Math 1350 Quiz 4 - July 28, 2010

(4 points) Name: Solutions

1. (8 points) Show that

$$\begin{bmatrix} 2 & 5 \\ 1 & 4 \end{bmatrix}^{-1} \equiv \begin{bmatrix} 4 & 1 \\ 5 & 6 \end{bmatrix} \pmod 8$$

Method 1

$$\begin{bmatrix} 2 & 5 \\ 1 & 4 \end{bmatrix}^{-1} \equiv (8-5)^{-1}\begin{bmatrix} 4 & -5 \\ -1 & 2 \end{bmatrix} \pmod 8$$
$$\equiv 3^{-1}\begin{bmatrix} 4 & 3 \\ -1 & 2 \end{bmatrix} \equiv 3\cdot\begin{bmatrix} 4 & 3 \\ -1 & 2 \end{bmatrix} \pmod 8$$
$$\equiv \begin{bmatrix} 12 & 9 \\ -3 & 6 \end{bmatrix} \equiv \begin{bmatrix} 4 & 1 \\ 5 & 6 \end{bmatrix} \pmod 8$$

Method 2

$$\begin{bmatrix} 2 & 5 \\ 1 & 4 \end{bmatrix}\begin{bmatrix} 4 & 1 \\ 5 & 6 \end{bmatrix} \equiv \begin{bmatrix} 8+25 & 2+30 \\ 4+20 & 1+24 \end{bmatrix} \pmod 8$$
$$\equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \pmod 8,$$ and

since their product is the identity matrix, they are in fact inverses of each other.

2. With general matrices, we find the inverse of a matrix $A$ by multiplying a related matrix by $\frac{1}{\det A}$. This means that if $\det(A) = 0$, then we cannot invert $A$.

   (a) (5 points) When working with matrices modulo $m$, what must be true of $\det(A)$ for $A$ to be invertible? (*Hint:* Think about what "division" is in modular arithmetic and what we know must be true of a number to do this "division".)

   det(A) must be relatively prime to the modulus $m$, for it to have a multiplicative inverse and so for the matrix A to have an inverse.

   (b) (4 points) Give an example of a non-zero matrix that <u>CANNOT</u> be a key matrix for the Hill Cipher. Any matrix with even determinant or a multiple of 13 will work, as it needs to not be relatively prime to 26.

   Examples $\begin{bmatrix} 2 & 2 \\ 1 & 2 \end{bmatrix}, \begin{bmatrix} 14 & 1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 10 & 9 \\ 2 & 7 \end{bmatrix}, \begin{bmatrix} 6 & 4 \\ 1 & 5 \end{bmatrix}, \ldots$

3. (4 points) What is something that you learned while preparing and/or giving your presentation, beyond the details of your cipher? (You may use the back of this sheet to answer.)