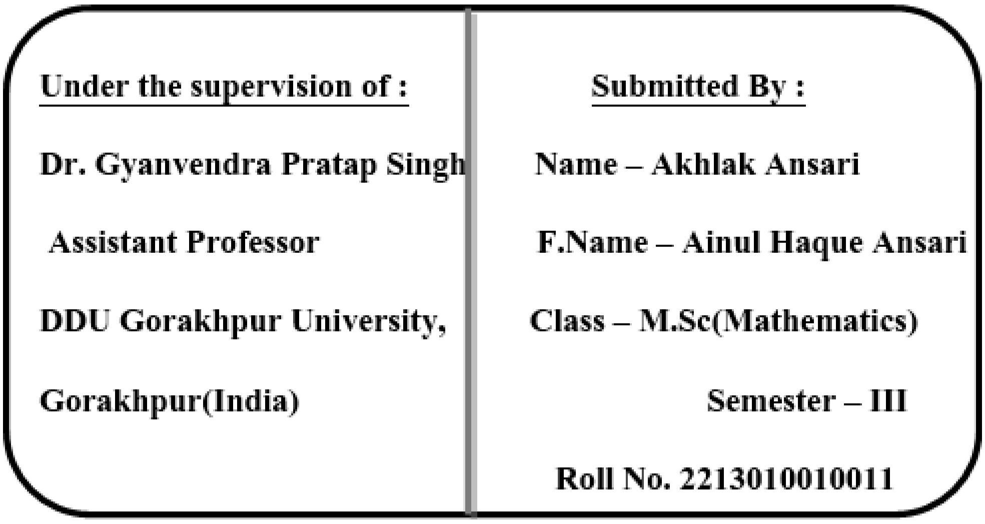
ASSIGNMENT: NUMBER THEORY

Akhlak Ansari

December 8, 2022

Department of Mathematics and Statistics



Under the supervision of :	Submitted By :
Dr. Gyanvendra Pratap Singh	Name – Akhlak Ansari
Assistant Professor	F.Name – Ainul Haque Ansari
DDU Gorakhpur University,	Class – M.Sc(Mathematics)
Gorakhpur(India)	Semester – III
	Roll No. 2213010010011

Fall ′ 2022 − 23

Assignment Questions:

1. Determine all positive solutions of the following Diophantine equations

   (a) $123x + 360y = 99$

   (b) $158x - 57y = 7$

2. If a and b are integers, not both of which are zero, prove that

$$\gcd(a, b) = \gcd(-a, b) = \gcd(a, -b) = \gcd(-a, -b).$$

3. Explain Hill Cipher Method in Cryptography. Also encrypt and decrypt the message "We live in an insecure world" by Hill Cipher Method with key $K = \begin{bmatrix} 27 & 1 \\ 3 & 2 \end{bmatrix}$.

4. Define complete and reduced residue system with examples. Also verify that the set

   $S = \{-19, -1, 22, 43, 46, 79, 113, 452\}$ is a reduced residue system.

5. If $n \geq 1$ and a is a integer such that $\gcd(a, n) = 1$ then prove that

$$a^{\phi(n)} \equiv 1 (\text{mod } n)$$

   where $\phi(n)$ denotes the Euler's function.

Solutions

Solution of Question No 1(a).

Given linear diophantine equation is,

$$123x + 360y = 99 \tag{1}$$

Let's find out the, $\gcd(\text{Coefficient of } x, \text{Coefficient of } y)$. i.e.

$$\begin{aligned} &\gcd(123, 360)\\ 360 &= 123 \times 2 + 114\\ 123 &= 114 \times 1 + 9\\ 114 &= 9 \times 12 + 6\\ 9 &= 6 \times 1 + 3\\ 6 &= 3 \times 2 + 0\\ \text{Hence, } \gcd(123, 360) &= 3 \end{aligned}$$

Since, $\gcd(123, 360) = 3|99$, so our diophantine equation is solvable for integers.

Now, just write down the equation for the **remainders**,

$$\begin{aligned} 114 &= 360(1) + 123(-2)\\ 9 &= 123(1) + 114(-1)\\ 6 &= 114(1) + 9(-12)\\ 3 &= 9(1) + 6(-1) \end{aligned}$$

Now let us consider the last remainder,

$$3 = 9(1) + 6(-1)$$

Now using the backward substitutions for the remainders, the above equation transformed as,

$$\begin{aligned} 3 &= 9(1) + [114(1) + 9(-12)](-1)\\ &= 9(1) + 114(-1) + 9(12)\\ &= 9(13) + 114(-1)\\ &= [123(1) + 114(-1)](13) + 114(-1) \end{aligned}$$

$$\begin{aligned}
3 &= 123(13) + 114(-13) + 114(-1) \\
&= 123(13) + 114(-14) \\
&= 123(13) + [360(1) + 123(-2)](-14) \\
&= 123(13) + 360(-14) + 123(28) \\
3 &= 123(41) + 360(-14)
\end{aligned}$$

Now, Multiply with 33 to the above equation, we have

$$99 = 123(1353) + 360(-462) \tag{2}$$

This is the linear combination of 123 and 360 of the given problem.

Now, comparing equation(2) with equation(1) we get as,

$$\boxed{x = 1353 \text{ and } y = -462.}$$

This is called the particular solution of the given diophantine equation.

- General Solution:

For general solution, we have the expression,

$$x_{gen.} = x + \left\{ \frac{b}{\gcd(a,b)} \right\} \cdot t$$

$$y_{gen.} = y - \left\{ \frac{a}{\gcd(a,b)} \right\} \cdot t$$

where $\forall\ t \in \mathbb{Z}$.

Thus our general solution is given by,

$$\boxed{x_{gen.} = 1353 + \left\{\tfrac{360}{3}\right\} t = 1353 + 120t}$$

$$\boxed{y_{gen.} = -462 - \left\{\tfrac{123}{3}\right\} t = -462 - 41t}$$

where $\forall\ t \in \mathbb{Z}$.

- For positive solutions,

we must have these conditions,

$$x_{gen.} > 0 \text{ and } y_{gen} > 0.$$

Thus,

$$\begin{aligned}1353 + 120t &> 0\\ t &> -\frac{1353}{120}\\ t &> -11.275\end{aligned}$$

and,

$$\begin{aligned}-462 - 41t &> 0\\ t &< \frac{-462}{41}\\ t &< -11.268\end{aligned}$$

It concludes that $-11.275 < t < -11.268$.But t is an integer and there is no such integer in this interval.

Hence, the positive solution of given linear diophantine equation doesn't exists.

Solution of Question No 1(b).

Given linear diophantine equation is,

$$158x - 57y = 7 \tag{1}$$

Let's find out the, gcd(Coefficient of x, Coefficient of y). i.e.

$$\begin{aligned}&\gcd(158, -57)\\ 158 &= -57 \times (-2) + 44\\ -57 &= 44 \times (-2) + 31\\ 44 &= 31 \times 1 + 13\\ 31 &= 13 \times 2 + 5\\ 13 &= 5 \times 2 + 3\\ 5 &= 3 \times 1 + 2\\ 3 &= 2 \times 1 + 1\\ 2 &= 1 \times 2 + 0\end{aligned}$$

Hence, $\gcd(158, -57) = 1$

Since, $\gcd(158, -57) = 1|7$, so our diophantine equation is solvable for integers.

Now, just write down the equation for the **remainders**,

$$\begin{aligned}
44 &= 158(1) + 57(-2)\\
31 &= 57(-1) + 44(2)\\
13 &= 44(1) + 31(-1)\\
5 &= 31(1) + 13(-2)\\
3 &= 13(1) + 5(-2)\\
2 &= 5(1) + 3(-1)\\
1 &= 3(1) + 2(-1)
\end{aligned}$$

Now let us consider the last remainder,

$$1 = 3(1) + 2(-1)$$

Now using the backward substitutions for the remainders, the above equation transformed as,

$$\begin{aligned}
1 &= 3(1) + [5(1) + 3(-1)](-1)\\
&= 3(1) + 5(-1) + 3(1)\\
&= 3(2) + 5(-1)\\
&= [13(1) + 5(-2)](2) + 5(-1)\\
&= 13(2) + 5(-4) + 5(-1)\\
&= 13(2) + 5(-5)\\
&= 13(2) + [31(1) + 13(-2)](-5)\\
&= 13(2) + 31(-5) + 13(10)\\
&= 13(12) + 31(-5)\\
&= [44(1) + 31(-1)](12) + 31(-5)\\
&= 44(12) + 31(-12) + 31(-5)\\
&= 44(12) + 31(-17)\\
&= 44(12) + [57(-1) + 44(2)](-17)\\
&= 44(12) + 57(17) + 44(-34)
\end{aligned}$$

$$
\begin{aligned}
1 &= 44(-22) + 57(17) \\
&= [158(1) + 57(-2)](-22) + 57(17) \\
&= 158(-22) + 57(44) + 57(17) \\
1 &= 158(-22) + 57(61)
\end{aligned}
$$

Now, Multiply with 7 to the above equation, we have

$$7 = 158(-154) - 57(-427) \tag{2}$$

This is the linear combination of 158 and -57 of the given problem.

Now, comparing equation(2) with equation(1) we get as,

$$\boxed{x = -154 \text{ and } y = -427.}$$

This is called the particular solution of the given diophantine equation.

- General Solution:

For general solution, we have the expression,

$$
\begin{aligned}
x_{gen.} &= x + \left\{ \frac{b}{\gcd(a,b)} \right\} \cdot t \\
y_{gen.} &= y - \left\{ \frac{a}{\gcd(a,b)} \right\} \cdot t
\end{aligned}
$$

where $\forall\ t \in \mathbb{Z}$.

Thus our general solution is given by,

$$\boxed{x_{gen.} = -154 + \left\{\tfrac{-57}{1}\right\} t = -154 - 57t}$$

$$\boxed{y_{gen.} = -427 - \left\{\tfrac{158}{1}\right\} t = -427 - 158t}$$

where $\forall\ t \in \mathbb{Z}$.

- For positive solutions,

we must have these conditions,

$$x_{gen.} > 0 \text{ and } y_{gen} > 0.$$

Thus,

$$
\begin{aligned}
-154 - 57t &> 0 \\
t &< -\frac{154}{57} \\
t &< -2.70
\end{aligned}
$$

and,

$$
\begin{aligned}
-427 - 158t &> 0 \\
t &< \frac{-427}{158} \\
t &< -2.70
\end{aligned}
$$

It concludes that $t < -2.70$.i.e the integers in the interval $-\infty < t \leq -3$ are all the **positive solutions of the given linear diophantine equation.**

Solution of Question No 2.

Let us consider $a, b \in \mathbb{Z}$ not both zero at a time.

$$\text{Let } \gcd(a,b) = d \tag{1}$$

$$\implies d|a, d|b \text{ ; If } c|a, c|b \text{ then } c|d \ \forall \ c \in \mathbb{Z}$$

$$\text{Since, } d|a, d|b \iff d|-a, d|b.$$

$$\text{therefore } d|-a, d|b \text{ and if, } c|-a, \ c|b \text{ then } c|d$$

$$\implies \gcd(-a,b) = d \tag{2}$$

Again,

$$\text{Since, } d|a, d|b \iff d|a, d|-b.$$

$$\text{therefore } d|a, d|-b \text{ and if, } c|a, \ c|-b \text{ then } c|d$$

$$\implies \gcd(a,-b) = d \tag{3}$$

Next,

$$\text{Since, } d|a, d|b \iff d|-a, d|-b.$$

$$\text{therefore } d|-a, d|-b \text{ and if, } c|-a, \ c|-b \text{ then } c|d$$

$$\implies \gcd(-a,-b) = d \tag{4}$$

From equations (1), (2), (3) and (4) we have,

$$\boxed{\gcd(a,b) = \gcd(-a,b) = \gcd(a,-b) = \gcd(-a,-b)}$$

Hence, we have the result.

This shows that gcd of any number wheather it is positive or negative , in all the cases are likely to be the same value.

Solution of Question No 3.

Hill cipher:

Hill Cipher, in the pretext of classical cryptography, follows a polygraphic substitution cipher, which means there is uniform substitution across multiple levels of blocks. This polygraphic substitution cipher makes it possible for Hill Cipher to work seamlessly with digraphs (two-letter blocks), trigraphs (three-letter blocks), or any multiple-sized blocks for the purpose of building a uniform cipher.

Hill Cipher is based on linear algebra, the sophisticated use of matrices in general (matrix multiplication and matrix inverses), as well as rules for modulo arithmetic. Evidently, it is a more mathematical cipher compared to others.

The Hill Cipher is also a block cipher. A block cipher is an encryption method that implements a deterministic algorithm with a symmetric key to encrypt a block of text. It doesn't need to encrypt one bit at a time like in stream ciphers. Hill Cipher being a block cipher theoretically, means that it can work on arbitrary-sized blocks.

While Hill Cipher is digraphic in nature, it is capable of expanding to multiply any size of letters to add more complexity and reliability for better use. Since most of the problems and solutions for Hill Ciphers are mathematical in nature, it becomes easy to conceal letters with precision.

We will cover both Hill Cipher encryption and decryption procedures solving 2×2 matrices. However, it is possible to use Hill Cipher for higher matrices $(3 \times 3, 4 \times 4, 5 \times 5,$ or $6 \times 6)$ with a higher and advanced level of mathematics and complexity. Here, we will demonstrate simple examples that will provide more understanding of the Hill Cipher.

In Hill cipher, key K must be a square matrix and non-singular. and $gcd(|K|, 26) = 1$ i.e co-prime or relatively-prime.

Hill cipher Algorithm:

$$\text{Encryption: } C \equiv (K \cdot P)(\text{mod } 26)$$

$$\text{Decryption: } P \equiv (K^{-1} \cdot C)(\text{mod } 26)$$

Now,

- Let's Encrypt and Decrypt the message `We live in an insecure world` with key $\begin{bmatrix} 27 & 1 \\ 3 & 2 \end{bmatrix}$.

Solution:

Given message is : `we live in an insecure world`

Now, Break the message into digraphs :

```
we li ve in an in se cu re wo rl da
```

(If the message did not consist of an even number of letters, we would place a null at the end.)

Now convert each pair of letters to its number-pair equivalent. We will use our usual $a = 0, 1, \cdots z = 25$.

22 4, 11 8, 21 4, 8 13, 0 13, 8 13, 18 4, 2 20, 17 4, 22 14, 17 11, 3 0.

Encryption:

Now, encrypt the each pair using the key, which is matrix $\begin{bmatrix} 27 & 1 \\ 3 & 2 \end{bmatrix}$.

Make the first pair of numbers into column vector $(w(22)\ e(4))$, and multiply that matrix by the key.

$$\begin{aligned} \begin{bmatrix} 27 & 1 \\ 3 & 2 \end{bmatrix} \begin{bmatrix} 22 \\ 4 \end{bmatrix} &= \begin{bmatrix} 27 \times 22 + 1 \times 4 \\ 3 \times 22 + 2 \times 4 \end{bmatrix} \\ &= \begin{bmatrix} 598 \\ 74 \end{bmatrix} \end{aligned}$$

of course, we need our result to be **mod 26**. thus,

$$\begin{bmatrix} 598 \\ 74 \end{bmatrix} \equiv \begin{bmatrix} 0 \\ 22 \end{bmatrix} \text{mod } 26$$

$$\boxed{\text{The cipher text is A(0) W(22)}}$$

For the next pair l(11) i(8),

$$\begin{bmatrix} 27 & 1 \\ 3 & 2 \end{bmatrix} \begin{bmatrix} 11 \\ 8 \end{bmatrix} \equiv \begin{bmatrix} 19 \\ 23 \end{bmatrix} \text{mod } 26$$

$$\boxed{\text{19 corressponds to T and 23 corresponds to X}}$$

Again, For the next pair v(21) e(4),

$$\begin{bmatrix} 27 & 1 \\ 3 & 2 \end{bmatrix} \begin{bmatrix} 21 \\ 4 \end{bmatrix} \equiv \begin{bmatrix} 25 \\ 19 \end{bmatrix} \text{mod } 26$$

$$\boxed{\text{25 corressponds to Z and 19 corresponds to T}}$$

Again, For the next pair i(8) n(13),

$$\begin{bmatrix} 27 & 1 \\ 3 & 2 \end{bmatrix} \begin{bmatrix} 8 \\ 13 \end{bmatrix} \equiv \begin{bmatrix} 21 \\ 24 \end{bmatrix} \text{mod } 26$$

$$\boxed{\text{21 corressponds to V and 24 corresponds to Y}}$$

Again, For the next pair $a(0)$ n(13),

$$\begin{bmatrix} 27 & 1 \\ 3 & 2 \end{bmatrix} \begin{bmatrix} 0 \\ 13 \end{bmatrix} \equiv \begin{bmatrix} 13 \\ 0 \end{bmatrix} \text{mod } 26$$

$$\boxed{\text{13 corresspонds to N and 0 corresponds to A}}$$

Again, For the next pair i(8) n(13),

$$\begin{bmatrix} 27 & 1 \\ 3 & 2 \end{bmatrix} \begin{bmatrix} 8 \\ 13 \end{bmatrix} \equiv \begin{bmatrix} 21 \\ 24 \end{bmatrix} \text{mod } 26$$

$$\boxed{\text{21 corressponds to V and 24 corresponds to Y}}$$

Again, For the next pair $s(18)$ e(4),

$$\begin{bmatrix} 27 & 1 \\ 3 & 2 \end{bmatrix} \begin{bmatrix} 18 \\ 4 \end{bmatrix} \equiv \begin{bmatrix} 22 \\ 10 \end{bmatrix} \text{mod } 26$$

$$\boxed{\text{22 corressponds to W and 10 corresponds to K}}$$

Again, For the next pair c(2) u(20),

$$\begin{bmatrix} 27 & 1 \\ 3 & 2 \end{bmatrix} \begin{bmatrix} 2 \\ 20 \end{bmatrix} \equiv \begin{bmatrix} 22 \\ 20 \end{bmatrix} \text{mod } 26$$

$$\boxed{\text{22 corressponds to W and 20 corresponds to U}}$$

Again, For the next pair r(17) e(4),

$$\begin{bmatrix} 27 & 1 \\ 3 & 2 \end{bmatrix} \begin{bmatrix} 17 \\ 4 \end{bmatrix} \equiv \begin{bmatrix} 21 \\ 7 \end{bmatrix} \text{mod } 26$$

$$\boxed{\text{21 corressponds to V and 7 corresponds to H}}$$

Again, For the next pair w(22) o(14),

$$\begin{bmatrix} 27 & 1 \\ 3 & 2 \end{bmatrix} \begin{bmatrix} 22 \\ 14 \end{bmatrix} \equiv \begin{bmatrix} 10 \\ 16 \end{bmatrix} \text{mod } 26$$

$$\boxed{\text{10 corressponds to K and 16 corresponds to Q}}$$

Again, For the next pair r(17) $l(11)$,

$$\begin{bmatrix} 27 & 1 \\ 3 & 2 \end{bmatrix} \begin{bmatrix} 17 \\ 11 \end{bmatrix} \equiv \begin{bmatrix} 2 \\ 21 \end{bmatrix} \text{mod } 26$$

$$\boxed{\text{2 corressponds to C and 21 corresponds to V}}$$

Again, For the next pair d(3) $a(0)$,

$$\begin{bmatrix} 27 & 1 \\ 3 & 2 \end{bmatrix} \begin{bmatrix} 3 \\ 0 \end{bmatrix} \equiv \begin{bmatrix} 3 \\ 9 \end{bmatrix} \bmod 26$$

$$\boxed{\text{3 corressponds to D and 9 corresponds to J}}$$

Gathering the encrypted data of all the pairs, the cipher text for whole message is,

`Ciphertext,` C $\equiv$ `AW TX ZT VY NA VY WK WU VH KQ CV DJ`

Decryption:

The determinant of $\begin{bmatrix} 27 & 1 \\ 3 & 2 \end{bmatrix}$ is $27 \times 2 - 3 \times 1 = 54 - 3 = 51 \equiv 25 \bmod 26$.

Since, gcd(25,26) = 1 i.e 25 and 26 are co-prime. Thus 25 has a multiplicative inverse modulo 26, this matrix has an inverse. The inverse of the matrix is

$$\begin{bmatrix} \frac{2}{25} & \frac{-1}{25} \\ \frac{-3}{25} & \frac{27}{25} \end{bmatrix} \bmod 26$$

Dividing by 25 modulo 26 is the same as the multiplying by the multiplicative inverse of 25 modulo 26. But, we know that multiplicative inverse of 25 is 25 modulo 26.So, the inverse of the matrix is

$$\begin{bmatrix} \frac{2}{25} & \frac{-1}{25} \\ \frac{-3}{25} & \frac{27}{25} \end{bmatrix} \bmod 26 \equiv \begin{bmatrix} 2 \times 25 & -1 \times 25 \\ -3 \times 25 & 27 \times 25 \end{bmatrix} \bmod 26$$

$$\equiv \begin{bmatrix} 50 & -25 \\ -75 & 675 \end{bmatrix} \bmod 26 \equiv \begin{bmatrix} 24 & 1 \\ 3 & 25 \end{bmatrix}$$

We use the inverse key $\begin{bmatrix} 24 & 1 \\ 3 & 25 \end{bmatrix}$ to decrypt `AW`, which is the first digraph of the ciphertext.

`A` corresponds to 0, and `W` corresponds to 22.

$$\begin{bmatrix} 24 & 1 \\ 3 & 25 \end{bmatrix} \begin{bmatrix} 0 \\ 22 \end{bmatrix} \equiv \begin{bmatrix} 22 \\ 550 \end{bmatrix} \bmod 26 = \begin{bmatrix} 22 \\ 4 \end{bmatrix}$$

`w`(22) `e`(4).

In a similar manner, we can decrypt the remainder of the ciphertext.
Eventually, the Plaintext $P \equiv$ `we li ve in an in se cu re wo rl da`
or, `we live in an insecure world`.

Solution of Question No 4.

Complete Residue System:

Let m be a fixed positive integer then the set of integers $\{a_1, a_2, \cdots, a_k\}$ is called complete residue system if it satisfies the following conditions:

1. $a_i \not\equiv a_j (\text{mod m}) \; \forall \; i \neq j$

2.For each integer n their correspond an unique integer a_i such that,

$$n \equiv a_i (\text{mod m})$$

Example:

The set of integers $\{49, 20, 10, 17, -18, -21\}$ is a complete residue system modulo 6.

Let's assign $a_1 = 49, a_2 = 20, a_3 = 10, a_4 = 17, a_5 = -18, a_6 = -21$

$\implies \quad a_i \not\equiv a_j (\text{mod } 6) \; \forall \; i \neq j$

6	49	20	10	17	-18	-21
	1	2	4	5	0	3

Here the digits on the bottom cells are remainder when the digits of the top cells are divided by 6.

i.e $49 \not\equiv 20(\text{mod } 6)$, $20 \not\equiv 10(\text{mod } 6)$
so, $a_i \neq a_j(\text{mod } 6)$, for $i \neq j$

Since,

$$1 \equiv 49 \; (\text{mod } 6), 5 \equiv 17(\text{mod } 6)$$

$$2 \equiv 20(\text{mod } 6) \; , \; 0 \equiv -18(\text{mod } 6)$$

$$4 \equiv 10(\text{mod } 6) \; , \; 3 \equiv -21(\text{mod } 6)$$

Reduced Residue System:

The set of integers $\{a_1, a_2, \cdots, a_k\}$ is called a reduced residue system mod n if it satisfies the following conditions,

1. $\gcd(a_i, m) = 1$ for every $i = 1, 2, \cdots, k$

2. $a_i \not\equiv a_j (\text{mod } n) \; \forall \; i \neq j$

3. For each integer n , relatively prime to m therefore correspond an unique integer a_i such that,

$$n \equiv a_i (\text{mod n})$$

.

Example:

The set of integers $\{1, 5, 7, 11\}$ is a reduced residue system modulo 12 because gcd(1,12) = gcd(5,12) = gcd(7,12) = gcd(11,12) = 1.

Let's assign $a_1 = 1,\ a_2 = 5,\ a_3 = 7,\ a_4 = 11$

therefore $a_i \not\equiv_j$ for $i \neq j$.

Put $n = 17,\ m = 12 \implies$ gcd(17,12) = 1 and

$$17 \equiv 5 \text{ mod } 12$$

Put $n = 25,\ m = 12 \implies$ gcd(25,12) = 1 and

$$25 \equiv 1 \text{ mod } 12$$

Put $n = 19,\ m = 12 \implies$ gcd(19,12) = 1 and

$$19 \equiv 7 \text{ mod } 12$$

Put $n = 35,\ m = 12 \implies$ gcd(35,12) = 1 and

$$35 \equiv 11 \text{ mod } 12$$

Now, let's solve the given problem ,

$S = \{-19, -1, 22, 43, 46, 79, 113, 452\}$ is a reduced residue system modulo 15, because,

gcd(-19,15) = gcd(-1,15) = gcd(22,15) = gcd(43,15) = gcd(46,15) = gcd(79,15) = gcd(113,15) = gcd(452,15) = 1.

Put,
$a_1 = -19,\ a_2 = -1,\ a_3 = 22,\ a_4 = 43,\ a_5 = 46,\ a_6 = 79,\ a_7 = 113,\ a_8 = 452.$

This shows that $a_i \neq a_j$ for $i \neq j$.

Now,
Put, $n = 11,\ m = 15 \implies$ gcd(11,15) = 1 and $11 \equiv -19$(mod 15)

Put, $n = 14,\ m = 15 \implies$ gcd(14,15) = 1 and $14 \equiv -1$(mod 15)

Put, $n = 7,\ m = 15 \implies$ gcd(7,15) = 1 and $7 \equiv 22$(mod 15)

Put, $n = 13,\ m = 15 \implies$ gcd(13,15) = 1 and $13 \equiv 43$(mod 15)

Put, $n = 1,\ m = 15 \implies$ gcd(1,15) = 1 and $1 \equiv 46$(mod 15)

Put, $n = 4,\ m = 15 \implies$ gcd(4,15) = 1 and $4 \equiv 79$(mod 15)

Put, $n = 8,\ m = 15 \implies$ gcd(8,15) = 1 and $8 \equiv 113$(mod 15)

Put, $n = 2,\ m = 15 \implies$ gcd(2,15) = 1 and $2 \equiv 452$(mod 15).

Solution of Question No 5.

We have to prove that,

$a^{\phi(n)} \equiv 1(\text{mod } n)$, $\forall\ n \geq 1 \in \mathbb{Z}$ and $a \in \mathbb{Z}$ such as $\gcd(a, n) = 1$.

Proof:

If $n = 1$ then $\phi(n) = 1$.

and $a' = a \equiv 1(\text{mod } 1)$

Now, we assume $n > 1$. Let $a_1, a_2, \cdots, aa_{\phi(n)}$ be the positive integer less than n which are relatively prime to n .i.e $(a_i, n) = 1$

We consider $aa_1, aa_2, \cdots a_{\phi(n)}$ for each i ;

$$1 \leq i \leq \phi(n)\ ,\ aa_i \not\equiv 0 \text{ mod n}$$

because $n|aa_i$, $(a, n) = 1 \implies n|a_i$

Which is not possible because,

$$aa_i \equiv aa_j \text{ mod n}$$

$$\implies n|(aa_i - aa_j) \implies n|a(a_i - a_j)$$

and $(a, n) = 1$

$$\implies n|(a_i - a_j)$$

$$\implies a_i \equiv a_j \text{ mod n}$$

Which is again not possible.

Thus $aa_1, aa_2, \cdots\cdots, aa_{\phi(n)}$ are $\phi(n)$ mutually congruent integer and therefore,

$$\begin{gathered} aa_1 \equiv aa'_1 \text{ (mod n)} \\ aa_2 \equiv aa'_2 \text{ (mod n)} \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ aa_{\phi(n)} \equiv aa'_{\phi(n)} \text{ (mod n)} \end{gathered}$$

where $a'_1, a'_2, \cdots\cdots$ and $a_1, a_2, \cdots\cdots$ are in same in other order.

multiplying these relations we get as,

$$aa_1 \cdot aa_2 \cdots\cdots aa_{\phi(n)} \equiv a'_1 a'_2 \cdots\cdots a'_{\phi(n)} \text{ (mod n)}$$

$$a^{\phi(n)}a_1a_2\cdots\cdots a_{\phi(n)} \equiv a_1a_2\cdots\cdots a_{\phi(n)} \text{ (mod n)}$$

Since each a_i is co-prime to n, we have $(a_1\ a_2\ \cdots\cdots\cdots a_{\phi(n)})$ is co-prime to n. Therefore,

$$\boxed{a^{\phi(n)} \equiv 1 \text{ (mod n)}}$$