tem with enciphering matrix $A_2 \in M_2(\mathbf{Z}/N\mathbf{Z})^*$ is also a linear enciphering transformation.

12. In order to increase the difficulty of breaking your cryptosystem, you decide to encipher a digraph-vector in the 26-letter alphabet by first applying the matrix

$$\begin{pmatrix} 3 & 11 \\ 4 & 15 \end{pmatrix},$$

working modulo 26, and then applying the matrix

$$\begin{pmatrix} 10 & 15 \\ 5 & 9 \end{pmatrix},$$

working modulo 29. (Note that applying two matrices in succession while working with the same modulus is equivalent to applying a single matrix, as shown in Exercise 11; but if you change modulus the two-step encryption is much more complicated.) Thus, while your plaintexts are in the 26-letter alphabet, your ciphertexts will be in the 29-letter alphabet we used in Exercise 9.

(a) Encipher the message "SEND."

(b) Describe how to decipher a ciphertext by applying two matrices in succession, and decipher "ZMOY."

13. Prove that if a non-invertible $A \in M_2(\mathbf{Z}/N\mathbf{Z})$ is used to encipher digraph vectors by means of the formula $C = AP$, then every ciphertext one sends can be deciphered as coming from at least two different possible plaintexts.

14. You intercept the message "S GNLIKD?KOZQLLIOMKUL.VY" (here the blank after the S is part of the message). Suppose that a linear enciphering transformation $C = AP$ is being used with a 30-letter alphabet, in which A—Z have the usual numerical equivalents 0—25, blank=26, .=27, ,=28, ?=29. You also know that the last six letters of the plaintext are the signature KARLA followed by a period. Find the deciphering matrix A^{-1} and the full plaintext message.

15. You intercept the message "KVW? TA!KJB?FVR ." (The blanks after ? and R are part of the message, but the final . is not.) You know that a linear enciphering transformation is being used with a 30-letter alphabet, in which A—Z have numerical equivalents 0—25, blank=26, ?=27, !=28, .=29. You further know that the first six letters of the plaintext are "C.I.A." Find the deciphering matrix A^{-1} and the full plaintext message.

16. Suppose that $N = mn$, where $g.c.d.(m, n) = 1$. Any $A \in M_2(\mathbf{Z}/N\mathbf{Z})$ can be considered in $M_2(\mathbf{Z}/m\mathbf{Z})$ or $M_2(\mathbf{Z}/n\mathbf{Z})$ by simply reducing the entries modulo m or n. Let $\overline{A}$ and $\tilde{A}$ denote the corresponding matrices in $M_2(\mathbf{Z}/m\mathbf{Z})$ and $M_2(\mathbf{Z}/n\mathbf{Z})$, respectively.

(a) Prove that the map that takes A to the pair $(\overline{A}, \tilde{A})$ is a 1-to-1 correspondence between $M_2(\mathbf{Z}/N\mathbf{Z})$ and the set $M_2(\mathbf{Z}/m\mathbf{Z}) \times M_2(\mathbf{Z}/n\mathbf{Z})$ of all pairs of matrices, one modulo m and one modulo n.