Problem Sheet 8 : MTH3121 Saral 30 618 428

Question 4

a) So we are told that x is a solution to :

$$\begin{cases} x \equiv 1 \bmod 43 & \text{(Congruence 4.0)} \\ x \equiv 46 \bmod 47 & \text{(Congruence 4.1)} \end{cases}$$

We can think of moduli as a clock. With Congruence 4.1,
we have ticked on the ' 47 ' clock 46 times in some direction.

This gives the same result as if we were to have ticked on the ' 47 ' clock ' -
1 ' times (just ticking once in the opposite direction). Thus :

$x \equiv -1 \bmod 47$ (Congruence 4.2)

For the next of this part its helpful to think the other characterisation of a modular expression :

"For some integers a,b and c, $a \cong b \bmod c$, is the same as
saying, $a - b = ck$, where k is some integer" (Characterisation 4.3)

Thus we can write from Congruence 4.0 and Congruence 4.1 that :

$x - 1 = 43m$, for some integer m (Equation 4.4)

$x + 1 = 47n$, for some integer n (Equation 4.5)

Now mulitplying Equation 4.4 and Equation 4.5 together gives :

$(x - 1)(x + 1) = 2021\,mn$ (Equation 4.6)

Now expanding the brackets on the left side of Equation 4.6 gives :

$x^2 - 1 = 2021\,mn$ (Equation 4.7)

We can let $k = mn$, to rewrite Equation 4.7 as :

$x^2 - 1 = 2021\,k$ (Equation 4.8)

So we have found that x^2 subtract one is divisible by 2021.

Thus using Characterisation 4.3 we know that Equation 4.8 is saying that :

$x^2 \cong 1 \bmod 2021$ (Congruence 4.9)

b) First let ' s write the ' basic fact ' shown in lectures :

' If $c \mid n$ and $x \cong b \bmod n$ then $x \cong b \bmod c$ ' (Basic Fact)

Using the Basic Fact and TRC we can split Congruence 4.9 into :

$x^2 \equiv 1 \bmod 43$ (Congruence 4.10)

$x^2 \equiv 1 \bmod 47$ (Congruence 4.11)

So now the question is what are these congruences telling us ?

To answer this lets focus just on Congruence 4.10 and then generalise our conclusions to Congruence 4.11.

Firsly let ' s make a helpful definition for congruences :

"a ≅ b mod c, can be thought of as 'Ticking from '0' 'a' times gives position b on the 'c' clock'". (Definition 4.12)

Congruence 4.10 is telling us that :

"For some number x, If I tick x^2 times from '0' on the '43' clock I arrive at a 1"

Now how can this be possible ?

If x = 1, then if we tick x^2 = 1 times from ' 0 ' we would arrive at a 1. Hence :

Thus x ≡ 1 mod 43

To find another value we will first observe the following characteristic of integers :

"x^2 is the same as adding x to itself x times" (Rule 4.13)

Now why is this important ?

If x = 42 then ticking x^2 = 42^2 times from ' 0 ', would be the same as doing 42 ticks, 42 times :

So the first time we tick 42 times, we arrive at 42.

Second time, we start from 42, so doing 42 ticks puts us at 41.

Third time, we start from 41, so doing 42 ticks puts as at 40, and so on.

So what we find is that at each successive iteration of our ' 42 ' ticks we go back position on the ' 43 ' clock :

position 42 α 1 iteration

position 41 α 2 iterations

position 40 α 3 iterations

position 39 α 4 iterations

... .

position 30 α 13 iterations

....

position 20 α 23 iterations

... ...

position 10 α 33 iterations

... ..

position 3 α 40 iterations

position 2 α 41 iterations

position 1 α 42 iterations.

Thus after going around our clock $x^2 = 42^2$,
times we arrive at position 1. This means that $x^2 \equiv 1 \bmod 43$ and since we had $x = 42$:

$x \equiv 42 \bmod 43$ (Congruence 4.14)

Using this same logic we know Congruence 4.10 and Congruence 4.11 can be broken up into :

$x \equiv 1 \bmod 43$ (Congruence 4.15)

$x \equiv 42 \bmod 43$ (Congruence 4.16)

$x \equiv 1 \bmod 47$ (Congruence 4.17)

$x \equiv 46 \bmod 47$ (Congruence 4.18)

(just thought I would restate Congruence 4.15 and Congruence 4.18 incase they were forgotten by now, I defined them earlier)

From the four congruences above we can construct four systems of possible solutions :

$$\begin{cases} x \equiv 1 \bmod 43 & \text{(System 1)} \\ x \equiv 1 \bmod 47 & \square \end{cases}$$

$$\begin{cases} x \equiv 1 \bmod 43 & \text{(System 2)} \\ x \equiv 46 \bmod 47 & \square \end{cases}$$

$$\begin{cases} x \equiv 42 \bmod 43 & \text{(System 3)} \\ x \equiv 1 \bmod 47 & \square \end{cases}$$

$$\begin{cases} x \equiv 42 \bmod 43 & \text{(System 4)} \\ x \equiv 46 \bmod 47 & \square \end{cases}$$

And since the greatest common divisor of each of the pairs of moduli in each system is 1,
each system as a unique solutions.

Thus there are at least four solutions to the congruence :

$x^2 \equiv 1 \bmod 2021$

Question 8

If n, n + 1 and n + 2 are all Normian numbers then for some s, t, u bigger than 1 :

$$\begin{cases} n \equiv 0 & \bmod s^2 \\ n \equiv -1 & \bmod t^2 \quad \text{(System 8.0)} \\ n \equiv -2 & \bmod u^2 \end{cases}$$

By the CRT for System 8.0 to have solutions s^2, t^2 and u^2 must all be coprime.

If they are coprime then this means that there is a unique solution to System 8.0 mod $s^2 t^2 u^2$.

We can choose s, t and u such that the product $s^2 t^2 u^2$ is
less than 1000 to ensure that the solution, n, is less than 1000.

Additionally we can choose s, p and t such that there are at least 6 solutions to System 8.0.

Question 9

a) $\begin{cases} 2x \equiv 5 & \text{mod } 27 \\ x \equiv 73 & \text{mod } 84 \\ 4x \equiv 61 & \text{mod } 63 \end{cases}$ (System 9.0)

To solve this system of congruences we will start
by breaking down each individual congruence, starting with :

$2x \equiv 5 \bmod 27$ (Congruence 9.1)

Since gcd $(2, 27) = 1$, we know that an inverse for 2 exists in the world of 27.

We know that the inverse of 2 has to satisfy :

$2 * 2^{-1} \equiv 1 \bmod 27$

And since $2 * 14 \cong 1 \bmod 27$, the inverse of 2 is 14.

So we can rewrite Congruence 9.1 as :

$x \equiv 5 * 14 \bmod 27$

Which evaluates to :

$x \equiv 16 \bmod 27$ (Congruence 9.2)

Now we will break down the congruence :

$x \equiv 73 \bmod 84$ (Congruence 9.3)

Since $84 = 4 \times 21$, we can rewrite congruence 9.3 as :

$x \equiv 73 \bmod 21$ (Congruence 9.4)

$x \equiv 73 \bmod 4$ (Congruence 9.5)

Which evaluate to :

$x \equiv 10 \bmod 21$ (Congruence 9.6)

$x \equiv 1 \bmod 4$ (Congruence 9.7)

We can further break down Congruence 9.6 using the fact that $21 = 7 \times 3$, into :

$x \equiv 1 \bmod 3$ (Congruence 9.8)

$x \equiv 3 \bmod 7$ (Congruence 9.9)

Now we break down the final congruence in system 9.0 :

$4x \equiv 61 \bmod 63$ (Congruence 9.10)

Since gcd $(4, 63) = 1$, we know that an inverse of 4 exists in the world of 63.

The inverse of 4 satisfies :

$4 * 4^{-1} \equiv 1 \bmod 63$

And since $4 * 16 = 64 \equiv 1 \bmod 63$, $4^{-1} = 16$.

So we can rewrite Congruence 9.10 as :

$x \equiv 61 * 16 \bmod 63$ (Congruence 9.11)

Which evaluates to :

$x \equiv 31 \bmod 63$ (Congruence 9.12)

Since $63 = 9 \times 7$, we can break down Congruence 9.12 into :

$x \equiv 31 \bmod 7$ (Congruence 9.13)

$x \equiv 31 \bmod 9$ (Congruence 9.14)

Which evaluate to :

$x \equiv 3 \bmod 7$ (Congruence 9.15)

$x \equiv 4 \bmod 9$ (Congruence 9.16)

So at this point we have broken down all the congruences in System 9.0.

Collecting them together we get the congruences :

$x \equiv 16 \bmod 27$ (Congruence 9.2)

$x \equiv 1 \bmod 4$ (Congruence 9.7)

$x \equiv 1 \bmod 3$ (Congruence 9.8)

$x \equiv 3 \bmod 7$ (Congruence 9.9)

$x \equiv 4 \bmod 9$ (Congruence 9.16)

Now taking a closer look at Congruence 9.2 and Congruence 9.16,
and rewriting them using Characterisation 4.3 :

$x - 16 = 27k$, for some integer k (Equation 9.17)

$x - 4 = 9z$, for some integer z (Equation 9.18)

Subtracting Equation 9.17 from Equation 9.18 gives the result :

$12 = 9z - 27k$ (Equation 9.20)

And since $\gcd(9, 27) = 9$, does not divide 12, Equation 9.20 has no solutions which means that Congruence 9.2 and Congruence 9.16 are inconsistent.

Therefore System 9.0 has no solutions.

b) $$\begin{cases} 3x \equiv 75 \bmod 108 \\ 2x \equiv 38 \bmod 84 \\ 4x \equiv 52 \bmod 80 \end{cases} \quad \text{(System 9.21)}$$

To solve the System 9.21 of congruences we will break down each individual congruence starting with :
$3x \equiv 75 \bmod 108$ (Congruence 9.22)

Since gcd $(3, 108) = 3$, and 3 divides 75 we can divide the congruence throughout by 3 :

$x \equiv 25 \bmod 36$ (Congruence 9.23)

And since $36 = 9 \times 4$, we can further break down Congruence 9.23 into :

$x \equiv 25 \bmod 9$ (Congruence 9.24)

$x \equiv 25 \bmod 4$ (Congruence 9.25)

Which evaluate to :

$x \equiv 7 \bmod 9$ (Congruence 9.26)

$x \equiv 1 \bmod 4$ (Congruence 9.27)

Now we will break down the congruence :

$2x \equiv 38 \bmod 84$ (Congruence 9.28)

Since gcd $(2, 84) = 2$, and 2 divised 38 we can divide Congruence 9.28 throughout by 2 :

$x \equiv 19 \bmod 42$ (Congruence 9.29)

And since $42 = 6 \times 7$, we can further break down Congruence 9.29 into :

$x \equiv 19 \bmod 6$ (Congruence 9.30)

$x \equiv 19 \bmod 7$ (Congruence 9.31)

Which evaluate to :

$x \equiv 1 \bmod 6$ (Congruence 9.32)

$x \equiv 5 \bmod 7$ (Congruence 9.33)

Again since $6 = 2 \times 3$, we can break down Congruence 9.32 into :

$x \equiv 1 \bmod 2$ (Congruence 9.34)

$x \equiv 1 \bmod 3$ (Congruence 9.35)

Now we break down the final congruence in System 9.21 :

$4x \equiv 52 \bmod 80$ (Congruence 9.36)

Since gcd $(4, 80) = 4$, and 4 divides 52 we can divide Congruence 9.36 throughout by 4 to give :

$x \equiv 13 \bmod 20$ (Congruence 9.37)

Since $20 = 4 \times 5$, we can break down Congruence 9.37 into :

$x \equiv 13 \bmod 4$ (Congruence 9.38)

$x \equiv 13 \bmod 5$ (Congruence 9.39)

Which evaluate to :

$x \equiv 1 \bmod 4$ (Congruence 9.40)

$x \equiv 3 \bmod 5$ (Congruence 9.41)

So at this point we have split all the moduli in the congruences of System 9.21 into their prime power factors.

Now gathering all the resulting congruences :

$x \equiv 7 \bmod 9$ (Congruence 9.26)

$x \equiv 1 \bmod 4$ (Congruence 9.27)

$x \equiv 5 \bmod 7$ (Congruence 9.33)

$x \equiv 1 \bmod 2$ (Congruence 9.34)

$x \equiv 1 \bmod 3$ (Congruence 9.35)

$x \equiv 3 \bmod 5$ (Congruence 9.41)

From the congruences we have gathered we have to find which ones are redundant. So we will have to look at the congruences where one of the moduli is a power of another.

So first we will look at Congruence 9.26 and Congruence 9.35.

Using Characterisation 4.3 we can rewrite Congruence 9.26 and Congruence 9.35 as :

$x - 7 = 9k$, for some integer k (Equation 9.42)

$x - 1 = 3z$, for some integer z (Equation 9.43)

Subtracting Equation 9.42 from Equation 9.43 gives the result :

$6 = 3z - 9k$ (Equation 9.44)

And since $\gcd(3, 9) = 3$, divides 6, Equation 9.44 has a solution. This means that Congruence 9.26 and Congruence 9.35 provide the same information.

But since Congruence 9.26 has a greater modulus (9) we will discard Congruence 9.35.

Now we will look at Congruence 9.27 and Congruence 9.34.

Congruence 9.34 implies that x is even and if x is even then Congruence 9.27 will also hold.

Since Congruence 9.27 has a higher modulus (4) we will discard Congruence 9.34.

This gives the resulting set of congruences :

$x \equiv 7 \bmod 9$ (Congruence 9.26)

$x \equiv 1 \bmod 4$ (Congruence 9.27)

$x \equiv 5 \bmod 7$ (Congruence 9.33)

$x \equiv 3 \bmod 5$ (Congruence 9.41)

And to solve this set of congruences, since all the moduli are coprime we can use the CRT.

I ' m going to put all the relevant information for this in a table :

.	n_n	b_n	N_n	x_n
1	9	7	140	2
2	4	1	315	3
3	7	5	180	3
4	5	3	252	3

(Table 9.45)

Thus our solutions x can be obtained by computing :

$$x \equiv \sum_{n=1}^{4} x_n N_n b_n \bmod N = (2)(140)(7) + (3)(315)(1) + (3)(180)(5) + (3)(252)(3) \bmod (9 \times 4 \times 7 \times 5) \quad \text{(Equation 9.46)}$$

Which gives the final result :

$x \equiv 313 \bmod 1260$

Question 12

$m = 15^3 \times 67^2 \times 89$ (Equation 12.0)

$n = 41 \times 51 \times 53 \times 23^3$ (Equation 12.1)

To find what $m - n \bmod 9$ is we need the following two properties of mods,
for some integers a, b and c :

$a \pm b \bmod c = (a \bmod c \pm b \bmod c) \bmod c$ (Property 12.2)

$a \times b \bmod c = (a \bmod c \times b \bmod c) \bmod c$ (Property 12.3)

To see that these properties are true, if we were to write :

$a = kc + r_1$, where k is some integer and r_1 is the remainder of dividing a by c.

$b = dc + r_2$, where d is some integer and r_2 is the remainder of dividing b by c.

Then the properties above naturally appear.

So now using these properties we can calculate $m - n \bmod 9$:

$(m - n) \bmod 9$

$(m \bmod 9 - n \bmod 9) \bmod 9$ (By Property 12.2)

$(15^3 \times 67^2 \times 89 \bmod 9 - 41 \times 51 \times 53 \times 23^3 \bmod 9)$ (Substituting m and n)

$((15 \times 15 \times 15 \times 67 \times 67 \times 89) \bmod 9 - (41 \times 51 \times 53 \times 23 \times 23 \times 23) \bmod 9)$
(Making the exponents all 1)

$((9 \times 25 \times 15 \times 4 \times 4 \times 8) \bmod 9 - (5 \times 6 \times 8 \times 5 \times 5 \times 5) \bmod 9))$ (Using Property 12.3)

$(0 - (5 \times 6 \times 8 \times 8) \bmod 9)$ (Since $125 \bmod 9 = 8$)

$(0 - (30 \times 64) \bmod 9)$

$(0 - (3 \times 1)) \bmod 9$

-3

Since -3 is the same as 6 in the world of 9 :

$m - n \equiv 6 \bmod 9$ (Congruence 12.4)

Using this same process we can compute $m - n \bmod 10$ and $m - n \bmod 11$ to be :

$m - n \equiv 4 \bmod 10$ (Congruence 12.5)

$m - n \equiv 0 \bmod 11$ (Congruence 12.6)

So now we can create a system of congruences for $m - n$:

$$\begin{cases} m - n \equiv 6 \bmod 9 \\ m - n \equiv 4 \bmod 10 \\ m - n \equiv 0 \bmod 11 \end{cases} \quad \text{(System 12.7)}$$

And since all the moduli in System 12.7 are coprime, it has a unique solution modulo $9 \times 10 \times 11$.

I won't show all the calculations here
(I did them on paper don't worry) but eventually you get to this step :

$$m - n \equiv \sum_{n=1}^{3} x_n b_n N_n \bmod 990 \quad \text{(Congruence 12.8)}$$

$$\sum_{n=1}^{3} x_n b_n N_n = (9)(4)(99) + (5)(6)(110) + 0 = 9 \quad \text{(Equation 12.9)}$$

And substituting Equation 12.9 into Congruence 12.8 gives the result :

$m - n \equiv 924 \bmod 990$ (Congruence 12.10)

Now the calculator is supposed to be correct to eight digits.

The calculator displayed m and n as both being 1 348 383 400.

This means that only the last two digits of m and n differ.

So their difference must be less that 100.

Thus our final answer is $924 - 990 = -66$.

$m - n = -66$

Question 16

So we are asked to prove that an integer, n, exists such that :

a) n has exactly 1000 decimal digits.

b) The last 400 digits of n are all 7's.

c) $2021 \mid n$ and

d) 3121 does not divide n.

Starting with b), lets first make the following observations :

17 ends with a 7 and $17 \equiv 7 \bmod 10$

177 ends with two 7 ' s and $177 \equiv 77 \bmod 10^2$

1777 ends with three 7 ' s and $1777 \equiv 777 \bmod 10^3$

17 777 ends with four sevens and $17\,777 \equiv 7777 \bmod 10^4$

So if the last 400 digits of n are all 7 ' s then this means that :

$n \equiv$ 400 sevens $\bmod 10^{400}$ (Congruence 16.0)

For c) we are told that 2021 divides n therefore :

$n \equiv 0 \bmod 2021$ (Congruence 16.1)

the property d) implies that for some $0 < k < 3121$:

$n \equiv k \bmod 3121$ (Congruence 16.2)

Now lets make another observation :

12 has two digits and $12 \equiv 2 \bmod 10$

122 has three digits and $122 \equiv 22 \bmod 10^2$

1222 has four digits and $1222 \equiv 222 \bmod 10^3$

So if n has exactly 1000 decimal digits then this means that :

$n \equiv$ (last 999 digits of n) $\bmod 10^{999}$ (Congruence 16.3)

So have now have the following set of congruences involving n :

$n \equiv$ 400 sevens $\bmod 10^{400}$ (Congruence 16.0)

$n \equiv 0 \bmod 2021$ (Congruence 16.1)

$n \equiv k \bmod 3121$, where $0 < k < 3121$ (Congruence 16.2)

$n \equiv$ (last 999 digits of n) $\bmod 10^{999}$ (Congruence 16.3)

Now looking at Congruence 16.3 and Congruence 16.0,
we can simply choose some n where in the last 999 digits of n it ends with 400 sevens.

So Congruence 16.3 and 16.0 are saying similar
things and they can be combined into one congruence :

$n \equiv$ (last 999 digits of n where the last 400 digits are all sevens) $\bmod 10^{999}$ (Congruence 16.4)

This gives us the following system :

$$\begin{cases} n \equiv \text{(last 999 digits of n where the last 400 digits are all sevens)} & \bmod 10^{999} \\ n \equiv 0 & \bmod 2021 \\ n \equiv k & \bmod 3121, \text{ where } 0 < k < 3121 \end{cases}$$

(System 16.5)

And since the moduli of System 16.5 are all coprime,
System 16.5 has a unique solutions modulo $10^{999} \times 2021 \times 3121$.

Thus there exists an integer n that has the properties of a) , b) , c) and d) .