Math/Cmsc 456, Jeffrey Adams
Test I, March 11, 2009 SOLUTIONS

1. (a) We can take any b, but a has to be relatively prime to 25.

   (b) There are 25 choices of b. Since $\phi(25) = 25(1 - \frac{1}{5}) = 20$, there are 20 choices of b, and $25 \times 20 = 500$ keys.

   (c) We have $E_{6,3}(E_{7,9}(x)) = E_{6,3}(7x + 9) = 6(7x + 9) + 3 \pmod{25}$, or $42x + 57 \pmod{25}$, or $17x + 7 \pmod{25}$. This is $E_{17,7}(x)$.

2. [15]

   (a) It can't be 1 since 1 is followed by 1 or 0. It can't be 2 since 11 is followed by 1 or 0. It can't be 3 since 111 is followed by 1 or 0. It can be 4 (and in fact $x_n = x_{n-2} + x_{n-4}$).

   (b) The relation is $a_{n+1} = a_1$.

3.
$$\begin{aligned}\frac{1}{-9}\begin{pmatrix}13 & -9\\ -1 & 2\end{pmatrix} &= -3\begin{pmatrix}13 & -9\\ -1 & 2\end{pmatrix}\\ &= \begin{pmatrix}-39 & 27\\ 3 & -6\end{pmatrix}\\ &= \begin{pmatrix}13 & 1\\ 3 & -6\end{pmatrix}\end{aligned}$$

   So we have

$$\begin{pmatrix}a & b\\ c & d\end{pmatrix} = \begin{pmatrix}13 & 1\\ 3 & -6\end{pmatrix}\begin{pmatrix}1 & 1\\ 1 & 2\end{pmatrix}$$

   Multiplying this out gives

$$M = \begin{pmatrix}a & b\\ c & d\end{pmatrix} = \begin{pmatrix}14 & 15\\ -3 & -9\end{pmatrix}$$

4. Recall $\phi(n) = n\prod(1-\frac{1}{p})$ where the product is over distinct primes dividing n.

   (a) $\phi(100) = 100(1-\frac{1}{4})(1-\frac{1}{5}) = 40$. Since 101 is prime $\phi(101) = 100$. Since $102 = 2 \times 3 \times 17$, $\phi(102) = 102(1-\frac{1}{2})(1-\frac{1}{3})(1-\frac{1}{17}) = 32$.

   (b) We know that $m^{\phi(1024)} = 1 \pmod{1024}$ for any $(m, 1024) = 1$, i.e. m odd. That is $m^{\phi(1024)+1} = m \pmod{1024}$, so solve $3b = \phi(1024) + 1$. Since $1024 = 2^{10}$, $\phi(1024) = 1024(1-\frac{1}{2}) = 512$. (Directly: every odd numer is relative prime to 1024, which is half of the numbers, i.e. $1024/2 = 512$). Therefore $3b = 513$, or $b = 171$.

5. (a) The ciphertext is $2^{13} = 2^6 2^6 2 = 9 \times 9 \times 2 = 26 \times 2 = 52 \pmod{55}$.

   (b) Since $\phi(55) = 40$, we have to solve $13d = 1 \pmod{40}$. Note that $3 \times 13 = 39 = -1 \pmod{40}$, so $3 \times (-13) = 1 \pmod{40}$. So $d = -13 = 27 \pmod{40}$.

   (c) Note that $11^2 = 121 = 11 \pmod{55}$. Then $11^e = 11 \times 11 \times 11 \cdots \times 11 =$ (multiplying one at a time) $= 11 \pmod{55}$. So 11 encrypts to 11 for any key $(35, e)$.