

Number Theory  
Problem Set 5  
Enciphering Matrices

1. Find the inverses of the following matrices mod  $N$ . Write the entries in the inverse matrix as nonnegative integers less than  $N$ .

(a)  $\begin{pmatrix} 1 & 3 \\ 4 & 3 \end{pmatrix} \pmod{5}$

(b)  $\begin{pmatrix} 1 & 3 \\ 4 & 3 \end{pmatrix} \pmod{29}$

(c)  $\begin{pmatrix} 15 & 17 \\ 4 & 9 \end{pmatrix} \pmod{26}$

(d)  $\begin{pmatrix} 40 & 0 \\ 0 & 21 \end{pmatrix} \pmod{841}$

(e)  $\begin{pmatrix} 197 & 62 \\ 603 & 271 \end{pmatrix} \pmod{841}$

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

(a)

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

(b)

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

(c)

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

(d)

$$\begin{aligned}x + 4y &\equiv 0 \pmod{9} \\5x + 8y &\equiv 0 \pmod{9}\end{aligned}$$

3. 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.