A LUCAS-TYPE THEOREM FOR FIBONOMIAL-COEFFICIENT RESIDUES

John M. Holte
Gustavus Adolphus College, St. Peter, MN 56082
(Submitted April 1992)

1. INTRODUCTION

A remarkable theorem of Lucas ([8], pp. 229-30) states that the value of the binomial coefficient $\binom{n}{k}$ is congruent, modulo a prime p, to the product of the binomial coefficients of the respective base-p digits of n and k. In other words, if

$$n = \sum n_j p^j, \quad \text{where } 0 \le n_j < p \text{ for each } j$$

and

$$k = \sum k_j p^j, \quad \text{where } 0 \le k_j < p \text{ for each } j,$$

then

$$\binom{n}{k} \equiv \prod \binom{n_j}{k_j} \pmod{p}. \tag{1}$$

For example, since $2280 = (6435)_7$ and $1823 = (5213)_7$, we have

$$\binom{2280}{1823} \equiv \binom{6}{5}\binom{4}{2}\binom{3}{1}\binom{5}{3} \equiv 6 \cdot 6 \cdot 3 \cdot 3 \equiv 2 \pmod{7}.$$

Formula (1) is equivalent to Lucas's earlier generalization of an 1869 result of H. Anton ([1], pp. 303-06; [7], p. 52; [2], p. 271):

$$\binom{n}{k} \equiv \binom{n \operatorname{div} p}{k \operatorname{div} p}\binom{n \bmod p}{k \bmod p} \pmod{p}, \tag{2}$$

where $n \operatorname{div} p$ denotes the integer quotient of n by p, and $n \bmod p$ its remainder. For short proofs, see [3] and [9]. For our purposes, it is better to reformulate this theorem in terms of

$$B(m,n) := \binom{m+n}{m} = \binom{m+n}{n}:$$

$$B(m,n) \equiv B(m \operatorname{div} p,\ n \operatorname{div} p)\ B(m \bmod p,\ n \bmod p) \pmod{p}. \tag{3}$$

[If $(m+n) \operatorname{div} p = m \operatorname{div} p + n \operatorname{div} p$ and $(m+n) \bmod p = m \bmod p + n \bmod p$, then this just re-expresses (2); if not, then, again by (2), both sides may be shown to be congruent to 0.] Repeated application of (3) yields the following counterpart of (1):

$$B(m,n) \equiv \prod B(m_j, n_j) \pmod{p}, \tag{4}$$

where m_j and n_j are the base-p digits of m and n, respectively. Our goal is to obtain formulas corresponding to (3) and (4) for Fibonomial coefficients.

In analogy with the usual definition of binomial coefficients

$$B(m,n)=\binom{m+n}{m}=\prod_{j=0}^{m-1}\frac{m+n-j}{m-j}\quad (m,n\ge 0),$$

we define the Fibonomial coefficients by

$$C(m,n)=\begin{bmatrix}m+n\\ m\end{bmatrix}=\prod_{j=0}^{m-1}\frac{F_{m+n-j}}{F_{m-j}}\quad (m,n\ge 0), \tag{5}$$

where F_k denotes the k^{th} Fibonacci number, and an empty product is taken to be 1 (see [8], §9; also [4] and [5]). Some values of $C(m,n)$ are tabulated in Table 1; there $C(0,0)$ appears at the upper left corner. We note that, for $m,n\ge 0$,

$$C(m,0)=1,\ C(0,n)=1,\ \text{and}\ C(m,n)=C(n,m).$$

TABLE 1: Fibonomial Coefficients

1	1	1	1	1	1	1	1
1	1	2	3	5	8	13	21
1	2	6	15	40	104	273	714
1	3	15	60	260	1092	4641	19635
1	5	40	260	1820	12376	85085	582505
1	8	104	1092	12376	136136	1514513	16776144
1	13	273	4641	85085	1514513	27261234	488605194
1	21	714	19635	582505	16776144	488605194	14169550626

Using the identity

$$F_{m+n}=F_{m+1}F_n+F_mF_{n-1}\quad (m,n\ge 0) \tag{6}$$

and the definition, (5), one may deduce (see [4]) the key recurrence formula for $m,n\ge 1$:

$$C(m,n)=F_{m+1}C(m,n-1)+F_{n-1}C(m-1,n). \tag{7}$$

This is the Fibonomial counterpart of the Pascal triangle recurrence,

$$B(m,n)=B(m,n-1)+B(m-1,n).$$

[Alternatively, by symmetry, we also have

$$C(m,n)=F_{m-1}C(m,n-1)+F_{n+1}C(m-1,n).$$

Then, in terms of the Lucas numbers $L_k=F_{k-1}+F_{k+1}$, we have, by addition, the symmetric recurrence formula

$$2C(m,n)=L_mC(m,n-1)+L_nC(m-1,n).]$$

From (7) it follows that the Fibonomial coefficients must be integers ([8], p. 203).

2. COMPUTING FIBONOMIAL COEFFICIENTS MODULO A PRIME

To state our theorem, we need to introduce

$$r = r(p) := \min\{k > 0 : p | F_k\},$$

the rank of apparition of p in the Fibonacci sequence, and

$$t = t(p) := \text{the period of } (F_k \bmod p).$$

It is known [10] that, for any prime p, $t/r = 1, 2,$ or 4.

Theorem: Assume p is a prime number $\neq 5$. Let $m' = m \operatorname{div} r$, $m'' = (m \bmod t) \operatorname{div} r$, $m^* = m \bmod t$, and similarly for n. Then

$$C(m, n) \equiv B(m', n')\{B(m'', n'')^{-1} \bmod p\} C(m^*, n^*) \pmod p,$$

where the term in braces is the modulo-p multiplicative inverse of $B(m'', n'')$.

Notice that the first factor here is a *binomial* coefficient and is the same as the first factor in (3) except that r replaces p. The last factor is a Fibonomial coefficient from the initial $t \times t$ (instead of $p \times p$) block of Fibonomial coefficients. We observe that the peculiar middle factor can only be: 1 if $t/r = 1$; 1 or $2^{-1} \bmod p$, if $t/r = 2$; and the mod-p inverse of 1, 2, 3, 4, 6, 10, or 20, if $t/r = 4$. The omitted prime, $p = 5$, can be handled by the proposition we shall give later, from which we shall derive Theorem 1.

By repeated application of Lucas's theorem, we get our counterpart of formula (4). It is not so tidy as the binomial case, depending as it does on the use of two mixed-radix representations:

$$m = m_k p^{k-1} r + m_{k-1} p^{k-2} r + \cdots + m_1 p^0 r + m_0,$$

where $$0 \le m_0 < r \text{ and } 0 \le m_j < p \text{ for } j \ge 1,$$

and $$m = m''' t + m'' r + m_0,$$

where $$0 \le m'' < t/r, \quad 0 \le m''' < \infty, \text{ and } m^* = m'' r + m_0,$$

and similarly for n. Then, for a prime $p \neq 5$, we have our main formula:

$$C(m, n) \equiv \prod_{j \ge 1} B(m_j, n_j)\{B(m'', n'')^{-1} \bmod p\} C(m^*, n^*) \pmod p. \tag{8}$$

As an example, let us compute $C(23, 12) \bmod 3$. Here $p = 3, r = 4, t = 8$,

$$\begin{aligned} m &= \underline{1} \cdot 3^1 \cdot 4 + \underline{2} \cdot 3^0 \cdot 4 + \underline{3} \\ &= \underline{2} \cdot 8 + \underline{1} \cdot 4 + \underline{3} \end{aligned}$$

and

$$\begin{aligned} n &= \underline{1} \cdot 3^1 \cdot 4 + \underline{0} \cdot 3^0 \cdot 4 + \underline{0} \\ &= \underline{1} \cdot 8 + \underline{1} \cdot 4 + \underline{0} \end{aligned}$$

So

$$\begin{aligned} C(23, 12) &\equiv B(1, 1)B(2, 0)\{B(1, 1)^{-1} \bmod 3\} C(7, 4) && \pmod 3 \\ &\equiv 2 \cdot 1 \cdot \{2^{-1} \bmod 3\} \cdot 1 && \pmod 3 \\ &\equiv 2 \cdot 1 \cdot 2 \cdot 1 \equiv 1 && \pmod 3. \end{aligned}$$

The value for $C(7, 4)$ mod 3 was obtained from Table 2, which was generated by means of the basic recurrence formula. It also includes enough additional values to corroborate our answer for $C(23, 12)$.

TABLE 2. Fibonomials mod 3

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
1	1	1	2	0	2	2	1	0	1	1	2	0	2	2	1	0
2	1	2	0	0	1	2	0	0	1	2	0	0	1	2	0	0
3	1	0	0	0	2	0	0	0	1	0	0	0	2	0	0	0
4	1	2	1	2	2	1	2	1	0	0	0	0	1	2	1	2
5	1	2	2	0	1	2	2	0	0	0	0	0	2	1	1	0
6	1	1	0	0	2	2	0	0	0	0	0	0	1	1	0	0
7	1	0	0	0	1	0	0	0	0	0	0	0	2	0	0	0
8	1	1	1	1	0	0	0	0	0	0	0	0	1	1	1	1
9	1	1	2	0	0	0	0	0	0	0	0	0	2	2	1	0
10	1	2	0	0	0	0	0	0	0	0	0	0	1	2	0	0
11	1	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0
12	1	2	1	2	1	2	1	2	1	2	1	2	2	1	2	1
13	1	2	2	0	2	1	1	0	1	2	2	0	1	2	2	0
14	1	1	0	0	1	1	0	0	1	1	0	0	2	2	0	0
15	1	0	0	0	2	0	0	0	1	0	0	0	1	0	0	0
16	1	1	1	1	2	2	2	2	0	0	0	0	2	2	2	2
17	1	1	2	0	1	1	2	0	0	0	0	0	1	1	2	0
18	1	2	0	0	2	1	0	0	0	0	0	0	2	1	0	0
19	1	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0
20	1	2	1	2	0	0	0	0	0	0	0	0	2	1	2	1
21	1	2	2	0	0	0	0	0	0	0	0	0	1	2	2	0
22	1	1	0	0	0	0	0	0	0	0	0	0	2	2	0	0
23	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0

Exercises for the Reader: **(a)** Find $C(7, 4)$ mod 2; **(b)** find $C(1759, 984)$ mod 7.

[Answers: **(a)** $B(1, 0)B(0, 1)\{B(0, 0)^{-1} \bmod 2\}C(1, 1) \equiv 1 \pmod 2$; cf. $C(7, 4)$=582505 from Table 1; **(b)** $B(4, 2)B(3, 3)B(2, 4)\{B(1, 1)^{-1} \bmod 7\}C(15, 8) \equiv 1 \pmod 7$; using Table 3 below.]

3. DEDUCING THE RESIDUES OF THE FIBONOMIALS MOD p

Let p be a fixed prime. Let $r, t, m', n', m'', n'', m^*$, and n^* be as in the Theorem. Also, let $m_0 = m \bmod r$ and $n_0 = n \bmod r$.

We shall deduce the residues of $C(m, n)$ mod p in the following steps:

Step 1: Show $C(m, n) \equiv 0 \pmod p$ for (m, n) in the $(r-1) \times (r-1)$ triangles where $m_0 + n_0 \geq r$.

Step 2: Calculate $C(m'r, n'r)$ mod p $(m', n' = 0, 1, 2, \ldots)$.

Step 3: Determine the remaining values mod p from the basic recurrence relation (7).

TABLE 3. Fibonomials mod 7

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
1	1	1	2	3	5	1	6	0	6	6	5	4	2	6	1	0
2	1	2	6	1	5	6	0	0	1	2	6	1	5	6	0	0
3	1	3	1	4	1	0	0	0	6	4	6	3	6	0	0	0
4	1	5	5	1	0	0	0	0	1	5	5	1	0	0	0	0
5	1	1	6	0	0	0	0	0	6	6	1	0	0	0	0	0
6	1	6	0	0	0	0	0	0	1	6	0	0	0	0	0	0
7	1	0	0	0	0	0	0	0	6	0	0	0	0	0	0	0
8	1	6	1	6	1	6	1	6	2	5	2	5	2	5	2	5
9	1	6	2	4	5	6	6	0	5	2	3	6	4	2	2	0
10	1	5	6	6	5	1	0	0	2	3	5	5	3	2	0	0
11	1	4	1	3	1	0	0	0	5	6	5	1	5	0	0	0
12	1	2	5	6	0	0	0	0	2	4	3	5	0	0	0	0
13	1	6	6	0	0	0	0	0	5	2	2	0	0	0	0	0
14	1	1	0	0	0	0	0	0	2	2	0	0	0	0	0	0
15	1	0	0	0	0	0	0	0	5	0	0	0	0	0	0	0

To get started, we note that, for binomial coefficients, we have $B(m, n) \equiv 0 \pmod{p}$ if $m \bmod p + n \bmod p \geq p$. Similarly, for Fibonomial coefficients, we have

Lemma 1: $C(m, n) \equiv 0 \pmod{p}$ if $m_0 + n_0 \geq r$.

Proof #1: It follows from Knuth & Wilf's extension of Kummer's theorem to Fibonomial coefficients ([6], Theorem 2) that $p|C(m, n)$ if and only if there is at least one carry across or to the left of the radix point when m/r and n/r are added in base p.

If $m \bmod r + n \bmod r \geq r$, then there will be a carry across the radix point. □

Proof #2: This time we appeal to another theorem of Lucas ([8], p. 206):

$$\gcd(F_m, F_n) = F_{\gcd(m, n)}.$$

It follows from this theorem that all the Fibonacci numbers divisible by any prime power p^s have indices of the form $kr(p^s)$, where $r(p^s)$ is the rank of apparition of p^s. Now consider $C(m, n) = C(m'r + m_0, n'r + n_0)$:

$$C(m, n) = \prod_{j=0}^{m'r+m_0-1} F_{(m'+n')r+m_0+n_0-j} \,/\, F_{m'r+m_0-j}.$$

Our hypothesis is that $m_0 + n_0 \geq r$. Therefore, $F_{(m'+n'+1)r}$ is a numerator factor, and so the factors that are divisible by p are the $m' + 1$ numerator factors

$$F_{(m'+n'+1)r}, F_{(m'+n')r}, \ldots, F_{(n'+1)r}$$

and the m' denominator factors

$$F_{m'r}, F_{(m'-1)r}, \ldots, F_r.$$

Furthermore, by the consequence of Lucas's theorem noted above, every factor $F_{kr(p^s)}$ in the denominator is matched by such a factor in the numerator, without using the extra numerator factor $F_{(m'+n'+1)r}$. So $p|C(m,n)$. □

In preparation for the next step, we note the following formula:

$$F_{kr+1} \equiv F_{kr-1} \equiv F_{r-1}^k \pmod{p} \quad (k \geq 0). \tag{9}$$

Since $F_{kr} \equiv 0 \pmod{p}$, the first congruence is clear. The second then follows by applying identity (6) with $n = r$ and $m = r-1, 2r-1, \ldots, (k-1)r-1$.

Lemma 2: $C(m'r, n'r) \equiv B(m', n')F_{r-1}^{rm'n'} \pmod{p}$.

Proof: To simplify the notation, let us suppress the primes on m and n during this proof. If $m = 0$ or $n = 0$, then

$$C(mr, nr) = 1 \text{ and } B(m,n)F_{r-1}^{rmn} = 1 \cdot F_{r-1}^0 = 1.$$

Now assume $m \geq 1$ and $n \geq 1$. Applying the basic Fibonomial recurrence (7) and Lemma 1 repeatedly, we get

$$\begin{aligned} C(mr, (n-1)r+1) &= F_{mr+1}C(mr, (n-1)r) + F_{(n-1)r}C(mr-1, (n-1)r+1) \\ &\equiv F_{mr+1}C(mr, (n-1)r) \pmod{p}; \end{aligned}$$

$$\begin{aligned} C(mr, (n-1)r+2) &= F_{mr+1}C(mr, (n-1)r+1) + F_{(n-1)r+1}C(mr-1, (n-1)r+2) \\ &\equiv F_{mr+1}C(mr, (n-1)r+1) \pmod{p} \\ &\equiv F_{mr+1}^2 C(mr, (n-1)r) \pmod{p}; \end{aligned}$$

$$\cdots$$

$$\begin{aligned} C(mr, (n-1)r+r-1) &= F_{mr+1}C(mr, (n-1)r+r-2) + F_{(n-1)r+r-2}C(mr-1, (n-1)r+r-1) \\ &\equiv F_{mr+1}C(mr, (n-1)r+r-2) \pmod{p} \\ &\equiv F_{mr+1}F_{mr+1}^{r-2}C(mr, (n-1)r) \pmod{p} \\ &= F_{mr+1}^{r-1}C(mr, (n-1)r) \pmod{p}. \end{aligned}$$

Similarly,

$$C((m-1)r+r-1, nr) \equiv F_{nr-1}^{r-1}C((m-1)r, nr) \pmod{p}.$$

Then

$$\begin{aligned} C(mr, nr) &= F_{mr+1}C(mr, nr-1) + F_{nr-1}C(mr-1, nr) \\ &\equiv F_{mr+1}^r C(mr, (n-1)r) + F_{nr-1}^r C((m-1)r, nr) \pmod{p}. \end{aligned}$$

By (9), $F_{mr+1}^r \equiv F_{mr-1}^r \equiv F_{r-1}^{rm} \pmod{p}$ and $F_{nr-1}^r \equiv F_{r-1}^{rn} \pmod{p}$. So, for $m, n \geq 1$,

$$C(mr, nr) \equiv F_{r-1}^{rm}C(mr, (n-1)r) + F_{r-1}^{rn}C((m-1)r, nr) \pmod{p}. \tag{10}$$

Let $C'(m,n) := C(mr, nr)$. Then (10) becomes

$$C'(m,n) \equiv F_{r-1}^{rm}C'(m, n-1) + F_{r-1}^{rn}C'(m-1, n) \pmod{p}, \tag{11}$$

a recurrence formula that uniquely determines the values of $C'(m,n)$ for $m, n \geq 1$, given the boundary conditions

$$C'(m,0)=1 \text{ and } C'(0,n)=1 \ (m,n\geq 1). \tag{12}$$

Hence, to complete the proof, we need only verify that $C''(m,n) := B(m,n)F_{r-1}^{rmn} \bmod p$ satisfies (11) and (12). The boundary conditions (12) are readily verified. Modulo p we have

$$\begin{aligned}
&F_{r-1}^{rm}C''(m,n-1)+F_{r-1}^{rn}C''(m-1,n) \equiv F_{r-1}^{rm}B(m,n-1)F_{r-1}^{rm(n-1)}+F_{r-1}^{rn}B(m-1,n)F_{r-1}^{r(m-1)n}\\
&\equiv F_{r-1}^{rmn}B(m,n-1)+F_{r-1}^{rmn}B(m-1,n)\\
&\equiv F_{r-1}^{rmn}B(m,n) \ \text{[by the Pascal triangle rule]}\\
&\equiv C''(m,n),
\end{aligned}$$

showing that (11) is satisfied. □

We can refine Lemma 2 a little. By (9),

$$F_{r-1}^{rm'n'} \equiv F_{r^2m'n'-1} \pmod p.$$

Here

$$rm' = r(m \operatorname{div} r) = m - m \bmod r \equiv (m \bmod t - m \bmod r) \pmod t = m''r,$$

where $m'' = (m \bmod t) \operatorname{div} r$. Because t is the period of the Fibonacci sequence modulo p,

$$F_{rm'rn'-1} \equiv F_{rm''rn''-1} \pmod p,$$

and so Lemma 2 becomes

$$C(m'r,n'r) \equiv B(m',n')F_{r^2m''n''-1} \pmod p. \tag{13}$$

We shall complete our determination of the Fibonomial coefficient residues by applying the basic recurrence formula (7), $C(m,n) = F_{m+1}C(m,n-1)+F_{n-1}C(m-1,n)$, to the determination of $C(m'r+m_0,n'r+n_0) \bmod p$ from $C(m'r,n'r)$. By Lemma 1 we have

$$C(m'r+m_0,n'r-1) \equiv 0 \pmod p \ (1\leq m_0<r) \tag{14}$$

and

$$C(m'r-1,n'r+n_0) \equiv 0 \pmod p \ (1\leq n_0<r) \tag{15}$$

and by Lemma 2 we know $C(m'r,n'r) \bmod p$. We observe that application of the basic recurrence formula (7) with these boundary conditions will uniquely determine $C(m'r+m_0,n'r+n_0)$ for $0\leq m_0,n_0<r$, and that this solution matrix is proportional to the value $C(m'r,n'r)$. Also, the solution matrix depends on the coefficients used, namely, $F_{m'r+1},\ldots,F_{m'r+r-1}$ and $F_{n'r-1},\ldots,F_{n'r+r-2}$. Accordingly, we may make this

Definition: Let $A(m',n';m_0,n_0)$ be the solution $C(m'r+m_0,n'r+n_0)$ of the basic recurrence formula (7) satisfying the boundary conditions (14), (15), and (the possibly contrary-to-fact condition) $C(m'r,n'r) = 1$.

Since the coefficients $F_k \bmod p$ have period t, and since $m'r+m_0 \equiv m''r+m_0$ and $n'r+n_0 \equiv n''r+n_0 \pmod t$, we have $A(m',n';m_0,n_0) \equiv A(m'',n'';m_0,n_0) \pmod p$. Thus, we have proved

Lemma 3: $C(m,n) \equiv C(m'r,n'r)A(m'',n'';m_0,n_0) \pmod p$.

By (13) and Lemma 3, we now have our general proposition.

Proposition: $C(m,n) \equiv B(m',n')F_{r^2m''n''-1}A(m'',n'';m_0,n_0) \pmod{p}$.

As an example, let us determine $C(437, 151)$ mod 5. Here $p = 5$, $r = 5$, and $t = 20$.

$m' = 437 \text{ div } 5 = 87 = (322)_5$; $n' = 151 \text{ div } 5 = 30 = (110)_5$;

$m_0 = 437 \bmod 5 = 2$; $n_0 = 151 \bmod 5 = 1$;

$m'' = 437 \bmod 20 \text{ div } 5 = 17 \text{ div } 5 = 3$; $n'' = 151 \bmod 20 \text{ div } 5 = 11 \text{ div } 5 = 2$.

So $C(437,151) \equiv B(3,1)B(2,1)B(2,0)F_{5^2\cdot 3\cdot 2-1}A(3,2;2,1) \equiv 4\cdot 3\cdot 1\cdot 4\cdot 4 \equiv 2 \pmod 5$. (We looked up the last factor in Table 4.)

TABLE 4. $A(m'', n''; m_0, n_0)$ for $p = 5$

m'' \ n''	0	1	2	3
0	1 1 1 1 1 1 1 2 3 0 1 2 1 0 0 1 3 0 0 0 1 0 0 0 0	1 1 1 1 1 3 3 1 4 0 4 3 4 0 0 2 1 0 0 0 1 0 0 0 0	1 1 1 1 1 4 4 3 2 0 1 2 1 0 0 4 2 0 0 0 1 0 0 0 0	1 1 1 1 1 2 2 4 1 0 4 3 4 0 0 3 4 0 0 0 1 0 0 0 0
1	1 3 4 2 1 1 3 3 1 0 1 1 4 0 0 1 4 0 0 0 1 0 0 0 0	1 3 4 2 1 3 4 4 3 0 4 4 1 0 0 2 3 0 0 0 1 0 0 0 0	1 3 4 2 1 4 2 2 4 0 1 1 4 0 0 4 1 0 0 0 1 0 0 0 0	1 3 4 2 1 2 1 1 2 0 4 4 1 0 0 3 2 0 0 0 1 0 0 0 0
2	1 4 1 4 1 1 4 2 2 0 1 3 1 0 0 1 2 0 0 0 1 0 0 0 0	1 4 1 4 1 3 2 1 1 0 4 2 4 0 0 2 4 0 0 0 1 0 0 0 0	1 4 1 4 1 4 1 3 3 0 1 3 1 0 0 4 3 0 0 0 1 0 0 0 0	1 4 1 4 1 2 3 4 4 0 4 2 4 0 0 3 1 0 0 0 1 0 0 0 0
3	1 2 4 3 1 1 2 3 4 0 1 4 4 0 0 1 1 0 0 0 1 0 0 0 0	1 2 4 3 1 3 1 4 2 0 4 1 1 0 0 2 2 0 0 0 1 0 0 0 0	1 2 4 3 1 4 3 2 1 0 1 4 4 0 0 4 4 0 0 0 1 0 0 0 0	1 2 4 3 1 2 4 1 3 0 4 1 1 0 0 3 3 0 0 0 1 0 0 0 0

Finally, we get the formula stated in our Theorem by observing that in most cases we can find the $r \times rA$-blocks hidden in the initial $t \times t$ C-block. In this block

$$C(m''r + m_0, n''r + n_0) \equiv B(m',n')F_{r^2m''n''-1}A(m'',n'';m_0,n_0) \pmod{p}$$

and $m' = m''$ and $n' = n''$. So, if $B(m'', n'') \not\equiv 0 \pmod p$, then

$$F_{r^2m''n''-1}A(m'',n'';m_0,n_0) \equiv B(m'',n'')^{-1}C(m''r + m_0, n''r + n_0) \pmod{p}. \tag{16}$$

Here $0 \le m'', n'' < t/r$. Since $t/r \le 4$, the possible values of $B(m'', n'')$ are 1, 2, 3, 4, 6, 10, and 20. The only case where some value of $B(m'', n'') \equiv 0 \pmod p$ is $p = 5$; then $t/r = 4$, and $B(1, 2) = B(2, 1) = 10$ and $B(2, 2) = 20$ are not invertible mod 5. So, if $p \neq 5$, we may use (16) in the Proposition to determine the residue modulo p of the Fibonomial coefficient $C(m, n)$ in terms

of the binomial coefficients $B(m', n')$ and $B(m'', n'')$ and the Fibonomial coefficient $C(m''r + m_0, n''r + n_0) = C(m^*, n^*)$, thus proving our Lucas-type theorem for Fibonomial-coefficient residues.

REFERENCES

1. H. Anton. "Die Elferprobe und die Proben für die Modul Neun, Dreizehn und Hunderteins. Für Volksund Mittelschulen." *Archiv Math. Phys.* **49** (1869):241-341.
2. L. E. Dickson. *History of the Theory of Numbers.* Vol. I. New York: Chelsea, 1952.
3. N. J. Fine. "Binomial Coefficients Modulo a Prime." *Amer. Math. Monthly* **54** (1947):589-592.
4. V. E. :Hoggatt, Jr. "Fibonacci Numbers and Generalized Binomial Coefficients." *A Primer for the Fibonacci Numbers.* Ed. Marjorie Bicknell & Verner E. Hoggatt, Jr. Santa Clara, Calif: The Fibonacci Association, 1972.
5. D. Jarden & Th. Motzkin. "The Product of Sequences with a Common Linear Recursion Formula of Order 2." *Riveon Lematematika* **3** (1949):25-27, 38. (Reprinted in D. Jarden, *Recurring Sequences*, 3rd ed. [Jerusalem: Riveon Lematematika, 1973].)
6. Donald E. Knuth & Herbert S. Wilf. "The Power of a Prime that Divides a Generalized Binomial Coefficient." *J. reine angew. Math.* **396** (1989):212-19.
7. E. Lucas. "Sur les congruences des nombres eulériens et des coefficients différentiels des fonctions trigonométriques, suivant un module premier." *Bull. Soc. Math. France* **6** (1877-1878):49-54.
8. E. Lucas. "Théorie des fonctions numérique simplement périodiques." *Amer. J. Math.* **1** (1878):184-240.
9. Richard J. McIntosh. "A Generalization of a Congruential Property of Lucas." *Amer. Math. Monthly* **99** (1992):231-38.
10. D. W. Robinson. "The Fibonacci Matrix Modulo *m*." *The Fibonacci Quarterly* **1.1** (1963): 29-36.

AMS Classification Numbers: 11B39, 11B50, 11B65

❖❖❖