Euclid's Algorithm

- Euclid's Algorithm finds the Greatest Common Divisor of two numbers.
- Consider a two factorable integers a and b.
- Express a and b in terms of prime factors.
- A number is said to be prime if it cannot be divided by any other number except by itself and 1.
- Assume a = $p1^{e1}$ x $p2^{e2}$x . . . pr^{er}
- Similarly b = $p1^{f1}$ x $p2^{f2}$x . . . pr^{fr}
- Then GCD of a and b is product of those prime factors with minimum exponents.

Example

- GCD of 32 and 48.

32=4*8

=(2^2)*(2^3)

=2^5.

48=6*8

=2*3*(2^3)

- Compare the factors of 32 and 48
- Common is 2^4. Therefore GCD of 32 and 48 is 16.

But finding the factors of very large number in this approach is not efficient so we go for Euclid's Algorithm.

<u>Euclid's Algorithm</u>

It is Based on Recursion theorem - GCD(a,b) = GCD(b, a mod b) - if a > b

Find the GCD of 48 and 32 using recursion theorem.

GCD(48,32) = GCD(32, 48 mod 32)

= GCD(32,16)

= GCD(16, 32 mod 16)

GCD(48,32) = GCD(16, 0)

= 16

Algorithm: Euclid (a, b)

- **Input : Two integers a and b**
- **Output: GCD of a and b**

1. if b == 0
2. return a
3. else return Euclid(b, a mod b)