MAT 421 Number Theory
Takehome Exam 2

Note: Read the test instructions in my email carefully and thoroughly before you begin your exam. Failure to follow the instructions could result in point reductions or no point on individual problems.

1. In the 27-letter alphabet (with blank=26), use the affine enciphering transformation with key $a = 13$, $b = 9$ to encipher the message "HELP ME."

   Solution. The enciphering transformation is

$$C \equiv 13P + 9 \mod 27$$

Plaintext	H	E	L	P		M	E
P	7	4	11	15	26	12	4
C	19	7	17	15	23	3	7
Ciphertext	T	H	R	P	X	D	H

2. In a long string of ciphertext which was encrypted by means of an affine map on single-letter message units in the 26-letter alphabet, you observe that the most frequently occurring letters are "Y" and "V", in that order. Assuming that those ciphertext message units are the encryption of "E" and "T", respectively, read the message "QAOOYQQEVHEQV".

   Solution. Let $P \equiv a'C + b' \mod 26$. Assuming that ciphertexts Y and V correspond to E and T, respectively, we have the system of congruences

$$\begin{aligned} 4 &\equiv 24a' + b' \mod 26 \\ 19 &\equiv 21a' + b' \mod 26 \end{aligned}$$

Subtracting the second equation from the first one, we obtain $3a' = 11 \mod 26$. Since $(3,26) = 1$, there exists $3^{-1} \in \mathbb{Z}/26\mathbb{Z}$ which is 9. Thus a' is found to be

$$a' \equiv 9 \cdot 11 \mod 26 \equiv 21 \mod 26$$

and subsequently, from the first equation, b' is given by

$$b' \equiv 4 - 24a' \mod 26 \equiv 20 \mod 26$$

The deciphering transformation is then

$$P \equiv 21C + 20 \mod 26$$

Ciphertext	*Q*	*Q*	*O*	*O*	*Y*	*Q*	*Q*	*E*	*V*	*H*	*E*	*Q*	*V*
C	16	0	14	14	24	16	16	4	21	7	4	16	21
P	18	20	2	2	4	18	18	0	19	11	0	18	19
Plaintext	*S*	*U*	*C*	*C*	*E*	*S*	*S*	*A*	*T*	*L*	*A*	*S*	*T*

3. Find the inverse matrix of

$$\begin{pmatrix} 15 & 17 \\ 4 & 9 \end{pmatrix} \mod 26$$

Write the entries in the inverse matrix as nonnegative integers less than 26.

Solution.

$$\begin{aligned} \det \begin{pmatrix} 15 & 17 \\ 4 & 9 \end{pmatrix} &= 15 \cdot 9 - 17 \cdot 4 \\ &\equiv 15 \mod 26 \end{aligned}$$

Since $(15,26) = 1$, there exists $15^{-1} \in \mathbb{Z}/26\mathbb{Z}$ which is 7. The inverse matrix is then given by

$$\begin{pmatrix} 7 \cdot 9 & -7 \cdot 17 \\ -7 \cdot 4 & 7 \cdot 15 \end{pmatrix} \equiv \begin{pmatrix} 11 & 11 \\ 24 & 1 \end{pmatrix} \mod 26$$

4. Find all solutions $\begin{pmatrix} x \\ y \end{pmatrix} \mod N$, writing x and y as nonnegative integers less than N.

(a)

$$\begin{aligned} x+4y &\equiv 1 \mod 9 \\ 5x+7y &\equiv 1 \mod 9 \end{aligned}$$

Solution. The system of congruences is equivalent to the matrix equation

$$\begin{pmatrix} 1 & 4 \\ 5 & 7 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} \equiv \begin{pmatrix} 1 \\ 1 \end{pmatrix} \mod 9$$

$\det\begin{pmatrix} 1 & 4 \\ 5 & 7 \end{pmatrix} \equiv 5 \mod 9$ and $(5,9)=1$, so there exists $5^{-1} \in \mathbb{Z}/9\mathbb{Z}$ which is 2. The inverse matrix is

$$\begin{pmatrix} 2\cdot 7 & -2\cdot 4 \\ -2\cdot 5 & 2\cdot 1 \end{pmatrix} \equiv \begin{pmatrix} 5 & 1 \\ 8 & 2 \end{pmatrix} \mod 9$$

The solution is then given by

$$\begin{aligned} \begin{pmatrix} x \\ y \end{pmatrix} &\equiv \begin{pmatrix} 5 & 1 \\ 8 & 2 \end{pmatrix}\begin{pmatrix} 1 \\ 1 \end{pmatrix} \mod 9 \\ &\equiv \begin{pmatrix} 6 \\ 1 \end{pmatrix} \mod 9 \end{aligned}$$

(b)

$$\begin{aligned} x+4y &\equiv 1 \mod 9 \\ 5x+8y &\equiv 2 \mod 9 \end{aligned}$$

Solution. $\det\begin{pmatrix} 1 & 4 \\ 5 & 8 \end{pmatrix} = -12 \equiv 6 \mod 9$ but $(6,9)=3>1$, so there does not exist $6^{-1} \in \mathbb{Z}/9\mathbb{Z}$ and subsequently the matrix does not have an inverse matrix in $\mathbb{Z}/9\mathbb{Z}$.

Let us multiply the first equation by 2 and then subtract the resulting equation from the second equation. Then we obtain $3x \equiv 0 \mod 9$ whose solutions are $x = 0,3,6$. If $x=0$, then from the first equation, we have $4y \equiv 1 \mod 9$ whose solution is $y \equiv 7 \mod 9$. If

$x = 3$, then from the first equation, we have $4y \equiv 7 \mod 9$ whose solution is $y \equiv 4 \mod 9$. If $x = 6$, then from the first equation, we have $4y \equiv 4 \mod 9$ whose solution is $y \equiv 1 \mod 9$. Therefore, there are three solutions

$$\begin{pmatrix} 0 \\ 7 \end{pmatrix}, \begin{pmatrix} 3 \\ 4 \end{pmatrix}, \begin{pmatrix} 6 \\ 1 \end{pmatrix}$$

5. You intercepted the message “SONAFQCHMWPTVEVY”, which you know resulted from a linear enciphering transformation of digraph-vectors, where the sender used the usual 26-letter alphabet A-Z with numerical equivalents 0-25, respectively An earlier statistical analysis of a long string of intercepted ciphertext revealed that the most frequently occurring ciphertext digraphs were “KH” and “XW” in that order. You take a guess that those digraphs correspond to “TH” and “HE”, respectively, since those are the most frequently occurring digraphs in most long plaintext messages on the subject you think is being discussed. Find the deciphering matrix, and read the message.

   Solution. Assuming that ciphertext digraphs KH and XW correspond to plaintext digraphs TH and HE, respectively, the enciphering matrix A is given by

$$\begin{aligned} A &= CP^{-1} \\ &= \begin{pmatrix} 10 & 23 \\ 7 & 22 \end{pmatrix} \begin{pmatrix} 19 & 7 \\ 7 & 4 \end{pmatrix}^{-1} \\ &= \begin{pmatrix} 10 & 23 \\ 7 & 22 \end{pmatrix} \begin{pmatrix} 4 & -7 \\ -7 & 19 \end{pmatrix} \\ &\equiv \begin{pmatrix} 9 & 3 \\ 4 & 5 \end{pmatrix} \mod 26 \end{aligned}$$

   The ciphertext message SONAFQCHMWPTVEVY is represented by the matrix C as

$$C = \begin{pmatrix} 18 & 13 & 5 & 2 & 12 & 15 & 21 & 21 \\ 14 & 0 & 16 & 7 & 22 & 19 & 4 & 24 \end{pmatrix}$$

   The deciphering matrix A^{-1} is given by

$$A^{-1} = \begin{pmatrix} 15 \cdot 5 & -15 \cdot 3 \\ -15 \cdot 4 & 15 \cdot 9 \end{pmatrix} \equiv \begin{pmatrix} 23 & 7 \\ 18 & 5 \end{pmatrix} \mod 26$$

The deciphering of C is then

$$\begin{aligned}
P &= A^{-1}C \\
&= \begin{pmatrix} 23 & 7 \\ 18 & 5 \end{pmatrix} \begin{pmatrix} 18 & 13 & 5 & 2 & 12 & 15 & 21 & 21 \\ 14 & 0 & 16 & 7 & 22 & 19 & 4 & 24 \end{pmatrix} \\
&\equiv \begin{pmatrix} 18 & 13 & 19 & 17 & 14 & 10 & 17 & 1 \\ 4 & 0 & 14 & 19 & 14 & 1 & 8 & 4 \end{pmatrix} \mod 26
\end{aligned}$$

The plaintext message is ”SENATORTOOKBRIBE“.