Protected: POW 2012-6 Matrix modulo p

Let p be a prime number and let n be a positive integer. Let $A = \left(\binom{i+j-2}{i-1}\right)_{1\le i\le p^n, 1\le j\le p^n}$ be a $p^n \times p^n$ matrix. Prove that $A^3 \equiv I \pmod p$, where I is the $p^n \times p^n$ identity matrix.

Solution. Let a 2×2 matrix $M \in GL_2(\mathbf{Z}/p\mathbf{Z})$ be given. For $k>1$, define $M_k \in GL_k(\mathbf{Z}/p\mathbf{Z})$ to be the $k\times k$ matrix such that

$$\begin{pmatrix} x_M^{k-1} \\ x_M^{k-2}y_M \\ x_M^{k-3}y_M^2 \\ \vdots \\ x_M y_M^{k-2} \\ y_M^{k-1} \end{pmatrix} = M_k \begin{pmatrix} x^{k-1} \\ x^{k-2}y \\ x^{k-3}y^2 \\ \vdots \\ xy^{k-2} \\ y^{k-1} \end{pmatrix}$$

where $\begin{pmatrix} x_M \\ y_M \end{pmatrix} = M \begin{pmatrix} x \\ y \end{pmatrix}$. Then, it is trivial that $(MN)_k = M_k N_k$ for any $M, N \in GL_2(\mathbf{Z}/p\mathbf{Z})$.

Let $J = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$ which plays the critical role in this solution. The fact that $J^3 = -I$ will be used in the end.

–

Claim. If $K = p^n$, then $J_K = A$ over $\mathbf{Z}/p\mathbf{Z}$.

It is easy to see that $[J_K]_{ij} = [x^{K-j}y^{j-1}](x-y)^{K-i}x^{i-1} = (-1)^{j-1}\binom{K-i}{j-1}$. Hence, $[J_K]_{i1} = 1$ for $1 \le i \le K$ and

$$[J_K]_{1j} = (-1)^{j-1}\binom{K-1}{j-1} \equiv 1 \pmod p$$ for $1 \le j \le K$.

This can be verified using $(1-x)^K \equiv 1 - x^K \pmod p$, so $(1-x)^{K-1} \equiv \sum_{j=1}^K x^{j-1} \pmod p$. Also,

$$[J_K]_{ij} = [J_K]_{i(j-1)} + [J_K]_{(i-1)j}$$

for $1 < i, j \le K$ from the formula $\binom{K-i+1}{j-1} = \binom{K-i}{j-2} + \binom{K-i}{j-1}$. On the other hand, the given matrix A also has the exactly same structure, i.e. $[A]_{i1} = [A]_{1j} = 1$ and $[A]_{ij} = [A]_{i(j-1)} + [A]_{(i-1)j}$. This proves that $J_K = A$.

–

By the claim, $A^3 = (J_K)^3 = (J^3)_K = (-I)_K = I$ over $\mathbf{Z}/p\mathbf{Z}$. Therefore, $A^3 \equiv I \pmod p$.