Chapter 1

PRELIMINARIES

1. **Concept of Divisibility:** A non-zero integer '*t*' is said to be a divisor of an integer '*s*' if there is an integer *u* such that $s = tu$. In this case we write *t*|*s*.

Example :

(*i*) 6|12 as 12 can be written as 12 = 6.2

So 6 divides 12

(*ii*) $5 \nmid 7$, since there is no *u*, s.t. 7 = 5*u*. Hence 5 does not divide 7.

2. **Prime Number :** A prime number is a positive integer greater than 1 whose only positive divisors are 1 and itself. e.g. 17, 13, 11 etc.

3. **Division Algorithm :** Let '*a*' and '*b*' integers with *b* > 0. Then there exist unique integer is *q* and *r* with the property that $a = bq + r$ where $0 \le r < b$, *q* is called the quotient and *r* is remainder.

e.g. for *a* = 17 and *b* = 5 division algorithm gives 17 = 5. 3 + 2

for *a* = –23, *b* = 6, –23 = 6(–4) + 1

4. **G.C.D. (Greatest Common Divisor):** The greatest common divisor of two non-zero integers '*a*' and '*b*' is the largest of all common divisors of *a* and *b*. We denote this integer by gcd(*a*, *b*)

Remarks : If $a, b \in \mathbb{Z} - \{0\}$, then there exist $x, y \in \mathbb{Z}$ such that $\gcd(a, b) = ax + by$.

Example :

(*i*) *g.c.d.* (5, 12) = 1, since '1' is the only number which divides 5 and 12 both.

(*ii*) *g.c.d.* (4, 12) = 4 is greatest common divisor as 4|4 and 4|12

(*iii*) *g.c.d.* (10, 25) = 5 as 5|10 and 5|25 but no other number divisors of both which is also greater than 5.

SOLVED EXAMPLES

(i). What is the smallest positive positive integer in the set $\{24x + 60y + 2000z \mid x, y, z \in \mathbb{Z}\}$

(a) 2 (b) 4 (c) 6 (d) 24

[CSIR-NET-2013-(II)]

Soln. $\gcd(24, 60, 2000) = 4$

Hence, correct option is (b).

(ii). For positive integer *m* and *n*. Let $F_n = 2^{2^n} + 1$ and $G_m = 2^{2^m} - 1$. Which of the following statement are true?

(a) F_n divides G_m whenever $m > n$ (b) $\gcd(F_n, G_m) = 1$ whenever $m \ne n$

(c) $\gcd(F_n, F_m) = 1$ whenever $m \ne n$ (d) G_m divides F_n whenever $m < n$

[CSIR-NET-2014-(I)]

Soln. Take $m = 3$; $n = 2$ option (b) contradicted

Take $m = 2$; $n = 3$ option (d) contradicted

So, option (a) and (c) are correct.

(iii). True or False

The equation $63x + 70y + 15z = 2010$ has an integral solution

[TIFR-2011]

Soln. By definition of $\gcd(63, 70, 15)$ there exist $x, y, z \in \mathbb{Z}$ such that $1 = \gcd(63, 70, 15) = 63x + 70y + 15z$,

then $\begin{aligned} 2010 &= 63(2010x) + 70(2010y) + 15(2010z) \\ 2010 &= 63x' + 70y' + 15z' \end{aligned}$

So we get x', y', z' are integral solution of the equation. **Hence this is true statement.**

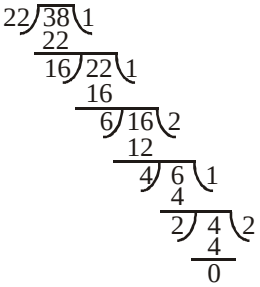
5. **Relatively Prime Integers or Coprime integer :** When $\gcd(a,b) = 1$, we say a and b are relatively prime or coprime integer e.g. $\gcd(9,10) = 1, \gcd(5,8) = 1$

Example :

g.c.d. (10, 20) = 10 as 10 is the greatest common divisor of (10, 20) so, they are not relatively prime.

6. **Composite number:** which are not prime numbers. i.e. (other then prime number integer all number is composite)

e.g. To compute $\gcd(a,b)$ by Euclidean Algorithm. Exp: To compute $\gcd(38, 22)$



38 = 22.1 + 16
22 = 16.1 + 6
16 = 6.2 + 4
6 = 4.1 + 2
4 = 2.2 + 0
gcd(38, 22)

gcd(2520, 154)

2520 = 154.16 + 56
154 = 56.2 + 42
56 = 42.1 + 14
42 = 14.3 + 0
gcd(2520, 154)

7. **Euclid's Lemma:** If p is a prime number that divides $a.b$, then p divides a or p divides b.

i.e. $p \mid ab \Rightarrow p \mid a$ or $p \mid b$

Exp. $3 \mid 12 \Rightarrow 3 \mid 4.3 \Rightarrow 3 \mid 3$

When p is not a prime, then Euclid's Lemma may fail.

$6 \mid 4.3$ but $6 \nmid 4$ and $6 \nmid 3$

8. **Fundamental Theorem of Arithmetic:** Every integer greater than 1 is a prime or a product of primes. This product is unique, except for the order in which the factors appear. Thus, if $n = p_1 p_2 \ldots . p_r$ and $n = q_1 q_2 \ldots . q_s$ where p's and q's are primes, then $r = s$ and, after re-numbering the q's, we have $p_i = q_i$ for all i.

Example :

(*i*) $30 = 2 \times 3 \times 5$, Thus, $p_1 = 2,\ p_2 = 3,\ p_3 = 5$

(*ii*) $15 = 3 \times 5$, $p_1 = 3,\ p_2 = 5$

(*iii*) $42 = 2 \times 3 \times 7$, $p_1 = 2,\ p_2 = 3,\ p_3 = 7$

These expression are unique. No other primes exists other than these which gives same number in each example given above.

9. **Least Common Multiple: LCM (*a, b*):** The least common multiple of two non-zero integers a and b is the smallest positive integer that is a multiple of both a and b. e.g. *lcm*(4, 6) = 12

Example :

(*i*) *l.c.m.* (5, 8) = 40

(*ii*) *l.c.m.* (10, 20) = 20

Remarks : $a \cdot b = \text{lcm}(a, b).\gcd(a, b)$, so, if *g.c.d.* (*a*, *b*) = 1, then *l.c.m.* (*a*, *b*) = *a*·*b*.

■ If $a \mid m$ and $b \mid m$ then $l \mid m$ [where *l* is lcm (*a*, *b*).

SOLVED EXAMPLES

(i). True or False

Given any integer $n \geq 2$ we can always find an integer *m* such that each of $n-1$ consecutive integers $m+2$, $m+3, ..., m+n$ are composite.

[TIFR-2012]

Ans. True

Soln. Take $m = \text{lcm}\{2, 3, 4, ..., n\}$, we can take common $2, 3, 4, ..., n$ from each term which will show that numbers are composite.

10. Modular Arithmetic: Modular arithmetic is an abstraction of a method of counting that you often use. for example, if it is now January, what will be 25^{th} month from now? of course February.

25 = 12.2 + 1, when $a = nq + r$, where q is the quotient and *r* is the remainder upon dividing a by *n*, we write

$a \bmod n = r$ or $a \equiv r \bmod n$

Thus $3 \bmod 2 = 1$ since $3 = 2.1+1$, $6 \bmod 2 = 0$ since $6 = 2.3+0$

$62 \bmod 85 = 62$ since $62 = 85.0 + 62$

More generally, if *a* and *b* are integers and *n* is a positive integer, we often write $a \equiv b \bmod n$ whenever $n \mid (a-b)$.

$(ab) \bmod n = ((a \bmod n)(b \bmod n)) \bmod n$, $(a+b) \bmod n = ((a \bmod n) + (b \bmod n)) \bmod n$

$(17+23) \bmod 10 = ((17 \bmod 10) + (23 \bmod 10)) \bmod 10 = (7+3) \bmod 10 = 10 \bmod 10 = 0$

Example :

$12 \equiv -2 \pmod 7$ means $7 \mid 12-(-2) \Rightarrow 7 \mid 14$

This gives the remainder after dividing by 7 to 12 – (–2)

Some properties of modular Arithmetic

if $a \equiv b \pmod n$

Then,

(*i*) $a + c \equiv b + c \pmod n$

(*ii*) $a\,c \equiv b\,c \pmod n$

(*iii*) $a^p \equiv b^p \pmod n$

(*iv*) $p(a) \equiv p(b) \pmod n$

where $p(a)$ – polynomial in *a*.

but converse of the property (ii), (iii) and (iv) does not hold.

as, $9 \equiv 6 \pmod 3$

also $3.3 \equiv 3.2 \pmod 3$

but $3 \equiv 2 \pmod 3$ not hold

Similarly for others.

SOLVED EXAMPLES

(i). The last digit of 2^{80} is

(a) 2 (b) 4 (c) 6 (d) 8

[TIFR-2010]

Soln. Using modular arithmetic ; $2^4 \equiv 6 \mod 10$

Use property (iii) if $a \equiv b \pmod n$ and $a^P \equiv b^P \pmod n$

So we get $(2^4)^{20} = 6^{20} \pmod{10}$

$2^{80} = 6 \pmod{10}$

$\Rightarrow$ last digit of 2^{80} is 6

Hence, correct option is (c).

(ii). Which of the following statement is FALSE ?

(a) There exist a natural number which when divided by 3, leaves remainder 1 and which when divided by 4, leaves remainder 0.

(b) There exist a natural number which when divided by 6, leaves remainder 2 and which when divided by 9, leaves remainder 1.

(c) There exist a natural number which when divided by 7, leaves remainder 1 and which when divided by 11, leaves remainder 3.

(d) There exist a natural number which when divided by 12, leaves remainder 7 and which when divided by 8, leaves remainder 3.

[TIFR-2010]

Soln. Apply modular arithmetic, check it by option

(b) assume such natural number exist say x then $x \equiv 2 \mod 6$ and $x \equiv 1 \mod 9$

$\Rightarrow \quad x = 6q + 2$ and $x = 9q' + 1$

$\Rightarrow \quad 6q + 1 = 9q'$

$\Rightarrow \quad (6q + 1) \bmod 9 = 0 \qquad \ldots (*)$

use $(a + b) \bmod n = (a \pmod n + b \pmod n) \bmod n$ then

$(6q + 1) \bmod 9 = (6q \pmod 9 + 1 \pmod 9) \bmod 9$

$$= \left.\begin{array}{l} (0+1) \bmod 9 = 1 \\ \text{or} \quad (3+1) \bmod 9 = 4 \\ \text{or} \quad (6+1) \bmod 9 = 7 \end{array}\right\} \neq 0$$

which is contradiction to (*), hence option (b) is not true.

Hence, correct option is (b).

(iii). What is the last digit of 97^{2013} ?

(a) 1 (b) 3 (c) 7 (d) 9

[TIFR-2014]

Soln. By modular arithmetic

$(97)^4 \equiv 1 \mod 10$

$((97)^4)^{503} \equiv 1 \mod 10$ by property (iii)

$97^{2012} \equiv 1 \mod 10$

$97^{2013} \equiv 97 \mod 10$ by property (ii)

$= 7 \mod 10$

Hence, correct option is (c).

(iv). Which of the following primes satisfy the congruence $a^{24} \equiv (6a + 2) \mod 13$

(a) 41 (b) 47 (c) 67 (d) 83

[CSIR-NET-2015-(I)]

Soln. $(41)^{24} \equiv (6.41 + 2) \bmod 13 \equiv (246 + 2) \bmod 13 \equiv (248) \bmod 13 \equiv 1 \bmod 13$

$(41^2)^{12} \equiv 1 \bmod 13$

Use Euler Theorem $\gcd(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \bmod n$, $a = 41^2$; $n = 13$ then $a^{12} \equiv 1 \bmod 13$

Hence, correct options are (a) and (c).

(v). The last two digit of 7^{81} are

(a) 07 (b) 17 (c) 37 (d) 47

[CSIR-NET-2012-(II)]

Soln. $7^{81} \equiv r \bmod 100$. Find r.

$$\left.\begin{array}{rcl} 7^4 & \equiv & 01 \pmod{100} \\ (7^4)^{20} \cdot 7 \quad 7^{80} & \equiv & 01 \pmod{100} \\ 7^{81} & \equiv & 07 \pmod{100} \end{array}\right] \text{ use modular arithmatic property.}$$

$\Rightarrow \quad r = 07$

Hence, correct option is (a).

(vi). The last digit of $(38)^{2011}$ is

(a) 6 (b) 2 (c) 4 (d) 8

[CSIR-NET-2012-(I)]

Soln. $38 \equiv 8 \pmod{10}$

$(38)^4 \equiv (8)^4 \pmod{10} = (6 \bmod 10)$

$((38)^4)^{502} \equiv 6 \pmod{10}$

$(38)^{2008} \equiv 6 \pmod{10}$

$\Rightarrow \quad (38)^{2009} \equiv 8 \pmod{10}$

$\Rightarrow \quad (38)^{2010} \equiv 4 \pmod{10}$

$\Rightarrow \quad (38)^{2011} \equiv \underset{\text{last digit}}{2} \pmod{10}$

Hence, correct option is (b).

(vii). The unit digit of 2^{100} is

(a) 2 (b) 4 (c) 6 (d) 8

[CSIR-NET-2011-(I)]

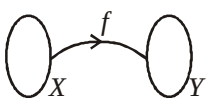
Soln. $2^4 \equiv 6 \pmod{10}$

$(2^4)^{25} \equiv (6)^{25} \pmod{10} \equiv \underset{\text{unit digit}}{6} \pmod{10}$

Hence, correct option is (c).

Functions (Mappings) and Relations

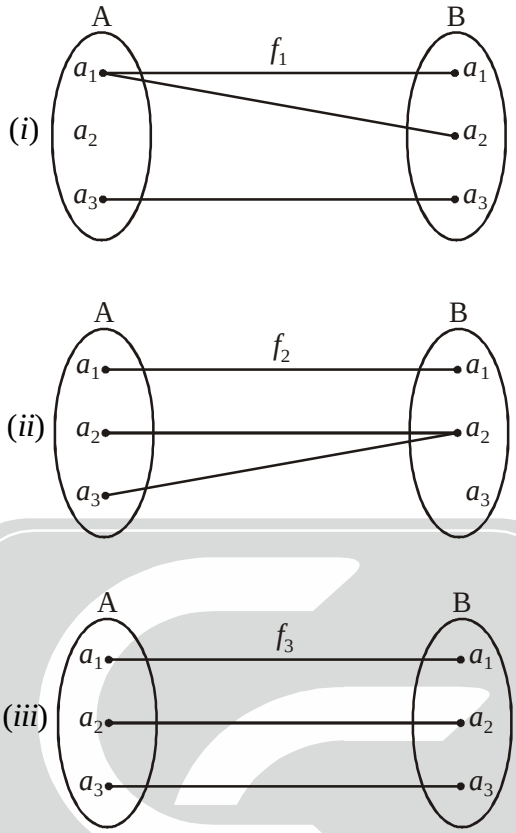
11. Function (Mapping): A function (or mapping) '*f* ' from a set '*X*' to a set '*Y*' is a rule which assigns to each element *x* of *X* exactly one element *y* of *Y*.



Domain Co-domain

$'f : X \to Y'$

Example :--

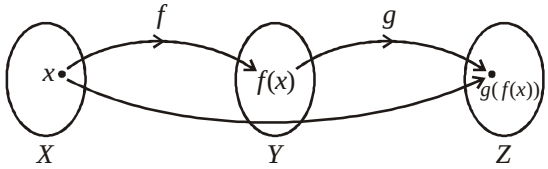


By the definition of function that "a rule that assigns to each element x of X exactly one element y of Y.

Thus in above examples f_1 is not a function since a_1 maps to a_1 and a_2 both which contradicts the definition of a function.

12. Composition of Functions: Let $f : X \to Y$ and $g : Y \to Z$. The composition gof (or gf) is the mapping from X to Z defined by

$(gof)(x) = g(f(x))$ for all $x \in X$.



Example :

Let $f(x) = 2x$, $\quad g(x) = x^2 + 1$

Then $fog(x) = f[g(x)] = f \cdot [x^2 + 1]$

$= 2 \cdot (x^2 + 1) = 2x^2 + 2$

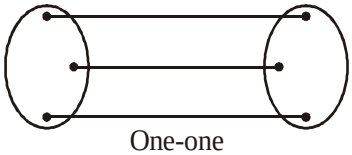
but $gof(x) = g \cdot [f(x)] = g \cdot [2x]$

$\Rightarrow g(2x) = (2x)^2 + 1 = 4x^2 + 1$

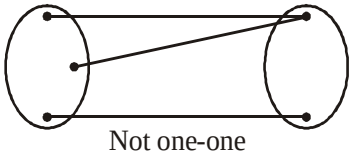
Thus, $2x^2 + 2 \neq 4x^2 + 1$

Hence composition of two function need not be commutative. i.e., $fog(x) \neq gof(x)$.

13. One to one Function: A function $f: X \to Y$ is called one to one if $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$ or equivalently $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$.

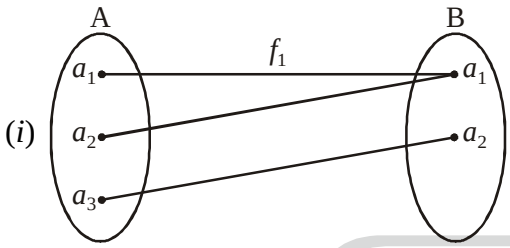


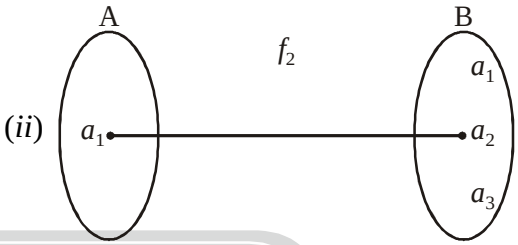
One-one



Not one-one

Example :





Remarks :

(*i*) If domain has more elements than codomain $\Rightarrow$ function can not be one-one (by definition of a function)

(*ii*) If domain has only one element then any function which is defined on to that domain always be one-one (by definition of a function)

(*iii*) If $|x| = m,\ |y| = n\ ;\ m \leq n$ then number of one-one map is $n_{p_m} = \dfrac{n!}{(n-m)!}$.

SOLVED EXAMPLES

(i). Let $m \leq n$ be natural number. The number of injective maps from a set of cardinality m to a set of cardinality n is

(a) $m!$ (b) $n!$ (c) $(n-m)!$ (d) None

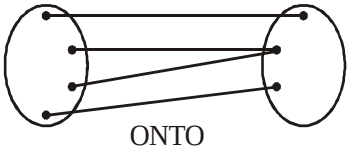
[TIFR-2011]

Soln. By remark (iii)

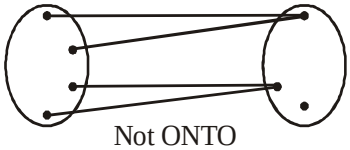
Number of one to one function is $n_{p_m} = \dfrac{n!}{(n-m)!}$

Hence, correct option is (d).

14. ONTO Functions: A function $f: X \to Y$ is said to be onto if each element of Y is the image of atleast one element of X.



ONTO



Not ONTO

Remarks :

(*i*) Similarly if codomain has more element than domain of a function $\Rightarrow$ function can not be onto.

(*ii*) If codomain of a function with non empty domain then it will be always onto means for each $y \in Y\ ;\ \exists$ at-least one $x \in X$ such that $f(x) = y$.

(*iii*) If $|x| = m,\ |y| = n\ ;\ m \geq n$ then number of onto map is

$$n^m - \left[n_{C_1}(n-1)^m - n_{C_2}(n-2)^m + n_{C_3}(n-3)^m - \cdots + (-1)^{k+1} n_{C_k}(n-k)^m \right]$$

SOLVED EXAMPLES

(i). Number of surjective maps from a set of 4 elements to a set of 3 element is
(a) 36 (b) 64 (c) 69 (d) 81

[CSIR-NET-2014-(II)]

Soln. Use remark (iii)

$\Rightarrow \quad n^m - \left[n_{c_1} (n-1)^m - n_{c_2} (n-2)^m + n_{c_3} (n-3)^m ..... \right]$

$m = 4 \ ; \ n = 3$

$\Rightarrow \quad 3^4 - \left[3_{c_1} (3-1)^4 - 3_{c_2} (3-2)^4 + 3_{c_3} (3-3)^4 \right]$

$= 81 - \left[3(2)^4 - 3(1)^4 \right]$

$= 81 - \left[48 - 3 \right] \Rightarrow 81 - 45 = 36$

Hence, correct option is (a).

15. Properties of Functions: Given functions $f : X \to Y, g : Y \to Z$ and $h : Z \to W$. Then

(i) $h(gf) = (hg) f$ (associativity)

(ii) If *f* and *g* are one-to-one, then *gof* and *fog* is one-to-one.

(iii) If *f* and *g* are onto, then *gof* and *fog* is onto.

(iv) If *f* is one-to-one and onto, then there exist a function f^{-1} from *Y* onto *X* such that

$(f^{-1} of)(x) = x \ \forall \ x \in X$ and $(fof^{-1})(y) = y \ \forall \ y \in Y$

16. Relation: Let A and B be two sets. A relation from A to B is a subset of A×B where A×B is cartesian product of sets A and B i.e. A × B is a set of ordered pairs (*a*, *b*) such that $a \in A$ and $b \in B$.

Example :

$A = \{1, 2, 3, 4\}$, $B = \{a, b, c\}$. Then $A \times B = \{(x, y) : x \in A \text{ and } y \in B\}$. Then power set of $A \times B$ defined as relations on $A \times B$. Infact, each element of power set of $A \times B$ defines a relation and each relation defined on $A \times B$ gives a subset of $A \times B$.

as, $N \times N = \begin{cases} (1,1), & (1,2), & (1,3), ... \\ (2,1), & (2,2), & (2,3), ... \\ (3,1), & (3,2), & (3,3), ... \\ \ | & \ | & \ | & ..... \\ \ | & \ | & \ | & ..... \end{cases}$

Then if we take all order pairs (a, b) s.t. $1 \le a \le 4$ and $b = 3$. Then $R = \{(1, 3), (2, 3), (3, 3), (4, 3)\}$ which is a subset of $N \times N$

Relation on a set A:

A relation on a set A is subset of A×A.

17. Types of relation on a set:

(i) Reflexive Relation: Let R be a relation on a set A i.e. let R be a subset of A × A, then R is called a reflexive relation if $(a, a) \in R, \forall a \in A$.

i.e. R is reflexive if we have, $aRa, \forall\, a \in A$

A relation R on a set A is NOT REFLEXIVE if there is atleast one element $a \in A$, such that $(a, a) \notin R$.

Example : (*i*) Reflexive : $A = \{1, 2, 3\}$

Then $R_1 = \{(1, 1), (2, 2)\}$ ×

$R_2 = \{(1, 1), (2, 2), (3, 3), (3, 4)\}$ √

$R_3 = \{(1, 1), (2, 2), (3, 3)\}$ √

$R_4 = \{(1, 2), (2, 1), (2, 3), (3, 2), (1, 3), (3, 1)\}$ ×

R_1 and R_4 are not reflexive since they have not all possible pairs of $(a, a)\ \forall\ a \in A$.

In R_2, R_3 they are reflexive since $\{(1, 1), (2, 2), (3, 3)\} \subseteq R_2$

Similarly ; $\{(1, 1), (2, 2), (3, 3)\} \subseteq R_2$

(ii) Symmetric relation: Let R be a relation on a set A i.e. let R be a subset of A × A. Then R is said to be a symmetric relation if $(a, b) \in R \Rightarrow (b, a) \in R$. Thus R is symmetric if we have bRa whenever we have aRb. A relation R on a set A is not symmetric if there exist two distinct elements $a, b \in A$, such that aRb but $b \not R a$.

i.e. $(a, b) \in R$ but $(b, a) \notin R$.

Example :

Set A = {1, 2, 3, 4}

$R_1 = \{(1, 2), (2, 1)\}$ √

$R_2 = \{(1, 2), (1, 3), (3, 1), (4, 4)\}$ ×

$R_3 = \{(1, 1), (2, 2), (3, 3), (4, 4)\}$ √

R_2 is not symmetric, since $(1, 2) \in R_2$ but $(2, 1) \notin R_2$

(iii) Anti-symmetric relation: Let R be a relation on a set A i.e. let R be a subset of A × A. Then R is said to be an anti-symmetric relation if $(a, b) \in R$ and $(b, a) \in R$ implies $a = b$.

i.e. $(a, b) \in R$, and $(b, a) \in R \Rightarrow a = b$

or $a \neq b \Rightarrow (a, b) \notin R$ or $(b, a) \notin R$ or $(a, b) \in R \Rightarrow (b, a) \notin R$

R is not anti-symmetric if there exist elements $a \neq b$ such that $(a, b) \in R$ as well as $(b, a) \in R$

(iv) Transitive relation: Let R be a relation on a set A i.e. let R be subset of A × A. Then R is said to be a transitive relation if $(a, b) \in R$ and $(b, c) \in R \Rightarrow (a, c) \in R$. A relation R on a set A is not transitive if there exist elements *a*, *b* and *c* in A, not necessarily distinct, such that

$(a, b) \in R, (b, c) \in R$ but $(a, c) \notin R$

Example :

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

$R_1 = \{(1,1),(2,2)\}$ √

$R_2 = \{(3,3),(3,4)\}$ √

$R_3 = \{(1,2),(2,1),(1,1)\}$ ×

R_1 and R_2 are transitive but R_3 is not since $(2,1) \in R_3$ and $(1,2) \in R_3$ but $(2,2) \notin R_3$.

17. **Equivalence Relation:** Let R be a relation on a set A. Then R is said to be an equivalence relation iff the following three conditions hold simultaneously $\forall\ a \in A$.

(i) R is reflexive i.e. $a \in A \Rightarrow (a,a) \in R$

(ii) R is symmetric i.e. $(a,b) \in R \Rightarrow (b,a) \in R$

(iii) R is transitive i.e. $(a,b) \in R$ and $(b,c) \in R \Rightarrow (a,c) \in R$

Ex. (*i*) Set of parallel lines.

(a) Reflexive:-- Each line is parallel to itself.

(b) Symmetric:-- If $L_1 \parallel L_2$ then $L_2 \parallel L_1$. Hence symmetric hold.

(c) Transitivity:-- If $L_1 \parallel L_2$ and $L_2 \parallel L_3 \Rightarrow L_1 \parallel L_3$. Hence set of parallel lines defines an equivalence relation.

Ex. (*ii*) Set of all male human being, relation defines brotherhood :--

(a) Reflexivity :-- Each male human being is brother to itself (in mathematics it is hold).

(b) Symmetric :-- If A_1 is brother of A_2 then A_2 is also brother of A_1. (Since we have the set of all male human being).

(c) Transitive :-- Also hold. Hence an equivalence relation.

18. **Examples:** which is not equivalence relation.

(i) set of perpendicular lines

(a) not reflexive as a line cannot perpendicular to itself.

(b) it is symmetric

(c) not transitive

Hence not an equivalence relation.

19. **Equivalence Class:** If $\sim$ is an equivalence relation on a set A and $a \in A$, then the set $[a] = \{x \in A : x \sim a\}$ is called the equivalence class of A containing '*a*'.

$[a]$ is a subset of A.

20. **Properties of Equivalence Classes:** Let A be a non-empty set and let R be an equivalence relation on A. Let *a* and *b* be arbitrary elements of A. Then

(i) $a \in [a]$

(ii) If $b \in [a]$, then $[b] = [a]$

(iii) $[a] = [b]$ iff aRb i.e. $(a,b) \in R$

(iv) Either $[a] = [b]$ or $[a] \cap [b] = \phi$ i.e. two equivalence classes are either disjoint or identical.

Proof: (i) Since R is reflexive, we have aRa. But $[a] = \{x \mid x \in A$ and $aRa\}$. Hence $a \in R$ and aRa imply $a \in [a]$.

(ii) Let $b \in [a] \Rightarrow bRa$. Now if, *x* be any arbitrary element of [*b*]. Then $x \in [b] \Rightarrow xRb$. But *R* is transitive, therefore xRb and $bRa \Rightarrow xRa \Rightarrow x \in [a]$. Thus $x \in [b] \Rightarrow x \in [a]$. Therefore $[b] \subseteq [a]$. Again, let *y* be any arbitrary element of [*a*]. Then $y \in [a] \Rightarrow yRa$.

Since R is symmetric, therefore $bRa \Rightarrow aRb$. Now yRa and $aRb \Rightarrow yRb \Rightarrow y \in [b]$

Thus $y \in [a] \Rightarrow y \in [b]$. Therefore $[a] \subseteq [b]$. Finally $[a] \subseteq [b]$ and $[b] \subseteq [a] \Rightarrow [a] = [b]$

(iii) **First Part:** $[a] = [b] \Rightarrow aRb$

We have $[a] = [b]$

Since R is reflexive, therefore we have aRa.

Now $aRa \Rightarrow a \in [a] \Rightarrow a \in [b]$ $[\because [a] = [b]]$ $\Rightarrow aRb$

Thus $[a] = [b] \Rightarrow aRb$

Converse part: Suppose that aRb, then to prove that $[a] = [b]$.

Let *x* be any arbitrary element of [*a*]. Then xRa. But it is given that aRb.

Therefore, xRa and $aRb \Rightarrow xRb$ [R is transitive]

$\Rightarrow x \in [b]$

Thus $x \in [a] \Rightarrow x \in [b]$. Therefore $[a] \subseteq [b]$

Again let *y* be any arbitrary element of [*b*]. Then $y \in [b] \Rightarrow yRb$

Now, we are given that aRb. From this we have bRa since *R* is symmetric.

Now, yRb and $bRa \Rightarrow yRa \Rightarrow y \in [a]$

Thus $y \in [b] \Rightarrow y \in [a]$, therefore $[b] \subseteq [a]$. Hence, $[a] \subseteq [b]$ and $[b] \subseteq [a] \Rightarrow [a] = [b]$

Finally since $[a] = [b] \Rightarrow aRb$ and $aRb \Rightarrow [a] = [b]$

Therefore, $[a] = [b]$ iff aRb

(iv) If $[a] \cap [b] = \phi$, then we have nothing to prove. So let us suppose that $[a] \cap [b] \neq \phi$ therefore there exist an element $x \in A$ such that $x \in [a] \cap [b]$

$\Rightarrow x \in [a]$ and $x \in [b]$

$\Rightarrow xRa$ and xRb

$\Rightarrow aRx$ and xRb [R is symmetric]

$\Rightarrow aRb$ [R is transitive]

$\Rightarrow [a] = [b]$

Thus, $[a] \cap [b] \neq \phi \Rightarrow [a] = [b]$

21. **Partition:** A partition of a set S is a collection of non-empty disjoint subsets of S whose union is S.

Example 1: Consider the set $S = \{1, 2, 3, 4\}$, then $\{\{1, 2\}, \{3\}, \{4\}\}$ is a partition of S.

Example 2: Let *Z* be the set of all integers we know that $x \equiv y \pmod 3$ is an equivalence relation on *Z*. Consider the set of three equivalence classes

$[0] = \{...., -6, -3, 0, 3, 6, ...\}$ $[1] = \{...., -7, -4, 1, 4, 7, ...\}$ $[2] = \{...., -8, -5, 2, 5, 8, ...\}$

We observe that

(i) The sets [0], [1] and [2] are non-empty

(ii) The sets [0], [1] and [2] are pairwise disjoint

(iii) $Z = [0] \cup [1] \cup [2]$

Hence, $\{[0], [1], [2]\}$ is a partition of Z, under the relation $x \equiv y \pmod 3$.

22. Relation induced by a partition of a set: Corresponding to any partition of a set S, we can define a relation R on S by the requirement that xRy iff x and y belong to the same subset of S belonging to the partition. The relation R is then said to be induced by the partition.

Example 1 : Consider the set $S = \{1, 2, ...9, 10\}$ and its subsets

$B_1 = \{1, 3\}, B_2 = \{7, 8, 10\}, B_3 = \{2, 5, 6\}, B_4 = \{4, 9\}$.

The set $p = \{B_1, B_2, B_3, B_4\}$ is such that

(i) B_1, B_2, B_3, B_4 are all non-empty subsets of S.

(ii) $B_1 \cup B_2 \cup B_3 \cup B_4 = S$, and

(iii) For any sets B_i, either $B_i = B_j$ or $B_i \cap B_j = \varnothing$.

Hence the set $\{B_1, B_2, B_3, B_4\}$ is a partition of S.

23. Fundamental theorem on equivalence relation: An equivalence relation R on a non-empty set S determine a partition of S and conversely a partition of S defines an equivalence relation on S. OR
The equivalence classes of an equivalence relation on a set S constitute a partition of S conversely, for any partition P of S, there is an equivalence relation on S whose equivalence classes are the elements of P.

Proof: Let R be an equivalence relation in S. Let A be the set of equivalence classes of S with respect to R i.e. let

$A = \{[a] : a \in S\}$

where $[a] = \{x : x \in S \text{ and } xRa\}$.

Since R is an equivalence relation, therefore $\forall a \in S$, we have aRa. Hence $a \in [a]$ and thus $[a] \neq \varnothing$. Further every element a of S is an element of the equivalence class $[a]$ in A. From this we conclude that $S = \bigcup_{a \in S} [a]$.

Finally, if $[a]$ and [b] are two equivalence classes then either $[a] = [b]$ or $[a] \cap [b] = \varnothing$.

Hence A is a partition of S. Thus we see that an equivalence relation R in S decomposes the set S into equivalence classes any two of which are either equal or mutually disjoint.

Converse. Let $P = \{T_a, T_b, T_c, ...\}$ be any partition of S. If $p, q \in S$, let us define a relation R in S by pRq iff there is a T_i in the partition such that $p, q \in T_i$.

Now $S = T_a \cup T_b \cup T_c ...$ Therefore $\forall x \in S$, there exists $T_i \in P$ such that $x \in T_i$ for some i.

Hence $x \in T_i$ and $x \in T_i$ means xRx. Thus $\forall x \in S$, we have xRx and thus R is reflexive.

Again if we have xRy, then there exists $T_i \in P$ such that $x \in T_i$ and $y \in T_i$.

But $x \in T_i$ and $y \in T_i \Rightarrow y \in T_i$ and $x \in T_i \Rightarrow yRx$.

Therefore, R is symmetric.

Finally suppose xRy and yRz. Then by the definition of R there exist subsets T_j and T_k (not necessarily distinct) such that $x, y \in T_j$ and $y, z \in T_k$. Since $y \in T_j$ and also $y \in T_k$, therefore $T_j \cap T_k \neq \varnothing$. But T_j and T_k belong to a partition of S. Therefore $T_j \cap T_k \neq \varnothing$ implies $T_j = T_k$. Now $T_j = T_k$ implies $x, z \in T_j$

and consequently we have xRz. Thus R is transitive.

Since R is reflexive, symmetric and transitive, therefore R is an equivalence relation.

SOME IMPORTANT FUNCTIONS

1. **ϕ – function :** It is called Euler phi-function and defined as

$\phi(n)$ = number of positive integers co-prime to n and less than or equal to n.

Ex. (*i*) $\phi(10) = 4$ as 1, 3, 7, 9 (total 4) integers which are co-prime to 10.

Method for finding number of positive integers co-prime to n :--

If $n = p^a\, q^b \cdot r^c, \ldots\ldots$ where $p, q, r, \ldots\ldots$ are prime and $a, b, c, \ldots\ldots$ are natural number.

Then $\phi(n) = n \cdot \left(1 - \frac{1}{p}\right) \cdot \left(1 - \frac{1}{q}\right)\left(1 - \frac{1}{r}\right) \ldots\ldots$

Ex. (*ii*) $\phi(100) = 2^2 \cdot 5^2 \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{5}\right)$

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

$= 2 \cdot 5\,(1) \cdot (4)$

$= 40$

SOLVED EXAMPLES

(i). For a positive integer m, let $\phi(m)$ denote the number of integers k such that $1 \le k \le m$ and $\gcd(k, m) = 1$. Then which of the following statement are necessarily true

(a) $\phi(n)$ divides n for every positive integer n

(b) n divides $\phi(a^n - 1)$ for all positive integer a and n

(c) n divides $\phi(a^n - 1)$ for all positive integer a and n such that $\gcd(a, n) = 1$

(d) a divides $\phi(a^n - 1)$ for all positive integer a and n such that $\gcd(a, n) = 1$

[CSIR-NET-2012-(II)]

Soln. (b) and (c)

For (a) take $n = 3$ and For (d) take $a = 3$, $n = 2$, then both (a) and (d) are contradicted.

(ii). The number of element in the set $\{m : 1 \le m \le 1000,\ m \text{ and } 1000 \text{ are relatively prime}\}$ is

(a) 100 (b) 250 (c) 300 (d) 400

[CSIR-NET-2011-(I)]

Soln. $\phi(1000) = \phi(10^3) = 4 \times 10^2 = 400$ By property 5.

Hence, correct option is (d).

(iii) What is the cardinality of the set $\{z \in \mathbb{C} \mid z^{98} = 1 \text{ and } z^n \ne 1 \text{ for any } 0 < n < 98\}$?

(a) 0 (b) 12 (c) 42 (d) 49

[CSIR-NET-2015-(II)]

Soln. Given group is isomorphic to cyclic group of order 98 i.e., $\mathbb{Z}_{98}$ then number of elements in $\mathbb{Z}_{98}$ which is coprime to 98 is $\phi(98) = 42$.

Hence, correct option is (c).

2. $\tau(n)$**: (**τ **(tau) function)**:-- It gives total number of divisors of n, including 1 and n both.

If $n = p^a \cdot q^b \cdot r^c, \ldots\ldots\ldots$ where $p, q, r, \ldots\ldots\ldots$ are distinct primes and $a, b, c \ldots\ldots\ldots \in \mathbb{N}$.

Then $\tau(n) = (a+1)(b+1)(c+1)\ldots\ldots\ldots$

Note: It includes 1 and and the number itself.

$\tau(100) = 2^2 \cdot 5^2 = (2+1)(2+1) = (3)(3) = 9$

(*iii*) $\sigma(n)$:-- (Sigma function) :-- It gives the sum of all divisors. It too includes 1 and the number n itself.

If $n = p^a \cdot q^b \cdot r^c \ldots\ldots\ldots, p, q, r$ primes $a, b, c \in \mathbb{N}$.

Then $\sigma(n) = \left(\frac{p^{a+1}-1}{p-1}\right) \cdot \left(\frac{q^{b+1}-1}{q-1}\right) \cdot \left(\frac{r^{c+1}-1}{r-1}\right) \ldots\ldots\ldots$

Ex. $\sigma(20) = \sigma\left(2^2 \cdot 5\right) = \left(\frac{2^3-1}{1}\right) \cdot \left(\frac{5^2-1}{4}\right) = (7) \times \left(\frac{24}{2}\right) = 7 \times 6 = 42$

SOLVED EXAMPLES

(i). The number of positive divisor of 50,000 is

(a) 20 (b) 30 (c) 40 (d) 50

[CSIR-NET-2012-(I)]

Soln. $n = 50,000 = 5 \times 10^4 = 2^4 \cdot 5^5$

$\tau(n) = (4+1)(5+1) = 5 \cdot 6 = 30$

Hence, correct option is (b).

Properties :

1. In particular when n is prime say p,

$\phi(p) = p-1, \tau(p) = 2, \sigma(p) = p+1$

2. If g.c.d. $(m, n) = 1$ then

(*i*) $\phi(m \cdot n) = \phi(m) \cdot \phi(n)$

(*ii*) $\tau(m \cdot n) = \tau(m) \cdot \tau(n)$

(*iii*) $\sigma(m \cdot n) = \sigma(m) \cdot \sigma(n)$

3. A "number theoratic" function f is said to be multiplicative if $f(m, n) = f(m) \cdot f(n)$. Whenever g.c.d. $(m, n) = 1$ hence ϕ, τ, σ are multiplicative functions.

4. For $n > 2$, $\phi(n)$ is always an even integer.

5. $\phi(10^n) = 4 \times 10^{n-1}$

Important Theorems :

(I) Gauss : For each positive integer $n \geq 1$.

$\boxed{n = \sum_{d/n} \phi(d)}$ where sum being extended over all positive divisors 'd' of n.

(II) Theorem : For $n > 1$, the sum of the positive integers less than n and relatively prime to n is

$$\boxed{\sum_{\substack{(K,n)=1 \\ 1 \leq K \leq n}} K = \frac{1}{2} n \cdot \phi(n)}$$

(III) Fermat's Theorem : If p is prime, then $a^p \equiv a \pmod{p}$.

(IV) Fermat's little Theorem : If p is prime, then $a^{p-1} \equiv 1 \pmod{p}$
converse of Fermat's theorem is need not to be true.

(V) Euler Theorem : If n is a positive integer and g.c.d. $(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \pmod{n}$, $\phi(n)$ is Euler phi function "Euler Theorem is generalization of Fermat's Theorem". OR

$$\#\left[\begin{array}{l}\text{i.e. if } x^k \equiv a \pmod{n} \text{ and } \gcd(k, \phi(n)) = d \text{ ; } n \text{ is prime} \\ \Leftrightarrow a^{\phi(n)/d} \equiv 1 \pmod{n}, \text{where } \phi(n) \text{ is Euler } \phi \text{ function}\end{array}\right]$$

(VI) Wilson's Theorem : If p is a prime, then $(p-1)! \equiv -1 \pmod{p}$ or $(p-1)! + 1 \equiv 0 \pmod{p}$.

(VII) Pseudo Prime : A composite integer 'n' is called pseudo prime if it satisfies the congruence equations. $2^n \equiv 2 \pmod{n}$.

(VIII) Chinese Remainder Theorem

Let $x \equiv a_i \bmod m_i : i = 1, \ldots, n$, for which m_i are pairwise relatively prime the solution of the set of congruence is $x = \left(a_1 b_1 \frac{m}{m_1} + \cdots a_n b_n \frac{m}{m_n} \right) \bmod m$, where $m = m_1 m_2 \ldots m_n$ and b_i satisfy $b_i \frac{m}{m_i} = 1 \pmod{m_i}$

If $m_1, m_2, \ldots, m_n$ are pairwise relatively prime positive integers and if $a_1, a_2, \ldots, a_n$ are any integers then simultaneous congruence $x = a_i \bmod m_i \text{ ; } i = 1, \ldots, n$ have a solution and solution is unique modulo m, where $m = m_1 m_2 \ldots m_n$.

SOLVED EXAMPLES

(i). The equation $x^{22} \equiv 2 \pmod{23}$ has
(a) no solution (b) 23 solution
(c) exactly one solution (d) 22 solution

[TIFR-2011]

Soln. Use Euler theorem (*v*)
$k = 22 \text{ ; } a = 2 \text{ ; } n = 23 \text{ ; } d = \gcd(22, \phi(23)) = \gcd(22, 22) = 22$, then
$2^{\phi(23)/d} \equiv 1 \pmod{n} \Rightarrow 2^{22/22} \equiv 1 \pmod{23} \Rightarrow 2 \equiv 1 \pmod{23}$ which is contradiction. Hence no solution exist.
Hence, correct option is (a).

(ii). If n is the positive integer such that the sum of all positive integer a satisfying $1 \le a \le n$ and $\gcd(a, n) = 1$ is equal to 240 n then number of summand namely $\phi(n)$ is
(a) 120 (b) 124 (c) 240 (d) 480

[CSIR-NET-2014-(I)]

Soln. Use theorem II

$$\sum_{\substack{(k,n)=1 \\ 1 \le k \le n}} k = \frac{1}{2} n \cdot \phi(n)$$

$$\Rightarrow \quad 240\, n = \frac{1}{2} n\, \phi(n) \quad \Rightarrow \quad \phi(n) = 480$$

Hence, correct option is (d).