DECOMPOSITION OF PASCAL'S KERNELS MOD p^s

Richard P. Kubelka
Department of Mathematics, San Jose State University, San Jose, CA 95192-0103, USA
kubelka@math.sjsu.edu

Received: 12/11/01, Revised: 11/18/02, Accepted: 12/18/02, Published: 12/18/02

Abstract

For a prime p we define Pascal's Kernel $\mathbf{K}(p,s) = [k(p,s)_{ij}]_{i,j=0}^{\infty}$ as the infinite matrix satisfying $k(p,s)_{ij} = \frac{1}{p^s}\binom{i+j}{j} \mod p$ if $\binom{i+j}{j}$ is divisible by p^s and $k(p,s)_{ij} = 0$ otherwise. While the individual entries of Pascal's Kernel can be computed using a formula of Kazandzidis that has been known for some time, our purpose here will be to use that formula to explain the global geometric patterns that occur in $\mathbf{K}(p,s)$. Indeed, if we consider the finite (truncated) versions of $\mathbf{K}(p,s)$, we find that they can be decomposed into superpositions of tensor products of certain primitive $p \times p$ matrices.

Most of us have seen the beautiful geometric patterns that result when Pascal's Triangle is viewed modulo a prime p. In fact, if we consider *Pascal's Rectangle*, the infinite matrix $\mathbf{R} = [r_{ij}]_{i,j=0}^{\infty}$, where $r_{ij} = \binom{i+j}{j}$, and its truncated (non-infinite) versions $\mathbf{R_n} = [r_{ij}]_{i,j=0}^{p^n-1}$, then we can describe these patterns explicitly in a concise manner by noting that

$$\mathbf{R_n} \equiv \mathbf{R_1} \otimes \cdots \otimes \mathbf{R_1} \mod p, \tag{1}$$

where there are n factors on the right. Here "$\otimes$" signifies the Kronecker tensor product of two matrices [Ser]: if $\mathbf{A}$ is an $m \times n$ matrix and $\mathbf{B}$ is an $r \times s$ matrix, then $\mathbf{A} \otimes \mathbf{B}$ is the $mr \times ns$ matrix whose ijth $r \times s$ block is $a_{ij}\mathbf{B}$. Moreover, if $\mathbf{M}_0, \ldots, \mathbf{M}_n$ are $p \times p$ matrices and $a_0 + a_1p^1 + \cdots + a_np^n$ and $b_0 + b_1p^1 + \cdots + b_np^n$ are the *p-adic expansions* of a and b, then

$$(\mathbf{M}_0 \otimes \cdots \otimes \mathbf{M}_n)_{ab} = (\mathbf{M}_0)_{a_nb_n} \cdot \cdots \cdot (\mathbf{M}_n)_{a_0b_0} \tag{2}$$

The proof of (1) follows readily from (2) and from the result of Lucas [Luc] that

$$\binom{a}{b} \equiv \prod_{i=0}^{n} \binom{a_i}{b_i} \mod p \tag{3}$$

It should be noted that by the multinomial version of Lucas' Theorem [Dick], results similar to (1) hold for *Pascal's Simplices*, higher dimensional arrays of multinomial coefficients.

Modulo powers of a prime p, we still have beautiful geometric patterns, but they are subtler and less easily described. In this paper, as a first step toward describing and explaining these patterns, we will examine *Pascal's Kernels*, rectangular arrays obtained from those binomial coefficients which are divisible by p^s. To be more precise, let us recall the notation employed in [Sing]: if $\binom{a}{b} = d_e p^e + \cdots + d_n p^n$ and $d_e \neq 0$, let $E\binom{a}{b} = e$ and $F\binom{a}{b} = d_e$. Now define the Pascal's Kernel $\mathbf{K}(p,s) = [k(p,s)_{ij}]_{i,j=0}^{\infty}$ as the infinite matrix satisfying $k(p,s)_{ij} = \frac{1}{p^s}\binom{i+j}{j} \mod p$ if $E\binom{i+j}{j} \geq s$, and $k(p,s)_{ij} = 0$ otherwise. (Note: $k(p,s)_{ij} = d_s$ in the p-adic expansion of $\binom{a}{b}$ if $s \leq e$; in particular, if $E\binom{i+j}{j} = s$, then $k(p,s)_{ij} = F\binom{i+j}{j}$.) As above, define truncated matrices $\mathbf{K}(p,s,n)$ by $\mathbf{K}(p,s,n) = [k(p,s)_{ij}]_{i,j=0}^{p^n-1}$.

Remark 1. The name *Pascal's Kernel* is suggested by the fact that the entries of $\mathbf{K}(p,s,n)$ live in $\mathbb{Z}_p$ as it is mapped isomorphically onto the kernel of the mod p^s reduction map in the exact sequence

$$0 \;\rightarrow\; \mathbb{Z}_p \xrightarrow[p^s]{} \mathbb{Z}_{p^{s+1}} \;\rightarrow\; \mathbb{Z}_{p^s} \;\rightarrow\; 0.$$

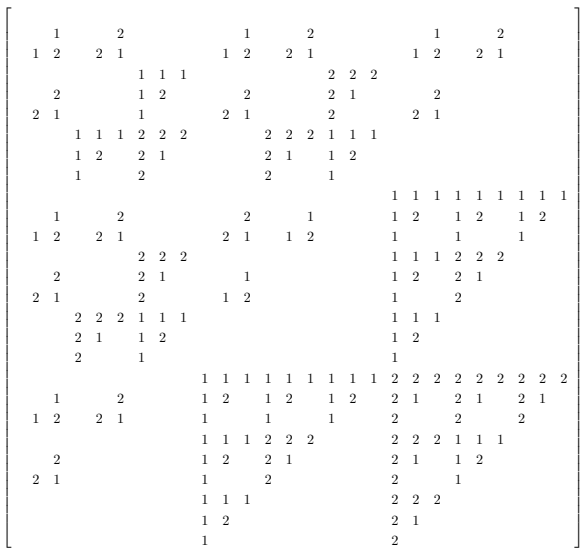

Figure 1: $\mathbf{K}(3,1,3)$

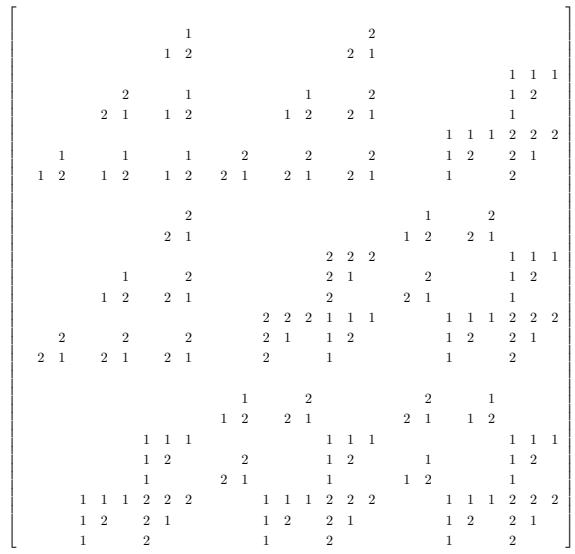

Figure 2: $\mathbf{K}(3,2,3)$

Figures 1 and 2 show $\mathbf{K}(3,1,3)$ and $\mathbf{K}(3,2,3)$, for example, (with zeros suppressed). Note that our definition implies that for $s \neq t$, $\mathbf{K}(p,s,n)$ and $\mathbf{K}(p,t,n)$ have no *overlap*. That is, for all i,j, at most one of $k(p,s,n)_{ij}$ and $k(p,t,n)_{ij}$ is nonzero.

While a formula for $F\binom{a}{b}$ has been known for some time [Kaz], it is the purpose of this paper to interpret that formula in a way that explains the geometric patterns that occur

in Pascal's Kernels in terms of a superposition of tensor products of certain primitive matrices. Specifically, we have the following

Theorem. *Let p be a prime. For $s > n$, $\mathbf{K}(p,s,n) = 0$. For $s \le n$, there exist $p \times p$ matrices $\mathbf{M}_{1,0}$, $\mathbf{M}_{0,1}$, $\mathbf{M}_{0,0}$, and $\mathbf{M}_{1,1}$, which depend only on p, such that $\mathbf{K}(p,s,n)$ is the sum of all tensor products $\mathbf{M}_{t_{n-1},t_{n-2}} \otimes \mathbf{M}_{t_{n-2},t_{n-3}} \otimes \cdots \otimes \mathbf{M}_{t_1,t_0} \otimes \mathbf{M}_{t_0,0}$ with $t_k \in \{0,1\}$ and precisely s of the $t_0, t_1, \ldots t_{n-1}$ equal 1.*

Remark 2. There are evidently $\binom{n}{s}$ summands in $\mathbf{K}(p,s,n)$.

The $p \times p$ matrix $\mathbf{M}_{r,s}$ is defined as having ij-th entry $\Phi_{r,s}(i,j) \mod p$ if $0 \le i+j+s-pr < p$ and 0 otherwise, where

$$\Phi_{r,s}(i,j) = (-1)^r \frac{(i+j+s-pr)!}{i!j!}.$$

Remark 3. (i) $(\mathbf{M}_{1,0})_{ij} \equiv \frac{1}{p}\binom{i+j}{j} \mod p$ if $i+j \ge p$ and $(\mathbf{M}_{1,0})_{ij} = 0$ otherwise. In fact, $\mathbf{M}_{1,0} = \mathbf{K}(p,1,1)$.

(ii) $(\mathbf{M}_{0,1})_{ij} = \frac{(i+j+1)!}{i!j!} = (i+j+1)\binom{i+j}{j} \mod p$.

(iii) $(\mathbf{M}_{0,0})_{ij} = \frac{(i+j)!}{i!j!} = \binom{i+j}{j} \mod p$. In fact, $\mathbf{M}_{0,0} = \mathbf{K}(p,0,1)$.

(iv) $(\mathbf{M}_{1,1})_{ij} \equiv \frac{i+j+1}{p}\binom{i+j}{j} \mod p$ if $i+j \ge p-1$ and $(\mathbf{M}_{1,1})_{ij} = 0$ otherwise.

(v) $(\mathbf{M}_{1,1})_{ij} \equiv (\mathbf{M}_{0,0})^{-1}_{(p-1-j)(p-1-i)} = \binom{2p-2-i-j}{p-1-i}^{-1}$ if $i+j \ge p-1$ and $(\mathbf{M}_{1,1})_{ij} = 0$ otherwise. Therefore $\mathbf{M}_{1,1}$ is just $\mathbf{M}_{0,0}$ reflected across its anti-diagonal with its nonzero entries inverted; here inverses are taken in the field $\mathbf{Z}/p$.

(vi) $(\mathbf{M}_{1,0})_{ij} \equiv -(\mathbf{M}_{0,1})^{-1}_{(p-1-j)(p-1-i)} = -(2p-1-i-j)^{-1}\binom{2p-2-i-j}{p-1-i}^{-1}$ if $i+j \ge p$ and $(\mathbf{M}_{1,0})_{ij} = 0$ otherwise. Therefore $\mathbf{M}_{1,0}$ is just $\mathbf{M}_{0,1}$ reflected across its anti-diagonal with its nonzero entries inverted and negated; inverses and negatives are taken in the field $\mathbf{Z}/p$.

Remark 4. As we will see in the course of the proof below, although $\mathbf{K}(p,s,n)$ is expressed as a sum of matrices, these matrices don't "overlap." That is, for each entry of $\mathbf{K}(p,s,n)$, at most one of the summands is nonzero in that position. In terms of the geometric picture, $\mathbf{K}(p,s,n)$ is a "mosaic," with little pieces set in the holes between the bigger pieces.

Examples.

$$\mathbf{K}(p,0,1) = \mathbf{M}_{0,0} \quad \text{and} \quad \mathbf{K}(p,1,1) = \mathbf{M}_{1,0}, \text{ as noted above.}$$

$$\mathbf{K}(p,1,3) = \mathbf{M}_{1,0} \otimes \mathbf{M}_{0,0} \otimes \mathbf{M}_{0,0} + \mathbf{M}_{0,1} \otimes \mathbf{M}_{1,0} \otimes \mathbf{M}_{0,0} + \mathbf{M}_{0,0} \otimes \mathbf{M}_{0,1} \otimes \mathbf{M}_{1,0} \qquad (4)$$

$$\mathbf{K}(p,2,3) = \mathbf{M}_{1,0} \otimes \mathbf{M}_{0,1} \otimes \mathbf{M}_{1,0} + \mathbf{M}_{0,1} \otimes \mathbf{M}_{1,1} \otimes \mathbf{M}_{1,0} + \mathbf{M}_{1,1} \otimes \mathbf{M}_{1,0} \otimes \mathbf{M}_{0,0} \qquad (5)$$

In the case $p = 3$, we have:

$$\mathbf{M}_{1,0} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 2 \end{bmatrix},\ \mathbf{M}_{0,1} = \begin{bmatrix} 1 & 2 & 0 \\ 2 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix},\ \mathbf{M}_{0,0} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 0 \\ 1 & 0 & 0 \end{bmatrix},\ \mathbf{M}_{1,1} = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 2 & 1 \\ 1 & 1 & 1 \end{bmatrix},$$

and the reader may verify (4) and (5) by examining Figures 1 and 2.

Proof of the Theorem. Consider $k(p,s,n)_{ij}$. Our definition implies that this equals $F\binom{i+j}{j}$ if $E\binom{i+j}{j} = s$ and zero otherwise. We will show that if $E\binom{i+j}{j} \neq s$, then the ij-th entry of every one of the tensor product summands called for in the Theorem must be 0. On the other hand, we will show that if $E\binom{i+j}{j} = s$, the ij-th entries of all such summands will be 0 except for precisely one, which will equal $F\binom{i+j}{j}$.

First express i, j, and $i+j$ p-adically: $i = b_0 + b_1p^1 + \cdots + b_{n-1}p^{n-1}$, $j = c_0 + c_1p^1 + \cdots + c_{n-1}p^{n-1}$, and $i+j = a_0 + a_1p^1 + \cdots + a_np^n$, where $0 \leq a_k, b_k, c_k < p$ as usual and b_n and c_n are both 0.

We take our main tools from [Sing]:

$$e = E\binom{i+j}{j} = \sum_{k=0}^{n} (b_k + c_k - a_k)/(p-1) \qquad (6)$$

$$F\binom{i+j}{j} \equiv (-1)^e \prod_{k=0}^{n} \frac{a_k!}{b_k!c_k!} \mod p \qquad (7)$$

Remark 5. It is crucial to note (as was pointed out in [Sing]) that the number e obtained in (6) is exactly the number of carries that we get when we add i and j p-adically. For example, if there are no carries, then $e = 0$, $a_k = b_k + c_k$ for all k, and (7) reduces to (3).

Considering the p-adic addition of i and j more closely, let r_k denote the carry digit from the k-th place to the $(k+1)$-st place. So $a_k = b_k + c_k + r_{k-1} - pr_k$, with $r_k, r_{k-1} \in \{0,1\}$ and r_{-1} and r_n both 0. By Remark 5, $\sum_{k=0}^{n} r_k = e$, and so (7) becomes

$$\begin{aligned} F\binom{i+j}{j} &\equiv (-1)^e \prod_{k=0}^{n} \frac{(b_k + c_k + r_{k-1} - pr_k)!}{b_k!c_k!} \\ &\equiv \prod_{k=0}^{n} (-1)^{r_k} \frac{(b_k + c_k + r_{k-1} - pr_k)!}{b_k!c_k!} = \prod_{k=0}^{n} \Phi_{r_k, r_{k-1}(b_k, c_k)} \mod p. \end{aligned} \qquad (8)$$

That (6) gives the number of carries implies immediately that $E\binom{i+j}{j} \leq n$. So if $s > n$, we must have $k(p,s,n)_{ij} = 0$.

Now suppose $s \leq n$ and consider a typical $\mathbf{M}_{t_{n-1},t_{n-2}} \otimes \mathbf{M}_{t_{n-2},t_{n-3}} \otimes \cdots \otimes \mathbf{M}_{t_1,t_0} \otimes \mathbf{M}_{t_0,0}$ summand of $\mathbf{K}(p,s,n)$ as called for by the Theorem. By (2) its contribution to $k(p,s,n)_{ij}$ should be

$$(\mathbf{M}_{t_{n-1},t_{n-2}})_{b_{n-1}c_{n-1}} \cdot \cdots \cdot (\mathbf{M}_{t_0,0})_{b_0c_0} \tag{9}$$

with $\sum_{k=0}^{n} t_k = s$. If $E\binom{i+j}{j} = \sum_{k=0}^{n} r_k > s$, then for some smallest k, $r_k = 1$ and $t_k = 0$. But $r_k = 1$ implies that $b_k + c_k \geq p-1$ (if $k > 0$ and $r_{k-1} = 1$ also), or $b_k + c_k \geq p$ (if $r_{k-1} = 0$). In the former case our assumption that k is minimal implies that $\mathbf{M}_{t_k,t_{k-1}} = \mathbf{M}_{0,1}$. Hence $b_k + c_k \geq p-1$ here implies that $(\mathbf{M}_{t_k,t_{k-1}})_{b_kc_k} = 0$. In the latter case, $b_k + c_k \geq p$ implies that $(\mathbf{M}_{t_k,t_{k-1}})_{b_kc_k} = 0$ regardless of whether t_{k-1} equals 0 or 1. Both cases therefore yield zero summands, which is exactly what we need. The case where $E\binom{i+j}{j} < s$ is dispatched by the same argument, with the roles of 0 and 1 for the r_k's and t_k's reversed.

If $E\binom{i+j}{j} = s$, we noted earlier that $k(p,s,n)_{ij} = F\binom{i+j}{j}$. We will show that a typical summand of $k(p,s,n)_{ij}$ as called for by the Theorem and as given by (9) will be nonzero precisely when $t_k = r_k$ for $k = 0, \ldots n-1$ and that in that case the value of the summand will be given by the last expression in (8). We start our inductive proof of this by considering the case where $b_0 + c_0 \leq p-1$, and thus $r_0 = 0$. If $t_0 = 1$ in our summand, then $(\mathbf{M}_{t_0,0})_{b_0c_0} = (\mathbf{M}_{1,0})_{b_0c_0} = 0$, by the definition of $\mathbf{M}_{1,0}$. On the other hand, if $t_0 = 0$, then

$$(\mathbf{M}_{t_0,0})_{b_0c_0} = (\mathbf{M}_{0,0})_{b_0c_0} = \Phi_{0,0}(b_0,c_0) = \Phi_{r_0,r_{-1}}(b_0,c_0).$$

Thus, working from right to left, the first factor in (9) will match the $k=0$ factor in (8). Moreover, in the case where $b_0 + c_0 \geq p$, a similar argument will also give us the match of those factors.

Now proceeding inductively, we assume that $t_k = r_k$ for all $k < m$ and so

$$(\mathbf{M}_{t_k,t_{k-1}})_{b_kc_k} = (\mathbf{M}_{r_k,r_{k-1}})_{b_kc_k} = \Phi_{r_k,r_{k-1}}(b_k,c_k) \tag{10}$$

for all $k < m$. Thus the first m factors in (8) match the first m factors in (9) (read right-to-left). To advance the induction, we need to show that $t_m = r_m$. This and the inductive hypothesis will then guarantee that $(\mathbf{M}_{t_m,t_{m-1}})_{b_mc_m} = \Phi_{r_m,r_{m-1}}(b_m,c_m)$, and then the first $m+1$ factors will match à la (10), and our induction will be complete. The proof that $t_m = r_m$ proceeds by contradiction, using the same argument—with the "minimal k" replaced by m—that we employed above in considering the cases where $E\binom{i+j}{j} > s$ and $E\binom{i+j}{j} < s$. □

Proof of Remaining Items from Remark 3. For item (i), we must show $\frac{1}{p}\binom{i+j}{j} \equiv -\frac{(i+j-p)!}{i!\,j!} \mod p$ when $i + j \geq p$. This amounts to showing that

$$(i+j)!/p \equiv -(i+j-p)! \mod p. \tag{11}$$

But $(i+j)!/(i+j-p)!$ is a product of p consecutive integers, one from each residue class mod p. Since $0 \le i, j < p$, one of those factors will be exactly p and no other will be divisible by p. Therefore

$$\frac{(i+j)!}{p\,(i+j-p)!} \equiv (p-1)! \equiv -1 \mod p,$$

this last congruence being Wilson's Theorem [Edg]. This completes the proof of (11), and hence of item (i).

A nearly identical argument gives us item (iv), that $\frac{i+j+1}{p}\binom{i+j}{j} \equiv -\frac{(i+j+1-p)!}{i!\,j!} \mod p$ when $i+j \ge p-1$.

For items (v) and (vi), note that if $\mathbf{H}$ is a $p\times p$ matrix with rows and columns numbered from 0 to $p-1$, the matrix $\tilde{\mathbf{H}}$ with entries $\tilde{h}_{ij} = h_{(p-1-j)(p-1-i)}$ is $\mathbf{H}$ reflected across its anti-diagonal. The proofs of items (v) and (vi) combine this fact with straightforward applications of the following

Lemma. *For* $0 \le m \le p-1$, $[(p-1-m)!]^{-1} \equiv (-1)^{p-m} m! \mod p$.

The proof of the Lemma once again follows directly from Wilson's Theorem. □

Remark 6. As a final aside, let us note that the matrix $\mathbf{M}_{0,0}$ has the further property that $\mathbf{M}_{0,0}^2$ is just $\mathbf{M}_{0,0}$ reflected across its anti-diagonal. Furthermore, $\mathbf{M}_{0,0}^4 = \mathbf{M}_{0,0}$ and, since $\mathbf{M}_{0,0}$ is invertible, $\mathbf{M}_{0,0}^3 = \mathbf{I}$. (See [Stra] for details.)

Acknowledgement. I would like to thank the referee for suggestions that markedly simplified the statement and proof of the results in this paper.

References

[Dick] L. E. Dickson, "Theorems on the residues of multinomial coefficients with respect to a prime modulus," Quart. J. Pure Appl. Math., 33 (1901-2), 378-384.

[Edg] H. M. Edgar, *A First Course in Number Theory*, Wadsworth, Belmont, (1988), 41.

[Kaz] G. S. Kazandzidis, "Congruences on the binomial coefficients," Bull. Soc. Math. Grèce (NS), 9 (1968), 1-12.

[Luc] E. Lucas, *Théorie des Nombres*, Gauthier-Villars, Paris (1891), 417-420.

[Ser] J.-P. Serre, *Linear Representations of Finite Groups*, Springer, New York (1977), 8.

[Sing] D. Singmaster, "Notes on binomial coefficients I–a generalization of Lucas' congruence," J. London Math. Soc. (2), 8 (1974), 545-548.

[Stra] N. Strauss and I. Gessel, Solution to Advanced Problem #6527, Amer. Math. Monthly, 95 (1988), 564-565.