# IA Assignment 3

KDSMIL001 2IA MAM2000W

**7 September 2020**

1. (a) First of all, we use the basic division theorem:

$$\begin{aligned} 47 &= (1)27 + 20 \\ 27 &= (1)20 + 7 \\ 20 &= (2)7 + 6 \\ 7 &= (1)6 + 1 \end{aligned}$$

So we know that $\gcd(47, 27) = 1$, i.e. they are coprime, so there exists a number $b$ such that $1 = 27b + 47k$, for some integer k, which is the inverse of $27 \pmod{47}$, or more generally $[27]^{-1}$. We can find this $b$ using the extended division algorithm:

$$\begin{aligned} 1 &= 7 - 6 \\ &= 7 - (20 - (2)7) \\ &= (3)7 - 20 \\ &= (3)(27 - 20) - 20 \\ &= (3)27 - (4)20 \\ &= (3)27 - (4)(47 - 27) \\ &= (7)27 - (4)47 \end{aligned}$$

and so we have $27^{-1} = 7 \pmod{47}$.

(b) Given the congruence $[135][x] = [15] \pmod{235}$ we must first check if 135 and 235 are coprime. To do this we use the division algorithm:

$$\begin{aligned} 235 &= 135 + 100 \\ 135 &= 100 + 35 \\ 100 &= (2)35 + 30 \\ 35 &= 30 + 5 \\ 30 &= (6)5 \end{aligned}$$

So they are not coprime, but we can see that our congruence can be divided by 5, so we have

$$[27][x] = [3] \pmod{47}$$

To solve this we need the inverse of 27 (mod 47), but we already know this from (a), so we have

$$\begin{aligned}[x] &= [3][27]^{-1} \\ &= [3][7] \\ &= [3 \cdot 7] \\ &= [21]\end{aligned}$$

And we're done.

(c) As we saw above in (b), 135 and 235 are not coprime, but this time we have the congruence

$$[135][x] = [14] \pmod{235}$$

and $5 \nmid 14$, so there is no solution for $x$.