Math 110 - Midterm Exam - Fall, 2016

1. Let p be a prime. By the *projective line* $\mathbb{P}^1(\mathbb{Z}_p)$ over $\mathbb{Z}/p$ we will mean the set

$$\mathbb{Z}_p \cup \{\infty\}$$

where ∞ is a formal symbol. It does not connote a notion of size or infinity on the set $\mathbb{Z}_p$. Let A denote the matrix

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

where a, b, c, and d denote members of $\mathbb{Z}_p$, and $ad - bc \neq 0$. By the *fractional linear transformation* associated to A on $\mathbb{P}^1(\mathbb{Z}_p)$, we will mean the transformation $\hat{A}$ given by

$$z \longrightarrow \frac{az+b}{cz+d}$$

where $z \in \mathbb{P}^1(\mathbb{Z}_p)$. Here it is understood that if $cz + d = 0$, then the fraction is to be interpreted as $= \infty$, and that if $z = \infty$, the fraction is to be interpreted as $\frac{a}{c}$.

(a) Suppose you are given two invertible 2×2 matrices A and B over $\mathbb{Z}_p$. it follows that $A \cdot B$ is also invertible. Give a simple description of $\hat{A} \circ \hat{B}$ in terms of operations involving A and B.

(b) Show that if I is the identity matrix, then $\hat{I}$ is the identity on $\mathbb{P}^1(\mathbb{Z}_p)$.

(c) Suppose that we have an alphabet with $p + 1$ elements, and we code the letters by a one to one assignment π from the letters to $\mathbb{P}^1(\mathbb{Z}_p)$. For any message m, we also write $\pi(m)$ for the message obtained by replacing each letter λ by $\pi(\lambda)$. Show that for any invertible matrix A over $\mathbb{Z}_p$, there is an easy way to decrypt the message obtained by applying $\hat{A}$ to $\pi(m)$, and then applying π^{-1}.

(d) For $p = 31$ in part (c), and a 32 letter alphabet, describe the decryption scheme for the encryption scheme associated to the transformation

$$z \rightarrow \frac{2z+5}{7z+16}$$

2. Suppose we construct a block cipher, with blocks of length 2, as follows. We will use an invertible 2×2 matrix A over $\mathbb{Z}_{26}$ and a 2-vector v, also over $\mathbb{Z}_{26}$. Each block β of length two is encoded as a 2-vector over $\mathbb{Z}_{26}$, and and is then encrypted using the assignment

$$\beta \longrightarrow A\beta + v$$

(a) Show that for A and v as above, it is possible to decrypt any message, and give an explicit description of the decryption algorithm.

(b) Does the above procedure work for A given by

$$\begin{bmatrix} 7 & 5 \\ 9 & 11 \end{bmatrix}$$

and v given by

$$\begin{pmatrix} 4 \\ 9 \end{pmatrix}?$$

Why or why not? If it does, give the decryption formula.

(c) Does the above procedure work for A given by

$$\begin{bmatrix} 1 & 2 \\ 17 & 5 \end{bmatrix}$$

and v given by

$$\begin{pmatrix} 7 \\ 2 \end{pmatrix}?$$

Why or why not? If it does, give the decryption formula.

3. How many solutions to the equation

$$x^2 = 50$$

are there in $\mathbb{Z}_{4891}$? If there are any, enumerate them.

4. Construct addition and multiplication tables for a finite field with 9 elements. Find a primitive root, and give its order.

5. Show that if $gcd(e, 24) = 1$, then $e^2 \cong 1 (\mathrm{mod}\ 24)$. Show that if you use 35 as your RSA modulus, then the decryption and encryption exponents are always the same.