University of Bahrain

College of Information Technology

Department of Computer Engineering

Assignment 2

Systematically Calculate the Multiplicative Inverse

Name: Sayed Jaafar Sadeq Ahmed **ID: 20184311**

Name: Maitham Ali Isa Maki **ID: 20186039**

Required points: -

The language program you implemented. **Python**

1- **Overview of the program**

   Asking the user to enter 2 positive integer and find the Multiplicative inverse of it, and if there is no multiplicative inverse it will show you the output.

2- **Prerequisite.**

   python 3.x (no matter the verion)

3- **Provide the procedures (steps) for the compiling and executing**

   The user must enter 2 positive number (a) to find the multiplicative invers for and the modules (b), after the user enter these data, the program will module (a) % (b) and the output will be in terminal

4- **Show the type of the input data and provide a snapshot**

   Enter a number (a) to find its multiplicative inverse for: 3
   Enter a number (b) which is the modulos: 11
   The multiplicative inverse of 3 mod 11 is 4.

5- **Sample of the output**

```
Enter a number (a) to find its multiplicative inverse for: 3
Enter a number (b) which is the modulos: 11

The multiplicative inverse of 3 mod 11 is 4.
```

6- Test your program with the following inputs:

a. Input: 3 and 11
b. Input: 10 and 17
c. Input: 2 and 4

A. Output (11 mod 3)

```
Enter a number (a) to find its multiplicative inverse for: 11
Enter a number (b) which is the modulos: 3

The multiplicative inverse of 11 mod 3 is 2.
```

B. Output (17 mod 10)

```
Enter a number (a) to find its multiplicative inverse for: 17
Enter a number (b) which is the modulos: 10

The multiplicative inverse of 17 mod 10 is 3.
```

C. Output (4 mod 2)

```
Enter a number (a) to find its multiplicative inverse for: 4
Enter a number (b) which is the modulos: 2

The multiplicative inverse of 4 does not exist in mod 2.
```

Proving :

A. $11^{-1} \bmod 3$

$gcd(3, 11) = \ 11 = 3 \times 3 + 2 \quad \rightarrow \quad 2 = 11 - 3 \times 3$

$gcd(2, 3) = 3 = 1 \times 2 + 1 \quad \rightarrow \quad 1 = 3 - 2$

$gcd(1, 2) = \ 2 = 1 \times 2 + 0 \quad \rightarrow \quad 0 = 2 - 2$

$gcd(0, 1) = 1 \rightarrow coprime, so\ we\ have\ multiplicative\ inverse$

Se substitute (2) by (11-3x3)

$1 = 3 - 2$

$1 = 3 - (11 - 3 \times 3)$

$= 4 \times 3 - 11$

So, MI of 11 is → $-1\ mod\ 3 \ \equiv 2\ mod\ 3$

B. $17^{-1}\ mod\ 10$

$gcd\ (10, 17) = \ 17 = 1 \times 10 + 7 \quad \rightarrow \quad 7 = 17 - 10$

$gcd\ (7, 10) = \ 10 = 1 \times 7 + 3 \quad \rightarrow \quad 3 = 10 - 7$

$gcd\ (3, 7) = 7 = 2 \times 3 + 1 \quad \rightarrow \quad 1 = 7 - 2 \times 3$

$gcd\ (1, 3) = \ 3 = 3 \times 1 + 0 \quad \rightarrow \quad 0 = 3 - 3$

$gc\ d(0, 1) = 1 \rightarrow coprime, so\ we\ have\ multiplicative\ inverse$

We substitute (3) by (10-7)

$1 = 7 - 2 \times 3$

$1 = 7 - 2 \times (10 - 7)$

$3 \times 7 - 2 \times 10$

We Substitute (7) by (17-10)

$3 \times (17 - 10) - 2 \times 10$

$3 \times 17 - 5 \times 10$

So, MI of 17 is → $3\ mod\ 10$

C. $4^{-1}\ mod\ 2$

gcd(2,4) = (0,2) = 2

So, we don't have Multiplicative inverse for 4^{-1} and the output for python program is correct. It shows there is no MI.