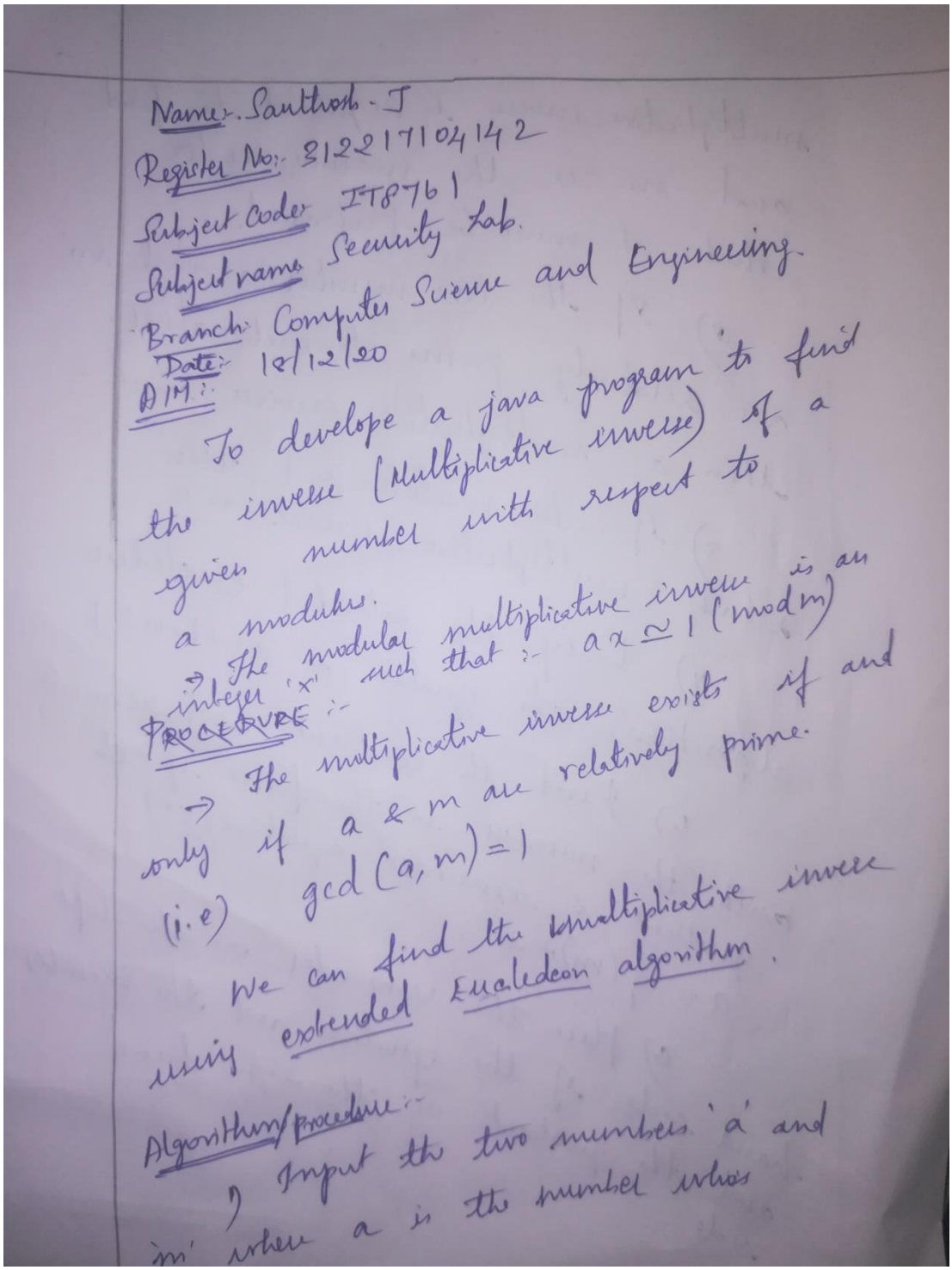
Name: Santhosh J

Register number: 312217104142

IT8761-Security Lab SEMESTER PRACTICALS



Name:- Santhosh - J
Register No:- 312217104142
Subject Code:- IT8761
Subject name:- Security Lab.
Branch:- Computer Science and Engineering.
Date:- 18/12/20

AIM:-

To develope a java program to find the inverse (Multiplicative inverse) of a given number with respect to a modulus.

⇒ The modular multiplicative inverse is an integer 'x' such that :- $ax \equiv 1 \pmod{m}$

PROCEDURE :-

→ The multiplicative inverse exists if and only if a & m are relatively prime.

(i.e) $\gcd(a, m) = 1$

We can find the multiplicative inverse using extended Eualedean algorithm.

Algorithm/procedure :-

1) Input the two numbers 'a' and 'm' where a is the number whos

multiplicative inverse is required to find and 'm' is the modulo under which it must be performed.

2) If the two number 'a' and 'm' are relatively prime to each other, then a multiplicative inverse exist.

3) If the modulus is 1, then multiplicative inverse is 0.

4) Using the extended euclidean algorithm, the equation is $ax+bm=1$

5) Find the quotient and remainder with the number in the form of the quotient & remainder equation (i.e) $a = q(m)+r$.

6) Place the remainder on the left hand side of the equation and the number and the quotient on the right hand side.

7) Substitute the number in the equation until we get the number whose inverse is required.

8) Iterate through steps (5) to (7) untill gcd becomes 1.

9) Return the multiple of the number in the equation which is the inverse

10) Terminate the program.

Result:-

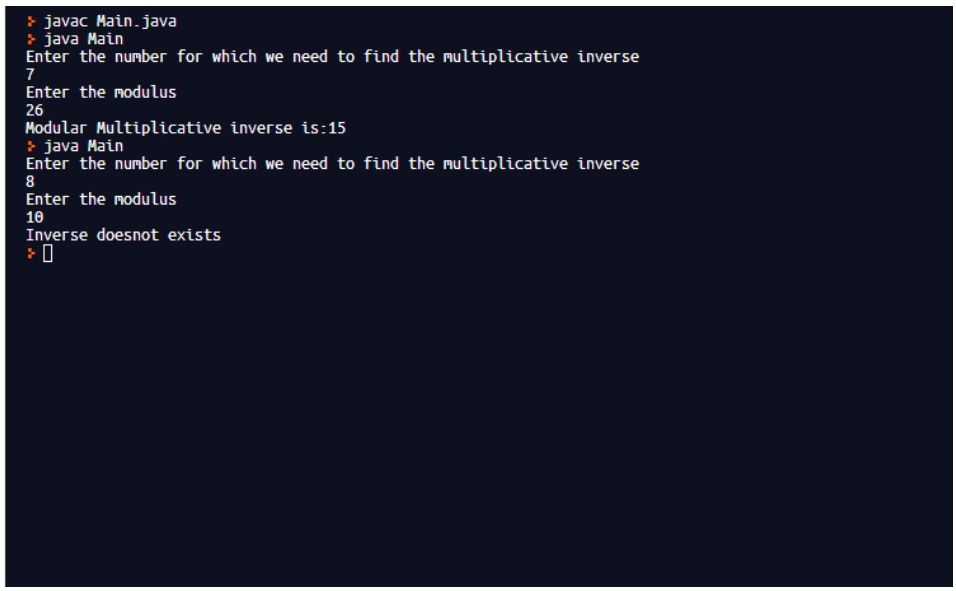
Thus java program to find the Multiplicative inverse of a given number with respect to modulus is implemented and verified.

CODE

```
//TO DEVELOP A JAVA PROGRAM TO FIND MODULAR MULTIPLICATIVE INVERSE OF THE GIVEN NUMBER
import java.util.*;
import java.io.*;
class Main{
   public static int gcd(int a, int b)
    {
      if (b == 0)
        return a;
      return gcd(b, a % b);
    }
  public static int modinverse(int a,int m)
  {
    if(gcd(a,m)==1)
    {
    int m0=m;
    int y=0,x=1;

    if(m==1)
       return 0;
    while(a>1 && m!=0)
    {
      int q=a/m;
      int t=m;
     // System.out.println(" "+m);
      m=a%m;
      a=t;
      t=y;
      y=x-q*y;
      x=t;
    }
    if(x<0)
        x+=m0;

    return x;
    }
    else
    {
      return -1;
    }

  }
  public static void main(String args[])
  {
    Scanner sc=new Scanner(System.in);
    System.out.println("Enter the number for which we need to find the multiplicative
inverse");
    int a=sc.nextInt();
    System.out.println("Enter the modulus");
    int m=sc.nextInt();
    int ans=modinverse(a,m);
    if(ans==-1)
        {
```

```
            System.out.println("Inverse doesnot exists");
        }
    else
    {
        System.out.println("Modular Multiplicative inverse is:"+modinverse(a,m));
    }
  }

}
```

SAMPLE INPUT/OUTPUT:



`