$$\begin{pmatrix} 2 & 4 \\ 3 & 2 \end{pmatrix} + 13A_1$$

for A^{-1} in the equation

$$A^{-1}\begin{pmatrix} 22 & 13 \\ 10 & 2 \end{pmatrix} = \begin{pmatrix} 6 & 21 \\ 8 & 4 \end{pmatrix}$$

(this means entry-by-entry congruence mod 26), we eliminate all but 2 possibilities, namely,

$$A_1 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix},$$

i.e.,

$$A^{-1} = \begin{pmatrix} 15 & 4 \\ 16 & 15 \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} 15 & 17 \\ 16 & 15 \end{pmatrix}.$$

Attempting to decipher with the first matrix yields "GIVEGHEMHP," which must be wrong. Deciphering with the second matrix

$$A^{-1} = \begin{pmatrix} 15 & 17 \\ 16 & 15 \end{pmatrix}$$

leads to "GIVETHEMUP." So that must be correct. Although a certain amount of trial and error is involved, it's better than running through all 157,248 possibilities for a deciphering matrix $A^{-1} \in M_2(\mathbf{Z}/26\mathbf{Z})^*$.

Remark. In Example 7 it would perhaps be more efficient to adjust the entries in $\overline{A}^{-1}$ by multiples of 13 so that they become divisible by 2, i.e., to define A_1 by writing:

$$A^{-1} = \begin{pmatrix} 2 & 4 \\ 16 & 2 \end{pmatrix} + 13A_1.$$

Then one can obtain information on A_1 by working modulo 2, since we now have $A_1C \equiv P \ mod\ 2$.

Affine enciphering transformations. A more general way to encipher a digraph-vector $P = \binom{x}{y}$ is to apply a 2 × 2–matrix $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in M_2(\mathbf{Z}/N\mathbf{Z})$ and then add a constant vector $B = \binom{e}{f}$:

$$C = AP + B,$$

i.e.,

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} e \\ f \end{pmatrix} = \begin{pmatrix} ax + by + e \\ cx + dy + f \end{pmatrix}.$$

This is called an "affine" map, and is analogous to the enciphering function $C = aP + b$ that we studied in §1 when we were using single-letter message