

**Q02A** If our we set  $[a]$  to be  $[7]$  our system of equations and multiply the first equation by 5 and the second by 3 we get:

$$\begin{cases} [35][x] + [15][y] &= [5](1) \\ [6][x] + [15][y] &= [-3](2) \end{cases}$$

Subtracting equation (1) by equation (2) we will get the new equation:  $[29][y] = [8]$ . Note that  $[29] = [5]$  our equation will become:

$$[5][x] = [8]$$

We know that  $[5]$  and 12 are co-prime, and thus by INV (with integers) we know that  $[5]$  will have a mathematical inverse, thus if we multiply both sides we will get:

$$[5]^{-1}[5][y] = [8][5]^{-1}$$

By definition  $[5]^{-1}[5] = 1$  and we know that  $[5][5] = [1] \pmod{12}$  and thus the mathematical inverse of  $[5]$  is  $[5]$ . Our equation thus becomes:

$$[x] = [40] = [4]$$

Plugging this into equation (2) we get that:

$$\begin{aligned} [6][x] + [15][y] &= [-3] \\ [15][y] &= [-3] - [6][4] \\ [3][y] &= [-3] - [0] \\ [3][y] &= [9] \end{aligned}$$

We know this condition will be satisfied if  $[y] = [3]$  and thus our solution is:  $[x] = [4]$  and  $[y] = [3]$

**Q01B** Visually we know that  $\mathbb{Z}_7$  is a field, if we look at the multiplication table, each possible congruence class  $[a]$  has a corresponding congruence class  $[b]^{-1}$  such that:

$$[a][b] = 1$$

This happens because 7 is a prime and  $[a]$  is co-prime to 7. This means that  $d = \gcd([a], 7) = 1$  and by definition of MAT since  $d|1$  there must be a solution  $[b]$  for each  $[a]$  that solves the above equality (which means  $[a]$  will have a multiplicative inverse).

On the other hand 8 is not prime and thus not all  $[a]$ 's are co-prime to 8. If  $[a]$  is not coprime to 7 this would result in  $d = \gcd([a], 8) \neq 1$  and thus MAT could not apply as  $d \nmid 1$ , which means for all  $[b]$  of that a:

$$[a][b] \neq 1$$

Which means that  $[a]$  has no multiplicative inverse. As an illustrative example let's consider  $[a] = [2]$  the multiplicative table will give us:

$\cdot$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[6]$	$[7]$
$[2]$	$[0]$	$[2]$	$[4]$	$[6]$	$[0]$	$[2]$	$[4]$	$[6]$

We can thus see that  $[1]$  is never a result and thus  $[a]$  will never have a multiplicative inverse.