Lab – 6

Subject: NIS

Aim: Write a Program to generate the Points on the Elliptical Curve E_p(a,b)

Program: -

```
import java.util.*;
import java.lang.*;

public class ecc
{
    public static boolean isPerfactSquare(long n){

        double sqrt = Math.sqrt((double)n);
        return (sqrt - Math.floor(sqrt)==0);

    }

    public static long pow(long a,long b){
        if(b == 0){
            return 1;
        }
        else{
            return a * pow(a,--b);
        }

    }

    public static long isCongruant(long a , long n){

        if((a+1) % n == 0){
            return -1;
        }
        else
        {
            return 1;
        }

    }

    public static long positiveInvers(long inverse,long n){

         while(inverse < 0){
            inverse = inverse + n;
         }
        return inverse;
     }
```

```
public static void elipticalCurve(long a,long b,long p)
{

    long x = 0;
    long w = 0;
    while(x<p){

        w = (pow(x,3) + a*x + b) % p;
        long temp = pow(w,((p-1)/2)) % p;

        if(isCongruant(temp,p) == -1){
            System.out.println("No Solution For : " + x);
            x++;
            continue;
        }

        if(isCongruant(temp,p) == 1){

            while(!isPerfactSquare(w)){

                if((p*p) <= w){
                    break;
                }
                w =w + p;
            }
            w = (long)Math.sqrt(w);

            long pointA = ~(w-1);
            pointA = positiveInvers(pointA,p);


            System.out.println("( " + x +" , " + pointA +")");
            System.out.println("( " + x +" , " + w +")");

        }
        x++;
    }

}

public static void main(String[] args) {

    int i=0;
    long a=0,b=0;

    while(true){
        if(((int)Math.pow(i,3)*4 + 27*(int)Math.pow(i,2))!=0){
```

```
                a=i;
                b=i;
                break;
            }
            i++;
        }
        System.out.println("a is : " + a +" b is : " + b);
        long p = 13;
        elipticalCurve(a,b,p);

    }
}
```

Output: -

P=13

```
D:\DDIT\sem6\NIS\LAB\lab6>javac ecc.java

D:\DDIT\sem6\NIS\LAB\lab6>java ecc
a is : 1 b is : 1
( 0 , 12)
( 0 , 1)
( 1 , 9)
( 1 , 4)
No Solution For : 2
No Solution For : 3
( 4 , 11)
( 4 , 2)
( 5 , 12)
( 5 , 1)
No Solution For : 6
( 7 , 0)
( 7 , 0)
( 8 , 12)
( 8 , 1)
No Solution For : 9
( 10 , 7)
( 10 , 6)
( 11 , 11)
( 11 , 2)
( 12 , 8)
```

P = 17

```
D:\DDIT\sem6\NIS\LAB\lab6>java ecc
a is : 1 b is : 1
( 0 , 18)
( 0 , 1)
No Solution For : 1
( 2 , 12)
( 2 , 7)
No Solution For : 3
No Solution For : 4
( 5 , 13)
( 5 , 6)
No Solution For : 6
( 7 , 16)
( 7 , 3)
No Solution For : 8
( 9 , 13)
( 9 , 6)
( 10 , 17)
( 10 , 2)
No Solution For : 11
No Solution For : 12
( 13 , 11)
( 13 , 8)
( 14 , 17)
( 14 , 2)
( 15 , 16)
( 15 , 3)
( 16 , 16)
( 16 , 3)
No Solution For : 17
No Solution For : 18
```