TRIBHUVAN UNIVERSITY

Institution of Science and Technology

Bachelor Level/ First Year/ Second Semester/Science Full Marks: 60 + 20 + 20
Discrete Structure (CSC 160) Pass Marks: 24 + 8 + 8
Time: 3 hours.

MODEL QUESTIONS-ANWERS

Candidates are required to give their answers in their own words as for as practicable.

The figures in the margin indicate full marks.

Section A (Long Answer Question Section)

Attempt any TWO questions. **[2x10=20]**

1. Why breaking down of large integer into set of small integers is preferred while performing integer arithmetic? Find sum of numbers 123,684 and 413,456 by representing the numbers as 4-tuple by using reminders modulo of pair-wise relatively prime numbers less than 100. [2+8]

Ans: Breaking down of large integer into set of small integers is preferred while performing integer arithmetic has several valuable features. First, it can be used to perform arithmetic with integers larger than can ordinarily be carried out on a computer. Second, computations with respect to the different moduli can be done in parallel, speeding up the arithmetic.

The numbers 95,97,98,99 are pairwise relatively prime.Then we can represent any integer less than$99 \cdot 98 \cdot 97 \cdot 95 = 89\ 403\ 930$asa quadruple of the remainders with respect to these numbers.To calculate the sum123684 + 413456we first represent the sum as quadruples(nmod 99,nmod 98,nmod 97,nmod 95)and then add them:

(33, 8, 9, 89) + (32, 92, 42, 16)= (65 mod 99, 100 mod 98, 51 mod 97, 105 mod 95) = (65, 2, 51, 10)

To convert the result back to a number, we solve the system of congruence's $x \equiv 65 \pmod{99}$, $x \equiv 2 \pmod{98}$, $x \equiv 51 \pmod{97}$, $x \equiv 10 \pmod{96}$ and find x= 537,140.

Using Chinese remainder theorem

$m = 99 \times 98 \times 97 \times 95 = 98403930$

We know that,

$M_{15} = m$

i.e, $M_1 = 903070$, $M_2 = 912285$

$M_3 = 921690$, $M_4 = 941094$

Finding y_k

i.e., $903070 \times y_1 = 1 \pmod{99}$ ... (i)

$912285 \times y_2 = 1 \pmod{98}$ ... (ii)

$921690 \times y_3 = 1 \pmod{97}$ ... (iii)

$941094 \times y_4 = 1 \pmod{95}$ ... (iv)

For equation (i)

Using extended Euclidean also

$903070 = 99 \times 91291 + 91$

$99 = 91 \times 1 + 8$

$91 = 3 \times 2 + 2$

$3 = 2 \times 1 + 1$

$2 = 1 \times 2 + 2$

i.e. $1 = 3 + 2 - (1)$

$= 3 + 8 (-1) + 3 (2)$

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

$= 91 (3) + 8 (-34)$

$= 99 (33 + 44_3) + 903070 (37)$

$\therefore \quad y_1 = 37$

Similarly,

we get,

$y_2 = 33$, $y_3 = 24$ and $y_4 = 4$

Finally,

$x = a, y, M_1 + a_2y_2M_2 + a_3y_3M_3 + a_4y_4M_4 \pmod{m}$

$= 3397886480 \bmod m$

$= 3397886480 \bmod (89403930)$

$= 537140$

2. **Define linear homogeneous recurrence relation. Solve the recurrence relation $a_n=a_{n/2}+n+1$, with $a_1=1$. Also discuss about probabilistic primality testing with example. [2+5+3=10 Marks]**

Ans: **Difinition 1:** A linear homogeneous recurrent relation of degree k with constant coefficient is a recurrent relation of the form

$a_n = c_1a_{n-1} + c_2a_{n-2} + \ldots + c_ka_{n-k}$ (*)

Where, $c_1, c_2 \ldots c_k \in \mathbb{R}$ and $c_k = 0$.

Linear refers to the facts that $a_n - 1, a_{n-2}, \ldots a_{n-k}$ appear in separate terms and to the first power.

Homogeneous refers to the fact that the total degree of each term is the same (thus there is no constant term) Constant Coefficients refers to the fact that $C_1, C_2, \ldots, c_k$ are fixed real number that do not depend on *n*.

Degree k refers to the fact that the expression for a_n contains the previous k terms $a_{n-1}, a_{n-2}, \ldots, a_{n-k}$.

A *probabilistic primality test* is a primality test that outputs "probable prime" or "composite" and has a certain probability of error if the output is "probable prime."

Probabilistic primality tests typically pick a random number called a *witness* and verify some criteria involving the witness and the candidate being tested. Most probabilistic primality tests

used in practice will not err when declaring an integer to be composite, but have a probability of error when declaring an integer to be prime: They either declare a candidate to be *definitely composite* or *probably prime*. A candidate that passes such a test – whether prime or composite – is called a *probable prime* for that test. A composite number that erroneously passes such a test is called a pseudoprime.

3. **How Zero-one matrix and diagraphs can be used to represent a relation? Explain the process of identifying whether the graph is reflexive, symmetric, or anti-symmetric by using matrix or diagraph with suitable example.** **[4+6]**

Ans: **Difinition 1:** A matrix all of whose entries are either 0 or 1 is called a zero-one matrix. Algorithms operating on discrete structure represented by zero-one matrices arebased on Boolen arithmetic defined by the following Boolean operations:

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

A relation can be represented with a zero-one matrix.

Let R be a relation from $A = \{a_1, \ldots, a_m\}$ to $B = \{b_1, \ldots, b_n\}$.

The relation R can be represented by the matrixc $M_R = [m_{ij}]$

Where:

$$m_{ij} = \begin{cases} 1 & \text{if } (a_i, b_j) \in R \\ 0 & \text{if } (a_i, b_j) \notin R \end{cases}$$

This is, the matrix has a 1 at its (i, j) entry when a_i is related to b_j and a 0 when they are not related.

Definition: If A is finite and $R \subseteq A \times A$ is relation. We represent R pictorially as follows:

- Draw a small circle, called a vertex/node, for each element of A and label the circle with the corresponding element of A.
- Draw an arrow, called an edge, from vertex a_i to vertex a_j iff a_i R a_j.

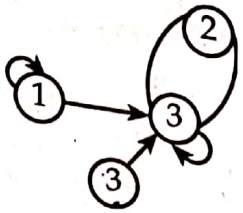
The resulting pictorial representation of R is called a directed graph or digraph of R.

Example: Let A = {1, 2, 3, 4} and

R = {(1, 1)}, (1, 2), (2, 1), (2, 2), (2, 3), (2, 4), (3, 4), (4, 1)}

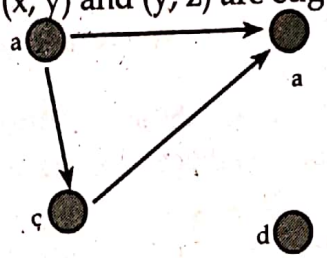
The digraph of R :

Example: Let A = {1, 2, 3, 4} and .



Determining which properties a Relation has from its Diagraph

- Reflectivity: A loop must by present at all vertices the garph.
- Symmetry: If (x, y), is an edge, then so is (y, x).
- Ant symmetry: If (x, y) with $x \neq y$ is an edge, then (x, y) is not an edge.
- Transitivity: If (x, y) and (y, z) are edge,, then so is (x, z).



Reflective? No, there are no loops
Symmetric? No, for example, there is no edge from c to a
Anti-symmetric? Yes, whenever there is an edge from one Vertex to another, there is not one going back
Transitive? Yes, there is an edge (a, b) given (a, c) and (c, b).

Section B (Short Answer Questions)

Attempt any EIGHT questions. **[8 × 5=40]**

4. **Prove that $\overline{A \cap B} = A \cup B$ by using set builder notation. How sets are represented by usingbit string? Why it is preferred over unordered representation of sets?** **[3+2]**

Ans: $\overline{A \cup B}$

$= \{x \mid x \notin A \cup B\}$ by definition of complement

$= \{x \mid \neg (x \in (A \cup B))\}$ by definition of does not belong symbol

$= \{x \mid \neg (x \in x \in B)\}$ by definition of union

$= \{x \mid \neg (x \in A) \neg (x \in B)\}$ by definition of union.

$= \{x \mid x \notin A \wedge x \notin B)\}$ by definition of does not belong symbol

$= \{x \mid x \in \bar{A}\ \bar{x} \in \bar{B})\}$ by definition of complement

$= \{x \mid x \in \bar{A} \cap \bar{B})\}$ by definition of intersection

$= \bar{A} \cap \bar{B}$ by set builder notation

A bit string is a sequence of zero or more bits. The length of this string is the number of bits in the string.

Assume that the universal set U is finite (and of reasonable size so that the number of elements of U is not larger than the memory size of the computer being used).

First, specify an arbitrary ordering of the elements of U, for instance $a_1, a_2, \ldots, a_n$. Represent a subset A of U with the bit string of length n, where the i^{th} bit in this string is 1 if a_i belongs to A and is 0 if a_i does not belong to A. The following example illustrates this technique.

Example

Let U = {1, 2, 3, 4, 5, 6, 7, 8, 9, 10}, and the ordering of elements of U has the elements in increasing order; that is, $a_i = i$. What bit strings

represent the subset of all odd integers in U, the subset of all even integers in U, and the subset of integers not exceeding 5 in U?

- The set of all odd integers in U is {1, 3, 5, 7, 9},
  The bit string is 1010101010
- The set of all even integers in U is {2, 4, 6, 8, 10}
  The bit string is 0101010101
- The set of integers not exceeding 5 in U is {1, 2, 3, 4, 5}, The bit string is 1111100000

A data structure for an unordered set would require at least ceil(log2(N)) bits per element to store, where N is the number of possible elements. Testing an unordered set data structure for inclusion of a particular element requires a linear search (i.e., O(N) time) while testing a bit string requires O(1) time. Set operations such as union, intersection, and difference can easily be performed on bit strings using bitwise operators. For example, given two sets, A and B, union (A, B) : A | B intersection(A, B) : A & B difference(A, B) : A & (~B)

One further advantage of bit strings is that there is a unique (canonical) representation for any given set, so set equality can be defined thus: equal(A, B) : A == B

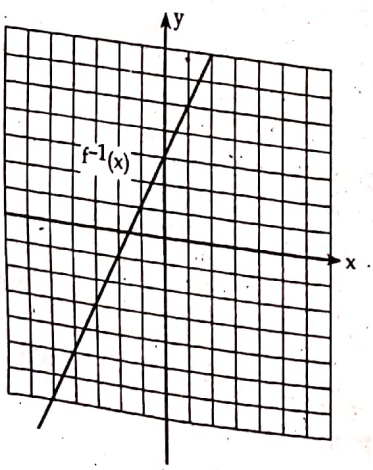
But an unordered set data structure would require extra steps to determine equality.

Also, an unordered set data structure could contain duplicate elements, so the "remove" operation would have to account for that, unless the "insert" operation prevented duplicates.

5. **How can you related domain and co-domain of functions with functions in programming language? Discuss composite inverse of function with suitable example.**

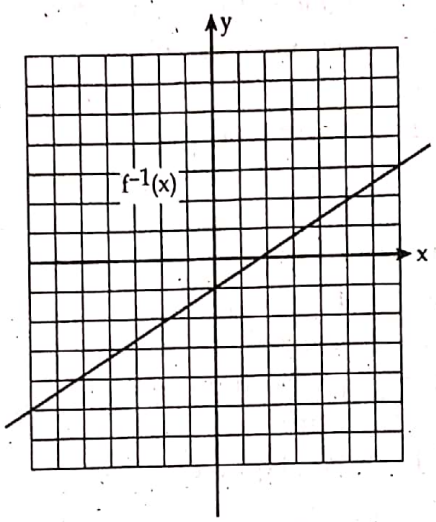
Ans: **Definition of Inverse Function** **[2 +3]**

An inverse function, which is notated $f^{-1}(x)$, is defined as the inverse function f(x) if it consistently reverse the f(x) process. That is, if f(x) turns a into b, then $f^{-1}(x)$ must turn b into a. More concisely and formally, $f^{-1}(x)$ is the inverse function of f(x) if: $f(f^{-1}(x)) = x$



Let, $f(x) = 3 + 2x$ be a linear function.Each x-value is mapped onto a unique y-value that is given by $y = 3 + 2x$.
Since the function is linear, you can also find a unique x-value for each y-value. You can describe x b a function of y by letting $x = \frac{y-3}{2}$. This "reverse" function is called the inverse function of f and it is denoted f^{-1}.
By convention y is used to denoted the function value and x is used for the variable. After finding the inverse function (by expressing x in terms of y) you swap the y and the which yield $y = \frac{x-3}{2}$.

We now have that $f^{-1}(x) = \frac{x-3}{2}$.



Example: If $f(x) = 2x$ and $g(x) = x^2 - 1$, evaluate f(g(3)) and g(f(3)).
To evaluate f(g(3)), first substitute, or input the value of 3 into g(x) and find the output. Then substitute that value into the f(x) function, and simplify:
$9(3) = (3)^2 - 1 = 9 - 1 = 8$
$f(8) = -2(8) = -16$
Therefore, $f(g(3)) = -16$
To evaluate (g(f(3)), find f(3) and then use that output value as the input value into the g(x) function.
$f(3) = -2(3) = -6$
$g(-6) = (-6)^2 - 1 = 36 - 1 = 35$
Therefore, $g(f(3)) = 35$

6. **State Euclidean and extended Euclidean theorem. Write down extended Euclidean algorithm and illustrate it with example.** **[1+4]**

Ans: The Euclidean algorithm is an efficient method to compute the greatest common divisor (gcd) of two integers. We write gcd (a, b) = d to mean that d is the largest number that will divide both a and b. If gcd (a, b) = 1 then we say that a and b are coprime

or relatively prime. The gcd is sometimes called the highest common factor (hcf).

Algorithm: (Euclidean algorithm) Computing the greatest common divisor of two integers.

INPUT: Two non-negative integers a and b with $a \geq b$.

OUTPUT: gcd(a, b).

1. While b > 0, do
   a. Set r = a mod b,
   b. a = b,
   c. b = r
2. Return *a*.

The proof uses the *division algorithm* which states that for any two integers *a* and *b* with b > 0 there is a unique pair of integers *q* and *r* such that a = qb + r and 0 <= r < b. Essentially, *a* gets smaller with each step, and so, being a positive integer, it must eventually converge to a solution (i.e. it cannot get smaller than 1).

If you have negative values for *a* or *b*, just use the absolute values |a| and |b| in the above algorithm. By convention, if b = 0 then the gcd is *a*.

Example: Find gcd (421, 111).

We use the Euclidean algorithm as follows:

421 = 111 x 3 + 88 (larger number on left)
111 = 88 x 1 + 23 (shift left)
88 = 23 x 3 + 19 (note how 19 moves down the "diagonal")
23 = 19 x 1 + 4
19 = 4 x 4 + 3
4 = 3 x 1 + 1 (last non-zero remainder is 1)
3 = 1 x 3 + 0

The last non-zero remainder is 1 and therefore gcd(421, 111) = 1.

Extended Euclidean Algorithm:

Extended Euclidean algorithm also finds integer coefficients x and y such that: ax + by = gcd(a, b)

Input: Integer a and b

Output: Integers x, y, and d, where d = gcd (a, b) = ax + by

Set $d_0 = a$ set $x_0 = 1$ set $y_0 = 0$
Set $d_1 = b$ set $x_1 = 0$ set $y_1 = 1$

While $d_1 \neq 0$ Do
Set $q = [d_0/d_1]$
Set $d_2 = d_1$ Set $x_2 = x_1$ Set $y_2 = y_1$
Set $d_1 = d_0 - qd_1$
Set $x_1 = x_0 - qx_1$
Set $y_1 = y_0 - qy_1$
Set $d_0 = d_2 - qy_1$

Set $x_0 = x_2$
Set $y_0 = y_2$
End while
$[d, x, y] = [d_0, x_0, y_0]$
Find two integers x and y such that 1914x + 899y =gcd(1914,899).
First use Euclid's algorithm to find the GCD:

$$\begin{aligned} 1914 &= 2 \times 899 + 116 \\ &= 7 \times 116 + 87 \\ &= 1 \times 87 + 29 \\ &= 3 \times 29 + 0 \end{aligned}$$

From this, the last non-zero remainder (GCD) is 2929. Now we use the extended algorithm:

$29 = 116 + (-1) \times 87$
$87 = 899 + (-7) \times 116.$
Substituting for 87 in the first equation, we have

$$\begin{aligned} 29 &= 16+(-1)\times(899+(-7)\times116) \\ &= (-1)\times899+8\times116 \\ &= (-1)\times899+8\times(1914+(-2)\times899) \\ &= 8\times1914+(-17)\times899 \\ &= 8\times1914-17\times899. \end{aligned}$$

Since we now wrote the GCD as a linear combination of two integers, we terminate the algorithm and conclude
$x = 8, y = -17$

7. **State and prove generalized pigeonhole principle? How many cards should be selected froma deck of 52 cards to guarantee at least three cards of same suit?** **[2.5+ 2.5]**

Ans: The word "pigeonhole" literally refers to the shelves in the form of square boxes or holes that were utilized to place pigeon's earliar in the United States. In mathematics, there is a concept, inspired by such pigeonholes, known as pigeonhole principle which was introduced in 1834 by a German mathematician Peter Gustav Lejeune Dirichlet. On his name, this principle is also termed as Dirichlet principle.

Pigeonhole Principle: If k is a positive integer and k + 1 objects are placed into k boxes, then at least one box contains two or more objects.

Proof: We use a proof by contraposition. Suppose none of the k boxes has more than one object. Then the total number of objects would be at most k.

This contradicts the statement that we have k + 1 objects.

THE GENERALIZED PIGEONHOLE PRINCIPLE. If N objects are placed into k boxes, then there is at least one box containing celi(N/k) objects.

How many cards must be selected from a standard deck of 52 cards to guarantee that at least three cards of the same suit are chosen?

Solution: Suppose there are four boxes, one for each suit, and as cards are selected they are placed in the box reserved for cards of that suit. Using the generalized pigeonhole principle, we see that if N cards are selected, there is at least one box containing celi(N/4) cards. Consequently, we know that at least three cards of one suit are selected if celi(N/4)>=3. The smallest integer N such that celi(N/4)>=3 is 2 4+1=9, so nine cards suffice.

Note that if eight cards are selected, it is possible to have two cards of each suit, so more than eight cards are needed. Consequently, nine cards must be selected to guarantee that at least three cards of one suit are chosen. One good way to think about this is to note that after the eighth card is chosen, there is no way to avoid having a third card of some suit

8. **Represent the argument "If it does not rain or if is not foggy then the sailing race will be held and the lifesaving demonstration will go on. If sailing race is held then trophy will be awarded. The trophy was not awarded. Therefore it rained" in propositional logic and prove the conclusion by using rules of inferences.** [2+3]

Ans: Define the following:

- R = "It rains"
- F = "It is foggy"
- S = "The sailing race will be held"
- D = "Life-saving demonstrations will go on"
- T = "The trophy will be awarded"

We can now proceed to prove the claim:

(1) $\neg T$	hypothesis
(2) $S \rightarrow T$	hypothesis
(3) $\neg S$	modus tollens from (1), (2)
(4) $\neg S \vee \neg D$	addition
(5) $\neg(S \wedge D)$	DeMorgan
(6) $(\neg R \vee \neg F) \rightarrow (S \wedge D)$	hypothesis
(7) $\neg(\neg R \vee \neg F)$	modulstollens from (5),(6)
(8) $R \wedge F$	DeMorgan
(9) R	simplification

Thus, it rained

9. **Discuss common mistakes in proof briefly. Show that n is even if n^3+5 is odd by using indirect proof.** [2+3]

Ans: **Theorem:** If n3 + 5 is even then n is odd for all natural numbers.

Proof by contradiction: Assume that there exist at least one value of n so that n3 + 5 is even and n is even.

If n is even then there exist an integer k so that so that n = 2k by definition of even. So we now have that

$n^3 + 5 = (2k)^3 + 5$

$= 8k^3 + 4 + 1$

$= 2(4k^3 + 2) + 1 = 2f + 1$ where $f = 4k^3 + 2$ is an integer.

So by definition of odd, $n^3 + 5 = 2f + 1$ is odd. This is a contradiction to the sufficient condition that $n^3 + 5$ is even. Therefore n must be odd.

10. How mathematical induction differ from strong induction? Prove that $1^2 + 2^2 + 3^2 + \ldots n^2 \frac{(n+1)(2n+1)}{6}$ by strong induction. [1 + 4]

Ans: With simple induction you use "if p(k) is true then p(k + 1) is true" while in strong induction you use "if p(i) is true for all i less than or equal to k then p(k + 1) is true", where p(k) is some statement depending on the positive integer k. They are NOT "identical" but they are equivalent. It is easy to see that if simple induction is true then strong induction is true: if you know that statement p(i) is true for all i less than or equal to k, then you know that it is true, in particular, for i = k and can use simple induction. It is harder to prove, but still true, that if strong induction is true, then simple induction is true. That is what we mean by "equivalent."

The strong induction principle says that you can prove a statement of the form:

P (n) for each positive integer n.

as follows:

Base can: P(1) is true.

Strong inductive step: Suppose k is a positive integer such that P(1), P(2), . . . P(k) are all true. Prove that P(k + 1) is true.

So the key step is to show:

$$P(1), P(2), \ldots, P(k) \Rightarrow P(k+1).$$

So to speak, the statement is true if you can prove that:

1. The first domino has fallen.
2. If k is such that the first k domains have fallen, then the $(k+1)^{th}$ domino has fallen.

Let $p(n) = 1^2 + 2^2 + 3^2 + \ldots + n^2 = \frac{(n+1)(2n+1)}{6}$

Base case

$$P(1) = \frac{1(1+1)(2\times1+1)}{6} = \frac{2\times3}{6} = \frac{6}{6} = 1$$

$$F(2) = \frac{2(2+1)(2\times2+1)}{6} = \frac{2\times3\times5}{6} = 5$$

$(\because 1^2 + 2^2 = 1 + 4 = 5)$

$(\therefore$ true$)$

$$F(3) = \frac{3(3+1)(2\times3+1)}{6} = \frac{3\times4\times7}{6} = 14$$

$(\therefore 1^2 + 2^2 + 3^2 = 1 + 4 + 9 = 14)$

$(\therefore$ true$)$

$$F(4) = \frac{4(4+1)(2\times4+1)}{6} = \frac{4\times5\times9}{6} = 30$$

$\therefore 1^2+2^2+3^2+4^2 = 1+4+16 = 30$

$\therefore$ true

Likewise,

$P(n) = (\therefore 1^2+2^2+3^2+\ldots, n^2 = \frac{(n+1)(2n+1)}{6}$ *Prove.*

11. Write down recursive algorithm for computing a^n. Argue that your algorithm is correct by using induction. [2.5+2.5]

Ans: An algorithm is called recursive algorithm if it solves a problem by reducing it to an instances of same problem with smaller input.

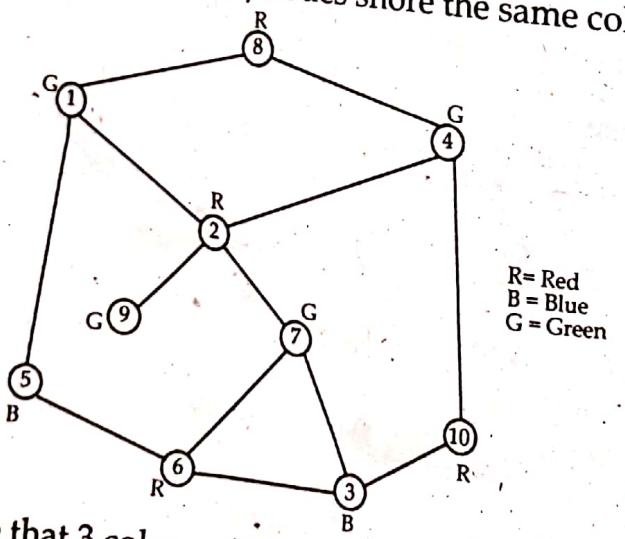
```
1.  procedure power N(int base, int n)
2.  if (n <0) then
3.  return ("Illegal Power Argument")
4.  if (n == 0) then
5.  return1
6.  else
7.  return base * power N(base, n - 1)
8.  end power N
```

12. What is meant by chromatic number? How can you use graph coloring to schedule exams? Justify by using 10 subjects assuming that the pairs {(1,2), (1,5), (1,8), (2,4), (2,9), (2,7),(3,6), (3,7), (3,10), (4,8), (4,3), (4,10), (5,6), (5,7)} of subjects have common students. [1+4]

Ans: The chromatic number of a graph G is the smallest number of colors needed to color the vertices of G so that no two adjacent vertices share the same color.

Assuming 10 subject as a nodes, from the given point of subjects having common standards, we have the following graph.

According to chromatic theory definition we color each node such that no two adjacent vertices/nodes shore the same color as:



As we can see that 3 colours (R.G.B) is enough to colour the graph.

$\therefore$ Chromatic number = 3

TRIBHUVAN UNIVERSITY

Institution of Science and Technology

Bachelor Level/ First Year/ Second Semester/ Science Full Marks: 60
Microprocessor (CSC 162) Pass Marks: 24
Time: 3 hours.

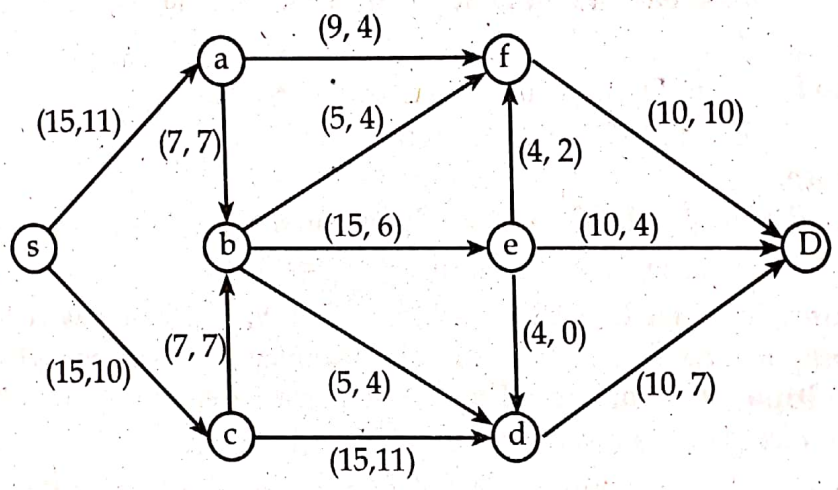
TU QUESTIONS-ANSWERS 2075

Candidates are required to give their answers in their own words as for as practicable.
The figures in the margin indicate full marks.

Section A (Long Answer Question Section)

Attempt any TWO questions. **(2x10=20)**

1. **What is S-D cut? For the following network flow find the maximal flow from S to D.** **[2 + 8]**



Ans: In a flow network, an **s-t cut** is a **cut** that requires the source 's' and the sink 't' to be in different subsets, and it consists of edges going from the source's side to the sink's side. The capacity of an **s-t cut** is defined by the sum of the capacity of each edge in the **cut**-set.

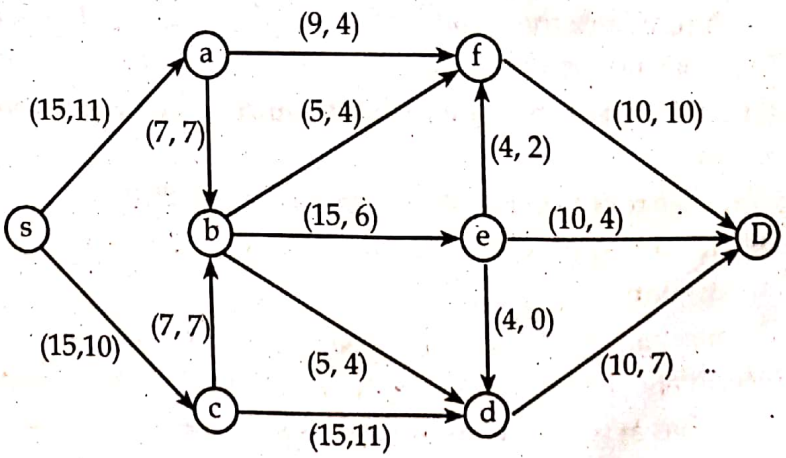


Fig: residual graph

Taking augmented path:

Ⓢ → ⓐ → ⓕ → ⓔ → Ⓓ

We can increase the flow by 2

Saturating the edge ⓕ → ⓔ

Taking augmented path

Ⓢ → ⓐ → ⓕ → ⓑ → ⓔ → Ⓓ

We can increase the flow by 2 again saturating the edge Ⓢ → ⓐ

Taking augmented path

Ⓢ → ⓒ → ⓓ → Ⓓ

We can increase the flow by 3 saturating the edge ⓐ Ⓓ

Again,

Taking augmented path

Ⓢ → ⓒ → ⓓ → ⓑ → ⓔ → Ⓓ

We can increase the flow by 1 saturating the edge ⓒ → ⓓ

Here,

No from s to D can be increased any more.

∴ The maximum flow will be 29.

Since,

Total outpoint flow (15 + 14 = 29) is equal to

Total incoming flow at D (10 + 9 + 10) = 29

2. **Consider a set U = {1, 2, 3, 4, 5, 6, 7, 8, 9, 10}. What will be t he computer representation for set containing the number which are multiple of 3 not exceeding 6? Describe injective, surjective and bijective function with example.** **[2 + 8]**

Ans: Assume that the universal set U is finite (and of reasonable size so that the number of elements of U is not larger than the memory size of the computer being used).

First, specify an arbitrary ordering of the elements of U, for instance $a_1, a_2, \ldots, a_n$. Represent a subset A of U with the bit string of length n, where the i^{th} bit in this string is 1 if a_i belongs to A and is 0 if a_i does not belong to A.

Let set A represent the no which are multiple of 3 not exceeding 6.

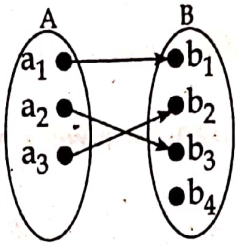
i.e. A = {3, 6}

So computer representation bit string for A is 0010010000.

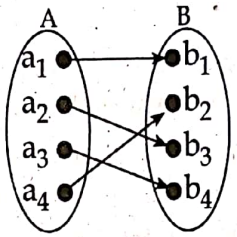
- **Definition:** A function f is said to be one-to-one or injective (or an injection) if

  ∀ x and y in the domain of f, f(x) = f(y) ⇒ x = y
- Intuitively, an injection simply means that each element in the range has at most one preimage (antecedent).
- It is useful to think of the contra positive of this definition.

- $x \neq y \Rightarrow f(x) \neq f(y)$



- Is this function
  - It this a function
    - One-to-one (injective)? Why Yes, no, b_i has 2 preimages
    - Onto (surjective)? Why? No, b_4 has no preimage
- **Definition:** A function $f : A \rightarrow B$ is called onto or surjective (or an surjection) if
  $\forall b \in \exists a \in A$ with $f(a) = b$
- Intuitively, a surjection means that every elements in the codomain is mapped into (i.e., it is an image, has an antecedent)
- Thus, the range is the sameas the codemain



- Is this a function
  - One-to-one (injective)? Thus, it is a bijection or a
  - Onto (surjective)? one-to-one correspondence

3. Compute the following values.

a. 3 mod 4 **b. 7 mod 5** **c. – 5 mod 3**

d. 11 mod 5 **e. – 8 mod 6**

Write down recursive algorithm to find the value of b" and prove its correctness using induction. **[5 + 5]**

Ans: 3 mod 4= 3

7 mod 5= 2

-5 mod 3=1

11 mod 5=1

-8mod 6=4

Recursive algorithm to find b^n

An algorithm is called recursive algorithm if it solves a problem by reducing it to an instances of same problem with smaller input.

```
1. procedure powerN(int base, int n)
2. if (n <0) then
3. return ("Illegal Power Argument")
4. if (n == 0) then
```

5. return1
6. else
7. return base * powerN(base, n - 1)
8. end powerN

Section B (Short Answer Questions)

Attempt any EIGHT questions: [8 × 5 = 40]

4. Solve the recurrence relation $a_n = 5a_{n-1} - 6a_{n-2}$ with initial conditions $a_0 = 1$ and $a_1 = 2$. [5]

Ans: Let c_1 and c_2 be real number. Suppose that $r^2 - c_1r - c_2 = 0$ has two distinct roots r_1 and r_2. Then the sequence $\{a_n\}$ is a solution of the recurrence relation $a_n = c_1a_{n-1} + c_2a_{n-2}$ if and only if $a_n = \alpha 1r_1^n + \alpha 2r_2^n$ for $n = 0, 1, 2 \ldots$ Where α_1 and α_2 are constants.

The characteristic equation of the recurrence relation is

$r^2 - 5r + 6 = 0$

Solving we get the root $r_1 = 1$ and $r_2 = 6$

Hence, the sequence $\{a_n\}$ is a Solution to the recurrence relation if any only if

$a_n = \alpha_1 r_1^n + \alpha_2 r_2^n$

For some constant α_1 and α_2

From initial condition, it flows that

$a_0 = 1 = \alpha_1 + \alpha_2$ ... (i)

$a_1 = 2 = \alpha_1 .1 + \alpha_2 . 6$ ... (i) ($\because c_1 = \alpha_1 r_1 + \alpha_2 + \alpha_2 r_2$)

Solving equation (i) and (ii), we get

$$\alpha_1 = \frac{1}{5} \text{ and } \alpha_2 = \frac{4}{5}$$

Therefore, the solution to the recurrence relation and initial condition is the sequence $\{a_n\}$ with.

$$a_n = \alpha_1 r_1^n + \alpha_2 r_2^n$$

$$\therefore \quad a_n = \frac{1}{5}(1)^n + \frac{4}{5}(6)^n.$$

5. Find the value of x such that $x \equiv 1 \pmod 5$ and $x \equiv 2 \pmod 7$ using Chinese remainder theorem. [5]

Ans: Theorem: (Chinese Remainder Theorem). Let $m_1, m_2 \ldots m_r$ be a collection of pair wise relatively prime integers. Then the system of simultaneous congruences.

$x \equiv a_1 \pmod{m_1}$

$x \equiv a_2 \pmod{m_2}$

$\vdots$

$x \equiv a_r \pmod{m_r}$

has a unique solution modulo $M = m_1m_2, \ldots m_r$, for any given integers $a_1, a_2, \ldots a_r$.

Proof of CRT. Put $M = m_1 \ldots m_r$ and for each $k = 1, 2, r$, r let $M_k = \frac{M}{m_k}$. then gcd $(M_k, m_k) = 1$ for all k. Let y_k be an inverse of M_k modulo m_k, for each k. Then by definition of inverse we have $M_k y_k \equiv 1 \pmod{m_k}$. Let

$$x = a_1M_1 + a_2M_2y_2 + \ldots + a_rM_ry_r$$

Then x is a simultaneous solution to all of the congruences. Since the moduli $m_1, \ldots, m_r$ are pairwise relatively prime, any two simultaneous solutions to the system must be congruent modulo. Thus the solution is a unique congruence class modulo M, and the value of x computed above is in that class.

$x = 1 \pmod 5$
$x = 2 \pmod 7$

Here,

$a_1 = 1$ $\quad m_1 = 5$
$a_2 = 2$ $\quad m_2 = 7$

$M = m_1 \times m_2$
$= 5 \times 7$
$= 35$

$M_1 = M/m_1$
$= \frac{35}{5}$
$= 7$

$M_2 = M/m_1$
$= \frac{35}{7}$
$= 5$

Finding y_k

$7 \times y_1 = 1 \pmod 5$
$5 \times y_2 = 1 \pmod 7$

Now,

$7 = 5 \times 1 + 2$
$5 = 2 \times 2 + 1$
$2 = 1 \times 2 + 0$

or, Using extended Euclidean also

$1 = 5 + 2 (- 2)$
$1 = 5 (3) + 4 (- 2)$ $\quad (\therefore$ after subtraction)

or, $y_1 = - 2 \bmod 5 = 3$
$y_2 = 3$

Finally,

$x = a, m_1, y_1 + a_2M_2y_2$
$= 1. 7. 3 + 2. 5. 3$
$= 21 + 30 \pmod M$
$= 51 \pmod{35}$
$= 16$

6. Prove that $5^n - 1$ is divisible by 4 using mathematical induction.[5]

Ans: Let $P(n) = 5^n - 1$

1. Basic step:

For n = 1, we have

P (1) = 5 – 1 = 4 divisible by 4.

2. **Indicutive Hypothesis**
Assume P (K) is true for n = k
i.e. $P(k) = 5^k - 1$ is true.

3. **Inductive step:**
$P(k+1) = 5^{k+1} - 1$
$= 5^k \times 5 - 1$
$= 5 \times 5^{k-1}$
$= (4 \times 5^k + 5^k) - 1$
$= (4 \times 5^k) + (5^k - 1)$

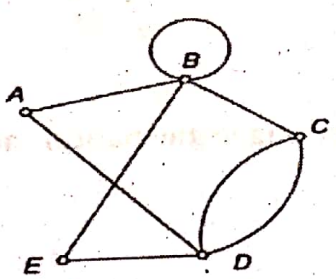
Here,
4×5^k is divisible by 4
Also,
$5^k - 1$ is also divisible by 4
From Inductive hypothesis.
Therefore, P (k + 1) is true.
Hence proved.

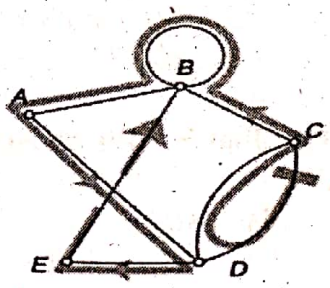
7. Let A="Aldo is Italian" and B="Bob is English". Formalize the following sentences into proposition.
Aldo isn't Italian
Aldo is Italian while Bob is English
If Aldo is Italian then Bob is not English
Aldo is Italian or if Aldo isn't Italian then Bob is English
Either Also is Italian and Bob is English, or neither Aldo is Italian nor Bob is English.

Ans: (a) $\neg A$
(b) $A \vee B$
(c) $A \rightarrow \neg B$
(d) $A \vee (\neg A \rightarrow B)$
(e) $(A \wedge B) \vee \neg (A \vee B)$

8. **Define Euler path and Hamilton path with example. Draw the Hasse diagram for the divisibility relation on the set {1, 2, 5, 8, 16, 32} and find the maximal, minimal, greatest and least element if exist.** **[2+3=5]**

Ans: An Euler path in G is a simple path containing every edge of G. It starts and ends at different vertices.





Another Euler Path: CBCBBADEB

The criterion for Euler Paths

The inescapable conclusion ("based on reason alone!")

If a graph G has an Euler path, then it must have exactly two odd vertices.

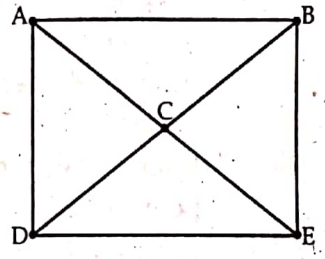
Or to put it another way.

If the number of odd vertices in G is anything other than 2, then G cannot have an Euler path.

Hamilonian Path – A simple path in a graph that passes through every vertex exactly once is called a hamiltonian path. Unlike Euler paths and circuits, there is no simple necessary and sufficient criteria to determine if there are any Hamiltonian paths or circuits in a graph

Example: Hamilton Path.

- Graph (a) shown has Hamilton path A, B, C, D, E, D. The graph also has Hamilton path C, B, A, D, E. Can you find some others?



In order theory, a Hasse diagram is a type of mathematical diagram used to represent a finite partially ordered set, in the form of a drawing of its transitive reduction.

A Hass diagram is a graphical representation of the relation of elements of partially ordered set (poset) with an implied upward orientation. A point is drawn for each element of the partially ordered set (poset) and joined with the line segment according to the following rules:

- If $p < q$ in the poset, then the point corresponding to p appears lower in the drawing than the point corresponding to q.
- The two points p and q will be joined by line segment iff p is related to q.

To draw a Hasses diagram, provided set must be a poset

A poset or partially ordered set A is a pair, $(B, \leq)$ of a set B whose elements are called the vertices of A and obeys following rules.

1. Reflexivity $\rightarrow p \leq p \; \forall \; p \in B$
2. Anti-symmetric $\rightarrow p \leq q$ and $q \leq p$ iff $p = q$
3. Transitivity $\rightarrow$ if $p \leq q$ and $q \leq r$ then $p \leq r$

For Regular Hasses Diagram.

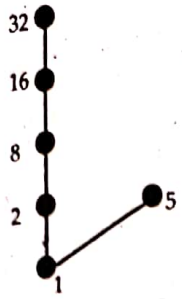
- Maximal elements are those which are not succeeded by another element.
- Minimal elements are those which are not preceded by another element.

- Greatest element (if it exists) is the element succeeding all other elements.
- Least element is the element that precedes all other elements.

let the set is A

i.e. A = {(1 ≤ 2), (1 ≤ 5), (1 ≤ 8), (1 ≤ 16), (1 ≤ 32), (1 ≤ 8), (1 ≤ 16), (1 ≤ 32), (1 ≤ 16), (8 ≤ 32), (16 ≤ 32)}

So, Hasse diagram will be.



Maximal element = 32
Minimal element = 1
Greatest element = 32
Least element = 1

9. **What does primality testing means? Describe how little fermat's theorem test for prime numbers with suitable example..**

Ans: A primality test is a test to determine whether or not a given number is prime, as opposed to actually decomposing the number into its constituent prime factors (which is known as prime factorization).

Primality tests come in two varieties: deterministic and probabilistic. Deterministic tests determine with absolute certainty whether a number is prime. Examples of deterministic tests include the Lucas-Lehmer test and elliptic curve primality proving. Probabilistic tests can potentially (although with very small probability) falsely identify a composite number as prime (although not vice versa). However, they are in general *much* faster than deterministic tests. Numbers that have passed a probabilistic prime test are therefore properly referred to as probable primes until their primality can be demonstrated deterministically.

Fermat's Little Theorem: If p is prime and a is an integer not divisible by p, then

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

Furthermore, for every integer a we have

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

Remark: Fermat's little theorem tells us that if $a \in z_p$, then $a^{p-1} = 1$ in Z_p

Example: Find 7^{222} and 11.

Solution: We can fermat's little theorem to evaluate 7^{222} mod 11 rather than using the fast modular exponentiaion algorithm. By Fermat's little theorem we know that $7^{10} \equiv$ (mod 11), so $(7^{10})^k \equiv 1$

(mod 11) for every positive integer k. To take advantage of this last congruence, we divide the exponent 222 by 10, findings that 222 = 22. 10 + 2. We know see that

$7^{222} + 7^{22.10+2} = (7^{10})\, 7^2 \equiv (1)^{22} . 49 \equiv 5 \pmod{11}$

If follow that $7^{222} \bmod 11 = 5$

Example 9 Illustrated how we can use Fermat's little theorem compute $a^n \bmod p$, which p is prime and p × a : First, we use the division algorithm to find the quotient q and remainder r when n is divided by p – 1, so that n = q (p – 1) + r where $0 \le r < p - 1$. It follows that $a^n = a^{q}(p-1) + r = (a^{p-1})^q a^r \equiv 1 q a^r \equiv a^r \pmod{p}$. Hence, to find $a^n \bmod p$, we only need to compute $a^r \bmod p$. We will take advantage of the simplification many times in our study of number theory.

10. **List any two applications of conditional probability. You have 9 families you would like to invite to a wedding. Unfortunately, you can only invite 6 families. How many different sets of invitations could you write?**

Ans: Two application of conditional probability

- Drawing a 2nd Ace from a deck of cards given we got the initial Ace.
- Finding the probability of liking Harry Potter given we know the individual prefers fiction.

Since order doesn't matter while selecting families, we use combination for the solution.

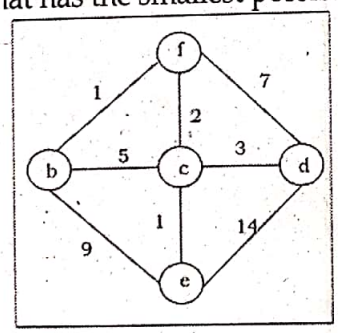
9C6 = 84

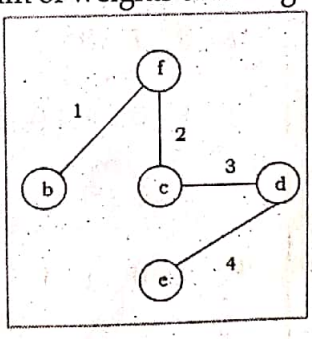
11. **Design spanning tree and minimum spanning tree. Mention the condition of two graph for being isomorphic with example .**

Ans: Let G be a simple graph. A spanning tree of G is a sub-graph of G that is a tree containing every vertex of G.

A simple graph with a spanning tree must be connected, because there is a path in the spanning tree between any two vertices. The converse is also true; that is, every connected simple graph has a spanning tree .

A minimum spanning tree in a connected weighted graph is a spanning tree that has the smallest possible sum of weights of its edges.





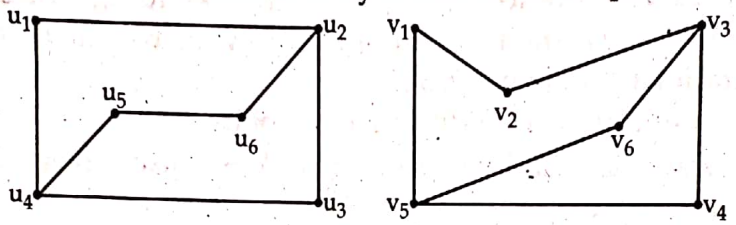
Two algorithms

1. prism's algorithm and
2. Kruskal algorithm are used to find the minimum spanning tree.

The simple graphs $G1 = (V1, E1)$ and $G2 = (V2, E2)$ are *isomorphic* if there exists a oneto- one and onto function f from $V1$ to $V2$ with the property that a and b are adjacent in $G1$ if and only if $f(a)$ and $f(b)$ are adjacent inG2, for all a and b in $V1$. Such a function f is called an *isomorphism*. *Two simple graphs that are not isomorphic are called *nonisomorphic*.

Example: Determine whether the gaphs G and H displayed in figure are isomorphic.

Solution: Both G and H have six vertices and seven edges. Both have four vertices of degree two and two vertices of degree three. It is also easy to see the sub-graphs of G and H consisting of all vertices of degree two and the edges connecting them are isomorphic (as the reader should verify). Because G and H agree with respect to these invariants, it is reasonable to try to find an isomorphism f.



Graph G and H

We now will define a function f and then determine whether it is an isomorphism. Because deg $(u_1)_2$ and because u_1 is not adjacent to any other vertex of degree two, the image of u_1 must be either v_4. or v_6,. [If we found that this choice did not lead to isomorphism, we would then try $f(u_1) = u_4$] Because u_2 is adjacent to u_1, the possible images of u_2 are v_3 digress as a guide, we set $f(u_3) = u_4$. $f(u_5) = v_5$, $f(u_4) = v_1$ and $f(u_6) = v_2$. We now have a one-to-one correspondence between the vertex set of G and the vertex set of H. Namely, $f(u_1) = v_6$, $f(u_2) = v_3$, $f_{(u_3)} = v_4$, $f(u_4) = v_5$, $f(u_5) = v_1$, $f(u)_6 = v_2$. To see whether f preserves edges, we examine the adjacency matrix of G.

$$A_G = \begin{array}{c} \\ u_1 \\ u_2 \\ u_3 \\ u_4 \\ u_5 \\ u_6 \end{array} \begin{array}{c} \begin{array}{cccccc} u_1 & u_2 & u_2 & u_4 & u_5 & u_6 \end{array} \\ \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 \end{bmatrix} \end{array}$$

And the adjacency matrix of H with the rows and columns labeled by the images of the corresponding vertices in G.

$$A_G = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \\ v_6 \end{array} \begin{array}{c} \begin{array}{cccccc} v_1 & v_2 & v_2 & v_4 & v_5 & v_6 \end{array} \\ \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 \end{bmatrix} \end{array}$$

Because $A_G = A_H$, it follows that f preserves edges. We conclude that f is an isomorphism, So G and H are isomorphic. Note that if f turned out not to be an isomorphism, we would not have established that G and H are not isomorphic, because another correspondence of the vertices in G and H may be an isomorphism.

12. **Prove that the product xy is odd if and only if both x and y are odd integers.**

Ans: The product xy is odd if and only if both x and y are odd.

Proof:

Part 1

If x and y are both odd then xy is odd.

Proof: By definition a = 2n + 1 and b = 2m + 1 for n, m integers.

Now consider the product ab = (2n + 1)(2m + 1)

= 4nm +2n +2m +1

= 2(2nm +n + m) + 1

= 2k

Where k = 2nm + n + m is an integer. Therefore the product xy is odd by definition of odd.

Part 2

If xy is odd then x and y are each odd.

Proof: (by contradiction)

Given that xy is odd assume that x and y are not both odd. If x and y are not both even then we must consider two cases

Case 1: Let x be even and y is odd. By definition we have x = 2n and y = 2m + 1 where n, m are integers.

Consider xy = (2n)(2m +1)= 4nm + 2n = 2(2nm +n) which is even. This contradicts that xy is in fact odd.

Case 2: Let x and y both be even. By definition x = 2n and y = 2m for n, m integers.

Consider the product xy = (2n)(2m) = 2(2nm) = 2k for k = 2nm is an integer. There we have that xy is even which is a contradiction to the fact that xy is odd.

Therefore by the two cases above x and y must both be odd.