solving the congruence $P \equiv A^{-1}C \ mod\ n$ and after taking into account that $p \nmid det(A^{-1})$.

(b) Suppose that $p$ does *not* divide all of the entries in $C$. Describe how to use the congruence $P \equiv A^{-1}C \ mod\ p$ to further reduce the number of possibilities for $A^{-1}$. How many possibilities are you now left with? Example 8 and Exercise 15 illustrate this in the case $p = 2$.

23. You want to find a $2 \times 2$ enciphering matrix $A$ modulo 30. You have two plaintext/ciphertext digraph pairs (in a 30-letter alphabet), which enables you to write $AP \equiv C \ mod\ 30$, where

$$P = \begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix}, \qquad C = \begin{pmatrix} 17 & 8 \\ 8 & 29 \end{pmatrix}.$$

(a) Working modulo 10, write $A$ in the form $A \equiv A_0 + 10A_1 \ mod\ 30$, where $A_1$ is an unknown matrix modulo 3 (whose entries are 0, 1 or 2) and $A_0$ is a matrix you know from your mod 10 computations. Choose $A_0$ so that all of its entries are between 0 and 29 and are divisible by 3.

(b) Working modulo 3, find the second column of the matrix $A_1$.

(c) How many possibilities are there for the original matrix $A$? List them all.

24. Let

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbf{Z}/N\mathbf{Z})^*$$

be the matrix of a linear enciphering transformation of digraphs in an $N$-letter alphabet. By a *fixed digraph* of $A$ we mean a digraph vector $P$ whose corresponding ciphertext vector $C$ is the same as $P$, i.e., $AP = P$. In this problem we suppose that $A$ is not the identity matrix. (After all, there's no point in considering the enciphering transformation that doesn't even make a half-hearted attempt to disguise anything.)

(a) Show that the digraph "AA"$= \binom{0}{0}$ is always fixed, and find a condition on

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

which is equivalent to "AA" being the *only* fixed digraph.

(b) If $N$ is a prime number and if "AA" is not the only fixed digraph, prove that there are exactly $N$ fixed digraphs.

25. You intercept the message

"WUXHURWZNQR XVUEXU!JHALGQGJ?",

which you know was encoded using an **affine** transformation of vectors $\binom{x}{y}$ in an 841-letter alphabet. Here the numerical equivalent of a digraph is the number $x = 29x_1 + x_2$, where $x_1$ is the number of the first letter and $x_2$ is the number of the second letter in the digraph (the 29 letters are numbered as in Exercise 9). Thus, each block of four letters