DEMONSTRATIO MATHEMATICA
Vol. XLII No 1 2009

D. Doan, B. Kivunge, J. J. Poole, J. D. H Smith,
T. Sykes, M. Teplitskiy

PARTIAL SEMIGROUPS AND PRIMALITY INDICATORS IN THE FRACTAL GENERATION OF BINOMIAL COEFFICIENTS TO A PRIME SQUARE MODULUS

Abstract. This paper, resulting from two summer programs of Research Experience for Undergraduates, examines the congruence classes of binomial coefficients to a prime square modulus as given by a fractal generation process for lattice path counts. The process depends on the isomorphism of partial semigroup structures associated with each iteration. We also consider integrality properties of certain critical coefficients that arise in the generation process. Generalizing the application of these coefficients to arbitrary arguments, instead of just to the prime arguments appearing in their original function, it transpires that integrality of the coefficients is indicative of the primality of the argument.

1. Introduction

The general topic of this paper is the investigation of a fractal generation process for modular binomial coefficients. Previous work in the area, more recently from a dynamical systems viewpoint, has most often focussed on the distinction between zero and non-zero congruences [1] [3] [6] [8] [9], connecting back to Kummer's classical results on the divisibility of binomial coefficients by prime powers [5]. Our concern is rather with an algebraic fractal generation process for each modulus, exhibiting isomorphisms of total or partial semigroup structures defined on sets of digits and on sets of

2000 *Mathematics Subject Classification*: Primary 11B65; Secondary 11A07, 11A51, 20M99.

Key words and phrases: binomial coefficient, Pascal's triangle, lattice paths, fractal, semigroup, partial algebra, rectangular band, primality test.

During the second summer of work on this project, Kivunge, Poole, Smith and Teplitskiy were partially supported by NSF grant DMS-0353880. Poole and Sykes received additional funding from the Alliance and the George Washington Carver Program.

squares under the *Pascal addition* or *tile sum* of Definition 2.3. Throughout the paper, p will denote a given prime number. Section 2 reviews the case of modulus p. (Although this case is already well understood, our algebraic approach will serve as a useful model for the more complex prime square case.) Theorem 2.4 gives an isomorphism from the (total) additive group C_p of integers modulo the prime p to a set of $p \times p$ tiles appearing in Pascal's square modulo p. The main theorem of the paper, proved in the final Section 6, is the corresponding result for modulus p^2 (Theorem 4.5). This theorem gives an isomorphism to a set of $p \times p$ tiles appearing in Pascal's square modulo p^2 from a partial semigroup structure D_p on an indexed set of digits modulo p^2 (Definition 3.1). The set of tiles here is the image of the homomorphism (4.3). The isomorphism, which also functions as the key iterative step in the fractal generation process (Corollary 4.6), is defined in terms of certain *production coefficients* (Definition 4.1) that may be viewed as modular harmonic sums, or discrete modular versions of the logarithmic integral $\int_1^r dt/t = \log r$. Section 5 generalizes the application of these coefficients to arbitrary arguments, instead of just to the prime arguments appearing in their original function. It transpires that integrality of the coefficients is indicative of the primality of the argument. Problems 5.5 and 5.6 ask for a determination of exact conditions for this integrality, and for a combinatorial interpretation of the coefficients in those cases where they are integral.

A distinguishing feature of our approach is the way we address binomial coefficients, using *Pascal's square* as partially displayed in Table 1.

$x\backslash y$	0	1	2	3	4	5	$\dots$
0	1	1	1	1	1	1	$\dots$
1	1	2	3	4	5	6	$\dots$
2	1	3	6	10	15	21	$\dots$
3	1	4	10	20	35	56	$\dots$
4	1	5	15	35	70	126	$\dots$
5	1	6	21	56	126	252	$\dots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

Table 1. Pascal's Square.

Thus the binomial coefficient $\binom{x+y}{y}$ appears in the location with coordinates (x, y). We consider the square as the result of the iterative construction process initialized by placing an entry of 1 at each location having at least one zero coordinate, and then filling in by the linear *assembly rule*

$$\binom{x+y}{y} = \binom{x+y-1}{y-1} + \binom{x-1+y}{y} \tag{1.1}$$

at each location with both coordinates positive. Displaying binomial coefficients in this form, rather than in the more customary Pascal's triangle, is well known to identify $\binom{x+y}{y}$ directly as the number of "geodesics" or minimal-length paths through points of the square lattice from $(0,0)$ to (x,y). Indeed, each such path arriving at (x,y) previously passed through either $(x,y-1)$ or $(x-1,y)$, while points on the border have a unique geodesic from the origin. In the fractal generation process embodied in Corollary 4.6, the expansion of each digit of Pascal's square modulo p^2 depends on the residues of its addressing coordinates x,y modulo p.

2. Prime moduli

We begin by considering an algebraic fractal construction of Pascal's square to the prime modulus p.

Lemma 2.1. *There is a $p \times p$ block*

$$\begin{array}{|cccccc}
\hline
1 & 1 & 1 & \dots & 1 & 1 \\
1 & 2 & 3 & \dots & p-1 & 0 \\
1 & 3 & \ddots & & 0 & 0 \\
\vdots & \vdots & & & \vdots & \vdots \\
1 & p-1 & 0 & \dots & 0 & 0 \\
1 & 0 & 0 & \dots & 0 & 0
\end{array}$$

appearing in Pascal's square modulo p. In particular, all the elements below the diagonal are zero.

Proof. A $p \times p$ block bordered on the left and the top by ones appears in the NW corner $\{(x,y) \mid 0 \le x, y < p\}$ of the ordinary, non-modular Pascal's square. Consider the diagonal $\{(x,y) \mid x+y=p\}$ just below the diagonal from the SW to the NE corner of the block. All the binomial coefficients appearing on that diagonal are of the form $\binom{p}{y}$ with $0 < y < p$. Now

$$\binom{p}{y} = \frac{p!}{y!(p-y)!}.$$

In this fraction, all the numbers multiplied together in the denominator are strictly less than p, so do not cancel the p appearing in the numerator. This implies that $\binom{p}{y}$ with $0 < y < p$ is divisible by p. Thus there are zeroes in the corresponding places of the modular square, and the rest of the block is completed by zeroes according to the assembly rule (1.1). ∎

Lemma 2.2. *For each $0 \leq r < p$, a $p \times p$ block of the form*

$$\begin{array}{|cccccc}
\hline
r & r & r & \dots & r & r \\
r & 2r & 3r & \dots & (p-1)r & 0 \\
r & 3r & \ddots & & 0 & 0 \\
\vdots & \vdots & & & \vdots & \vdots \\
r & (p-1)r & 0 & \dots & 0 & 0 \\
r & 0 & 0 & \dots & 0 & 0
\end{array}$$

is assembled according to the rule (1.1) *of Pascal's square modulo p.*

Proof. The assembly rule is linear, so the blocks of Lemma 2.2 are obtained as the multiples by r of the block of Lemma 2.1. ∎

Definition 2.3 (Pascal sum, tile sum). Given $p \times p$ blocks

$$\begin{array}{|cccc}
\hline
x_{11} & x_{12} & \dots & x_{1p} \\
x_{21} & \ddots & & x_{2p} \\
\vdots & & & \vdots \\
x_{p1} & x_{p2} & \dots & x_{pp}
\end{array}
\quad \text{and} \quad
\begin{array}{|cccc}
\hline
y_{11} & y_{12} & \dots & y_{1p} \\
y_{21} & \ddots & & y_{2p} \\
\vdots & & & \vdots \\
y_{p1} & y_{p2} & \dots & y_{pp}
\end{array},$$

their *Pascal sum* or *tile sum* is defined to be the $p \times p$ block obtained by filling in the bottom $p \times p$ right-hand corner

$$\begin{array}{|cccc}
\hline
z_{11} & z_{12} & \dots & z_{1p} \\
z_{21} & \ddots & & z_{2p} \\
\vdots & & & \vdots \\
z_{p1} & z_{p2} & \dots & z_{pp}
\end{array}$$

of the scheme

$$
\begin{array}{cccc|cccc}
 & & & & y_{11} & y_{12} & \cdots & y_{1p} \\
 & & & & y_{21} & \ddots & & y_{2p} \\
 & & & & \vdots & & & \vdots \\
 & & & & y_{p1} & y_{p2} & \cdots & y_{pp} \\
\hline
x_{11} & x_{12} & \cdots & x_{1p} & z_{11} & z_{12} & \cdots & z_{1p} \\
x_{21} & \ddots & & x_{2p} & z_{21} & \ddots & & z_{2p} \\
\vdots & & & \vdots & \vdots & & & \vdots \\
x_{p1} & x_{p2} & \cdots & x_{pp} & z_{p1} & z_{p2} & \cdots & z_{pp}
\end{array}
$$

according to the assembly rule (1.1) of Pascal's square.

THEOREM 2.4. *For $0 \leq r < p$, let $[r]$ denote the $p \times p$ block*

$$
\begin{array}{|cccc}
\hline
r & r & \cdots & r \\
r & \ddots & & 0 \\
\vdots & & & \vdots \\
r & 0 & \cdots & 0
\end{array}
$$

from Lemma 2.2. Then there is an isomorphism $r \mapsto [r]$ from the additive group C_p of integers modulo p to the set of $p \times p$ blocks under Pascal addition modulo p.

Proof. For each $0 \leq r, s < p$, consider the modular Pascal addition

$$
\begin{array}{cccc|cccc}
 & & & & s & s & \cdots & s \\
 & & & & s & \ddots & & 0 \\
 & & & & \vdots & & & \vdots \\
 & & & & s & 0 & \cdots & 0 \\
\hline
r & r & \cdots & r & * & & & \\
r & \ddots & & 0 & & & & \\
\vdots & & & \vdots & & & & \\
r & 0 & \cdots & 0 & & & &
\end{array}
$$

of $[r]$ to $[s]$. The square marked by $*$ is filled in as $r + s$ (modulo p). Because of the adjoining zeroes, the remaining squares in the same row and the same column as the marked square are also filled in as $r+s$. This creates $[r+s]$ as the Pascal sum of $[r]$ and $[s]$ modulo p. ∎

Corollary 2.5. *The Pascal square to a prime modulus p is generated by the following fractal process:*

(1) *Start with an initial configuration of* 1*;*
(2) *For each iterative step, the output configuration is obtained by applying the production rule $r \mapsto [r]$ to each entry of the input configuration.*

For $p=2$, the first steps of the process may be illustrated as follows:

0	0
0	1

→

1	0	1
0	1	1
1	1	0

→

2	00	01	10	11
00	1	1	1	1
01	1	0	1	0
10	1	1	0	0
11	1	0	0	0

→ ...

Here, each stage of the square is presented together with the addresses of its entries (in binary notation). The boldface numbers count the steps in the process. In the Pascal square mod p, the *ancestry* of the entry addressed by a given pair (x,y) of natural numbers consists of all those $p \times p$ blocks that expand in the generation process to include the (x,y)-entry, along with the single entries at each stage that have expanded to these respective $p \times p$ blocks. For example, in the above illustration modulo 2, the ancestry of the $(01,11)$-entry contains the 2×2 blocks starting at $(0,0)$ in Step 1 and $(00,10)$ in Step 2, as well as the $(0,0)$-entry of Step 0 and the $(0,1)$-entry in Step 1. The ancestry of the $(10,11)$-entry contains the 2×2 blocks starting at $(0,0)$ in Step 1 and $(10,10)$ in Step 2, as well as the $(0,0)$-entry of Step 0 and the $(1,1)$-entry in Step 1.

For each natural number x, let $\dots x_2 x_1 x_0$ be the base-p expansion of x, so that

$$x = \sum_{i=0}^{\infty} x_i p^i \tag{2.1}$$

with integers $0 \le x_i < p$. The following immediate consequence of Corollary 2.5 is a well-known instance of Kummer's criterion [3] [5].

Corollary 2.6. *If there is a natural number i such that $x_i + y_i \ge p$, then*

$$\binom{x+y}{y} \equiv 0 \pmod{p}.$$

Proof. The (x, y)-entry of Pascal's square modulo p includes an (x_i, y_i)-entry of a tile $[r]$ in its ancestry. By Lemma 2.2, this entry is 0, which expands to an all-zero tile at each subsequent step. ∎

3. The partial semigroup

Definition 3.1 of this section specifies the partial semigroup structure D_p, involving residues modulo p^2, that for the prime square case plays a role analogous to that played by the cyclic group C_p of residues modulo p in Theorem 2.4. The modular locations of the definition will correspond to the modulo p residues x_0, y_0 of coordinates x, y of absolute locations in Pascal's square, according to the notation of (2.1). This modular addressing is a key feature of our fractal generation process.

Definition 3.1. The *algebra of located residues modulo p* is defined to be the set D_p of all elements r_{xy} with $r \in \mathbb{Z}/p^2\mathbb{Z}$, $x, y \in C_p$ such that

$$\exists x' \equiv x \pmod p.\ \ \exists y' \equiv y \pmod p.\ \ \binom{x'+y'}{y'} \equiv r \pmod{p^2}. \tag{3.1}$$

The residues x, y modulo p are known as the *modular locations*. The *partial addition* on D_p is defined by

$$r_{x(y-1)} + s_{(x-1)y} = (r+s)_{xy} \tag{3.2}$$

if and only if $\exists x' \equiv x \pmod p$. $\exists y' \equiv y \pmod p$.

$$\binom{x'+y'-1}{y'-1} \equiv r \pmod{p^2}, \quad \binom{x'-1+y'}{y'} \equiv s \pmod{p^2}.$$

From the discussion of Remark 3.3 below, it will transpire that the algebra structure defined on D_p by (3.2) is a partial semigroup.

Example 3.2. Table 2 gives the partial addition table for D_2. The columns have been labelled in a different order to the rows, so that transposition of Pascal's square modulo 4 corresponds to transposition of the table. Note that 1_{11} and 3_{11} do not appear in D_2, according to Corollary 2.6.

Remark 3.3. One might choose to extend the partial addition (3.2) on the set D_p to a total addition

$$r_{xz} + s_{ty} = (r+s)_{xy} \tag{3.3}$$

on the set

$$T_p = \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} = \{r_{xy} \mid r \in \mathbb{Z}/p^2\mathbb{Z},\ x, y \in \mathbb{Z}/p\mathbb{Z}\}.$$

Note that the subset

$$\{0_{xy} \mid x, y \in \mathbb{Z}/p\mathbb{Z}\} \tag{3.4}$$

	0_{00}	0_{10}	0_{01}	0_{11}	1_{00}	1_{10}	1_{01}	2_{00}	2_{10}	2_{01}	2_{11}	3_{00}	3_{10}	3_{01}
0_{00}				0_{01}										
0_{01}		0_{00}				1_{00}			2_{00}				3_{00}	
0_{10}			0_{11}											
0_{11}	0_{10}				1_{10}			2_{10}				3_{10}		
1_{00}				1_{01}							3_{01}			
1_{01}		1_{00}				2_{00}			3_{00}				0_{00}	
1_{10}							2_{11}							0_{11}
2_{00}				2_{01}										
2_{01}		2_{00}				3_{00}			0_{00}				1_{00}	
2_{10}										0_{11}				
2_{11}					3_{10}							1_{10}		
3_{00}				3_{01}							1_{01}			
3_{01}		3_{00}				0_{00}			1_{00}				2_{00}	
3_{10}							0_{11}							2_{11}

Table 2. Partial addition on D_2.

is a subalgebra of T_p that forms a so-called *rectangular band* [7, §1.3]. It is apparent that the operation (3.3) is associative, making T_p a semigroup, namely the product of the cyclic group $\mathbb{Z}/p^2\mathbb{Z}$ with the rectangular band (3.4). However, T_p is certainly not a group, since for example $0_{00} + 0_{00} = 0_{00} = 0_{01} + 0_{00}$.

4. The fractal process

Just as in the modulo p case, the fractal generation process for Pascal's square modulo p^2 expands digits into $p \times p$ blocks. The expansion process involves multiplication of the modular locations of the digit by certain coefficients that may be viewed as modular harmonic sums, or discrete modular versions of $\int_1^r dt/t = \log r$.

DEFINITION 4.1. For each positive integer r less than p, define the *production coefficient*

$$\lambda_r = \frac{1}{1} + \frac{1}{2} + \cdots + \frac{1}{r} \tag{4.1}$$

as a residue modulo p (recalling that the non-zero residues $1, 2, \ldots, r$ are invertible modulo p). By convention for $r = 0$, the production coefficient λ_0 is defined to be zero.

For odd primes, the production coefficients are symmetrical.

LEMMA 4.2. *For odd p and $0 \leq r < p/2$, one has $\lambda_r = \lambda_{p-1-r}$.*

Proof. For $0 < s < p$, there is a congruence

$$s\left(\frac{1}{s} + \frac{1}{p-s}\right) = s\frac{1}{s} - (p-s)\frac{1}{p-s} = 1 - 1 = 0$$

modulo p, so that $\frac{1}{s} + \frac{1}{p-s} = 0$ [4, §7.8]. The statement of the lemma is proved by downward induction: it is trivially true for $r = (p-1)/2$. Suppose $\lambda_s = \lambda_{p-1-s}$. Then $(\lambda_s - \lambda_{p-1-s}) - (\lambda_{s-1} - \lambda_{p-1-(s-1)}) = \frac{1}{s} + \frac{1}{p-s} = 0$, so $\lambda_{s-1} - \lambda_{p-1-(s-1)} = 0$ as required. ∎

COROLLARY 4.3. *If p is odd, then $\lambda_{p-1} = \lambda_0 = 0$.*

Note that $\lambda_{p-1} = 1$ for $p = 2$. The key role of the production coefficients appears in the following:

DEFINITION 4.4. Suppose $r \in \mathbb{Z}/p^2\mathbb{Z}$, $x, y \in C_p$. Then the *located block* $[r]_{xy}$ is defined to be the $p \times p$ array of $\mathbb{Z}/p^2\mathbb{Z}$-elements

$$\begin{array}{|ccccc} r & r(1+p\lambda_1 x) & r(1+p\lambda_2 x) & \dots & r(1+p\lambda_{p-1} x) \\ r(1+p\lambda_1 y) & \dots & & & \vdots \\ r(1+p\lambda_2 y) & \dots & & & \vdots \\ \vdots & \dots & & & \vdots \\ r(1+p\lambda_{p-1} y) & \dots & \dots & \dots & \end{array} \tag{4.2}$$

completed according to the assembly rule (1.1) modulo p^2. (Since $\lambda_0 = 0$, the top left-hand entry may also be written in the equivalent forms $r(1+p\lambda_0 x) = r(1+p\lambda_0 y)$, consistent with the remaining first row and column entries respectively.)

The main theorem may now be stated as follows, along with its immediate corollary yielding the fractal generation process for Pascal's square modulo p^2.

THEOREM 4.5. *There is a homomorphism*

$$r_{xy} \mapsto [r]_{xy} \tag{4.3}$$

from the partial semigroup D_p of located residues modulo p^2 to the algebra of located $p \times p$ blocks under Pascal addition modulo p^2.

The proof of Theorem 4.5 is given in Section 6. (The homomorphism concept used in the statement of Theorem 4.5 is that of [2, 2.1.1(i)] — compare the beginning of Section 6.)

COROLLARY 4.6. *The Pascal square to a prime square modulus p^2 is generated by the following fractal process:*

(1) *Start with an initial configuration of* 1_{00}*;*
(2) *For each iterative step, the output configuration is obtained by applying the production rule $r_{xy} \mapsto [r]_{xy}$ to each modularly located entry of the input configuration.*

REMARK 4.7. The homomorphism of Theorem 4.5 cannot extend to the total semigroup T_p of Remark 3.3, since it would take associative additions of T_p to non-associative "unlocated" tile additions.

5. Generalized production coefficients

In this section, we digress from the context of Theorem 4.5 to consider the *generalized production coefficients*

$$(5.1)\quad \lambda_r(q) = \frac{1}{q}\left\{\binom{q+r}{q} - 1\right\} = \frac{1}{q\cdot r!}\{(q+r)(q+r-1)\dots(q+1) - r!\}$$

for arbitrary positive integers q and $0 < r < q$. For q prime, the generalized production coefficients reduce to the modular production coefficients of Definition 4.1 (see Corollary 5.2 below). Our concern is the question of when the generalized production coefficients take integral values. The following propositions suggest that integrality of the coefficients $\lambda_r(q)$ is an indicator of the primality of q. We use Landau's "big O" notation in an algebraic sense, to identify a certain integral multiple $\mathrm{O}(n)$ of an integer n (contrast with [4, §1.6]).

PROPOSITION 5.1. *Suppose that r is a prime divisor of a composite positive integer q. Then the generalized production coefficient $\lambda_r(q)$ is not integral.*

Proof. The generalized production coefficient (5.1) expands as

$$(5.2)\qquad \begin{aligned}\lambda_r(q) &= \frac{1}{q\cdot r!}\Big\{\mathrm{O}(q^2) + q\cdot r!\Big[\frac{1}{1}+\frac{1}{2}+\dots+\frac{1}{r}\Big]\Big\}\\ &= \frac{\mathrm{O}(q) + r! + \frac{r!}{2} + \dots + \frac{r!}{r-1} + (r-1)!}{r!},\end{aligned}$$

a fraction in which all the terms in the numerator and denominator are positive integers. Recalling that r divides q, it is apparent that the prime r is a divisor of each summand in the numerator except the last. Thus the numerator, not being congruent to 0 modulo r, does not contain a factor of

r that would cancel the prime factor r of the denominator. In other words, the coefficient $\lambda_r(q)$ is not integral in this case. ∎

Corollary 5.2. *If q is prime, then the generalized production coefficients reduce modulo q to the production coefficients of Definition 4.1.*

Proof. Equation (5.2) shows that (5.1) is congruent to (4.1) when q is the prime p of Section 4. ∎

Remark 5.3. For a prime r, the non-integrality condition of Proposition 5.1 is necessary for r to divide q, but not sufficient. For example, $\lambda_5(27)$ is not integral (although $\lambda_7(27)$ is).

Proposition 5.4. *The generalized production coefficient $\lambda_r(q)$ is integral for all positive integers r that are less than the smallest prime divisor p of q.*

Proof. For $r < p$, there is an integer

$$\binom{q+r}{q} - 1 = \frac{(q+r)\dots(q+1)}{r!} - 1 = \frac{qP(q)}{r!}, \tag{5.3}$$

where $P(q)$ is a polynomial in q with integer coefficients. For any positive integer $m \le r < p$, the number m does not divide q, and so $r!$ is coprime to q. Thus $r!$ cancels with $P(q)$ in the final term of (5.3), and

$$\lambda_r(q) = \frac{1}{q}\left\{\binom{q+r}{q} - 1\right\} = \frac{P(q)}{r!}$$

is also integral. ∎

Propositions 5.1 and 5.4 suggest the following:

Problem 5.5. For each positive integer q, determine exactly which values of r make the generalized production coefficient $\lambda_r(q)$ integral.

Problem 5.6. Is there a combinatorial interpretation of the coefficient $\lambda_r(q)$ in those cases for which it is integral?

6. Proof of the main theorem

This section is devoted to the proof of Theorem 4.5. The proof demonstrates the preservation of the located partial addition

$$r_{x(y-1)} + s_{(x-1)y} = (r+s)_{xy} \tag{6.1}$$

from D_p under the production rule (4.3). It depends on a local version of the transposition symmetry of the modulo p Pascal square.

Lemma 6.1. *In the context of (6.1), there is a congruence*

$$rx \equiv sy \pmod{p}. \tag{6.2}$$

Proof. For natural numbers x, y, one has

$$\binom{x+y-1}{x}x = \frac{(x+y-1)!}{(x-1)!(y-1)!} = \binom{x-1+y}{y}y. \tag{6.3}$$

The desired result (6.2) is then just the modulo p reduction of (6.3). ∎

In view of the anomalous behavior of λ_{p-1} for $p = 2$, it is convenient to treat that case separately.

Proposition 6.2. *There is a homomorphism $r_{xy} \mapsto [r]_{xy}$ from the algebra D_2 of located residues modulo 4 to the algebra of located 2×2 blocks under Pascal addition modulo 4.*

Proof. For $p = 2$, the block (4.2) completes to

$$[r]_{xy} = \begin{array}{|cc} \hline r & r(1+2x) \\ r(1+2y) & 2r(1+x+y) \end{array}\,.$$

Corresponding to the partial addition (6.1) in D_2, one then has the tile sum

$$\begin{array}{cc|cc} & & s & s[1+2(x-1)] \\ & & s(1+2y) & 2s(x+y) \\ \hline r & r(1+2x) & r+s+2(rx+sy) & (r+s)(1+2x) \\ r[1+2(y-1)] & 2r(x+y) & (r+s)(1+2y) & 2(r+s)(1+x+y) \end{array}$$

To verify the homomorphic property, it remains to establish that

$$rx + sy \equiv 0 \pmod 2.$$

But this follows immediately by the case $p = 2$ of Lemma 6.1. ∎

Example 6.3. The case $p = 3$ of Theorem 4.5 is also sufficiently direct that it is worth exhibiting explicitly. The block (4.2) now completes to

$$[r]_{xy} = \begin{array}{|ccc} \hline r & r(1+3x) & r \\ r(1+3y) & 2r+3r(x+y) & 3r(1+x+y) \\ r & 3r(1+x+y) & 6r(1+x+y) \end{array}\,.$$

The tile sum corresponding to the partial addition (6.1) in D_3 is

$$\begin{array}{cc|ccc} & & \vdots & \vdots & \vdots \\ & & s & 3s(x+y) & 6s(x+y) \\ \hline \dots & r & r+s & (r+s)+3s(x+y) & r+s \\ \dots & 3r(x+y) & r+s+3r(x+y) & \dots & \dots \\ \dots & 6r(x+y) & r+s & \dots & \dots \end{array}$$

To verify the homomorphic property, it remains to establish

$$3s(x+y) = 3(r+s)x \quad \text{and} \quad 3r(x+y) = 3(r+s)y.$$

These equations follow immediately by the case $p = 3$ of Lemma 6.1, namely $rx \equiv sy \pmod 3$.

For the proof of Theorem 4.5 in the general odd prime case, a fuller description of $[r]_{xy}$ is provided by Proposition 6.7 below. The proposition depends on three lemmas. The reciprocals on the right hand sides of the equations (6.4), (6.5) and (6.6) in the statements of the lemmas are interpreted as in Definition 4.1.

LEMMA 6.4. *For an odd prime p and $0 < y < p$, there is a congruence*

$$\binom{p-1+y}{y} \equiv py^{-1} \pmod{p^2}. \tag{6.4}$$

Proof.

$$\begin{aligned}\binom{p-1+y}{y} &= \frac{(p+y-1)(p+y-2)\dots(p+1)p}{y(y-1)\dots 2\cdot 1} \\ &\equiv \frac{(y-1)(y-2)\dots 2\cdot 1\cdot p}{y(y-1)\dots 2\cdot 1} \equiv py^{-1} \pmod{p^2}. \quad \blacksquare\end{aligned}$$

LEMMA 6.5. *For an odd prime p and $0 < y < p$, there is a congruence*

$$\binom{2p-1+y}{y} - \binom{p-1+y}{y} \equiv py^{-1} \pmod{p^2}. \tag{6.5}$$

Proof.

$$\begin{aligned}&\binom{2p-1+y}{y} - \binom{p-1+y}{y} \\ &= \frac{(2p+y-1)(2p+y-2)\dots(2p+1)2p}{y(y-1)\dots 2\cdot 1} \\ &\quad - \frac{(p+y-1)(p+y-2)\dots(p+1)p}{y(y-1)\dots 2\cdot 1} \\ &\equiv p\frac{(y-1)(y-2)\dots 2\cdot 1\cdot 2}{y(y-1)\dots 2\cdot 1} - p\frac{(y-1)(y-2)\dots 2\cdot 1}{y(y-1)\dots 2\cdot 1} \\ &\equiv p\frac{(y-1)(y-2)\dots 2\cdot 1}{y(y-1)\dots 2\cdot 1} \equiv py^{-1} \pmod{p^2}. \quad \blacksquare\end{aligned}$$

LEMMA 6.6. *For an odd prime p and $0 < y < p$, there is a congruence*

$$\binom{p+y+p-1}{p-1} - \binom{p-1+y}{p-1} \equiv py^{-1} \pmod{p^2}. \tag{6.6}$$

Proof.

$$\begin{aligned}&\binom{p+y+p-1}{p-1}\\&=\frac{(2p+y-1)(2p+y-2)\dots(2p+1)2p(2p-1)\dots(p+1)p}{(p+y)(p+y-1)\dots(p+1)p(p-1)\dots2\cdot1}\\&\equiv\frac{(2p+y-1)(2p+y-2)\dots(2p+1)2p}{y(y-1)\dots2\cdot1}\\&\equiv\binom{2p-1+y}{y}\pmod{p^2}.\end{aligned}$$

The desired result then follows by (6.5). ∎

Proposition 6.7. *If p is odd, then the located block $[r]_{xy}$ of (4.2) completes to*

$$\begin{array}{|ccccc}\hline r & \dots & r(1+p\lambda_j x) & \dots & r\\ \vdots & & & & \vdots\\ r(1+p\lambda_i y) & \dots & \dots & \dots & rpi^{-1}(1+x+y)\\ \vdots & & & & \vdots\\ r & \dots & rpj^{-1}(1+x+y) & \dots & -rp(1+x+y)\end{array}\tag{6.7}$$

Proof. By the linearity of the assembly rule (1.1), it suffices to prove that

$$\begin{array}{|ccccc}\hline 1 & \dots & 1+p\lambda_j x & \dots & 1\\ \vdots & & & & \vdots\\ 1+p\lambda_i y & \dots & \dots & \dots & pi^{-1}(1+x+y)\\ \vdots & & & & \vdots\\ 1 & \dots & pj^{-1}(1+x+y) & \dots & -p(1+x+y)\end{array}\tag{6.8}$$

is correctly completed from its left-hand column and top row according to (1.1) modulo p^2. By linearity and the symmetry of Pascal's square, it suffices in turn to prove that

$$\begin{array}{|ccccc}\hline 1 & \dots & 1 & \dots & 1\\ \vdots & & & & \vdots\\ 1 & \dots & \dots & \dots & pi^{-1}\\ \vdots & & & & \vdots\\ 1 & \dots & pj^{-1} & \dots & -1\end{array}\tag{6.9}$$

and

$$(6.10)\qquad \begin{array}{|ccccc} \hline 0 & \dots & p\lambda_j & \dots & 0 \\ \vdots & & & & \vdots \\ 0 & \dots & \dots & \dots & pi^{-1} \\ \vdots & & & & \vdots \\ 0 & \dots & pj^{-1} & \dots & -p \end{array}$$

are correctly completed from their left-hand columns and top rows according to (1.1) modulo p^2. Now the form of (6.9) in the top left hand corner of Pascal's square modulo p^2 follows by Lemma 6.4. On the other hand, the tile (6.10) is bordered on the left hand column and top row by the difference

$$(6.11)\qquad \begin{array}{|ccccc} \hline 1 & \dots & 1+p\lambda_j & \dots & 1 \\ \vdots & & & & \\ 1 & & & & \\ \vdots & & & & \\ 1 & & & & \end{array} \; - \; \begin{array}{|ccccc} \hline 1 & \dots & 1 & \dots & 1 \\ \vdots & & & & \\ 1 & & & & \\ \vdots & & & & \\ 1 & & & & \end{array} .$$

By (5.1) with $q = p$ and $r = j$, it is apparent that the completion of the left-hand term of (6.11) occupies the locations

$$\{(x, y) \mid p \leq x < 2p,\ 0 \leq y < p\}$$

in the modulo p^2 Pascal square. The completion of the right-hand term occupies the locations $\{(x, y) \mid 0 \leq x, y < p\}$ in the modulo p^2 Pascal square. That (6.10) completes as indicated then follows by Lemmas 6.5 and 6.6. ∎

Remark 6.8. On dividing the tile (6.10) by p, one obtains a curious natural example of the emergence of a symmetrical output (the right hand column and bottom row) from an asymmetrical input (the left hand column and top row) under the assembly rule (1.1) modulo p. For instance, the $p = 5$ case yields

$$\begin{array}{|ccccc} \hline 0 & 1 & 4 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 & 3 \\ 0 & 1 & 2 & 4 & 2 \\ 0 & 1 & 3 & 2 & 4 \end{array} .$$

The proof of the main theorem is now readily concluded along the lines exhibited for $p = 3$ by Example 6.3.

PROPOSITION 6.9. *For an odd prime p, there is a homomorphism* $r_{xy} \mapsto [r]_{xy}$ *from the algebra* D_p *of located residues modulo* p^2 *to the algebra of located* $p \times p$ *blocks under Pascal addition modulo* p^2.

Proof. Using Proposition 6.7, the top row of the tile sum $[r]_{x(y-1)} + [s]_{(x-1)y}$ is computed as follows:

$$\begin{array}{c|lllll} & \vdots & \dots & \dots & \dots & \\ & s & \dots & p(j-1)^{-1}s(x+y) & pj^{-1}s(x+y) & \dots \\ \hline r & r+s & \dots & (r+s)+p\lambda_{j-1}s(x+y) & (r+s)+p\lambda_j s(x+y) & \dots \end{array}$$

(recall $\lambda_1 = 1^{-1}$). By Lemma 6.1 (local symmetry), the typical entry

$$(r+s) + p\lambda_j s(x+y)$$

of the top row of the tile sum reduces to

$$(r+s)(1 + p\lambda_j x),$$

since the sy term may be replaced by rx. The top row of the tile sum is thus of the required form. By symmetry, the left hand column also appears in the required form, so that $[r]_{x(y-1)} + [s]_{(x-1)y}$ is indeed given by $[r+s]_{xy}$. ∎

Acknowledgment.

We are grateful to an anonymous referee for helpful comments on an earlier version of this paper.

References

[1] B. A. Bondarenko, *Generalized Triangles and Pyramids of Pascal* (Russian), Uzbek Academy of Sciences, Tashkent, 1990.

[2] P. Burmeister, *A Model Theoretic Oriented Approach to Partial Algebras*, Akademie-Verlag, Berlin, 1986.

[3] F. v. Haeseler, H.-O. Peitgen, G. Skorder, *Pascal's triangle, dynamical systems and attractors*, Ergodic Th. and Dynamical Systems, 12 (1992), 479–486.

[4] G. H. Hardy, E. M. Wright, *An Introduction to the Theory of Numbers*, Clarendon Press, Oxford, 1968.

[5] E. E. Kummer, *Über Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen*, J. Reine Angew. Math. 44 (1852), 93–146.

[6] H.-O. Peitgen, H. Jürgens, D. Saupe, *Fractals for the Classroom, Part II*, Springer, New York, NY, 1992.

[7] A. B. Romanowska, J. D. H. Smith, *Modes*, World Scientific, River Edge, NJ, 2002.

[8] M. Sved, *The geometry of the binomial array modulo p^2 and p^3*, Discrete Math. 92 (1991), 395–416.

[9] M. Sved, J. Pitman, *Divisibility of binomials by prime powers*, Ars Combinatoria 26 (1988), 197–222.

D. Doan, J. J. Poole, J. D. H Smith, T. Sykes, M. Teplitskiy
DEPARTMENT OF MATHEMATICS
IOWA STATE UNIVERSITY
AMES, IOWA 50011-2064, USA
B. Kivunge
DEPARTMENT OF MATHEMATICS
KENYATTA UNIVERSITY
PO BOX 43844-00100
NAIROBI, KENYA
E-mail: dddoan@iastate.edu
bkivunge2004@yahoo.com
jespoo@sbcglobal.net
jdhsmith@math.iastate.educ
mishat@rice.edu
http://orion.math.iastate.edu/jdhsmith/

Received March 15, 2008; revised version May 12, 2008.