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

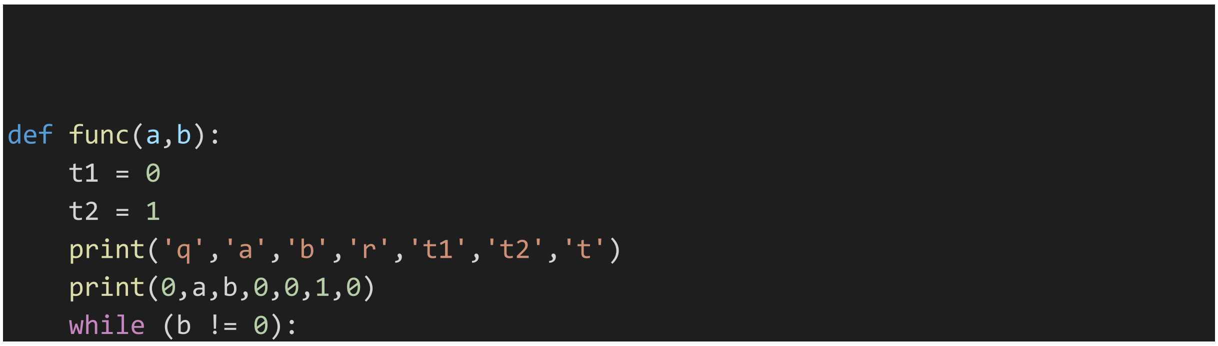
Theory:

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 :

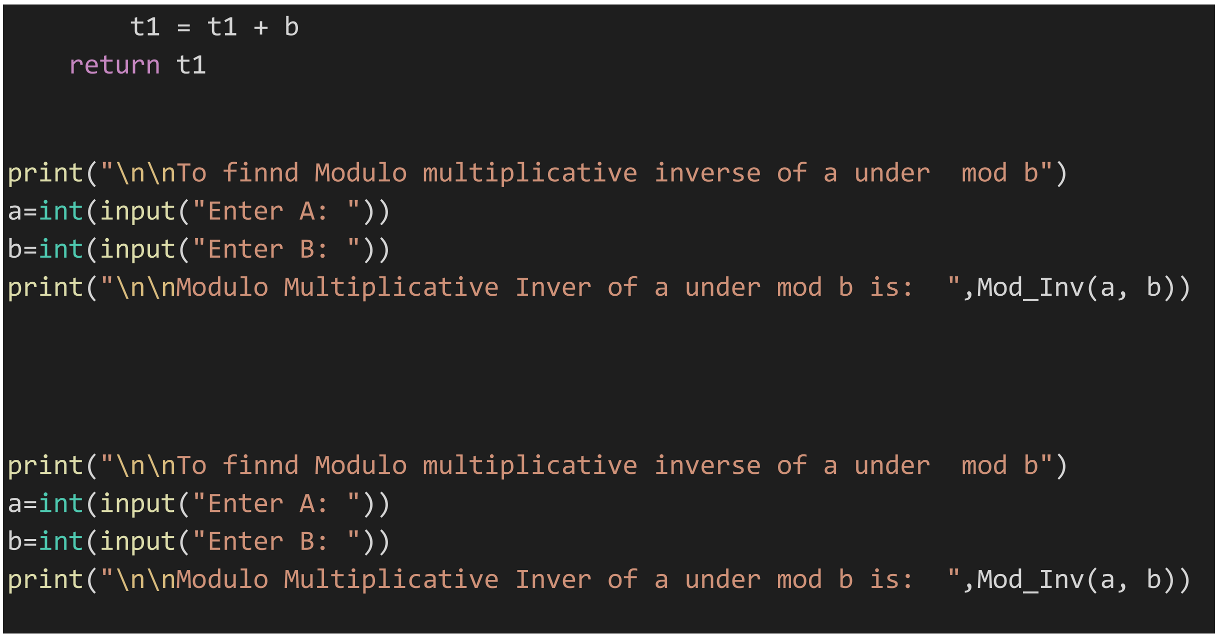


```
def func(a,b):
    t1 = 0
    t2 = 1
    print('q','a','b','r','t1','t2','t')
    print(0,a,b,0,0,1,0)
    while (b != 0):
        q = a // b
        r = a % b
        a = b
        b = r
        t = t1 - (q * t2)
        t1 = t2
        t2 = t
        print(q,a,b,r,t1,t2,t)
    return a

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 = 6432428153848273761187304470153420054103716013509288496568501453281514
041701282284606029140622859329
// #M = 3422791410885954911209017566457478096056639581004086348546638507870523
375216157007565302295541354669484500347299470224831129942087853904154717533231
1829055758977182751275432094586376377033351685613086
```

Modulo Multiplicative Inverse: -

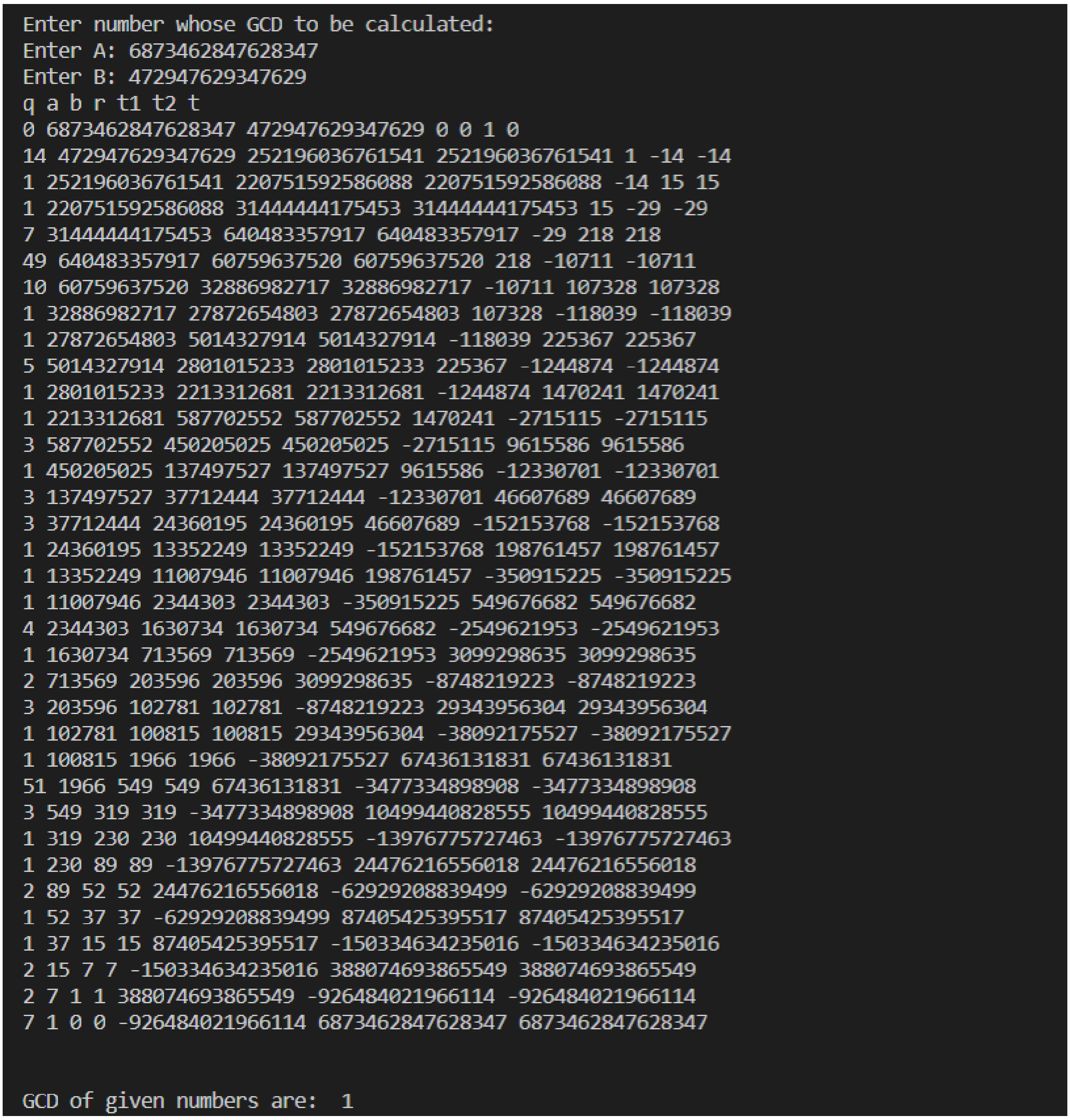
```


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))
```

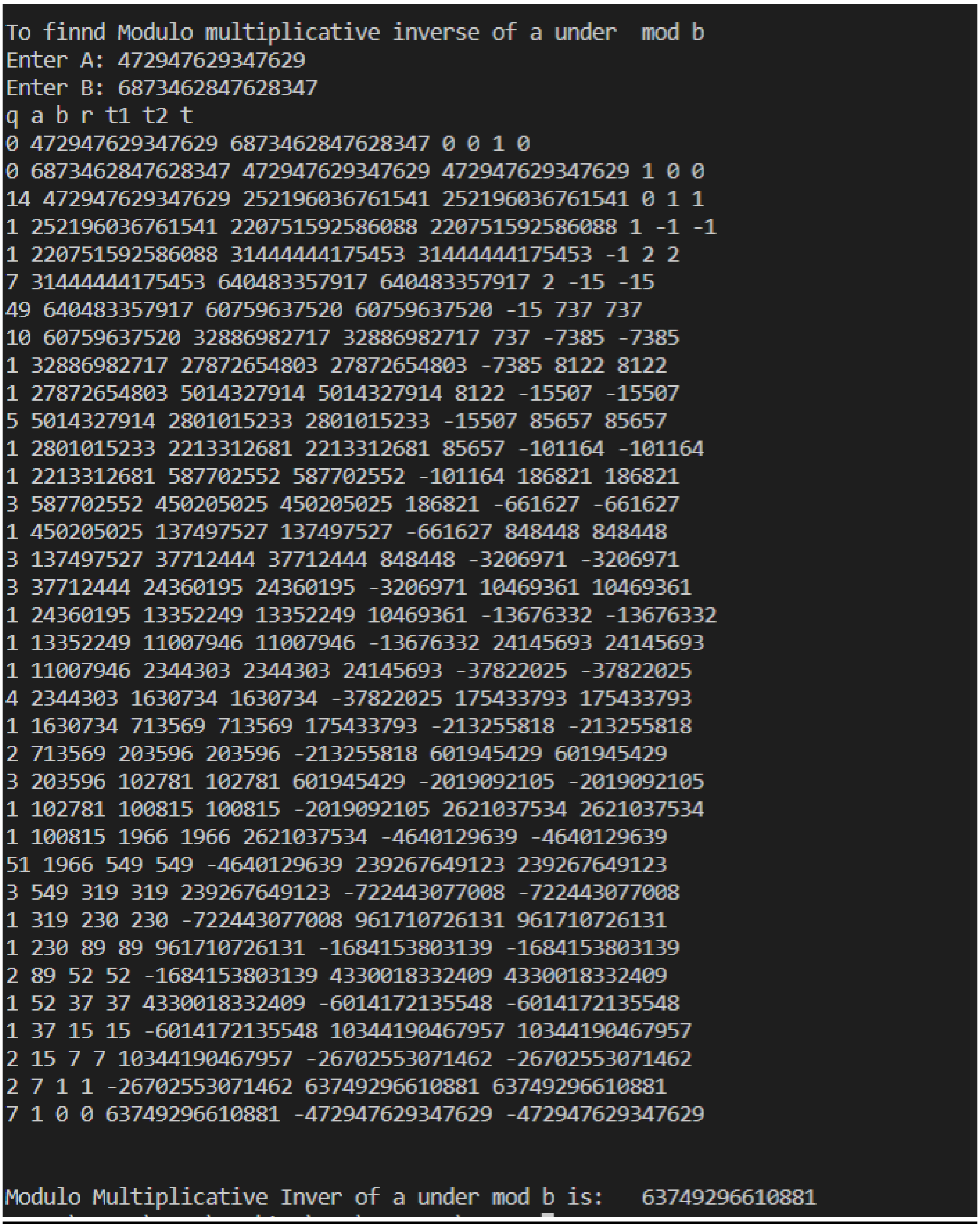
Output:

GCD output :



```
Enter number whose GCD to be calculated:
Enter A: 6873462847628347
Enter B: 472947629347629
q a b r t1 t2 t
0 6873462847628347 472947629347629 0 0 1 0
14 472947629347629 252196036761541 252196036761541 1 -14 -14
1 252196036761541 220751592586088 220751592586088 -14 15 15
1 220751592586088 31444444175453 31444444175453 15 -29 -29
7 31444444175453 640483357917 640483357917 -29 218 218
49 640483357917 60759637520 60759637520 218 -10711 -10711
10 60759637520 32886982717 32886982717 -10711 107328 107328
1 32886982717 27872654803 27872654803 107328 -118039 -118039
1 27872654803 5014327914 5014327914 -118039 225367 225367
5 5014327914 2801015233 2801015233 225367 -1244874 -1244874
1 2801015233 2213312681 2213312681 -1244874 1470241 1470241
1 2213312681 587702552 587702552 1470241 -2715115 -2715115
3 587702552 450205025 450205025 -2715115 9615586 9615586
1 450205025 137497527 137497527 9615586 -12330701 -12330701
3 137497527 37712444 37712444 -12330701 46607689 46607689
3 37712444 24360195 24360195 46607689 -152153768 -152153768
1 24360195 13352249 13352249 -152153768 198761457 198761457
1 13352249 11007946 11007946 198761457 -350915225 -350915225
1 11007946 2344303 2344303 -350915225 549676682 549676682
4 2344303 1630734 1630734 549676682 -2549621953 -2549621953
1 1630734 713569 713569 -2549621953 3099298635 3099298635
2 713569 203596 203596 3099298635 -8748219223 -8748219223
3 203596 102781 102781 -8748219223 29343956304 29343956304
1 102781 100815 100815 29343956304 -38092175527 -38092175527
1 100815 1966 1966 -38092175527 67436131831 67436131831
51 1966 549 549 67436131831 -3477334898908 -3477334898908
3 549 319 319 -3477334898908 10499440828555 10499440828555
1 319 230 230 10499440828555 -13976775727463 -13976775727463
1 230 89 89 -13976775727463 24476216556018 24476216556018
2 89 52 52 24476216556018 -62929208839499 -62929208839499
1 52 37 37 -62929208839499 87405425395517 87405425395517
1 37 15 15 87405425395517 -150334634235016 -150334634235016
2 15 7 7 -150334634235016 388074693865549 388074693865549
2 7 1 1 388074693865549 -926484021966114 -926484021966114
7 1 0 0 -926484021966114 6873462847628347 6873462847628347


GCD of given numbers are:  1
```

<u>Modulo Multiplcative Inverse Output :</u>



```
To finnd Modulo multiplicative inverse of a under  mod b
Enter A: 472947629347629
Enter B: 6873462847628347
q a b r t1 t2 t
0 472947629347629 6873462847628347 0 0 1 0
0 6873462847628347 472947629347629 472947629347629 1 0 0
14 472947629347629 252196036761541 252196036761541 0 1 1
1 252196036761541 220751592586088 220751592586088 1 -1 -1
1 220751592586088 31444444175453 31444444175453 -1 2 2
7 31444444175453 640483357917 640483357917 2 -15 -15
49 640483357917 60759637520 60759637520 -15 737 737
10 60759637520 32886982717 32886982717 737 -7385 -7385
1 32886982717 27872654803 27872654803 -7385 8122 8122
1 27872654803 5014327914 5014327914 8122 -15507 -15507
5 5014327914 2801015233 2801015233 -15507 85657 85657
1 2801015233 2213312681 2213312681 85657 -101164 -101164
1 2213312681 587702552 587702552 -101164 186821 186821
3 587702552 450205025 450205025 186821 -661627 -661627
1 450205025 137497527 137497527 -661627 848448 848448
3 137497527 37712444 37712444 848448 -3206971 -3206971
3 37712444 24360195 24360195 -3206971 10469361 10469361
1 24360195 13352249 13352249 10469361 -13676332 -13676332
1 13352249 11007946 11007946 -13676332 24145693 24145693
1 11007946 2344303 2344303 24145693 -37822025 -37822025
4 2344303 1630734 1630734 -37822025 175433793 175433793
1 1630734 713569 713569 175433793 -213255818 -213255818
2 713569 203596 203596 -213255818 601945429 601945429
3 203596 102781 102781 601945429 -2019092105 -2019092105
1 102781 100815 100815 -2019092105 2621037534 2621037534
1 100815 1966 1966 2621037534 -4640129639 -4640129639
51 1966 549 549 -4640129639 239267649123 239267649123
3 549 319 319 239267649123 -722443077008 -722443077008
1 319 230 230 -722443077008 961710726131 961710726131
1 230 89 89 961710726131 -1684153803139 -1684153803139
2 89 52 52 -1684153803139 4330018332409 4330018332409
1 52 37 37 4330018332409 -6014172135548 -6014172135548
1 37 15 15 -6014172135548 10344190467957 10344190467957
2 15 7 7 10344190467957 -26702553071462 -26702553071462
2 7 1 1 -26702553071462 63749296610881 63749296610881
7 1 0 0 63749296610881 -472947629347629 -472947629347629


Modulo Multiplicative Inver of a under mod b is:   63749296610881
```

Conclusion:

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