MASSACHUSETTS INSTITUTE
OF TECHNOLOGY

ARTIFICIAL INTELLIGENCE LABORATORY

Working Paper 275 **July 1985**

Jordan Form of $\binom{i+j}{j}$ over Z_p

Nicholas Strauss Department of Mathematics, Boston University Boston, MA. 02215 Artificial Intelligence Laboratory M.I.T.,Cambridge, MA. 02139

The Jordan Form over field Z_p of $J^p_{p^n}$ is diagonal for $p > 3$ with characteristic polynomial, $\Phi(x) = x^3 - 1$, for p prime, n natural number. These matrices have dimension p^n x p^n, with entries $\binom{i+j}{j}$. I prove these results with the method of generating functions.

In this paper, I will prove the theorems necessary to construct a Binomial Coefficient superidentity. By the term, superidentity, I wish to indicate the set of four identities which taken together, prove the existence of an entity which is most properly expressible in matrix language. This entity is the Jordan form of the class of matrices $J^p_{p^n}$, over the finite field Zp. All operations are taken modulo p.

Let J_n be a n x n matrix such that

$$J_n(i,j) = \binom{i+j}{j}$$

for $0 \leq i, j < n$. Let J^p_n be the same matrix with entries taken modulo p. This paper considers the class of matrices $J^p_{p^n}$ for p prime, and n positive integer.

In summary, I introduce four theorems to prove the existence of the Jordan Form which is stated in Theorems 4 and 5.

Theorem 0 states that each matrix in this class is expressible in terms of an iterated tensor product of more elementary matrices.

Theorem 1 states that the characteristic polynomial for any matrix in this class is:

$$\Phi(x) = x^3 - 1$$

Thus there are only three eigenvalues, the cube roots of unity. The method of proof involves well-known generating function techniques, though there are major simplifications due to the finite field. For example: $(x-1)^{p-1} = \sum_{i=0}^{p-1} x^i$.

Theorems 2 and 3 completely specify the multiplicity of the eigenvalues. By a second application of Theorem 1, it follows immediately that the matrices are all diagonal for $p > 3$.

To reduce terminology, I refer to the formula, $\binom{p}{k} = \binom{p-1}{k} + \binom{p-1}{k-1}$ as the recurrence relation for Binomial Coefficients. This is the well-known formula used in constructing Pascal's Triangle.

Theorem 0

$$J^p_{p^n} = \otimes_{i=1}^n J^p_p$$

where p is prime, and $\otimes$ is the Kronecker product. The Kronecker product is also sometimes referred to as a Tensor product.

Proof Consider J^p_p. The left to right diagonal, consists of terms $\binom{p-1}{k}$ for $k = 0, \ldots, p-1$ But $\binom{p-1}{k} = (-1)^k$ by the recurrence relation for Binomial Coefficients and $\binom{p}{k} = 0$. Thus the lower right half of the square is all zero, the left to right diagonal is $(-1)^k$. The recurrence relation for Binomial Coefficients then induces a recurrence relation for these matrices. The 1 in the lower left corner and the 1 in the upper right corner grow a copy of J^p_p to

either side. These in turn, add to form $2J_p^p$. The process continues until the prime modulus is reached and then a giant $J_{p^2}^p$ matrix has been constructed. The proof then follows by induction. Wolfram termed the prime case "strongly regular".

Theorem 1

$$\left(J_{p^n}^p\right)^3 = I$$

for any p prime, for any n positive integer.

Proof All equalities are mod p. The statement above is equivalent to showing,

$$\sum_{j,k=0}^{p-1} \binom{r+j}{j}\binom{j+k}{k}\binom{k+s}{s} = \delta_r^s$$

since $J_{p^n}^p = J_p^p \otimes \ldots \otimes J_p^p$ by Theorem 0. δ_r^s is the Kronecker delta. Let

$$f_{rs} = \sum_{j,k=0}^{p-1} \binom{r+j}{j}\binom{j+k}{k}\binom{k+s}{s}$$

Introduce generating function, $F(x,y) = \sum_{r,s\geq 0} f_{rs}x^r y^s$.

$$F(x,y) = \sum_{r,s\geq 0}^{\infty}\sum_{j,k=0}^{p-1} \binom{r+j}{j}\binom{j+k}{k}\binom{k+s}{s}x^r y^s$$

$$= \sum_{j,k=0}^{p-1} \binom{j+k}{k}\frac{1}{(1-x)^{j+1}(1-y)^{k+1}}$$

$$= \frac{1}{(1-x)(1-y)}\sum_{j,k=0}^{p-1} \binom{j+k}{k}\frac{1}{(1-x)^j(1-y)^k}$$

The theorem is true if,

$$\frac{(1-xy)^{p-1}}{(1-x)^{p-1}(1-y)^{p-1}} = \sum_{j,k=0}^{p-1} \binom{j+k}{k}\frac{1}{(1-x)^j(1-y)^k}$$

since

$$\sum_{r,s\geq 0} f_{rs}x^r y^s = \frac{(1-xy)^{p-1}}{(1-x)^p(1-y)^p}$$

Let $\alpha = 1/(1-x), \beta = 1/(1-y)$. The above formula is equivalent to,

$$(\alpha+\beta-1)^{p-1} = \sum_{j,k=0}^{p-1} \binom{j+k}{k}\alpha^j\beta^k$$

Let right hand side be denoted $G(\alpha, \beta)$.

$$G(\alpha,\beta) = \sum_{r=0}^{p-1}\sum_{s=0}^{r}\binom{r}{s}\alpha^r\beta^{r-s}$$
$$= \sum_{r=0}^{p-1}(\alpha+\beta)^r$$

But left hand side is

$$(\alpha+\beta-1)^{p-1} = \sum_{r=0}^{p-1}\binom{p-1}{r}(\alpha+\beta)^r(-1)^{p-1-r}$$

But

$$\binom{p-1}{r} = (-1)^{p-1-r}$$

This proves Theorem 1.

Theorem 2

$$(R_{p^n}J_{p^n}^p)^2 = I_{p^n}$$

where I_{p^n} is the p^n x p^n identity matrix, and R_{p^n} is the p^n x p^n matrix of ones on the lower left to upper right diagonal such that $(R_{p^n})^2 = I_{p^n}$. The equality is mod p, p as always is prime.

Proof By theorem 0, the above statement is equivalent to proving that

$$F(i,k) = \sum_{j=0}^{p-1}\binom{p-1-i+j}{j}\binom{p-1-j+k}{k} = \delta_i^k$$

Introduce the generating function,

$$G(x,y) = \sum_{i=0}^{p-1}\sum_{k=0}^{\infty}F(i,k)x^iy^k$$
$$= \sum_{i=0}^{p-1}\sum_{j=0}^{p-1}\binom{p-1-i+j}{j}x^i/(1-y)^{p-j}$$
$$= \sum_{i=0}^{p-1}\sum_{j=0}^{p-1}\binom{i+j}{j}x^{p-1-i}/(1-y)^{p-j}$$
$$= \frac{x^{p-1}}{(1-y)^p}\sum_{i=0}^{p-1}\sum_{j=0}^{p-1}\binom{i+j}{j}(1/x)^i(1-y)^j$$
$$= \frac{x^{p-1}}{(1-y)^p}(1-1/x-1+y)^{p-1}$$
$$= \frac{(yx-1)^{p-1}}{(1-y)^p}$$

This is the desired conclusion, hence Theorem 2 is proven.

Theorem 3

$$trace(J_p^p) = \begin{cases} -1, & \text{if (p-1)/3 integer;} \\ 1, & \text{otherwise.} \end{cases}$$

Proof The above statement is equivalent to showing that,

$$\sum_{k=0}^{p-1} \binom{2k}{k} = \begin{cases} -1, & \text{if (p-1)/3 integer;} \\ 1, & \text{otherwise.} \end{cases}$$

But, $\binom{2k}{k} = (-4)^k \binom{-1/2}{k} = (-4)^k \binom{(p-1)/2}{k}$. And the entries in the sum from $(p-1)/2$ to $p-1$ are zero. So,

$$\sum_{k=0}^{(p-1)/2} \binom{2k}{k} = \sum_{k=0}^{(p-1)/2} (-4)^k \binom{(p-1)/2}{k}$$

which is, $(-4+1)^{(p-1)/2}$ or $(-3)^{(p-1)/2}$. This proves Theorem 3.*

All four theorems have been proven and construction of the superidentity is a straightforward task. There are two cases, when $(p-1)/3$ is integer, and when it is not.

Theorem 4 The Jordan form of J_p^p is diagonal for $p > 3$, and has three eigenvalues. In the real case, when $(p-1)/3$ is an integer, then the eigenvalues are $1, f, f^2$ where f is a cube root of unity in Z_p. These have multiplicities $(p+2)/3, (p-1)/3$, and $(p-1)/3$. In the complex case, when $(p-1)/3$ is not an integer, then the eigenvalues are $1, \varsigma, \varsigma^*$ where ς is an extension element to the field Z_p and ς^* is its conjugate. These eigenvalues have multiplicities $(p-2)/3, (p+1)/3$, and $(p+1)/3$.

Proof For $p > 3$, off-diagonal terms remain after cubing, since the cube of the Jordan block of any such matrix has off-diagonal terms. Only 2 x 2 or 3 x 3 Jordan blocks could have diagonal cubes. This contradicts the cube of the matrix being the identity. Hence the Jordan form must be diagonal. In the case $p = 3$, there is one eigenvalue 1, and one 3x3 Jordan block for this eigenvalue. Cubing this matrix, modulo 3, results in the identity.

In the complex case, when $(p-1)/3$ is not integer, the characteristic polynomial $\Phi(t)$ can be factored.

$$\Phi(t) = (t^2 + t + 1)^a (t-1)^b$$

where $t^2 + t + 1$ is irreducible. In the real case, when $(p-1)/3$ is an integer, the characteristic polynomial factors.

$$\Phi(t) = (t-1)^c (t-f)^b (t-f^2)^a$$

*The proof given here is due to Professor I. Gessel. There is a slightly longer proof of the same result by Professor R. Stanley. Both were proven in response to my conjecture.

a, b, c are the multiplicities which we seek.

In the real case, the following three equations hold.

$$a + b + c = p$$
$$af^2 + bf + c = 1 \pmod{p}$$
$$b = a$$

The first expresses the dimensional constraint, the second from Theorem 3, the trace being equal to the second coefficient of the characteristic polynomial, and the third from Theorem 2.

In the complex case, the following two equations hold.

$$2a + c = p$$
$$c - a = -1 \pmod{p}$$

The first equation is the dimensional constraint and the second again from Theorem 3.

Solving these linear equations, in the first case gives, $a = 1/(f^2 + f - 2) \pmod{p}$ or employing $f^2 + f + 1 = 0 \pmod{p}$ we get $a = -1/3 \pmod{p}$. Thus $a = (p-1)/3$.

In the complex case, $a = 1/3 \pmod{p}$. Hence $a = (p+1)/3$. Thus Theorem 4 is proven.

Theorem 5 The Jordan form of $J_{p^n}^p$ is the Kronecker product of the Jordan form found in Theorem 4.

Proof This follows immediately from Theorem 0.

I term Theorem 5, a superidentity because it ties together several identities into one result clearly expressible in matrix form. The result is quite suprising, and I ask the reader to find me another matrix whose cube gives the identity.

This matrix superidentity results in a whole class of combinatorial identities which are new. They are all modular and concern finite sums. There is also some identities that can be seen by considering Stirling numbers of the first and second kinds as matrices. This work has not yet been completed.

Binomial Coefficients and Stirling numbers, modulo an integer, when exhibited in tabular form exhibit fractal structure termed, "self-similar". However, "self-similar" does not imply Tensor product. Stirling numbers do not form Tensor products, and neither do Binomial Coefficients to a composite modulus. That such pleasing patterns have such important algebraic consequence is suprising. In the case of a prime modulus, the binomial coefficients form a tensor product. At the present time, there is no explanation for this.

I acknowledge my use of MACSYMA ** for its flawless modular arithmetic. I wish to thank Professor G.J.Sussman, Professor R.P.Stanley, and David Meyer.

References

1. Algebra:An Elementary Text-Book,
G.Chrystal, Adam and Charles Black, Edinburgh, 1889.
2. An Introduction to the Theory of Numbers,
fifth edition, G.H.Hardy and E.M.Wright,
Oxford University Press, Oxford, 1983.
3. Combinatorial Identities,
John Riordan, John Wiley, New York,1968.
4. Geometry of Binomial Coefficients,
Stephen Wolfram, American Mathematical Monthly,
November, 1984.
5. Linear Algebra,
second edition, Kenneth Hoffman and Ray Kunze,
Prentice Hall, Englewood Cliffs, New Jersey, 1971.
6. MACSYMA Reference Manual,
version ten, Laboratory of Computer Science, M.I.T.,
Cambridge,MA.,January, 1983.
7. Mathematical Carnival,
Martin Gardner, Vintage, New York, 1975.
8. Matrix Theory and its Applications,
N.J.Pullman, Marcel Dekker, New York, 1976.

**MACSYMA was created in part by support from the National Aeronautics and Space Administration (NASA), the Office of Naval Research (ONR), and the U.S. Department of Energy (DOE).