(a)

$$2x+3y\equiv 1 \; mod\; 26,$$
$$7x+8y\equiv 2 \; mod\; 26;$$

(b)

$$x+3y\equiv 1 \; mod\; 26,$$
$$7x+9y\equiv 2 \; mod\; 26;$$

(c)

$$x+3y\equiv 1 \; mod\; 26,$$
$$7x+9y\equiv 1 \; mod\; 26.$$

Solution. The matrix form of the system (a) is $AX \equiv B\, mod\, 26$, where A is the matrix in Example 1, $X = \binom{x}{y}$, and $B = \binom{1}{2}$. We obtain the unique solution

$$X \equiv A^{-1}B \equiv \begin{pmatrix} 14 & 11 \\ 17 & 10 \end{pmatrix} \begin{pmatrix} 1 \\ 2 \end{pmatrix} \equiv \begin{pmatrix} 10 \\ 11 \end{pmatrix} \; mod\; 26.$$

The matrix of the systems (b)–(c) does not have an inverse modulo 26, since its determinant is 14, which has a common factor of 2 with 26. However, we can work modulo 13, i.e., we can find the solution to the same congruence mod 13 and see if it gives a solution which works modulo 26. Modulo 13 we obtain

$$\begin{pmatrix} x \\ y \end{pmatrix} \equiv \begin{pmatrix} 9 & 10 \\ 6 & 1 \end{pmatrix} \begin{pmatrix} e \\ f \end{pmatrix}$$

(where $\binom{e}{f} = \binom{1}{2}$ in part (b) and $\binom{1}{1}$ in part (c)). This gives $\binom{x}{y} \equiv \binom{3}{8}$ and $\binom{6}{7}$ *mod* 13, respectively. Testing the possibilities modulo 26, we find that in part (b) there are *no* solutions, and in part (c) there are *two* solutions: $x = 6,\ y = 7$ and $x = 19,\ y = 20$.

Another way to solve systems of equations (preferable sometimes, especially when the matrix is not invertible) is to eliminate one of the variables (e.g., in parts (b) and (c), one could subtract 7 times the first congruence from the second).

To return to cryptography, we see from Proposition III.2.1 that we can get enciphering transformations of our digraph-vectors by using matrices $A \in M_2(\mathbf{Z}/N\mathbf{Z})$ whose determinant has no common factor with N:

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \qquad D = ad - bc, \qquad g.c.d.(D, N) = 1.$$

Namely, each plaintext message unit $P = \binom{x}{y}$ is taken to a ciphertext $C = \binom{x'}{y'}$ by the rule