SOME FORMULAE FOR THE FIBONACCI SEQUENCE WITH GENERALIZATIONS

GEORGE H. ANDREWS
Pennsylvania State University, University Park, Pa.

1. INTRODUCTION

In this paper we shall study the following formulae for the Fibonacci numbers.

$$(1.1) \qquad F_n = \sum_{{}^{\alpha\nearrow} n=-\infty}^{\infty} (-1)^{\alpha} \binom{n-1}{[\frac{1}{2}(n - 1 - 5\alpha)]} \quad ,$$

$$(1.2) \qquad = \sum_{\alpha=-\infty}^{\infty} (-1)^{\alpha} \binom{n}{[\frac{1}{2}(n - 1 - 5\alpha)]} \quad .$$

where $\binom{m}{n}$ is the ordinary binomial coefficient, and $[x]$ is the greatest integer function.

In Section 2, we shall prove these formulae and shall show how directly they imply the following famous congruences [4; p. 150].

$$(1.3) \qquad F_{p-\left(\frac{5}{p}\right)} \equiv 0 \pmod{p} \quad ,$$

$$(1.4) \qquad F_p \equiv \left(\frac{5}{p}\right) \pmod{p},$$

where $\left(\frac{5}{p}\right)$ is the Jacobi-Legendre symbol.

Chapter IV of Dickson's History, Vol. 1 [2; pp. 105-112] is devoted to studying $(u^{p-1} - 1)/p \pmod{p}$. In particular, Einstein made several contributions to this problem among which was the following. If $p \neq 2$,

$$(2^{p-1} - 1)/p \equiv 1 + 1/3 + 1/5 + \cdots + 1/p - 2 \pmod{p} \; .$$

*Partially supported by National Science Foundation Grant GP 6663.

We shall prove analogous formulae for

$$F_{p-\left(\frac{5}{p}\right)}\Big/p$$

and

$$\left(F_p - \left(\frac{5}{p}\right)\right)\Big/p$$

in Section 3. Namely, if $p \equiv \pm 2 \pmod 5$,

$$(1.5) \qquad F_{p+1}\big/p \equiv 2(-1)^{\frac{1}{2}(p-1)} \sum_{\substack{m\equiv 1,5 \pmod{10} \\ |m|<p}} \frac{\left(\frac{m+1}{5}\right)\left(\frac{-1}{m}\right)}{p-m} \pmod p .$$

If $p \equiv \pm 1 \pmod 5$,

$$(1.6) \qquad F_{p-1}\big/p \equiv 2(-1)^{\frac{1}{2}(p-1)} \sum_{\substack{m\equiv 5,7 \pmod{10} \\ |m|<p}} \frac{\left(\frac{m+1}{5}\right)\left(\frac{-1}{m}\right)}{p-m} \pmod p .$$

For all primes p,

$$(1.7) \qquad \left(F_p - \left(\frac{5}{p}\right)\right)\Big/p \equiv 2(-1)^{\frac{1}{2}(p-1)} \sum_{\substack{m\equiv 1,7 \pmod{10} \\ |m|<p}} \frac{\left(\frac{m+2}{5}\right)\left(\frac{-1}{m}\right)}{p-m} \pmod p.$$

In Section 4, we make the natural generalization of (1.1) and (1.2) by replacing 5 by an arbitrary odd number. This leads us immediately to an n-dimensional analog of the Fibonacci numbers which is closely related to one considered by Raney.

In Section 5, we point out an application of these generalized sequences to the factorization of large numbers, and in Section 6, we discuss related sequences.

2. THE NEW FORMULAE

Let us define

$$F_n(b) = \sum_{\alpha=-\infty}^{\infty} (-1)^{\alpha} \binom{n}{[\frac{1}{2}(n - b - 5\alpha)]} \quad .$$

Then if $\beta = \exp(2\pi i/5)$,

$$F_n(b) = (-1)^b \sum_{\alpha=-\infty}^{\infty} (-1)^{5\alpha+\beta} \binom{n}{[\frac{1}{2}(n - b - 5\alpha)]}$$

$$= \frac{(-1)^b}{5} \sum_{j=0}^{4} \sum_{\alpha=-\infty}^{\infty} (-1)^{\alpha} B^{j(\alpha-b)} \binom{n}{[\frac{1}{2}(n - \alpha)]}$$

$$= \frac{(-1)^{b+n}}{5} \sum_{j=0}^{4} \beta^{-jb} \sum_{\alpha=-\infty}^{\infty} (-1)^{\alpha} \beta^{j(-\alpha+n)} \binom{n}{[\frac{1}{2}\alpha]}$$

$$= \frac{(-1)^{b+n}}{5} \sum_{j=0}^{4} \beta^{j(n-b)} \left\{ \sum_{\alpha=-\infty}^{\infty} \beta^{-2j\alpha} \binom{n}{\alpha} \right.$$

$$\left. - \beta^{-j} \sum_{\alpha=-\infty}^{\infty} \beta^{-2j\alpha} \binom{n}{\alpha} \right\}$$

$$= \frac{(-1)^{b+n}}{5} \sum_{j=0}^{4} \beta^{j(n-b)} (1 - \beta^{-j})(1 + \beta^{-2j})^n$$

$$= \frac{(-1)^b}{5} \sum_{j=1}^{4} \beta^{-jb} (1 - \beta^{-j})(-2 \cos 2\pi j/5)^n$$

$$= \frac{(-1)^b}{5} \sum_{j=1}^{2} (\beta^{-jb} + \beta^{jb} - \beta^{-j(b+1)} - \beta^{j(b+1)}) \times$$
$$\times (-2 \cos 2\pi j/5)^n$$

$$= \frac{2(-1)^b}{5} \sum_{j=1}^{2} (\cos 2\pi jb/5 - \cos 2\pi j(b + 1)/5) \times$$
$$\times (-2 \cos 2\pi j/5)^n \quad .$$

Now

$$-2 \cos 2\pi/5 = -2 \cos 8\pi/5 = \tfrac{1}{2}(1 - 5^{\frac{1}{2}}) ,$$

and

$$-2 \cos 4\pi/5 = -2 \cos 6\pi/5 = \tfrac{1}{2}(1 + 5^{\frac{1}{2}}) .$$

Hence

$$\begin{aligned} F_n(0) &= \frac{1}{5}(2 + \frac{1}{2}(1 - 5^{\frac{1}{2}})(\tfrac{1}{2}(1 - 5^{\frac{1}{2}}))^n + \frac{1}{5}(2 + \frac{1}{2}(1 + 5^{\frac{1}{2}}))(\tfrac{1}{2}(1 + 5^{\frac{1}{2}}))^n \\ &= 5^{-\frac{1}{2}}((\tfrac{1}{2}(1 + 5^{\frac{1}{2}}))^{n+1} - (\tfrac{1}{2}(1 - 5^{\frac{1}{2}}))^{n+1}) \\ &= F_{n+1}, \text{ the } (n+1)^{st} \text{ Fibonacci number } [4;\ p.\ 148] . \end{aligned}$$

$$\begin{aligned} F_n(1) &= -\frac{1}{5}(-\tfrac{1}{2}(1 - 5^{\frac{1}{2}}) + \tfrac{1}{2}(1 + 5^{\frac{1}{2}}))(\tfrac{1}{2}(1 - 5^{\frac{1}{2}}))^n \\ &\qquad - \frac{1}{5}(-\tfrac{1}{2}(1 + 5^{\frac{1}{2}}) + \tfrac{1}{2}(1 - 5^{\frac{1}{2}}))(\tfrac{1}{2}(1 + 5^{\frac{1}{2}}))^n \\ &= 5^{-\frac{1}{2}}((\tfrac{1}{2}(1 + 5^{\frac{1}{2}}))^n - (\tfrac{1}{2}(1 - 5^{\frac{1}{2}}))^n) \\ &= F_n, \text{ the } n^{th} \text{ Fibonacci number } [4;\ p.\ 148] . \end{aligned}$$

Thus we have (1.1) and (1.2).

We now turn our attention to proving (1.3) and (1.4) utilizing (1.1) and (1.2). Our proof rests on the following elementary congruence

$$(2.1) \qquad \binom{p}{a} \equiv \begin{cases} 1 & \text{if } a = 0, p \\ 0 & \text{otherwise} \end{cases} \pmod{p} ,$$

where p is any prime.

If $p = 5m \pm 2$, then for any integer α,

$$[\tfrac{1}{2}(p - 5\alpha)] \neq 0, p ;$$

therefore by (2.1) p divides every term of the sum in (1.1) with $n = p + 1$, and (1.3) is established in this case. Utilizing (1.2) with $n = p = 5m \pm 2$, we may verify that (1.4) holds in this case. If

$$n - 1 = p = 5m \pm 1 ,$$

then by means of (1.1) we verify that

$$F_{p+1} \equiv -1 \pmod{p},$$

and by means of (1.2) with

$$n = p = 5m \pm 1$$

we verify that $F_p \equiv 1 \pmod{p}$. Thus we have completely established (1.4) with $p \neq 5$, and

$$F_{p-1} = F_{p+1} - F_p \equiv -1 + 1 \equiv 0 \pmod{p}$$

establishes completely (1.3) with $p \neq 5$. Finally since $F_5 = 5$ we have (1.3) and (1.4) proved in this exceptional case as well.

3. EINSTEIN FORMULAE FOR F_n.

This section is devoted to proving (1.5), (1.6), and (1.7). We shall utilize the following congruence

$$\text{(3.1)} \qquad p^{-1}\binom{p}{a} \equiv -(-1)^a a^{-1} \pmod{p}, \quad 0 < a < p$$

In the following sums, we note that the only terms to be considered are those for which initially the lower entry of the binomial coefficient is in the open interval (0,p). We shall thus not trouble to indicate the range of summation until the final line in each case.

From (1.1) with $n - 1 = p = 2m + 1$,

$$\text{(3.2)} \quad F_{2m+2} = \sum_{\alpha=-\infty}^{\infty} (-1)^{\alpha} \binom{p}{[\frac{1}{2}(2m + 1 - 5\alpha)]} = \sum_{\alpha=-\infty}^{\infty} \left\{ \binom{p}{m - 5\alpha} - \binom{p}{m - 2 - 5\alpha} \right\}.$$

Hence

$$F_{p+1}/p \equiv \sum \left\{ \frac{-(-1)^{m+\alpha}}{m - 5\alpha} + \frac{(-1)^{m+\alpha}}{m - 5\alpha - 2} \right\} \pmod{p}$$

$$\equiv 2(-1)^{\frac{1}{2}(p-1)} \sum \left\{ \frac{(-1)^{\alpha+1}}{p - 1 - 10\alpha} + \frac{(-1)^{\alpha}}{p - 5 - 10\alpha} \right\} \pmod{p}$$

$$\equiv 2(-1)^{\frac{1}{2}(p-1)} \sum_{\substack{m \equiv 1,5 \pmod{10} \\ |m| < p}} \frac{\left(\frac{m+1}{5}\right)\left(\frac{-1}{m}\right)}{p - m} \pmod{p} .$$

From (1.2) with $n = p = 2m + 1$,

$$(3.3) \qquad F_{2m+1} = \sum_{\alpha=-\infty}^{\infty} (-1)^{\alpha} \binom{p}{\frac{1}{2}(2m - 5\alpha)} = \sum_{\alpha=-\infty}^{\infty} \left\{ \binom{p}{m - 5\alpha} - \binom{p}{m - 3 - 5\alpha} \right\} .$$

Therefore if p is a prime $\equiv \pm 1 \pmod 5$, we have by (3.2) and (3.3)

$$(3.4) \qquad F_{p-1} = F_{p+1} - F_p = \sum_{\alpha=-\infty}^{\infty} \left\{ \binom{p}{m - 3 - 5\alpha} - \binom{p}{m - 2 - 5\alpha} \right\} .$$

Hence from (3.4) with $p \equiv \pm 1 \pmod 5$,

$$F_{p-1}/p \equiv \sum_{\alpha=-\infty}^{\infty} \left\{ \frac{(-1)^{m+\alpha}}{m - 3 - 5\alpha} + \frac{(-1)^{m+\alpha}}{m - 2 - 5\alpha} \right\} \pmod{p}$$

$$\equiv 2(-1)^{\frac{1}{2}(p-1)} \sum \left\{ \frac{(-1)^{\alpha}}{p - 7 - 10\alpha} + \frac{(-1)^{\alpha}}{p - 5 - 10\alpha} \right\} \pmod{p}$$

$$\equiv 2(-1)^{\frac{1}{2}(p-1)} \sum_{\substack{m \equiv 5,7 \pmod{10} \\ |m| < p}} \frac{\left(\frac{m+1}{5}\right)\left(\frac{-1}{m}\right)}{p - m} \pmod{p} .$$

Finally from (3.3) with $p = 2m + 1$

$$\left(F_p - \left(\frac{5}{p}\right)\right)/p \equiv -\sum\left\{\frac{(-1)^{m+\alpha}}{m - 5\alpha} + \frac{(-1)^{m+\alpha}}{m - 3 - 5\alpha}\right\} \pmod{p}$$

$$\equiv -2(-1)^{\frac{1}{2}(p-1)}\sum\left\{\frac{(-1)^{\alpha}}{p - 1 - 10\alpha} + \frac{(-1)^{\alpha}}{p - 7 - 10\alpha}\right\} \pmod{p}$$

$$\equiv 2(-1)^{\frac{1}{2}(p-1)} \sum_{\substack{m \equiv 1,7 \pmod{10} \\ |m|<p}} \frac{\left(\frac{m+2}{5}\right)\left(\frac{-1}{m}\right)}{p - m} \pmod{p} .$$

Thus we have established (1.5), (1.6), and (1.7).

Let us now consider a specific example. By (1.1)

$$F_{14} = \binom{13}{6} - \binom{13}{4} - \binom{13}{9} + \binom{13}{1} + \binom{13}{11} = 1716 - 715 - 715 + 13 + 78 = 377$$

By (1.3),

$$F_{14}/13 \equiv 2\left\{\frac{1}{13 - 11} + \frac{1}{13 - 5} - \frac{1}{13 - 1} - \frac{1}{13 + 5} + \frac{1}{13 + 9}\right\}$$
$$\equiv 1 + 1/4 - 1/6 - 1/9 + 1/11 \equiv 1 + 10 - 11 - 3 + 6 \equiv 3 \pmod{13},$$

and indeed,

$$F_{14}/13 = 29 \equiv 3 \pmod{13} .$$

4. GENERALIZATIONS

In this section we discuss the natural generalization of (1.1) and (1.2). We define

$$(4.1) \qquad F_{k,n}(b) = \sum_{\alpha=-\infty}^{\infty} (-1)^{\alpha} \binom{n}{\frac{1}{2}[n - b - (2k + 1)\alpha)]} .$$

Exactly as in Section 2, only now setting

$$\beta = \exp(2\pi i/2k+1) ,$$

we obtain

$$(4.2) \qquad F_{k,n}(b) = \frac{2(-1)^b}{2k+1}\sum_{j=1}^{k}(\cos(2\pi bj/2k+1) - \cos(2\pi(b+1)j/2k+1)) \times$$
$$\times (-2\cos(2\pi j/2k+1))^n,$$

where $k \geq 0$, $n \geq 0$.

From (4.2) we may easily ascertain the linear recurrence in n satisfied by the $F_{k,n}(b)$. Consider the sequence of polynomials defined by

$$f_0(x) = 1, \quad f_1(x) = x - 1, \quad f_k(x) = xf_{k-1}(x) - f_{k-2}(x) .$$

Then the roots of $f_k(x)$ are

$$-2\cos 2\pi j/2k+1, \qquad 1 \leq j \leq k$$

[3; p. 264]. Hence from the elementary theory of finite difference (with

$$E^r a_n = a_{n+r}),$$

we have

$$(4.3) \qquad f_k(E)F_{k,n}(b) = 0 .$$

The n-dimensional Fibonacci sequence studied by Raney [5] has as its auxiliary polynomial $D_n(x)$ [5; p. 347] where in our notation

$$f_n(x) = (-1)^{\frac{1}{2}n(n-1)} x^n D_n(x^{-1}) .$$

Raney remarks that many of the elementary formulae related to the Fibonacci numbers maybe generalized to his sequences, and the same is true of $F_{k,n}(b)$. Most of these results may be derived from (4.2); but the proofs are clumsy. It would be nice to relate these sequences to some set of matrices as Raney has done for his sequences;perhaps then easy proofs could be given for analogs of Theorems 7 and 8 of Raney's paper.

5. FACTORIZATION OF LARGE NUMBERS

As is well known the Fibonacci and Lucas numbers are closely related to Lucas's famous test for the primality of the Mersenne numbers $2^p - 1$. We shall derive some similar necessary conditions for the primality of $(k^p - 1)/k - 1$ utilizing some analogs of the Lucas sequence which are related to the generalized Fibonacci sequences discussed in Section 4. For example, when $k = 2$, we shall prove the necessity part of Lucas's theorem on the primality of $2^q - 1$ (with $q \equiv 3 \pmod 4$) [4; p. 224]. When $k = 2$ and $q \equiv 1 \pmod 4$, we shall prove the following result.

Theorem 3. Let r_n be defined by

$$r_1 = 3, \quad r_{n+1} = r_n^2 - 2 .$$

If $q \equiv 1 \pmod 4$ and $M_q = 2^q - 1$ are both primes, then $r_q \equiv 3 \pmod{M_q}$.

When $k = 3$ and $q \equiv 1 \pmod 6$, we have the following theorem.

Theorem 4. Let $s_0 = 1$, $t_0 = -2$, and in general

$$s_{n+1} = s_n^3 - 3s_n t_n - 3; \quad t_{n+1} = t_n^3 + 3s_n t_n + 3 .$$

If $q \equiv 1 \pmod 6$ and $M_q = \frac{1}{2}(3^q - 1)$ are both primes, then

$$s_q \equiv 4 \pmod{M_q} ,$$
$$t_q \equiv -11 \pmod{M_q} .$$

Our first object in this section will be the derivation of a general theorem which will imply Theorems 3 and 4.

Let $A_j(k)$ denote the set of all ordered j-tuples of the first k positive integers. We define

$$L_{k,n}(j) = \sum (-2 \cos 2\pi n_1 /2k + 1)^n \cdots (-2 \cos 2\pi n_j /2k + 1)^n$$

where the summation is over all

$$(n_1, \cdots, n_j) \in A_j(k) \quad .$$

We shall also need the polynomials

$$w_m(x) = \sum_{j=0}^{m} \binom{2m}{2j} x^{2m-2j}(1 - x^2)^j \; ;$$

these polynomials have the property that

$$\cos 2m\beta = w_m (\cos \beta) \; .$$

<u>Lemma 1.</u> Let p be an odd prime, $p \equiv n \pmod{2k + 1}$, $0 \leq n \leq 2k$. Then there exists a rational integer $\alpha(k;j;n)$, which depends only on k, j, and n and not on the magnitude of p such that

$$L_{k,(k-1)p+1}(j) \equiv \alpha(k;\, j;\, n) \quad (\text{mod } p) \; .$$

<u>Proof.</u> Define n' to be n if n is even and n + 2k + 1 if n is odd; $n\star = \frac{1}{2}n'$. Then in the ring of integers of $Q(-2 \cos 2\pi/2k + 1)$

$$(-2 \cos 2\pi j/2k + 1)^p = (-2)^p 2^{-p+1} \sum_{i=0}^{\frac{1}{2}(p-1)} \binom{p}{m + i + 1} \cos 2\pi(2i + 1)j/2k + 1$$

$$\equiv -2 \cos 2\pi pj/2k + 1 \qquad (\text{mod } (p)\,)$$

$$\equiv -2 \cos 2\pi nj/2k + 1 \qquad (\text{mod } (p)\,)$$

$$\equiv -2 \cos 2\pi n'j/2k + 1 \qquad (\text{mod } (p)\,) \; ,$$

where (p) is the principal ideal generated by p in the ring of integers of $Q(-2 \cos 2\pi/2k + 1)$ and this first equality is from [1; p. 83]. Consequently

$$(5.1)\qquad L_{k,(k-1)p+1}(j) \equiv \sum (-2 \cos 2\pi m' n_1/2k + 1)^{k-1}(-2 \cos 2\pi m_1/2k + 1) \cdots$$

$$\cdots (-2 \cos 2\pi m' n_j /2k + 1)^{k-1}(-2 \cos 2\pi m_j /2k + 1) \pmod{(p)}$$

$$(5.2)\qquad = \sum (-2w_{n*} (\cos 2\pi m_1 /2k + 1))^{k-1}(-2 \cos 2\pi m_1/2k + 1) \cdots$$

$$\cdots (-2w_{n*} (\cos 2\pi m_j /2k + 1))^{k-1}(-2 \cos 2\pi m_j /2k + 1) \pmod{(p)}.$$

We now define $\alpha(k;j;n)$ to be the expression appearing on the right side of (5.1) (or, what is the same thing, (5.2)). Now (5.2) shows that $\alpha(k;j;n)$ is a symmetric polynomial in $\cos 2\pi m/2k + 1$, $1 \le m \le k$; since these are the roots of $f_k(-2x)$ (c. f. Section 4), we see by the symmetric function theorem that $\alpha(k;j;n)$ is a rational number. On the other hand, (5.1) shows that $\alpha(k;j;n)$ is an integer of the field $Q(-2 \cos 2\pi/2k + 1)$; since the rational integers are integrally closed in $Q(-2 \cos 2\pi/2k + 1)$, we see that $\alpha(k;j;n)$ must be a rational integer. Hence

$$L_{k,(k-1)p+1}(j) \equiv \alpha(k; j; n) \pmod{(p)}$$

holds in the ring of integers of $Q(-2 \cos 2\pi/2k + 1)$. Since this congruence involves only rational integers, it must also hold in Z, the ring of rational integers. Thus Lemma 1 is proved.

Corollary 1. If in Lemma 1, n = 1 or 2k, then

$$L_{k,(k-1)p+1}(j) \equiv L_{k,k}(j) \pmod{p} .$$

Proof. In (5.1) with n' either 2k or 2k + 2, we have

$$\alpha(k;j;n) = \sum (-2 \cos 2\pi m_1 /2k + 1)^k \cdots (-2 \cos 2\pi m_j /2k + 1)^k = L_{k,k}(j).$$

The desired results now follow directly from Lemma 1.

We now proceed to our main result.

Theorem 1. Let $k \geq 2$ be an integer. Let

$$\sigma_{k,j} = \sigma_{k,j}(x_1, \cdots, x_n)$$

be the j^{th} elementary symmetric function of $x_1, \cdots, x_k$. Let $g_j(y_1, \cdots, y_k)$ be the polynomial with integral coefficients such that

$$\sigma_{k,j}(x_1^k, \cdots, x_k^k) = g_j(\sigma_{k,1}, \cdots, \sigma_{k,k}) .$$

Let

$$v_{k,0}(j) = L_{k,1}(j)$$

and

$$v_{k,n+1}(j) = g_j(v_{k,n}(1), \cdots, v_{k,n}(k)) .$$

If $k\star = \text{g.c.d}(k - 1, 2k + 1)$, define $m = k\star(2k + 1)$, and let $\phi(m) = m'$, $\phi(m') = m''$ where ϕ is Euler's totient function.

If $q > m$ and $M_q = (k^q - 1)/k - 1$ are both primes, then there exist integers $\beta(k;j;i)$, $1 \leq i \leq m''$ depending only on k and j such that

$$v_{k,q}(j) \equiv \beta(k;j;n) \pmod{M_q} ,$$

if $q \equiv a_n \pmod{m''}$, where $a_1, \cdots, a_{\phi(m'')}$ constitute a reduced residue class system (mod m'').

Proof. From the definition of $L_{k,n}(j)$, one easily verifies by induction that $L_{k,k^n}(j) = v_{k,n}(j)$. One also may verify that the residue of M_q (mod $2k + 1$), say r, is completely determined by the residue of q (mod m''). Therefore if both $q > m$ and M_q are primes,

$$v_{k,q}(j) = L_{k,k^q}(j) = L_{k,(k-1)M_q+1}(j) \equiv \alpha(k;\, j;\, r) \pmod{M_q} .$$

If we define

$$\beta(k;\ j;\ n) \ = \ \alpha(k;\ j;\ r)$$

where $q \equiv a_n \pmod{m''}$, then the theorem follows.

For small values of k we may prove more explicit theorems.

Theorem 2. (Lucas) Let r_n be defined by

$$r_1 = 3, \quad r_{n+1} = r_n^2 - 2 .$$

If $q \equiv 3 \pmod 4$ and $M_q = 2^p - 1$ are both primes, then $r_{q-1} \equiv 0 \pmod{M_q}$.

Proof. In Theorem 1, with $k = 2$, we find that for $n > 0$

$$v_{2,n}(2) = (-2\cos 2\pi/5)^{2^n}(-2\cos 4\pi/5)^{2^n} = (-1)^{2^n} = 1.$$

Also

$$x_1^2 + x_2^2 = \sigma_{2,1}^2 - 2\sigma_{2,2} .$$

Hence

$$g_1(y_1, y_2) = y_1^2 - 2y_2 .$$

Thus we see that $r_n = v_{2,n}(1)$.

As in Lemma 1, we have (mod M_q)

$$\begin{aligned} r_q = L_{2,M_q+1}(1) &\equiv (-2\cos 4\pi/5)(-2\cos 2\pi/5) + (-2\cos 8\pi/5)(-2\cos 4\pi/5) \\ &= 2(-2\cos 4\pi/5)(-2\cos 2\pi/5) = -2 . \end{aligned}$$

Therefore

$$r_{q-1}^2 = r_q + 2 \equiv -2 + 2 \equiv 0 \pmod{M_q}.$$

Thus since M_q was assumed prime,

$$r_{q-1} \equiv 0 \pmod{M_q} .$$

This concludes the proof of Theorem 2.

Proof of Theorem 3. We proceed exactly as in Theorem 2, except that now by Corollary 1

$$r_q \equiv L_{2,M_q+1}(1) \equiv L_{2,2}(1) = 3.$$

Proof of Theorem 4. In Theorem 1, with $k = 3$, we find that for $n \geq 0$

$$v_{3,n}(3) = (-2 \cos 2\pi/7)^{3^n}(-2 \cos 4\pi/7)^{3^n}(-2 \cos 6\pi/7)^{3^n} = (-1)^{3^n} = -1.$$

Now

$$x_1^3 + x_2^3 + x_3^3 = \sigma_{3,1}^3 - 3\sigma_{3,1}\sigma_{3,2} + 3\sigma_{3,3} ,$$

and thus

$$g_1(y_1, y_2, y_3) = y_1^3 - 3y_1y_2 + 3y_3 .$$

Also

$$x_1^3x_2^3 + x_2^3x_3^3 + x_1^3x_3^3 = \sigma_{3,2}^3 - 3\sigma_{3,1}\sigma_{3,2}\sigma_{3,3} + 3\sigma_{3,3}^2 ,$$

and thus

$$g_2(y_1, y_2, y_3) = y_2^3 - 3y_1y_2y_3 + 3y_3^2 .$$

Thus we see that

$$s_n = v_{3,n}(1)$$

and

$$t_n = v_{3,n}(2) .$$

Utilizing Corollary 1, we have (mod M_q)

$$s_q = L_{3,2M_q+1}(1) \equiv L_{3,3}(1) = 4 \;;$$

$$t_q = L_{3,2M_q+1}(2) \equiv L_{3,3}(2) = -11 \;.$$

This concludes Theorem 4.

Theorem 5. Under the conditions of Theorem 4, with the single change that $q \equiv 5 \pmod 6$, if both q and M_q are primes, then

$$s_q \equiv 4 \pmod{M_q}.$$

Proof. Since $q \equiv 5 \pmod 6$, $M_q \equiv 2 \pmod 7$. Hence by Lemma 1 we have (mod M_q)

$$\begin{aligned} s_q = L_{3,2M_q+1}(1) &\equiv \sum_{j=1}^{3}(-2\cos 4\pi j/7)^2(-2\cos 2\pi j/7) \\ &= 4\sum_{j=1}^{3}(2\cos^2 2\pi j/7 - 1)^2(-2\cos 2\pi j/7) \\ &= \sum_{j=1}^{3}((-2\cos 2\pi j/7)^2 - 4(-2\cos 2\pi j/7)^3 \\ &\qquad\qquad + 4(-2\cos 2\pi j/7)) \\ &= L_{3,5}(1) - 4L_{3,3}(1) + 4L_{3,1}(1) \\ &= 16 - 16 + 4 = 4\,. \end{aligned}$$

We now consider some numerical examples of the theorems we have proved. First take $q = 5$, $M_5 = 121$ in Theorem 5. In this case

n	s_n (mod 121)	t_n (mod 121)
0	1	-2
1	4	-11
2	72	-8
3	-6	-59
4	50	-66
5	-18	

Consequently Theorem 5 proves that $121 = \frac{1}{2}(3^5 - 1)$ is not a prime, and indeed $121 = 11^2$.

Next we consider Theorem 4, with $q = 7$, $M_7 = 1093$. In this case

n	s_n (mod 1093)	t_n (mod 1093)
0	1	-2
1	4	-11
2	193	-367
3	-249	-386
4	-510	-96
5	-569	-78
6	-127	-387
7	4	-11

Thus we see that $1093 = \frac{1}{2}(3^7 - 1)$ satisfies the necessity conditions of Theorem 4, and indeed it turns out that 1093 is a prime.

There appears to be a great number of possibilities for further work on the subjects treated in this section. One would hope that Theorem 1 could be strengthened to include sufficiency conditions for the primality of $(k^p - 1)/(k - 1)$. Possibly the arithmetic of the fields $Q(-2 \cos (2\pi/2k + 1))$ would yield such results.

6. RELATED SEQUENCES

It is possible to exhibit a large number of sums similar to those given in (1.1), (1.2), or (4.1). To indicate the possibilities we list three such.

$$G_{k,n}(b) = \sum_{\alpha=-\infty}^{\infty} \binom{n}{[\frac{1}{2}(n - b - (2k + 1)\alpha)]} ; \tag{6.1}$$

$$J_{k,n}(b) = \sum_{\alpha=-\infty}^{\infty} (-1)^{\alpha} \binom{n}{[\frac{1}{2}(n - b - (2k + 1)2\alpha)]} ; \tag{6.2}$$

$$(6.3) \qquad K_{k,n}(b) = \sum_{\alpha=-\infty}^{\infty} (-1)^{\alpha} \binom{n}{[\frac{1}{2}(n - b - (2k+1)(2n+1))]} \; .$$

Following the method of Section 2, we find

$$(6.4) \qquad G_{k,n}(b) = \frac{2}{2k+1} \sum_{j=1}^{k} (\cos 2\pi bj/(2k+1) + \cos 2\pi(b+1)j/2k+1) \times \times (2 \cos 2\pi j/2k+1)^{n} \quad ;$$

$$(6.5) \qquad J_{k,n}(b) = \frac{1}{2k+1} \sum_{j=1}^{2k} (\cos \pi b(4j+2k+1)/(4k+2) + \cos \pi(b+1) \times \times (4j+2k+1)/4k+2)(-2 \sin 2\pi j/2k+1)^{n};$$

$$(6.6) \qquad K_{k,n}(b) = \frac{-(-1)^{k}}{2k+1} \sum_{j=1}^{2k} (\sin \pi b(4j+2k+1)/(4k+2) + \sin \pi(b+1) \times \times (4j+2k+1)/4k+2)(-2 \sin 2\pi j/2k+1)^{n}.$$

As in Section 4 (c.f. (4.3)), we may give linear recurrence formulae for the above expressions as sequences in n.

$$(6.7) \qquad (-1)^{k}(E - 2)f_{k}(-E)G_{k,n}(b) = 0 \; ;$$

$$(6.8) \qquad E^{-1}((E + 2)f_{k}^{2}(E) - 2)J_{k,n}(b) = 0 \; ;$$

$$(6.9) \qquad E^{-1}((E + 2)f_{k}^{2}(E) - 2)K_{k,n}(b) = 0 \; .$$

Equations (6.7) through (6.9) are easily derived from Eqs. (6.4) through (6.6) utilizing the fact that the roots of $(-1)^{k}(x - 2)f_{k}(-x)$ are $2 \cos 2\pi j/(2k+1)$, $0 \le j \le k$ [3; p. 264] and the fact that the roots of $x^{-1}((x + 2)f_{k}^{2}(x) - 2)$ are $-2 \sin 2\pi j/2k + 1$, $1 \le j \le 2k$ [3; pp. 267-268].

As is clear from their definitions, all these generalized sequences satisfy congruences similar to (1.3) and (1.4). For example if p is an odd prime, $p \neq 2k + 1$, then

$$K_{k,p}(0) \equiv 0 \pmod p . \tag{6.10}$$

If p is an odd prime, $p \neq 2k + 1$, $p \not\equiv \pm 1 \pmod{4k + 2}$, then

$$J_{k,p}(0) \equiv 0 \pmod p . \tag{6.11}$$

If $p = (2k + 1)m + a$ is a prime with $0 < a \leq k$, $m \geq 2$, then

$$G_{k,p+c}(0) \equiv F_{k,p+c}(0) \equiv 0 \pmod p , \tag{6.12}$$

where $0 \leq c \leq a - 2$.

If $p = (2k + 1)m + a$ is a prime with $k < a \leq 2k$, $m \geq 1$, then

$$G_{k,p+c}(0) \equiv F_{k,p+c}(0) \equiv 0 \pmod p , \tag{6.13}$$

where $0 \leq c \leq 2k - 2 - a$. Equations (6.10) through (6.14) are proved exactly the way (1.3) and (1.4) were.

REFERENCES

1. H. T. Davis, The Summation of Series, Principia Press, San Antonio, 1962.
2. L. E. Dickson, History of the Theory of Numbers, Vol. I, Chelsea, New York, 1952.
3. H. Hancock, "Trigonometric Realms of Rationality," Rendiconti del Circolo Matematico di Palermo, 49 (1925), pp. 263-276.
4. G. H. Hardy and E. M. Wright, An Introduction to the Theory of Numbers, Oxford University Press, Oxford, 4th ed., 1960.
5. G. Raney, "Generalization of the Fibonacci Sequence to n-Dimensions," Canadian J. Math., 18 (1966), pp. 332-349.

★ ★ ★ ★ ★