401 a)

+	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[0]	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[1]	[1]	[2]	[3]	[4]	[5]	[6]	[0]
[2]	[2]	[3]	[4]	[5]	[6]	[0]	[1]
[3]	[3]	[4]	[5]	[6]	[0]	[1]	[2]
[4]	[4]	[5]	[6]	[0]	[1]	[2]	[3]
[5]	[5]	[6]	[0]	[1]	[2]	[3]	[4]
[6]	[6]	[0]	[1]	[2]	[3]	[4]	[5]

X	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[2]	[0]	[2]	[4]	[6]	[1]	[3]	[5]
[3]	[0]	[3]	[6]	[2]	[5]	[1]	[4]
[4]	[0]	[4]	[1]	[5]	[2]	[6]	[3]
[5]	[0]	[5]	[3]	[1]	[6]	[3]	[1]
[6]	[0]	[6]	[5]	[4]	[3]	[1]	[1]

b) $\mathbb{Z}_7$ is a field because for $[7]^{-1}$ to exist, $[1][7]^{-1} = [1]$ and there is a $[1]$ in every non-zero row in the multiplication table of $\mathbb{Z}_7$ meaning every non-zero $[a]$ has a $[a]^{-1}$ it can multiply with to get $[1]$

Q02 a)

$$[7][x] + [3][y] = [1]$$
$$[2][x] + [5][y] = [-1]$$

$$[2][x] + [5][y] = [-1]$$
$$[6]([2][x] + [5][y]) = [-1][6]$$
$$[12][x] + [30][y] = [-6]$$
$$[0][x] + [6][y] = [6]$$
$$[6][y] = [6]$$

$$[2]([7][x] + [3][y]) = [1][2]$$
$$[14][x] + [6][y] = [2]$$
$$[2][x] + [6] = [2]$$
$$[2][x] = [-4]$$
$$[2][x] = [8]$$

$$[2][x] + [5][y] = [-1]$$
$$[8] + [5][y] = [-1]$$
$$[5][5][y] = [-9][5]$$
$$[25][y] = [-45]$$
$$[y] = [3]$$

$$[7][x] + [3][y] = [1]$$
$$[-5]([7][x] + [37][3]) = [1][-5]$$
$$[-35][x] + [-45] = [-5]$$
$$[x] + [3] = [7]$$
$$[x] = [4]$$

b)

$$[a][x] + [3][y] = [1]$$
$$[2][x] + [5][y] = [-1]$$

$$[2][x] + [5][y] = [-1]$$
$$[5][y] = [11] - [2][x]$$
$$[25][y] = [55] - [10][x]$$
$$[y] = [7] - [10][x]$$

$$[a][x] + [3][y] = [1]$$
$$[a][x] + [3]([7] - [10][x]) = [1]$$
$$[a][x] + [21] - [30][x] = [1]$$
$$[a][x] + [9] - [6][x] = [1]$$
$$([a] - [6])[x] = [-8]$$
$$([a] - [6])[x] = [4]$$

let $[b] = [a] - [6]$

By MAT, $[b][x] = [4]$ has a solution if $\gcd(b, 12) \mid 4$

$\therefore b = 1, 2, 4, 5, 7, 8, 10, 11$

let $d = \gcd(b, 12)$

Solutions are given by $[x_0], [x_0 + \frac{m}{d}], [x_0 + 2\frac{m}{d}] \ldots$
$[x_0 + (d-1)\frac{m}{d}]$

$\therefore$ for each value of b, there are d solutions

$\therefore$ There are 2 solutions for $b = 2, 10$ where $\gcd(b, 12) = 2$

$\therefore a = 4, 8$

As $[y]$ can be written as a function of $[x]$, there is only one value for $[y]$ for every value of $[x]$

$\therefore$ There are two solutions for $([x], [y])$ for $a = 4, 8$

c) By MAT, there are d solutions where $d = \gcd(b, 12)$ where $[b] = [a] - [6]$ if $d \mid 4$. $d = 6$ if and only if $b = 6$

But $6 \nmid 4$ $\therefore$ There is no value for a where there are 6 solutions

Q03 $9797 = 97 \times 101$ $\gcd(97, 101) = 1$

$$x^2 + 5149x + 2332 \equiv 0 \pmod{9797}$$

$$x^2 + 5149x + 2332 \equiv 0 \pmod{97}$$

$$x^2 + 5149x + 2332 \equiv 0 \pmod{101}$$

$$x^2 + 5149x + 2332 \equiv 0 \pmod{97}$$

$$x^2 + 9x + 4 \equiv 0 \pmod{97}$$

$$(x+2)^2 \equiv 0 \pmod{97} \Rightarrow 97 \mid (x+2)(x+2)$$

By Euclid's Lemma, since 97 is prime, $97 \mid (x+2)$

$$x \equiv -2 \pmod{97}$$

$$x \equiv 12123 \pmod{97}$$

$$x^2 + 5149x + 2332 \equiv 0 \pmod{101}$$

$$x^2 - 6x + 9 \equiv 0 \pmod{101}$$

$$(x-3)^2 \equiv 0 \pmod{101} \Rightarrow 101 \mid (x-3)(x-3)$$

By Euclid's Lemma, since 101 is prime, $101 \mid x-3$

$$x \equiv 3 \pmod{101}$$

$$x \equiv 12123 \pmod{101}$$

$$x \equiv 12123 \pmod{9797}$$

$$x \equiv 2326 \pmod{9797}$$

Q04 a) If $a^{2n-1} \not\equiv 1 \pmod{2^n}$, then a is even

$a^{2n-1} \not\equiv 1 \pmod{2^n}$ By repeated use of the splitting modulus theorem, $a^{2n-1} \not\equiv 1 \pmod{2} \Rightarrow 2 \nmid a^{2n-1} - 1$

∴ It follows that $a^{2n-1} - 1$ is odd and a^{2n-1} is even,

Since if a is odd, a^{2n-1} must also be odd, a must be even

b) By repeated use of the splitting modulus theorem

$a^{2^{n-1}(p-1)} \not\equiv 1 \pmod{2^n p} \Rightarrow a^{2^{n-1}(p-1)} \not\equiv 1 \pmod{2}$

or $a^{2^{n-1}(p-1)} \not\equiv 1 \pmod{p}$

In the previous part, we proved that if $a^{2n-1} \not\equiv 1 \pmod{2^n}$, then a is even

This means the contrapositive is also. Since a is odd,

$a^{2n-1} \equiv 1 \pmod{2^n}$

$(a^{2n-1})^{p-1} \equiv 1^{p-1} \pmod{2^n}$ ∴ $a^{(2n-1)(p-1)} \not\equiv 1 \pmod{p}$

$a^{(2n-1)(p-1)} \equiv 1 \pmod{2^n}$

By fermat's little theorem if a is not divisible by p

$a^{p-1} \equiv 1 \pmod{p}$

The contrapositive must also be true, if $a^{p-1} \not\equiv 1 \pmod{p}$

by which it follows that $a^{(2n-1)(p-1)} \not\equiv 1 \pmod{p}$ then a must be divisible by p.

Q05 a) $[x]^{p_2} + [x] - [1] = [0]$

$\downarrow$

$x^{p_2} + x - 1 \equiv 0 \pmod{m}$

By SmT

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

$x^{p_2} + x - 1 \equiv 0 \pmod{p_2}$ $\quad$ By Corollary 8.1.2

$x + x - 1 \equiv 0 \pmod{p_2}$

$2x \equiv 1 \pmod{p_2}$

Since $(p_1 - 1) \mid (p_2 - 1)$ there exists an integer n where

$p_2 - 1 = n(p_1 - 1)$

$p_2 = n(p_1 - 1) + 1$

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

$x^{n(p_1-1)+1} + x - 1 \equiv 0 \pmod{p_1}$

$(x)x^{n(p_1-1)} + x - 1 \equiv 0 \pmod{p_1}$

$x(x^{p_1-1})^n + x - 1 \equiv 0 \pmod{p_1}$

$x(1)^n + x - 1 \equiv 0 \pmod{p_1}$

$2x \equiv 1 \pmod{p_1}$

$p \nmid x$ proof:

Suppose $p \mid x$, then $x \equiv 0 \pmod{p}$

then $x^{p_2} \equiv 0 \pmod{p_1}$

$\therefore 0 + 0 - 1 \equiv 0 \pmod{p_1}$

$-1 \equiv 0 \pmod{p_1}$ which is a contradiction because $p \nmid -1 \therefore p_1 \nmid x$

$\therefore$ FLT applies

$\therefore$ By CRT, since p_1 and p_2 are primes, $\gcd(p_1, p_2) = 1$

since $2x \equiv 1 \pmod{p_1}$ and $2x \equiv 1 \pmod{p_2}$

$2x \equiv 1 \pmod{m}$ since p_1 and p_2 are odds m must also be odd $\therefore \gcd(2, m) = 1$ By LCT, the number of solutions $= \gcd(2, m) = 1$ $\therefore$ There is one unique solution to $[x]^{p_2} + [x] - [1] = [0]$ in $\mathbb{Z}_m$

b) $2x \equiv 1 \pmod{m}$ by CD since $\gcd(2, m) = 1$

$x \equiv \frac{m+1}{2} \pmod{m}$

$\therefore x_0 = \frac{m+1}{2}$