Q05A We know that the orginal expression can be expressed as:

$$[x]^{p_2} + [x] - [1] \equiv [0] \pmod{p_1 p_2}$$

We know that since p_1 and p_2 are distinct odd primes such that $\gcd(p1, p2) = 1$. This means we can apply SMT, so we get two equations the together will have the same solution as in the $\pmod{m}$ case:

$$\begin{cases} 1) \quad [x]^{p_2} + [x] - [1] \equiv [0] \pmod{p_1} \\ 2) \quad [x]^{p_2} + [x] - [1] \equiv [0] \pmod{p_2} \end{cases}$$

Before we continue we know that (p_1 -1) | (p_2 - 1) by the definition of divisibility this implies for some integer n:

$$\begin{aligned} n(p_1 - 1) &= p_2 - 1 \\ n(p_1 - 1) + 1 &= p_2 \end{aligned}$$

Taking the the first equation we can thus subsitute it in (Note the use of FLT):

$$\begin{aligned} [x]^{p_2} + [x] - [1] &\equiv [0] \pmod{p_1} \\ [x]^{n(p_1-1)+1} + [x] - [1] &\equiv [0] \pmod{p_1} \\ [x]^{n(p_1-1)}[x]^1 + [x] - [1] &\equiv [0] \pmod{p_1} \\ ([x]^{(p_1-1)})^n[x]^1 + [x] - [1] &\equiv [0] \pmod{p_1} \\ ([1])^n[x]^1 + [x] - [1] &\equiv [0] \pmod{p_1} \\ [x]^1 + [x] &\equiv [1] \pmod{p_1} \\ [2][x] &\equiv [1] \pmod{p_1} \end{aligned}$$

We know from Corollary 13 that $[2]^{-1}$ exists and is unique. We willl let this unique integer be [a] = $[2]^{-1} \pmod{p_1}$, our equation thus becomes:

$$\begin{aligned} [2][x] &\equiv [1] \pmod{p_1} \\ [2]^{-1}[2][x] &\equiv [1][2]^{-1} \pmod{p_1} \\ [x] &\equiv [a] \pmod{p_1} \end{aligned}$$

We thus will have an equation in the form of (where s is an integer):

$$[x] = [a] + [s] \cdot p_1$$

If we move on to the second equation now we can simplify (also used FLT):

$$\begin{aligned} [x]^{p_2} + [x] - [1] &\equiv [0] \pmod{p_2} \\ [x]^{p_2-1}[x]^1 + [x] - [1] &\equiv [0] \pmod{p_2} \\ [1][x]^1 + [x] - [1] &\equiv [0] \pmod{p_2} \\ [2][x] &\equiv [1] \pmod{p_2} \end{aligned}$$

We know from Corollary 13 that $[2]^{-1}$ exists and is unique. We willl let this unique integer be [b] $= [2]^{-1} \pmod{p_2}$, our equation thus becomes:

$$[2][x] \equiv [1] \pmod{p_2}$$
$$[2]^{-1}[2][x] \equiv [1][2]^{-1} \pmod{p_2}$$
$$[x] \equiv [b] \pmod{p_2}$$

We thus get an equation in the form of (where t is an integer):

$$[x] = [b] + [t] \cdot p_2$$

CRT tells us that since $\gcd(p_1, p_2) = 1$ we can apply it and find a solution in $\mathbb{Z}_m$ by replacing t with our value found for equation 1:

$$\begin{aligned}[x] \equiv& [b] + ([a] + [s] \cdot p_1) \cdot p_2 \pmod{m} \\ [x] \equiv& [b] + [a][p_2] + [s][p_1][p_2] \pmod{m} \\ [x] \equiv& [b] + [a][p_2] + [s][m] \pmod{m} \\ [x] \equiv& [b] + [a][p_2] \pmod{m}\end{aligned}$$

Since a and b and p_2 can only be one set value, CRT thus shows that a unqiue solution [x] exists within $\mathbb{Z}_m$.

Q05B We know a solution will satisfy that equation if it satisfies both:

$$\begin{cases} 1)[2][x] \equiv [1] \pmod{p_1} \\ 2)[2][x] \equiv [1] \pmod{p_2} \end{cases}$$

are satisfied. Thus consider $m = 39, p_1 = 3, p_2 = 13$ and our solution $x_0 = 20$. Notice that the solution is less then 39 and that:

$$\begin{cases} 1)[2][20] \equiv [40] \equiv [1] \pmod{3} \\ 2)[2][20] \equiv [40] \equiv [1] \pmod{13} \end{cases}$$

Since it satifies the conidtion we have given an example and shown that it therefore exists.