NIS

LAB - 8

- → Name : shubham shingala p.
- → ID NO.: 19CEUOS159
- → Roll No.: CE146

* **AIM:** Write a program to implement Eliptical curve cryptograph. (point Generation). create points for the given Eliptical cryptosystem ECC cryptography.

* **source code:**

```
#include <bits/stdc++.h>
#define ll long long
#define loop(var, s, n) for(ll var=s; var<n; var++)
#define pb push_back
using namespace std;

class Point {
  public:
      ll x, y;
      point(ll X, ll Y) { x=X; y=Y; }
      void print() { cout<<"("<<x<<","<<y<<")"; }
};

ll squareMultiply (ll base, ll exp, ll mod)
{
          // base^exp (% mod)
}
```

```
bool    is Prime (ll n)
{
    // if(Prime) return true;   else  false;
}

ll   mod (ll a, ll b)
{
        ll  mode  =  a % b ;
        if (mode <0)
            mode  +=b;
        return   mode;
}

vector<Point>    PointGeneration( ll a, ll b, ll P)
{
     vector<Point>   Points;
     loop (x, 0, P)
     {
          ll  y_square  = mod((x*x*x)+(a*x) +b
                                        , P) ;
          ll r=  squaremultiply (y_square,(P-1)/2,P)
          if (r == 1)
          {
               ll  y = sqrt(y_square) ;
               while ( y*y  != y_square)  {
                    y_square  += P;
                    y =  sqrt(y_square);
               }
               ll   y1  =  mod (-y, P) ;
```

```
                points.pb(point(x,y));
                points.pb(point(x,y1));
            }
            else if(r == 0)
                points.pb(point(x,0));
        }
        return points;
    }

    int main()
    {
        ll a, b, p;
        cout << "Enter a and b :";
        cin >> a >> b;
        while (1) {
            cout << "Enter prime number:";
            cin >> p;
            if(!is prime(p))
                cout<< p <<" is not a prime numbe
                            so, ";
            else
                break;
        }

        vector<point> points = pointGeneration
                                    (a; b, p);
        loop(i,0, points.size()) points[i].
                                    print();
        cout<< endl;
    }
```

* **Test-case-1:**

Input: a=1 , b=1

prime number P=13

output:

```
(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)
```

* **Test-case-2:**

Input: a=12 , b=213

P = 312

— 312 is not prime numbe so, Enter prime number : 317

output:

```
(0,3)   (0,14)  (3,2)   (3,15)
(4,6)   (4,11)  (6,5)   (6,12)
(9,8)   (9,9)   (13,4)  (13,13)
(16,8)  (16,9)
```