

RESIDUES OF GENERALIZED BINOMIAL COEFFICIENTS MODULO A PRIME

JOHN M. HOLTE

ABSTRACT. Given a sequence $\{u_n\}$ of positive integers generated by $u_1 = 1, u_2 = a, u_n = au_{n-1} + bu_{n-2} (n \geq 3)$, define the generalized factorial $[n]! = u_1 u_2 \cdots u_n$ and the generalized binomial coefficient $C(m, n) = [m+n]! / ([m]![n]!)$. An 1878 theorem of Lucas gives a formula for the residues modulo a prime of ordinary ($u_n = n$) binomial coefficients $B(m, n)$, and Wells (*Abstracts* **14** (1993), 32) has proven one for the generalized case. The author's proof of the formula when $\{u_n\}$ are the Fibonacci numbers (A Lucas-type theorem for fibonomial-coefficient residues, *Fibonacci Quart.* **32** (1994), 60–68) is extended to give a simpler proof of the generalized Lucas formula in the following form. Let p be a prime, $r = \min\{n > 0 : p|u_n\}$, $t = \text{period of } \{u_n \bmod p\}$, $s = t/r$, $n' = n \div r, n'' = n' \bmod s$, and $n^* = n \bmod t$. **Theorem:** Assume $p \nmid b$. Let $\lambda = \max\{0, m'' + n'' - (p-1)\}$. Then $C(m, n) \equiv B(m', n')B(m'', n'' + \lambda s)^{-1}C(m^*, n^* + \lambda t) \pmod{p}$. As a consequence, the pattern of residues is that of the array of binomial coefficients superimposed upon a doubly periodic “tiling” by s^2 different $r \times r$ matrices.

1. INTRODUCTION

A remarkable theorem of E. Lucas [10] provides a simple way to compute the binomial coefficient $\binom{N}{m}$ modulo a prime p in terms of the binomial coefficients of the base- p digits of N and m : If $N = \sum N_j p^j$ and $m = \sum m_j p^j$ where $0 \leq N_j, m_j < p$, then

$$\binom{N}{m} \equiv \prod \binom{N_j}{m_j} \pmod{p}.$$

This paper will generalize the following alternative version of Lucas's theorem: Let

$$B(m, n) = \binom{m+n}{m} = \frac{(m+n)!}{m!n!};$$

then

$$B(m, n) \equiv B(m \div p, n \div p)B(m \bmod p, n \bmod p) \pmod{p}$$

where $m \div p$ is the integer quotient of m by p , and $m \bmod p$ is the remainder. It follows that if $m = \sum m_j p^j$ and $n = \sum n_j p^j$ where $0 \leq m_j, n_j < p$, then

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

As a corollary, $p|B(m, n)$ if and only if $m_{j_1} + n_j \geq p$ for some j .

This theorem also implies that the residues of Pascal's triangle modulo p have a self-similar structure; see, e.g., [12], [2], [4], [5], [9], [17], and [1]. For example, if $p = 3$, then $[B(m, n) \bmod p]$ for $0 \leq m, n < 9$ is given as follows:

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 2 & 2 & 2 & 0 & 0 & 0 \\ 1 & 2 & 0 & 2 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \equiv \begin{bmatrix} 1\mathbf{B} & 1\mathbf{B} & 1\mathbf{B} \\ 1\mathbf{B} & 2\mathbf{B} & 0\mathbf{B} \\ 1\mathbf{B} & 0\mathbf{B} & 0\mathbf{B} \end{bmatrix} \pmod{p},$$

where

$$\mathbf{B} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 3 \\ 1 & 3 & 6 \end{bmatrix} \equiv \begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 0 \\ 1 & 0 & 0 \end{bmatrix} \pmod{p},$$

so this matrix is the tensor (or, Kronecker) product $\mathbf{B} \otimes \mathbf{B} \bmod p$. Generally, as noted in [11], modulo p we have that $[B(m, n) \bmod p]$ for $0 \leq m, n < p^k$ will be $\mathbf{B}^{\otimes k}$, the k -fold tensor product of $\mathbf{B} = [B(i, j) \bmod p]$ where $0 \leq i, j < p$. Note that matrix indices start at index pair $(0, 0)$.

Generalized binomial coefficients are defined corresponding to a given sequence $\langle u_n \rangle$ by replacing $n!$ by the product of u_1 through u_n . This paper uses recurrence-relation techniques to deduce generalizations of Lucas's theorem for generalized binomial coefficients based on a sequence generated by a second-order recurrence relation (see Theorems 1 and 3). One resulting generalization is equivalent to the theorem (Theorem 4 below) obtained by Wells [13] by an intricate analysis. The new approach to the proof clarifies and explains the complexities of Wells's formula.

2. THE UNDERLYING SEQUENCE $\langle u_n \rangle$

Definition 1. Let $a, b \in \mathbb{Z}$. Let p be a prime. Define the sequence $\langle u_n \rangle$ recursively as follows:

$$u_0 = 0; u_1 = 1; u_n = au_{n-1} + bu_{n-2} \quad \text{for } n = 2, 3, 4, \dots$$

(or $u_1 = 1; u_2 = a; u_n = au_{n-1} + bu_{n-2}$ for $n = 3, 4, 5, \dots$).

For example, when $a = 2$ and $b = -1$, then $u_n = n$; when $a = 1 + q$ and $b = -q$, then $u_n = 1 + q + q^2 + \dots + q^{n-1}$; and when $a = 1$ and $b = 1$, then $u_n = F_n$, the n^{th} Fibonacci number.

Definition 2. Let r denote the rank of apparition of p ; thus, $r = \min\{n \in \mathbb{N} : u_n \equiv 0 \pmod{p}\}$. Let t denote the (least) period of $\langle u_n \bmod p \rangle$, if it exists. Let $s = t/r$.

From now on, consider the prime p and the integers a and b fixed, and assume a and b are not both zero. We shall usually assume that $p \nmid b$. If $p|b$, then $u_n \equiv a^{n-1} \pmod{p}$, and so either $p|a$ and $u_n \equiv 0 \pmod{p}$ for $n \geq 2$ while $u_1 = 1$ so that t is undefined, or $p \nmid a$ and $r = \infty$. In any case, the recurrence relation $u_n \equiv au_{n-1} + bu_{n-2} \pmod{p}$ defines a transformation

$$\begin{bmatrix} u_{n+1} \\ u_n \end{bmatrix} \equiv \begin{bmatrix} a & b \\ 1 & 0 \end{bmatrix} \begin{bmatrix} u_n \\ u_{n-1} \end{bmatrix} \pmod{p}$$

mapping $\{0, \dots, p-1\}^2$ to itself. If $p \nmid b$, then the transformation is invertible, and consequently it must be periodic with period $t \leq p^2$, and, since $u_0 = 0$ and 0 repeats, $r \leq t$.

The following basic addition formula, which appears, e.g., in [7], may be proved by induction.

Lemma 1. (*Extended recurrence*) For $m \geq 1$ and $n \geq 0$,

$$u_{m+n} = u_m u_{n+1} + b u_{m-1} u_n.$$

Many basic properties of the sequence $\langle u_n \rangle$ follow immediately from this lemma.

Corollary 0. Let $z = \min\{n \in \mathbb{N} : u_n = 0\}$. Then $z > 1$, and if $z < \infty$, then $\{n \in \mathbb{N} : u_n = 0\} = \{z, 2z, 3z, \dots\}$.

Proof. If $z < \infty$, Lemma 1 implies that

$$u_{kz+n} = u_{kz} u_{n+1} + b u_{kz-1} u_n,$$

from which the conclusion easily follows by induction if $b \neq 0$. If $b = 0$, then $u_n = a^{n-1}$ for $n > 0$ where $a \neq 0$ (by the assumption above), so $z = \infty$. \square

Corollary 1. If $p \nmid b$, then $\{n \in \mathbb{N} : u_n \equiv 0 \pmod{p}\} = \{r, 2r, 3r, \dots\}$.

Corollary 2. If $p \nmid b$, then s (defined as t/r) is an integer.

Corollary 3. If $r < \infty$, then for $k = 1, 2, 3, \dots$,

$$b u_{kr-1} \equiv u_{kr+1} \equiv u_{r+1}^k \pmod{p}.$$

Corollary 4. If $p \nmid b$, then $u_1 = 1, u_{r+1}, u_{2r+1}, \dots, u_{(s-1)r+1}$ —or, equivalently, u_{r+1}^k for $0 \leq k < s$ —are all distinct modulo p .

Corollary 5. If $p \nmid b$, then the sequence $\langle u_{r+1}^n \pmod{p} \rangle_{n=0}^\infty$ has period s : $u_{r+1}^n \equiv u_{r+1}^{n \bmod s} \pmod{p}$.

Corollary 6. If $p \nmid b$, then $s|p-1$.

Definition 3. The rank of apparition of k , denoted $r(k)$, is the least index n for which k divides u_n : $r(k) = \min\{n \in \mathbb{N} : k|u_n\}$. (If k does not divide any u_n , then $r(k) = \infty$.) Note that $r = r(p)$.

Definition 4. The sequence $\langle u_n \rangle$ is regularly divisible by p if, for every positive integer i , $\{n \in \mathbb{N} : p^i | u_n\} = \{kr(p^i) : k \in \mathbb{N}\}$.

Corollary 7. (*Wells*) If $p \nmid b$, then the sequence $\langle u_n \rangle$ is regularly divisible by p .

3. GENERALIZED BINOMIAL COEFFICIENTS

Definition 5. Given $\langle u_n \rangle$, define the generalized, or bracket, factorial $[n]!$ for $n = 0, 1, 2, \dots$ by

$$[n]! = \prod_{j=1}^n u_j.$$

For $m \geq 0$ and $n \geq 0$, define the generalized binomial coefficient $C(m, n)$ by

$$C(m, n) = \binom{m+n}{m} = \frac{[m+n]!}{[m]![n]}.$$

If some factors are zero, then it is to be understood that zeros in the numerator and denominator are to be cancelled in pairs. By Corollary 0, if there are some zero factors u_j , their indices j are multiples of some $z > 1$, so the number of zero factors in the numerator will either equal the number in the denominator or exceed it by 1.

When $a = 2$ and $b = -1$, then $u_n = n$ and the generalized binomial coefficients become the ordinary binomial coefficients: $C(m, n) = B(m, n)$. When $a = 1 + q$ and $b = -q$, then $u_n = 1 + q + q^2 + \dots + q^{n-1}$ and the generalized binomial coefficients are the Gauss q -binomial coefficients. When $a = 1$ and $b = 1$, then $u_n = F_n$ and the generalized binomial coefficients become the fibonomial coefficients.

Obviously, the generalized binomial coefficients are symmetric: $C(m, n) = C(n, m)$. Also, they satisfy the following *boundary conditions*:

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

Lemma 2. (*Basic Recurrence*) For $m \geq 1, n \geq 1$,

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

Proof.

$$\begin{aligned} & u_{m+1}C(m, n-1) + bu_{n-1}C(m-1, n) \\ &= \frac{u_{m+1}[m+n-1]!u_n}{[m]![n-1]!u_n} + \frac{u_m bu_{n-1}[m-1+n]!}{u_m[m-1]![n]} \\ &= \frac{[m+n-1]!(u_{m+1}u_n + bu_mu_{n-1})}{[m]![n]} \\ &= C(m, n), \end{aligned}$$

because $u_n u_{m+1} + bu_{n-1} u_m = u_{n+m}$, by Lemma 1. \square

Corollary. *If a and b are integers, then the generalized binomial coefficients are all integers.*

4. GENERALIZED BINOMIAL COEFFICIENTS MODULO p

When $p|b$, the generalized binomial coefficients modulo p are very simple. If $p|b$, then $u_n \equiv a^{n-1} \pmod{p}$, and, by Lemma 2, $C(m, n) \equiv u_{m+1}C(m, n-1) \pmod{p}$.

Also $C(m, 0) = 1$ for $m \geq 0$. Therefore, for $m, n \geq 0$,

$$\text{if } p|b, \text{ then } C(m, n) \equiv a^{mn} \pmod{p}.$$

Here $0^0 \equiv 1$.

When $p \nmid b$, the pattern of the residues is more complex. There may be a self-similar pattern, as in the case of binomial coefficients presented above. But the pattern may be more complicated. For example, see Table 1 for the layout of Fibonomial coefficients modulo 3.

When $p \nmid b$, a formula for the mod- p residues of $C(m, n)$ may be derived in three steps: (1) Show that $C(m, n) \equiv 0 \pmod{p}$ when $m \bmod r + n \bmod r \geq r$; (2) find a recurrence for $C'(m, n)$, defined as $C(mr, nr)$, and solve it; and (3) complete the solution by using the basic recurrence relation in Lemma 2. This procedure parallels and extends that given in [6], which may be consulted for further details.

Notation: If $r < \infty$, then for each nonnegative integer n , let

$$\begin{aligned} n_0 &= n \bmod r, \\ n' &= n \div r, \\ n^* &= n \bmod t, \\ n'' &= n^* \div r = n' \bmod s. \end{aligned}$$

Lemma 3. *If $p \nmid b$, then*

$$C(m, n) \equiv 0 \pmod{p} \text{ when } m_0 + n_0 \geq r.$$

Proof. This result is a consequence of Knuth and Wilf's generalization of Kummer's theorem: According to [8], $C(m, n)$ will be divisible by p if there is a carry across the radix point when m/r and n/r are added in base p ; this happens when $m_0 + n_0 \geq r$. \square

Lemma 4. (*r-step recurrence*) *If $p \nmid b$, then for every $m \geq 1$ and $n \geq 1$,*

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

Proof. For $h = 1, 2, \dots, r-1$, we have, by Lemma 2,

$$\begin{aligned} C(mr, (n-1)r + h) &\equiv \\ u_{mr+1} C(mr, (n-1)r + h - 1) &+ b u_{(n-1)r+h-1} C((m-1)r + r - 1, (n-1)r + h) \\ &\equiv u_{mr+1} C(mr, (n-1)r + h - 1) \pmod{p}, \end{aligned}$$

because $C((m-1)r + r - 1, (n-1)r + h) \equiv 0$, by Lemma 3. Together with Corollary 3, this implies that

$$C(mr, (n-1)r + r - 1) \equiv u_{r+1}^{m(r-1)} C(mr, (n-1)r) \pmod{p}. \quad (1)$$

Similarly,

$$C((m-1)r + r - 1, nr) \equiv u_{r+1}^{n(r-1)} C((m-1)r, nr) \pmod{p}. \quad (2)$$

1 1 1 1	1 1 1 1	1 1 1 1	1 1 1 1	1 1 1 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	1 1 2 0	2 2 1 0	1 1 2 0	2 2 1 0	1 1 2 0
1 2 0 0	1 2 0 0	1 2 0 0	1 2 0 0	1 2 0 0	1 2 0 0	1 2 0 0	1 2 0 0	1 2 0 0
1 0 0 0	2 0 0 0	1 0 0 0	2 0 0 0	1 0 0 0	2 0 0 0	1 0 0 0	2 0 0 0	1 0 0 0
1 2 1 2	2 1 2 1	0 0 0 0	1 2 1 2	2 1 2 1	0 0 0 0	1 2 1 2	2 1 2 1	0 0 0 0
1 2 2 0	1 2 2 0	0 0 0 0	2 1 1 0	2 1 1 0	0 0 0 0	1 2 2 0	1 2 2 0	0 0 0 0
1 1 0 0	2 2 0 0	0 0 0 0	1 1 0 0	2 2 0 0	0 0 0 0	1 1 0 0	2 2 0 0	0 0 0 0
1 0 0 0	1 0 0 0	0 0 0 0	2 0 0 0	2 0 0 0	0 0 0 0	1 0 0 0	1 0 0 0	0 0 0 0
1 1 1 1	0 0 0 0	0 0 0 0	1 1 1 1	0 0 0 0	0 0 0 0	1 1 1 1	0 0 0 0	0 0 0 0
1 1 2 0	0 0 0 0	0 0 0 0	2 2 1 0	0 0 0 0	0 0 0 0	1 1 2 0	0 0 0 0	0 0 0 0
1 2 0 0	0 0 0 0	0 0 0 0	1 2 0 0	0 0 0 0	0 0 0 0	1 2 0 0	0 0 0 0	0 0 0 0
1 0 0 0	0 0 0 0	0 0 0 0	2 0 0 0	0 0 0 0	0 0 0 0	1 0 0 0	0 0 0 0	0 0 0 0
1 2 1 2	1 2 1 2	1 2 1 2	2 1 2 1	2 1 2 1	2 1 2 1	0 0 0 0	0 0 0 0	0 0 0 0
1 2 2 0	2 1 1 0	1 2 2 0	1 2 2 0	2 1 1 0	1 2 2 0	0 0 0 0	0 0 0 0	0 0 0 0
1 1 0 0	1 1 0 0	1 1 0 0	2 2 0 0	2 2 0 0	2 2 0 0	0 0 0 0	0 0 0 0	0 0 0 0
1 0 0 0	2 0 0 0	1 0 0 0	1 0 0 0	2 0 0 0	1 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0
1 1 1 1	2 2 2 2	0 0 0 0	2 2 2 2	1 1 1 1	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0
1 1 2 0	1 1 2 0	0 0 0 0	1 1 2 0	1 1 2 0	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0
1 2 0 0	2 1 0 0	0 0 0 0	2 1 0 0	1 2 0 0	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0
1 0 0 0	1 0 0 0	0 0 0 0	1 0 0 0	1 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0
1 2 1 2	0 0 0 0	0 0 0 0	2 1 2 1	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0
1 2 2 0	0 0 0 0	0 0 0 0	1 2 2 0	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0
1 1 0 0	0 0 0 0	0 0 0 0	2 2 0 0	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0
1 0 0 0	0 0 0 0	0 0 0 0	1 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0
1 1 1 1	1 1 1 1	1 1 1 1	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0
1 1 2 0	2 2 1 0	1 1 2 0	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0
1 2 0 0	1 2 0 0	1 2 0 0	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0
1 0 0 0	2 0 0 0	1 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0
1 2 1 2	2 1 2 1	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0
1 2 2 0	1 2 2 0	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0
1 1 0 0	2 2 0 0	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0
1 0 0 0	1 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0
1 1 1 1	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0
1 1 2 0	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0
1 2 0 0	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0
1 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0

TABLE 1. The Fibonomial coefficients modulo 3

By Lemma 2 again,

$$C(mr, nr) \equiv u_{mr+1}C(mr, nr-1) + bu_{nr-1}C(mr-1, nr) \pmod{p}.$$

Equations (1) and (2) and Corollary 3 transform this result into the desired conclusion. \square

Introduce $C'(m, n) = C(mr, nr)$. By Lemma 4,

$$C'(m, n) \equiv u_{r+1}^{rm}C'(m, n-1) + u_{r+1}^{rn}C'(m-1, n) \pmod{p}. \quad (3)$$

Also

$$C'(m, 0) \equiv 1 \quad \text{and} \quad C'(0, n) \equiv 1 \pmod{p} \quad \text{for } m, n \geq 0. \quad (4)$$

One may check that the unique solution of congruence (3) satisfying the boundary conditions (4) is given by the following formula. This step involves the Pascal triangle rule, $B(m, n) = B(m, n-1) + B(m-1, n)$.

Lemma 5. *If $p \nmid b$, then for every $m \geq 0$ and $n \geq 0$,*

$$C(mr, nr) \equiv B(m, n)u_{r+1}^{rnm} \pmod{p}.$$

Definition 6. For $i, j \geq 0$ and for $0 \leq k, l < r$, let $A_{i,j}(k, l)$ denote the solution of the modulo- p recurrence relation

$$A_{i,j}(k, l) \equiv u_{ir+k+1}A_{i,j}(k, l-1) + bu_{jr+l-1}A_{i,j}(k-1, l)$$

for $0 \leq k, l < r$ together with the boundary conditions

$$A_{i,j}(k, -1) \equiv 0 \pmod{p} \quad \text{for } 1 \leq k < r$$

and

$$A_{i,j}(-1, l) \equiv 0 \pmod{p} \quad \text{for } 1 \leq l < r$$

and

$$A_{i,j}(0, 0) \equiv 1 \pmod{p}.$$

If $(i, j) = (m', n')$ and $(k, l) = (m_0, n_0)$, and if the final boundary condition in this definition were $A_{m',n'}(0, 0) \equiv C(m'r, n'r)$, then these would be the congruences satisfied by $C(m'r + m_0, n'r + n_0)$ for $0 \leq m_0, n_0 < r$. Because $u_{m'r+m_0+1} \equiv u_{m''r+m_0+1} \pmod{p}$ where $m'' = m' \pmod{r}$, and similarly for $u_{n'r+n_0-1}$, these congruences imply that

$$A_{m',n'}(m_0, n_0) \equiv A_{m'',n''}(m_0, n_0) \pmod{p}, \quad (5)$$

and so $C(m, n) \pmod{p}$ is given as follows.

Lemma 6. *If $p \nmid b$, then for $m \geq 0$ and $n \geq 0$,*

$$C(m, n) \equiv C(m'r, n'r)A_{m'',n''}(m_0, n_0) \pmod{p}.$$

Definition 7. If $r < \infty$, then for $i, j \geq 0$ and $0 \leq k, l < r$, define

$$H_{i,j}(k, l) = u_{r+1}^{rij}A_{i,j}(k, l).$$

By Corollary 5 and equation (5), $H_{m',n'}(m_0, n_0) \equiv H_{m'',n''}(m_0, n_0) \pmod{p}$.

5. THE PATTERN OF THE RESIDUES

Recall that $n_0 = n \bmod r$, $n' = n \div r$, $n^* = n \bmod t$, and $n'' = n' \bmod s$, where r is the rank of apparition of the prime p in $\langle u_n \rangle$, t is the period of $\langle u_n \bmod p \rangle$, and $s = t/r$. Lemmas 5 and 6 yield the following formula.

Theorem 1. *If $p \nmid b$, then, for $m, n \geq 0$,*

$$C(m, n) \equiv B(m', n')H_{m'', n''}(m_0, n_0) \pmod{p}.$$

This result simplifies nicely when $s = 1$. Then $m'' = n'' = 0$, and $H_{0,0}(m_0, n_0) \equiv C(m_0, n_0) \pmod{p}$ for $0 \leq m_0, n_0 < r$. Thus, in this case, as in the Pascal “triangle” case, the pattern of residues exhibits self-similarity upon scaling by p .

Corollary. *If $p \nmid b$ and $s = 1$, then, for $m, n \geq 0$,*

$$C(m, n) \equiv B(m', n')C(m_0, n_0) \pmod{p},$$

or, letting \mathbf{B} denote the matrix $[B(i, j)]$ with $0 \leq i, j < p$ and $\mathbf{C}_k = [C(m, n)]$ with $0 \leq m, n < rp^k$, we have

$$\mathbf{C}_k \equiv \mathbf{B}^{\otimes k} \otimes \mathbf{C}_0 \pmod{p}.$$

Example 1: q -binomial coefficients. Take $u_n = \sum_{k=0}^{n-1} q^k$ to obtain the q -binomial coefficients. If $p|q$, then $u_n \equiv 1$ for $n \geq 1$, so $C(m, n) \equiv 1 \pmod{p}$ for $m, n \geq 0$. So assume $p \nmid q$. Then $1 + q + \cdots + q^{r-1} = u_r \equiv 0 \pmod{p}$, so $q^r - 1 = qu_r - u_r \equiv 0 \pmod{p}$, whence $u_{r+1} = u_r + q^r \equiv 0 + 1 \equiv 1 \pmod{p}$. Thus, $(u_r, u_{r+1}) \equiv (u_0, u_1)$, and so the period, t , equals r , and so $s = 1$. Therefore, the corollary covers the case of q -binomial coefficients when $p \nmid q$, yielding a result given originally by Fray [3].

For a numerical example, take $q = 2$ and $p = 5$. Then $u_1 = 1, u_2 = 3, u_3 = 7, u_4 = 15, u_5 = 31, \dots$, whence $r = 4$, and

$$\mathbf{C}_0 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 3 & 7 & 15 \\ 1 & 7 & 35 & 155 \\ 1 & 15 & 155 & 1395 \end{bmatrix} \equiv \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 3 & 2 & 0 \\ 1 & 2 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \pmod{5},$$

so

$$\mathbf{C}_1 \equiv \mathbf{B} \otimes \mathbf{C}_0 \equiv \begin{bmatrix} 1\mathbf{C}_0 & 1\mathbf{C}_0 & 1\mathbf{C}_0 & 1\mathbf{C}_0 & 1\mathbf{C}_0 \\ 1\mathbf{C}_0 & 2\mathbf{C}_0 & 3\mathbf{C}_0 & 4\mathbf{C}_0 & 0\mathbf{C}_0 \\ 1\mathbf{C}_0 & 3\mathbf{C}_0 & 1\mathbf{C}_0 & 0\mathbf{C}_0 & 0\mathbf{C}_0 \\ 1\mathbf{C}_0 & 4\mathbf{C}_0 & 0\mathbf{C}_0 & 0\mathbf{C}_0 & 0\mathbf{C}_0 \\ 1\mathbf{C}_0 & 0\mathbf{C}_0 & 0\mathbf{C}_0 & 0\mathbf{C}_0 & 0\mathbf{C}_0 \end{bmatrix} \pmod{5}.$$

Individual residues may be calculated easily by the corollary. For example,

$$C(222, 161) \equiv B(55, 40)C(2, 1) \equiv B(2, 1)B(1, 3)B(0, 0)C(2, 1) \equiv 3 \cdot 4 \cdot 1 \cdot 2 \equiv 4 \pmod{5}.$$

Example 2: Fibonomial coefficients modulo p . Let $a = b = 1$ so that $u_n = F_n$, and, for illustration, let $p = 3$. Then $r = 4$, $t = 8$, and $s = 2$. The initial part of the table of fibonomial coefficients modulo 3 is given in Table 1.

$$\begin{bmatrix} 1\mathbf{H}_{0,0} & 1\mathbf{H}_{0,1} & 1\mathbf{H}_{0,0} & 1\mathbf{H}_{0,1} & 1\mathbf{H}_{0,0} & 1\mathbf{H}_{0,1} & 1\mathbf{H}_{0,0} & 1\mathbf{H}_{0,1} & 1\mathbf{H}_{0,0} & \cdots \\ 1\mathbf{H}_{1,0} & 2\mathbf{H}_{1,1} & 0\mathbf{H}_{1,0} & 1\mathbf{H}_{1,1} & 2\mathbf{H}_{1,0} & 0\mathbf{H}_{1,1} & 1\mathbf{H}_{1,0} & 2\mathbf{H}_{1,1} & 0\mathbf{H}_{1,0} & \cdots \\ 1\mathbf{H}_{0,0} & 0\mathbf{H}_{0,1} & 0\mathbf{H}_{0,0} & 1\mathbf{H}_{0,1} & 0\mathbf{H}_{0,0} & 0\mathbf{H}_{0,1} & 1\mathbf{H}_{0,0} & 0\mathbf{H}_{0,1} & 0\mathbf{H}_{0,0} & \cdots \\ 1\mathbf{H}_{1,0} & 1\mathbf{H}_{1,1} & 1\mathbf{H}_{1,0} & 2\mathbf{H}_{1,1} & 2\mathbf{H}_{1,0} & 2\mathbf{H}_{1,1} & 0\mathbf{H}_{1,0} & 0\mathbf{H}_{1,1} & 0\mathbf{H}_{1,0} & \cdots \\ 1\mathbf{H}_{0,0} & 2\mathbf{H}_{0,1} & 0\mathbf{H}_{0,0} & 2\mathbf{H}_{0,1} & 1\mathbf{H}_{0,0} & 0\mathbf{H}_{0,1} & 0\mathbf{H}_{0,0} & 0\mathbf{H}_{0,1} & 0\mathbf{H}_{0,0} & \cdots \\ 1\mathbf{H}_{1,0} & 0\mathbf{H}_{1,1} & 0\mathbf{H}_{1,0} & 2\mathbf{H}_{1,1} & 0\mathbf{H}_{1,0} & 0\mathbf{H}_{1,1} & 0\mathbf{H}_{1,0} & 0\mathbf{H}_{1,1} & 0\mathbf{H}_{1,0} & \cdots \\ 1\mathbf{H}_{0,0} & 1\mathbf{H}_{0,1} & 1\mathbf{H}_{0,0} & 0\mathbf{H}_{0,1} & 0\mathbf{H}_{0,0} & 0\mathbf{H}_{0,1} & 0\mathbf{H}_{0,0} & 0\mathbf{H}_{0,1} & 0\mathbf{H}_{0,0} & \cdots \\ 1\mathbf{H}_{1,0} & 2\mathbf{H}_{1,1} & 0\mathbf{H}_{1,0} & 0\mathbf{H}_{1,1} & 0\mathbf{H}_{1,0} & 0\mathbf{H}_{1,1} & 0\mathbf{H}_{1,0} & 0\mathbf{H}_{1,1} & 0\mathbf{H}_{1,0} & \cdots \\ 1\mathbf{H}_{0,0} & 0\mathbf{H}_{0,1} & 0\mathbf{H}_{0,0} & 0\mathbf{H}_{0,1} & 0\mathbf{H}_{0,0} & 0\mathbf{H}_{0,1} & 0\mathbf{H}_{0,0} & 0\mathbf{H}_{0,1} & 0\mathbf{H}_{0,0} & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \cdots \end{bmatrix}$$

TABLE 2. Submatrices of the fibonomial coefficients mod 3

By Definition 7,

$$\mathbf{H}_{0,0} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 2 & 0 \\ 1 & 2 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}; \mathbf{H}_{0,1} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 2 & 2 & 1 & 0 \\ 1 & 2 & 0 & 0 \\ 2 & 0 & 0 & 0 \end{bmatrix}; \mathbf{H}_{1,0} = \begin{bmatrix} 1 & 2 & 1 & 2 \\ 1 & 2 & 2 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}; \mathbf{H}_{1,1} = \begin{bmatrix} 1 & 2 & 1 & 2 \\ 2 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 2 & 0 & 0 & 0 \end{bmatrix}.$$

The structure of the matrix of fibonomial coefficients modulo 3, in accordance with Theorem 1, is given in Table 2. Wells [16] also gives a formula for these residues, one that is a special case of her Theorem 4 given below, and she provides a detailed description of the pattern of these submatrices from a “triangular” perspective.

Modulo $p = 2$, the Fibonacci sequence has $r = t = 3$, so $s = 1$ and, in accordance with the corollary, the fibonomial coefficients modulo 2 exhibit a pattern similar to that of the binomial coefficients, but with a different \mathbf{C}_0 . Wells [15] presents the equivalent of this result in an interesting context. The pattern of fibonomial coefficients modulo any prime is treated in [6].

Theorem 1 and the example show that the infinite matrix $[C(i, j) \bmod p]$ may be partitioned into $r \times r$ submatrices which form basic, natural “tiling units.” The pattern of the residues is obtained by superimposing the self-similar array of binomial coefficients modulo p upon the doubly periodic “tiling” of the plane by “hidden” $r \times r$ \mathbf{H} matrices. The binomial structure is self-similar upon scaling by the factor p . The $r \times r$ tiling structure has period s both horizontally and vertically, and so the period is t at the element level.

When $s = 1$, there are $p - 1$ different nonzero $r \times r$ submatrices, one for each nonzero residue value of $B(m', n') \bmod p$ times \mathbf{C}_0 . In the general case, by Corollary 4, there are also $s \cdot s$ different $H_{m'', n''}$ -matrices. This suggests that there may be $(p - 1)s^2$ different nonzero “tiles.” In the case of the the fibonomial coefficients modulo 3, the

exhibited matrix shows these seven submatrices:

$$1\mathbf{H}_{0,0}, 1\mathbf{H}_{0,1}, 1\mathbf{H}_{1,0}, 1\mathbf{H}_{1,1}, 2\mathbf{H}_{0,1}, 2\mathbf{H}_{1,0}, 2\mathbf{H}_{1,1}.$$

The missing case, $2\mathbf{H}_{0,0}$, must be sought farther out. The places of the missing $2\mathbf{H}_{0,0}$ are $(5, 11), (11, 5), (5, 13), (13, 5) \dots$ in Table 2.

Theorem 2. *Assume $p \nmid b$. The number of different nonzero $r \times r$ submatrices of the infinite matrix $[C(i, j) \bmod p]$ is $(p-1)s^2$.*

Proof. The proof is trivial for $s = 1$, so assume $s > 1$. First we verify that the tiles $\rho\mathbf{H}_{\mu,\nu}$ are distinct for different (ρ, μ, ν) 's with $1 \leq \rho < p$ and $0 \leq \mu, \nu < s$. By Definition 6 and Corollary 3, $A_{\mu,\nu}(0,0) \equiv 1$, $A_{\mu,\nu}(0,1) \equiv u_{\mu r+1} \equiv u_{r+1}^\mu$, and $A_{\mu,\nu}(1,0) \equiv bu_{\nu r-1} \equiv u_{r+1}^\nu \pmod{p}$, so by Definition 7, $H_{\mu,\nu}(0,0) \equiv u_{r+1}^{r\mu\nu}$, $H_{\mu,\nu}(0,1) \equiv u_{r+1}^{r\mu\nu+\mu}$, and $H_{\mu,\nu}(1,0) \equiv u_{r+1}^{r\mu\nu+\nu} \pmod{p}$. Note that $p \nmid u_{r+1}$. If $\rho\mathbf{H}_{\mu,\nu} \equiv \tilde{\rho}\mathbf{H}_{\tilde{\mu},\tilde{\nu}} \pmod{p}$ where $1 \leq \rho, \tilde{\rho} < p$ and $0 \leq \mu, \nu, \tilde{\mu}, \tilde{\nu} < s$, or $\mathbf{H}_{\mu,\nu} \equiv \rho_1\mathbf{H}_{\tilde{\mu},\tilde{\nu}} \pmod{p}$ where $\rho_1 \equiv \rho^{-1}\tilde{\rho}$, then $u_{r+1}^{r\mu\nu} \equiv \rho_1 u_{r+1}^{r\tilde{\mu}\tilde{\nu}}$, $u_{r+1}^{r\mu\nu+\mu} \equiv \rho_1 u_{r+1}^{r\tilde{\mu}\tilde{\nu}+\tilde{\mu}}$, and $u_{r+1}^{r\mu\nu+\nu} \equiv \rho_1 u_{r+1}^{r\tilde{\mu}\tilde{\nu}+\tilde{\nu}} \pmod{p}$, so $u_{r+1}^\mu \equiv u_{r+1}^{\tilde{\mu}}$ and $u_{r+1}^\nu \equiv u_{r+1}^{\tilde{\nu}} \pmod{p}$, whence, by Corollary 4, $\mu = \tilde{\mu}$ and $\nu = \tilde{\nu}$, and therefore going back one finds $\rho_1 \equiv 1$, i.e., $\rho = \tilde{\rho}$. This proves that the mapping $(\rho, \mu, \nu) \mapsto \rho\mathbf{H}_{\mu,\nu}$ is one to one.

It remains to show that, given (ρ, μ, ν) with $1 \leq \rho < p$ and $0 \leq \mu, \nu < s$, one can find (m, n) such that $B(m', n') \equiv \rho \pmod{p}$ and $m'' = \mu$ and $n'' = \nu$. Let $m = r(1 + ip)$ and $n = r(\rho - 1 + jp^2)$, choosing i and j so that $i \equiv \mu - 1 \pmod{s}$, $j \equiv \nu - (\rho - 1) \pmod{s}$, and $0 \leq i, j < p$. Since $p \equiv 1$ and $p^2 \equiv 1 \pmod{s}$, by Corollary 6, we have

$$m'' = (m \div r) \bmod s = (1 + ip) \bmod s = (1 + i) \bmod s = \mu,$$

$$n'' = (\rho - 1 + jp^2) \bmod s = (\rho - 1 + j) \bmod s = \nu,$$

and, by Lucas's theorem,

$$B(m', n') \equiv B(0, j)B(i, 0)B(1, \rho - 1) \equiv \rho \pmod{p}.$$

(Modification of this construction can yield infinitely many occurrences of each possible tile.) \square

6. GENERALIZATION OF LUCAS'S THEOREM

Using Theorem 1, one may express $H_{m'', n''}(m_0, n_0)$ in terms of $C(m, n)$ for small values of (m, n) . The tricky part is to work around the cases when $B(m', n') \equiv 0 \pmod{p}$. Here is one approach.

Given (m, n) , let $\mu = m^*$ and $\nu = n^* + \lambda t$, where λ will be chosen later. By Theorem 1,

$$C(\mu, \nu) \equiv B(\mu', \nu')H_{\mu'', \nu''}(\mu_0, \nu_0) \pmod{p}. \quad (6)$$

Now,

$$\begin{aligned}
\mu_0 &= m^* \bmod r = (m \bmod t) \bmod r = m \bmod r = m_0, \\
\mu' &= m^* \div r = m'', \\
\mu'' &= \mu' \bmod s = m'' \bmod s = m'', \\
\nu_0 &= (n^* + \lambda t) \bmod r = n^* \bmod r = n_0, \\
\nu' &= (n^* + \lambda t) \div r = (n \bmod t) \div r + \lambda s = n'' + \lambda s, \quad \text{and} \\
\nu'' &= ((n^* + \lambda t) \bmod t) \div r = (n^* \bmod t) \div r = n^* \div r = n''.
\end{aligned} \tag{7}$$

Thus, equation (6) becomes

$$C(m^*, n^* + \lambda t) \equiv B(m'', n'' + \lambda s) H_{m'', n''}(m_0, n_0) \pmod{p}.$$

Now if λ is chosen so that $p \nmid B(m'', n'' + \lambda s)$, then

$$H_{m'', n''}(m_0, n_0) \equiv B(m'', n'' + \lambda s)^{-1} C(m^*, n^* + \lambda t) \pmod{p}. \tag{8}$$

Theorem 3. *Assume $p \nmid b$. Let $\lambda = \max\{0, m'' + n'' - (p - 1)\}$. Then*

$$C(m, n) \equiv B(m', n') B(m'', n'' + \lambda s)^{-1} C(m^*, n^* + \lambda t) \pmod{p}.$$

Proof. By Corollary 6, $s|p-1$. If $s < p-1$, then actually $s < (p-1)/2$, so $m'' + n'' < p-1$, whence $\lambda = 0$ and $p \nmid B(m'', n'' + \lambda s)$. If $s = p-1$ and $m'' + n'' < p$, then again we have $\lambda = 0$ and $p \nmid B(m'', n'' + \lambda s)$. Assume $s = p-1$ and $m'' + n'' \geq p$. Now $n'' + \lambda s = n'' + \lambda(p-1) = \lambda p + (n'' - \lambda)$ and $0 \leq n'' - \lambda < p-1$. By Lucas's theorem, $B(m'', n'' + \lambda s) \equiv B(0, \lambda) B(m'', n'' - \lambda) \pmod{p}$, and this is not congruent to 0 as long as $m'' + n'' - \lambda \leq p-1$. Thus, $\lambda = m'' + n'' - (p-1)$ is actually the *minimum* value that works. Now, in every case, equation (8) and Theorem 1 imply the desired conclusion. \square

Thus, except when $s = p-1$ and $m'' + n'' \geq p$, the residue $C(m, n) \bmod p$ is given by this simple, symmetric expression:

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

Example 3. Consider the fibonomial coefficient $C(6, 29) \bmod 3$. It appears in the 7th row and 30th column of Table 1. Since $u_n = F_n$ and $p = 3$, then $r = 4, t = 8$, and $s = 2$. Let $m = 6$ and $n = 29$. Then $m_0 = 2, m' = 1, m^* = 6$, and $m'' = 1$, while $n_0 = 1, n' = 7, n^* = 5$, and $n'' = 1$. Here $m'' + n'' - (p-1) = 1 + 1 - 2 = 0$, so $\lambda = 0$. Now $B(m', n') = B(1, 7) = B(1, 2 \times 3 + 1) \equiv B(0, 2) B(1, 1) \equiv 2 \pmod{3}$ and $B(m'', n'' + \lambda s) = B(1, 1) = 2$ and $2^{-1} \equiv 2 \pmod{3}$ and $C(m^*, n^* + \lambda t) = C(6, 5) \equiv 2 \pmod{3}$, so $C(m, n) \equiv B(m', n') B(m'', n'')^{-1} C(m^*, n^*) \equiv 2 \cdot 2 \cdot 2 \equiv 2 \pmod{3}$.

Theorem 3 may also be used to go back and extend Lemma 4 to a full r -step recurrence formula. The result is stated in the following tidy formula.

Corollary. *If $p \nmid b$, then for $m, n \geq r$,*

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

In terms of the $r \times r$ matrices $\mathbb{G}_{i,j} := [C(ir + h, jr + k)]$, where $0 \leq h, k < r$ and $i, j \geq 0$, and the diagonal matrix $\mathbb{D} = \text{diag}\{u_{r+1}^0, u_{r+1}^1, \dots, u_{r+1}^{r-1}\}$, the conclusion of the corollary may be rewritten as

$$\mathbb{G}_{i,j} \equiv u_{r+1}^{ir} \mathbb{D} \mathbb{G}_{i,j-1} + u_{r+1}^{jr} \mathbb{G}_{i-1,j} \mathbb{D} \pmod{p}.$$

For binomial coefficients, $u_{r+1} = p + 1 \equiv 1 \pmod{p}$ and $\mathbb{D} = \mathbb{I}$, so $\mathbb{G}_{i,j} \equiv \mathbb{G}_{i,j-1} + \mathbb{G}_{i-1,j} \pmod{p}$, the $p \times p$ generalization of the Pascal triangle rule noted by Long [9]. For fibonomial coefficients modulo 2, $u_{r+1} = F_4 \equiv 1 \pmod{2}$ and again $\mathbb{D} = \mathbb{I}$, so $\mathbb{G}_{i,j} \equiv \mathbb{G}_{i,j-1} + \mathbb{G}_{i-1,j} \pmod{2}$, as noted by Wells [15]. For fibonomial coefficients modulo 3, which were considered in Example 2, $u_{r+1} = F_5 \equiv 2 \pmod{3}$ and $\mathbb{D} \equiv \text{diag}\{1, 2, 1, 2\}$, so that $\mathbb{G}_{i,j} \equiv \mathbb{D} \mathbb{G}_{i,j-1} + \mathbb{G}_{i-1,j} \mathbb{D} \pmod{3}$, which the reader may see illustrated in Table 2. (Note first that $\mathbb{D} \mathbb{H}_{i,j} \equiv \mathbb{H}_{i,j \pm 1}$ and $\mathbb{H}_{i,j} \mathbb{D} \equiv \mathbb{H}_{i \pm 1, j} \pmod{3}$.)

7. WELLS'S THEOREM

By means of a bit of translation, Theorem 3 may be transformed into Wells's theorem. Let $N = m + n$ and, correspondingly, $N_0 = N \bmod r$, $N' = N \div r$, and $N'' = N' \bmod s$. Then

$$C(m, n) = \begin{bmatrix} N \\ m \end{bmatrix}$$

and

$$B(m', n') = \binom{N'}{m'}.$$

Let $N' = \sum_{j \geq 1} N_j p^{j-1}$ and $m' = \sum_{j \geq 1} m_j p^{j-1}$ be the base- p representations of N' and m' . By the original Lucas theorem,

$$\binom{N'}{m'} \equiv \prod_{j \geq 1} \binom{N_j}{m_j} \pmod{p}.$$

The result of Wells [14] is as follows.

Theorem 4. (Wells) *If $p \nmid b$, then for $N'' \geq m''$,*

$$\begin{bmatrix} N \\ m \end{bmatrix} \equiv \binom{N''}{m''}^{-1} \prod_{j \geq 1} \binom{N_j}{m_j} \begin{bmatrix} N''r + N_0 \\ m''r + m_0 \end{bmatrix} \pmod{p},$$

and for $N'' < m''$,

$$\begin{bmatrix} N \\ m \end{bmatrix} \equiv \begin{cases} \binom{s + N''}{m''}^{-1} \prod_{j \geq 1} \binom{N_j}{m_j} \begin{bmatrix} t + N''r + N_0 \\ m''r + m_0 \end{bmatrix} \pmod{p} & \text{if } s < p - 1; \\ \binom{s}{m''}^{-1} \prod_{j \geq 1} \binom{N_j}{m_j} \begin{bmatrix} (N'' + 1)t + N''r + N_0 \\ m''r + m_0 \end{bmatrix} \pmod{p} & \text{if } s = p - 1 \end{cases}$$

where $N_0 = N \bmod r$, $N' = N \div r$, and $N'' = N' \bmod s$.

Proof. Let $n = N - m$. First assume $m_0 + n_0 \geq r$. Then $\begin{bmatrix} N \\ m \end{bmatrix} = C(m, n) \equiv 0 \pmod{p}$, by Lemma 3. Also $N_0 = m_0 + n_0 - r$, so for $Kr = N''r, t + N''r$, or $(N'' + 1)t + N''r$, we have $\begin{bmatrix} Kr + N_0 \\ m''r + m_0 \end{bmatrix} = C(m''r + m_0, (K - 1 - m'')r + n_0) \equiv 0 \pmod{p}$, again by Lemma 3, and so all congruences in the theorem's conclusion reduce to $0 \equiv 0$ when $m_0 + n_0 \geq r$. Next assume $m_0 + n_0 < r$. Theorem 3 and the theorem of Lucas imply that

$$\begin{bmatrix} N \\ m \end{bmatrix} \equiv \binom{m'' + n'' + \lambda s}{m''}^{-1} \prod_{j \geq 1} \binom{N_j}{m_j} \begin{bmatrix} m^* + n^* + \lambda t \\ m^* \end{bmatrix} \pmod{p},$$

where $\lambda = \max\{0, m'' + n'' - (p - 1)\}$. Refer to the mixed-radix addition

$$\begin{array}{r} m = m'''t + m''r + m_0 \\ + n = n'''t + n''r + n_0 \\ \hline N = N'''t + N''r + N_0 \end{array}$$

where $0 \leq m_0, n_0, N_0 < r, 0 \leq m'', n'', N'' < s$, and $0 \leq m''', n''', N''' < \infty$. Since $m_0 + n_0 < r$, there is no carry out of the rightmost column. If $N'' \geq m''$, then $m'' + n'' = N'' < s \leq p - 1$, so $\lambda = 0$ and $m'' + n'' + \lambda s = N''$ and $m^* + n^* + \lambda t = m''r + m_0 + n''r + n_0 = N''r + N_0$, so the first formula is correct. Now assume $N'' < m''$. Then there is a carry out of the second column, so $N'' = m'' + n'' - s$. If $s < p - 1$, then $m'' + n'' < 2s < p - 1$, so $\lambda = 0$ and $m'' + n'' + \lambda s = s + N'' + 0$ and $m^* + n^* + \lambda t = m''r + m_0 + n''r + n_0 = (s + N'')r + (m_0 + n_0) = t + N''r + N_0$, and the formula for this case follows. Finally, if $s = p - 1$, then $\lambda = m'' + n'' - (p - 1) = N''$ and $m'' + n'' + \lambda s = s + N'' + N''s = s + N''(1 + s) = p - 1 + N''p$, whence $\binom{m'' + n'' + \lambda s}{m''} \equiv \binom{p-1}{m''} \binom{N''}{0} \equiv \binom{s}{m''}$, and $m^* + n^* + \lambda t = N''r + N_0 + 1t + N''t$, and the final case follows. \square

Example 4. Let's find the value of the fibonomial coefficient $\begin{bmatrix} 35 \\ 6 \end{bmatrix}$ modulo 3. This is equivalent to Example 3. Here $p = 3, r = 4, t = 8$, and $s = 2$. Corresponding to $m = 6$ we have $m_0 = 2, m' = 1$, and $m'' = 1$. Similarly, for $N = 35$ we have $N_0 = 3, N' = 8$, and $N'' = 0$. Also $m_1 = 1, m_2 = 0, N_1 = 2$, and $N_2 = 2$. Here $N'' < m''$ and $s = p - 1$, so

$$\begin{aligned} \begin{bmatrix} N \\ m \end{bmatrix} &\equiv \binom{s}{m''}^{-1} \binom{N_1}{m_1} \binom{N_2}{m_2} \begin{bmatrix} (N'' + 1)t + N''r + N_0 \\ m''r + m_0 \end{bmatrix} \\ &\equiv \binom{2}{1}^{-1} \binom{2}{1} \binom{2}{0} \begin{bmatrix} (0 + 1)8 + 0 \cdot 4 + 3 \\ 1 \cdot 4 + 2 \end{bmatrix} \\ &\equiv 2 \cdot 2 \cdot 1 \cdot 2 \equiv 2 \pmod{3}. \end{aligned}$$

This result is consistent, of course, with the calculation based on Theorem 3.

REFERENCES

- [1] Bondarenko, Boris A., *Generalized Pascal Triangles and Pyramids: Their Fractals, Graphs and Applications*, translated by Richard C. Bollinger, Fibonacci Association, Santa Clara, CA, 1993.
- [2] Broomhead, W. Antony, Pascal (mod p), *Mathematical Gazette*, **56** (1972), 268-271.

- [3] Fray, Robert D., Congruence properties of ordinary and q -binomial coefficients, *Duke Math. J.* **34** (1967), 467–480.
- [4] Harborth, von Heiko, Über die Teilbarkeit im Pascal-Dreieck, *Mathematisch-physikalische Semesterberichte* **22** (1975), 13–21.
- [5] Hexel, Erhard and Horst Sachs, Counting residues modulo a prime in Pascal’s triangle, *Indian J. of Math.* **20** (1978), 91–105.
- [6] Holte, John M., A Lucas-type theorem for fibonomial-coefficient residues, *Fibonacci Quart.* **32** (1994), 60–68.
- [7] Horak, P. and L. Skula, A characterization of the second-order strong divisibility sequences, *Fibonacci Quart.* **23** (1985), 126–132.
- [8] Knuth, D. E. and H. S. Wilf, The power of a prime that divides a generalized binomial coefficient, *J. reine angew. Math.* **396** (1989), 212–219.
- [9] Long, Calvin T., Pascal’s triangle modulo p , *Fibonacci Quart.* **19** (1981), 458–463.
- [10] Lucas, E., Théorie des fonctions numériques simplement périodiques, *Amer. J. Math.* **1** (1878), 184–240.
- [11] Razpet, Marko, On divisibility of binomial coefficients, *Discrete Math.* **135** (1994), 377–379.
- [12] Roberts, J. B., On binomial coefficient residues, *Canadian J. of Math.* **9** (1957), 363–370.
- [13] Wells, Diana L., Lucas’ theorem for generalized binomial coefficients, *AMS Abstracts* **14** (1993), 32.
- [14] Wells, Diana L., Lucas’ theorem for generalized binomial coefficients, preprint.
- [15] Wells, Diana L., The Fibonacci and Lucas triangles modulo 2, *Fibonacci Quart.* **32** (1994), 111–123.
- [16] Wells, Diana L., Residue counts modulo three for the Fibonacci triangle, *Applications of the Fibonacci Numbers, Vol. 6 (Pullman, WA, 1994)*, 521–536, Kluwer Acad. Publ., Dordrecht, 1996.
- [17] Wolfram, S., Geometry of binomial coefficients, *Amer. Math. Monthly* **92** (1984), 566–571.

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