Lesson Summary - GCD Algorithms

1. Introduction to GCD (HCF)

- Problem: Find the greatest common divisor of two numbers.

2. Method 1: List All Factors Method

- List factors of both numbers.

- Find the largest common factor.

- Time complexity: O(sqrt(n) + sqrt(m))

3. Method 2: Brute Force Linear Check

- Iterate from 1 to min(x, y).

- Time complexity: O(min(x, y))

4. Method 3: Euclidean Algorithm (Subtraction Version)

- Use property: GCD(a, b) = GCD(a-b, b) if a > b.

- Time complexity: O(max(a, b))

5. Method 4: Euclidean Algorithm (Modulo Version)

- Property: GCD(a, b) = GCD(b, a % b)

- Most efficient for software implementations.

- Time complexity: O(log(min(a, b)))

6. Method 5: Stein's Algorithm (Binary GCD Algorithm)

- Highly hardware-friendly (bitwise operations only).

- Steps:

a. If both a and b are even, factor out 2.

b. Remove all factors of 2 from both numbers.

c. Use subtraction and bit shifts to reduce.

d. Multiply back common powers of 2.

- Time complexity: O(log(max(a, b)))

- Uses only subtraction, bit shifts, no division or modulus.

- Used in embedded systems and cryptography.