**Cryptography & Network Security Lab**

**PRN/ Roll No: 2019BTECS00090**

**Full name: Udaykumar Gadikar**

**Assignment No. 8**

**Title: Euclidean and Extended Euclidean Algorithm**

**Aim: To Demonstrate Euclidean and Extended Euclidean Algorithm**

**Theory:**

**In mathematics, the Euclidean algorithm, or Euclid's algorithm, is an efficient method for computing the greatest common divisor (GCD) of two integers (numbers), the largest number that divides them both without a remainder.**

**The extended Euclidean algorithm is particularly useful when a and b are coprime. With that provision, x is the modular multiplicative inverse of a modulo b, and y is the modular multiplicative inverse of b modulo a.**

**Code:**

**GCD OF LARGE NUMBERS :**

def func(a,b):

    t1 = 0

    t2 = 1

    print('q','a','b','r','t1','t2','t')

    print(0,a,b,0,0,1,0)

    while (b != 0):

        q = a // b

        r = a % b

        a = b

        b = r

        t = t1 - (q \* t2)

        t1 = t2

        t2 = t

        print(q,a,b,r,t1,t2,t)

    return a

print("\n\nEnter number whose GCD to be calculated: ")

a=int(input("Enter A: "))

b=int(input("Enter B: "))

print("\n\nGCD of given numbers are: ",func(a, b))

print("\n\nGCD of given numbers are: ",func(a, b))

// #A = 6432428153848273761187304470153420054103716013509288496568501453281514041701282284606029140622859329

// #M = 34227914108859549112090175664574780960566395810040863485466385078705233752161570075653022955413546694845003472994702248311299420878539041547175332311829055758977182751275432094586376377033351685613086

**Modulo Multiplicative Inverse: -**

def Mod\_Inv( a, b):

    t1 = 0

    t2 = 1

    print('q','a','b','r','t1','t2','t')

    print(0,a,b,0,0,1,0)

    while (b != 0):

        q = a // b

        r = a % b

        a = b

        b = r

        t = t1 - (q \* t2)

        t1 = t2

        t2 = t

        print(q,a,b,r,t1,t2,t)

    if (t1 < 0):

        t1 = t1 + b

    return t1

print("\n\nTo finnd Modulo multiplicative inverse of a under  mod b")

a=int(input("Enter A: "))

b=int(input("Enter B: "))

print("\n\nModulo Multiplicative Inver of a under mod b is:  ",Mod\_Inv(a, b))

print("\n\nTo finnd Modulo multiplicative inverse of a under  mod b")

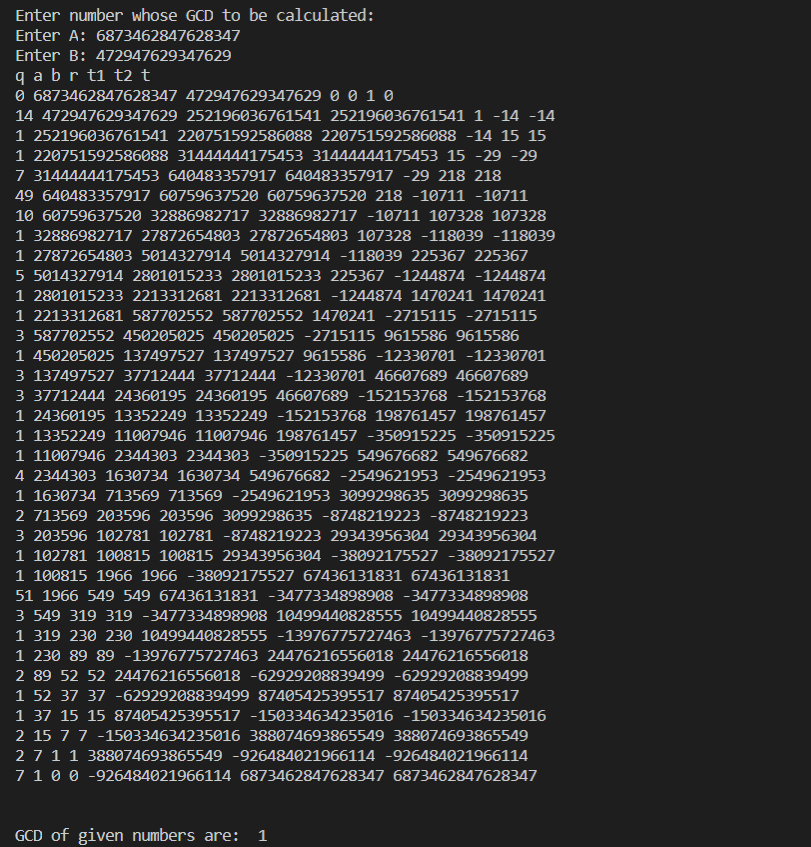
a=int(input("Enter A: "))

b=int(input("Enter B: "))

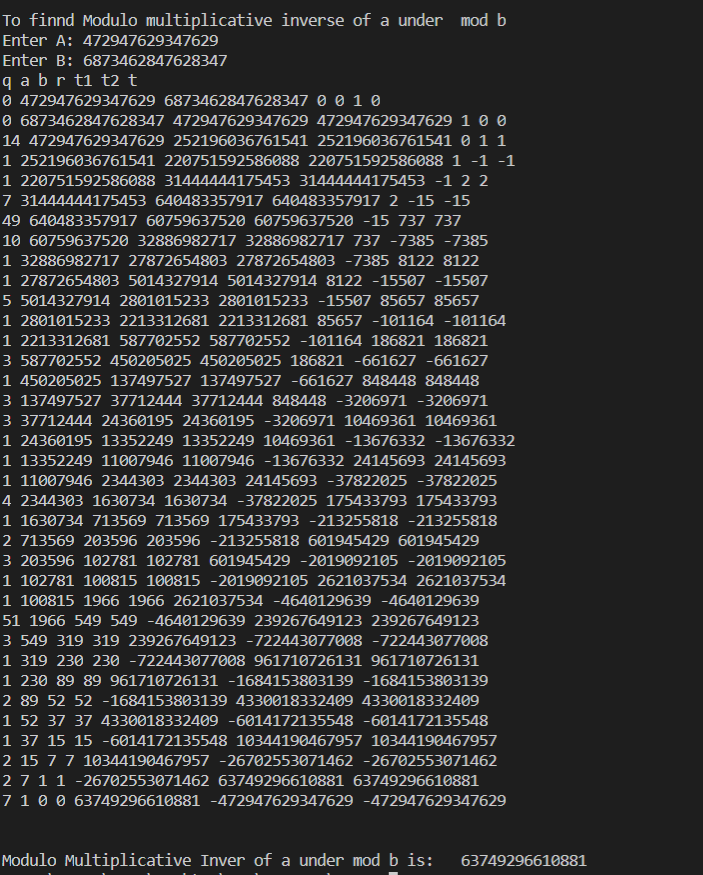
print("\n\nModulo Multiplicative Inver of a under mod b is:  ",Mod\_Inv(a, b))

**Output:**

**GCD output :**

****

**Modulo Multiplcative Inverse Output :**

****

**Conclusion:**

**The Euclidean and Extended Euclidean algorithm are used to find the GCD of numbers and the Multiplicative inverse of two coprime numbers respectively.**