Math 373/578 Homework, Week 7, Solutions

Instruction: In doing this set of problems, you can use any electronic devise to help your computation. But you need to present conclusions based on the analysis of your computation.

The English Alphabet: Unless otherwise stated, we will use the English alphabet with A – Z represented by the mod 26 numbers 0 - 25, respectively, as shown below.

| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

1. What is a cryptosystem? (Give the answer in your own language based on your understanding. It is OK to go to library to find information in a book, or to use google to find information in the web for you to answer this question. However, when you quote something that is not your origination, please give a reference of the source, such as a book, an article in a journal, and an url of a website.)

Purpose of this exercise: Train us to know how to find answers by using resources around us.

2. Solve the system of equations in $\mathbb{Z}_{26}$

\[
\begin{pmatrix}
2 & 3 \\
7 & 8
\end{pmatrix}
\begin{pmatrix}
x \\
y
\end{pmatrix}
=
\begin{pmatrix}
1 \\
-1
\end{pmatrix}
\]

by doing the following two steps: (No credit for solutions not doing these two steps).

(i) Let $A = \begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix}$. Find $A^{-1}$ in $\mathbb{Z}_{26}$.

(ii) Multiply both sides of the equations by $A^{-1}$ from the left to get the solutions of system of equations.

Purpose of this exercise: To become more familiar with matrix operations.

Solution First we compute the determinant $d = \text{det}(A) = 2 \cdot 8 - 3 \cdot 7 = -5 \equiv 21 \pmod{26}$. Thus

\[
A^{-1} = 21 \begin{pmatrix} 8 & -3 \\ -7 & 2 \end{pmatrix} \equiv \begin{pmatrix} 14 & 11 \\ 17 & 10 \end{pmatrix} \pmod{26}, \text{ and so } \begin{pmatrix} x \\ y \end{pmatrix} \equiv \begin{pmatrix} 14 & 11 \\ 17 & 10 \end{pmatrix} \begin{pmatrix} 1 \\ -1 \end{pmatrix} \equiv \begin{pmatrix} 3 \\ 7 \end{pmatrix} \pmod{26}.
\]

If we use matlab, we can do the following.

```
>> m=26; A=[2 3;7 8]
A =
    2    3
    7    8
>> format rat;
>> A1 = inv(A)
A1 =
   -8/5    3/5
    7/5   -2/5
>> A2=mod(5*A1, 26)
A2 =
    18     3
    24     7
```
3. We have intercepted the following messages QVNAYQHI and FWMDIQ. Intelligence agents have informed us that the cipher texts were encoded by the a cryptosystem using digraphs with a fixed but unknown enciphering matrix $A$. Moreover, the plain text of first six letters of QVNAYQHI are NOANSW.

(i) Find the enciphering matrix $A$ and the deciphering matrix $A^{-1}$.
(ii) Decrypt the cipher text QVNAYQHI.
(iii) Decrypt the cipher text FWMDIQ.

**Solution: (The routine method)**

(i) Find $A^{-1}$. The plain text we know is NOANSW, corresponding to the cipher text QVNAYQ. To compute $A^{-1}$, we let

$$P = NOSW = \begin{pmatrix} 13 & 18 \\ 14 & 22 \end{pmatrix}, \quad C = QVYQ = \begin{pmatrix} 16 & 24 \\ 14 & 22 \end{pmatrix}, \quad \text{and } A^{-1} = PC^{-1}.$$ 

But $C^{-1}$ does not exist. We let $A_1, P_1$ and $C_1$ be the matrices of $A, P$, and $C$ in $\mathbb{Z}_{13}$, respectively. Write

$$A^{-1} = A_1^{-1} + 13A_0, \pmod{26},$$

for some $A_0 \in M_2(\mathbb{Z}_2)$. Then

$$C_1 = \begin{pmatrix} 3 & 11 \\ 8 & 3 \end{pmatrix}, \quad \text{and } P_1 = \begin{pmatrix} 0 & 5 \\ 1 & 9 \end{pmatrix}.$$ 

This leads to

$$C_1^{-1} = \begin{pmatrix} 10 & 11 \\ 8 & 10 \end{pmatrix} \quad \text{and } A_1^{-1} = P_1C_1^{-1} = \begin{pmatrix} 1 & 11 \\ 4 & 10 \end{pmatrix} \pmod{13}.$$ 

To determine $A^{-1} = A_1 + 13A_0$, let

$$A_0 = \begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix}, \quad \text{where each } x_{ij} \in \mathbb{Z}_2.$$ 

Since $\det(A^{-1})$ has an inverse (mod 26), it must be an odd number, and so

$$\det(A^{-1}) \equiv (1 + x_{11})x_{22} - (1 + x_{12})x_{21} \equiv 1 \pmod{2}.$$
Therefore, either $1 + x_{11} \equiv x_{22} \equiv 1$ and $x_{21} \equiv 0$ or $1 + x_{12} \equiv 0$, or $(1 + x_{12})x_{21} \equiv 1$ and $1 + x_{11} \equiv 0$ or $x_{22} \equiv 0 \pmod{2}$. It follows that $A_0$ is one of the following:

\[
\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.
\]

Use matlab to test each of them and find $A_0 = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$. Thus $A^{-1} = \begin{pmatrix} 14 & 11 \\ 17 & 10 \end{pmatrix}$ and $A = \begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix}$.

(ii) The plain text is $\text{NOANSWER}$, by the following.

```matlab
>> A2 = [14 11;17 10]
>> C=[16 13 24 7; 21 0 16 8]
>> P = mod(A2*C, 26)
```

(iii) The plain text is $\text{ATTACK}$, by the following.

```matlab
>> A2 = [14 11;17 10]
>> C=[5 12 8; 22 3 16]
>> P = mod(A2*C, 26)
```

Another Solution: (use of algebra) As the plain text $\text{NOAN}$ corresponds to the cipher text $\text{QVNA}$, we can assume the enciphering matrix $A$ has the form

\[
A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \text{ such that } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 13 & 0 \\ 14 & 13 \end{pmatrix} = \begin{pmatrix} 16 & 13 \\ 21 & 0 \end{pmatrix}.
\]

To find $A$, it suffices to find $a, b, c,$ and $d$. The matrix equation corresponding to the system in $\mathbb{Z}_{26}$.

\[
\begin{cases} 
13a + 14b = 16 \\
13b = 13 \\
13c + 14d = 21 \\
13d = 0
\end{cases}.
\]

Solve $13b \equiv 13 \pmod{26}$ for $b$ to get $b \equiv 1 \pmod{2}$. Solve $13d \equiv 13 \pmod{26}$ for $d$ to get $d \equiv 0 \pmod{2}$.

Subtract $13b \equiv 13 \pmod{26}$ from $13a + 14b \equiv 16 \pmod{26}$ to get $13a + b \equiv 3 \pmod{26}$, or $13a \equiv 3 - b \pmod{26}$. This has a solution if and only if $3 - b \equiv 0 \pmod{13}$ or $b \equiv 3 \pmod{13}$. Since $0 \leq b \leq 25$ and since $b \equiv 1 \pmod{2}$, we must have $b = 3$. Substitute $b = 3$ in $13a + 14b \equiv 16 \pmod{26}$ to get $13a \equiv 0 \pmod{26}$. Thus $a \equiv 0 \pmod{2}$.

Similarly, subtract $13d \equiv 0 \pmod{26}$ from $13c + 14d \equiv 21 \pmod{26}$ to get $13c + d \equiv 21 \pmod{26}$, or $13c \equiv 21 - d \pmod{26}$. This has a solution if and only if $21 - d \equiv 0 \pmod{13}$ or $d \equiv 8 \pmod{13}$. Since $0 \leq d \leq 25$ and since $d \equiv 0 \pmod{2}$, we must have $d = 8$. Substitute $d = 8$ in $13c + 14d \equiv 21 \pmod{26}$ to get $13c \equiv 13 \pmod{26}$. Thus $c \equiv 1 \pmod{2}$.

We now know that $b = 3$ and $d = 8$. To determine $a$ and $c$, we use the fact that the plain text $\text{ANSW}$ corresponds to the cipher text $\text{NAYQ}$, and so

\[
\begin{pmatrix} a & 3 \\ c & 8 \end{pmatrix} \begin{pmatrix} 0 & 18 \\ 13 & 22 \end{pmatrix} = \begin{pmatrix} 13 & 24 \\ 0 & 16 \end{pmatrix}.
\]
This gives $24 \equiv 18a - 12 \pmod{26}$ and $16 \equiv 18c - 32 \pmod{26}$. Accordingly, we have $18a \equiv 10 \pmod{26}$ and $18c \equiv 22 \pmod{26}$. These imply that $9a \equiv 5 \pmod{13}$ or $a \equiv 2 \pmod{13}$, and $9c \equiv 11 \pmod{13}$ or $c \equiv 7 \pmod{13}$. Since $0 \leq a \leq 25$ and since $a \equiv 2 \pmod{13}$, we must have $a = 2$ or $a = 15$. Since we also know that $a \equiv 0 \pmod{2}$, we must have $a = 2$. Similarly, since $0 \leq c \leq 25$ and since $c \equiv 7 \pmod{13}$, we must have $c = 7$ or $c = 20$. Since we also know that $c \equiv 1 \pmod{2}$, we must have $c = 7$. This gives

$$A = \begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix} \text{ and so } A^{-1} = \begin{pmatrix} 14 & 11 \\ 17 & 10 \end{pmatrix}.$$