Thus, the recurrence

$$R(n + 1, n - k + 1, \lambda) - R(n, n - k, \lambda) = (\lambda + n - k + 1)R(n, n - k + 1, \lambda)$$

becomes

$$f_k(\lambda, E)\binom{n+1}{2k} - f_k(\lambda, E)\binom{n}{2k} = (\lambda + n - k + 1)f_{k-1}(\lambda, x)\binom{n}{2k-2}.$$

Since

$$\binom{n+1}{2k} - \binom{n}{2k} = \binom{n}{2k-1},$$

we have

$$f_k(\lambda, E)\binom{n}{2k-1} = (\lambda + n - k + 1)f_{k-1}(\lambda, x)\binom{n}{2k-2}. \tag{5.9}$$

Applying the finite difference operator Δ, we get

$$f_k(\lambda, E)\binom{n}{2k-1} = (\lambda + n - k + 2)f_{k-1}(\lambda, x)\binom{n}{2k-3} + f_{k-1}(\lambda, x)\binom{n}{2k-2} \tag{5.10}$$

Similarly, the recurrence

$$R_1(n+1, n-k+1, \lambda) - R_1(n, n-k, \lambda) = (\lambda+n)R_1(n, n-k+1, \lambda)$$

yields

$$(5.11) \qquad f_{1,k}(\lambda, E)\binom{n}{2k-1} = (\lambda+n)f_{1,k-1}(\lambda, E)\binom{n}{2k-2}$$

and

$$(5.12) \qquad f_{1,k}(\lambda, E)\binom{n}{2k-2} = (\lambda+n+1)f_{1,k-1}(\lambda, E)\binom{n}{2k-3} + f_{1,k-1}\binom{n}{2k-2}.$$

6. AN APPLICATION

We shall prove the following two formulas:

$$(6.1) \qquad R(n, n-k, 1-\lambda) = \sum_{t=0}^{k}\binom{k+n+1}{k-t}\binom{k-n-1}{k+t}R_1(k+t, t, \lambda),$$

and

$$(6.2) \qquad R_1(n, n-k, 1-\lambda) = \sum_{t=0}^{k}\left(\begin{matrix}k+n+1\\k-t\end{matrix}\right.\left(\begin{matrix}k-n-1\\k+t\end{matrix}\right)R(k+t, t, \lambda).$$

Note that the coefficients on the right of (6.1) and (6.2) are the same.

To begin with, we invert (2.9) and (3.8). It follows from (2.9) that

$$\begin{aligned}\sum_{n=k}^{\infty}R(n, n-k, \lambda)x^{n-k} &= \sum_{j=0}^{k}B(k, j, \lambda)x^{k-j}\sum\binom{n+j}{2k}x^{n-2k+j}\\ &= \sum_{j=0}^{k}B(k, j, \lambda)x^{k-j}\sum_{m=0}^{\infty}\binom{m+2k}{2k}x^{m}\\ &= (1-x)^{-2k-1}\sum_{j=0}^{k}B(k, j, \lambda)x^{k-j},\end{aligned}$$

so that

$$\begin{aligned}\sum_{j=0}^{k}B(k, k-j, \lambda)x^{j} &= (1-x)^{2k+1}\sum_{n=k}^{\infty}R(n, n-k, \lambda)x^{n-k}\\ &= \sum_{m=0}^{2k+t}(-1)^{m}\binom{2k+1}{m}x^{m}\sum_{t=0}^{\infty}R(k+t, t)x^{t}.\end{aligned}$$

It follows that

$$(6.3) \qquad B(k, k-j, \lambda) = \sum_{t=0}^{j}(-1)^{j-t}\binom{2k+1}{j-t}R(k+t, t, \lambda).$$

Similarly,

$$(6.4) \qquad B_1(k-k-j, \lambda) = \sum_{t=0}^{k}(-1)^{j-t}\binom{2k+1}{j-t}R_1(k+t, t, \lambda).$$

By (2.9), (4.3), and (6.4), we have

$$\begin{aligned}R(n, n-k, 1-\lambda) &= \sum_{j=0}^{k}B_1(k, k-j, \lambda)\binom{n+j}{2k}\\ &= \sum_{j=0}^{k}\binom{n+j}{2k}\sum_{t=0}^{j}(-1)^{j-t}\binom{2k+1}{j-t}R_1(k+t, t, \lambda)\end{aligned}$$

$$= \sum_{t=0}^{k} R_1(k+t,\ t,\ \lambda) \sum_{j=t}^{k} (-1)^{j-t} \binom{2k+1}{j-1} \binom{n+j}{2k}. \tag{6.5}$$

The inner sum is equal to

$$\sum_{j=0}^{k-t} (-1)^j \binom{2k+1}{j} \binom{n+t+j}{2k} = \binom{n+t}{2k} \sum_{j=0}^{k-t} \frac{(-2k-1)_j\,(n+t+1)_j\,(-k+t)_j}{j!\,(n+t-2k+1)_j\,(-k+t)_j}$$

$$= \binom{n+t}{2k} {}_3F_2 \left[\begin{matrix} -2k-1,\ n+t+1,\ -k+t \\ n+t-2k+1,\ -k+t \end{matrix} \right].$$

The ${}_3F_2$ is Saalschützian [1, p. 9], and we find, after some manipulation, that

$$\sum_{j=0}^{k-t} (-1)^j \binom{2k+1}{j} \binom{n+t+j}{2k} = \binom{k+n+1}{k-t} \binom{k-n-1}{k+t}.$$

Thus, (6.5) becomes

$$R(n,\ n-k,\ 1-\lambda) = \sum_{t=0}^{k} \binom{k+n+1}{k-t} \binom{k-n-1}{k+t} R_1(k+t,\ t,\ \lambda).$$

This proves (6.1). The proof of (6.2) is exactly the same.

7. BERNOULLI POLYNOMIALS OF HIGHER ORDER

Nörlund [9, Ch. 6] defined the Bernoulli function of order z by means of

$$\sum_{n=0}^{\infty} B_n^{(z)}(\lambda) \frac{u^n}{n!} = \left(\frac{u}{e^u - 1} \right)^z e^{\lambda u}. \tag{7.1}$$

It follows from (7.1) that $B_n^{(z)}(\lambda)$ is a polynomial of degree n in each of the parameters z, λ.

Consider

$$Q(n,\ n-k,\ \lambda) = \binom{n}{k} B^{(-n+k)}(\lambda) \tag{7.2}$$

and

$$Q_1(n,\ n-k,\ \lambda) = \binom{k-n-1}{k} B^{(n+1)}(1-\lambda). \tag{7.3}$$

It follows from (7.2) that

$$\sum_{n=k}^{\infty} Q(n,\ k,\ \lambda) \frac{u^n}{n!} = \sum_{n=k}^{\infty} \binom{u}{n-k} B_{n-k}^{(-k)}(\lambda) \frac{u^n}{n!} = \frac{u^k}{k!} \sum_{n=0}^{\infty} B_n^{(-k)}(\lambda) \frac{u^n}{n!}.$$

Hence, by (7.1), we have

$$\sum_{n=k}^{\infty} Q(n,\ k,\ \lambda) \frac{u^n}{n!} = \frac{1}{k!} (e^u - 1)^k e^{\lambda u}. \tag{7.4}$$

Comparison of (7.4) with (1.7) gives $Q(n,\ k,\ \lambda) = R(n,\ k,\ \lambda)$, so that

$$R(n,\ n-k,\ \lambda) = \binom{n}{k} B^{(-n+k)}(\lambda). \tag{7.5}$$

Next, by (7.3),

$$\begin{aligned}\sum_{n=k}^{\infty} Q_1(n,\ k,\ \lambda)\frac{u^n}{n!} &= \sum_{n=k}^{\infty}\binom{-k-1}{n-k}B_{n-k}^{(n+1)}(1-\lambda)\frac{u^n}{n!}\\ &= \sum_{n=k}^{\infty}(-1)^{n-k}\binom{n}{n-k}B_{n-k}^{(n+1)}(1-\lambda)\frac{u^n}{n!}\\ &= \frac{u^k}{k!}\sum_{n=0}^{\infty}(-1)^n B_{n-k}^{(n+1)}(1-\lambda)\frac{u^n}{n!}.\end{aligned}$$

It is known [8, p. 134] that

$$(1+t)^{x-1}\big(\log(1+t)\big)^k = \sum_{n=k}^{\infty}\frac{t^n}{(n-k)!}B_{n-k}^{(n+1)}(x).$$

Thus,

$$\begin{aligned}\sum_{k=0}^{\infty} y^k \sum_{n=k}^{\infty} Q_1(n,\ k,\ \lambda)\frac{u^n}{n!}y^k &= \sum_{k=0}^{\infty}\frac{y^k}{k!}(1-u)^{-\lambda}\left(\log\frac{1}{1-u}\right)^k\\ &= (1-u)^{-\lambda}(1-u)^{-y}.\end{aligned}$$

Therefore, $Q_1(n,\ k,\ \lambda) = R_1(n,\ k,\ \lambda)$, so that

$$R_1(n,\ n-k,\ \lambda) = \binom{k-n-1}{k}B_k^{(n+1)}(1-\lambda). \tag{7.6}$$

For $\lambda = 0$, (7.5) reduces to

$$S(n,\ n-k) = \binom{n}{k}B_k^{(-n+k)};$$

for $\lambda = 1$, we get

$$\begin{aligned}S(n+1,\ n-k+1) &= \binom{n}{k}B_k^{(-n+k)}(1) = \binom{n}{k}\left(1 - \frac{k}{-n+k-1}\right)B_k^{(-n+k-1)}\\ &= \binom{n+1}{k}B_k^{(-n+k-1)}.\end{aligned}$$

For $\lambda = 1$, (7.6) reduces to

$$S_1(n+1,\ n-k+1) = \binom{k-n-1}{k}B_k^{(n+1)};$$

for $\lambda = 0$, we get

$$S_1(n,\ n-k) = \binom{k-n-1}{k}\left(1 - \frac{k}{n}\right)B_k^{(n)} = \binom{k-n}{k}B_k^{(n)}.$$

Thus, in all four special cases, (7.5) and (7.6) are in agreement with the corresponding formulas for $S(n,\ n-k)$ and $S_1(n,\ n-k)$.

8. THE FUNCTIONS $R'(n,\ k,\ \lambda)$ AND $R_1'(n,\ k,\ \lambda)$

We may put

$$R(n,\ n-k,\ \lambda) = \sum_{j=0}^{k} R'(k,\ j,\ \lambda)\binom{n}{2k-j} \tag{8.1}$$

and

$$R_1(n,\ n-k,\ \lambda) = \sum_{j=0}^{k} R'(k,\ j,\ \lambda)\binom{n}{2k-j}. \tag{8.2}$$

The upper limit of summation is justified by (2.9) and (3.8).

Using the recurrence (2.3), we get

$$
\begin{aligned}
&R(n+1,\ n-k+1,\ \lambda) - R(n,\ n-k,\ \lambda)\\
&\quad = (n-k+1+\lambda)\sum_{j=0}^{k-1} R'(k-1,\ j,\ \lambda)\binom{n}{2k-j-2}\\
&\quad = \sum_{j=0}^{k-1}(2k-j-1)R'(k-1,\ j,\ \lambda)\binom{n}{2k-j-1}\\
&\qquad\qquad + \sum_{j=0}^{k-1}(k-j-1+\ \ )R'(k-1,\ j,\ \ \ )\binom{n}{2k-j-2}.
\end{aligned}
$$

Since

$$R(n+1,\ n-k+1,\ \lambda) - R(n,\ n-k,\ \lambda) = \sum_{j=0}^{k-1} R'(k,\ j,\ \lambda)\binom{n}{2k-j-1},$$

we get

$$R'(k,\ j,\ \lambda) = (2k-j-1)R'(k-1,\ j,\ \lambda) + (k-j+\lambda)R'(k-1,\ j-1,\ \lambda). \tag{8.3}$$

For $k = 0$, (8.1) gives

$$R'(0,\ 0,\ \lambda) = 1,\ R'(0,\ j,\ \lambda) = 0,\quad (j > 0). \tag{8.4}$$

The following values are easily computed using the recurrence (8.3).

$R'(k,\ j,\ \lambda)$

$k \backslash j$	0	1	2	3	4
0	1				
1	1	λ			
2	3	$1 + 3\lambda$	λ^2		
3	15	$10 + 15\lambda$	$1 + 4\lambda + 6\lambda^2$	λ^3	
4	105	$105 + 105\lambda$	$25 + 60\lambda + 45\lambda^2$	$1 + 5\lambda + 10\lambda^2 + 4\lambda^3$	λ^4

It is easily proved, using (8.3), that

$$R'(k,\ 0,\ \lambda) = 1.3.5\ \ldots\ (2k-1) \tag{8.5}$$

and

$$R'(k,\ k,\ \lambda) = \lambda^k. \tag{8.6}$$

Also,

$$\sum_{j=0}^{k}(-1)^j R'(k,\ j,\ \lambda) = (1-\lambda)_k. \tag{8.7}$$

Moreover, it is clear that $R'(k,\ j,\ \lambda)$ is a polynomial in λ of degree j.

To invert (8.1), multiply both sides by $(-1)^{m-n}\binom{m}{n}$ and sum over n. Changing the notation slightly, we get

$$R'(k,\ k-j,\ \lambda) = \sum_{t=0}^{j}(-1)^{j+t}\binom{k+j}{k+t}R(k+t,\ t,\ \lambda). \tag{8.8}$$

Turning next to (8.2) and employing (3.2), we get

$$\begin{aligned} &R_1(n+1,\ n-k+1,\ \lambda) - R_1(n,\ n-k,\ \lambda) \\ &\quad = (n+\lambda)\sum_{j=0}^{k-1} R_1'(k-1,\ j,\ \lambda)\binom{n}{2k-j-2} \\ &\quad = \sum_{j=0}^{k-1}(2k-j-1)R_1'(k-1,\ j,\ \lambda)\binom{n}{2k-j-1} \\ &\qquad\quad + \sum_{j=0}^{k-1}(2k-j-2+\lambda)R_1'(k-1,\ j,\ \lambda)\binom{n}{2k-j-2}. \end{aligned}$$

It follows that

(8.9) $R_1'(k,\ j,\ \lambda) = (2k-j-1)R'(k-1,\ j,\ \lambda) + (2k-j-1+\lambda)R_1'(k-1,\ j-1,\lambda).$

For $k = 0$, we have

(8.10) $$R_1'(0,\ 0,\ \lambda) = 1,\ R_1'(0,\ j,\ \lambda) = 0,\quad (j > 0).$$

The following values are readily computed by means of (8.9) and (8.10).

$R_1'(k,\ j,\ \lambda)$

k \ j	0	1	2	3	4
0	1				
1	1	λ			
2	3	$2 + 3\lambda$	$(\lambda)_2$		
3	15	$20 + 15\lambda$	$6 + 14\lambda + 6\lambda^2$	$(\lambda)_3$	
4	105	$210 + 105\lambda$	$130 + 165\lambda + 45\lambda^2$	$24 + 70\lambda + 50\lambda^2 + 10\lambda^3$	$(\lambda)_4$

We have

(8.11) $$R_1'(k,\ 0,\ \lambda) = 1.3.5\ \ldots\ (2k-1)$$

and

(8.12) $$R_1'(k,\ k,\ \lambda) = (\lambda)_k.$$

Also

(8.13) $$\sum_{j=0}^{k}(-1)^j R_1'(k,\ j,\ \lambda) = (1-\lambda)^k.$$

Clearly, $R_1'(k,\ j,\ \lambda)$ is a polynomial in λ of degree j.
Parallel to (8.8), we have

(8.14) $$R_1'(k,\ k-j,\ \lambda) = \sum_{t=0}^{j}(-1)^{j+t}\binom{k+j}{k+t}R_1(k+t,\ t,\ \lambda).$$

9. ADDITIONAL RELATIONS

(Compare [3, 4].) By (8.14) and (3.1), we have

$$\begin{aligned}
R_1'(k,\ k-j,\ \lambda) &= \sum_{t=0}^{j}(-1)^t\binom{k+j}{t}R_1'(k+j-t,\ j-t,\ \lambda)\\
&= \sum_{t=0}^{j}(-1)^t\binom{k+j}{t}\sum_{s=0}^{k}B_1(k,\ s,\ \lambda)\binom{k+j-t+s}{2k}\\
&= \sum_{s=0}^{k}B_1(k,\ s,\ \lambda)\sum_{t=0}^{j}(-1)^t\binom{k+j}{t}\binom{k+j-t+s}{2k}.
\end{aligned}$$

It can be verified that the inner sum is equal to $\binom{s}{k-j}$. Thus,

$$R_1'(k,\ j,\ \lambda) = \sum_{s=j}^{k}\binom{s}{j}B_1(k,\ s,\ \lambda). \tag{9.1}$$

Similarly,

$$R'(k,\ k-j,\ \lambda) = \sum_{s=k-j}^{k}\binom{s}{k-j}B(k,\ s,\ \lambda). \tag{9.2}$$

The inverse formulas are

$$B_1(k,\ t,\ \lambda) = \sum_{j=t}^{k}(-1)^{j-t}\binom{j}{t}R_1'(k,\ j,\ \lambda) \tag{9.3}$$

and

$$B(k,\ t,\ \lambda) = \sum_{j=t}^{k}(-1)^{j-t}\binom{j}{t}R'(k,\ j,\ \lambda). \tag{9.4}$$

In the next place, by (9.4) and (3.1),

$$\begin{aligned}
R_1(n,\ n-k,\ \lambda) &= \sum_{t=0}^{k}B_1(k,\ t,\ \lambda)\binom{n+t}{2k} = \sum_{t=0}^{k}B(k,\ k-t,\ 1-\lambda)\binom{n+t}{2k}\\
&= \sum_{t=0}^{k}B(k,\ t,\ 1-\lambda)\binom{n+k-t}{2k}\\
&= \sum_{t=0}^{k}\binom{n+k-t}{2k}\sum_{j=t}^{k}(-1)^{j-t}\binom{j}{t}R'(k,\ j,\ 1-\lambda)\\
&= \sum_{j=0}^{k}R'(k,\ j,\ 1-\lambda)\sum_{t=0}^{k}(-1)^{j-t}\binom{j}{t}\binom{n+k-t}{2k}.
\end{aligned}$$

The inner sum is equal to $(-1)^j\binom{n+k-j}{2k-j}$, and therefore

$$R_1(n,\ n-k,\ \lambda) = \sum_{j=0}^{k}(-1)^{k-j}\binom{n+j}{k+j}R'(k,\ k-j,\ 1-\lambda). \tag{9.5}$$

Similarly,

$$R(n,\ n-k,\ \lambda) = \sum_{j=0}^{k}(-1)^{k-j}\binom{n+j}{k+j}R_1'(k,\ k-j,\ 1-\lambda). \tag{9.6}$$

The inverse formulas are less simple. We find that

$$R_1'(n,\ k,\ \lambda) = \sum_{j=0}^{n} (-1)^{n-j} C_n(k,\ j) R(n + j,\ j,\ 1 - \lambda) \tag{9.7}$$

and

$$R'(n,\ k,\ \lambda) = \sum_{j=0}^{n} (-1)^{n-j} C_n(k,\ j) R_1(n + j,\ j,\ 1 - \lambda), \tag{9.8}$$

where

$$C_n(k,\ j) = \sum_{t=0}^{n-j} \binom{n - t}{k - t} \binom{2n - t}{n + j}. \tag{9.9}$$

It does not seem possible to simplify $C_n(k,\ j)$.

We omit the proof of (9.7) and (9.8).

Finally, we state the pair

$$R_1'(n,\ k,\ \lambda) = \sum_{t=0}^{k} (-1)^t \binom{n - t}{k - t} R'(n,\ t,\ 1 - \lambda), \tag{9.10}$$

$$R'(n,\ k,\ \lambda) = \sum_{t=0}^{k} (-1)^t \binom{n - t}{k - t} R_1'(n,\ t,\ 1 - \lambda). \tag{9.11}$$

The proof is like the proof of (8.8) and (8.14).

REFERENCES

1. W. N. Bailey. *Generalized Hypergeometric Series*. Cambridge, 1935.
2. L. Carlitz. "Note on Nörlund's Polynomial $B_n^{(z)}$." *Proc. Amer. Math. Soc.* 11 (1960):452-455.
3. L. Carlitz. "Note on the Numbers of Jordan and Ward." *Duke Math. J.* 38 (1971):783-790.
4. L. Carlitz. "Some Numbers Related to the Stirling Numbers of the First and Second Kind." *Publications de la Faculté d'Electrotechnique de l' Université a Belgrade* (1977):49-55.
5. L. Carlitz. "Polynomial Representations and Compositions, I." *Houston J. Math.* 2 (1976):23-48.
6. L. Carlitz. "Weighted Stirling Numbers of the First and Second Kind—I." *The Fibonacci Quarterly* 2 (1980):147-162.
7. G. H. Gould. "Stirling Number Representation Problems." *Proc. Amer. Math. Soc.* 11 (1960):447-451.
8. L. M. Milne-Thomson. *Calculus of Finite Differences*. London: Macmillan, 1951.
9. N. E. Nörlund. *Vorlesungen über Differenzenrechnung*. Berlin: Springer, 1924.

*****

A THEOREM CONCERNING HEPTAGONAL NUMBERS

HARVEY J. HINDIN
Polymathic Associates, 5 Kinsella St., Dix Hills, NY 11746

In this paper, we show that there are an infinite number of heptagonal numbers which are, at the same time, the sums and differences of distinct heptagonal numbers. Similar results have been found for triangular numbers [1] and pentagonal numbers [2].

The heptagonal numbers are given by $h_n = n(5n - 3)/2$, $n = 1, 2, 3, \ldots$, where $h_n - h_{n-1} = 5n - 4$. Heptagonal numbers are represented geometrically by regular heptagons homothetic with respect to one of the vertices and containing 2, 3, 4, ..., n points at equal distances along each side. The sum of all the points for a given n yields h_n. Both Dickson [3] and LeVeque [4] provide reviews concerning heptagonal and related figurate numbers.

Our analysis starts with the observation from a table of h_n values [5] that

$$h_{17} = h_6 + h_{16},\ h_{58} = h_{11} + h_{57}, \text{ and } h_{124} = h_{16} + h_{123}.$$

Note that each of these equations is of the form $h_m = h_{5k+1} + h_{m-1}$.

Since $h_{5k-1} = (125k^2 + 35k + 2)/2$, setting

$$h_m - h_{m-1} = 5m - 4 = h_{5k+1} = (125k^2 + 35k + 2)/2,$$

we have

$$m = (125k^2 + 35k + 10)/10.$$

An induction proof shows that m is an integer for all integers k. This leads us to:

Theorem 1: For any integer $k \geqq 1$,

$$h_{\frac{125k^2 + 35k\ \ 10}{10}} = h_{5k+1} + h_{\frac{125k^2 + 35k}{10}}.$$

Now consider the subset of heptagonal numbers in Theorem 1 which yields

$$(*) \qquad h_{\frac{125(5k)^2 + 35(5k) + 10}{10}} = h_{5(5k)+1} + h_{\frac{125(5k)^2 + 35(5k)}{10}}.$$

The LHS of (*) is equal to

$$(**) \qquad (9765625k^4 + 1093750k^3 + 74375k^2 + 2450k + 40)/40.$$

But suppose that $h_s - h_{s-1} = 5s - 4 = (**)$, so that we have

$$s = (9765625k^4 + 1093750k^3 + 74375k^2 + 2450k + 200)/200.$$

An induction proof shows that s is an integer for all positive integers k. Therefore, we have our major result,

Theorem 2: For any integer $k \geqq 1$,

$$h_{\frac{3125k^2 + 175k + 10}{10}} = h_{25k+1} + h_{\frac{3125k^2 + 175k}{10}}$$

and

$$h_{\frac{3125k^2 + 175k + 10}{10}} = h_{\frac{9765625k^4 + 1093750k^3 + 74375k^2 + 2450k + 200}{200}} - h_{\frac{9765625k^4 + 1093750k^3 + 74375k^2 + 2450k}{200}}.$$

Since these results hold for all integers $k \geq 1$, we see that there are an infinite number of heptagonal numbers which are, at the same time, the sums and differences of distinct heptagonal numbers. Q.E.D.

For $k = 1$, 2, and 3, respectively, Theorem 2 yields

$$h_{331} = h_{26} + h_{330} = h_{54682} - h_{54681},$$
$$h_{1286} = h_{51} + h_{1285} = h_{826513} - h_{826512},$$
$$h_{2866} = h_{76} + h_{2865} = h_{4106119} - h_{4106118}.$$

Verification is straightforward, if tedious. The list may be continued as desired.

Triangular, pentagonal, and heptagonal numbers all have the property exemplified by Theorem 2 for heptagonal numbers. Therefore, the question naturally arises as to whether either nonagonal or any or all other "odd number of sides" figurate numbers have the property. This conjecture is under investigation.

REFERENCES

1. W. Sierpinski. "Un théorème sur les nombres triangulaires." *Elemente der Mathematik*, Bank 23, Nr. 2 (Marz 1968), pp. 31-32.
2. R. T. Hansen. "Arithmetic of Pentagonal Numbers." *The Fibonacci Quarterly* 8, No. 1 (1970):83-87.
3. L. E. Dickson. *History of the Theory of Numbers*. Vol. II, Chapter 1. Chelsea, N.Y.: 1971.
4. W. J. LeVeque. *Reviews in Number Theory*. Providence, R.I.: American Mathematical Society, 1974. (Various locations.)
5. Bro. A. Brousseau. "Polygonal Numbers." Pp. 126-129 in *Number Theory Tables*. San Jose, Calif.: The Fibonacci Association, 1973.

*****

AN ALTERNATE REPRESENTATION FOR CÉSARO'S FIBONACCI-LUCAS IDENTITY

HARVEY J. HINDIN
Polymathic Associates, 5 Kinsella St., Dix Hills, NY 11746

E. Césaro's symbolic Fibonacci-Lucas identity $(2u+1)^n = u^{3n}$ allows us, after the binomial expansion has been performed, to use the powers as either Fibonacci or Lucas subscripts and obtain useful identities [1]. These have appeared many times in the literature, and most recently have been the subject of a problem [2].

Use of the identity enables us to provide a finite sum for F_{3n} (or L_{3n}) which is a linear combination of terms from F_0 (or L_0) to F_n (or L_n) inclusive. For example, we may derive

$$4L_2 + 4L_1 + L_0 = L_6$$

or, with algebraic effort, we obtain

$$16F_4 + 32F_3 + 24F_2 + 8F_1 + F_0 = F_{12}.$$

In this note, I show that

$$\sum_{r=0}^{n} 2^{n-r}\binom{n}{n-r}F_{n-r} = F_{3n} \tag{1}$$

is entirely equivalent to the Césaro identity where F_{3n} may be replaced by L_{3n}. This is of inherent interest and allows the direct determination of the multiplying coefficients for the finite sum without requiring a binomial expansion. For example, we may write, by inspection of (1), that

$$\begin{aligned} F_{24} = {} & 2^8\binom{8}{8}F_8 + 2^7\binom{8}{7}F_7 + 2^6\binom{8}{6}F_6 + 2^5\binom{8}{5}F_5 + 2^4\binom{8}{4}F_4 \\ & + 2^3\binom{8}{3}F_3 + 2^2\binom{8}{2}F_2 + 2^1\binom{8}{1}F_1 + 2^0\binom{8}{0}F_0. \end{aligned} \tag{2}$$

To derive or "discover" (1), construct, starting with $n = 0$, a Pascal triangle form of the coefficient multipliers of the LHS of the Césaro identity. This is shown in Figure 1a.

$$\begin{array}{cr} 1 & n = 0 \\ 2 \quad 2 & n = 1 \\ 4 \quad 4 \quad 1 & n = 2 \\ 8 \quad 12 \quad 6 \quad 1 & n = 3 \\ 16 \quad 32 \quad 24 \quad 8 \quad 1 & n = 4 \\ 32 \quad 80 \quad 80 \quad 40 \quad 10 \quad 1 & n = 5 \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot & \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot & \end{array}$$

Fig. 1a. Coefficient Multiplier Array for LHS of Césaro Identity

Note that this array may be written in the form shown in Figure 1b.

$$\begin{array}{cr} 1\ (1) & n = 0 \\ 2\ (1) \quad 1\ (1) & n = 1 \\ 4\ (1) \quad 2\ (2) \quad 1\ (1) & n = 2 \\ 8\ (1) \quad 4\ (3) \quad 2\ (3) \quad 1\ (1) & n = 3 \\ 16\ (1) \quad 8\ (4) \quad 4\ (6) \quad 2\ (4) \quad 1\ (1) & n = 4 \\ 32\ (1) \quad 16\ (5) \quad 8\ (10) \quad 4\ (10) \quad 2\ (5) \quad 1\ (1) & n = 5 \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot & \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot & \end{array}$$

Fig. 1b. Alternate Coefficient Multiplier Array for LHS of Césaro Identity

It may be seen that Figure 1b is the usual Pascal array with power of 2 multipliers. Indeed the rth term in the nth row, where $0 \leqq r \leqq n$ is given by $2^{n-r}\binom{n}{n-r}$. It follows directly that we may multiply each coefficient in row n by its corresponding Fibonacci or Lucas term, sum them, and set the result equal to the appropriate RHS of the Césaro identity to obtain

$$\sum_{r=0}^{n} 2^{n-r}\binom{n}{n-r}F_{n-r} = F_{3n}$$

for the Fibonacci case. Q.E.D.

This result, which clearly holds for Lucas numbers also, has not been noted previously as the equivalent of the Cesaro identity. The discovery method of derivation used here is particularly satisfying.

We may note in passing that the row sum in Figure 1b is given by

$$\sum_{r=0}^{n} 2^{n-r}\binom{n}{n-r} = 3^n. \tag{3}$$

Also, the right-rising diagonal generates the series 1, 2, 5, 12, 29, 70, ... given by $R_n = 2R_{n-1} + R_{n-2}$, and the left-rising diagonal yields 1, 1, 3, 5, 11, 21, ... given by $L_n = L_{n-1} + 2L_{n-2}$. Other properties of the array may be found by the reader.

REFERENCES

1. Various references to this formula are given in: L. E. Dickson. *History of the Theory of Numbers*. Vol. I, p. 402. 1971 reprint, Chelsea, N.Y.
2. G. Wulczyn. Problem B-339. *The Fibonacci Quarterly* 14, No. 3 (1976): 286.

*****

ON THE MATRIX APPROACH TO FIBONACCI NUMBERS AND THE FIBONACCI PSEUDOPRIMES

JACK M. POLLIN
United States Military Academy, West Point, NY
AND
I. J. SCHOENBERG
Mathematics Research Center, University of Wisconsin-Madison, WI 53706

INTRODUCTION

We consider sequences (x_n) of integers satisfying for all n the recurrence relation

$$x_{n+1} = x_n + x_{n-1}. \tag{1}$$

The x_n are uniquely defined if we prescribe the elements of the "initial vector" (x_0, x_1). On choosing $(x_0, x_1) = (0, 1)$, we obtain the *Fibonacci numbers* $x_n = F_n$, while the choise $(x_0, x_1) = (2, 1)$ gives the *Lucas numbers* $x_n = L_n$.

In [3], V. E. Hoggatt, Jr., and Marjorie Bicknell discuss the following conjecture of K. W. Leonard (unpublished).

Conjecture 1: *We have the congruence*

$$L_n \equiv 1 \pmod{n},\ (n > 1) \tag{2}$$

if and only if n is a prime number.

Among the many interesting results of [3], we single out the following:

Theorem 1: *The "if" part of Conjecture 1 is correct; i.e.,*

$$L_p \equiv 1 \pmod{p},\ \text{where } p \text{ is a prime}. \tag{3}$$

Theorem 2: *The "only if" part of Conjecture 1 is wrong, as shown by the congruence*

$$L_{705} \equiv 1 \pmod{705}, \tag{4}$$

while $705 = 3 \cdot 5 \cdot 47$ *is composite.*

Sponsored by the United States Army under Contract No. DAAG29-75-C-0024.

We are grateful to D. H. Lehmer for an informative letter [4] in which he expresses familiarity with these results; also, that composite numbers that satisfy (2) are called *Fibonacci pseudoprimes*, which we abbreviate F. Psps. In [3], the authors report, on the basis of computer results, that beyond 705 the next F. Psps are

$$2465,\ 2737,\ 3745,\ 4181. \tag{5}$$

Conjecture 1 was communicated to one of us several years ago by Richard S. Field, of Los Angeles. We became aware of the paper [3] only recently. Before this, in November 1976, George Logothetis, a graduate student in Computer Science in Madison, using Professor George Collins' SAC 2 program, found for us not only the five F. Psps already mentioned, but also two new ones:

$$5777,\ 6721, \tag{6}$$

He also found that these seven numbers are the only F. Psps that are $\leqq 9161$.

In the present paper we do the following:

1. Present a proof of Theorem 1 that uses from elementary number theory only Euclid's lemma.
2. Give a second proof of Theorem 2, and establish

Theorem 3: $L_{2465} \equiv 1 \pmod{2465}$.

These numerical results are here derived by the matrix approach as described in [2, Ch. 11]. In [3, p. 211], Theorem 2 is proved in a few lines by showing that the sequence L_n mod 705 has the period 704. Since $L_1 = 1$, the relation (4) follows. In §3 we describe this method of periods and show that while it proved Theorem 2, it did not work to establish Theorem 3. In [4], D. H. Lehmer stated that

$$2737 = 7 \cdot 17 \cdot 23 \textit{ is a Fibonacci pseudoprime}, \tag{7}$$

and that the method of periods will apply. This we verify.

3. Show, in §5, that the matrix approach allows us to develop *ab initio* some of the basic properties of Fibonacci numbers as presented in [1, §10.14]. As we assume no previous knowledge of Fibonacci numbers, this paper may serve as an introduction to these numbers.
4. The failure of the "only if" part of Conjecture 1 suggests a search for classes of composite numbers n which are *not* Fibonacci pseudoprimes. In §6 we state some modest results in this direction which suggested the following:

Conjecture 2: If $n > 1$, then

$$L_n \not\equiv 1 \pmod{n^2}. \tag{8}$$

Again George Logothetis showed (8) to hold for $n \leqq 7611$. Some further striking results obtained in the course of this computation are described at the end of the paper.

1. A PROOF OF THEOREM 1

Observe that the Lucas numbers L_n are explicitly given by

$$L_n = \left(\frac{1+\sqrt{5}}{2}\right)^n + \left(\frac{1-\sqrt{5}}{2}\right)^n \text{ for all } n, \tag{1.1}$$

because $(1 \pm \sqrt{5})/2$ are the roots of the characteristic equation $x^2 - x - 1 = 0$ of (1); hence, the right side of (1.1) satisfies (1), while it assumes the same initial values as L_n for $n = 0$ and $n = 1$. Now let $n = p$ be a prime > 2. Expanding the binomials and cancelling the irrational terms, we find that

$$L_p - 1 = \frac{1}{2^{p-1}}\left\{1 + \binom{p}{2}5 + \binom{p}{4}5^2 + \cdots + \binom{p}{p-1}5^{\frac{p-1}{2}}\right\} - 1$$
$$= \frac{1}{2^{p-1}}\left\{\binom{p}{2}5 + \cdots + \binom{p}{p-1}5^{\frac{p-1}{2}}\right\} - \frac{2^p - 2}{2^p}$$

Applying the binomial expansion of $(1+1)^p$ in the numerator of the last term, we obtain

$$L_p - 1 = \frac{1}{2^{p-1}}\left\{\binom{p}{2}5 + \cdots + \binom{p}{p-1}5^{\frac{p-1}{2}}\right\} - \frac{1}{2^p}\left\{\binom{p}{1} + \binom{p}{2} + \cdots + \binom{p}{p-1}\right\}.$$

The left side is an integer, while the right side is of the form pa/b, where p does not divide b, and therefore, $(p, b) = 1$. By Euclid's lemma, we conclude that b divides a, which proves (3).

2. THE MATRIX APPROACH AND A PROOF OF THEOREM 2

We replace the relation (1) by the *vector recurrence relation*

$$\begin{pmatrix} x_n \\ x_{n+1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} x_{n-1} \\ x_n \end{pmatrix} \tag{2.1}$$

to which is it visibly equivalent. Writing

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \tag{2.2}$$

and iterating (2.1), we obtain

$$\begin{pmatrix} x_n \\ x_{n+1} \end{pmatrix} = A^n\begin{pmatrix} x_0 \\ x_1 \end{pmatrix}. \tag{2.3}$$

This brings to bear on our problem the powerful tool of matrix multiplication. To prove Theorem 2, it suffices to work modulo 705. We observe that (2.3) implies

$$\begin{pmatrix} L_{704} \\ L_{705} \end{pmatrix} \equiv A^{704}\begin{pmatrix} 2 \\ 1 \end{pmatrix} \pmod{705}, \tag{2.4}$$

and that we are to determine the matrix A^{704} (mod 705). This is readily done with a hand calculator if we use the binary representation of 704:

$$704 = 64 + 128 + 512 = 2^6 + 2^7 + 2^9. \tag{2.5}$$

By successively squaring matrices, and working mod 705 throughout, we find A^{2^k} (mod 705) for $k = 1, 2, \ldots, 9$, and, in particular,

$$A^{2^6} \equiv \begin{pmatrix} 142 & 423 \\ 423 & 565 \end{pmatrix}, \; A^{2^7} \equiv \begin{pmatrix} 283 & 141 \\ 141 & 424 \end{pmatrix}, \; A^{2^9} \equiv \begin{pmatrix} 424 & 564 \\ 564 & 283 \end{pmatrix}, \pmod{705}.$$

Multiplying these matrices together, mod 705, we find, by (2.5), that

$$A^{704} \equiv \begin{pmatrix} 142 & 423 \\ 423 & 565 \end{pmatrix} \pmod{705}.$$

Now (2.4) shows that

$$\begin{pmatrix} L_{704} \\ L_{705} \end{pmatrix} \equiv \begin{pmatrix} 142 & 423 \\ 423 & 565 \end{pmatrix}\begin{pmatrix} 2 \\ 1 \end{pmatrix} = \begin{pmatrix} 707 \\ 1411 \end{pmatrix} \equiv \begin{pmatrix} 2 \\ 1 \end{pmatrix} \pmod{705}. \tag{2.7}$$

Therefore, $L_{705} \equiv 1$ (mod 705), and Theorem 2 is established.

A few remarks on these matrix operations are in order. Observe that A is a symmetric matrix, i.e., $A^T = A$. We also know that the product BC of two symmetric matrices that commute ($BC = CB$), is also symmetric. Since any two powers A^m and A^n clearly commute, it follows that all powers A^m are symmetric. This means that in multiplying two powers of A, we need to compute only one of the two elements off the main diagonal.

The matrix multiplications performed above require the following important check against errors. Passing to determinants, from $|A| = -1$, we conclude that $|A^m| = (-1)$. Since all the above exponents m are even, we see that $|A^m| = 1$, and, of course, $|A^m| \equiv 1 \pmod{705}$. The check is to verify that *after each matrix multiplication*, the resulting product M satisfies

$$|M| \equiv 1 \pmod{705}.$$

3. ON THE HOGGATT-BICKNELL PROOF OF THEOREM 2

In order to make this paper self-sufficient, we establish the known lemmas below. Let k be given, $k > 1$, and let us denote by (L_n, mod k) the sequence (L_n) of Lucas numbers reduced mod k.

Lemma 1: *The sequence (L_n, mod k) is periodic.*

Proof: Clearly, (L_n, mod k) is periodic if and only if for some r and s we have

$$(x_r, x_{r+1}) \equiv (x_s, x_{s+1}) \pmod{k}, \; r < s.$$

It follows that there is no periodicity if and only if

for every pair (r, s), such that $r < s$
we have $(x_r, x_{r+1}) \not\equiv (x_s, x_{s+1}) \pmod{k}$.

But this is obviously impossible, as there are only k^2 distinct pairs (u, v) (mod k) available.

The Hoggatt-Bicknell proof of Theorem 2 is based on the following sufficient conditions for (L_n, mod k) to have the period m.

Lemma 2: *If the following conditions are satisfied,*

$$k = \prod_{i=1}^{t} a_i, \; (a_i, a_j) = 1 \textit{ if } i \neq j, \tag{3.1}$$

$$A_i \textit{ is a period of } (L_n, \bmod a_i), \tag{3.2}$$

$$A_i | m \textit{ for all } i, \tag{3.3}$$

then

$$m \textit{ is a period of } (L_n, \bmod k). \tag{3.4}$$

Proof: By (3.2), $L_{n+A_i} \equiv L_n \pmod{a_i}$ for all n. By (3.3), if follows that

$$L_{n+m} \equiv L_n \pmod{a_i} \text{ for all } n, \text{ and all } i, \tag{3.5}$$

because a multiple of a period is also a period. Now (3.1) and (3.5) imply that $L_{n+m} \equiv L_n \pmod{k}$ for all n, which proves (3.4).

Lemma 2 applied nicely to the case of $k = 705 = 3 \cdot 5 \cdot 47$, for (3.1) holds with $t = 3$, $a_1 = 3$, $a_2 = 5$, $a_3 = 47$. Simple direct calculations with L_n show that (3.2) is satisfied with $A_1 = 8$, $A_2 = 4$, $A_3 = 32$. Also (3.3) holds for $m = 704$, because 8, 4, and 32 are all divisors of 704. By Lemma 2, we conclude that $L_{n+704} \equiv L_n \pmod{705}$ for all n. In particular for $n = 1$ we obtain $L_{705} \equiv 1 \pmod{705}$, which proves Theorem 2. For $n = 0$ we also obtain that $L_{704} \equiv L_0 = 2 \pmod{705}$, which we already know from (2.7).

This method will not allow us to prove Theorem 3. Indeed, the relation (4.3) below shows that $m = 2464$ is *not* a period of (L_n, mod 2465).

4. A PROOF OF THEOREM 3

By (2.3) we are to determine

$$A^{2464} \pmod{2465}. \tag{4.1}$$

From $2464 = 32 + 128 + 256 + 2048 = 2^5 + 2^7 + 2^8 + 2^{11}$, we obtain

$$A^{2464} = A^{2^5} \cdot A^{2^7} \cdot A^{2^8} \cdot A^{2^{11}}. \tag{4.2}$$

By successive squaring of matrices mod 2465, we find that

$$A^{2^5} \equiv \begin{pmatrix} 379 & 1714 \\ 1714 & 2093 \end{pmatrix},\ A^{2^7} \equiv \begin{pmatrix} 1393 & 1886 \\ 1886 & 814 \end{pmatrix},$$

$$A^{2^8} \equiv \begin{pmatrix} 495 & 1482 \\ 1482 & 1977 \end{pmatrix},\ A^{2^{11}} \equiv \begin{pmatrix} 1858 & 1221 \\ 1221 & 614 \end{pmatrix},\ \pmod{2465}.$$

Multiplying these together, we find by (4.2) that

$$A^{2464} \equiv \begin{pmatrix} 117 & 783 \\ 783 & 900 \end{pmatrix},$$

and finally, by (2.3)

$$\begin{pmatrix} L_{2464} \\ L_{2465} \end{pmatrix} \equiv \begin{pmatrix} 117 & 783 \\ 783 & 900 \end{pmatrix} \begin{pmatrix} 2 \\ 1 \end{pmatrix} = \begin{pmatrix} 1017 \\ 2466 \end{pmatrix} \equiv \begin{pmatrix} 1017 \\ 1 \end{pmatrix} \pmod{2465}. \tag{4.3}$$

Thus, $L_{2465} \equiv 1 \pmod{2465}$, which proves Theorem 3.

The information that $L_{2464} \equiv 1017 \pmod{2465}$ shows that $m = 2464$ *is not a period of* (L_k, mod 2465), and this is the reason why the method of §3 would not work.

Similarly, we can work out on a hand-calculator, such as SR-51A, the matrix $A^{n-1} \pmod{n}$ for any $n < 10^5$. Indeed, all matrix multiplications, mod n, are feasible, because all numbers that we encounter are $< 10^{10}$, the capacity of the calculator.

In [4], D. H. Lehmer pointed out that the second number of (5), namely $2737 = 7.17.23$ is a Fibonacci pseudoprime, and that Lemma 2 applies to show it. This is easily verified: Lemma 2 applies to $k = 2737$ with

$$t = 3,\ a_1 = 7,\ a_2 = 17,\ a_3 = 23,\ A_1 = 16,\ A_2 = 36,\ A_3 = 48, \text{ and } m = 2736.$$

Therefore, 2737 is a period of (L_n, mod 2737) and it follows that $L_{2736} \equiv 2$, $L_{2737} \equiv 1 \pmod{2737}$. Therefore, (7) is established.

5. FURTHER APPLICATIONS OF THE MATRIX APPROACH

Out applications in §2 and §4 were mainly computational. We now wish to show how the matrix A allows us to develop *ab initio* some of the best known properties of the Fibonacci numbers.

Let us make the relation (2.3) or

$$\begin{pmatrix} x_n \\ x_{n+1} \end{pmatrix} = A^n \begin{pmatrix} x_0 \\ x_1 \end{pmatrix} \tag{5.1}$$

more explicit by writing

$$A^n = \begin{pmatrix} a_n & b_n \\ c_n & d_n \end{pmatrix} \tag{5.2}$$

where it becomes

$$\begin{aligned} x_n &= a_n x_0 + b_n x_1 \\ x_{n+1} &= c_n x_0 + d_n x_1. \end{aligned} \tag{5.3}$$

This easily generalizes to

$$\begin{aligned} x_{n+k} &= a_n x_k + b_n x_{k+1} \\ x_{n+k+1} &= c_n x_k + d_n x_{k+1} \end{aligned}. \tag{5.4}$$

Indeed, by (5.1),

$$\begin{pmatrix} x_{n+k} \\ x_{n+k+1} \end{pmatrix} = A^{n+k}\begin{pmatrix} x_0 \\ x_1 \end{pmatrix} = A^n \cdot A^k \begin{pmatrix} x_0 \\ x_1 \end{pmatrix} = A^n \begin{pmatrix} x_k \\ x_{k+1} \end{pmatrix},$$

again by (5.1). This and (5.2) show that (5.4) holds. We obtain $x_n = F_n$ if we choose $x_0 = F_0 = 0$ and $x_1 = F_1 = 1$, and (5.3) shows that

$$\begin{aligned} F_n &= b_n \\ F_{n+1} &= d_n \end{aligned}. \tag{5.5}$$

Applying (5.4) to $x_n = F_n$ and $k = 1$, and observing that $F_1 = 1$, $F_2 = 1$, we obtain

$$\begin{aligned} F_{n+1} &= a_n + b_n \\ F_{n+2} &= c_n + d_n. \end{aligned}$$

These relations and (5.5) show that

$$\begin{aligned} a_n &= F_{n+1} - F_n = F_{n-1} \\ c_n &= F_{n+2} - F_{n+1} = F_n \end{aligned}.$$

We have thus shown that

$$A^n = \begin{pmatrix} F_{n-1} & F_n \\ F_n & F_{n+1} \end{pmatrix}. \tag{5.6}$$

See also [2, Theorem II].

Our previous remark that $|A^n| = (-1)^n$ shows that

$$F_{n+1}F_{n-1} - F_n^2 = (-1)^n, \tag{5.7}$$

which is a known relation derived in the same way in [2, Theorem III]. From (5.6), we also see that the elements of all the matrices of §2 and §4 are appropriate Fibonacci numbers reduced by the moduli 705 and 2465, respectively.

Let us derive the known property that

$$F_n \textit{ divides } F_{nr} \textit{ if } r > 0. \tag{5.8}$$

From (5.4) and (5.6), we obtain for $x_n = F_n$ the relation

$$\begin{pmatrix} F_{n+k} \\ F_{n+k+1} \end{pmatrix} = \begin{pmatrix} F_{n-1} & F_n \\ F_n & F_{n+1} \end{pmatrix}\begin{pmatrix} F_k \\ F_{k+1} \end{pmatrix}. \tag{5.9}$$

Replacing n and k by nr and n, respectively, we obtain

$$\begin{pmatrix} F_{n(r+1)} \\ F_{n(r+1)+1} \end{pmatrix} = \begin{pmatrix} F_{nr-1} & F_{nr} \\ F_{nr} & F_{nr+1} \end{pmatrix}\begin{pmatrix} F_n \\ F_{n+1} \end{pmatrix},$$

whence

$$F_{n(r+1)} = F_{nr-1}F_n + F_{nr}F_{n+1}.$$

This shows that if F_n divides F_{nr}, then F_n also divides $F_{n(r+1)}$, which proves (5.8) by induction, since (5.8) is obvious if $r = 1$.

As a further example, let us establish the known property:

$$\textit{If } (m, n) = d, \textit{ then } (F_m, F_n) = F_d. \tag{5.10}$$

Since d divides m and also n, it follows from (5.8) that

$$F_d \text{ divides } F_m \text{ and also } F_n. \tag{5.11}$$

It remains to show that F_d is the *greatest* common divi r of F_m and F_n. Let r and s be such that $d = mr + ns$. From (5.9), on replacing n and k by mr and ns, respectively, we obtain

$$\begin{pmatrix} F_{mr+ns} \\ F_{mr+ns+1} \end{pmatrix} = \begin{pmatrix} F_{mr-1} & F_{mr} \\ F_{mr} & F_{mr+1} \end{pmatrix} \begin{pmatrix} F_{ns} \\ F_{ns+1} \end{pmatrix}.$$

This shows in particular that $F_d = F_{mr+ns}$ can be written as

$$F_d = F_{mr-1}F_{ns} + F_{mr}F_{ns+1}. \tag{5.12}$$

By (5.8), any divisor δ of F_m and of F_n also divides F_{mr} and F_{ns}, and by (5.12) that δ also divides F_d. Therefore, F_d is the greatest common divisor of F_m, F_n, and (5.10) is established.

A last example concerns the Lucas numbers. *Let us show that*

$$L_{n+1}L_{n-1} - L_n^2 = (-1)^{n+1} \cdot 5. \tag{5.13}$$

From (5.1) and (5.6), we have

$$\begin{pmatrix} L_n \\ L_{n+1} \end{pmatrix} = \begin{pmatrix} F_{n-1} & F_n \\ F_n & F_{n+1} \end{pmatrix} \begin{pmatrix} 2 \\ 1 \end{pmatrix}.$$

Again for $x_n = L_n$, but from (5.4) with $k = -1$, we get that

$$\begin{pmatrix} L_{n-1} \\ L_n \end{pmatrix} = \begin{pmatrix} F_{n-1} & F_n \\ F_n & F_{n+1} \end{pmatrix} \begin{pmatrix} -1 \\ 2 \end{pmatrix}$$

because $L_{-1} = -1$, $L_0 = 2$. The last two relations combined give

$$\begin{pmatrix} L_{n-1} & L_n \\ L_n & L_{n+1} \end{pmatrix} = \begin{pmatrix} F_{n-1} & F_n \\ F_n & F_{n+1} \end{pmatrix} \begin{pmatrix} -1 & 2 \\ 2 & 1 \end{pmatrix}.$$

Passing to determinants and using (5.7), we obtain (5.13).

6. SOME COMPOSITE NUMBERS THAT ARE NOT FIBONACCI PSEUDOPRIMES

We have defined a number n as a *Fibonacci pseudoprime* (F. Psps) if it is composite and satisfies $L_n \equiv 1 \pmod{n}$. F. Psps are rare: We have seen that there are only seven F. Psps ≤ 9161. It would seem of interest to exhibit some composite n which are not F. Psps. A modest beginning in this direction are the following results.

__*Theorem 4*__: *The numbers*

$$2^k, \ (k > 1) \tag{6.1}$$

are not Fibonacci pseudoprimes. Actually

$$L_{2^k} \equiv 2^k - 1 \pmod{2^k}. \tag{6.2}$$

__*Theorem 5*__: *If p is an odd prime such that*

$$L_p \not\equiv 1 \pmod{p^2}, \tag{6.3}$$

then

$$L_{p^k} \not\equiv 1 \pmod{p^k} \textit{ for } k > 1, \tag{6.4}$$

hence p^k is not a Fibonacci pseudoprime.

For brevity, we omit proofs which might be given elsewhere. We rather discuss the assumption (6.3).

Computer computations made by George Logothetis (Nov. 1976) show that

$$L_n \not\equiv 1 \pmod{n^2} \text{ if } 2 \leq n \leq 7611, \tag{6.5}$$

whether n is prime or composite. He computed the remainder r_n, hence

$$L_n \equiv r_n \pmod{n^2},\ 0 \leqq r_n < n^2, \tag{6.6}$$

for all n such that $2 \leq n \leq 7611$, with the following results.

1. *The remainders* $r_n = 0$ *and* $r_n = 1$ *were never found*. This result led us to formulate Conjecture 2 of our Introduction.

2. *The value* $r_n = 2$ *appeared only if* $n \equiv 0 \pmod{24}$.

For $n = 24k$, *he found that* $r_n = 2$ *precisely for the following* 100 *values of* k:

$k =$	1	2	3	4	5	6	8	9	10	12
	14	15	16	18	20	24	25	27	28	30
	32	36	40	42	45	46	48	50	51	54
	55	56	57	60	64	70	72	75	80	81
	84	90	92	96	98	100	102	108	110	112
	114	120	125	126	128	135	138	140	144	150
	153	155	160	162	165	168	171	180	182	184
	188	192	195	200	204	205	210	215	220	224
	225	228	230	240	243	250	252	255	256	270
	275	276	280	285	288	294	300	305	306	310

This is remarkable numerical evidence. From generally large values, the remainder r_n in (6.6) drops down to $r_n = 2$ for $n = 24k$ and values of k as listed. We also mention that the last Lucas number, L_{7611}, has 1591 digits.

From the identity $L_{4n} - 2 = 5(F_{2n})^2$ [2, Identity I_{16}, p. 59], it follows that $L_{24k} - 2 = 5(F_{12k})^2$. Therefore, $L_{24k} - 2 \equiv 0$ [mod $(24k)^2$] if and only if

$$F_{12k} \equiv 0 \pmod{24k}. \tag{6.7}$$

From the computer results above, we see that (6.7) holds for the 100 values of k listed above, and does not hold for the other values of

$$k \leqq [7611/24] = 317.$$

REFERENCES

1. G. H. Hardy & E. M. Wright. *An Introduction to the Theory of Numbers*. 3rd ed. Oxford: Oxford University Press, 1954.
2. V. E. Hoggatt, Jr. *Fibonacci and Lucas Numbers*. Boston: Houghton Mifflin Co., 1969.
3. V. E. Hoggatt, Jr., & Marjorie Bicknell. "Some Congruences of the Fibonacci Numbers Modulo a Prime p." *Math. Magazine* 47 (1974):210-214.
4. D. H. Lehmer. Personal letter to the authors, November 28, 1976.

*****

FREE GROUP AND FIBONACCI SEQUENCE

G. WALTHER

Institut für Didaktik der Mathematik, Postfach 380, W. Germany

Let X be a nonempty set $X = \{x_i \mid i \in I\}$ where I is a suitable index set and X^{-1} another set in one-to-one correspondence with X. A word of length n in the elements of $X \cup X^{-1}$ is an ordered set of n elements ($n \geqq 0$) each of $X \cup X^{-1}$.

A word of length n will be written as $x_{i_1}^{s_1} \ldots x_{i_n}^{s_n}$ where each sign s_i is i or -1. With "1" we denote the unique word of length 0. The product of two words is defined as follows. Let a be an arbitrary word $1a = a1 : a$.

Let a and b be words of positive lengths m and n; i.e.,

$$a = x_{i_1}^{s_1} \ldots x_{i_m}^{s_m} \quad \text{and} \quad b = x_{j_1}^{t_1} \ldots x_{j_n}^{t_n},$$

then

$$ab \; : = x_{i_1}^{s_1} \ldots x_{i_m}^{s_m} x_{j_1}^{t_1} \ldots x_{j_n}^{t_n}$$

and the length of the product is $m + n$.

If we define the relation "adjacent" between words, which turns out to be an equivalence relation, and the product $[a][b] \; : = [ab]$ of equivalence classes $[a]$ and $[b]$ of words a and b, we get the free group $F(X)$ over the generating set X.

A word in $X \cup X^{-1}$ is reduced if it has the form

$$x_{i_1}^{s_1} \ldots x_{i_m}^{s_m} \quad \text{and} \quad x_{i_{k+1}}^{s_{k+1}} \neq x_{i_k}^{-s_k} \text{ for } k = 1, 2, \ldots, m - 1.$$

Two elements, $x_i^{s_i}$ and $x_j^{s_j} \in X \cup X^{-1}$, will be called an inverse couple of elements if

$$x_i^{s_i} x_j^{s_j} = 1 \quad \text{or} \quad x_j^{s_j} x_i^{s_i} = 1.$$

Now we are in the position to formulate our problem.

Let $a = a_1 \ldots a_n$ be a word of length n with $a_i \in X \cup X^{-1}$ for $1 \leq i \leq n$. What is the maximum number of ways in which it could be reduced

a. to different words of length g $(n \geq g)$?

b. to different words?

c. to words of length g?

Theorem: Let A_{gn}, B_n, and C_{gn} be the numbers mentioned above. Then we get

α) $$A_{gn} = \begin{cases} \dbinom{\frac{g+n}{2}}{g} & \text{if } g \text{ and } n \text{ have the same parity and } g \leq n \\ 0 & \text{otherwise} \end{cases}$$

β) $$B_n = B_{n-1} + B_{n-2},\; B_0 = B_1 = 1$$

γ) $$C_{gn} = \begin{cases} \dbinom{n-1}{t} - \dbinom{n-1}{t-2} & \text{for } g = n - 2t \text{ and } 0 \leq t < \frac{n}{2} \\ 1 & \text{for } g = n \\ 0 & \text{otherwise} \end{cases}$$

Corollary: Expression of B_n as a sum of binomial coefficients.

With the convention $\binom{n}{0} = 1$, $\binom{n}{m} = 0$, for $n < m$,

we get the well-known relation

$$B_n = \binom{n}{0} + \binom{n-1}{1} + \binom{n-2}{2} + \cdots .$$

To prove the theorem, we use a known procedure to construct the reduced word for $a = a_1 \ldots a_n$.

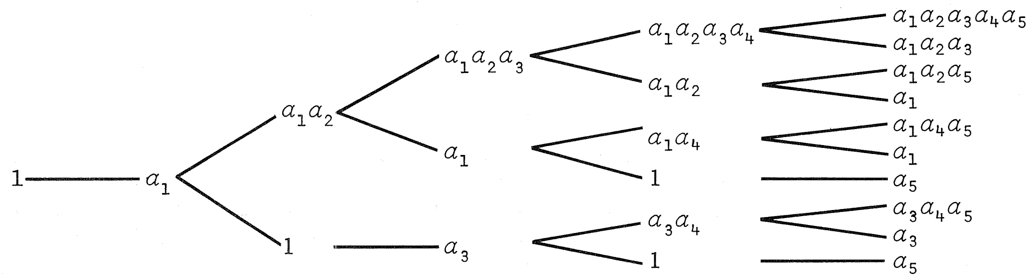
Let $w_0 \; : = 1$ and $w_1 \; : = a_1$, and let w_i be found for $1 \leq i < n$.

i) If w_i does not end in a_{i+1}^{-1}, then $w_{i+1} \; : = w_i a_i$.

ii) If w_i does end in a_{i+1}^{-1}, then $w_{i+1} \; : = z$, where $w_i = z a_{i+1}^{-1}$.

In a somehow "inverse" sense, we can get a survey over the reduction process by means of a tree.

Take the word $a = a_1 a_2 a_3 a_4 a_5$ for example:



It is evident, from the cancellation process, that $A_{gn} = C_{gn} = 0$ iff g and n have different parity.

Proof:

α) As cancellation diminishes the length of a word by 2, it is clear, from rules (i) and (ii) that

$$A_{gn} = A_{g,n-2} + A_{g-1,n-1} \text{ for } n \geq 2,$$

with the additional conditions $A_{gn} = 0$ iff g and n have different parity, $A_{0n} = 1$, $A_{gg} = 1$ for $0 \leq g \leq n$, $A_{gn} = 0$ for $g > n$.

The transformation $D_{ik} := A_{k,2i-k}$ for $0 \leq k \leq i$, $D_{ii} = 1$ for $i \geq 0$,

$$D_{i0} = \begin{cases} 1 & \text{if } i \text{ is even} \\ 0 & \text{if } i \text{ is odd,} \end{cases}$$

and $D_{ik} = 0$ for $k > i$, together with its inverse transformation,

$$A_{pq} = D_{\frac{p+q}{2},p},$$

yields the fundamental binomial relation

$$D_{ik} = D_{i-k,k} + D_{i-1,k-1} \text{ for } i, k \geq 1,$$

with solution $D_{ik} = \binom{i}{k}$. Translating this result, we get $A_{gn} = \binom{\frac{g+n}{2}}{g}$.

β) For $n = 0, 1, 2$, the proposition is true. Let $a = a_1 \ldots a_{n-2}a_{n-1}a_n$ be a word of length $n - 2$. Then we distinguish two cases:

1. $a_i a_n \neq 1$ for $i < n$ (i.e., a_i is the last "letter" of a word of maximum length $n - 1$). By the induction hypothesis, the maximum number of different words to which a word of length $n - 1$ can be reduced is B_{n-1}. The B_{n-1} different words $w_1, \ldots, w_{B_{n-1}}$ consequently lead to B_{n-1} different words $w_1a_n, \ldots, w_{B_{n-1}} a_n$.

2. $a_i a_n = 1$. I.e., a_i, a_n is an inverse couple for $i < n$; therefore, the length of words under consideration is reduced by 2. Consequently, we have a contribution of B_{n-2} to the amount of B_n.

γ) For illustration consider the word $w = a_1a_2a_3a_4a_5$ which could be reduced to a_1, for example, in exactly two ways:

a_2, a_3 and a_2, a_5 are two inverse couples;
a_2, a_3 and a_4, a_5 are two inverse couples (cf. the tree above).

The cancellation process yields the following special relations:

$$C_{mn} = 0 \text{ for } m > n;\ C_{mm} = 1;\ C_{mn} = 0 \text{ for } m, n, \text{ with different parity;}$$

$$C_{0n} = C_{1,n-1} \text{ for } n \geq 1.$$

A simple induction argument shows that $C_{n-2,n} = n - 1$ for $n \geq 2$.

We get all possible reduced words w' from $w = a \ldots a_{n-1}a_{n-2}a_n$ of length $n - 2$ *either* extending all $n - 2$ words

$$w'' = x_{i_1} \ldots x_{i_{n-2}}$$

$$(i_1 < i_2 < \cdots < i_{n-2} \text{ and } x_{i_j} \in \{a_1, \ldots, a_{n-2}\})$$

with a_n, i.e., $w' = w''a_n$ *or* from the single word $a_1 \ldots a_{n-2}$.. In the latter case, a_{n-1}, a_n is the only inverse couple of w.

Besides the special relations for C_{mn}, we have the general relation

$$(*) \qquad C_{mn} = C_{m+1,n-1} + C_{m-1,n-1} \text{ for } m, n \geq 1.$$

Let $E_{ik} := C_{k,i+k}$ for $i, k \geq 0$, respectively, $C_{mn} = E_{n-m,m}$ for $n \geq m$ and $n, m \geq 0$. From $C_{0n} = C_{1,n-1}$ follows $E_{i0} = E_{i-2,1}$ for $i \geq 2$.

From (*), we get

$$(**) \qquad E_{ik} = E_{i,k-1} + E_{i-2,k+1} \text{ for } i \geq 2,\ k \geq 1.$$

Considering $C_{n-2,n} = n - 1$ for $n \geq 2$, we have $E_{2k} = 1 + k$.

Next we express E_{ik} by $E_{i-2,k}$ for $i \geq 2$; (**) yields

$$E_{ik} = \sum_{p=1}^{k+1} E_{i-2,p}.$$

An iteration procedure and $E_{2k} = 1 + k$ leads to the following "monstrous" expression:

$$E_{2t,k_{t-1}} = \sum_{k_{t-2}=1}^{k_{t-1}+1} \cdots \sum_{k_1=1}^{k_2+1} \sum_{r=1}^{k_1+1} (r+1) \text{ for } t \geq 2,\ k_i \geq 0.$$

Remark: Since $C_{mn} = 0$ for m, n with different parity, we have $E_{ik} = 0$ for i an odd number.

We prove by induction that

$$E_{2t,k_{t-1}} = \binom{k_{t-1} + 2t - 1}{t} - \binom{k_{t-1} + 2t - 1}{t - 2},\ t \geq 2.$$

For $t = 2$, we have

$$E_{2,k_1} = \sum_{r=1}^{k_1+1} (r+1) = \frac{(k_1 + 4)(k_1 + 1)}{2} = \frac{(k_1 + 3)(k_1 + 2)}{2} - 1$$

$$= \binom{k_1 + 3}{2} - \binom{k_1 + 3}{0}.$$

To show

$$\sum_{k_{t-1}=1}^{k_t+1} \left[\binom{k_{t-1} + 2t - 1}{t} - \binom{k_{t-1} + 2t - 1}{t - 2}\right] = \binom{k_t + 2t + 1}{t + 1} - \binom{k_t + 2t + 1}{t - 1}$$

$$= E_{2(t+1),k_t},$$

we need the following

Lemma: $$\sum_{k=1}^{n+1} \binom{c + k}{j} = \binom{c + n + 2}{j + 1} - \binom{c + 1}{j + 1}.$$

Proof of the Lemma: On the one hand

$$\sum_{k=1}^{n}\prod_{i=0}^{j}(k+i) = (j+1)!\sum_{k=1}^{n}\binom{k+j}{j+1};$$

on the other hand

$$\sum_{k=1}^{n}\prod_{i=0}^{j}(k+i) = \frac{1}{j+2}\sum_{i=0}^{j+1}(n+i).$$

Combining these two identities yields

$$(***) \qquad \sum_{k=1}^{n}\binom{k+j}{j+1} = \binom{n+j+1}{j+2}.$$

From

$$\sum_{k=1}^{n+1}\binom{c+k}{j} = \sum_{k=0}^{c+n-j+2}\binom{k+j-1}{j} - \sum_{k=0}^{c-j+1}\binom{k+j-1}{j},$$

follows, with (***), the assertion.

Now we continue the proof of the theorem. With the aid of the lemma,

$$\sum_{k_{t-1}=1}^{k_t+1}\left[\binom{k_{t-1}+2t-1}{t} - \binom{k_{t-1}+2t-1}{t-2}\right]$$

$$= \binom{k_t+2t+1}{t+1} - \binom{2t}{t+1} - \binom{k_t+2t+1}{t-1} + \binom{2t}{t-1}$$

$$= \binom{k_t+2t+1}{t+1} - \binom{k_t+2t+1}{t-1} = E_{2(t+1),\,k_t}.$$

To prove the corollary, we use

$$B_n = \sum_{g\le n} A_{gn} = \sum_{g\le n}\binom{\frac{g+n}{2}}{g} = \binom{n}{n} + \binom{n-1}{n-2} + \cdots$$

$$= \binom{n}{0} + \binom{n-1}{1} + \cdots .$$

$\binom{\frac{g+n}{2}}{g}$ is defined, because g and n have the same parity.

*****

ELEMENTARY PROBLEMS AND SOLUTIONS

Edited by
A. P. HILLMAN
University of New Mexico, Albuquerque, NM 87131

Send all communications regarding ELEMENTARY PROBLEMS AND SOLUTIONS to PROFESSOR A. P. HILLMAN, 709 Solano Dr., S.E., Albuquerque, New Mexico 87108. Each solution or problem should be on a separate sheet (or sheets). Preference will be given to those typed with double spacing in the format used below. Solutions should be received within 4 months of the publication date.

DEFINITIONS

The Fibonacci numbers F_n and Lucas numbers L_n satisfy $F_{n+2} = F_{n+1} + F_n$, $F_0 = 0$, $F_1 = 1$ and $L_{n+2} = L_{n+1} + L_n$; $L_0 = 2$, $L_1 = 1$. Also a and b designate the roots $(1 + \sqrt{5})/2$ and $(1 - \sqrt{5})/2$, respectively, of $x^2 - x - 1 = 0$.

PROBLEMS PROPOSED IN THIS ISSUE

B-430 *Proposed by M. Wachtel, H. Klauser, and E. Schmutz, Zürich, Switz.*

For every positive integer a, prove that

$$(a^2 + a - 1)(a^2 + 3a + 1) + 1$$

is a product $m(m + 1)$ of two consecutive integers.

B-431 *Proposed by V. E. Hoggatt, Jr., San Jose State University, San Jose, CA.*

For which fixed ordered pairs (h, k) of integers does

$$F_n(L_{n+h}^2 - F_{n+h}^2) = F_{n+4}(L_{n+k}^2 - F_{n+k}^2)$$

for all integers n?

B-432 *Proposed by V. E. Hoggatt, Jr., San Jose State University, San Jose, CA.*

Let $G_n = F_n F_{n+3}^2 - F_{n+2}^3$. Prove that the terms of the sequence

$$G_0, G_1, G_2, \ldots$$

alternate in sign.

B-433 *Proposed by J. F. Peters and R. Pletcher, St. John's University, Collegeville, MN.*

For each positive integer n, let q_n and r_n be the integers with

$$n = 3q_n + r_n \quad \text{and} \quad 0 \leq r_n < 3.$$

Let $\{T(n)\}$ be defined by

$$T(0) = 1,\ T(1) = 3,\ T(2) = 4, \text{ and } T(n) = 4q_n + T(r_n) \text{ for } n \geq 3.$$

Show that there exist integers a, b, c such that

$$T(n) = \left[\frac{an + b}{c}\right],$$

where $[x]$ denotes the greatest integer in x.

B-434 *Proposed by Herta T. Freitag, Roanoke, VA.*

For which positive integers n, if any, is

$$L_{3n} - (-1)^n L_n$$

a perfect square?

B-435 *Proposed by M. Wachtel, H. Klauser, and E. Schmutz, Zürich, Switz.*

For every positive integer a, prove that no integral divisor of

$$a^2 + a - 1$$

is congruent to 3 or 7, modulo 10.

SOLUTIONS

First Term as GCD

B-406 *Proposed by Wray G. Brady, Slippery Rock State College, PA.*

Let $x_n = 4L_{3n} - L_n^3$ and find the greatest common divisor of the terms of the sequence $x_1, x_2, x_3, \ldots$.

Solution by Paul S. Bruckman, Concord, CA.

$$x_n = L_n(4L_{3n}/L_n - L_n^2) = L_n[4a^{2n} - 4(ab)^n + 4b^{2n} - a^{2n} - 2(ab)^n - b^{2n}]$$
$$= 3L_n[a^{2n} - 2(ab)^n + b^{2n}] = 3L_n(a^n - b^n)^2 = 15L_nF_n^2,$$

or

$$x_n = 15F_nF_{2n},\ n = 1, 2, 3, \ldots .$$

Note that $x_1 = 15F_1F_2 = 15$. Hence, $x_1 | x_n$, $n = 1, 2, 3, \ldots$. It follows that the greatest common divisor of $\{x_n\}$ is $x_1 = 15$.

Also solved by Herta T. Freitag, John W. Milsom, Bob Prielipp, E. Schmutz, A.G. Shannon, Sahib Singh, Lawrence Somer, M. Wachtel, Gregory Wulczyn, and the proposer.

Generator of Pascal Triangle

B-407 *Proposed by Robert M. Giuli, University of California, Santa Cruz, CA.*

Given that

$$\frac{1}{1 - x - xy} = \sum_{n=0}^{\infty} \sum_{k=0}^{\infty} a_{nk} x^n y^k$$

is a double ordinary generating function for a_{nk}; determine a_{nk}.

Solution by Paul S. Bruckman, Concord, CA.

$$(1 - x - xy)^{-1} = (1 - x(1 + y))^{-1} = \sum_{n=0}^{\infty} x^n(1 + y)^n = \sum_{n=0}^{\infty} x^n \sum_{k=0}^{n} \binom{n}{k} y^k$$
$$= \sum_{n=0}^{\infty} \sum_{k=0}^{n} \binom{n}{k} x^n y^k.$$

The binomial coefficient $\binom{n}{k}$ is defined to be zero for $k > n$. Hence, we may extend the second sum above over all nonnegative k, i.e.,

$$(1 - x - xy)^{-1} = \sum_{n=0}^{\infty} \sum_{k=0}^{\infty} \binom{n}{k} x^n y^k.$$

Thus,

$$a_{nk} = \binom{n}{k}, \ (n, k = 0, 1, 2, \ldots).$$

Also solved by W. O. J. Moser, A. G. Shannon, Sahib Singh, and the proposer.

Proposal Tabled

B-408 *No solutions received.*

Exact Divisor

B-409 *Proposed by Gregory Wulczyn, Bucknell University, Lewisburg, PA.*

Let $P_n = F_n F_{n+a}$. Must $P_{n+6r} - P_n$ be an integral multiple of

$$P_{n+4r} - P_{n+2r}$$

for all nonnegative integers a and r?

Solution by Sahib Singh, Clarion State College, Clarion, PA.

Yes. Using

$$L_n = a^n + b^n, \ F_n = \frac{a^n - b^n}{a - b},$$

we see that divisibility of

$$P_{n+6r} - P_n \text{ by } P_{n+4r} - P_{n+2r}$$

is equivalent to divisibility of

$$L_{2n+12r+a} - L_{2n+a} \text{ by } L_{2n+8r+a} - L_{2n+4r+a}.$$

The result follows immediatly by seeing that

$$L_{2n+12r+a} - L_{2n+a} = (L_{2n+8r+a} - L_{2n+4r+a})(L_{4r} + 1).$$

Also solved by Paul S. Bruckman, Bob Prielipp, and the proposer.

Golden Limit

B-410 *Proposed by M. Wachtel, Zürich, Switz.*

Some of the solutions of

$$5(x^2 + x) + 2 = y^2 + y$$

in positive integers x and y are:

$$(x, y) = (0, 1), (1, 3), (10, 23), (27, 61).$$

Find a recurrence formula for the x_n and y_n of a sequence of solutions (x_n, y_n). Also find $\lim(x_{n+1}/x_n)$ and $\lim(x_{n+2}/x_n)$ as $n \to \infty$ in terms of $a = (1 + \sqrt{5})/2$.

Solution by Paul S. Bruckman, Concord, CA.

Multiplying the given Diophantine equation throughout by 4, completing the square, and simplifying yields:

(1) $$Y^2 - 5X^2 = 4,$$

where

(2) $$X = 2x + 1, \ Y = 2y + 1.$$

The solutions of (1) in positive integers are known to be

(3) $$(X_m, Y_m) = (F_{2m}, L_{2m})_{m=0}^{\infty}.$$

However, due to (2), X and Y must also be odd. By inspection of the first few values (mod 3) of the Fibonacci and Lucas sequences, it is apparent that these values are even if and only if their subscripts are multiples of 3. Hence, we must have $m \equiv \pm 1 \pmod 3$ in (3). Distinguishing between these cases, we obtain two distinct sets of solutions:

(4) $$(X_m^{(1)}, Y_m^{(1)}) = (F_{6m+2}, L_{6m+2})_{m=0}^{\infty};$$

(5) $$(X_m^{(2)}, Y_m^{(2)}) = (F_{6m+4}, L_{6m+4})_{m=0}^{\infty}.$$

In terms of the original problem, this yields the following distinct solution sequences:

(6) $$(x_n^{(1)}, y_n^{(1)}) = \left\{\tfrac{1}{2}(F_{6n+2} - 1), \tfrac{1}{2}(L_{6n+2} - 1)\right\}_{n=0}^{\infty};$$

(7) $$(x_n^{(2)}, y_n^{(2)}) = \left\{\tfrac{1}{2}(F_{6n+4} - 1), \tfrac{1}{2}(L_{6n+4} - 1)\right\}_{n=0}^{\infty}.$$

It is apparent from the fact that the successive indices of the Fibonacci and Lucas sequences in (6) and (7) "increase by sixes," that we are interested in the second-order equation for a^6, which must be the same for b^6. Since $a^6 = 8a + 5$ and $a^{12} = 144a + 89$ (special cases of $a^r = aF_r + F_{r-1}$), it is evident that a and b satisfy the common equation:

(8) $$z^{12} - 18z^6 + 1 = 0.$$

Let

(9) $$D_n = z_{n+2} - 18z_{n+1} + z_n, \text{ where } z_n = x_n^{(k)} \text{ or } y_n^{(k)}, k = 1 \text{ or } 2.$$

We see from (6) and (7) that $D_n = \frac{1}{2}(-1 + 18 - 1)$ [using (8)], or

(10) $$D_n = 8, n = 0, 1, 2, \ldots .$$

This is a recursion for the $x_n^{(k)}$ and $y_n^{(k)}$, as required.

A *homogeneous* recursion may be obtained by noting simply that

$$D_{n+1} - D_n = 0.$$

This is equivalent to the following third-order recursion:

(11) $$z_{n+3} - 19z_{n+2} + 19z_{n+1} - z_n = 0, n = 0, 1, 2, \ldots .$$

It is evident from (6) and (7) that

(12) $$\lim_{n\to\infty} x_{n+1}^{(k)}/x_n^{(k)} = \lim_{n\to\infty} y_{n+1}^{(k)}/y_n^{(k)} = a^6,$$

and

(13) $$\lim_{n\to\infty} x_{n+2}^{(k)}/x_n^{(k)} = \lim_{n\to\infty} y_{n+2}^{(k)}/y_n^{(k)} = a^{12} \quad (k = 1 \text{ or } 2).$$

Also solved by the proposer.

Tridiagonal Determinants

B-411 *Proposed by Bart Rice, Crofton, MD.*

Tridiagonal n by n matrices $A_n = (a_{ij})$ of the form

$$a_{ij} = \begin{cases} 2a \ (a \text{ real}) & \text{for } j = i \\ 1 & \text{for } j = i \pm 1 \\ 0 & \text{otherwise} \end{cases}$$

occur in numerical analysis. Let $d_n = \det A_n$.

(i) Show that $\{d_n\}$ satisfies a second-order homogeneous linear recursion.

(ii) Find closed-form and asymptotic expressions for d_n.

(iii) Derive the combinatorial idantity

$$\sum_{k=0}^{[(n-1)/2]} \binom{n}{2k+1}(-x)^k = (x+1)^{(n-1)/2}\frac{\sin rn}{\sin r},\ x > 0,\ r = \tan^{-1}\sqrt{x}.$$

Solution by Paul S. Bruckman, Concord, CA.

We see that

$$(1)\qquad A_n = \begin{pmatrix} 2a & 1 & 0 & 0 & 0 & \cdots \\ 1 & 2a & 1 & 0 & 0 & \cdots \\ 0 & 1 & 2a & 1 & 0 & \cdots \\ 0 & 0 & 1 & 2a & 1 & \cdots \\ 0 & 0 & 0 & 1 & 2a & \cdots \\ 0 & 0 & 0 & 0 & 1 & \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \end{pmatrix}_{n \times n}$$

Taking determinants along the first row, we find that $d_n = 2ad_{n-1} - \det B_n$, where

$$B_n = \begin{pmatrix} 1 & 1 \quad 0 \quad 0 \quad \cdots \quad 0 \\ 0 & \\ 0 & \\ \vdots & \Bigg(\qquad A_{n-2} \qquad \Bigg) \\ 0 & \end{pmatrix}_{(n-1)\times(n-1)}$$

Taking the determinant of B_n along its first column, we see easily that det $B_n = d_{n-2}$. Hence, we have the following recursion:

$$(3)\qquad d_{n+2} - 2ad_{n+1} + d_n = 0,\ n = 1, 2, 3, \ldots .$$

Note also the initial values of the recursion:

$$(4)\qquad d_1 = 2a,\ d_2 = 4a^2 - 1.$$

The characteristic polynomial of (3) is

$$(b)\qquad p(x) = x^2 - 2ax + 1,$$

which has the zeros

$$(6)\qquad u = a + \sqrt{a^2 - 1},\ v = a - \sqrt{a^2 - 1}.$$

It follows that d_n is of the form $pu^n + qv^n$, for some constants p and q which are determined from the initial conditions. Note that

$$uv = 1,\ u + v = 2a.$$

We then find

$$(7)\qquad d = \frac{u^{n+1} - v^{n+1}}{u - v},\ n = 1, 2, 3, \ldots .$$

The behavior of d_n as $n \to \infty$ depends on the magnitude of a, and we distinguish several cases.

Case I: $0 \le |a| < 1$.

Let $a = \cos\theta$. Then $u = e^{i\theta}$, $v = e^{-i\theta}$, and so

$$(8)\qquad d_n = \sin(n+1)\theta/\sin\theta.$$

In this case, the sequence (d_n) is dense in

$$(-\csc\theta,\ \csc\theta) \equiv (-(1-a^2)^{-\frac{1}{2}},\ (1-a^2)^{-\frac{1}{2}})$$

and oscillates within this interval without lending itself to approximation by an asymptotic expression.

Case II: $a = -1$.

Then $u = v = -1$. Since

$$d_n = \sum_{k=0}^{n} u^{n-k}v^k,$$

thus

$$d_n = \sum_{k=0}^{n} (-1)^k = \tfrac{1}{2}(1 + (-1)^n) = \begin{cases} 1, & n \text{ even} \\ 0, & n \text{ odd} \end{cases}.$$

Clearly, d_n oscillates between these two values only, in this case.

Case III: $a = 1$.

Here $u = v = 1$. Hence,

$$d_n = \sum_{k=0}^{n} u^{n-k}v^k = \sum_{k=0}^{n} 1 = n + 1.$$

Therefore, for this case, $d_n \sim n$ as $n \to \infty$.

Case IV: $a < -1$.

Then $v < -1 < u < 0$, which implies $u^n \to 0$ as $n \to \infty$. Hence

$$d_n \sim \frac{v^{n+1}}{v - u} \text{ as } n \to \infty.$$

Case V: $a > 1$.

Then $0 < v < 1 < u$, which implies $v^n \to 0$ and $d_n \sim \dfrac{u^{n+1}}{u - v}$ as $n \to \infty$.

To prove the given combinatorial identity, note that

$$\begin{aligned} \tfrac{1}{2}(u - v)d_{n-1} = \tfrac{1}{2}(u^n - v^n) &= \tfrac{1}{2}\sum_{k=0}^{n}\binom{n}{k}a^{n-k}(a^2 - 1)^{\frac{1}{2}k}(1 - (-1)^k) \\ &= \sum_{k=0}^{[\frac{1}{2}(n-1)]}\binom{n}{2k+1}a^{n-2k-1}(a^2 - 1)^{k+\frac{1}{2}} \\ &= \tfrac{1}{2}(u - v)a^{n-1}\sum_{k=0}^{[\frac{1}{2}(n-1)]}\binom{n}{2k+1}\left(\frac{1 - a^2}{a^2}\right)^k(-1)^k, \text{ or} \end{aligned}$$

$$d_{n-1} = a^{n-1}\sum_{k=0}^{[\frac{1}{2}(n-1)]}\binom{n}{2k+1}\left(\frac{1 - a^2}{a^2}\right)^k(-1)^k. \tag{9}$$

In (9), let $x = a^{-2} - 1$, supposing Case I above, so that we can have $x > 0$. Then, since $r = \tan^{-1}\sqrt{x}$ is in $(0, \frac{1}{2}\pi)$,

$$r = \tan^{-1}\{(1 - a^2)^{\frac{1}{2}}/|a|\} = \cos^{-1}\{|a|\}.$$

Also, $\sin r = (1 - a^2)^{\frac{1}{2}}$. Using the notation of Case I, $r = \theta$ if $a > 0$ and

$r = \pi - \theta$ if $a < 0$. In either case, $\sin\theta = \sin r$. Thus, using (8),

$$d_{n-1} = \sin n\theta/\sin\theta = \begin{cases} \sin nr/\sin r, & \text{if } a > 0; \\ (-1)^{n-1}\sin nr/\sin r, & \text{if } a < 0. \end{cases}$$

Also, $a^2 = (1 + x)^{-1}$, which implies that

$$a^{n-1} = \begin{cases} (1 + x)^{-\frac{1}{2}(n-1)}, & a > 0; \\ (-1)^{n-1}(1 + x)^{-\frac{1}{2}(n-1)}, & a < 0. \end{cases}$$

In either case, it follows from (9) that

$$(1 + x)^{-\frac{1}{2}(n-1)} \sum_{k=0}^{[\frac{1}{2}(n-1)]} \binom{n}{2k + 1}(-x)^k = \sin rn/\sin r,$$

which is equivalent to the desired identity.

Also solved by the proposer.

*****

ADVANCED PROBLEMS AND SOLUTIONS

Edited by
RAYMOND E. WHITNEY
Lock Haven State College, Lock Haven, PA 17745

Send all communications concerning ADVANCED PROBLEMS AND SOLUTIONS to RAYMOND E. WHITNEY, Mathematics Department, Lock Haven State College, Lock Haven, PA 17745. This department especially welcomes problems believed to be new or extending old results. Proposers should submit solutions or other information that will assist the editor. To facilitate their consideration, solutions should be submitted on separate, signed sheets within two months after publication of the problems.

PROBLEMS PROPOSED IN THIS ISSUE

H-317 *Proposed by Lawrence Somer, Washington, D.C.*

Let $\{G_n\}_{n=0}^{\infty}$ be any generalized Fibonacci sequence such that

$$G_{n+2} = G_{n+1} + G_n, \ (G_0, G_1) = 1,$$

and $\{G_n\}$ is not a translation of the Fibonacci sequence. Show that there exists at least one prime p such that both

$$G_n + G_{n+1} \equiv G_{n+2} \pmod{p}$$

and

$$G_{n+1} \equiv rG_n \pmod{p}$$

for a fixed $r \not\equiv 0 \pmod{p}$ and for all $n \geq 0$.

H-318 *Proposed by James Propp, Harvard College, Cambridge, Mass.*

Define the sequence operator M so that for any infinite sequence $\{u_i\}$,

$$M(u_n) = M(u_n) - \sum_{i|n} M(u_i)\mu\left(\frac{n}{1}\right),$$

where is the Möbius function. Let the "Möbinacci Sequence" S be defined so that $S_1 = 1$ and

$$S_n = M(S_n) + M(M(S_n)), \text{ for } n > 1.$$

Find a formula for S_n in terms of the prime factorization of n.

H-319 *Proposed by Verner E. Hoggatt, Jr., San Jose State University, San Jose, CA.*

If $F_n < x < F_{n+1} < y < F_{n+2}$, then $x + y$ is never a Fibonacci number.

2 Corrected Problem Proposals

H-294 *Proposed by Gregory Wulczyn, Bucknell University, Lewisburg, PA.*

Evaluate

$$\Delta = \begin{vmatrix} F_{2r+1} & F_{6r+3} & F_{10r+5} & F_{14r+7} & F_{18r+9} \\ F_{4r+2} & -F_{12r+6} & F_{20r+10} & -F_{28r+14} & F_{36r+18} \\ F_{6r+3} & F_{18r+9} & F_{30r+15} & F_{42r+21} & F_{54r+27} \\ F_{8r+4} & -F_{24r+12} & F_{40r+20} & -F_{56r+28} & F_{72r+36} \\ F_{10r+5} & F_{30r+15} & F_{50r+25} & F_{70r+35} & F_{90r+45} \end{vmatrix}$$

H-295 *Proposed by G. Wulczyn, Bucknell University, Lewisburg, PA.*

Establish the identities:

(a) $F_kF^2_{k+6r+3} - F_{k+8r+4}F^2_{k+2r+1} = (-1)^{k+1}F^3_{2r+1}L_{2r+1}L_{k+4r+2}$;

(b) $F_kF^2_{k+6r} - F_{k+8r}F^2_{k+2r} = (-1)^{k+1}F^3_{2r}L_{2r}L_{k+4r}$.

SOLUTIONS

One or Five

H-285 *Proposed by V. E. Hoggatt, Jr., San Jose State University, San Jose, CA. (Vol. 16, No. 5, October 1978)*

Consider two sequences $\{H_n\}^{\infty}_{n=1}$ and $\{G_n\}^{\infty}_{n=1}$ such that

(a) $(H_n, H_{n+1}) = 1$,
(b) $(G_n, G_{n+1}) = 1$,
(c) $H_{n+2} = H_{n+1} + H_n$ $(n \geq 1)$, and
(d) $H_{n+1} + H_{n-1} = sG_n$ $(n \geq 1)$,
where s is independent of n.

Show $s = 1$ or $s = 5$.

Solution by Lawrence Somer, Washington, D.C.

The following examples from the Fibonacci and Lucas sequences show that s may actually attain both values of 1 and 5:

$$F_{n-1} + F_{n+1} = 1 \cdot L_n,\ L_{n-1} + L_{n+1} = 5F_n.$$

We are also evidently assuming that s is nonnegative. Otherwise, let

$$\{H_n\} = \{-F_n\} \text{ and } \{G_n\} = \{L_n\}.$$

Then $H_{n-1} + H_{n+1} = (-1)G_n$. Similarly, if

$$\{H_n\} = \{-L_n\} \text{ and } \{G_n\} = \{F_n\},$$

then $H_{n-1} + H_{n+1} = (-5)G_n$.

Now suppose that $s \neq 1$ or 5. Since $(H_n, H_{n+1}) = 1$ and $(G_n, G_{n+1}) = 1$, clearly $s \neq 0$. I claim that the period (mod s) of $\{H_n\}$ divides 4. This follows, since $H_1 + H_3 \equiv 0 \pmod{s}$ and $H_3 + H_5 \equiv 0 \pmod{s}$ together imply that $H_1 \equiv H_5 \pmod{s}$. Similarly, $H_2 \equiv H_6 \pmod{s}$.

Now, $H_1 + H_3 \equiv 0 \pmod{s}$ and $H_1 + H_2 \equiv H_3 \pmod{s}$ imply that $H_2 \equiv -2H_1$ (mod s). Thus, using the recursion relation for $\{H_n\}$, the first five terms of $\{H_n\}$ (mod s) are

$$H_1,\ H_2 \equiv -2H_1,\ H_3 \equiv -H_1,\ H_4 \equiv -3H_1, \text{ and } H_5 \equiv -4H_1.$$

Thus, $-4H_1 \equiv H_1$ or $5H_1 \equiv 0 \pmod{s}$. If $(5, s) = 1$, then $5H_1 \equiv 0 \pmod{s}$ implies that $H_1 \equiv 0 \pmod{s}$. But then $H_2 \equiv -2H_1 \equiv 0 \pmod{s}$ and $(H_1, H_2) \neq 1$. Hence, $s > 5$ and $(5, s) = 5$. However, then $5H_1 \equiv 0 \pmod{s}$ implies that $(s/5)|(H_1, s)$. But then since $H_2 \equiv -2H_1 \pmod{s}$ and a fortiori $H_2 \equiv -2H_1 \equiv 0$ (mod $s/5$), $(s/5)|H_2$ also. Therefore, $(s/5)|(H_1, H_2)$ and $(H_1, H_2) \neq 1$ as we assumed. Thus, $s = 1$ or 5.

Also solved by P. Bruckman and G. Lord.

Power Mod

H-286 *Proposed by P. Bruckman, Concord, CA. (Vol. 16, No. 5, October 1978)*

Prove the following congruences:

(1) $F_{5^n} \equiv 5^n \pmod{5^{n+3}}$;

(2) $F_{5^n} \equiv L_{5^{n+1}} \pmod{5^{2n+1}}$, $n = 0, 1, 2, \ldots$.

Solution by the proposer.

Proof of (1): We will use the following identity,

(3) $$F_{5m} = 25F_m^5 + 25(-1)^m F_m^3 + 5F_m, \; m = 0, 1, 2, \ldots .$$

Let S be the set of nonnegative integers n for which (1) holds. Since $F_5 = 5$, clearly $1 \in S$. Even more obviously, $F_1 = 1 = 5^0$, so $0 \in S$. Suppose $k \in S$, and let $m = 5^k$. Then, for some integer a, $F_m = m(1 + 125a)$. Hence, by (3),

$$\begin{aligned} F_{5m} &= 5^2m^5(1 + 5^3a)^5 - 5^2m^3(1 + 5^3a)^3 + 5m(1 + 5^3a) \\ &\equiv 5^2m^5 - 5^2m^3 + 5m \pmod{5^4m}. \end{aligned}$$

But $5^2 | m^2$, assuming k is positive. Hence, $5^4m | 5^2m^3 | 5^2m^5$. Thus, $F_{5m} \equiv 5m$ $\pmod{5^4m}$, i.e.,

$$F_{5^{k+1}} \equiv 5^{k+1} \pmod{5^{k+4}}.$$

Therefore, $k \in S \Rightarrow (k + 1) \in S$. The result of (1) now follows by induction.

Proof of (2): We will use the following identities,

$$\left.\begin{aligned} &(4) \qquad L_{5m} = L_m^5 - 5(-1)^m L_m^3 + 5L_m, \\ &(5) \qquad L_m^2 = 5F_m^2 + 4(-1)^m, \end{aligned}\right\} \; m = 0, 1, 2, \ldots .$$

Let $m = 5^n$. Then $L_{5m} - L_m = (L_m^3 + L_m)(L_m^2 + 4) = 5F_m^2(L_m^3 + L_m)$. But, by (1), $m | F_m$, which implies $5m^2 | 5F_m^2$. Therefore, $L_{5m} \equiv L_m \pmod{5m^2}$, i.e.,

$$L_{5^{n+1}} \equiv L_{5^n} \pmod{5^{2n+1}},$$

which proves (2).

More Identities

H-288 *Proposed by G. Wulczyn, Bucknell University, Lewisburg, PA. (Vol. 16, No. 5, October 1978)*

Establish the identities:

(a) $F_k L_{k+6r+3}^2 - F_{k+8r+4} L_{k+2r+1}^2 = (-1)^{k+1} L_{2r+1}^3 F_{2r+1} L_{k+4r+2}$;

(b) $F_k L_{k+6r}^2 - F_{k+8r} L_{k+2r}^2 = (-1)^{k+1} L_{2r}^3 F_{2r} L_{k+4r}$.

Solution by the Proposer

(a) $F_k L_{k+6r+3}^2 - F_{k+8r+4} L_{k+2r+1}^2 =$

$$\begin{aligned} &= \frac{1}{\sqrt{5}}\{(\alpha^k - \beta^k)[\alpha^{2k+12r+6} + \beta^{2k+12r+6} + 2(-1)^{k+1}] \\ &\qquad - (\alpha^{k+8r+4} - \beta^{k+8r+4})[\alpha^{2k+4r+2} + \beta^{2k+4r+2} + 2(-1)^{k+1}]\} \\ &= \frac{(-1)^{k+1}}{\sqrt{5}}\{\alpha^{k-4r-2}(\alpha^{16r+8} - 2\alpha^{12r+6} + 2\alpha^{4r+2} - 1) \\ &\qquad - \beta^{k-4r-2}(\beta^{16r+8} - 2\beta^{12r+6} + 2\beta^{4r+2} - 1)\} \\ &= \frac{(-1)^{k+1}}{\sqrt{5}}\{\alpha^{k-4r-2}(\alpha^{4r+2} - 1)(\alpha^{4r+2} + 1) - \beta^{k-4r-2}(\beta^{4r+2} - 1)(\beta^{4r+2} + 1)\} \\ &= \frac{(-1)^{k+1}}{\sqrt{5}}\{\alpha^{k+4r+2}(\alpha^{2r+1} + \beta^{2r+1})^3(\alpha^{2r+1} - \beta^{2r+1}) \\ &\qquad + \beta^{k+4r+2}(\alpha^{2r+1} + \beta^{2r+1})^3(\alpha^{2r+1} - \beta^{2r+1})\} \\ &= (-1)^{k+1} L_{2r+1}^3 F_{2r+1} L_{k+4r+2}. \end{aligned}$$

(b) $F_k L^2_{k+6r} - F_{k+8r} L^2_{k+2r}$

$$= F_k[L_{2k+12r} + 2(-1)^k] - F_{k+8r}[L_{2k+4r} + 2(-1)^k]$$

$$= \frac{(-1)^{k+1}}{\sqrt{5}}\{\alpha^{k-4r}(\alpha^{16r} + 2\alpha^{12r} - 2\alpha^{4r} - 1) - \beta^{k-4r}(\beta^{16r} + 2\beta^{12r} - 2\beta^{4r} - 1)\}$$

$$= \frac{(-1)^{k+1}}{\sqrt{5}}\{\alpha^{k-4r}(\alpha^{4r} - 1)(\alpha^{4r} + 1)^3 - \beta^{k-4r}(\beta^{4r} - 1)(\beta^{4r} + 1)^3\}$$

$$= \frac{(-1)^{k+1}}{\sqrt{5}}\{\alpha^{k+4r}(\alpha^{2r} - \beta^{2r})(\alpha^{2r} + \beta^{2r})^3 + \beta^{k+4r}(\alpha^{2r} - \beta^{2r})(\alpha^{2r} + \beta^{2r})^3\}$$

$$= (-1)^{k+1}F_{2r}L^3_{2r}L_{k+4r}.$$

Also solved by P. Bruckman.

Series Consideration

H-289 *Proposed by L. Carlitz, Duke University, Durham, N.C.*
(Vol. 16, No. 5, October 1978)

Put the multinomial coefficient

$$(m_1, m_2, \ldots, m_k) = \frac{(m_1 + m_2 + \cdots + m_k)!}{m_1!m_2! \ldots m_k!}.$$

Show that

$$(*) \quad \sum_{r+s+t=\lambda} (r, s, t)(m - 2r, n - 2s, p - 2t)$$

$$= \sum_{i+j+k+u=\lambda} (-2)^{i+j+k}(i, j, k, u)(m - j - k, n - k - i, p - i - j) \quad (m+n+p \geq 2\lambda).$$

Solution by Paul Bruckman, Concord, CA.

Let

$$(1) \qquad A(m, n, p) = \sum_{r+s+t=\lambda} (r, s, t)(m - 2r, n - 2s, p - 2t),$$

$$(2) \qquad B(m, n, p) = \sum_{i+j+k+u=\lambda} (-2)^{i+j+k}(i, j, k, u)(m - j - k, n - k - i, p - i - j).$$

Also, let

$$(3) \qquad F(x, y, z) = \sum_{m+n+p\geq 2\lambda} A(m, n, p)x^m y^n z^p,$$

$$(4) \qquad G(x, y, z) = \sum_{m+n+p\geq 2\lambda} B(m, n, p)x^m y^n z^p,$$

assuming λ is fixed. It will suffice to show that F and G are identical functions, for then the desired result would follow by comparing coefficients.

Now

$$\begin{aligned} F(x, y, z) &= \sum_{r+s+t=\lambda} (r, s, t) \sum_{m+n+p \geq 2\lambda} (m - 2r, n - 2s, p - 2t)x^m y^n z^p \\ &= \sum_{r+s+t=\lambda} (r, s, t) \sum_{m \geq 2r, n \geq 2s, p \geq 2t} (m - 2r, n - 2s, p - 2t)x^m y^n z^p \\ &= \sum_{r+s+t=\lambda} (r, s, t)x^{2r}y^{2s}z^{2t} \sum_{m,n,p \geq 0} (m, n, p)x^m y^n z^p. \end{aligned}$$

Now

$$\begin{aligned} \sum_{m,n,p \geq 0} (m, n, p)x^m y^n z^p &= \sum_{k=0}^{\infty} \sum_{m+n+p=k} (m, n, p)x^m y^n z^p \\ &= \sum_{k=0}^{\infty} (x + y + z)^k = (1 - x - y - z)^{-1}. \end{aligned}$$

Hence,

$$F(x, y, z) = (1 - x - y - z)^{-1} \sum_{r+s+t=\lambda} (r, s, t)x^{2r}y^{2s}z^{2t},$$

or

$$F(x, y, z) = (x^2 + y^2 + z^2)^{\lambda}(1 - x - y - z)^{-1}. \tag{5}$$

Also,

$$\begin{aligned} G(x, y, z) = &\sum_{i+j+k+u=\lambda} (-2)^{i+j+k}(i, j, k, u) \\ &\cdot \sum_{m+n+p \geq 2\lambda} (m - j - k, n - k - i, p - i - j)x^m y^n z^p. \end{aligned}$$

The condition $m + n + p \geq 2\lambda$ is equivalent to

$$(m - j - k) + (n - k - i) + (p - i - j) \geq 2(\lambda - i - j - k) = 2u.$$

Hence,

$$\begin{aligned} G(x, y\ \ z) &= \sum_{i+j+k+u=\lambda} (-2)^{i+j+k}(i, j, k, u)\, x^{j+k}y^{k+i}z^{i+j} \\ &\quad \cdot \sum_{m+n+p \geq 2u} (m, n, p)x^m y^n z^p \\ &= \sum_{i+j+k+u=\lambda} (-2)^{i+j+k}(i, j, k, u)x^{j+k}y^{k+i}z^{i+j} \\ &\quad \cdot \sum_{h=2u}^{\infty} \sum_{m+n+p=h} (m, n, p)x^m y^n z^p \\ &= \sum_{i+j+k+u=\lambda} (-2)^{i+j+k}(i, j, k, u)x^{j+k}y^{k+i}z^{i+j}\sum_{h=2u}^{\infty} (x+y+z)^h \\ &= (1 - x - y - z)^{-1} \sum_{i+j+k+u=\lambda} (-2)^{i+j+k} \\ &\quad \cdot (i, j, k, u)x^{j+k}y^{k+i}z^{i+j}(x + y + z)^{2u} \end{aligned}$$

$$= (1 - x - y - z)^{-1} \sum_{i+j+k+u=\lambda} (-2yz)^i (-2xz)^j (-2xy)^k (x + y + z)^{2u} (i,\ j,\ k,\ u)$$

$$= (1 - x - y - z)^{-1}\{-2yz - 2xz - 2xy + (x + y + z)^2\}^\lambda$$

$$= (1 - x - y - z)^{-1}(x^2 + y^2 + z^2)^\lambda = F(x,\ y,\ z). \quad \text{Q.E.D.}$$

Also solved by the proposer.

Identical

H-290 *Proposed by Gregory Wulczyn, Bucknell University, Lewisburg, PA. (Vol. 16, No. 6, December 1978)*

Show that

(a) $F_k F^2_{k+6r+3} - F^3_{k+4r+2} = (-1)^{k+1} F^2_{2r+1}(F_{k+8r+4} - 2F_{k+4r+2});$

(b) $F_k F^2_{k+6r} - F^3_{k+4r} = (-1)^{k+1} F^2_{2r}(F_{k+8r} + 2F_{k+4r}).$

Solution by the proposer.

(a) $F_k F^2_{k+6r+3} - F^3_{k+4r+2}$

$$= \frac{1}{5\sqrt{5}}\{(\alpha^k - \beta^k)[\alpha^{2k+2r+6} + \beta^{2k+2r+6} + 2(-1)^k] - [\alpha^{3k+2r+6} - \beta^{3k+2r+6} + 3(-1)^{k+1}]\}$$

$$= \frac{(-1)^{k+1}}{5\sqrt{5}}\{\alpha^k(\alpha^{12r+6} - 3\alpha^{4r+2} - 2) - \beta^k(\beta^{12r+6} - 3\beta^{4r+2} - 2)\}$$

$$= \frac{(-1)^{k+1}}{5\sqrt{5}}\{\alpha^k(\alpha^{4r+2} + 1)^2(\alpha^{4r+2} - 2) - \beta^k(\beta^{4r+2} + 1)(\alpha^{4r+2} - 2)\}$$

$$= \frac{(-1)^{k+1}}{5\sqrt{5}}\{\alpha^{k+4r+2}(\alpha^{2r+1} - \beta^{2r+1})^2(\alpha^{4r+2} - 2) - \beta^{k+4r+2}(\alpha^{2r+1} - \beta^{2r+1})^2(\beta^{4r+2} - 2)\}$$

$$= (-1)^{k+1}F^2_{2r+1}(F_{k+8r+4} - 2F_{k+4r+2}).$$

(b) $F_k F^2_{k+6r} - F^3_{k+4r}$

$$= \frac{1}{5\sqrt{5}}\{(\alpha^k - \beta^k)[\alpha^{2k+12r} + \beta^{2k+12r} + 2(-1)^{k+1}]$$
$$- [\alpha^{3k+12r} - \beta^{3k+12r} + 3(-1)^{k+1}(\alpha^{k+4r} - \beta^{k+4r})]\}$$

$$= \frac{(-1)^{k+1}}{5\sqrt{5}}\{\alpha^k(\alpha^{12r} - 3\alpha^{4r} + 2) - \beta^k(\beta^{12r} - 3\beta^{4r} + 2)\}$$

$$= \frac{(-1)^{k+1}}{5\sqrt{5}}\{\alpha^k(\alpha^{4r} - 1)^2(\alpha^{4r} + 2) - \beta^k(\beta^{4r} - 1)(\beta^{4r} + 2)\}$$

$$= \frac{(-1)^{k+1}}{5\sqrt{5}}\{\alpha^{k+4r}(\alpha^{2r} - \beta^{2r})^2(\alpha^{4r} + 2) - \beta^{k+4r}(\alpha^{2r} - \beta^{2r})^2(\beta^{4r} + 2)\}$$

$$= (-1)^{k+1}F^2_{2r}(F_{k+8r} + 2F_{k+4r})$$

Also solved by P. Bruckman.

Square Your Cubes

H-291 *Proposed by George Berzsenyi, Lamar University, Beaumont, TX. (Vol. 16, No. 6, December 1978)*

Prove that there are infinitely many squares which are differences of consecutive cubes.

Solution by Bob Prielipp, University of Wisconsin-Oshkosh, WI.

Clearly, it suffices to show that the equation $(x + 1)^3 - x^3 = y^2$ has infinitely many solutions (x, y) where x and y are positive integers. But the preceding equation is equivalent to $(2y)^2 - 3(2x + 1)^2 = 1$. Hence, we need only determine the solutions of the Pell's equation $u^2 - 3v^2 = 1$ in positive integers u, v such that u is even and v is odd. Its least solution in positive integers is $u_0 = 2$, $v_0 = 1$. Thus, all of its positive integer solutions are contained in the infinite sequence (u_k, v_k), $k = 1, 2, \ldots$, where

$$u_{k+1} = 2u_k + 3v_k \quad \text{and} \quad v_{k+1} = u_k + 2v_k,\ k = 0, 1, 2, \ldots .$$

[The preceding is an immediate consequence of the following result which is generally established as part of the theory involving Pell's equation: All of the solutions of the equation $u^2 - Dv^2 = 1$ in positive integers are contained in the infinite sequence

$$(u_0, v_0), (u_1, v_1), (u_2, v_2), \ldots,$$

where (u_0, v_0) is the least positive integer solution and (u_k, v_k) is defined inductively by $u_{k+1} = u_0u_k + Dv_0v_k$, $v_{k+1} = v_0u_k + u_0v_k$, $k = 1, 2, \ldots$.]

It is easily seen that, if u_k is even and v_k is odd, then u_{k+1} is odd and v_{k+1} is even. Also, if u_k is odd and v_k is even, then u_{k+1} is even and v_{k+1} is odd. This implies that all of the solutions of the equation

$$u^2 - 3v^2 = 1$$

in positive integers u, v with u even and v odd are (u_{2k}, v_{2k}) where $k = 0, 1, 2, \ldots$. Therefore, the equation $(x + 1)^3 - x^3 = y^2$ has infinitely many positive integer solutions.

Also solved by H. Klauser, P. Bruckman, E. Starke, L. Somer, G. Wulczyn, W. Brady, S. Singh, G. Chainbus, and the proposer.

Get the Point

H-292 *Proposed by F. S. Cater and J. Daily, Portland State University, Portland, OR. (Vol. 16, No. 6, December 1978).*

Find all real numbers $r \in (0, 1)$ for which there exists a one-to-one function f_r mapping $(0, 1)$ onto $(0, 1)$ such that

(1) f_r and f_r^{-1} are infinitely many times differentiable on $(0,1)$, and

(2) the sequence of functions

$$f_r,\ f_r \circ f_r,\ f_r \circ f_r \circ f_r,\ f_r \circ f_r \circ f_r \circ f_r,\ \ldots$$

converges pointwise to r on $(0, 1)$.

Solution by the proposers.

Let q denote the golden ratio $\frac{1}{2}(-1 + \sqrt{5})$, let $f(x) = 1 - (1 - x^2)^2$ and $g(x) = f(x) - x$. Then $f(q) - q = g(q) = 0$ by inspection and $g''(x) = -12x^2 + 4$

changes sign once in $(0, 1)$, from positive to negative. Since $g(0) = g(1) = 0$, it follows that $g(x) < 0$ for $0 < x < q$ and $g(x) > 0$ for $q < x < 1$. Also f and f^{-1} are evidently increasing on $(0, 1)$, so for any $x \in (0, q)$,

$$x < f^{-1}(x) < (f^{-1} \circ f^{-1})(x) < (f^{-1} \circ f^{-1} \circ f^{-1})(x) < \cdots < q,$$

and for $x \in (q, 1)$,

$$x > f^{-1}(x) > (f^{-1} \circ f^{-1})(x) > (f^{-1} \circ f^{-1} \circ f^{-1})(x) > \cdots > q.$$

In either case, this sequence converges to some point $w \in (0, 1)$. Since f^{-1} is continuous at w, $f^{-1}(w) = w$. But q is the only fixed point of f and of f^{-1} in $(0, 1)$, so $w = q$. Thus,

$$f^{-1},\ f^{-1} \circ f^{-1},\ f^{-1} \circ f^{-1} \circ f^{-1},\ \ldots$$

converges pointwise to q on $(0, 1)$. Also,

$$f^{-1}(x) = (1 - (1 - x)^{\frac{1}{2}})^{\frac{1}{2}},$$

so f and f^{-1} are both infinitely many times differentiable on $(0, 1)$. More generally, put $t = (\log q)/(\log r)$. Then, $f_r(x) = (f^{-1}(x^t))^{1/t}$ satisfies (1) and (2). Thus, all numbers $r \in (0, 1)$ satisfy the requirements of the problem.

Remark: Functions similar to f_r given here were studies by R. I. Jewett, in "A Variation on the Weierstrass Theorem," *PAMS* 14 (1963):690.

The Old Hermite

H-293 *Proposed by Leonard Carlitz, Duke University, Durham, N.C.*
(Vol. 16, No. 6, December 1978)

It is known that the Hermite polynomials $\{H_n(x)\}_{n=0}^{\infty}$ defined by

$$\sum_{n=0}^{\infty} H_n(x)\frac{z^n}{n!} = e^{2xz - z^2}$$

satisfy the relation

$$\sum_{n=0}^{\infty} H_{n+k}(x)\frac{z^n}{n!} = e^{2xz - z^2} H_k(x - z), \quad (k = 0, 1, 2, \ldots).$$

Show that, conversely, if a set of polynomials $\{f_n(x)\}_{n=0}^{\infty}$ satisfy

$$(1) \qquad \sum_{n=0}^{\infty} f_{n+k}(x)\frac{z^n}{n!} = \sum_{n=0}^{\infty} f_n(x)\frac{z^n}{n!}f_k(x - z), \quad (k = 0, 1, 2, \ldots),$$

where $f_0(x) = 1$, $f_1(x) = 2x$, then

$$f_n(x) = H_n(x), \quad (n = 0, 1, 2, \ldots).$$

Solution by Paul F. Byrd, San Jose State University, San Jose, CA.

Let

$$(1) \qquad G(x, z) = \sum_{n=0}^{\infty} f_n(x)\frac{z^n}{n!},$$

$$\left[G(x, 0) = f_0(x) = 1, \left.\frac{\partial G}{\partial z}\right|_{z=0} = f_1(x) = 2x\right],$$

denote the generating function for the set of polynomials $\{f_n(x)\}$. Then the given relation can be written as

$$(2)\qquad \sum_{n=0}^{\infty} f_{n+k}(x)\frac{z^n}{n!} = G(x,\ z)f_k(x - z),\ (k = 0,\ 1,\ 2,\ \ldots).$$

Multiplying this by $u^k/k!$ and summing yields

$$(3)\qquad \sum_{k=0}^{\infty}\sum_{n=0}^{\infty} f_{n+k}(x)\frac{z^n u^k}{n!k!} = G(x,\ z)\sum_{k=0}^{\infty} f_k(x - z)\frac{u^k}{k!}.$$

Now with the use of Cauchy's product rule, the lefthand side of (3) becomes

$$(4)\qquad \sum_{k=0}^{\infty}\sum_{n=0}^{\infty} f_{n+k}(x)\frac{z^n u^k}{n!k!} = \sum_{n=0}^{\infty} f_n(x)\sum_{k=0}^{n}\frac{z^{n-k}u^k}{k!(n-k)!}$$

$$= \sum_{n=0}^{\infty} f_n(x)\frac{(z+u)^n}{n!} = G(x,\ z + u).$$

But the righthand side of (3) is clearly equal to $G(x, z)G(x - z, u)$. Thus, from (3) and (4), we have the functional equation

$$(5)\qquad G(x,\ z + u) = G(x,\ z)G(x - z,\ u)$$

whose unique solution is

$$(6)\qquad G(x,\ z) = e^{2xz - z^2},\ \text{(for any value of } u\text{)}.$$

But, this is precisely the same well-known generating function for the Hermite polynomials $H_n(x)$. Hence,

$$(7)\qquad e^{2xz - z^2} = \sum_{n=0}^{\infty} f_n(x)\frac{z^n}{n!},$$

and it follows from Taylor's theorem that

$$(8)\qquad f_n(x) = e^{x^2}\left[\frac{\partial^n}{\partial z^n}e^{-(x-z)^2}\right]_{z=0} = (-1)^n e^{x^2}\cdot\frac{d^n}{dx^n}(e^{x^2}) = H_n(x),$$

with $f_0(x) = 1 = H_0(x)$, $f_1(x) = 2x = H_1(x)$.

Also solved by P. Bruckman, T. Shannon, and the proposer.

*****