Unit V

5 Introduction to Number Theory

5.1 : Binary Operations

Q.1 What are the two basic binary operations on the set of integers ? Write properties of these two operations.

Ans. : There are two basic binary operations (i) Addition denoted by '+' and (ii) Multiplication denoted by '.' on the set of integers Z. If $a, b \in Z$, then $a + b$ is called the **sum** and $a \cdot b$ or more simply written as ab is called the **product** of a nd b. The basic properties of these two operations are as given below :

A_1. **Closure for addition :** $a + b \in Z \ \forall \ a, b \in Z$.

A_2. **Commutativity of addition :** $a + b = b + a \ \forall \ a, b \in Z$.

A_3. **Associativity of addition :** $a + (b + c) = (a + b) + c \forall \ a, b, c \in Z$.

A_4. **Existence of identity for addition :** There exists a unique integer '0' such that

$$a + 0 = a = 0 + a \ \forall \ a \in Z.$$

This integer 0 is called the **additive identity.**

A_5. **Existence of additive inverse of each integer :** If $a \in Z$, then there exists a unique integer $-a \in Z$ such that $-a + a = 0 = a + (-a)$.

The integer - a is called the **negative** or the **additive inverse** of the integer a.

M_1. **Closure for multiplication :** $ab \in Z$ for all $a, b \in Z$.

M_2. **Commutativity of multiplication :** $ab = ba \ \forall \ a, b \in Z$.

M_3. **Associativity of multiplication :** $(ab)c = a(bc) \ \forall \ a, b, c \in Z$.

M_4. **Existence of identity for multiplication :** There exist a unique integer '1' such that,

$$1a = a = a1 \ \forall \ a \in Z.$$

The integer is called the **multiplicative** identity.

- **Difference of two integers :** The difference of two integers a and b denoted by 'a – b' is defined as,

$$a - b = a + (-b)$$

e.g. $a = 10, b = 3$

$\therefore \quad 10 - 3 = 10 + (-3) = 7$

5.2 : Order Relations

Q.2 What do you mean by order relations on the set of integers ? List properties of it.

Ans. : Order Relations on the set of integers

Definition : If $a, b \in Z$ and $a - b \in Z^+$, then we say that a is greater than b and write $a > b$. Alternatively we say that b is less than a and write $b < a$.

If $a < b$ or $a = b$, we write $a \leq b$ and if $a > b$ or $a = b$, we write $a \geq b$.

Obviously, a is positive iff $a > 0$ and a is negative iff $a < 0$. Also if $a \in Z$, then one and only one of the following is true :

$$a \in Z^+, a = 0, -a \in Z^+$$

i.e. $a > 0, a = 0, a < 0.$

Some important properties of the order relations on Z

1. If $a, b \in Z$, then one and only one of the following is true : $a > b$, $a = b$, $a < b$.
2. Transitivity of the order relations, if $a, b, c \in Z$, then,
   i) $a < b, b < c \Rightarrow a < c$ and ii) $a > b, b > c \Rightarrow a > c$
3. If $a, b, c \in Z$, then,
   i) $a < b \Rightarrow a + c < b + c$ and $a - c < b - c$
   ii) $a > b \Rightarrow a + c > b + c$ and $a - c > b - c$
4. If $a, b, c \in Z$, then,
   i) $a > b, c > 0 \Rightarrow ac > bc$ and ii) $a > b, c < 0 \Rightarrow ac < bc$
5. If $a \in Z, a \neq 0$, then $a^2 = a \cdot a > 0$.

Q.3 What is well ordering principle ? Explain with few examples.

Ans. : 1) Least integer in a subset of Z : Let S be a non empty subset of Z. If there exists an integer $m \in S$ such that $x \geq m$ for all $x \in S$ then m is said to be smallest or the least integer in S.

If there exists an integer $n \in S$ such that $x \leq n$ for all $x \in S$, then n is said to be the greatest integer in S.

2) **Well ordering principle :** The well ordering principle states that "every non empty subset of the set of positive integers has a least member."

Example :

i) If $Z^+ = \{1, 2, 3, \ldots\}$ then 1 is the smallest positive integer.

ii) If $S = \{10, 11, 12, \ldots, 100\}$ then 10 is the smallest positive integer.

Note : If $k \in Z^+$ then there exists no integer a such that $k < a < k + 1$.

Q.4 Write two porms of principle of mathematical induction.

Ans. : First Form : Let K be a subset of N such that i) $1 \in K$ and ii) $n \in K \Rightarrow n + 1 \in K$, then $K = N$.

Second Form : Let K be a subset of N such that i) $1 \in K$ and ii) $k \in K$ for all k satisfying $1 \leq k < n \Rightarrow n \in K$, then $K = N$.

5.3 : Division Algorithm

Q.5 Define a) Divisors b) Proper Divisor c) Improper divisors.

Ans. : Divisor : Let a, b be two integers and $a \neq 0$. If there exists an integer c such that $b = ac$, then we say that a divides **b or a is a divisor of b** or **a is a factor of b** or **b is a multiple of a.**

When a is a divisor of b, we write, "$a \mid b$". This is read as 'a is a divisor of b'. If a is a divisor of b, then b is a multiple of a and we also write it as $b = M(a)$. Here M(a) is read as '**integral multiple of a**'.

If a is not a divisor of b, then we write '$a \nmid b$' which is read as 'a is not a divisor of b'.

For example,

i) $3 \mid 18$ as $18 = 36$

ii) $(-5) \mid 30$ as $30 = (-5)(-6)$

iii) $a \mid 0$, for all $a \in Z$ and $a \neq 0$, since $0 = a \cdot 0$.

Thus 0 is a multiple of every integer or every non-zero integer a is a divisor of 0.

iv) $3 \nmid 5$ i.e. 3 is not a divisor of 5 because there exists no integer q such that $5 = 3q$.

Thus division is not everywhere defined in Z.

Improper divisors : For every integer $a \neq 0$, ± 1 and $\pm a$ are always divisors of a. These are called improper divisors of a.

Proper divisors : If a has any divisors other than these, then they are called **proper divisors** of a. For example the only divisors of 7 are ± 1 and ± 7 and so 7 has no proper divisors. On the other hand 8 possesses proper divisors. Besides ± 1 and ± 8, ± 2 and ± 4 are also divisors of 8 and these are proper divisors of 8.

Q.6 State and prove the division algorithm.

Ans. : The theorem known as division algorithm is of great importance in the development of number theory.

Theorem 1 If a is any integer and $b \neq 0$, then there exist unique integers q, r such that,

$$a = bq + r, \qquad \text{where } 0 \leq r < |b|$$

Proof : Consider the set $S = \{a - bx : x \in Z\}$. Since $a = a - b \cdot 0$ where $0 \in Z$, therefore at least $a \in S$ and thus S is not empty.

If $b < 0$ i.e., $b \leq -1$, then $b \cdot |a| \leq -|a| \leq a$

$\Rightarrow (a-b) \cdot |a| \geq 0$ i.e., $(a-b) \cdot |a|$ is non-negative.

Now $(a-b) \cdot |a| \in S$ because $|a| \in Z$

If $b < 0$, then S contains at least one non-negative integer i.e., $(a-b) \cdot |a|$.

If $b > 0$ i.e., if $b \geq 1$, then $b(-|a|) \leq -|a| \leq a$

$\Rightarrow a - b \cdot (-|a|) \geq 0$.

Now $a - b \cdot (-|a|) \in S$ because $-|a| \in Z$.

Therefore if $b > 0$, then S contains at least one non-negative integer i.e. $a - b \cdot (-|a|)$

Thus whether $b > 0$ or $b < 0$, the set S always contains non-negative integers. Therefore by the well-ordering principle the non-empty subset of S consisting of non-negative integers has a least number. Let $r = a - bq$ where $q \in Z$, be the smallest non-negative integer belonging to S. Since r is non-negative, therefore $0 \leq r$. We claim that $r < |b|$.

To fulfil our claim first we show that $r - |b| \in S$ whether $b > 0$ or $b < 0$.

If $b > 0$, then $r - |b| = r - b = a - bq - b = a - (q + 1)b \in S$ since $(q + 1) \in Z$. If $b < 0$, then

$r - |b| = r - (-b) = a - bq + b = a - (q - 1)\, b \in S$ since $(q - 1) \in Z$.

Now $b \neq 0$. Therefore $r - |b| < r$. If $r \geq |b|$, then $r - |b| \geq 0$ i.e., $r - |b|$ is non-negative. Thus if $r \geq |b|$, them $r - |b|$ is a non-negative integer

belonging to S and $r - |b| < r$. This is against the choice of r as the smallest non-negative integer $\in$ S. Hence we must have $r < |b|$.

Thus there exist integers q and r such that,

$$r = a - bq$$

i.e., $$a = bq + r \text{ and } 0 \leq r < |b|$$

Now to show that the integers q, r are unique. Suppose we should find another pair q' and r' such that

$$a = bq' + r',\ 0 \leq r' < |b|$$

The $bq' + r' = bq + r \Rightarrow b(q' - q) = r - r'$

$\Rightarrow b|(r - r')$

Without any loss of generality we can assume that $r \geq r'$.

- Then $0 \leq r < |b|$ and $0 \leq r' < |b'| \Rightarrow 0 \leq r - r' < |b|$. Therefore r is a divisor of $r - r'$ is positive only if $r - r' = 0$. Therefore $r' = r$.

$\therefore$ Putting $r = r'$, we get $bq' + r' = bq + r \Rightarrow bq' = bq \Rightarrow q = q'$. Thus $r = r'$ and $q = q'$. Hence q and r are unique. Hence the proof.

5.4 : Greatest Common Divisor

Q.7 Define : a) Greatest common divisor
b) Greatest common divisor of more than two integers.

Ans. : Let a and b be two integers not both zero (at least one of them is non zero). Then the Greatest Common Division (GCD) of a and b is a positive integer d such that,

i) $d|a$ and $d|b$ i.e. d is a common divisor of a and b and

ii) If an integer c, $c|a$ and $c|b$ then $c|d$ i.e. every common divisor of a and b is a divisor of d.

If d is the greatest common divisor of a and b then it is denoted by $d = (a, b)$. It is also known as the Highest Common Factor (HCF).

Example :

1, 3, 5 and 15 are common divisors of 45 and 60. Out of these each of 1, 3 and 5 is a divisor of 15.

$\therefore$ $\gcd(45, 60) = 15$

Note : $(a, b) = (-a, b) = (a, -b)$

Greatest Common Divisor of more than two Integers

Definition : Let $\{a_1, a_2, \ldots, a_n\}$ be a finite set of integers, not all zero. If there exists a positive integer d such that

i) d is a common divisor of $a_1, a_2, \ldots, a_n$ and ii) each common divisor of $a_1, a_2, \ldots, a_n$ is also a divisor of d, then d is called the greatest common divisor of $a_1, a_2, \ldots, a_n$. Symbolically, we write

$$d = (a_1, a_2, \ldots, a_n)$$

For example, $(20, 60, 45, -30) = 5$

Important Theorems to be Remembered

I) Existence and uniqueness of Greatest Common Divisor Theorem : Every pair of integers a and b, not both zero, has a unique greatest common divisor (a, b) which can be expressed in the form

$(a, b) = xa + yb$, for some integers x and y.

II) Construction of G.C.D. by Repeated use of Division Algorithm.

If $a, b \in Z$, $b \neq 0$ and $a = bq + r$, $0 \leq r \leq |b|$ then $(a, b) = (b, r)$.

III) Theorem : If $a, b \in Z$, $b \neq 0$ and $a = bq + r$, $0 \leq r < |b|$ then $(a, b) = (b, r)$.

Q.8 By using the Euclidean algorithm, find the greatest common divisor d of the numbers 1109 and 4999 and then find integers x and y to satisfy $d = 1109x + 4999y$.

Ans. : By repeatedly applying the process of division algorithm, we get,

$4999 = (1109) \cdot 4 + 563,$ ...(Q.8.1)

$1109 = (563) \cdot 1 + 546,$ ...(Q.8.2)

$563 = (546) \cdot 1 + 17,$ ...(Q.8.3)

$546 = (17) \cdot 32 + 2,$ ...(Q.8.4)

$17 = (2) \cdot 8 + 1,$ ...(Q.8.5)

$2 = (1) \cdot 2 + 0.$ ...(Q.8.6)

Hence (1109, 4999) = the last non-zero remainder in the above repeated divisions = 1.

Now substituting backwords, we have

$1 = 17 - (2) \cdot 8$

$= 17 - [546 - (17) \cdot 32] \cdot 8,$ [by equation(Q.8.5)]

$= (17) \cdot 257 - 546 \cdot 8$ substituting for 2 from equation(Q.8.4)

$= [563 - (546) \cdot 1] \cdot 257 - 546 \cdot 8,$

substituting for 17 from equation(Q.8.3)

$= 563 \cdot 257 - 546 \cdot 265$

$= 563 \cdot 257 - [1109 - (563) \cdot 1] \cdot 265,$

substituting for 546 from equation (Q.8.2)

$= 563 \cdot 522 - 1109 \cdot 265$

$= [4999 - (1109) \cdot 4] \cdot 522 - 1109 \cdot 265,$

substituting for 563 from equation (Q.8.1)

$= 4999 \cdot 522 - 1109 \cdot 2353$

Hence $(1109, 4999) = 1 = 1109 \cdot (-2353) + 4999 \cdot (522)$

$= 1109x + 4999y,$ where $x = -2353, y = 522.$

Q.9 Find the G.C.D. of 275 and 200 and express it in the form $m \cdot 275 + n \cdot 200$.

Ans. : By repeatedly applying the process of division algorithm, we get,

$275 = (200) \cdot 1 + 75,$ ...(Q.9.1)

$200 = (75) \cdot 2 + 50,$ ...(Q.9.2)

$75 = (50) \cdot 1 + 25,$ ...(Q.9.3)

$50 = (25) \cdot 2 + 0,$ ...(Q.9.4)

Hence (275, 200) = the last non-zero remainder in the above repeated divisions = 25.

Now substituting backwords, we have,

$25 = 75 - (50) \cdot 1$ [by equation(Q.9.3)]

$= 75 - [200 - (75) \cdot 2] \cdot 1,$ substituting for 50 from equation(Q.9.2)

$= 75 \cdot 3 - 200 \cdot 1$

$= [275 - (200) \cdot 1] \cdot 3 - 200 \cdot 1,$

substituting for 75 from equation(Q.9.1)

$= 275 \cdot 3 - 200 \cdot 4$

$= (3) \cdot 275 + (-4) \cdot 200$

Hence $(275, 200) = 25 = (3) \cdot 275 + (-4) \cdot 200$ so that $m = 3, n = -4.$

Q.10 If $a = -427$, $b = 616$, find (a, b) and express it in the form $(a, b) = ax + by$.

Ans. : Since $(a, b) = (|a|, |b|)$, therefore in order to find $(-427, 616)$, we shall find (427, 616).

We construct Euclidean algorithm for 427, 616 :

$$616 = (427) \cdot 1 + 189, \quad \ldots(Q.10.1)$$

$$427 = (189) \cdot 2 + 49, \quad \ldots(Q.10.2)$$

$$189 = (49) \cdot 3 + 42, \quad \ldots(Q.10.3)$$

$$49 = (42) \cdot 1 + 7, \quad \ldots(Q.10.4)$$

$$42 = (7) \cdot 6 + 0. \quad \ldots(Q.10.5)$$

Hence (427, 616) = the last non-zero remainder in the above repeated divisions = 7.

Now substituting backwords, we have

$$7 = 49 - (42) \cdot 1 \quad \text{[by equation(Q.10.4)]}$$

$$= 49 - [189 - (49) \cdot 3] \cdot 1 \quad \text{[by equation(Q.10.3)]}$$

$$= (49) \cdot 4 - 189$$

$$= [427 - (189) \cdot 2] \cdot 4 - 189 \quad \text{[by equation(Q.10.2)]}$$

$$= (427) \cdot 4 - (189) \cdot 9$$

$$= (427) \cdot 4 - [616 - (427) \cdot 1] \cdot 9$$

$$= (427) \cdot 13 + (616) \cdot (9)$$

Hence $(-427, 616) = 7 = (-427) \cdot (-13) + (616) \cdot (-9)$

$= ax + by,$ where $x = -13, y = -9.$

Q.11 Write short note on Extended Euclidean Algorithm.

Ans. : Used to find GCD, Bezout's coefficients s and t and the multiplicative inverse of an integer.

- Algorithm : (Find multiplicative inverse of x with respect to m)

1. Let $r_1 = x$ $r_2 = m$, $s_1 = 1$, $s_2 = 0$ $t_1 = 0$, $t_2 = 1$ and r, s, t be integers
2. While (r_2 != 0)
3. do

i. $r = r_1 - q \cdot r_2$;

ii. $s = s_1 - q \cdot s_2$;

iii. $t = t_1 - q \cdot t_2$;

iv. $r_1 = r_2$; $r_2 = r$

v. $s_1 = s_2$; $s_2 = s$

vi. $t_1 = t_2$; $t_2 = t$

4. Done

5. GCD = r_1; Bezout's coefficient = s_1 and t_1, and Multiplicative inverse of $x = r_1$ with respect to $m = r_2$ is s_1 or vice versa Multiplicative inverse of $m = r_2$ with respect to $x = r_1$ is t_1.

Example - Extended Euclidean Algorithm

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
0	33	86	33	1	0	1	0	1	0
2	86	33	20	0	1	–2	1	0	1
1	33	20	13	1	–2	3	0	1	–1
1	20	13	7	–2	3	–5	1	–1	2
1	13	7	6	3	–5	8	–1	2	–3
1	7	6	1	–5	8	–13	2	–3	5
6	6	1	0	8	–13	86	–3	5	–33
--	1 = GCD	0	--	–13 = s	86	--	5 = t	–33	--

Multiplicative Inverse of 33 is – 13 ≡ 73 (mod 86) and Multiplicative Inverse of 86 is 5 (mod 33)

Bezout's Identity is
1 = – 13 * 33 + 5 * 86

Example - Extended Euclidean Algorithm

q	r_1	r_2	r	s_1	s_2	s
0	33	86	33	1	0	1
2	86	33	20	0	1	–2
1	33	20	13	1	–2	3
1	20	13	7	–2	3	–5
1	13	7	6	3	–5	8
1	7	6	1	–5	8	–13
6	6	1	0	8	–13	86
--	1 = GCD	0	--	–13 = s	86	--

If the intension is to find multiplicative inverse, then you need to find only variable s which gives you inverse of r_1 with respect to r_2 (modulus m), no need to do calculations for t.

Multiplicative Inverse of 33 (r_1) is –13 ≡ 73 [mod 86 (r_2)]

Q.12 Define a) Relatively prime integers, b) Least common multiple, c) Prime integers, d) Composite integers.

Ans. : a) Relatively prime integers : Two integers a and b are said to be relatively prime if their greatest common divisor is 1 i.e., if $(a, b) = 1$. If $(a, b) = 1$, we also say that a and b are co-prime or prime to each other. If a and b are relatively prime, then a and b have no common factors except 1 or – 1. For example,

i) 14, – 9 are relatively prime integers since $(14, -9) = 1$.

ii) 18, 14 are not relatively prime integers since $(18, 14) = 2$.

b) Least common multiple : Let a and b be two non-zero integers. The Least Common Multiple (L.C.M.) of a and b is the unique positive integer m such that

i) $a \mid m$, $b \mid m$ and ii) $a \mid s$, $b \mid s \Rightarrow m \mid s$

Notation : L.C.M. of a and b is denoted by [a, b]

Example : i) [12, 18] = 36, ii) [10, 25] = 50

c) Prime integers : A non-zero integer p is called a **prime** if it is neither 1 nor – 1 and if its only divisors are 1, – 1, p, – p.

For example,

i) The integers 5 and – 11 are primes, while $12 = 4 \times 3$ and $-36 = 3 \cdot (-12)$ are not primes.

ii) The first 10 positive primes are,

2, 3, 5, 7, 11, 13, 17, 19, 23, 29.

Note (1) : By definition, 1 is not prime. It is obvious that – p is a prime iff p is a prime.

Note (2) : 2 is the only even integer which is a prime. Every other even integer has 2 as a factor and so it cannot be a prime. Therefore if p is a prime and $p \neq 2$, then p must be an odd integer.

Note (3) : If p is a prime and a is any integer, then either $p \mid a$ or $(p, a) = 1$.

d) Composite integers : If an integer a can be written as $a = bc$, where b and c are integers such that $|b| > 1$ and $|c| > 1$, then a is called a **composite integer.**

For example $6 = 2 \cdot 3$ where $|2| > 1$ and $|3| > 1$. Therefore 6 is a **composite integer.**

Every integer $a \neq 0, \pm 1$ is either a prime or a composite.

If a is a positive integer, then a is a composite iff there exist two positive integers b and c such that,

$$a = bc, \quad \text{where } 1 < b < a, 1 < c < a.$$

Important to be Remembered

- **Theorem :** Two integers a and b are relatively prime if and only if we can find integers x and y such that $ax + by = 1$
- **Euclid's Lemma :** If p is a prime number and a, b are any integers then $p \mid ab \Rightarrow p \mid a$ or $p \mid b$.
- **Corollary :** If p is a prime and $a, b \in Z$ are such that $0 < a < p$, $0 < b < p$, then p cannot be a divisor of ab.
- **Theorem :** If a prime number p divides the product $a_1, a_2, \ldots, a_n$ of certain integers, then p must divide at least one of $a_1, a_2, \ldots, a_n$.
- **Theorem :** If a is a possible integer greater than 1 then a has a prime factor.
- **Theorem :** The fundamental theorem of **arithmetic** or the **Unique Factorisation theorem.** Every positive integer $a > 1$ can be expressed uniquely as a product of positive primes.

Q.13 Find the G.C.D. and the L.C.M. of a = 5040, b = 14850 by writing each of the numbers a and b in prime factorization canonical form.

Ans. : We have $a = 2^4 \cdot 3^2 \cdot 5^1 \cdot 7^1$ and $b = 2^1 \cdot 3^3 \cdot 5^2 \cdot (11)^1$

$\therefore$ G.C.D. of a and b i.e., $(a, b) = 2^1 \cdot 3^2 \cdot 5^1 = 90$.

Also L.C.M. of a and b i.e. $[a, b] = 2^4 \cdot 3^3 \cdot 5^2 \cdot 7^1 \cdot (11)^1 = 831600$

Q.14 Find the number of distinct positive integral divisors and their sum for the integer 56700.

Solution : Expressing in prime factorization canonical form, we have

$$\begin{aligned} 56700 &= 2 \times 28350 = 2^2 \times 14175 \\ &= 2^2 \times 3 \times 4725 = 2^2 \times 3^2 \times 1575 \\ &= 2^2 \times 3^3 \times 525 = 2^2 \times 3^4 \times 175 \\ &= 2^2 \times 3^4 \times 5 \times 35 = 2^2 \times 3^4 \times 5^2 \times 7^1, \end{aligned}$$

where $p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7$ and

$\alpha_1 = 2, \alpha_2 = 4, \alpha_3 = 2, \alpha_4 = 1.$

$\therefore$ $T(56700)$ = The number of distinct positive integral divisors of 56700

$= (\alpha_1+1)(\alpha_2+1)(\alpha_3+1)(\alpha_4+1)$

$= (2+1)(4+1)(2+1)(1+1) = 3\times5\times3\times2$

$= 90.$

Also $\sigma(56700)$ = The sum of all the distinct positive integral divisors of 56700

$$= \frac{2^{2+1}-1}{2-1}\cdot\frac{3^{4+1}-1}{3-1}\cdot\frac{5^{2+1}-1}{5-1}\cdot\frac{7^{1+1}-1}{7-1}$$

$$= \frac{2^3-1}{1}\cdot\frac{3^5-1}{2}\cdot\frac{5^3-1}{4}\cdot\frac{7^2-1}{6}$$

$$= 7\times121\times31\times8 = 210056.$$

Q.15 If $p = 2^n - 1$ is a prime, prove that n is a prime.

Solution : Let n be not a prime. Then there exist positive integers r and s such that

$n = rs$ where $1 < r < n,\ 1 < s < n.$

$\therefore$ $p = 2^n - 1 = 2^{rs} - 1 = (2^r)^s - 1$

$= a^s - 1$ where $a = 2^r$

$= (a-1)(a^{s-1} + a^{s-2} + \ldots + a + 1)$ ...(Q.14.1)

Now $a - 1 > 1$ because $a = 2^r > 2$ Also $a - 1 = 2^r - 1 < p$ because $p = (2^r)^s - 1$. Thus $a - 1$ is a positive integer such that $1 < a - 1 < p$ and from (1), $a - 1$ is a divisor of p.

Hence p is not a prime. But this is a contradiction.

Hence n must be a prime.

Note : The converse of the above statement is not true. For example if we taken $n = 11$, then n is prime. But $2^{11} - 1 = 2047 = 23\times89$ and thus $2^{11} - 1$ is not prime. Hence n is prime does not necessarily imply that $2^n - 1$ is prime.

Q.16 Define Mersenne Numbers.

Ans. : The members of the form $M_n = 2^n - 1$, where n is a prime are known as **Mersenne numbers**. All the Mersenne numbers are not prime. For example $M_{11} = 2^{11} - 1 = 2047$ is composite because 23 is a divisor of 2047.

Q.17 Prove that the product of r consecutive natural numbers is divisible by r !.

Ans. : Let $x \in N$ and x, x+1, x+2, ..., x+r – 1 be r consecutive natural numbers.

$$P = \text{Product of these r consecutive natural numbers}$$

$$= x(x+1)(x+2)\ldots(x+r-1)$$

$$= \frac{(x+r-1)!}{(x-1)!}$$

We have to prove that P is divisible by r ! i.e. we have to prove that $\frac{(x+r-1)!}{(x-1)!r!}$ is an integer.

For this we have to show that the highest power of every prime factor p contained in the product (x – 1) ! r ! is not greater than the highest power of p in (x+r–1) !

Now we know that if a, b are any real numbers, then

$$I(a+b) \geq I(a) + I(b),$$

Where I(a)

stands for the integral part of a.

$$\therefore I\left(\frac{x+r-1}{p}\right) \geq I\left(\frac{x-1}{p}\right) + I\left(\frac{r}{p}\right),$$

$$I\left(\frac{x+r-1}{p^2}\right) \geq I\left(\frac{x-1}{p^2}\right) + I\left(\frac{r}{p^2}\right),$$

$$I\left(\frac{x+r-1}{p^3}\right) \geq I\left(\frac{x-1}{p^3}\right) + I\left(\frac{r}{p^3}\right),$$

... ...

... ...

Adding the above inequalities, we have

$$I\left(\frac{x+r-1}{p}\right)+I\left(\frac{x+r-1}{p^2}\right)+I\left(\frac{x+r-1}{p^3}\right)+\ldots$$

$$\geq \left[I\left(\frac{x-1}{p}\right)+I\left(\frac{x-1}{p^2}\right)+\ldots\right]+\left[I\left(\frac{r}{p}\right)+I\left(\frac{r}{p^2}\right)+\ldots\right]$$

$\therefore$ The higest power of p in $(x + r - 1)\,! \geq$ the highest power of p in the product $(x-1)\,!\, r\,!$

Hence $(x - 1)\,!\, r\,!$ is a divisor of $(x + r - 1)\,!$ and consequently $r\,!$ is a divisor of
$x(x + 1)\ldots (x + 2)\ldots((x + r - 1)$.

Note : From the above result we can immediately deduce that the product of any r consecutive integers is divisible by r !

Q.18 If n > 2, show that $n^5 - 5n^3 + 4n$ divisible by 120.

Solution : We have $n^5 - 5n^3 + 4n = n(n^4 - 5n^2 + 4)$

$$= n(n^2 - 1)(n^2 - 4)$$

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

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

Thus if $n > 2$, then $n^5 - 5n^3 + 4n$ has been expressed as a product of five consecutive natural numbers and so it is divisible by 5 ! i.e., 120.

Q.19 Write short note on congruence of integers.

Ans. : Definition : Let m be any positive integer i.e. $m > 0$. Then an integer 'a' is said to be congruent to another integer b modulo m if $m \mid (a - b)$ i.e. if m is a divisior of $(a - b)$.

Symbolically we write

$$a \equiv b \pmod{m}.$$

It will be read as "a is congruent to b modulo m".

Thus $a \equiv b \pmod{m}$ iff $a - b = km$ ffor some integer k i.e., iff $a - b$ is a mulitple of m.

If m is not a divisor of a – b, then say that 'a is not congruent to b modulo m' and we write $a \not\equiv b \pmod{m}$.

For example :

$89 \equiv 25 \pmod 4$ since $89 - 25 = 64$ and $4 \mid 64$

$25 \equiv 1 \pmod 4$ since $25 - 1 = 24$ and $4 \mid 24$

$153 \equiv -7 \pmod 8$ since $153 - (-7) = 160$ and $8 \mid 160$

$13 \equiv 3 \pmod 5$ since $13 - 3 = 10$ and $5 \mid 10$.

But $24 \not\equiv 3 \pmod 5$ since $24 - 3 = 21$ and 5 is not a divisor of 21.

Also note that $m \mid a \Leftrightarrow a \equiv 0 \pmod m$.

Q.20 Prove that 'the relation' congruence modulo m is on equivalence relation in the set of integers.

Ans. : Theorem 1 : The relation "congruence modulo m" is an equivalence relation in the set of integers.

Proof : Let Z be the set integers. If m is any fixed positive integer, then we say that $a \equiv b \pmod m$ if $m \mid (a - b)$. We shall show that this defines an equivalence realtion on the set Z.

Reflexivity : Let a be any integer. Then $a - a = 0$ and $m \mid 0$.

Thus $a \equiv a \pmod m$ $\forall$ $a \in Z$. Therefore the relation is reflexive.

Symmetry : Let $a, b \in Z$ be such that $a \equiv b \pmod m$. Then we have

$m \mid (a - b) \Rightarrow a - b = km$ for some $k \in Z$

$\Rightarrow b - a = (-k)\, m$ where $-k \in Z$

$\Rightarrow m \mid (b - a) \Rightarrow b \equiv a \pmod m$

Thus $a \equiv b \pmod m \Rightarrow b \equiv a \pmod m$ and therefore the relation is symmetric.

Transitivity : Let $a, b, c \in Z$ be such that $a \equiv b \pmod m$, $b \equiv c \pmod m$. Then we have,

$m \mid (a - b)$ and $m \mid (b - c)$

$\Rightarrow m \mid \{(a - b) + (b - c)\} \Rightarrow m \mid (a - c)$

$\Rightarrow a \equiv c \pmod m$

Thus $a \equiv b \pmod m$ and $b \equiv c \pmod m \Rightarrow a \equiv c \pmod m$. Therefore the relation is transitive.

Hence congruence modulo m is an equivalence relation on Z.

Q.21 Prove that if $a \equiv b \pmod m$, then, for all $x \in Z$, $a + x \equiv b + x \pmod m$ and $ax = bx \pmod m$.

Ans. : We have $a \equiv b \pmod m \Rightarrow m \mid (a-b)$

$\Rightarrow m \mid \{(a+x)-(b+x)\} \quad \forall x \in Z$

$\Rightarrow a + x \equiv b + x \pmod m \quad \forall x \in Z$

Similarly, $a \equiv b \pmod m \Rightarrow m \mid (a - b)$

$\Rightarrow m \mid x(a-b)$ for all $x \in Z$

$\Rightarrow m \mid (ax-bx) \quad \forall x \in Z$

$\Rightarrow ax \equiv bx \pmod m \quad \forall x \in Z.$

Q.22 Prove that if $a \equiv b \pmod m$ and $c \equiv d \pmod m$, then $a + c \equiv b + d \pmod m$,
$a - c \equiv b - d \pmod m$, $ac \equiv bd \pmod m$.

Ans. : We have ,

$$a \equiv b \pmod m \Rightarrow m \mid (a - b)$$

and $$c \equiv d \pmod m \Rightarrow m \mid (c - d)$$

Now $m \mid (a - b)$ and $m \mid (c - d)$

$\Rightarrow m \mid \{(a - b) + (c - d)\} \Rightarrow m \mid \{(a + c) - (b + d)\}$

$\Rightarrow a + c \equiv b + d \pmod m$

Similarly $m \mid (a - b)$ and $m \mid (c - d)$

$\Rightarrow m \mid \{(a - b) - (c - d) \Rightarrow m \mid \{(a - c) - (b - d)\}$

$\Rightarrow a - c \equiv b - d \pmod m$.

Finally $m \mid (a - b)$ and $m \mid (a - b)$

$\Rightarrow m \mid \{c (a - b) + b (c - d)\} \Rightarrow m \mid (ac - bd)$

Q.23 If $a \equiv b \pmod m$ and m_1 is a positive divisor of m, then $a \equiv b \pmod{m_1}$.

Ans. : If m_1 is a positive divisor of m, then $m = m_1 q_1$ for some $q_1 \in Z^+$.

Now $$a \equiv b \pmod m \; m \mid (a - b)$$

$\Rightarrow$ $a - b = q_2 m$ for some $q_2 \in Z$

$\Rightarrow$ $a - b = q_2 (m_1 q_1) = m_1 (q_1 q_2)$ where $q_1 q_2 \in Z$

$\Rightarrow m_1 \mid (a - b) \Rightarrow a \equiv b \pmod{m_1}$

5.5 : Residue Classes

Important Points to Remember

Residue classes : Definition : We know that if m is a fixed positive integer, then 'congruence modulo m' is an equivalence relation on the set of integers Z. Consequently it partitions Z into a collection of mutually disjoint equivalence classes. These equivalence classes are called **'residue classes modulo m'.**

We shall denote the set of all residue classes of integers modulo m by $\bar{Z}_m$ or by Z/(m). It is also called the set of integers modulo m.

) Let m be a fixed positive integer and

$$S = \{0, 1, 2, \ldots. m - 1\}$$

Then no two integers of S are congruent modulo m to each other and every $x \in Z$ is congruent modulo m to one of the integers of S.

3) **Euler's ϕ Function : Definition :** The Euler ϕ-function is the function $\phi: Z^+ \to Z^+$ defined as follows :

i) $\phi(1) = 1$ and

ii) for n' $(> 1) \in Z^+$, (ϕ) n = The number of positive integers less than n and relatively prime to n.

4) **Theorem 1 :** If m and n are relatively prime positive integers i.e. (m, n) = 1 then,

$\phi(m, n) = \phi(m) \cdot \phi(n)$

5) **Theorem 2 :** If $n > 1$ and $p_1, p_2, \ldots, p_m$ are the distinct prime factors of n, then

$$\phi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots\left(1-\frac{1}{p_m}\right)$$

6) **Theorem 3 :** Fermat's Theorem. If p is a positive prime and a is any integer such that p is not a divisor of a so that (a, p) =1, then

$$a^{p-1} \equiv (\text{mod } p)$$

7) **Corollary :** If p is a positive prime and a is any integer, then $a^p \equiv a \pmod p$ i.e., (p) $a^p - a$ is a multiple of p.

8) **Theorem 4 : Euler's theorem :** If m is a positive integer and a is any integer such that (a, m) = 1, then $\alpha^{\phi(m)} \equiv 1 \pmod m$.

9) **Corollary :** Fermat's t[illegible]s a corollary of Euler's theorem. If in Euler's theorem [illegible]n = p where p is a prime, then

$\phi(n$ [illegible] $p-1$

∴ The result $a^{\phi(m)} \equiv 1 \pmod{m}$ takes the form

$a^{p-1} \equiv 1 \pmod{p}$, which is Fermat's theorem.

10) Theorem 5 : Wilson's theorem. If p is a positive prime then $(p-1)! + 1 \equiv 0 \pmod{p}$ i.e., $(p-1)! + 1$ is a multiple of p.

11) Fermat's little Thm : Fermat's little theorem states that if p is a prime number, then for any integer x, the number $x^p - x$ is an integer multiple of p. In the notation of modular arithmetic, this is expressed as

$x_p \equiv x \pmod{p}$ [Example $8^{13} \equiv 8 \bmod 13$]

- If a is not divisible by p, Fermat's little theorem is equivalent to the statement that $a^{p-1} - 1$ is an integer multiple of p, or in symbols :

$x^{p-1} \equiv 1 \pmod{p}$ [Example $40^{12} \equiv 1 \bmod 13$]

Example $87^{25} \bmod 7 \equiv (87^{6*4+1} \bmod 7) \equiv (87^6 \bmod 7)^4 * (87 \bmod 7) \equiv 3$

12) Chinese Remain der Thm : Statement : Let $n_1, n_2, n_3, \ldots, n_r$ be positive integers such that gcd $(n_i, n_j) = 1$ for $i \neq j$. The system of linear congruences

$$x \equiv a_1 \pmod{n_1}$$
$$x \equiv a_2 \pmod{n_2}$$
$$x \equiv a_3 \pmod{n_3}$$
$$\vdots \quad \vdots$$
$$x \equiv a_r \pmod{n_r}$$

has a simultaneous solution, which is unique modulo the integer $n_1 n_2 n_3 \ldots n_r$.

Procedure to solve examples :

Consider $n = n_1 n_2 n_3 \ldots n_r$

For each $k = 1, 2, 3, \ldots r$, Let

$$N_k = \frac{n}{n_k} = n_1 n_2 \ldots n_{k-1} n_{k+1} \ldots n_r$$

Solve $N_k x \equiv 1 \pmod{n_k}$ and call the unique solution x_k.

Now $\bar{x} = a_1 N_1 x_1 + a_2 N_2 x_2 + \ldots + a_r N_r x_r$

Therefore $\bar{x} \equiv x' \pmod{n}$ where $n \mid (\bar{x} - x')$

Q.24 Find the number of positive integers < 3600 that are relatively prime to 3600.

Ans. : We have to find $\phi(3600)$.

We shall first express 3600 in canonical form

We have $3600 = 2^4 \times 3^2 \times 5^2$

$$\therefore \quad \phi(3600) = \phi(2^4 \times 3^2 \times 5^2) = \phi(2^4) \cdot \phi(3^2) \cdot \phi(5^2)$$

$$= 2^4\left(1-\frac{1}{2}\right) \cdot 3^2\left(1-\frac{1}{3}\right) \cdot 5^2\left(1-\frac{1}{5}\right)$$

$$= 2^4 \cdot 3^2 \cdot 5^2\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)$$

$$= 3600 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 960$$

Q.25 Solve $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$, $x \equiv 2 \pmod 7$.

Ans. : We have $a_1 = 2$, $a_2 = 3$, $a_3 = 2$ and $n_1 = 3$, $n_2 = 5$ and $n_3 = 7$.

n_1, n_2 and n_3 are relatively primes

$$\therefore \quad n = n_1 \cdot n_2 \cdot n_3 = 3 \cdot 5 \cdot 7 = 105$$

and $$N_1 = \frac{n}{n_1} = \frac{3 \cdot 5 \cdot 7}{3} = 35, \quad N_2 = \frac{n}{n_2} = 3 \times 7 = 21$$

$$N_3 = \frac{n}{n_3} = 3.5 = 15$$

Now, Linear congruences are

$$N_1 x \equiv 1 \pmod{n_1}$$

$35 x \equiv 1 \pmod 3$, $21 x \equiv 1 \pmod 5$ and $15 x \equiv 1 \pmod 7$

These equations are satisfied by $x_1 = 2$, $x_2 = 1$, $x_3 = 1$ respectively

Therefore, the solution of the system is given by

$$\bar{x} = a_1 N_1 x_1 + a_2 N_2 x_2 + a_3 N_3 x_3$$

$$\bar{x} = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 233$$

Hence $$\bar{x} \equiv x' \pmod n$$

$$233 \equiv x' \pmod{105}$$

$$233 \equiv 23 \pmod{105}$$

This is the required unique solution.

END...