then we could try to use that pair of columns in place of either the first or second columns of P and C, hoping to obtain then an invertible matrix. But suppose we have no further information, or that none of the known plaintext digraphs give us an invertible matrix P. Then we cannot find A^{-1} exactly. However, we might be able to get enough information about A^{-1} to cut down drastically the number of possibilities for the deciphering matrix. We now illustrate this with an example. (For more on this, see the exercises at the end of the section.)

Example 7. Suppose we know than our adversary is using an enciphering matrix A in the 26-letter alphabet. We intercept the ciphertext "WKNCCHSSJH," and we know that the first word is "GIVE." We want to find the deciphering matrix A^{-1} and read the message.

Solution. If we try to proceed as in Example 6, writing

$$P = \text{“}GIVE\text{”} = \begin{pmatrix} 6 & 21 \\ 8 & 4 \end{pmatrix},$$

$$C = \text{“}WKNC\text{”} = \begin{pmatrix} 22 & 13 \\ 10 & 2 \end{pmatrix}, \qquad \text{and} \qquad A^{-1} = PC^{-1};$$

we immediately run into a problem, since $det(C) = 18$ and $g.c.d.(18, 26) = 2$. We can proceed as follows. Let $\overline{A}$ denote the reduction modulo 13 of the matrix A, and similarly for $\overline{P}$ and $\overline{C}$. If we consider these matrices in $M_2(\mathbf{Z}/13\mathbf{Z})$, we can take C^{-1} (more precisely, $\overline{C}^{-1}$), because $g.c.d.(det(C), 13) = 1$. Thus, from $\overline{P} = \overline{A}^{-1}\overline{C}$ we can compute

$$\overline{A}^{-1} = \overline{P}\,\overline{C}^{-1} = \begin{pmatrix} 6 & 8 \\ 8 & 4 \end{pmatrix}\begin{pmatrix} 9 & 0 \\ 10 & 2 \end{pmatrix}^{-1} = \begin{pmatrix} 2 & 4 \\ 3 & 2 \end{pmatrix}.$$

Since the entries of A^{-1}, which are integers mod 26, must reduce to

$$\begin{pmatrix} 2 & 4 \\ 3 & 2 \end{pmatrix}$$

modulo 13, it follows that there are two possibilities for each entry in the matrix A^{-1}. More precisely,

$$A^{-1} = \begin{pmatrix} 2 & 4 \\ 3 & 2 \end{pmatrix} + 13A_1,$$

where $A_1 \in M_2(\mathbf{Z}/2\mathbf{Z})$ is a 2×2–matrix of 0's and 1's. That leaves $2^4 = 16$ possibilities. However, in the first place, since A^{-1} is invertible, its determinant must be prime to 26, and hence also prime to 2 (i.e., odd). This consideration rules out all but 6 possibilities for A_1. In the second place, when we substitute