The Map Behind a Binomial Coefficient Matrix Over $\mathbb{Z}/p\mathbb{Z}$

William C. Waterhouse*
Department of Mathematics
The Pennsylvania State University
University Park, Pennsylvania 16802

Submitted by Richard A. Brualdi

ABSTRACT

The $p^n \times p^n$ matrix over $\mathbb{Z}/p\mathbb{Z}$ whose entries are $\binom{i+j}{j}$ for $0 \leqslant i, j < p^n$ expresses the operation $f \mapsto f(1/(1-x))$ on functions $\mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$. This interpretation makes the behavior of the matrix transparent.

Let $q = p^n$ be a power of a prime, let $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ be the field with p elements, and let J be the $q \times q$ matrix over $\mathbb{F}_p$ whose (i, j) entry is the binomial coefficient $\binom{i+j}{j}$, $0 \leqslant i, j \leqslant q-1$. In a recent paper [1], N. Strauss demonstrated the surprising fact that $J^3 = I$, and he went on to find the multiplicities of the eigenvalues. His results were proved by the method of generating functions. In this note I shall exhibit a natural linear transformation that is represented by the matrix J in a suitable basis. Strauss's results will then follow easily.

THEOREM 1. *Let $\mathbb{F}_q$ be the field with q elements. Let V be the vector space of all functions from $\mathbb{F}_q$ to itself. Let $f_j(x) = x^j$ for $0 \leqslant j \leqslant q-1$, a basis of V. Let $T: V \to V$ be the linear mapping given by $(Tf)(x) = f(1/(1-x))$. Then the matrix of T in the basis f_j is precisely $\binom{i+j}{j}$.*

*This work was supported in part by grants from the National Science Foundation.

52 Vanderbilt Ave., New York, NY 10017 0024-3795/88/$3.50

Proof. We must of course clarify what $(Tf)(1)$ is supposed to be. The point is that the operation $x \mapsto 1/(1-x)$ is a bijection on the "projective line" $\mathbb{F}_q \cup \{\infty\}$. We can extend elements $f \in V$ to functions on this larger set by prescribing $f(\infty) = -\sum_{x \in \mathbb{F}_q} f(x)$, thus embedding V as those functions on $\mathbb{F}_q \cup \{\infty\}$ whose values sum to zero. Composition with the bijection $x \mapsto 1/(1-x)$ obviously is a linear isomorphism for the functions on the projective line, and it clearly preserves V. In this way we do have a well-defined operation on V that we can reasonably write as $(Tf)(x) = f(1/(1-x))$.

Now we observe that for every i and j we have

$$\begin{aligned}(-1)^i(q-1-j)(q-1-j-1)\cdots(q-j-i)\\ = (j+1)(j+2)\cdots(j+i) \qquad \text{in } \mathbb{F}_p,\end{aligned}$$

and hence

$$(-1)^i\binom{q-1-j}{i} = \binom{i+j}{i} = \binom{i+j}{j} \qquad \text{in } \mathbb{F}_p.$$

This implies that the entries in J below the secondary diagonal—those with $i+j \geqslant q$—are zero. (This can also be seen directly.) More important is the fact that for $1 \neq x \in \mathbb{F}_q$ we now have

$$(1-x)^{-j} = (1-x)^{q-1-j} = \sum_i (-1)^i \binom{q-1-j}{i} x^i = \sum_i \binom{i+j}{j} x^i.$$

Thus the theorem is very nearly proved; it remains only to check it at $x = 1$. Using our extension of the functions, we can equally well check it at $x = \infty$, which we now do. We have $(Tf_j)(\infty) = f_j(0)$, which is 1 when $j = 0$ and zero otherwise. On the other hand, the function

$$\sum_i \binom{i+j}{j} x^i \qquad \text{at } \infty$$

is

$$-\sum_{y \in \mathbb{F}_q} \sum_i \binom{i+j}{j} y^i.$$

The sum $\Sigma_{y \in \mathbb{F}_q} y^i$ is equal to 0 except for $i = q-1$, where it is -1; as $\binom{q-1+j}{j}$ is 0 in $\mathbb{F}_q$ unless $j = 0$, the theorem is proved. ■

COROLLARY 1. $J^3 = I$.

Proof. This is an immediate consequence of Theorem 1 and the simple fact that the operation $x \mapsto 1/(1-x)$ has order 3 as a function on the projective line. ■

THEOREM 2. *Let*

$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & \cdots & 0 \\ 1 & 1 & 1 & 1 & \cdots & 1 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 1 & y & y^2 & y^3 & \cdots & y^{q-1} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \end{pmatrix}$$

be the Vandermonde matrix formed from the elements $0, 1, \ldots, y, \ldots$ *of* $\mathbb{F}_q$. *Then* MJM^{-1} *has the form*

$$\left(\begin{array}{cc|cccc} 0 & 1 & 0 & 0 & \cdots & 0 \\ -1 & -1 & -1 & -1 & \cdots & -1 \\ \hline \multicolumn{2}{c|}{0} & \multicolumn{4}{c}{P} \end{array}\right),$$

where P is a permutation matrix. The structure of the permutation is:

(i) *two elements fixed, all others permuted in 3-cycles, if* $q \equiv 1 \pmod 3$;
(ii) *all elements permuted in 3-cycles, if* $q \equiv 2 \pmod 3$; *and*
(iii) *one element fixed, all others permuted in 3-cycles, if q is a power of* 3.

Proof. We now look at the other natural basis of V, the functions g_y where $g_y(y) = 1$ and $g_y(z) = 0$ for all other $z \in \mathbb{F}_q$. [Note then $g_y(\infty) = -1$.] Clearly $f_k = \Sigma_y y^k g_y$. Thus the Vandermonde matrix M gives the base change, and MJM^{-1} is the matrix of the operation T in the basis g_y. It is trivial to see that $Tg_y = g_{1-1/y} - g_1$ except for $y = 0$, where we get $Tg_0 = -g_1$. This gives us all the structure of the matrix except the analysis of the permutation, which is simply the permutation induced by $y \mapsto 1 - 1/y$ on $\mathbb{F}_q \setminus \{0,1\}$. As the map has order 3, each element is either fixed or sent in a 3-cycle. Clearly an element y is fixed iff $y^2 - y + 1 = 0$. When $p = 3$, this equation has the unique root $y = 2$. Otherwise, its roots are $-\zeta$, $-\zeta^2$, where ζ is a nontrivial cube root of 1. Such roots exist in $\mathbb{F}_q$ iff $q \equiv 1 \pmod 3$. ■

COROLLARY 2. *If $q \equiv 2 \pmod 3$, then J is similar to a block matrix containing 1×1 blocks with eigenvalue 1 and 2×2 blocks of the form*

$$\begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}.$$

There are $(q-2)/3$ blocks of the first type and $(q+1)/3$ of the second type. If $q \equiv 1 \pmod 3$, the same type of structure occurs, but there are $(q+2)/3$ blocks of the first type and $(q-1)/3$ of the second type.

Proof. As $p \neq 3$ and $T^3 = I$, the matrix MJM^{-1} is separable, and hence it is similar to the direct sum of P and the upper corner $\begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$. Clearly P is similar to the direct sum of the permutation matrices for the cycles in it. Each cyclic permutation of three basis vectors e_1, e_2, e_3 splits its space into two subspaces, the spans of $e_1 + e_2 + e_3$ and of $e_1 - e_3$, $e_1 - e_2$, and a trivial computation shows that it thus yields one block of each type. ■

Over $\mathbb{F}_{p^2}$, of course, each of our 2×2 blocks splits to give two 1×1 blocks with eigenvalues ζ and ζ^2 (the cube roots of unity). This happens over $\mathbb{F}_p$ iff $p \equiv 1 \pmod 3$.

Finally, a different splitting works well when $p = 3$. If we split V then as the direct sum of 3-dimensional invariant subspaces where the functions have zero values except on $y = 2$ and on the elements of one 3-cycle in $\mathbb{F}_q \cup \{\infty\}$, it is trivial to see that each such subspace yields a single 3×3 Jordan block with eigenvalue 1.

REFERENCE

1 N. Strauss, Jordan form of a binomial coefficient matrix over $\mathbb{Z}_p$, *Linear Algebra Appl.* 90:65–72 (1987).

Received 8 September 1987; final manuscript accepted 10 September 1987