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:

$$b(t) \equiv 1(mod n)$$

i.e. $t = b^{-1}$

This can be written as:

$$b(t) = n(q) + 1$$

$$b(t) + n(-q) = 1$$

Comparing it with: $b(x) + a(y) = GCD(b, a)$

We inferred that inverse of 'b' (t) exist or $b(t) \equiv 1(mod n)$ only holds, when $GCD(b, n) = 1$ and $b^{-1} = t = x$ 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: $r1 = b, r2 = n, t1 = 0 \; and \; t2 = 1$

Repeat following steps till$(r2 > 0)$:

1. $q = r1//r2$ -------- {Where, // refers to integer division}
2. $r = r1 - q * r2$
3. $r1, r2 = r2, r$ ------- {Interchange r1 and r2 with r2 and r}

4. $t = t1 - q * t2$

5. $t1, t2 = t2, t$ ------- {Interchange t1 and t2 with t2 and t}

After completion of iteration if $r1 = 1 \Rightarrow GCD(b,n) = 1$ then inverse exist and it is stored in $t1(b^{-1})$ 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, $r1 != 1$ 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 m
ultiplicative 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:

```
Please enter the value of two numbers to find their multiplicative inverse: 95 77
Inverse of b = 40
```

	q	r1	r2	r	t1	t2	t
0	1.0	95	77	18.0	0	1	-1.0
1	4.0	77	18	5.0	1	-1	5.0
2	3.0	18	5	3.0	-1	5	-16.0
3	1.0	5	3	2.0	5	-16	21.0
4	1.0	3	2	1.0	-16	21	-37.0
5	2.0	2	1	0.0	21	-37	95.0
6	NaN	1	0	NaN	-37	95	NaN

```
Please enter the value of two numbers to find their multiplicative inverse: 7000 85
Inverse doesn't exist
```

	q	r1	r2	r	t1	t2	t
0	82.0	7000	85	30.0	0	1	-82.0
1	2.0	85	30	25.0	1	-82	165.0
2	1.0	30	25	5.0	-82	165	-247.0
3	5.0	25	5	0.0	165	-247	1400.0
4	NaN	5	0	NaN	-247	1400	NaN