with entries in a ring R can be multiplied by a column-vector $\binom{x}{y}$ with $x,\ y \in R$ to get a new vector $\binom{x'}{y'}$:

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

This gives a "linear map" from vectors to vectors, meaning that a linear combination $\binom{k_1x_1+k_2x_2}{k_1y_1+k_2y_2}$, where k_1 and k_2 are in the ring R, is taken to $\binom{k_1x'_1+\ kx'_2}{k_1y'_1+k_2y'_2}$. The only difference with the situation earlier in our review of linear algebra is that now everything is in our ring R rather than in the real numbers.

We shall want to apply all of this when our ring is $R = \mathbf{Z}/N\mathbf{Z}$. The next proposition will be stated in that case, although the analogous proposition is true for any R.

Proposition III.2.1. *Let*

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbf{Z}/N\mathbf{Z}) \quad \text{and set} \quad D = ad - bc.$$

The following are equivalent:

(a) *g.c.d.(D,N)=1;*

(b) *A has an inverse matrix;*

(c) *if x and y are not both 0 in $\mathbf{Z}/N\mathbf{Z}$, then $A\binom{x}{y} \neq \binom{0}{0}$;*

(d) *A gives a 1-to-1 correspondence of $(\mathbf{Z}/N\mathbf{Z})^2$ with itself.*

Proof. We already showed that (a)$\Longrightarrow$(b). It suffices now to prove that (b)$\Longrightarrow$(d)$\Longrightarrow$(c)$\Longrightarrow$(a).

Suppose that (b) holds. Then part (d) also holds, because A^{-1} gives the inverse map from $\binom{x'}{y'}$ to $\binom{x}{y}$. Next, if we have (d), then $\binom{x}{y} \neq \binom{0}{0}$ implies that $A\binom{x}{y} \neq A\binom{0}{0} = \binom{0}{0}$, and so (c) holds. Finally, we prove (c)$\Longrightarrow$(a) by showing that (a) false $\Longrightarrow$ (c) false. So suppose that (a) is false, and set $m = g.c.d.(D, N) > 1$ and let $m' = N/m$. Three cases are possible.

Case (i). If all four entries of A are divisible by m, set $\binom{x}{y} = \binom{m'}{m'}$, to get a contradiction to (c).

Case (ii). If a and b are not both divisible by m, set $\binom{x}{y} = \binom{-bm'}{am'}$. Then

$$A\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} -bm' \\ am' \end{pmatrix} = \begin{pmatrix} -abm' + bam' \\ -cbm' + dam' \end{pmatrix} = \begin{pmatrix} 0 \\ Dm' \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix},$$

because $m|D$ and so $N = mm'|Dm'$.

Case (iii). If c and d are not both divisible by m, set $\binom{x}{y} = \binom{dm'}{-cm'}$, and proceed as in case (ii). These three cases exhaust all possibilities. Thus, (a) false implies (c) false. This completes the proof of Proposition III.2.1.

Example 2. Solve the following systems of simultaneous congruences: