DATE __/__/__

PAGE _____

# Assignment-4

## Section-A

**Ques1.** What is a Randomized Algorithm?

**Ans** A Randomized Algorithm is an Algorithm that makes random choices during its execution to achieve good expected performance or correctness. It uses random numbers to decide the steps it takes, which can help reduce complexity or handle uncertainty in inputs.

**Ques2.** Find out GCD of 96 and 36.

**Ans** Using the Euclid Algorithm,

$96 \div 36 = 2$ remainder 24

$36 \div 24 = 1$ remainder 12

$24 \div 12 = 2$ remainder 0

$\therefore$ GCD $(96, 36) = 12$.

**Ques3.** Define Approximate Algorithm.

**Ans** An approximation Algorithm is an Algorithm used to find near optimal solutions for optimization problems where finding an exact solution is computationally hard. It provides a solution close to the best possible one within a known bound.

**Ques4.** Write Quotient Remainder Theorem.

**Ans** Also called the Division Algorithm for integers:

For any integers $a$ (dividend) and $b$ (positive divisor) with $b > 0$, there exist unique integers $q$ (quotient) and $r$ (remainder) such that $a = bq + r$ with $0 \leq r < b$.

DATE / /

PAGE

Ques5. Define Modular Multiplication.

Ans Modular Multiplication is the process of multiplying two integers and taking the remainder when divided by a modulus n.

That is, for integers a, b and n:

$$(a \times b) \bmod n.$$

It gives the remainder after multiplying a and b and dividing by n.

## Section-B

Ques1. Explain Las-Vegas Algorithm with example.

Ans A las-Vegas Algorithm is a type of randomized algorithm that always produces a correct result, but the running time may vary depending on random choices made during its execution.

Key features:

- Output is always correct.
- Execution time may vary for different runs because of randomness.
- Randomness affects the efficiency, not the correctness.

Example: Randomized Quicksort.

Algorithm idea:-

- In normal Quick sort, we choose the first or last element as a pivot.
- In Randomized Quick Sort, we choose pivot randomly from the array.

Steps:-

DATE / /

PAGE

1. Select a random element as pivot.
2. Partition the array around the pivot.
3. Recursively sort the subarray.

Example:

Suppose we have an Array.

[3, 6, 8, 10, 1, 2, 1]

- A pivot is chosen randomly.
- The Array is partitioned into elements <6 and >6.
- Then, the process repeats recursively for each part.

Ques: Explain Monte-Carlo Algorithm with example.

Ans: A Monte-Carlo Algorithm is a type of randomized Algorithm that may produce an incorrect result with a small probability, but its running time is fixed or predictable. It uses randomness to achieve faster computation or simple logic, trading a little accuracy for efficiency.

Key features:-

- Execution time is fixed or predictable.
- Output may be incorrect with a small probability.
- Useful when exact Algorithm are too slow or complex.

Example: Primality Testing

Algorithm:-

1. Choose a random integer a, such that $1 < a < n-1$.
2. Compute $a^{n-1} \bmod n$.
3. If the result $\neq 1 \rightarrow n$ is composite.

DATE / /
PAGE

If the result $a^{n-1} \bmod n = 1$, n is probably prime.

Example:
Check if $n = 13$ is prime.
Choose random $a = 2$
$2^{12} \bmod 13 = 1 \rightarrow$ passes the test.
Choose $a = 5$
$5^{12} \bmod 13 = 1 \rightarrow$ passes again.

Hence, 13 is probably prime.
If we test $n = 15$,
$2^{14} \bmod 15 = 4 \neq 1 \rightarrow$ Composite

In short:
- Fixed running time.
- May give wrong answer.
- Formats: Primality Test, Monte Carlo Integration.

Ques 3. Define Lower Bound Theory in details.

Ans The lower bound theory in Algorithm analyses provides a theoretical limit on the best possible performance that any algorithm can achieve for a particular problem.

Purpose
The main goal of lower bound theory is to determine how efficient an Algorithm can possibly be.

Meaning:- If a problem requires atleast $f(n)$ operations to solve then:-

Lower Bound $= \Omega(f(n))$

DATE / /

PAGE

This means no Algorithm can solve the problem in fewer than $c \times f(n)$ operations for sufficiently large $n$.

Examples:-

1. Comparison-based Sorting:-

- Any Sorting Algorithm that sorts by comparing elements must make at least

$$\Omega(n \log n)$$

Comparisons in the worst case.

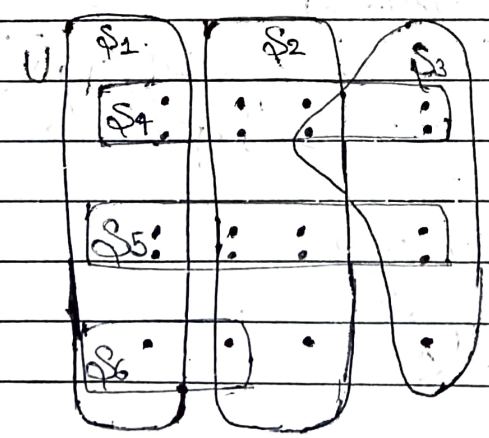
- Even the best Sorting Algorithm cannot do better than $n \log n$.

Importance of Lower Bound Theory:-

- It tells us how good an Algorithm can possibly get.
- Helps in identifying optimal Algorithms. If an Algorithm's time complexity matches the lower bound. That's the best possible one.
- Guides researchers to stop searching for faster Algorithms once the lower bound is reached.

## Section-C

Q1. Find Minimum Set Cover:-




Ans:- We can see, there are 6 sets: $S_1, S_2, S_3, S_4, S_5, S_6$

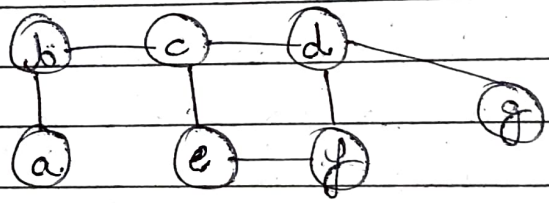
But observe,
$S_1$ covers whole first Column. (3 dots)
$S_2$ covers whole Second Column (3 dots).
$S_3$ covers whole third Column (3 dots).

Total dots = 9
These three Sets together cover all 9 dots.

→ Can two Sets cover all 9 dots?
No, each Set covers only 3 dots, so minimum Set need.

→ Final answer → Minimum Set Cover = $S_1, S_2, S_3$.

Ques: Find Vertex Cover from below diagram.




Ans: Step 1:
Vertices → $V = \{a, b, c, d, e, f, g\}$
Edges → (from the picture) →
$E = \{(a,b), (b,c), (c,d), (a,e), (e,f), (d,f), (d,g)\}$

Step 2: Show the graph is bipartite and choose a part one:
One Valid bipartition is →
- Left part $X = \{a, c, f, g\}$
- Right part $Y = \{b, e, d\}$

Step 3: Find a maximum matching. Find a matching one con

DATE / /

PAGE

ext matching is:→

$M = \{(a,b), (c,e), (d,g)\}$

These three edges are passive disjoint: They use the distinct vertices a, b, c, e, d, g. Thus, $|M| = 3$.

A matching of size 3 is largest possible here. So, the maximum matching size = 3.

Step-4 Konig's Theorem give a lower bound on Vertex cover.
Konig's Theorem: The size of a minimum vertex cover equals the size of a minimum matching. Therfore, any Vertex cover must have size at least $|M| = 3$. So, the minimum Vertex cover size $\geq 3$. If we find a cover of size 3 it will be minimum.

Step-5 Propose a Candidate Vertex Cover. Consider the set:

$C = \{b, d, e\}$

Verify it covers every edge,

- (a,b) → Covered by b.
- (b,c) → Covered by b.
- (c,d) → Covered by d.
- (c,e) → Covered by e.
- (e,f) → Covered by e.
- (d,f) → Covered by d.
- (d,g) → Covered by d.

So $C = \{b, d, e\}$ is a Vertex Cover and $|C| = 3$.
So C is minimum Vertex Cover.

Ques3. State Chinese remainder theorem. Solve the following Congruen-ces:→

DATE / /

PAGE

$x = 6 \pmod{11}$

$x = 13 \pmod{16}$

$x = 9 \pmod{21}$

$x = 19 \pmod{25}$

Ans Chinese Remainder Theorem

If $n_1, n_2, \ldots n_k$ are pairwise co-prime integers and $x = a_i \pmod{n_i}$, $(i = 1, \ldots k)$ then there exists a unique solution $x$ module $N = n_1 n_2 \ldots n_k$.

Moreover, one can construct the solution ($x$ module $N = n_1 n_2 \ldots n_k$) explicitly by standard CRT formula.

If $n_1 \ldots n_k$ are pairwise (coprime) and $x = a_i \pmod{n_i}$

$\Rightarrow x = \sum_{i=1}^{k} a_i N_i y_i \pmod{N}$ where $N_i = N/n_i$ and $y_i$ is the inverse of $N_i$ modulo $n_i$.

Moduli 11, 16, 21, 25 are pairwise Co-prime.

The moduli given are $n_1 = 11, n_2 = 16, n_3 = 21$ and $n_4 = 25$. As these are pairwise (co-prime, a unique soln exists modulo $N = 11 \times 16 \times 21 \times 25 = 92400$

→ From first Congruency $x = 11K + 6$ for some integer $K$. Substitute this into the second congruence:-

$11K + 6 = 13 \pmod{16}$.

$11K = 7 \pmod{16}$

⇒ The modular inverse of 11 mod 16 is 3 ($11 \times 3 = 33 \pmod{16}$)

$3(11)(K) = 3(7) \pmod{16}$

$K = 21 \pmod{16}$

$K = 5 \pmod{16}$

⇒ This means $K = 16j + 5$. Substitute the expression for $x_i$

DATE / /

PAGE

$x = 11(16j+5)+6 = 176j+55+6 = 176+61$

$\Rightarrow$ So $x \equiv 61 \pmod{176}$.

$\Rightarrow$ Now, substitute this into this:

$$176j+61 \equiv 9 \pmod{21}$$

$$176j \equiv -52 \pmod{21}$$

Since, $176 = 8\times21+8$ and $-52 \equiv -3$

$$8j \equiv 11 \pmod{21}$$

$\Rightarrow$ The modular inverse of 8 mod 21 is (mod 21),

$$8^{*}(8j) \equiv 8(11) \pmod{21}$$

$$j \equiv 88 \pmod{21}$$

$$j \equiv 4 \pmod{21}$$

$\Rightarrow$ This means $j = 21m+4$. Substitute into expression for $x$:

$$x = 176(21m+4)+61 = 3696m+704+61$$

So, $x \equiv 765 \pmod{3696}$.

$\Rightarrow$ Finally, substitute this into the fourth:

$$3696m+765 \equiv 19 \pmod{25}$$

$$3696m \equiv -746 \pmod{25}$$

Since, $3696 = 147\times25+21$ and $-746 \equiv -30\times24$

$$\Rightarrow 21m \equiv 4 \pmod{25}$$

$\Rightarrow$ The modular inverse of 21 and 25 is:

$$6(21\times6) = 126 = 5\times25+1 \equiv 1 \pmod{25}.$$

$$6(21m) \equiv 6(4) \pmod{25}.$$

$$m \equiv 24 \pmod{25}$$

$$m \equiv -1 \pmod{25}.$$

$\Rightarrow$ This means, $m = 25n-1$. Substitute this back into expression for $x$:

$$x = 3696(25n-1)+765 = 92400n-3696+765 = 92400n-2931$$

$\Rightarrow$ To get a positive solution, we can add modulus:

$$-2931+92400 = 89469$$

$\Rightarrow$ The smallest positive integer solution is 9469. The general soln is $\Rightarrow$ $x \equiv 89469 \pmod{92400}$.