**Experiment No. 1**

**Aim**: To find the multiplicative inverse of any number Zn using Extended Euclidean algorithm.

**Theory**: Extended Euclidean algorithm can be used to find the multiplicative inverse of number on modulus operation if exist. Relation can be derived as follows:

i.e.

This can be written as:

Comparing it with:

We inferred that inverse of exist or only holds, when and in Extended Euclidean equation.

Above equation also clear that we can use Extended Euclidean algorithm to find multiplicative inverse of a number. Let us look at algorithm and example:

**Extended Euclidean algorithm**:

Initialize:

Repeat following steps till):

1. -------- {Where, // refers to integer division}

2.

3. ------- {Interchange r1 and r2 with r2 and r}

4.

5. ------- {Interchange t1 and t2 with t2 and t}

After completion of iteration if then inverse exist and it is stored in variable.

**Example**:

Let b= 420, n = 69

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| q | r1 | r2 | r | t1 | t2 | t |
| 6 | 420 | 69 | 6 | 0 | 0 | -6 |
| 11 | 69 | 6 | 3 | 1 | -6 | 67 |
| 2 | 2 | 6 | 0 | -6 | 67 | -140 |
|  | 3 | 0 |  | 67 | -140 |  |

Since, multiplicative inverse of 420 doesn’t exist when mod with 69.

**Implementation**:

import pandas as pd  
  
def multiplicative\_inverse(b,n):  
 r1,r2,t1,t2 = b,n,0,1  
 arrays = [[] for \_ in range(7)]  
   
 while(r2>0):  
 q = r1//r2  
 arrays[0].append(q), arrays[1].append(r1), arrays[2].append(r2)  
   
 r = r1 - q\*r2  
 r1,r2 = r2,r  
 arrays[3].append(r), arrays[4].append(t1), arrays[5].append(t2)  
   
 t = t1 - q\*t2  
 t1,t2 = t2,t  
 arrays[6].append(t)  
   
 b\_inverse = t1 if r1 == 1 else False  
   
 arrays[0].append(None), arrays[1].append(r1), arrays[2].append(r2)  
 arrays[3].append(None), arrays[4].append(t1), arrays[5].append(t2)  
 arrays[6].append(None)  
   
 table = pd.DataFrame({  
 "q": arrays[0],  
 "r1": arrays[1],  
 "r2": arrays[2],  
 "r": arrays[3],  
 "t1": arrays[4],  
 "t2": arrays[5],  
 "t": arrays[6]  
 })  
   
 return b\_inverse,table   
  
b,n = map(int,input("Please enter the value of two numbers to find their multiplicative inverse: ").strip().split(" "))  
  
b\_inverse,table = multiplicative\_inverse(b,n)  
  
if not b\_inverse:  
 print("Inverse doesn't exist")  
else:  
 print(f"Inverse of b = {b\_inverse+n if b\_inverse<0 else b\_inverse}")  
  
table

**Output**:



