HW 5
Due: Friday, October 18

§3.13/39, 41; §6.6/2, 5, 6, 8, 9

3.13.39 For the first one, the determinant is $1-6=-5$. The inverse of -5 is 5 (as $-5\cdot 5=-25\equiv 1 \pmod{26}$). Thus the inverse is

$$5\begin{bmatrix}1 & -1\\ -6 & 1\end{bmatrix}=\begin{bmatrix}5 & -5\\ -30 & 5\end{bmatrix}\equiv\begin{bmatrix}5 & 21\\ 22 & 5\end{bmatrix} \pmod{26}.$$

For the second one, we need the determinant $1-b$ to be invertible. In other words, we need $2\nmid(1-b)$ and $13\nmid(1-b)$. The first condition is equivalent to b being even, and the second means $b\neq 14$. Thus b can be any even number with $b\not\equiv 14 \pmod{16}$.

6.6.5 We have $b=1$, $a=0$, $z=25$, $H=7$, $C=2$, $G=6$, $T=19$. Thus we have

$$\begin{bmatrix}1 & 0\\ 25 & 25\end{bmatrix}M=\begin{bmatrix}7 & 2\\ 6 & 19\end{bmatrix}$$

The inverse of the first matrix above is actually itself! Thus

$$M=\begin{bmatrix}1 & 0\\ 25 & 25\end{bmatrix}\cdot\begin{bmatrix}7 & 2\\ 6 & 19\end{bmatrix}=\begin{bmatrix}7 & 2\\ 13 & 5\end{bmatrix}.$$

6.6.9 The easiest choice is "AA", "BA", "AB", which yields the vectors $(0,0)$, $(1,0)$, $(0,1)$. When we plug these in, we get

$$(e,f),(a+e,b+f),(c+e,d+f),$$

respectively. Thus $(0,0)$ reveals e and f. We then subtract (e,f) from the last two ciphertexts to obtain a,b,c,d.