Let a, b and c are such $a \leq b$ and $b \leq c$

$\Rightarrow a \leq c \Rightarrow$ '$\leq$' is transitive.

'$\leq$' on $\mathbb{Z}$ is a partial order $(S, \leq)$ is po-set or partially - ordered set.

2019

2. Let X be a non-empty set then prove that P(X) together with relation '$\subseteq$' is a po-set.

1. Reflexivity

Since $\forall\ A \in P(X)$, ~~$A \subseteq A$~~ $A = A$

$\Rightarrow A \subseteq A$, '$\subseteq$' is reflexive.

2. Anti-symmetry

Let $A, B \in P(X)$ such that $A \subseteq B$ and $B \subseteq A$

$\Rightarrow A = B$

'$\subseteq$' is anti-symmetric

3. Transitivity

Let A, B and C are such that $A \subseteq B$ and $B \subseteq C$

$\Rightarrow A \subseteq C$

$\Rightarrow$ '$\subseteq$' is transitive

therefore '$\subseteq$' is partial order on P(X)

$(P(X), \subseteq)$ is po-set or partially ordered set.

3. Let $\mathbb{Z}^+$ is set of all positive integers then prove that $(\mathbb{Z}^+, |)$ is po-set where '$|$' is relation called 'divides' and defined as $a|b$ iff $b = ma$, $m \in \mathbb{Z}^+$.

1. Reflexive:

for each $a \in \mathbb{Z}^+$, $a = 1.a$

$\Rightarrow a|a$

'$|$' is reflexive

Scanned by CamScanner

2. Anti-symmetry

Let $a, b \in \mathbb{Z}^+$ such that $a|b$ and $b|a$

$\Rightarrow b = ma$ and $a = nb$

$\Rightarrow m = n = 1$

$\Rightarrow a = b$

3. Transitivity

Let $a, b, c \in \mathbb{Z}^+$ such that $a|b$ and $b|c$

$\Rightarrow b = ma$ and $c = nb$, $m, n \in \mathbb{Z}^+$

$\Rightarrow c = n(ma)$

$\Rightarrow c = (mn)a$

$\Rightarrow a|c$

$\Rightarrow$ '|' is transitive

Hence, $(\mathbb{Z}^+, |)$ is po-set.

Linearly - ordered or totally ordered set

Definition

Let (S, R) be a poset.

Let $a, b \in S$.

We say a and b are comparable if either aRb or bRa.

A po-set (S, R) is said to be linearly ordered or totally ordered if for each $a, b \in S$ either aRb or bRa.

Example 1: Let $S = \{1, 3, 9, 27, 81\}$ with partial order '|'

Then $(S, |)$ is linearly ordered.

Example 2: Let $S = \{1, 2, 3, 4, 5\}$ together with relation '|'

$(S, |)$ is not linearly ordered because $3, 5 \in S$ but neither $3|5$ nor $5|3$

Example 3: Let $S = \{1, 2, 3, 4, 5\}$ with partial order '$\leq$'

Then $(S, |)$ is linearly ordered.

Scanned by CamScanner

Successor

Let (S, R) be a po-set.

Let $a, b \in S$

We say element b is immediate successor of a if

i) aRb

ii) there does not exist any element in S such that aRc and cRb

18.01.2019

Greatest and least elements

Let (S, R) be po-set. An element say $a \in S$ is said to be greatest element if $xRa \ \forall \ x \in S$.

An element say $b \in S$ is said to be least element if

$bRx \ \forall \ x \in S$

Note:

If greatest and least elements exists then they are unique.

A set may ~~no~~ or may not have greatest or least elements.

Maximal and Minimal element

Let (S, R) be a poset.

An element $a \in S$ is said to be maximal element if there does not exist $x \in S$ such that aRx.

An element $b \in S$ is said to be minimal element if there does not exist $x \in S$ such that xRb.

Note:

Maximal and minimal elements if exists, are not unique.

Example: consider $S = \{1, 2, 3, 4, 5, 6\}$ with partial order '/' ~~and~~ $\leq$. Find

Scanned by CamScanner

greatest, least, maximal and minimal elements.

Greatest element : not present

Least element : 1

Maximal element : 4, 5, 6

Minimal element : 1

$X = \{1, 2, 3\}$

consider $(P(X), \subseteq)$

Find greatest, least, minimal, maximal elements.

$P(X) = \{\phi, X, \{1\}, \{2\}, \{3\}, \{1,2\}, \{2,3\}, \{3,1\}\}$

Maximal = greatest = X

Least = minimal = ϕ

Let (S, R) be poset and let $A \subseteq S$

An element $a \in S$ is said to be upperbound for A if $xRa \ \forall \ x \in A$.

upperbound may / may not belong to A.

Least upper bound

$u \in S$ is said to least upper bound for set A if

i) u is upper bound

ii) there does not exist any $x \in A$ such that uRx.

lower bound

$b \in S$ is said to be lower bound if $bRx \ \forall \ x \in A$.

Greatest lower bound

An element $u' \in S$ is said to be greatest lower bound ~~of~~ for set A if

i) u' is lower bound

ii) there does not exist any $x \in A$ such that xRu'

Scanned by CamScanner

$(\mathbb{Z}, \leq)$

Let $A = \{1, 2, 3, \ldots, \infty\}$

Find least upperbound and greatest lower bound

No upperbound $\Rightarrow$ therefore no least upperbound.

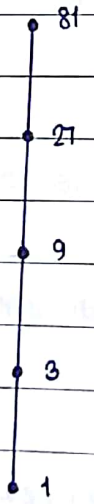
Greatest lower bound = 1

HASSE DIAGRAM

consider finite poset (S, R). The Hasse diagram for poset (S, R) is obtained as follows.

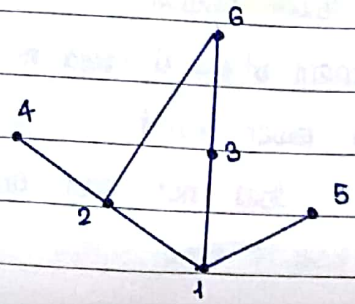
If y is immediate successor of element x then we represent (x, y) by points in plane and put y at higher level than x in plane and join x and y by straight line.

Find Hass diagram for poset $S = \{1, 3, 9, 27, 81\}$ with partial order '/'



2. $S = \{1, 2, 3, 4, 5, 6\}$

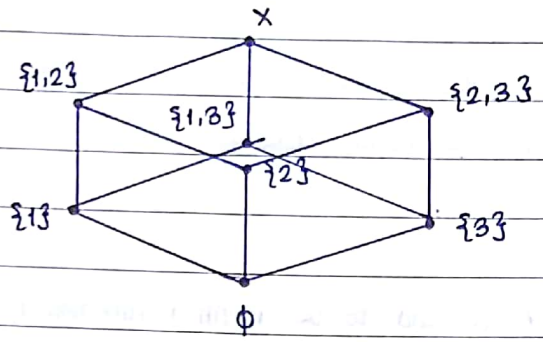
with partial order '/'



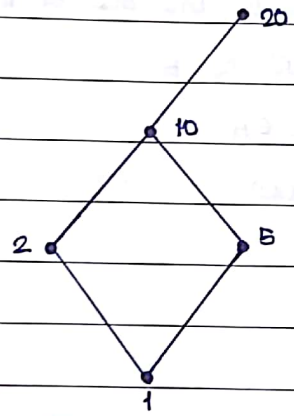
Scanned by CamScanner

3 Find Hass diagram $(P(X), \subseteq)$ where $X = \{1, 2, 3\}$

$P(X) = \{\phi, X, \{1\}, \{2\}, \{3\}, \{1,2\}, \{2,3\}, \{3,1\}\}$



4. Find Hass diagram for po-set $S = \{1, 2, 5, 10, 20\}$ with partial order '/'. Find least, greatest, minimal, maximal elements.



Function

18.01.2019

Let A and B are two non-empty set.

Function f from A to B denoted as $f: A \rightarrow B$ and it is an assignment which assigns to each element of A a unique element of B.

If under function f element $x \in A$ is assigned element y in B then we write it as $f(x) = y$.

y is called image of x under function f.

Set A is called domain of the function and set B is called co-domain of the function.

Range of the function

Scanned by CamScanner

Let $f: A \to B$ then the range of f is defined as

Range $(f) = \{ y \in B : y = f(x) \} \subseteq B$

1. constant function

A function $f: A \to B$ is said to be constant if

$f(x) = k$, k is some constant

2. Identity function

A function $I : A \to A$ is said to be identity function if

$I(x) = x \quad \forall \ x \in A$

3. One to one or injective function

A function $f: A \to B$ is said to be one-one or injective if f maps different elements of A to different elements of B.

that means whenever $x_1 \neq x_2 \in A$

$f(x_1) \neq f(x_2)$

or $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$

4. onto or subjective function

A function $f: A \to B$ is said to be onto or subjective if for each $y \in B$

$\exists$ some $x \in A$ such that $y = f(x)$

Note:

when the function is onto range of f is equal to codomain.

5. Bijective function

A function $f: A \to B$ is said to be bijective if it is both one to one and onto.

Inverse of a function

Scanned by CamScanner

Let $f: A \to B$ be a bijective function then inverse of f is denoted by f^{-1} and it is defined as $f^{-1}: B \to A$

Example: Define $f: \mathbb{N} \to \mathbb{Z}$ as $f(x) = x^2$

Find range of function.

Test if function is i) one to one

ii) onto

iii) bijective

$\therefore$ Range $(f) = \{ y \in \mathbb{Z} : y = f(x) \}$

$= \{ y \in \mathbb{Z} : y = x^2 \}$

$= \{ x^2 : x \in \mathbb{N} \}$

$= \{ 1, 4, 9, \ldots \} \subset \mathbb{Z}$

Range $(f) \neq \mathbb{Z}$

(i) one to one

Let x_1 and $x_2 \in \mathbb{N}$ such that

$f(x_1) = f(x_2)$

$x_1^2 = x_2^2$

$\Rightarrow x_1 = x_2$ (Since $x_1, x_2 \in \mathbb{N}$)

Hence function is one-one or injective.

(ii) onto

Let $y \in \mathbb{Z}$ such that $y = f(x)$

$y = x^2$

$x = \pm\sqrt{y}$

Since for $y = 3$

$x = \pm\sqrt{3} \notin \mathbb{N}$

Therefore it is not onto

Hence the function is not bijective.

Scanned by CamScanner

2. Define a function $f: \mathbb{R} \to \mathbb{R}$ as $f(x) = 2x+3$

show that f is bijective and hence find f^{-1}.

one-one

let $x_1, x_2 \in \mathbb{R}$ such that

$$f(x_1) = f(x_2)$$

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

$\Rightarrow 2x_1 = 2x_2$

$\Rightarrow x_1 = x_2$

Therefore, f is one-one.

onto

Let $y \in \mathbb{R}$ such that

$$y = f(x)$$

$\Rightarrow y = 2x+3$

$\Rightarrow x = \frac{y-3}{2} \in \mathbb{R} \ \forall \ y \in \mathbb{R}$

$\Rightarrow f$ is onto

Hence, f is bijective.

$f^{-1} : B \to A$

$f^{-1}(y) = \frac{y-3}{2}$

22.09.2019

1. Define $f: \mathbb{N} \to \mathbb{N}$ be defined as

$$f(x) = \begin{cases} \frac{n+1}{2}, & n \text{ is odd} \\ \frac{n}{2}, & n \text{ is even} \end{cases}$$

find whether f is bijective or not.

2. Define $f: \mathbb{R} - \{\frac{7}{5}\} \to \mathbb{R} - \{\frac{7}{5}\}$ and $f(x) = \frac{3x+4}{5x-7}$, show that f is bijective

Scanned by CamScanner

and hence find f^{-1}.

3. Define $f : \mathbb{R} \to \mathbb{R}$ as $f(x) = x^2 - 4x + 3$.

Find f is bijective.

4. Define $f : \mathbb{R} \to \mathbb{R}$ as

$$f(x) = \begin{cases} x^2 + 2 & , x \geq 0 \\ x + 2 & , x < 0 \end{cases}$$

Is f bijective? Justify your answer.

1. $f(x) = \begin{cases} \frac{n+1}{2} & , n \text{ is odd} \\ \frac{n}{2} & , n \text{ is even} \end{cases}$

case i) Let n_1, n_2 be odd such that

$$f(n_1) = f(n_2)$$

$$\frac{n_1 + 1}{2} = \frac{n_2 + 1}{2}$$

$$\Rightarrow n_1 = n_2$$

case ii) Let n_1, n_2 are even such that

$$f(n_1) = f(n_2)$$

$$\frac{n_1}{2} = \frac{n_2}{2}$$

$$n_1 = n_2$$

case iii) Let n_1 is odd and n_2 is even

To show $f(n_1) \neq f(n_2)$

Assume $f(n_1) = f(n_2)$

$$\Rightarrow \frac{n_1 + 1}{2} = \frac{n_2}{2}$$

$\Rightarrow n_1 + 1 = n_2$ which may be true for some n_1, n_2 or may not be true

Scanned by CamScanner

Hence whenever $n_1 \neq n_2$

does not imply $f(n_1) \neq f(n_2)$.

The function is not one-one.

onto

Range (f) = $A \cup B$

$A = \{ m \in \mathbb{N}$ such that $m = f(n)$, n is odd $\}$

$= \{1, 2, 3, \ldots\}$

$B = \{ m \in \mathbb{N}$ such that $m = f(n)$, n is even $\}$

$= \{1, 2, 3, \ldots\}$

Range (f) = $A \cup B$

$= \mathbb{N}$

= co-domain

The function is onto

since $A \cap B \neq \phi$. Hence function is not one-one.

1. test whether the function defined as

$$f(x) = \begin{cases} x^2 & , x \leq 0 \\ 2x & , x > 0 \end{cases}$$

where $f : \mathbb{R} \to \mathbb{R}$

is bijective or not.

Range (f) = $\mathbb{R}^+ + \mathbb{R}^+$

$\neq \mathbb{R}$

$\Rightarrow f$ is not onto

$\mathbb{R}^+ \cap \mathbb{R}^+ = \mathbb{R}^+ \neq \phi$

$\Rightarrow f$ is not one-one

4. $$f(x) = \begin{cases} x^2 + 2 & , x \geq 0 \\ x + 2 & , x < 0 \end{cases}$$

Range (f) = $A \cup B$

Scanned by CamScanner

$A = [2, \infty)$

$B = (-\infty, 2)$

Range $(f) = [2, \infty) \cup (-\infty, 2)$

$= (-\infty, \infty)$

$= \mathbb{R}$

$=$ co-domain

Therefore, f is onto

$A \cap B = \phi$

$\Rightarrow f$ is one-one

Therefore, f is bijective

5'. Define a function $f: \mathbb{R} \to \mathbb{R}$ and test if it is bijective.

$$f(x) = \begin{cases} x^2 + 2 & -1 \leq x \\ x + 2 & x < -1 \end{cases}$$

$D = D_1 \cup D_2$

$D_1 = [-1, \infty)$ and $D_2 = (-\infty, -1)$

$X = f(D_1) = [2, 3) \cup (2, \infty)$

$\uparrow$ A $\quad\quad$ $\uparrow$ B

$C = f(D_2) = (-\infty, 1)$

$A \cup B \cup C = (-\infty, 1) \cup [2, \infty) \neq \mathbb{R}$

$\Rightarrow f$ is not onto

$A \cap B \cap C \neq \phi$

$\Rightarrow f$ is not one-one

2. $f(x) = \dfrac{3x + 4}{5x - 7}$

one-one

Let $x_1, x_2 \in \mathbb{R} - \{\frac{7}{5}\}$ such that

$f(x_1) = f(x_2)$

Scanned by CamScanner

23.01.2019

MODULAR ARITHMETIC

congruence modulo 'm'

Let m be a positive integer then an integer a is congruent to an integer b modulo m if m divides b - a and this relation between a and b is denoted by the notation.

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

This is read as a congruent b modulo m

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

$$\Rightarrow \quad m \mid b-a$$

$$\Rightarrow \quad b-a = km, \quad k \in \mathbb{Z}$$

Theorem :

$a \equiv b \pmod{m}$ is an equivalence relation on set $\mathbb{Z}$

Proof :

Reflexivity

Let a be an arbitrary integer.

To prove $a \equiv a \pmod{m}$

Since $0 = 0.m$

$$\Rightarrow \quad m \mid 0$$

$$\Rightarrow \quad m \mid a-a$$

$$\Rightarrow \quad a \equiv a \pmod{m}$$

Symmetry

Let $a, b \in \mathbb{Z}$ such that $a \equiv b \pmod{m}$

$$\Rightarrow \quad m \mid b-a$$

$$\Rightarrow \quad b-a = km, \quad k \in \mathbb{Z}$$

$$\Rightarrow \quad a-b = (-k)m$$

$$\Rightarrow \quad m \mid a-b$$

$$\Rightarrow \quad b \equiv a \pmod{m}$$

Transitivity

Scanned by CamScanner

Let a, b and $c \in \mathbb{Z}$ such that

$a \equiv b \pmod m$ and $b \equiv c \pmod m$

$\Rightarrow m \mid b-a$ and $m \mid c-b$

$\Rightarrow b-a = k_1 m$ — ① and $c-b = k_2 m$ — ②

Adding ① and ②, we get

$c-a = (k_1+k_2)m$

$\Rightarrow m \mid c-a$

$\Rightarrow a \equiv c \pmod m$

Hence, congruence modulo relation on the set of integers is an equivalence relation.

Division algorithm or Division Lemma

Let a, b are two integers with $b \neq 0$.

Then we can find two integers say q and r such that

$$a = bq + r$$

where $0 \leq r < b$

Theorem:

$a \equiv b \pmod m$ iff a and b leave same remainder when divided by m.

Proof:

Suppose $a \equiv b \pmod m$

To show a and b leave same remainder when divided by m.

Let us assume that let r be the remainder.

Now, by division algorithm we have

$b = mq + r$ — ① where $0 \leq r < m$

since $a \equiv b \pmod m$

$a - b = mk_1$, $k_1 \in \mathbb{Z}$

$a = mk_1 + b$

$= mk_1 + mq + r$

Scanned by CamScanner

$a = m(k_1 + q) + r$ ——— ②

Hence, a and b leave same remainder when divided by m.

converse part:

Let a and $b \in \mathbb{Z}$ and m be a positive integer such that a and b leave the same remainder upon being divided by m. implies there exists integers r, q_1 and q_2 such that

$a = mq_1 + r$ ——— ③

$b = mq_2 + r$ ——— ④

subtracting ④ from ③

$a - b = m(q_1 - q_2) + r$

$\Rightarrow a \equiv b \pmod m$

Theorem

25.01.20

The integer r is remainder when a is divided by m iff

$a \equiv r \pmod m$, $0 \leq r < m$

Proof:

Let us assume that $a \equiv r \pmod m$

$\Rightarrow m \mid a - r$

$\Rightarrow a - r = mk$, $k \in \mathbb{Z}$

$\Rightarrow a = mk + r$ $0 \leq r < m$

This implies r is remainder when we divide a by m.

converse:

Let us assume that r is the remainder when we divide a by m

This implies there exists some integer q such that

$a = mq + r$, $0 \leq r < m$

$\Rightarrow a - r = mq$

$\Rightarrow m \mid a - r$

$\Rightarrow a \equiv r \pmod m$

From the last theorem it implies that every integer a is congruent to its remainder r modulo m.

Scanned by CamScanner

r is called least residue of a modulo m.

Now, since integer r has exactly m choices $0, 1, \ldots, m-1$

Therefore, every integer a is congruent to exactly 1 of $0, 1, \ldots, m-1$ modulo m

Prove that no prime number of the form $4n+3$ can be expressed as the sum of two squares.

Proof:

Let N be a prime number such that

$$N = 4n + 3 \quad \text{——— ①}$$

$$\Rightarrow N \equiv 3 \pmod 4 \quad \text{——— ②}$$

Assume $N = A^2 + B^2$

25.01.2019 Since N is odd this implies either A^2 is odd or B^2 is odd.

Let A^2 is odd, then B^2 will be even

$A^2 = (2n+1)^2$

$B^2 = (2n)^2$

$N = (2n+1)^2 + (2n)^2$

$= 4n^2 + 1 + 4n + 4n^2$

$= 8n^2 + 4n + 1$

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

$N = 4q + 1 \qquad q = 2n^2 + n$

$\Rightarrow N \equiv 1 \pmod 4$, but we also have $N \equiv 3 \pmod 4$ which is not possible

Since we know that every integer a is exactly congruent to one of the values $0, 1, \ldots, m-1$ modulo m.

Therefore, our assumption $N = A^2 + B^2$ is not true

Therefore $N = 4n+3$ cannot be expressed as a sum of squares of two numbers.

~~let~~ Theorem :

Let $a \equiv b \pmod m$ and $c \equiv d \pmod m$

then i) $a+c \equiv b+d \pmod m$

ii) $ac \equiv bd \pmod m$

Scanned by CamScanner

Proof :

Given $a \equiv b \pmod m$

$\Rightarrow a - b = k_1 m$, $k_1 \in \mathbb{Z}$ ——— (I)

$c \equiv d \pmod m$

$\Rightarrow c - d = k_2 m$, $k_2 \in \mathbb{Z}$ ——— (II)

i) $(a+c)-(b+d) = (a-b) + (c-d)$

$= k_1 m + k_2 m$

$= (k_1 + k_2) m$

Thus implies $m \mid (a+c) - (b+d)$

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

ii) Multiplying (I) by c and (II) by b we get

$ac - bc = k_1 cm$ ——— (III)

and $bc - bd = k_1 bm$ ——— (IV)

Adding (III) and (IV) we get

$ac - bd = k_1 cm + k_2 bm$

$ac - bd = (k_1 c + k_2 b) m$

Thus implies $m \mid ac - bd$

$\Rightarrow ac \equiv bd \pmod m$

Find the remainder when $1! + 2! + \ldots + 100!$ is divided by 15.

$1! = 1 = 1 \pmod{15}$

$2! = 2! \pmod{15}$

$3! = 3! \pmod{15}$

$4! = 4! \pmod{15}$

$24 = 9 \pmod{15}$

$\Rightarrow 4! = 9 \pmod{15}$

$5! = 0 \pmod{15}$

$6! = 0 \pmod{15}$

. .

. .

. .

Scanned by CamScanner

$k! \equiv 0 \pmod{15} \quad \forall\ k \geq 5$

$1! + 2! + 3! + 4! + \ldots + 100! \equiv 1 + 2 + 9 + 6 + 9 + 0 + \ldots + 0 \pmod{15}$

$\equiv 18 \pmod{15}$

$\equiv 3 \pmod{15}$

Theorem:

Let $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$

Then $a - c \equiv b - d \pmod{m}$

Proof: Given $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$

$\Rightarrow a - b = k_1 m$ and $c - d = k_2 m$, $k_1, k_2 \in \mathbb{Z}$

$(a - c) - (b - d) = (a - b) - (c - d)$

$= k_1 m - k_2 m$

$= (k_1 - k_2)\, m$

This implies $m \mid (a - c) - (b - d)$

$\Rightarrow a - c \equiv b - d \pmod{m}$

Theorem:

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

and let $c \in \mathbb{Z}$

Then 1. $a + c \equiv b + c \pmod{m}$

2. $ac \equiv bc \pmod{m}$

3. $a - c \equiv b - c \pmod{m}$

4. $a^2 \equiv b^2 \pmod{m}$

In general $a^n \equiv b^n \pmod{m} \quad \forall\ n \in \mathbb{N}$

Proof

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

$\Rightarrow a - b = km, \quad k \in \mathbb{Z}$ ——————— ①

1. $(a + c) - (b + c) = a - b$

$= km$ (By ①)

Scanned by CamScanner

$\Rightarrow \quad a+c \equiv b+c \pmod{m}$

2. ~~Multiplying a by c, we get~~

$ac - bc = (kc)m = c(a-b)$

$= c(km) \qquad$ (By ①)

$= (kc)m$

$= pm \qquad$ where $p = kc \in \mathbb{Z}$

$\Rightarrow \quad ac \equiv bc \pmod{m}$

3. $(a-c) - (b-c) = a - b$

$= km \qquad$ (By ①)

$\Rightarrow \quad (a-c) \equiv b-c \pmod{m}$

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

and $c \equiv d \pmod{m}$

$\Rightarrow \quad ac \equiv bd \pmod{m}$

let $c = a$ and $d = b$

$\Rightarrow \quad a^2 \equiv b^2 \pmod{m}$

Find the remainder when 16^{53} is divided by 7

$16 \equiv 2 \pmod{7}$ ——————— ①

$\Rightarrow \quad 16^{53} \equiv 2^{53} \pmod{7}$ ——————— ②

$53 = 17 \times 3 + 2$

$2^{53} = (2^{17})^3 \cdot 2^2$

$= (2^3)^{17} \cdot 2^2$

NOW $2^3 \equiv 1 \pmod{7}$

$(2^3)^{17} \equiv 1 \pmod{7}$

$2^{51} \equiv 1 \pmod{7}$

$(2^{51})\,2^2 \equiv 4 \pmod{7}$

$2^{53} \equiv 4 \pmod{7}$ ——————— ③

Scanned by CamScanner

From ② and ③,

$16^{53} = 4 \pmod 7$ (by transitivity)

$\Rightarrow$ 4 is the remainder when 16^{53} is divided by 7.

29.01.2019

1. Find remainder when 3^{247} is divided by 17

2. Find remainder when 3^{247} is divided by 25

3. Find remainder when 3^{181} is divided by 17

4. Find remainder when $1! + 2! + 3! + \ldots + 1000!$ is divided by 10

5. Find remainder when $1! + 2! + 3! + \ldots + 300!$ is divided by 13.

EULER'S FUNCTION

Let n be a positive integer then Euler's function is defined as

$\phi(n)$ = Number of positive integers less than or equal to n and relative prime to n

Note:

Two integers say a and b are said to be relative prime if $(a, b) = 1$

(a, b) → GCD of a, b

Example: $\phi(1) = 1$

$\phi(2) = 1$

$\phi(3) = 2$

$\phi(4) = 2$

$\phi(5) = 4$

Theorem:

Scanned by CamScanner

Let p be a prime number

Then $\phi(p) = p-1$

Theorem:

Let p be a prime number and k be a positive integer

Then $\phi(p^k) = p^k\left[1-\frac{1}{p}\right]$

Theorem:

Let m and n are two relatively prime positive prime numbers.

Then $\phi(mn) = \phi(m)\,\phi(n)$

Fermat's Theorem

Theorem 1:

Let p be a prime number and a be a positive integer such that $(a, p) = 1$.

Then $a^{p-1} \equiv 1 \pmod{p}$

Theorem 2:

Let p be a prime number and a be a positive integer such that $(a, p) = 1$.

Then $a^p \equiv a \pmod{p}$

Euler's Generalised Fermat's Theorem

Suppose a and m are two positive integers such that $(a, m) = 1$

Then $a^{\phi(m)} = 1 \pmod{p}$

where p is a prime number

Prove that $n^{16} - 1$ is divisible by 17

~~Sol~~ $(17, n) = 1$

$n^{17-1} \equiv 1 \pmod{17}$

Scanned by CamScanner

$n^{16} \equiv 1 \pmod{17}$

$17 \mid n^{16} - 1$

Prove that $x^{12} - y^{12}$ is divisible by 13 if x and y are co-prime to 13.

Since x and 13 are co-prime

$(x, 13) = 1$

By Fermat's theorem,

$x^{12} \equiv 1 \pmod{13}$ ——— ①

$(y, 13) = 1$

By Fermat's theorem,

$y^{12} \equiv 1 \pmod{13}$ ——— ②

Therefore, $x^{12} - y^{12} \equiv 0 \pmod{13}$

This implies $13 \mid x^{12} - y^{12}$

~~Prove that~~ If n and a are co-prime to 91 then prove that $n^{12} - a^{12}$ is divisible by 91.

~~Since~~ Given $(n, 91) = 1$ and $(a, 91) = 1$

& we have $91 = 13 \times 7$

Now, since 13 and 7 are prime numbers

$\Rightarrow (n, 13) = 1$ and $(a, 13) = 1$

$(n, 7) = 1$ and $(a, 7) = 1$

Since $(n, 13) = 1$ and $(a, 13) = 1$

$n^{12} \equiv 1 \pmod{13}$ ~~and $a^{12} \equiv 1 \pmod{13}$~~ ——— ①

and $a^{12} \equiv 1 \pmod{13}$ ——— ⑪

This implies $n^{12} - a^{12} \equiv 0 \pmod{13}$

$\Rightarrow 13 \mid n^{12} - a^{12}$ ——— ①

Again since $(n, 7) = 1$ and $(a, 7) = 1$

$n^6 \equiv 1 \pmod{7}$ ——— ⑪

and $a^6 \equiv 1 \pmod{7}$ ——— ⑩

$\Rightarrow (n^6)^2 = 1 \pmod{7} \Rightarrow n^{12} = 1 \pmod{7}$ ——— ⑪'

Scanned by CamScanner

similarly from (iv)

$a^{12} \equiv 1 \pmod 7$ ——— (iv)'

$n^{12} - a^{12} \equiv 0 \pmod 7$

$\Rightarrow 7 \mid n^{12} - a^{12}$ ——— (2)

since 7 and 13 are prime numbers and both 7 and 13 divide $n^{12} - a^{12}$

therefore $13 \times 7 = 91$ also divides $n^{12} - a^{12}$

$91 \mid n^{12} - a^{12}$

show that $a^{18} - b^{18}$ is divisible by 133 if both a and b are co-prime to 133.

Given $(a, 133) = 1$ ——— (i)

$(b, 133) = 1$ ——— (ii)

New $133 = 19 \times 7$

both 19 and 7 are prime numbers

$\Rightarrow (a, 19) = 1$ and $(b, 19) = 1$

$(a, 7) = 1$ and $(b, 7) = 1$

since $(a, 19) = 1$ and $(b, 19) = 1$

By fermat's theorem

$a^{18} \equiv 1 \pmod{19}$

and $b^{18} \equiv 1 \pmod{19}$

this implies $a^{18} - b^{18} \equiv 0 \pmod{19}$

$\Rightarrow 19 \mid a^{18} - b^{18}$

Again since $(a, 7) = 1$ and $(b, 7) = 1$

By fermat's theorem

$a^6 \equiv 1 \pmod 7$

and $b^6 \equiv 1 \pmod 7$

$\Rightarrow (a^6)^3 \equiv 1 \pmod 7 = a^{18} \equiv 1 \pmod 7$

similarly from (iv)

$b^{18} \equiv 1 \pmod 7$

Scanned by CamScanner

$a^{18} - b^{18} \equiv 0 \pmod 7$

$7 \mid a^{18} - b^{18}$

Since 7 and 19 are prime numbers and both 19 and 7 divide $a^{18} - b^{18}$

therefore $19 \times 7 = 133$ also divides $a^{18} - b^{18}$

$133 \mid a^{18} - b^{18}$

Scanned by CamScanner

30.01.2019

UNIT-2

PROPOSITIONAL CALCULUS

Any sentence that is true or false is known as proposition and it is denoted by p, q, r, etc.

p : today is sunday

q : we will go on picnic tomorrow

connectives (operators)

Propositions can be combined to form more complicated propositions by using words such as not, or, and, if then, if and only if. These combining operations are known as connectives or operators and they are denoted by the following notations.

1. $\neg$ not, negation
2. $\wedge$ and, conjunction
3. $\vee$ or, disjunction
4. $\rightarrow$ if then, conditional proposition, implication
5. $\leftrightarrow$ if and only if, biconditional

Example:

The expression $p \rightarrow q$ is read as 'if p then q' where p and q are two propositions.

The expression $p \wedge q$ is read as 'p and q' or 'p conjunction q'

Truth table

Truth table is a table that defines connectives for all possible truth values of their variables.

~~Truth table for~~

Truth table for $\neg$, $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$

Scanned by CamScanner

p	q	$\neg p$	$p \wedge q$	$p \vee q$	$p \rightarrow q$
T	T	F	T	T	T
F	F	T	F	F	T
T	F	F	F	T	F
F	T	T	F	T	T

well formed formulas

~~like any other programming language or any natural language whenever we deal with symbols.~~

Truth symbols is denoted by T or F

A well-formed formula is either a truth symbol or a propositional variable or negation of a propositional variable or a conjunction of two well-formed formulas or a disjunction of two well formed formulas or an implication of one well formed formula to another well formed formula surrounded by parantheses.

examples of some well-formed formula

1. $p \rightarrow q$
2. $\neg p \wedge q$
3. $\neg p \wedge q \vee (p \rightarrow q)$

Tautologies, contradictions and contigency

A well-formed formula is known as a tautology if all the truth table values of truth table are true.

Example : $p \vee \neg p$ is a tautology.

Scanned by CamScanner

p	¬p	p ∨ ¬p
T	F	T
F	T	T

contradiction

If all the ~~values~~ truth table values of a well-formed formula are false, then the well formed formula is called a contradiction.

Example : $p \wedge \neg p$ is a contradiction

p	¬p	p ∧ ¬p
T	F	F
F	T	F

contigency

A well formed formula is called if it contains

Equivalence of well-formed formulas

Two well formed ~~formulas are said to be~~ P and Q are said to be logically equivalent if they have the

$$P \equiv Q$$

Example : $p \rightarrow q \equiv \neg p \vee q$

Proof : Truth table

p	q	¬p	p → q	¬p ∨ q
T	T	F	T	T
F	F	T	T	T
T	F	F	F	F
F	T	T	T	T

Scanned by CamScanner

Therefore, $p \rightarrow q \equiv \neg p \vee q$

Basic equivalences

1. Idempotent
   a) $p \vee p \equiv p$
   b) $p \wedge p \equiv p$

2. Commutativity
   a) $p \vee q \equiv q \vee p$
   b) $p \wedge q \equiv q \wedge p$

3. Associativity
   a) $p \vee (q \vee r) \equiv (p \vee q) \vee r$
   b) $p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r$

4. Distributive
   a) $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
   b) $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$

5. Involution
   $\neg(\neg p) \equiv p$

6. Identity
   a) $p \vee F \equiv p$
   b) $p \vee T \equiv T$
   c) $p \wedge F \equiv F$
   d) $p \wedge T \equiv p$

7. Complement laws

Scanned by CamScanner

a) $p \vee \neg p \equiv T$

b) $p \wedge \neg p \equiv F$

c) $\neg T \equiv F$

d) $\neg F \equiv T$

8. Absorption laws

a) $p \wedge (p \vee q) \equiv p$

b) $p \vee (p \wedge q) \equiv p$

9. DeMorgan's laws

a) $\neg (p \vee q) \equiv \neg p \wedge \neg q$

b) $\neg (p \wedge q) \equiv \neg p \vee \neg q$

Show that

1. $(p \wedge q) \vee (p \wedge \neg q) \equiv p$

Proof :

LHS $= (p \wedge q) \vee (p \wedge \neg q)$

$\equiv p \wedge (q \vee \neg q)$

$\equiv p \wedge T$

$\equiv p$

04.02.2019

2. $(p \rightarrow q) \wedge (r \rightarrow q) \equiv (p \vee r) \rightarrow q$

LHS

$(p \rightarrow q) \wedge (r \rightarrow q)$

$\equiv (\neg p \vee q) \wedge (\neg r \vee q)$ $(p \rightarrow q \equiv \neg p \vee q)$

$\equiv q \vee (\neg p \wedge \neg r)$ (By distributive property)

$\equiv q \vee \neg (p \vee r)$

$\equiv \neg (p \vee r) \vee q$

$\equiv (p \vee r) \rightarrow q$

$\equiv$ RHS

Scanned by CamScanner

3. $p \rightarrow (q \rightarrow r) \equiv q \rightarrow (p \rightarrow r)$

LHS $\equiv p \rightarrow (q \rightarrow r)$

$\equiv \neg p \vee (q \rightarrow r)$

$\equiv \neg p \vee (\neg q \vee r)$

$\equiv \neg p \vee \neg q \vee r$ ——— ①

RHS $\equiv q \rightarrow (p \rightarrow r)$

$\equiv \neg q \vee (p \rightarrow r)$

$\equiv \neg q \vee (\neg p \vee r)$

$\equiv \neg p \vee \neg q \vee r$ ——— ②

Therefore from ① and ② LHS $\equiv$ RHS

TRUTH FUNCTIONS AND NORMAL FORM

A truth function is a function whose arguments can take only values which are either true or false.

$P(p, q, r) = p \rightarrow (q \rightarrow r)$

$P(p, q) = p \wedge q$

Note:

Every truth function is a well formed formula

LITERALS

A literal is propositional variable or its negation.

For example, p and $\neg p$ are literals.

FUNDAMENTAL CONJUNCTIONS

Fundamental conjunction is either a literal or conjunction of 2 or more than 2 literals.

Scanned by CamScanner

Example i) p

ii) $p \wedge \neg q$

iii) $p \wedge \neg p \wedge r$

DISJUNCTIVE NORMAL FORM

A disjunctive normal form is either a fundamental conjunction or disjunction of two or more than two fundamental conjunctions.

Example : i) p

ii) $p \vee (p \wedge q)$

iii) $(p \wedge \neg q) \vee (\neg p \wedge r) \vee p$

PRINCIPAL OR FULL DISJUNCTIVE NORMAL FORM

A disjunctive normal form is said to be principal or full disjunctive normal form if each fundamental conjunction has exactly n literals, one for each of the n variables appearing in the well formed formula.

FUNDAMENTAL DISJUNCTION

A fundamental disjunction is either a literal or disjunction of 2 or more than 2 literals.

Example i) p

ii) $p \vee q$

iii) $\neg p \vee q \vee r$

CONJUNCTIVE NORMAL FORM

A conjunctive normal form is either a fundamental disjunction or conjunction of 2 or more than 2 fundamental disjunctions

Example i) p

Scanned by CamScanner

ii) $p \wedge (p \vee q)$

iii) $(p \vee \neg q) \wedge (\neg p \vee r) \wedge p$

PRINCIPAL OR FULL CONJUNCTIVE NORMAL FORM

A conjunctive normal form is said to be principal or full conjunctive normal form if each fundamental disjunction ~~that~~ contains n literals, for each of the n variables appearing in the well formed formula.

Note:

i) A well formed formula which is not a contradiction is equivalent to a disjunctive normal form.

ii) A well formed formula which is not a tautology is equivalent to a conjunctive normal form.

Obtain the principal disjunctive normal form of the following well formed formula

i) $p \wedge (p \rightarrow q)$

ii) $p \vee (\neg p \rightarrow (q \vee (q \rightarrow \neg r)))$

iii) $p \rightarrow (p \rightarrow q) \wedge (\neg(\neg q \vee \neg p))$

i) $p \wedge (p \rightarrow q)$

$\equiv p \wedge (\neg p \vee q)$

$\equiv (p \wedge \neg p) \vee (p \wedge q)$

$\equiv f \vee (p \wedge q)$

$\equiv p \wedge q$ (principal disjunctive Normal form)

05.02.2019

ii) $p \vee (\neg p \rightarrow (q \vee (q \rightarrow \neg r)))$

$\equiv p \vee (\neg p \vee (q \vee (q \rightarrow \neg r)))$

$\equiv p \vee [p \vee [q \vee (\neg q \vee \neg r)]]$

Scanned by CamScanner

$\equiv p \vee p \vee q \vee \neg q \vee r$

$\equiv p \vee q \vee \neg q \vee r$

$\equiv T$

iii) $p \rightarrow (p \rightarrow q) \wedge [\neg(q \vee \neg p)] \vee (p \rightarrow q)$

$\equiv \neg p \vee (p \rightarrow q) \wedge [q \vee p] \vee (p \rightarrow q)$

$\equiv \neg p \vee (\neg p \vee q) \wedge (q \vee p) \vee (\neg p \vee q)$

$\equiv (q \vee p) \vee (\neg p \wedge q)$

$\equiv (p \wedge q) \vee (\neg p \vee q)$

$\equiv (p \wedge q) \vee (p \wedge q)$ $[(r \vee p) \wedge [r \wedge q] \vee p] \equiv (p \wedge q) \vee (p \wedge r)]$

$\equiv (p \wedge q \wedge \neg p) \vee (p \wedge q \wedge q)$

$\equiv F \vee (p \wedge q)$

$\equiv p \wedge q$

obtain the principal disjunctive normal form of the following well formed formulas:

i) $(p \rightarrow q) \rightarrow p$

ii) $(q \wedge \neg p) \rightarrow p$

iii) $p \rightarrow (q \rightarrow p)$

iv) $(p \wedge q) \wedge r$

v) $p \rightarrow (q \wedge r)$

v) Given $p \rightarrow (q \wedge r)$

$\equiv \neg p \vee (q \wedge r)$ (Disjunctive normal form)

$\equiv [\neg p \wedge (q \vee \neg q)] \wedge [(\neg r \wedge r) \vee (q \wedge r)]$

$\equiv [(\neg p \wedge q) \vee (p \wedge \neg q)] \wedge [(\neg r \vee r) \wedge (q \vee r)]$

$\equiv (\neg p \wedge q \wedge r) \vee (\neg p \wedge q \wedge \neg r) \vee (p \wedge \neg q \wedge r) \vee (p \wedge \neg q \wedge \neg r)$

$\equiv (\neg p \wedge q \wedge r) \vee (\neg p \wedge q \wedge \neg r) \vee (p \wedge \neg q \wedge r) \vee (p \wedge \neg q \wedge \neg r)$

(Principal disjunctive normal form)

Scanned by CamScanner

iv) $(p \vee q) \wedge r$

$\equiv r \wedge (p \vee q)$

$\equiv (r \wedge p) \vee (r \wedge q)$ (disjunctive normal form)

$\equiv [(p \wedge r) \wedge (q \vee \neg q)] \vee [(r \wedge q) \wedge (p \vee \neg p)]$

$\equiv (p \wedge q \wedge r) \vee (p \wedge \neg q \wedge r) \vee (r \wedge q \wedge p) \vee (r \wedge q \wedge \neg p)$

$\equiv (p \wedge q \wedge r) \vee (p \wedge \neg q \wedge r) \vee (r \wedge q \wedge p)$ (principal disjunctive normal form)

iii) $p \rightarrow (q \rightarrow p)$

$\equiv \neg p \vee (q \rightarrow p)$

$\equiv (q \rightarrow p) \wedge \bot$

$\equiv \top$

ii) $(q \wedge \neg p) \rightarrow p$

$\equiv \neg(q \wedge \neg p) \vee p$

$\equiv \neg q \vee p \vee p$

$\equiv p \vee \neg q$ (principal disjunctive normal form)

i) $p \rightarrow (q \rightarrow p)$

$\equiv \neg(p \rightarrow q) \vee (p \rightarrow p)$

$\equiv \neg(\neg p \vee q) \vee p$

$\equiv (p \wedge \neg q) \vee p$

$\equiv p \vee (p \wedge \neg q)$ (disjunctive normal form)

~~$\equiv (p \vee p) \wedge (p \vee \neg q)$~~

~~$\equiv p \wedge (p \vee \neg q)$~~

~~$\equiv p \vee (p \wedge \neg q)$~~

$\equiv [p \wedge (q \vee \neg q)] \vee (p \wedge \neg q)$

$\equiv (p \wedge q) \vee (p \wedge \neg q) \vee (p \wedge \neg q)$

$\equiv (p \wedge q) \vee (p \wedge \neg q)$ (principal disjunctive normal form)

Obtain the principal conjunctive normal form of the following well formed

Scanned by CamScanner

formulas

i) ~~$p \to \neg p$~~ $p \wedge (p \to q)$

ii) $[q \vee (p \wedge r)] \vee \neg [(p \vee r) \wedge q]$

i) $p \wedge (p \to q)$

$\equiv p \wedge (\neg p \vee q)$ (conjuctive normal form)

$\equiv [p \vee (q \wedge \neg q)] \wedge (\neg p \vee q)$

$\equiv (p \vee q) \wedge (p \vee \neg q) \wedge (\neg p \vee q)$ (principal conjunctive normal form)

ii) $[q \vee (p \wedge r)] \wedge \neg [(p \vee r) \wedge q]$

$\equiv [q \vee (p \wedge r)] \wedge [\neg (p \vee r) \vee \neg q]$

$\equiv [q \vee (p \wedge r)] \wedge [(\neg p \wedge \neg r) \vee \neg q]$

$\equiv (q \vee p) \wedge (q \vee r) \wedge (\neg p \wedge \neg q) \vee (\neg r \wedge \neg q)$

$\equiv (p \vee q) \wedge (q \vee r) \wedge (\neg p \vee \neg q) \wedge (\neg r \vee \neg q)$ (conjunctive normal form)

$\equiv [(p \vee q) \vee (r \wedge \neg r)] \wedge [(q \vee p) \vee (r \wedge \neg r)] \vee [(\neg r \vee r) \wedge (\neg p \vee \neg q)]$

$\equiv (p \vee q \vee r) \wedge (p \vee q \vee \neg r) \vee (r \wedge p \vee \neg p) \vee (r \wedge q \vee \neg p) \vee (r \wedge q \vee \neg q)$

$(r \wedge \neg p \vee \neg r) \vee (r \wedge \neg q \vee \neg r) \vee (\neg r \wedge p \vee q) \vee$

$(r \wedge \neg p \vee \neg q) \vee (r \wedge \neg q \vee \neg q)$

$\equiv (p \vee q \vee r) \wedge (p \vee q \vee \neg r) \wedge (r \wedge p \vee \neg p) \vee (r \wedge q \vee \neg p) \vee (r \wedge q \vee \neg q)$

$(r \wedge \neg p \vee \neg r) \vee (r \wedge \neg q \vee \neg r) \vee (\neg r \wedge p \vee q) \vee$

$(r \wedge \neg p \vee \neg q) \vee (r \wedge \neg q \vee \neg q)$ (principal conjunctive normal form)

08.02.2019

obtain the principal conjunctive normal form of the following well formed formulas

1. $p \wedge q$
2. $(\neg p \to r) \wedge (q \leftrightarrow p)$
3. $p \to [(p \to q) \wedge \neg (\neg q \vee p)]$

1. $p \wedge q$

$\equiv [p \vee (q \wedge \neg q)] \wedge [q \vee (p \wedge \neg p)]$

$\equiv (p \vee q) \wedge (p \vee \neg q) \wedge (q \vee p) \wedge (q \vee \neg p)$

$\equiv (p \vee q) \wedge (p \vee \neg q) \wedge (\neg p \vee q)$

Scanned by CamScanner

2. $(\neg p \rightarrow r) \wedge (q \leftrightarrow p)$

Prove that $p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$

Proof using truth table

p	q	$p \leftrightarrow q$	$p \rightarrow q$	$q \rightarrow p$	$(p \rightarrow q) \wedge (q \rightarrow p)$
T	T	T	T	T	T
F	F	F	T	T	T
T	F	F	F	T	F
F	T	F	T	F	F

Therefore $p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$

2. $(\neg p \rightarrow r) \wedge (q \leftrightarrow p)$

$\equiv (p \vee r) \wedge (p \rightarrow q) \wedge (q \rightarrow p)$

$\equiv (p \vee r) \wedge (\neg p \vee q) \wedge (\neg q \vee p)$ (Conjunctive Normal Form)

$\equiv [(p \vee r) \vee (q \wedge \neg q)] \wedge [(\neg p \vee q) \vee (r \wedge \neg r)] \wedge [(p \vee \neg q) \vee (r \wedge \neg r)]$

$\equiv$ ~~$[(p \vee r \vee q)$~~ $(p \vee q \vee r) \wedge (p \vee \neg q \vee r) \wedge (\neg p \vee q \vee r) \wedge (\neg p \vee q \vee \neg r) \wedge (p \vee \neg q \vee r) \wedge (p \vee \neg q \vee \neg r)$

$\equiv (p \vee q \vee r) \wedge (p \vee \neg q \vee r) \wedge (\neg p \vee q \vee r) \wedge (\neg p \vee q \vee \neg r) \wedge (p \vee \neg q \vee \neg r)$

(Principal conjunctive normal ~~Prime~~ form)

3. $p \rightarrow [(p \rightarrow q) \wedge \neg(\neg q \vee p)]$

$\equiv \neg p \vee [$ ~~$(\neg p \vee q) \wedge (q \wedge \neg p)]$~~ $(p \rightarrow q) \wedge \neg(\neg q \vee p)]$

$\equiv \neg p \vee [(\neg p \vee q) \wedge (q \wedge \neg p)]$

$\equiv$ ~~$\neg p \vee [(\neg p \vee q) \wedge (q \wedge \neg p)]$~~

$\equiv (\neg p \vee \neg p \vee q) \wedge [\neg p \vee (q \wedge \neg p)]$

$\equiv (\neg p \vee q) \wedge (\neg p \vee q) \wedge (\neg p \vee \neg p)$

$\equiv (\neg p \vee q) \wedge \neg p$ (conjunctive normal form)

$\equiv (\neg p \vee q) \wedge [\neg p \vee (q \wedge \neg p)]$

$\equiv (\neg p \vee q) \wedge (\neg p \vee q) \wedge (\neg p \vee \neg q)$

$\equiv (\neg p \vee q) \wedge (\neg p \vee \neg q)$ (Principal conjunctive normal form)

Scanned by CamScanner

Functionally complete set of connectives

Any set of connectives in which any well formed formula can be expressed as an equivalent well formed formula containing connectives from the set.

Prove that the set containing $A = \{\neg, \vee\}$ and $B = \{\neg, \wedge\}$ are functionally complete set of connectives.

$A = \{\neg, \vee\}$

i) $P \equiv \neg(\neg P)$

ii) $P \wedge Q \equiv \neg(\neg(P \wedge Q))$

$\equiv \neg(\neg P \vee \neg Q)$

iii) $P \rightarrow Q \equiv \neg P \vee Q$

iv) $P \leftrightarrow Q \equiv (P \rightarrow Q) \wedge (Q \rightarrow P)$

$B = \{\neg, \wedge\}$

i) $P \equiv \neg(\neg P)$

ii) $P \vee Q \equiv \neg(\neg(P \vee Q))$

$\equiv \neg(\neg P \wedge \neg Q)$

iii) $P \rightarrow Q \equiv \neg P \vee Q$

$\equiv \neg[\neg(\neg P \vee Q)]$

$\equiv \neg(P \wedge \neg Q)$

iv) $P \leftrightarrow Q \equiv (P \rightarrow Q) \wedge (Q \rightarrow P)$

NAND and NOR connectives

NAND

It is denoted by the symbol $\uparrow$ and defined as

$P \uparrow Q \equiv \neg(P \wedge Q)$

Scanned by CamScanner

AND NOR

It is denoted ~~as~~ by the symbol $\downarrow$ and defined as

$$P \downarrow Q \equiv \neg(P \vee Q)$$

Show that the ~~set~~ sets

i) $A = \{\uparrow\}$

ii) $B = \{\downarrow\}$

are functionally complete

i) $A = \{\uparrow\}$

i) $\neg P \equiv \neg(P \wedge P)$

$\equiv$ ~~$P \uparrow P$~~ $P \uparrow P$

ii) $P \wedge Q \equiv \neg(\neg(P \wedge Q))$

$\equiv \neg(P \uparrow Q)$

$\equiv (P \uparrow Q) \uparrow (P \uparrow Q)$

iii) $P \vee Q \equiv \neg(\neg(P \vee Q))$

$\equiv \neg(\neg P \wedge \neg Q)$

$\equiv \neg P \uparrow \neg Q$

$\equiv (P \uparrow P) \uparrow (Q \uparrow Q)$

iv) $P \rightarrow Q \equiv \neg P \vee Q$

$\equiv \neg(\neg(\neg P \vee Q))$

$\equiv \neg(P \wedge \neg Q)$

$\equiv P \uparrow \neg Q$

$\equiv P \uparrow (Q \uparrow Q)$

v) $P \leftrightarrow Q \equiv (P \rightarrow Q) \wedge (Q \rightarrow P)$

$\equiv \neg[\neg((P \rightarrow Q) \wedge (Q \rightarrow P))]$

ii) $B = \{\downarrow\}$

i) $\neg P \equiv \neg(P \vee P)$

$\equiv P \downarrow P$

Scanned by CamScanner

ii) $P \wedge Q \equiv \neg(\neg(P \wedge Q)$

$\equiv \neg(\neg P \vee \neg Q)$

$\equiv \neg P \downarrow \neg Q$

$\equiv (P \downarrow P) \downarrow (Q \downarrow Q)$

iii) $P \vee Q \equiv \neg(\neg(P \vee Q)$

$\equiv \neg(P \downarrow Q)$

$\equiv (P \downarrow Q) \downarrow (P \downarrow Q)$

iv) $P \rightarrow Q \equiv \neg P \vee Q$

$\equiv \neg(\neg(\neg P \vee Q)$

$\equiv \neg(\neg P \downarrow Q)$

$\equiv (\neg P \downarrow Q) \downarrow (\neg P \downarrow Q)$

$\equiv [(P \downarrow P) \downarrow Q] \downarrow [(P \downarrow P) \downarrow Q]$

v) $P \leftrightarrow Q \equiv (P \rightarrow Q) \wedge (Q \rightarrow P)$

$\equiv \neg(\neg((P \rightarrow Q) \wedge (Q \rightarrow P)))$

$\equiv \neg(\neg(P \rightarrow Q) \vee \neg(Q \rightarrow P))$

$\equiv [\neg(P \rightarrow Q)] \downarrow [\neg(Q \rightarrow P)]$

08.02.2019

Tautological Implications

A statement P is said to be tautologically implies another statement Q iff and only if $P \rightarrow Q$ is a tautology.

We denote it as $P \Rightarrow Q$

Converse of a statement formula

The converse of the implication $P \rightarrow Q$ is $Q \rightarrow P$

and $\neg P \rightarrow \neg Q$ is called inverse of the implication $P \rightarrow Q$

$\neg Q \rightarrow \neg P$ is called contrapositive of the implication $P \rightarrow Q$

Theory Inference for statement or propositional calculus

The main purpose of a logic is to provide rules of inference or principle of reasoning. The theory associated with such rules is called

Scanned by CamScanner

Inference theory.

This theory is concerned with inferring a conclusion from certain premises or hypothesis.

The rules of inference are criteria for determining value of an argument (sequence of statements or propositions)

All statements except the final one are called premises or hypothesis and the final statement is called as conclusion.

In any argument a conclusion is admitted to be true provided that the premises are ~~er~~ accepted as true and the reasoning used for deriving the conclusion from premises follows certain accepted rules of logical inference.

Formal Proof:

When a conclusion is derived from a set of premises or hypothesis using certain accepted rules of inference then such a derivation is called a deduction or a formal proof.

Definition

Any conclusion which is arrived at by following rules of inference is called a valid conclusion and the argument is known as valid argument.

Validity using truth table

Let P and Q are two ~~well~~ statement formulas or well formed formulas. We say Q logically follows from A or Q is a valid conclusion of the premise A if and only if $P \rightarrow Q$ is a tautology and it is denoted as $P \Rightarrow Q$

~~We say from A~~

Definition:

We say from a set of premises or hypothesis $\{H_1, H_2, \ldots, H_m\}$ a

Scanned by CamScanner

conclusion 'c' follows logically.

$H_1 \wedge H_2 \wedge H_3 \wedge \ldots \wedge H_m \Rightarrow C$

that is $H_1 \wedge H_2 \wedge H_3 \wedge \ldots \wedge H_m \rightarrow C \equiv T$

Example:

Determine whether the conclusion 'c' logically follows from the premises H_1 and H_2 defined as

$H_1 : p \rightarrow q, \quad H_2 : p, \quad C : q$

$H_1 \wedge H_2 \Rightarrow C$

To prove: $H_1 \wedge H_2 \rightarrow C \equiv T$

~~$H_1 \wedge H_2 \rightarrow C$~~

Now $H_1 \wedge H_2 \rightarrow C$

$\equiv [(p \rightarrow q) \wedge p] \rightarrow q$

$\equiv [(\neg p \vee q) \wedge p] \rightarrow q$

$\equiv \neg[(\neg p \vee q) \wedge p] \vee q$

$\equiv \neg[\neg p \vee q) \vee \neg p \vee q$

$\equiv (p \wedge \neg q) \vee \neg p \vee q$

$\equiv [(p \vee \neg p) \wedge (\neg p \vee \neg q)] \vee q$

$\equiv [T \wedge (\neg p \vee \neg q)] \vee q$

$\equiv \neg p \vee \neg q \vee q$

$\equiv \neg p \vee T$

$\equiv T$

Rules of Inference

1. If a statement formula P is assumed to be true and also $P \rightarrow Q$ is accepted as true then Q must be true and symbolically this is expressed as :

$$\frac{p \rightarrow q \quad p}{\therefore \quad q}$$

This rule is known as Modus Ponens rule

Scanned by CamScanner

2. whenever $P \to Q$ and $Q \to R$ are accepted as true then the implication $P \to R$ is also true.

Symbolically this is written as

$$\begin{array}{l} P \to Q \\ Q \to R \\ \hline \therefore P \to R \end{array}$$

This argument or rule is known as hypothetical syllogism rule.

3. Addition rule

$$\begin{array}{l} P \\ \hline \therefore P \vee q \end{array}$$

4. Modus Tollens Rule

$$\begin{array}{l} P \to q \\ \neg q \\ \hline \therefore \neg P \end{array}$$

5. Disjunctive syllogism rule

$$\begin{array}{l} P \vee q \\ \neg q \\ \hline \therefore P \end{array}$$

6. conjunction Rule

$$\begin{array}{l} P \\ q \\ \hline \therefore P \wedge q \end{array}$$

7. simplification

$$\frac{P \wedge q}{\therefore P} \quad \text{or} \quad \frac{P \wedge q}{\therefore q}$$

Scanned by CamScanner

18.02.2019

8. Disjunctive dilemma

$$\frac{(p \to q) \wedge (r \to s) \quad \neg q \vee \neg s}{\therefore \quad \neg p \vee \neg r}$$

Show that t is a valid conclusion derived from premises

$p \to q$, $q \to r$, $r \to s$, $\neg s$ and $p \vee t$

1.	$p \to q$	Premise (Given)
2.	$q \to r$	Premise (Given)
3.	$r \to s$	Premise (Given)
4.	$\neg s$	Premise (Given)
5.	$p \vee t$	Premise (Given)
6.	$p \to r$	(1, 2 and HS)
7.	$p \to s$	(3, 6 and HS)
8.	$\neg p$	(4, 7 and MP)
9.	t	(5, 8 and DS)

Show that r is a conclusion obtained from premises

$p \to q$, $q \to r$, p

1.	$p \to q$	Premise (Given)
2.	$q \to r$	Premise (Given)
3.	p	Premise (Given)
4.	$p \to r$	(1, 2 and HS)
5.	r	(3, 4 and MT)

Prove the validity of following Arguments

"If I get job and work hard, I will get promotted"

"If I get promoted then I will be happy"

"I will not be happy."

Scanned by CamScanner

Therefore either I will not get a job or I will not work hard.

p: I will get a job

q: I work hard

r: I get promoted

s: I will be happy

H_1 : $p \wedge q \rightarrow r$

H_2 : $r \rightarrow s$

H_3 : $\neg s$

C : $\neg p \vee \neg q$

1. $p \wedge q \rightarrow r$
2. $r \rightarrow s$
3. $\neg s$
4. $(p \wedge q) \rightarrow s$ (1, 2 and HS)
5. $\neg (p \wedge q)$ (3, 4 and MT)
6. $\neg p \vee \neg q$ CDM)

Deduction Theorem / CP rule

If we can derive s from premise r and set of premises then we can derive $r \rightarrow s$ from set of premises.

Show that $r \rightarrow s$ is a valid conclusion drawn from premises $p \rightarrow (q \rightarrow s)$, $\neg r \vee p$, q

To show that $r \rightarrow s$ is a valid conclusion ~~the~~ obtained from

H_1 : $p \rightarrow (q \rightarrow s)$

H_2 : $\neg r \vee p$

H_3 : q

Scanned by CamScanner

We use CP rule that means we need to show S is a valid conclusion obtained from premises H_1, H_2 and H_3.

1. $p \rightarrow (q \rightarrow s)$	Premise (Given)
2. $\neg r \vee p$	Premise (Given)
3. q	Premise (Given)
4. r	Premise (Additional)
5. p	(2, 4 and DS)
6. $q \rightarrow s$	(1, 5 and MP)
7. s	(3, 6 and MP)
8. $r \rightarrow s$	(By CP)

Indirect method of proof

1. Proof by contradiction

To show C is a valid conclusion obtained from premises $H_1, H_2, \ldots, H_n$. we assume $\neg C$ and additional premise and then prove that $\neg C$ and $H, H_2, \ldots, H_n$ give a contradiction.

Show that $\neg(p \wedge q)$ follows from $\neg p \wedge \neg q$

1. $\neg p \wedge \neg q$	
2. $p \wedge q$	(Additional premise)
3. p	(Simplification)
4. $\neg p$	(Simplification)
5. $p \wedge \neg p$	(Conjunction and 4, 5)

Scanned by CamScanner