Name: Connor Raymond Stewart
Student Number: 101041125

MATH 3101 Assignment 3:

1) Find a Solution $x \in \mathbb{Z}$, $0 \leq x < 55$ of the Congruence $6x \equiv 14 \pmod{55}$ using the technique illustrated in the "Solving linear Congruences" video:

$6x \equiv 14 \pmod{55}$

obtain s and t:

$1 = 6s + 55t$

Use euclidean Algorithm:

$55 = (6)q_0 + r_1$

↳ $q_0 = 9, r_1 = 1$ from $55 = 6(9)+1$

$6 = (1)q_1 + r_2$

↳ $q_1 = 6, r_2 = 0$ from $6 = 1(6)+0$

remainder is zero, thus $(6,55) = 1$

Nonzero Remainders:

$1 = 55 - 6(9)$

Substituting for Remainders:

$1 = 55 - 6(9)$

multiply equation by b (14):

$14 = 55(14) - 6(9)(14)$

$14 = (-54)(14) + 55(14)$ (Sub 55 with mod 55)

↳ $14 \equiv 14(6)(-9) \pmod{55}$

$14 \equiv -756 \pmod{55}$

$\equiv -41 \pmod{55}$

$\equiv 14 \pmod{55}$

Since:

$14 \equiv 6(-126) \pmod{55}$

thus $x = -126$ is a Solution, however any number's Congruent modulo to its remainder when divided by 55, thus:

$-126 = (55)(-3) + 39$

thus $\boxed{x = 39}$ is also a Solution

↳ $0 \leq 39 < 55$ thus x is in the range of $[0,55)$

Hence, 39 is the Solution to $6x \equiv 14 \pmod{55}$ with $0 \leq 39 < 55$

2)

a) Solve the System of linear Congruencies;

$x \equiv 2 \pmod 5$
$x \equiv 3 \pmod 8$

Using the Chinese Remainder Theorm:

Since $(5,8)=1$, we use Theorm 2.27 to Solve the System of Congruencies:

$x \equiv 2 \pmod 5$
$x \equiv 3 \pmod 8$

from the first Congruence we write $2+5k$, $k \in \mathbb{Z}$ & Substitute this into the Second Congruence for x:

$x \equiv 3 \pmod 8$

$\Rightarrow 2+5k \equiv 3 \pmod 8$

thus:

$5k \equiv 1 \pmod 8$
$5k \equiv -7 \pmod 8$
$5k \equiv -15 \pmod 8$

$\Rightarrow$ As $(5,8)=1$, we divide by 5

$$\frac{5k}{5} \equiv -\frac{15}{5} \pmod 8$$

$k \equiv -3 \pmod 8$

$k \equiv 5 \pmod 8$

thus:

$x \equiv 2+5(5) = \boxed{27}$ Satisfies the System &

$x \equiv 27 \pmod{5 \cdot 8}$ or $\boxed{x \equiv 27 \pmod{40}}$

gives all Solutions to the System of Congruences.

$\boxed{\therefore \text{ the Solution is } x \equiv 27 \pmod{40}}$

b) Solve the following System of linear Congruences;

$x \equiv 2 \pmod 5$

$x \equiv 3 \pmod 8$

$x \equiv 1 \pmod 3$

Using the Generalized Chinese Remainder Theorm:

Question 2a Showed us that $x \equiv 27 \pmod{40}$ is a Solution to the first two Congruencies. Pairing this Congruence with the third $x \equiv 1 \pmod 3$ in the System gives:

$x \equiv 27 \pmod{40}$

$x \equiv 1 \pmod 3$

So. with $x = 27 + 40k$, $k \in \mathbb{Z}$ gives:

$27 + 40k \equiv 1 \pmod 3$

$40k \equiv -26 \pmod 3$

$k \equiv -26 \pmod 3$

↳ As $40k \equiv k \pmod 3$

$k \equiv -2 \pmod 3$

↳ As $-26 \equiv -2 \pmod 3$

$k \equiv 1 \pmod 3$

↳ So if $x = 27 + 40k$ then $x = 27 + 40(1) = 67$

thus:

$x \equiv 67 \pmod{3 \cdot 40} \Rightarrow x \equiv 67 \pmod{120}$

$\boxed{\therefore\ x \equiv 67 \pmod{120} \text{ Satisfies the original System}}$

3) Determine weather the following Statements are true or false. Justify your Responce:

a) let $a,b,c,n \in \mathbb{Z}$ $(n>1)$. If $a \equiv b \pmod{n}$, then $ca \equiv cb \pmod{n}$:

<u>As $a \equiv b \pmod{n}$, we know:</u>

$$a-b = Kn, \quad K \in \mathbb{Z} \quad \text{(theorm 2.22 of text)}$$

Also, Since $ca \equiv cb \pmod{n}$, we know:

$$ca - cb = Kn \quad \text{(theorm 2.22 of text)}$$

$$c(a-b) = Kn$$

from $a \equiv b \pmod{n}$, we know $(a-b) = Kn$ & $K \in \mathbb{Z}$,

we also know $c \in \mathbb{Z}$, thus:

Since $a-b$ is a multiple of n & K is any integer, then any multiple of $a-b$ is also a multiple of n

<u>let $K = cK_1$ where $K_1 \in \mathbb{Z}$:</u>

$$\cancel{c}(a-b) = K_1 \cancel{c} n$$

$$a-b = K_1 n, \quad K_1 \in \mathbb{Z}$$

thus, we can Simplify $ca \equiv cb \pmod{n}$ back to $a \equiv b \pmod{n}$

$\therefore$ True

b) let $a,b,c,n \in \mathbb{Z}$ $(n>1)$. If $ca \equiv cb \pmod{n}$, then $a \equiv b \pmod{n}$:

take the following example:

<u>let $a=3, b=1, c=2, n=4$; then:</u>

$$ca \equiv cb \pmod{n}$$

$$(2)(3) \equiv (2)(1) \pmod{4}$$

$$6 \equiv 2 \pmod{4}$$

$\Rightarrow$ this is true

<u>Now, lets try for $a \equiv b \pmod{n}$:</u>

$$a \equiv b \pmod{n}$$

$$3 \equiv 1 \pmod{4}$$

$\Rightarrow$ this is <u>False</u>

there is thus a Contradiction w/ the above Claim, as $a \not\equiv b \pmod{n}$ in general

$\therefore$ False

c) let $a,b,n,m \in \mathbb{Z}$. Then the system of congruencies;

$$x \equiv a \pmod{m}$$
$$x \equiv b \pmod{n}$$

has a solution in $\mathbb{Z}$:

let $m=n=7$ & let $a=3, b=2$;

$$x \equiv 3 \pmod{7}$$
$$x \equiv 2 \pmod{7}$$

So by the Chinese Remainder Theorm:

$x = 3 + 7K$

thus, $x \equiv 2 \pmod{7}$ So $3 + 7K \equiv 2 \pmod{7}$

$7K \equiv -1 \pmod{7}$

↳ $7K \equiv 0K \pmod{7}$

$\cancel{0K} \equiv -1 \pmod{7}$

$0 \equiv -1 \pmod{7}$

↳ However $0 \not\equiv -1 \pmod{7}$, it's $0 \equiv 0 \pmod{7}$

$\therefore$ False thus, there's a contradiction since $0 \not\equiv -1 \pmod{7}$, meaning the system of congruencies does NOT have a solution in $\mathbb{Z}$.

d) let $a,b \in \mathbb{Z}$, & let p be a prime. If $ab \equiv 0 \pmod{p}$, then $a \equiv 0 \pmod{p}$ or $b \equiv 0 \pmod{p}$:

For $ab \equiv 0 \pmod{p}$:

$ab - 0 = Kp,\ K \in \mathbb{Z}$ (theorm 2.22 of text)

① If ab is prime & $ab \equiv 0 \pmod{p}$:

then since p is prime; $p > 1, p \in \mathbb{Z}$, p is only divisable by 1 & itself.

$ab = Kp$ & $p > 1$ thus $ab \neq 1$

$1 = \frac{Kp}{ab}$ & p is only divisable by itself

$\therefore\ ab = p$ So $K = 1$.

If $ab = p$ then either a or b equals p, since p cannot be the composite of any numbers

↳ Since $p \equiv 0 \pmod{p}$, & a or b is p, then either a or $b \equiv 0 \pmod{p}$

$\therefore$ True

② If ab is NOT Prime & $ab \equiv 0 \pmod{p}$:

p is Prime, $p>1$, p is divisible only by p & 1

$ab = kp$, $p>1$ thus $ab \neq 1$

Since p is only divisible by itself, & the numbers not Prime $ab \neq p$; as p is Prime & ab is not:

thus, ab must be some multiple of p such that one variable is Prime p & the other's some multiple for p.

this is because p can only be evenly divided by itself, so if p divides another number evenly that number must be a multiple of p.

I) If $a=p$ & $b=c, c \in \mathbb{Z}$:

$ab=kp$

$pb=kp$

$b=k$

$c=k$

II) If $b=p$ & $a=c, c \in \mathbb{Z}$:

$ab=kp$

$ap=kp$

$a=k$

$c=k$

thus either a or b must be a factor of p & the other must be some integer

So, either a or $b \equiv 0 \pmod{p}$ for the same reason shown in ①.

$\therefore$ True

III) If a & b are not p, then one must be a multiple of p:

$ab = kp$, let $a = pk_1$

$k_1 bp = kp$

$k_1 b = k$

If there's no multiple of p, we see:

$ab = kp$, p is only divisible by multiples of itself since it is Prime, yet:

$1 = \frac{kp}{ab}$, but a & b are not multiples of p, this is a Contradiction thus:

If ab is Prime, the Claim is true

If ab is NOT Prime, the Claim is true

Since an integer must be either prime or Composite & both are true ;

The Claim is True

$\therefore$ True