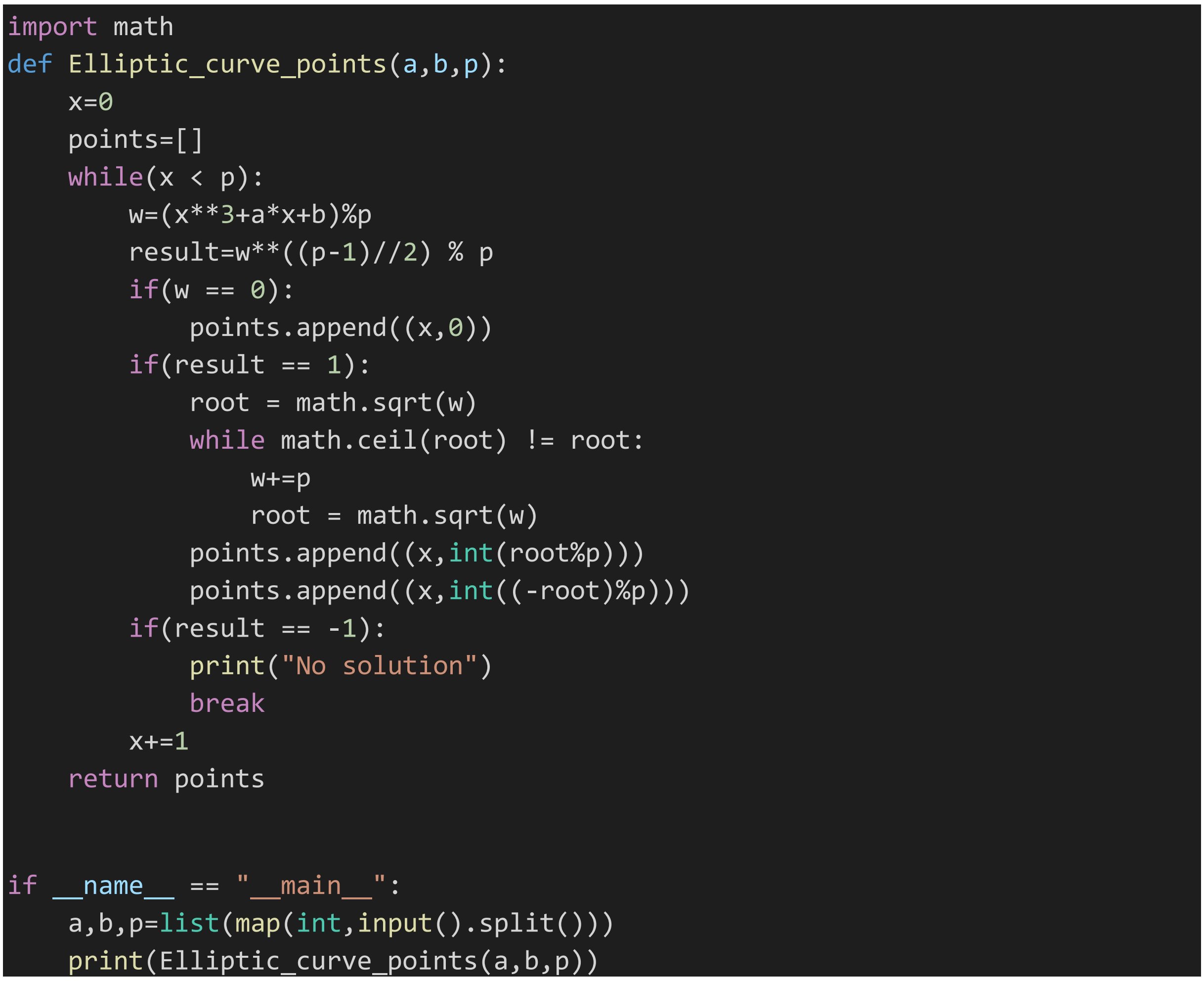
Lab – 6

Subject : NIS

Aim: Implementation of ECC cryptography algorithm.

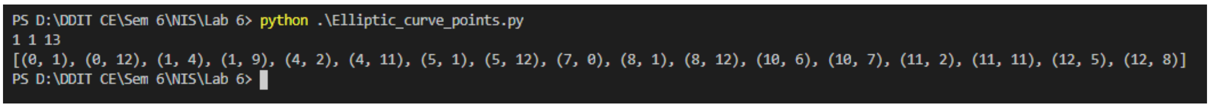
Program: -



```
import math
def Elliptic_curve_points(a,b,p):
    x=0
    points=[]
    while(x < p):
        w=(x**3+a*x+b)%p
        result=w**((p-1)//2) % p
        if(w == 0):
            points.append((x,0))
        if(result == 1):
            root = math.sqrt(w)
            while math.ceil(root) != root:
                w+=p
                root = math.sqrt(w)
            points.append((x,int(root%p)))
            points.append((x,int((-root)%p)))
        if(result == -1):
            print("No solution")
            break
        x+=1
    return points


if __name__ == "__main__":
    a,b,p=list(map(int,input().split()))
    print(Elliptic_curve_points(a,b,p))
```

Output:-



```
PS D:\DDIT CE\Sem 6\NIS\Lab 6> python .\Elliptic_curve_points.py
1 1 13
[(0, 1), (0, 12), (1, 4), (1, 9), (4, 2), (4, 11), (5, 1), (5, 12), (7, 0), (8, 1), (8, 12), (10, 6), (10, 7), (11, 2), (11, 11), (12, 5), (12, 8)]
PS D:\DDIT CE\Sem 6\NIS\Lab 6>
```

Description:-

- There are algorithms like RSA, Elgamal these are too costly for implementation that's why the concept of elliptical curve cryptography.

- Elliptic Curve Cryptography (ECC) is a key-based technique for encrypting data. ECC focuses on pairs of public and private keys for decryption and encryption of web traffic.
- ECC is frequently discussed in the context of the Rivest–Shamir–Adleman (RSA) cryptographic algorithm. RSA achieves one-way encryption of things like emails, data, and software using prime factorization.
- In this algorithm we are finding the point of curve.
- Take big prime number then take two points a and b then check the condition whether these a and b are valid or not, by using 4a^3 + 3b^3 != 0.
- Then put x = 0 and go through the loop until x < prime. And find all points.
- In algorithm we have to find w ^ (prime – 1)//2 mod prime == 1. Then an only there is a root otherwise not.
- If there is w ^ (prime – 1)//2 mod prime == prime – 1 then there is no solution for that particular x value.