DATE:

Chapter 2

Integers and Matrices

Integer:

In discrete structure, an integer is a mathematical concept that represents whole number without any fractional or decimal parts. Integer can be positive, negative or zero.

Division:

Division of integers involves dividing one integer by another and obtaining the quotient and remainder. For example: When dividing 17 by 5 the quotient is 3 and the remainder is 2.

Prime and Greatest Common Divisor:

Prime numbers are integers greater than 1 that have no positive divisiors other than 1 and themself.

The greater common divisor (GCD) of two integers is the largest positive integer that divides both of them without leaving a remainder. For example: GCD of 12 and 18 is 6.

Extended Euclidean Algorithm:

It is an algorithm that is to compute integers x and y such that,

$$ax + by = gcd(a, b)$$

The extended euclidean algorithm is an efficient algorithm for finding the greatest common

DATE:

divisor of two integers.

Integers and Algorithm:

Integers are often used in various algorithms, such as sorting algorithms (eg: bubble sort, merge sort) or searching algorithms (eg: binary search). These algorithms manipulate integer values to perform tasks efficiently and accurately.

Integer Sorting Algorithms:

Sorting algorithms aim to arrange a list of integers in a specific order, such as ascending or descending. There are various algorithms for sorting and the choice can have the significant impact on the efficiency and performance of the algorithms. For example: bubble sort, merge sort.

Integer Searching Algorithms:

Searching algorithm are used to locate a specific integer within a given set of integers.
Binary search is a common example of searching algorithm that operates on a sorted list of integers.

Integer Arithamatic:

This includes the process of performing basic arithematic operations, such as +, -, /, ×, on integers. Algorithms for integer arithematic focus on efficiently handling large integers and ensuring accuracy in the result.

Integers Optimization Algorithms:

This involves finding optional solutions to mathematical problems that involves integers as variables. Linear programming, quadratic programming are the optimization algorithm, where the decision variables are restricted to integer values.

Integer Based Data Structure:

Integer based data structure are fundamental components of many algorithms in discrete structure.

For example: array, linked list, hash table, etc.

Efficient manipulation and organization of integer based data structure are crucial for algorithmic performance.

Number Theory:

It is a branch of mathematics that focuses on the properties and relationships of integers and their patterns. It is a fundamental area of study in discrete structure, dealing with the discrete nature of numbers and their mathematical properties.

In number theory, mathematicians explore

DATE:

various topics such as prime numbers, divisibility, modular arithematic, congruences, diophantine equations and arithematic function. These concepts play a crucial role in understanding the fundamental properties of integers and their relationships.
Number theory plays a vital role in cryptography, coding theory and other areas of discrete structure.

Application of Number Theory:

1. Linear Congruencies:
It have various applications in cryptography random number generation, and error detection. For example: In cryptography, linear congurencies are used in generation of pseudorandom numbers or in designing secure encryption algorithms. They are also utilized in error detection and correction codes, where linear congruencies help identity and correct errors in transmitted data.

2. Chinese Remainder Theorem:
CRT has applications in computer science, cryptography and solving modular arithmetic problems effectively and efficiently. It states that if we have a system of congruences with different moduli, we can find a unique solution that satisfies all the congruences. Additionally, it is used in solving problems involving periodic phenomena and in various

computational algorithms.

3. Computer arithmetic with large integers:
Number theory plays a vital role in computer arithmetic, particularly in dealing with large integers. Large integers are encountered in cryptography, number theory calculations and various computational problems. It has the effective application areas such as digital signatures, secure communication systems, in general where, there the efficient computations with large integers are essentials.

Modular Arithmetic:
This type of arithmetic used for only integer number calculation. We know if any integer 'a' is divided by another positive integer 'm' and if not perfectly divide then remainder 'r' is obtained. Such that,

$$a = m * quotient + r$$

The operation which gives remainder is known as modular operation and thus the process is called as modular arithmetic.

If a and b are integers and m is positive integer, then a is congruent to b modulo m if m divide a-b.

For example: 17 congruent to 13 modulo 4.

DATE:

Q. Determine whether 37 is congruent to 2 modulo 5.

→ Sol:

Here,

$a = 37, b = 2, m = 5$

[* If b = 1 then it wont be true.]

Then,

$a - b = 37 - 2 = 35$

$\therefore \frac{a-b}{m} = \frac{35}{5} = 7$

So, it is true.

Applications of Modular Arithmetic: Congruence

a) Hashing function:

- Mapping of key or information

We know bank has records for each of its user to access the records quickly, the account number of user can be used as key information and using hashing function we can map key into particular memory location where record is kept.

There are different hashing function but to have the application from modular arithmetic we define,

$h(k) = k \bmod m$

Where, $k \longrightarrow$ value

$m \longrightarrow$ size of hash table

$h(k) \longrightarrow$ the memory location for the records that has 'k' as its key

DATE:

Q. Which memory location is assigned by the hashing function $h(k) = k \mod 200$, for the users of account number 62253129.

→ Sol:

Here,

$h = 62253129$

$m = 200$

Then,

$h(k) = k \mod m$

$\therefore h(62253129) = 62253129 \mod 200$

$= 129$

So, it is hash value or memory location and record of customer with account number 62253129 is assigned to memory location 129.

b) Pseudo Random Number:

- generated by a process/machine/algorithm whose outcome is unpredictable.
- pseudo → (Not true or fake)
- most commonly used for linear congruential method

The linear congruential method produces sequence of integer between 0 and m-1.

Using the following recursive formula.

$X_{i+1} = (aX_i + c) \mod m$

X_0 = Initial value

a & c = constants

m = modulo

For example:

Generate the first 6 random numbers using L.C.M. method with $X_0 = 27$, $a = 17$, $c = 43$ and $m = 100$.

DATE:

Sol;

Here,

$X_0 = 27$, $a = 17$, $c = 43$ and $m = 100$

Then,

$$X_1 = (a * X_0 + c) \bmod \cancel{100}\ m$$
$$= (17 * 27 + 43) \bmod 100$$
$$= 502 \bmod 100$$
$$= 2$$

$$X_2 = (a * X_1 + c) \bmod \cancel{100}\ m$$
$$= (17 * 2 + 43) \bmod 100$$
$$= 77$$

$$X_3 = (a * X_2 + c) \bmod m$$
$$= (17 * 77 + 43) \bmod 100$$
$$= 52$$

$$X_4 = (a * X_3 + c) \bmod m$$
$$= (17 * 52 + 43) \bmod 100$$
$$= 27$$

$$X_5 = (a * X_4 + c) \bmod m$$
$$= (17 * 27 + 43) \bmod 100$$
$$= 2$$

$$X_6 = (a * X_5 + c) \bmod m$$
$$= (17 * 2 + 43) \bmod 100$$
$$= 77$$

Prime factorization:

For example: $270 = 2 \times 3 \times 3 \times 3 \times 5 = 2 \times 3^3 \times 5$

$875 = 5 \times 5 \times 5 \times 7 = 5^3 \times 7$

Relative Prime:

Two integer a and b are said to be relative prime if $\gcd(a, b) = 1$.

DATE:

For example, $\gcd(3,5)=1$.

Pairwise Relative Prime:

The integers $a_1, a_2, \ldots\ldots, a_n$ are pairwise relatively prime if $\gcd(a_i, a_j)=1$ where $1 \le i \le j \le n$.

Q. Check if they are relatively prime or not:
40, 21, 13.

→ Sol:

Since, $\gcd(13, 21) = 1$
$\gcd(13, 40) = 1$
$\gcd(21, 40) = 1$

Therefore, the given number sequence 13, 21 and 40 are relatively prime.

Q. Use prime factorization to find the gcd of 18 and 42.

→ Sol:

$18 = 2 \times 3 \times 3$
$42 = 2 \times 3 \times 7$

$\therefore$ The $\gcd(18, 42) = 2 \times 3$
$= 6$

Euclidean Algorithm:

This algorithm is generally used to calculate greatest common divisor. Represented as $\gcd(a,b)$ and is defined as

$$\gcd(a,b) = d$$

Where, d is the largest number that divide both a and b.

DATE:

If gcd (a, b) = 1 then those numbers a and b are relatively prime.

Find gcd of 36 and 63.

Sol;

$36 = 2 \times 2 \times 3 \times 3$

$63 = 3 \times 3 \times 7$

$\therefore gcd(36, 63) = 2^{min(2,0)} \cdot 3^{min(2,2)} \cdot 7^{min(0,1)}$

$= 3 \times 3$

$= 9$

Find gcd of (421, 111) using euclidean algorithm.

Sol;

$421 = 111 \times 3 + 88$

$111 = 88 \times 1 + 23$

$88 = 23 \times 3 + 19$

$23 = 19 \times 1 + 4$

$19 = 4 \times 4 + 3$

$4 = 3 \times 1 + 1$

$3 = 3 \times 1 + 0$

Since, the last non-zero remainder is 1.

Hence, gcd of (421, 111) = 1.

~~Find gcd of (161, 28) using euclidean algorithm.~~

~~Sol;~~

DATE:

Extended Euclidean Algorithm:

Input: two non-negative integers a and b with $a \geq b$.

Output: $d = \gcd(a,b)$ and integers x and y satisfying $ax + by = d$.

s t

Where, $s = s_1 - qs_2$

$t = t_1 - qt_2$

s_1	s_2	t_1	t_2
1	0	0	1

opposite

Q. Find gcd of (161, 28) using euclidean algorithm.

→ Soln:

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
5	161	28	21	1	0	1	0	1	-5
1	28	21	7	0	1	-1	1	-5	6
3	21	7	0	1	-1	4	-5	6	-23
	7	0		-1	4		6	-23	

$\gcd(161, 28) = 7$.

or, $r_1 s + r_2 t = 7$

or, $161 \times (-1) + 28 \times 6 = 7$

or, $-161 + 168 = 7$

$\therefore 7 = 7$

DATE:

Boolean Matrix (Zero One Matrix):

The matrix having it's elements in boolean. Such matrix can be used to represent a binary relation between a pair of finite sets.

We have boolean operations as $\wedge, \vee, \neg$.

$$b_1 \wedge b_2 = \begin{cases} 1 & \text{if } b_1 = b_2 = 1 \\ 0 & \text{otherwise} \end{cases}$$

$$b_1 \vee b_2 = \begin{cases} 1 & \text{if } b_1 = 1 \text{ or } b_2 = 1 \\ 0 & \text{otherwise} \end{cases}$$

Product of two matrices:

$A = \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix}$ and $B = \begin{bmatrix} b_1 & b_2 \\ b_3 & b_4 \end{bmatrix}$.

Then,

$$A \vee B = \begin{bmatrix} a_1 \vee b_1 & a_2 \vee b_2 \\ a_3 \vee b_3 & a_4 \vee b_4 \end{bmatrix}$$

Similarly,

$$A \wedge B = \begin{bmatrix} a_1 \wedge b_1 & a_2 \wedge b_2 \\ a_3 \wedge b_3 & a_4 \wedge b_4 \end{bmatrix}$$

Q. Given $A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ and $B = \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix}$. Find $A \vee B$ and $A \wedge B$.

→ Soln;

Here,

$$A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$B = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}$$

Now,

$$A \vee B = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \vee \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 \vee 0 & 0 \vee 0 \\ 0 \vee 1 & 1 \vee 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$

$$A \wedge B = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \wedge \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 \wedge 0 & 0 \wedge 0 \\ 0 \wedge 1 & 1 \wedge 1 \end{bmatrix}$$

$$= \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

Boolean Product ($\odot$):

$$A = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \text{ and } B = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 0 & 0 \end{bmatrix}$$

Then,

$$A \odot B = \begin{bmatrix} (1\wedge 0)\vee(0\wedge 1)\vee(1\wedge 0) & (1\wedge 1)\vee(0\wedge 1)\vee(1\wedge 0) & (1\wedge 0)\vee(1\wedge 1)\vee(0\wedge 1) \\ (1\wedge 0)\vee(1\wedge 1)\vee(0\wedge 0) & (1\wedge 1)\vee(1\wedge 1)\vee(1\wedge 0) & (0\wedge 0)\vee(0\wedge 1)\vee(1\wedge 1) \\ (0\wedge 0)\vee(0\wedge 1)\vee(1\wedge 0) & (1\wedge 0)\vee(0\wedge 1)\vee(1\wedge 0) & (0\wedge 0)\vee(0\wedge 1)\vee(1\wedge 1) \end{bmatrix}$$

$$= \begin{bmatrix} 0\vee 0\vee 0 & 1\vee 0\vee 0 & 0\vee 0\vee 1 \\ 0\vee 1\vee 0 & 1\vee 1\vee 0 & 0\vee 1\vee 0 \\ 0\vee 0\vee 0 & 0\vee 0\vee 0 & 0\vee 0\vee 1 \end{bmatrix}$$

$$= \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$$

DATE:

The Chinese Remainder Theorem:

It is used to solve a set of different congruent equations with one variable but different moduli which are relatively prime.

The problem be like:

$x = a_1 \pmod{m_1}$

$x = a_2 \pmod{m_2}$

$x = a_n \pmod{m_n}$

CRT states that the above equation have a unique solution of the moduli are relatively prime.

$x = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1} + \dots + a_n M_n M_n^{-1})$
mod M

Q. Solve the following equations using CRT:
$x = 2 \pmod 3$, $x = 3 \pmod 5$, $x = 2 \pmod 7$

→ Sol^n:

Comparing with $x = a_n \pmod{m_n}$, we get

$a_1 = 2$, $a_2 = 3$, $a_3 = 2$

$m_1 = 3$, $m_2 = 5$, $m_3 = 7$

$M = m_1 * m_2 * m_3 = 3 * 5 * 7 = 105$

$M_1 = \frac{M}{m_1} = \frac{105}{3} = 35$

$M_2 = \frac{M}{m_2} = \frac{105}{5} = 21$

$M_3 = \frac{M}{m_3} = \frac{105}{7} = 15$

Now, we have to find M_1^{-1}, M_2^{-1} and M_3^{-1}.
In order to compute the multiplicative inverse we have the relation as

DATE:

$(M_i * M_i^{-1}) = 1 \pmod{m_i}$

Then,

$M_1 * M_1^{-1} = 1 \bmod m_1$

$\Rightarrow 35 * M_1^{-1} = 1 \bmod 3$

$\Rightarrow 35 * 2 = 1 \bmod 3$

$\therefore M_1^{-1} = 2$

Similarly,

$M_2 * M_2^{-1} = 1 \bmod m_2$

$\Rightarrow 21 * M_2^{-1} = 1 \bmod 5$

$\Rightarrow 21 * 1 = 1 \bmod 5$

$\therefore M_2^{-1} = 1$

And,

$M_3 * M_3^{-1} = 1 \bmod m_3$

$\Rightarrow 15 * M_3^{-1} = 1 \bmod 7$

$\Rightarrow 15 * 1 = 1 \bmod 7$

$\therefore M_3^{-1} = 1$

Hence,

$x = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1}) \bmod M$

$= (2*35*2 + 3*21*1 + 2*15\times1) \bmod 105$

$= 233 \bmod 105$

$= 23$

Q. Solve the following equations using CRT:
$4X = 5 \pmod 9$, $2X = 6 \pmod{20}$

→ Sol:

Re-writing the above equations to generalize them:

$4X = 5 \pmod 9$

Multiplying both sides with 4^{-1}:

$4^{-1} 4X = 4^{-1} * 5 \pmod 9$

$\Rightarrow X = 4^{-1} \pmod 9 * 5 \pmod 9$

$\therefore$ $x = 7 * 5 \pmod 9$ $\quad$ $x = 4^{-1} \bmod 9$

$= 35 \pmod 9$ $\quad$ $\Rightarrow x = 7$

$= 8 \pmod 9$

Again,

$2x = 6 \pmod{20}$

Dividing both sides by 2.

$\therefore x = 3 \pmod{20}$

Then, comparing with $x = a_n \pmod{m_n}$, we get

$a_1 = 8$, $a_2 = 3$

$m_1 = 9$, $m_2 = 20$

$M = m_1 * m_2 = 9 * 20 = 180$

$$M_1 = \frac{M}{m_1} = \frac{180}{9} = 20$$

$$M_2 = \frac{M}{m_2} = \frac{180}{20} = 9$$

Now, we have to find M_1^{-1}, M_2^{-1} and M_3^{-1}.

In order to compute the multiplicative inverse we have the relation as

$(M_i * M_i^{-1}) = 1 \pmod{m_i}$

Then,

$M_1 * M_1^{-1} = 1 \bmod m_1$

$\Rightarrow 20 * M_1^{-1} = 1 \bmod 9$

$\Rightarrow 20 * 5 = 1 \bmod 9$

$\therefore M_1^{-1} = 5$

Similarly,

$M_2 * M_2^{-1} = 1 \bmod m_2$

$\Rightarrow 9 * M_2^{-1} = 1 \bmod 20$

$\Rightarrow 9 * 9 = 1 \bmod 20$

$\therefore M_2^{-1} = 9$

DATE:

Hence,

$x = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1}) \bmod M$

$= (8 * 20 * 5 + 3 * 9 * 9) \bmod 180$

$= 1043 \bmod 180$

$= 143$ //

Q. Solve the following equations using CRT:

$x = 5 \pmod 3$, $x = 2 \pmod 5$, $x = 1 \pmod 4$

→ Sol:

Comparing with $x = a_n \pmod{m_n}$, we get

$a_1 = 5$, $a_2 = 2$, $a_3 = 1$

$m_1 = 3$, $m_2 = 5$, $m_3 = 4$

$M = m_1 * m_2 * m_3 = 3 * 5 * 4 = 60$

$M_1 = \frac{M}{m_1} = \frac{60}{3} = 20$

$M_2 = \frac{M}{m_2} = \frac{60}{5} = 12$

$M_3 = \frac{M}{m_3} = \frac{60}{4} = 15$

Now, we have to find M_1^{-1}, M_2^{-1} and M_3^{-1}.
In order to compute the multiplicative inverse we have the relation as

$(M_i * M_i^{-1}) = 1 \pmod{m_i}$

Then,

$M_1 * M_1^{-1} = 1 \bmod m_1$

$\cancel{\Rightarrow 35 * M_1^{-1} = 1 \bmod 3}$

$\Rightarrow 20 * M_1^{-1} = 1 \bmod 3$

$\Rightarrow 20 * 2 = 1 \bmod 3$

$\therefore M_1^{-1} = 2$

Similarly,

DATE:

$M_2 * M_2^{-1} = 1 \bmod m_2$

$\Rightarrow 12 * M_2^{-1} = 1 \bmod 5$

$\Rightarrow 12 * 3 = 1 \bmod 5$

$\therefore M_2^{-1} = 3$

And,

$M_3 * M_3^{-1} = 1 \bmod m_3$

$\Rightarrow 15 * M_3^{-1} = 1 \bmod 4$

$\Rightarrow 15 * 3 = 1 \bmod 4$

$\therefore M_3^{-1} = 3$

Hence,

$x = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1}) \bmod M$

$= (5*20*2 + 2*12*3 + 1*15*3) \bmod 60$

$= 317 \bmod 60$

$= 17$

DATE:

Exercise 1.1

1. Let $A = \{1, 2, 3, 4, 5\}$, $B = \{2, 3, 6\}$. Find
(a) $A \cup B$ (b) $A \cap B$ (c) $A - B$ (d) $B - A$

→ Sol;

Here,

$$A = \{1, 2, 3, 4, 5\}$$
$$B = \{2, 3, 6\}$$

Now,

a) $A \cup B = \{1, 2, 3, 4, 5\} \cup \{2, 3, 6\}$
$= \{1, 2, 3, 4, 5, 6\}$

b) $A \cap B = \{1, 2, 3, 4, 5\} \cap \{2, 3, 6\}$
$= \{2, 3\}$

c) $A - B = \{1, 2, 3, 4, 5\} - \{2, 3, 6\}$
$= \{1, 4, 5\}$

d) $B - A = \{2, 3, 6\} - \{1, 2, 3, 4, 5\}$
$= \{6\}$

---

2. Let A and B be sets. Show that
a) $A \cup B = B \cup A$ b) $A \cap B = B \cap A$

→ Sol;

a) L.H.S. $= A \cup B$
$= \{x : x \in (A \cup B)\}$
$= \{x : x \in A \vee x \in B\}$
$= \{x : x \in B \vee x \in A\}$
$= \{x : x \in B \cup A\}$
$= B \cup A$

∴ R.H.S. proved

b) L.H.S. $= A \cap B$
$= \{x : x \in (A \cap B)\}$
$= \{x : x \in A \wedge x \in B\}$

DATE:

$= \{x : x \in B \wedge x \in A\}$

$= \{x : x \in B \cap A\}$

$= B \cap A$

$\therefore$ R.H.S. proved

3. Find the sets A and B if $A-B = \{1, 5, 7, 8\}$, $B - A = \{2, 10\}$ and $A \cap B = \{3, 6, 9\}$.

→ Soln:

Here,

$A - B = \{1, 5, 7, 8\}$

$B - A = \{2, 10\}$

$A \cap B = \{3, 6, 9\}$

Now,

$A = (A - B) + (A \cap B)$

$= \{1, 5, 7, 8\} + \{3, 6, 9\}$

$= \{1, 3, 5, 6, 7, 8, 9\}$

$B = (B - A) + (A \cap B)$

$= \{2, 10\} + \{3, 6, 9\}$

$= \{2, 3, 6, 9, 10\}$

4. Show that if A, B and C are three sets, then $\overline{A \cap B \cap C} = \bar{A} \cup \bar{B} \cup \bar{C}$.

→ Soln:

$L.H.S. = \overline{A \cap B \cap C}$

$= \{x : x \in (\overline{A \cap B \cap C})\}$

$= \{x : \neg(x \in (A \cap B \cap C))\}$

$= \{x : \neg(x \in A \wedge x \in B \wedge x \in C)\}$

$= \{x : \neg(x \in A) \vee \neg(x \in B) \vee \neg(x \in C)\}$

$= \{x : x \notin A \vee x \notin B \vee x \notin C\}$

$= \{x : x \in \bar{A} \vee x \in \bar{B} \vee x \in \bar{C}\}$

$= \{x : x \in \bar{A} \cup \bar{B} \cup \bar{C}\}$

$= \bar{A} \cup \bar{B} \cup \bar{C}$

DATE:

5. Let $A=\{0,2,4,6,8,10\}$, $B=\{0,1,2,3,4,5,6\}$ and $C=\{4,5,6,7,8,9,10\}$. Find

a) $A \cap B \cap C$ b) $A \cup B \cup C$ c) $(A \cup B) \cap C$ d) $(A \cap B) \cup C$

→ Sol;

Here,

$A=\{0,2,4,6,8,10\}$

$B=\{0,1,2,3,4,5,6\}$

$C=\{4,5,6,7,8,9,10\}$

Now,

a) $A \cap B \cap C = \{0,2,4,6,8,10\} \cap \{0,1,2,3,4,5,6\} \cap \{4,5,6,7,8,9,10\}$

$= \{4,6\}$

b) $A \cup B \cup C = \{0,2,4,6,8,10\} \cup \{0,1,2,3,4,5,6\} \cup \{4,5,6,7,8,9,10\}$

$= \{0,1,2,3,4,5,6,7,8,9,10\}$

c) $(A \cup B) \cap C = \{0,2,4,6,8,10\} \cup \{0,1,2,3,4,5,6\} \cap C$

$= \{0,1,2,3,4,5,6,8,10\} \cap \{4,5,6,7,8,9,10\}$

$= \{4,5,6,8,10\}$

d) $(A \cap B) \cup C = \{0,2,4,6,8,10\} \cap \{0,1,2,3,4,5,6\} \cup C$

$= \{0,2,4,6\} \cup \{4,5,6,7,8,9,10\}$

$= \{0,2,4,5,6,7,8,9,10\}$

6. Suppose that the universal set is $U=\{1,2,3,4,5,6,7,8,9,10\}$. Express each of these sets with bit strings representation.

→ Sol;

Here,

$U=\{1,2,3,4,5,6,7,8,9,10\}$

Now,

For odd integers, $U=\{1,3,5,7,9\}$

Bit strings = 1010101010

DATE:

For even integers, $U = \{2, 4, 6, 8, 10\}$
Bit strings = 0101010101

7. Suppose that the universal set is $U = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. Find the set specified by each of these bit strings.

a) 1111001111
→ $U = \{1, 2, 3, 4, 7, 8, 9, 10\}$

b) 0101111000
→ $U = \{2, 4, 5, 6, 7\}$

c) 1000010011
→ $U = \{1, 6, 9, 10\}$

DATE:

Exercise 1.2

1. Let $X = \{1,2,3,4\}$. Determine whether or not each relation below is a function from X into X.

(i) $f = \{(1,1), (2,1), (3,1), (4,1), (3,3)\}$

→ Not a function X into X

(ii) $f = \{(1,1), (2,1), (3,1), (4,1)\}$

→ A function X into X

(iii) $f = \{(2,1), (3,4), (4,4)\}$

→ A function X into X

2. Find the value of

(i) $\lfloor 8.3 \rfloor = 8$

(ii) $\lfloor -8.7 \rfloor = -9$

(iii) $\lceil -5.9 \rceil = -5$

(iv) $\left\lceil \frac{1}{3} \right\rceil = 1$

(v) $\lceil \log_2 51 \rceil = 6$

(vi) $\lfloor \log_3 29 \rfloor = 3$

3. If $f(x) = x^2 - 2$ and the domain of the function is $\{-1, 0, 1, 2, 3\}$. Find the range of the function. Is it one-to-one?

→ Sol;

Here,

$f(x) = x^2 - 2$

domain $= \{-1, 0, 1, 2, 3\}$

Now,

To find range,

$f(-1) = (-1)^2 - 2 = -1$

DATE:

$f(0) = 0^2 - 2 = -2$

$f(1) = 1^2 - 2 = -1$

$f(2) = 2^2 - 2 = 2$

$f(3) = 3^2 - \cancel{2} = 7$

~~Since, two domain elements -1 and 1 have same range 1. So~~, It is ~~a~~ one-to-one function.

Let $A = \{x : x \neq \frac{1}{2}\}$ and define $f : A \rightarrow R$ by $f(x) = \frac{4x}{2x-1}$. Is f one-to-one? Find $R(f)$. Explain why $f : A \rightarrow R(f)$ has an inverse. Find dom f^{-1}, ran f^{-1} and a formula for $f^{-1}(x)$.

Soln;

Here,

$$A = \{x : x \neq \frac{1}{2}\}$$

$$f(x) = \frac{4x}{2x-1}$$

Yes, $f(x)$ is one-to-one function.

5. If the function $f: R \rightarrow R$ is defined by $f(x) = x^2+1$, for $x \in R$ and $x \geq 0$, find $f^{-1}(-8)$ and $f^{-1}(1$

→ Sol;

Here,

$f(x) = x^2+1 \quad x \in R$ and $x \geq 0$

$f^{-1}(-8) = ?$

$f^{-1}(17) = ?$

Let, $f(x)$ ~~by~~ be y.

$\therefore y = x^2+1$

Interchanging the values of x and y, we get

$x = y^2+1$

or, $x-1 = y^2$

$\therefore y = \sqrt{x-1}$

$\therefore f^{-1}(x) = \sqrt{x-1}$.

Now,

$f^{-1}(-8) = \sqrt{-8-1}$

$= \sqrt{-9}$

(invalid)

$f^{-1}(17) = \sqrt{17-1}$

$= \sqrt{16}$

$= 4$

DATE:

6. Let $S=\{1,2,3,4\}$ and define functions $f,g: S\to S$ by $f=\{(1,3),(2,2),(3,4),(4,1)\}$ and $g=\{(1,4),(2,3),(3,1),(4,2)\}$. Then find (i) $g^{-1}ofog$ (ii) $f^{-1}og^{-1}ofog$.

→ Soln;

Here,

$S=\{1,2,3,4\}$

$f=\{(1,3),(2,2),(3,4),(4,1)\}$

$g=\{(1,4),(2,3),(3,1),(4,2)\}$

$g^{-1}ofog=?$

$f^{-1}og^{-1}ofog=?$

Now, we can compute fog for ~~ete~~ each element ~~Using~~ of S: $fog(1)=1$

$fog(2)=4$

$fog(3)=2$

$fog(4)=3$

Then, we need to apply g^{-1} to each element of the range of fog.

$g(3)=1$ $\therefore g^{-1}(1)=3$

$g(4)=2$ $\therefore g^{-1}(2)=4$

$g(2)=3$ $\therefore g^{-1}(3)=2$

$g(1)=4$ $\therefore g^{-1}(4)=1$

Therefore, $g^{-1}ofog=\{(1,3),(2,4),(3,2),(4,1)\}$.

Again, ~~from~~

$f(4)=1$ $\therefore f^{-1}(1)=4$

$f(2)=2$ $\therefore f^{-1}(2)=2$

$f(1)=3$ $\therefore f^{-1}(3)=1$

$f(3)=4$ $\therefore f(4)=3$

DATE:

$og^{-1}ofog(1)=4$ $\quad$ $f^{-1}(4)=2$

$og^{-1}ofog(2)=2$ $\quad$ $f^{-1}(2)=3$

$og^{-1}ofog(3)=1$ $\quad$ $f^{-1}(1)=4$

$og^{-1}ofog(4)=3$ $\quad$ $f^{-1}(3)=1$

Then,

$f^{-1}og^{-1}ofog(1)=2$

$f^{-1}og^{-1}ofog(2)=3$

$f^{-1}og^{-1}ofog(3)=1$

$f^{-1}og^{-1}ofog(4)=4$

Therefore, $f^{-1}og^{-1}ofog=\{(1,8),(2,4),(3,2),(4,1)\}$.

7. Let $f: R\to R$ and $g: R\to R$ be two functions defined as $f(x)=2x+1$ and $g(x)=x^2-2$ then find the composite functions.

a) fog b) fof c) gof d) gog e) $fogof$

→ Sol:

Here,

$f(x)=2x+1$

$g(x)=x^2-2$

$fog=?$

$fof=?$

$gof=?$

$gog=?$

$fogof=?$

Now,

$fog=f(g(x))$
$=f(x^2-2)$
$=2(x^2-2)+1$
$=2x^2-4+1$
$=2x^2-3$

$fof=f(f(x))$
$=f(2x+1)$
$=2(2x+1)+1$
$=4x+2+1$
$=4x+3$

DATE:

$gof = g(f(x))$
$= g(2x+1)$
$= (2x+1)^2 - 2$
$= 4x^2 + 4x + 1 - 2$
$= 4x^2 + 4x - 1$

$gog = g(g(x))$
$= g(x^2 - 2)$
$= (x^2-2)^2 - 2$
$= x^4 - 4x^2 + 4 - 2$
$= x^4 - 4x^2 + 2$

$fogof = f(g(f(x)))$
$= f(g(2x+1))$
$= f((2x+1)^2 - 2)$
$= f(4x^2 + 4x - 1)$
$= 2(4x^2 + 4x - 1) + 1$
$= 8x^2 + 8x - 2 + 1$
$= 8x^2 + 8x - 1$

---

8. Let $f: R \to R$ defined by $f(x) = 3x - 7$. Find the formula for inverse function of f.

→ Soln;

Here, $f(x) = 3x - 7$

Let, $f(x)$ ~~be~~ y.

$\therefore y = 3x - 7$

Interchanging the value of x and y, we get

$x = 3y - 7$

or, $x + 7 = 3y$

$\therefore y = \frac{x+7}{3}$

$\therefore f^{-1}(x) = \frac{x+7}{3}$

DATE:

9. Find the formula for inverse of $f(x) = \frac{3x+2}{5x-7}$.

→ Sol;

Here, $f(x) = \frac{3x+2}{5x-7}$

Let, $f(x)$ by y.

$\therefore y = \frac{3x+2}{5x-7}$

Interchanging the value of x and y, we get

$x = \frac{3y+2}{5y-7}$

or, $x(5y-7) = 3y+2$

or, $5xy - 7x = 3y+2$

or, $5xy - 3y = 7x+2$

or, $y(5x-3) = 7x+2$

$\therefore y = \frac{7x+2}{5x-3}$

$\therefore f^{-1}(x) = \frac{7x+2}{5x-3}$,,

10. Let $A = B = R$, the set of real numbers. Function $f: A \to B$ be given by formula $f(x) = 2x^3 - 1$ and $g: B \to A$ be given by $g(y) = \sqrt[3]{\frac{y}{2} + \frac{1}{2}}$. Show that f is bijection between A and B and g is bijection between B and A.

→ Sol;

Here, $f(x) = 2x^3 - 1$

$g(y) = \sqrt[3]{\frac{y}{2} + \frac{1}{2}}$

Now, to show whether the function f is bijection between A and B, we have

if $x_1, x_2 \in R$ then $f(x_1) = f(x_2)$

$\Rightarrow 2x_1^3 - 1 = 2x_2^3 - 1$

$\Rightarrow 2x_1^3 = 2x_2^3$

$\Rightarrow x_1^3 = x_2^3$

$\Rightarrow x_1 = x_2$

This proves f is one-to-one.

Again, if $y \in R$, $y = f(x) = 2x^3 - 1$.

$\Rightarrow x = \sqrt[3]{\frac{y+1}{2}} \in R$

and,

$$f\left(\sqrt[3]{\frac{y+1}{2}}\right) = 2\left(\sqrt[3]{\frac{y+1}{2}}\right)^3 - 1 = \cancel{2}\left(\frac{y+1}{\cancel{2}}\right) - 1 = y+1-1 = y$$

$\therefore$ y is the ~~inver~~ image of $\sqrt[3]{\frac{y+1}{2}}$.

Again, to show whether the function f is bijection between B and A, we have

if $y_1, y_2 \in R$ then $g(y_1) = g(y_2)$

$\Rightarrow \sqrt[3]{\frac{y_1}{2} + \frac{1}{2}} = \sqrt[3]{\frac{y_2}{2} + \frac{1}{2}}$

$\Rightarrow \frac{y_1}{2} + \frac{1}{2} = \frac{y_2}{2} + \frac{1}{2}$

$\Rightarrow \frac{y_1}{2} = \frac{y_2}{2}$

$\Rightarrow y_1 = y_2$

This proves g is one-to-one.

Again, if $x \in R$, $x = g(y) = \sqrt[3]{\frac{y}{2} + \frac{1}{2}}$.

$\Rightarrow y = 2x^3 - 1$

and,

$$g(2x^3-1) = \sqrt[3]{\frac{(2x^3-1)}{2} + \frac{1}{2}}$$

$$= \sqrt[3]{\frac{2x^3}{2} \cancel{-\frac{1}{2}} \cancel{+\frac{1}{2}}}$$

$$= \sqrt[3]{\frac{\cancel{2}x^3}{\cancel{2}}}$$

$$= \sqrt[3]{x^3}$$

$$= x$$

$\therefore$ x is the image of $2x^3-1$.

Hence, f is bijection between A and B and g is bijection between B and A.

11. Let $A = B = C = R$ and consider the function and $g: B \to C$ defined by $f(a) = 2a+1$, $g(b) = \frac{b}{3}$ verify that $(gof)^{-1} = f^{-1}og^{-1}$.

$\Rightarrow$ Sol:

Here,

$$f(a) = 2a+1$$

$$g(b) = \frac{b}{3}$$

Let, $f(a)$ be x.

$\therefore f^{-1}(a) = \frac{a-1}{2}$

Let, $g(b)$ be y.

$\therefore g^{-1}(b) = 3b$

Then,

$$f^{-1}og^{-1} = f^{-1}(3b)$$

$$= \frac{3b-1}{2}$$

Now,

$$gof = g(2a+1)$$

$$= \frac{2a+1}{3}$$

DATE:

$(gof)^{-1} = \frac{3a-1}{2}$

Since, $A = B = C = R$.

Hence, $f^{-1}og^{-1} = (gof)^{-1}$. <u>Proved</u>

12. Let $f: R \to R$ be a function defined by $f(x) = x^2+1$ then find $f^{-1}(-8)$ and $f^{-1}(5)$.

→ Sol:

Here, $f(x) = x^2+1$

Let, $f(x)$ be y.

$\therefore y = x^2+1$

Interchanging the values of x and y, we get

$x = y^2+1$

or, $x-1 = y^2$

$\therefore y = \sqrt{x-1}$

$\therefore f^{-1}(x) = \sqrt{x-1}$

Now,

$f^{-1}(-8) = \sqrt{-8-1}$
$= \sqrt{-9}$
(invalid)

$f^{-1}(5) = \sqrt{5-1}$
$= \sqrt{4}$
$= 2$

13. Let the function $f: R \to R$ defined by

$$f(x) = \begin{cases} 2x-9 & \text{for } x > 4 \\ 3x^2+4 & -1 < x \leq 4 \\ x^2+7 & x \leq -1 \end{cases}$$ Find $f^{-1}(6)$.

→ Sol:

Here, $f(x) = 2x-9$

Let, $f(x)$ be y.

$\therefore y = 2x-9$

Interchanging the values of x and y, we get

$x = 2y-9$

DATE:

or, $x+9=2y$

$\therefore y=\frac{x+9}{2}$

$\therefore f^{-1}(x)=\frac{x+9}{2}$

Now,

$f^{-1}(6)=\frac{6+9}{2}$

$=\frac{15}{2}$,,

14. Let $f: A \to B$ and $g: B \to A$ verify that $g=f^{-1}$ of where $A=B=R$, $f(a)=\frac{a+1}{2}$, $g(b)=2b-1$.

→ Sol:

Here,

$f(a)=\frac{a+1}{2}$

$g(b)=2b-1$

Now,

Let $f(a)$ be x.

$x=\frac{a+1}{2}$

Interchanging the value of x and a, we get

$a=\frac{x+1}{2}$

or, $2a=x+1$

$\therefore x=2a-1$

$\therefore f^{-1}(a)=2a-1$

Since, $A=B=R$, ~~and~~ $f: A \to B$ and $g: B \to A$.

Hence, $g=f^{-1}$.

DATE:

15. If the function $f: R \to R$ defined by

$$f(x) = \begin{cases} 2x-4 & x > 1 \\ -3x+5 & x \leq 1 \end{cases}$$

Determine: $f(1)$, $f\left(\frac{1}{2}\right)$, $f^{-1}(2)$ and $f^{-1}(-5)$.

→ Sol;

Here,

$f(x) = 2x-4$ when $x > 1$

$f(x) = -3x+5$ when $x \leq 1$

Let $f(x)$ be y.

$\therefore y = 2x-4$ $\qquad$ $\therefore y = -3x+5$

Interchanging the values of x and y, we get

$x = 2y-4$ $\qquad$ $x = -3y+5$

or, $x+4 = 2y$ $\qquad$ or, $x-5 = -3y$

$\therefore y = \frac{x+4}{2}$ $\qquad$ $\therefore y = \frac{5-x}{3}$

$\therefore f^{-1}(x) = \frac{x+4}{2}$ $\qquad$ $\therefore f^{-1}(x) = \frac{5-x}{3}$

Now,

$f(1) = -3 \times 1 + 5 = -3+5 = 2$

$f\left(\frac{1}{2}\right) = -3 \times \frac{1}{2} + 5 = -\frac{3}{2} + 5 = \frac{7}{2}$

$f^{-1}(2) = \frac{2+4}{2} = \frac{6}{2} = 3$

$f^{-1}(-5) = \frac{5-(-5)}{3} = \frac{5+5}{3} = \frac{10}{3}$

DATE:

Exercise 1.3

1. Find at least three different sequences beginning with the terms 3, 5, 7 whose terms are generated by a simple formula or rule.

→ Here are three different sequences beginning with the terms 3, 5, 7 whose terms are generated by a simple formula or rule:

1. The sequence odd numbers: 3, 5, 7, 9, 11, 13, ...
   - Each term is generated by adding 2 to the previous term.
2. The sequence of multiples of 3: 3, 6, 9, 12, 15, 18, ...
   - Each term is generated by adding 3 to the previous term.
3. The sequence of squares of odd numbers: 3, 25, 49, 81, 121, 169, ...
   - Each term is generated by adding the next odd number to the previous term.

---

2. For each of these lists of integers, provide a simple formula or rule that generates the terms of an integer sequence that begins with the given list.

a. 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, ...

→ $a_n = (n \bmod 6) \bmod 3$

b. 1, 2, 2, 3, 4, 4, 5, 6, 6, 7, 8, 8, ...

→ $a_n = \text{ceil}(n/2) + \text{floor}(n/3) - 1$

c. 1, 0, 2, 0, 4, 0, 8, 0, 16, 0, ...

→ $a_n = 2^\wedge(\text{floor}((n-1)/2) \times (1 - n \bmod 2)$

DATE:

d. 3, 6, 12, 24, 48, 96, 192, ...

$\rightarrow a_n = 3 \times 2^{(n-1)}$

e. 15, 8, 1, -6, -13, -20, -27, ...

$\rightarrow a_n = 15 - 7n$

f. 2, 16, 54, 128, 250, 432, 686, ...

$\rightarrow a_n = n^3 - (n-2)^3$

3. Find the value of following summations:

a) $\sum_{x=1}^{6} (x+1)$

$= (1+1) + (2+1) + (3+1) + (4+1) + (5+1) (6+1)$

$= 2 + 3 + 4 + 5 + 6 + 7$

$= 27$

b) $\sum_{j=0}^{4} (-2)^j$

$= (-2)^0 + (-2)^1 + (-2)^2 + (-2)^3$

$= 1 - 2 + 4 - 8$

$= -5$

c) $\sum_{k=0}^{4} (2^{k+1} - 2^k)$

$= (2^{0+1} - 2^0) + (2^{1+1} - 2^1) + (2^{2+1} - 2^2) + (2^{3+1} - 2^3)$

$= (2^1 - 2^0) + (2^2 - 2^1) + (2^3 - 2^2) + (2^4 - 2^3)$

$= (2-1) + (4-2) + (8-4) + (16-8)$

$= 1 + 2 + 4 + 8$

$= 15$

DATE:

4. Compute each of these double sums.

a) $\sum_{i=1}^{2} \sum_{j=1}^{3} (i-j)$

$= \sum_{i=1}^{2} (i-1)+(i-2)+(i-3)$

$= \sum_{i=1}^{2} (3i-6)$

$= (3-6)+(3\times 2-6)$

$= -3+0$

$= -3$

b) $\sum_{i=0}^{3} \sum_{j=0}^{2} (3i+2j)$

$= \sum_{i=0}^{3} (3i+0)+(3i+2)$

$= \sum_{i=0}^{3} (6i+2)$

$= (0+2)+(6+2)+(18+2)$

$= 2+8+20$

$= 30$

5. What is the value of each of these sums of a geometric progression?

a) $\sum_{j=0}^{5} (3^j - 2^j)$

$= (3^0-2^0)+(3^1-2^1)+(3^2-2^2)+(3^3-2^3)+(3^4-2^4)+(3^5-2^5)$

$= (1-1)+(3-2)+(9-4)+(27-8)+(81-16)+(243-32)$

$= 0+1+5+19+65+211$

$= 301$

DATE:

b) $\sum_{j=0}^{5} (2.3^j + 3.2^j)$

$= (2.3^0 + 3.2^0) + (2.3^1 + 3.2^1) + (2.3^2 + 3.2^2) + (2.3^3 + 3.2^3) + (2.3^4 + 3.2^4)$

$= (2+3) + (6+6) + (18+12) + (54+24) + (162+48)$

$= 5 + 12 + 30 + 78 + 210$

$= 335$

c) $\sum_{i=0}^{7} 3.2^{i-1}$

$= 3.2^{0-1} + 3.2^{1-1} + 3.2^{2-1} + 3.2^{3-1} + 3.2^{4-1} + 3.2^{5-1} + 3.2^{6-1}$

$= \frac{3}{2} + 3 + 6 + 12 + 24 + 48 + 96$

$= \frac{381}{2}$

6. What are the terms a_0, a_1, a_2 and a_3 of the sequence $\{a_n\}$, where a_n equals:

a) $(-2)^n$

→ Soln;

$a_0 = (-2)^0 = 1$

$a_1 = (-2)^1 = -2$

$a_2 = (-2)^2 = 4$

$a_3 = (-2)^3 = -8$

b) $7 + 4^n$

→ Soln;

$a_0 = 7 + 4^0 = 7+1 = 8$

$a_1 = 7 + 4^1 = 7+4 = 11$

$a_2 = 7 + 4^2 = 7+16 = 23$

$a_3 = 7 + 4^3 = 7+64 = 71$

DATE:

c) $2^n + (-2)^n$

→ Sol;

$a_0 = 2^0 + (-2)^0 = 1 + 1 = 2$

$a_1 = 2^1 + (-2)^1 = 2 - 2 = 0$

$a_2 = 2^2 + (-2)^2 = 4 + 4 = 8$

$a_3 = 2^3 + (-2)^3 = 8 - 8 = 0$

7. List the first ten terms of each of these sequences:

a) The sequence that begins with 2 and in which each successive term is 3 more than the preceding terms.

→ 2, 5, 8, 11, 14, 17, 20, 23, 26, 29, ...

b) The sequence that begins with 3, where each succeeding term is three times the precedding term.

→ 3, 9, 27, 81, 243, 729, 2187, 6561, 19683, 59049, ...

c) The sequence whose first two terms are 1 and each succeeding terms is the sum of two preceding terms.

→ 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, ...

d) The squence whose n^{th} term is $3^n - 2^n$.

→ 1, 1, 4, 10, 22, 46, 94, 190, 382, 766, ...

DATE:

Exercise 2.0

1. Express the greatest common divisor of each of these pairs of integers as a linear combination of these integers.

a) 11, 17

→ Soln;

$11 = 11 \times 1$

$17 = 17 \times 1$

$\therefore \gcd(11, 17) = 1$

b) 63, 74

→ Soln;

$63 = 3 \times 3 \times 7 \times 1$

$74 = 2 \times 37 \times 1$

$\therefore \gcd(63, 74) = 1$

c) 33, 72

→ Soln;

$33 = 3 \times 11$

$72 = 2 \times 2 \times 2 \times 3 \times 3$

$\therefore \gcd(33, 72) = 3$

d) 21, 55

→ Soln;

$21 = 3 \times 7 \times 1$

$55 = 5 \times 11 \times 1$

$\therefore \gcd(21, 55) = 1$

e) 101, 203

→ Soln;

$101 = 101 \times 1$

$203 = 7 \times 29 \times 1$

$\therefore \gcd(101, 203) = 1$

f) 128, 325

→ Soln;

$128 = 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2$

$325 = 5 \times 5 \times 13$

$\therefore \gcd(128, 325) = 1$

DATE:

2. Show that 15 is an inverse of 7 modulo 26.

→ Sol;

Here,

~~$a = 15$, $b = 7$ and $m = 26$~~

Then,

~~$a - b = 15 - 7 = 8$~~

~~$\therefore \frac{a-b}{m} = \frac{8}{26} =$~~

→ Sol;

We know, From Euclidean algorithm,

$26 = 7 \times 3 + 5$

$7 = 5 \times 1 + 2$

$5 = 2 \times 2 + 1$

We can then work backwards to express 1 in terms of 26 and 7.

$1 = 5 - 2 \times 2$

$1 = 5 - 2 \times (7 - 5 \times 1)$

$= 5 \times 3 - 2 \times 7$

$1 = (26 - 7 \times 3) \times 3 - 2 \times 7$

$= 26 \times 3 - 7 \times 11$

Therefore, we ~~can~~ see that $7 * (-11)$ is congruent to 1 modulo 26.

Since, -11 is not a positive number, we can add 26 to it to get a positive number that is also congruent to -11 modulo 26. This gives us:

$$7 * (-11 + 26) = 7 \times 15 \equiv 1 \pmod{26}$$

So, the inverse of 7 modulo 26 is 15.

DATE:

3. Solve the congruence $4x \equiv 5 \pmod 9$.

→ Sol;

~~First, we find inverse of 3 by using Euclidean Algorithm as~~

~~$9 = 4 \times 1 + 5$~~

Multiplying both sides by 7, we get

$4x \times 7 = 5 \times 7 \pmod 9$

or, $28x = 35 \pmod 9$

Since, 28 is congruent to 1 modulo 9, we can simplify the equation to:

$x = 35 \pmod 9$

$x = 8$

Therefore, the solution to the congruence $4x = 5 \pmod 9$ is $x = 8$.

---

4. Determine whether the integers in each of following sequences are pairwise relatively prime.

a) 21, 34, 45

→ Sol;

Since, $\gcd(21, 34) = 1$

$\gcd(34, 45) = 1$

$\gcd(45, 21) = 3$

Therefore, the given number sequence 21, 34 and 45 are not pairwise relatively prime.

b) 17, 18, 23

→ Sol;

Since, $\gcd(17, 18) = 1$

$\gcd(18, 23) = 1$

$\gcd(23, 17) = 1$

DATE:

Therefore, the given sequences 17, 18 and 23 are pairwise relatively prime.

c) 11, 15, 19

→ Sol;

Since, $\gcd(11,15)=1$

$\gcd(15,19)=1$

$\gcd(19,11)=1$

Therefore, the given sequences 11, 15 and 19 are pairwise relatively prime.

d) 7, 8, 9, 11

→ Sol;

Since,

$\gcd(7,8)=1$

$\gcd(8,9)=1$

$\gcd(9,11)=1$

$\gcd(11,7)=1$

$\gcd(7,9)=1$

$\gcd(8,11)=1$

Therefore, the given sequence 7, 8, 9 and 11 are pairwise relatively prime.

5. What are the greatest common divisors and LCM of the following pairs of integers.

a) $2^2 \times 3^3 \times 5^5,\ 2^5 \times 3^3 \times 5^2$

→ Sol;

$\gcd = 2^2 \times 3^3 \times 5^2$,,

$LCM = 2^5 \times 3^3 \times 5^5$,,

DATE:

b) $2^2 \times 7, 5^3 \times 13$

→ Sol;

$gcd = 1$,,

$LCM = 2^2 \times 5^3 \times 7 \times 13$,,

c) $3^7 \times 5^3 \times 7^3, 2^1 \times 3^5 \times 5^9$

→ Sol;

$gcd = 3^5 \times 5^3$,,

$LCM = 2^1 \times 3^7 \times 5^9 \times 7^3$,,

6. Find gcd(1000, 625) and LCM(1000, 625) and verify that gcd(1000, 625) and LCM (1000, 625) = 1000 × 625.

→ Sol;

$1000 = 2 \times 2 \times 2 \times 5 \times 5 \times 5$

$625 = 5 \times 5 \times 5 \times 5$

∴ gcd(1000, 625) = 125,,

∴ LCM(1000, 625) = 5000,,

Now,

To verify that gcd(1000, 625) and LCM(1000, 625) = 1000 × 625,

gcd(1000, 625) = 125

LCM(1000, 625) = 5000

Multiplying 125 and 5000, we get

$125 \times 5000 = 625000$

Therefore, gcd(1000, 625) and LCM(1000, 625) are not equal to 1000 × 625.

DATE:

7. Find all solutions to the system of congruences.

$x \equiv 2 \pmod 3$

$x = 1 \pmod 4$

$x = 3 \pmod 5$

→ Soln:

Comparing with $x = a_n \pmod{m_n}$, we get

$a_1 = 2$, $a_2 = 1$ and $a_3 = 3$

$m_1 = 3$, $m_2 = 4$ and $m_3 = 5$

$M = m_1 * m_2 * m_3 = 3 * 4 * 5 = 60$

$M_1 = \frac{M}{m_1} = \frac{60}{3} = 20$

$M_2 = \frac{M}{m_2} = \frac{60}{4} = 15$

$M_3 = \frac{M}{m_3} = \frac{60}{5} = 12$

Now, we have to find M_1^{-1}, M_2^{-1} and M_3^{-1}.
In order to compute the multiplication inverse we have the relation as

$(M_i * M_i^{-1}) = 1 \pmod{m_i}$

Then,

$M_1 * M_1^{-1} = 1 \bmod m_1$

$\Rightarrow 20 * M_1^{-1} = 1 \bmod 3$

$\Rightarrow 20 * 2 = 1 \bmod 3$

$\therefore M_1^{-1} = 2$

Similarly,

$M_2 * M_2^{-1} = 1 \bmod m_2$

$\Rightarrow 15 * M_2^{-1} = 1 \bmod 4$

$\Rightarrow 15 * 3 = 1 \bmod 4$

$\therefore M_2^{-1} = 3$

And,

$M_3 * M_3^{-1} = 1 \bmod m_3$

DATE:

$\Rightarrow 12 * M_3^{-1} = 1 \mod 5$

$\Rightarrow 12 * 3 = 1 \mod 5$

$\therefore M_3^{-1} = 3$

Hence,

$x = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1}) \mod M$

$= (2*20*2 + 1*15*3 + 3*12*3) \mod 60$

$= (80 + 45 + 108) \mod 60$

$= 233 \mod 60$

$= 53$

8. Find all solutions to the system of congruences.

$x \equiv 1 (\mod 2)$

$x \equiv 2 (\mod 3)$

$x \equiv 3 (\mod 5)$

$x \equiv 4 (\mod 11)$

→ Sol:

Comparing with $x = a_n (\mod m_n)$, we get

$a_1 = 1, a_2 = 2, a_3 = 3$ and $a_4 = 4$

$m_1 = 2, m_2 = 3, m_3 = 5$ and $m_4 = 11$

$M = m_1 * m_2 * m_3 * m_4 = 2 * 3 * 5 * 11 = 330$

$M_1 = \frac{M}{m_1} = \frac{330}{2} = 165$

$M_2 = \frac{M}{m_2} = \frac{330}{3} = 110$

$M_3 = \frac{M}{m_3} = \frac{330}{5} = 66$

$M_4 = \frac{M}{m_4} = \frac{330}{11} = 30$

Now, we have to find $M_1^{-1}, M_2^{-1}, M_3^{-1}$ and M_4^{-1}.

In order to compute the multiplication inverse we have the relation as

$$(M_i * M_i^{-1}) = 1 \pmod{m_i}$$

Then,

$M_1 * M_1^{-1} = 1 \bmod m_1$

$\Rightarrow 165 * M_1^{-1} = 1 \bmod 2$

$\Rightarrow 165 * 1 = 1 \bmod 2$

$\therefore M_1^{-1} = 1$

Similarly,

$M_2 * M_2^{-1} = 1 \bmod m_2$

$\Rightarrow 110 * M_2^{-1} = 1 \bmod 3$

$\Rightarrow 110 * 2 = 1 \bmod 3$

$\therefore M_2^{-1} = 2$

And,

$M_3 * M_3^{-1} = 1 \bmod m_3$

$\Rightarrow 66 * M_3^{-1} = 1 \bmod 5$

$\Rightarrow 66 * 1 = 1 \bmod 5$

$\therefore M_3^{-1} = 1$

And,

$M_4 * M_4^{-1} = 1 \bmod m_4$

$\Rightarrow 30 * M_4^{-1} = 1 \bmod 11$

$\Rightarrow 30 * 7 = 1 \bmod 11$

$\therefore M_4^{-1} = 7$

Hence,

$X = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1} + a_4 M_4 M_4^{-1}) \bmod M$

$= (1 * 165 * 1 + 2 * 110 * 2 + 3 * 66 * 1 + 4 * 30 * 7) \bmod 330$

$= (165 + 440 + 198 + 840) \bmod 330$

$= 1643 \bmod 330$

$= 323$

DATE:

Find first five random number using linear congruential method with $X_0 = 29$, $a = 9$, $c = 49$ and $m = 100$.

Sol;

Here,

$X_0 = 29$, $a = 9$, $c = 49$ and $m = 100$

Then,

$X_1 = (a * X_0 + c) \bmod m$
$= (9 * 29 + 49) \bmod 100$
$= 310 \bmod 100$
$= 10$

$X_2 = (a * X_1 + c) \bmod m$
$= (9 * 10 + 49) \bmod 100$
$= 139 \bmod 100$
$= 39$

$X_3 = (a * X_2 + c) \bmod m$
$= (9 * 39 + 49) \bmod 100$
$= 400 \bmod 100$
$= 0$

$X_4 = (a * X_3 + c) \bmod m$
$= (9 * 0 + 49) \bmod 100$
$= 49 \bmod 100$
$= 49$

$X_5 = (a * X_4 + c) \bmod m$
$= (9 * 49 + 49) \bmod 100$
$= 490 \bmod 100$
$= 90$

Therefore, sequence of random number is 10, 39, 0, 49, 90, ...

DATE:

b) Find first three random number using linear congruential method with $X_0 = 37$, $a = 7$, $c = 49$ and $m = 100$.

→ Sol;

Here,

$X_0 = 37$, $a = 7$, $c = 49$ and $m = 100$

Then,

$X_1 = (a * X_0 + c) \bmod m$

$= (7 * 37 + 49) \bmod 100$

$= 308 \bmod 100$

$= 8$

$X_2 = (a * X_1 + c) \bmod m$

$= (7 * 8 + 49) \bmod 100$

$= 105 \bmod 100$

$= 5$

$X_3 = (a * X_2 + c) \bmod m$

$= (7 * 5 + 49) \bmod 100$

$= 84 \bmod 100$

$= 84$

Therefore, sequence of random number is 8, 5, 84, ...

10. Let $A = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ and $B = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix}$. Find

a) $A \vee B$ b) $A \wedge B$ c) $A \odot B$

→ Sol;

Here,

$$A = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

DATE:

$$B = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix}$$

$A \vee B = ?$

$A \wedge B = ?$

$A \odot B = ?$

Now,

$$A \vee B = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \vee \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 \vee 0 & 0 \vee 1 & 1 \vee 1 \\ 1 \vee 1 & 1 \vee 0 & 0 \vee 1 \\ 0 \vee 1 & 0 \vee 0 & 1 \vee 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$$

$$A \wedge B = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \wedge \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 \wedge 0 & 0 \wedge 1 & 1 \wedge 1 \\ 1 \wedge 1 & 1 \wedge 0 & 0 \wedge 1 \\ 0 \wedge 1 & 0 \wedge 0 & 1 \wedge 1 \end{bmatrix}$$

$$= \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$A \odot B = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \odot \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix}$$

DATE:

$$= \begin{bmatrix} (1\wedge 0)\vee(0\wedge 1)\vee(1\wedge 1) & (1\wedge 1)\vee(0\wedge 0)\vee(1\wedge 0) & (1\wedge 1)\vee(0\wedge 1)\vee(1\wedge 1) \\ (1\wedge 0)\vee(1\wedge 1)\vee(0\wedge 1) & (1\wedge 1)\vee(1\wedge 0)\vee(0\wedge 0) & (1\wedge 1)\vee(1\wedge 1)\vee(0\wedge 1) \\ (0\wedge 0)\vee(0\wedge 1)\vee(1\wedge 1) & (0\wedge 1)\vee(0\wedge 0)\vee(1\wedge 0) & (0\wedge 1)\vee(0\wedge 1)\vee(1\wedge 1) \end{bmatrix}$$

$$= \begin{bmatrix} 0\vee 0\vee 1 & 1\vee 0\vee 0 & 1\vee 0\vee 1 \\ 0\vee 1\vee 0 & 1\vee 0\vee 0 & 1\vee 1\vee 0 \\ 0\vee 0\vee 1 & 0\vee 0\vee 0 & 0\vee 0\vee 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$$

---

11. Find the Boolean product of A and B, where $A = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}$ and $B = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \\ 1 & 0 \end{bmatrix}$.

→ Soln;

Here,

$$A = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

$$B = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \\ 1 & 0 \end{bmatrix}$$

$A \odot B = ?$

Now,

DATE:

$$A \odot B = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix} \odot \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \\ 1 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} (1\wedge1)\vee(0\wedge1)\vee(0\wedge1)\vee(1\wedge1) & (1\wedge0)\vee(0\wedge1)\vee(0\wedge1)\vee(1\wedge0) \\ (0\wedge1)\vee(1\wedge0)\vee(0\wedge1)\vee(1\wedge1) & (0\wedge0)\vee(1\wedge1)\vee(0\wedge1)\vee(1\wedge0) \\ (1\wedge1)\vee(1\wedge0)\vee(1\wedge1)\vee(1\wedge1) & (1\wedge0)\vee(1\wedge1)\vee(1\wedge1)\vee(1\wedge0) \end{bmatrix}$$

$$= \begin{bmatrix} 1\vee0\vee0\vee1 & 0\vee0\vee0\vee0 \\ 0\vee0\vee0\vee1 & 0\vee1\vee0\vee0 \\ 1\vee0\vee1\vee1 & 0\vee1\vee1\vee0 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 \\ 1 & 1 \\ 1 & 1 \end{bmatrix}$$