

**Q02A** If our we set  $[a]$  to be  $[7]$  our system of equations for  $\mathbb{Z}_{12}$  and multiply the first equation by 5 and the second by 3 we get:

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

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

$$[5][x] \equiv [8]$$

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:

$$[5]^{-1}[5][y] \equiv [8][5]^{-1}$$

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:

$$[x] \equiv [40] \equiv [4]$$

Plugging this into equation (2) we get that:

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

We know this condition will be satisfied if  $[y] = [3]$  and thus our solution set is given by both:

$$\begin{aligned} \{x \in \mathbb{Z} : x & \equiv 4 \pmod{12}\} \\ \{y \in \mathbb{Z} : y & \equiv 3 \pmod{12}\} \end{aligned}$$

**Q02B** To start we will mutliply the first equation by 5 and the second by 3 so we will get:

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

substracting equation (1) by equation (2) we will get the new equation:

$$\begin{aligned} [5][a][x] - [6][x] & \equiv [8] \\ [x]([5][a] - [6]) & \equiv [8] \end{aligned}$$

Note that we cancelled out the y's, this implies that number of possible solution set pairs is limited by the possible  $[x]$  solutions. Let  $[b] = [5][a] - [6]$ :

$$[b][x] \equiv [8]$$

MAT tells us a solution  $[x]$  will only exist if  $d = \gcd(b, 12)$  such that  $d|8$ . MAT also tells us that for a solution  $(x_0)$  the set of solutions is given by:

$$[x_0], [x_0 + \frac{m}{d}], [x_0 + 2\frac{m}{d}] \dots [x_0 + (d-1)\frac{m}{d}]$$

In other words this shows us that the number of possible solutions for  $[x]$  will be equal to  $d$ . Therefore all congruence classes that have 2 solutions will have  $d = 2$ , this can only happen in these cases:

$$\begin{cases} 2 \equiv \gcd(b, 12) \equiv \gcd(2, 12) \\ 2 \equiv \gcd(b, 12) \equiv \gcd(10, 12) \end{cases}$$

Thus we see that  $b$  has to equal either  $[2]$  or  $[10]$ , solving for  $[2]$  we find that:

$$\begin{aligned} [5][a] - [6] &\equiv [b] \\ [5][a] &\equiv [2] - [6] \\ [5][a] &\equiv [8] \end{aligned}$$

We know from the previous question that the mathematical inverse of  $[5]$  is  $[5]$  so if we multiply both sides by the inverse:

$$\begin{aligned} [5]^{-1}[5][a] &\equiv [8][5]^{-1} \\ [a] &\equiv [8][5] \\ [a] &\equiv [4] \end{aligned}$$

If we know solve for the second case, when  $b$  is  $[10]$  we get:

$$\begin{aligned} [5][a] - [6] &\equiv [b] \\ [5][a] &\equiv [10] - [6] \\ [5][a] &\equiv [4] \\ [5]^{-1}[5][a] &\equiv [4][5]^{-1} \\ [a] &\equiv [8][5] \\ [a] &\equiv [8] \end{aligned}$$

Thus we know there are only 2  $[x]$  solutions when  $[a]$  is  $[8]$  or  $[2]$ , we also know there are only going to be 2 solution pairs  $([x], [y])$  when  $[a]$  is  $[8]$  or  $[2]$

**Q02C** We know from the previous equations that the equation for a possible  $[x]$  value will be:

$$[x]([5][a] - [6]) \equiv [8]$$

We also know that we want to find an  $[a]$  such that  $[x]$  has 6 solutions. MAT says this can only happen if

$$d = \gcd([5][a] - [6], 12) = 6$$

This is impossible as MAT tells us that a solution can only happen when  $d | 8$  and since  $6 \nmid 8$ , we know that no  $[a]$  exists such that there are 6 solution pairs  $([x], [y])$ .