7CM2

SUMA DE PUNTOS

SELECTED TOPICS IN CRYPTOGRAPHY

FRANCISCO UZIEL CORDOVA PICHARDO

Introducción:

La suma y el doblado de puntos en curvas elípticas son operaciones fundamentales en el álgebra de curvas elípticas, y juegan un papel clave en la criptografía de clave pública y en otros campos de la matemática aplicada.

En términos generales, una curva elíptica es una curva plana definida por una ecuación de la forma y^2 = x^3 + ax + b, donde a y b son constantes. Los puntos en la curva elíptica pueden ser sumados y duplicados, lo que significa que se pueden calcular la suma y el doble de cualquier par de puntos en la curva.

La suma de puntos en una curva elíptica es una operación geométrica que consiste en trazar una línea recta que atraviesa dos puntos en la curva, y luego encontrar el tercer punto en la curva que intercepta esa línea. El resultado de la suma es otro punto en la curva elíptica.

El doblado de un punto en una curva elíptica es simplemente la suma del punto consigo mismo. Es decir, se traza una línea tangente al punto, y luego se encuentra el segundo punto de intersección en la curva. El resultado de este proceso es otro punto en la curva elíptica.

La suma y el doblado de puntos en curvas elípticas tienen muchas aplicaciones en la criptografía, incluyendo la construcción de sistemas de cifrado asimétricos, tales como el cifrado ElGamal y el esquema de firma digital ECDSA. Estas técnicas también se utilizan en otros campos, como la geometría algebraica y la teoría de números.

Funciones:

Esta función es la que realiza la suma de puntos en el programa.

```java
public static int[] SumPun(int x1, int y1, int x2, int y2, int p) {
    System.out.println("Vamos a sumar los puntos");
    int m;
    int part1 = y2 - y1;
    int part2 = x2 - x1;
    long inversoMul[];
    part2 = part2 % p;
    part1 = part1 % p;
    if (part2 < 0) {
```

```
        part2 = p + part2;
    }
    if (part1 < 0) {
        part1 = p + part1;
    }
    //inverso multiplicativo de p2
    inversoMul = AEE.euclidesExtendido(part2, p);
    part2 = (int) inversoMul[1];

    //System.out.println("parte 2= " + part2);
    m = (part1 * part2) % p;
    int x3 = ((int) pow(m, 2)) - x1 - x2;
    x3 = x3 % p;
    int y3 = m * (x1 - x3) - y1;
    y3 = y3%p;
    if (y3 < 0) {
        y3 = p + y3;
    }
    if (x3 < 0) {
        x3 = p + x3;
    }
    System.out.println("x3= " + x3 + " y3= " + y3);
    int par[] = new int[2];
    par[0] = x3;
    par[1] = y3;
    return par;
}
```

En la función DobPun se realiza el doblado de punto es decir un punto sumado consigo mismo.

```
public static int[] DobPun(int x, int y, int a, int p) {
    System.out.println("Vamos a doblar el punto");
    int m;
    int part1 = (3 * ((int) pow(x, 2)) + a);
    int part2 = 2 * y;
    long inversoMul[];
    //inverso multiplicativo de p2
    //System.out.println(part2);
    part2 = part2 % p;
    part1 = part1 % p;
    if (part2 < 0) {
        part2 = p + part2;
    }
```

```
    if (part1 < 0) {
        part1 = p + part1;
    }
    inversoMul = AEE.euclidesExtendido(part2, p);
    part2 = (int) inversoMul[1];

    //System.out.println(part2);
    m = (part1 * part2) % p;
    //System.out.println(m);
    int x3 = ((int) pow(m, 2)) - x - x;
    x3 = x3 % p;
    int y3 = m * (x - x3) - y;
    y3 = y3 % p;
    System.out.println("x3= " + x3 + " y3= " + y3);
    if (y3 < 0) {
        y3 = p + y3;
    }
    if (x3 < 0) {
        x3 = p + x3;
    }
    int par[] = new int[2];
    par[0] = x3;
    par[1] = y3;
    return par;
}
```

Esta función retorna un verdadero si encuentra que el punto ingresado es un generador y un false si no es generador.

```
public static boolean esGenerador(int x, int y, int p, int a, int b,
CurvaEliptica ce) {
    int xAux = x;
    int yAux = y;
    int par[] = new int[2];
    int cont = 0;
    for (int i = 0; i < ce.x.length; i++) {
        if (x == xAux && y == yAux) {
            par=DobPun(xAux, yAux, a, p);
        } else {
            par=SumPun(x, y, xAux, yAux, p);
        }
        xAux = par[0];
        yAux = par[1];
        for(int j=0;j<ce.x.length;j++){
```

```
            if(xAux==ce.x[j]){
                if(yAux==(int)ce.y1[j]){
//                          System.out.println("Punto encontrado");
                    cont++;
                }else if(yAux==(int)ce.y2[j]){
//                          System.out.println("Punto encontrado");
                    cont++;
                }
            }
        }
    }
    System.out.println("Puntos generados "+cont);
    if (cont == ce.x.length){
        return true;
    }else
    return false;
}
```

Pruebas:

```
Bienvenido al programa para calcular suma de puntos en Curvas Elipticas
Programa hecho por Leizu
--------------------------------------------------------------------------------
Primero ingrese los datos de la curva eliptica a trabajar
Ingrese el valor de a: 1
Ingrese el valor de b: 6
Ingrese el valor de p: 11
-------------------------------------------------
-------------------------------------------------
Puntos de la curva eliptica:
(2,4) (2,7)
(3,5) (3,6)
(5,2) (5,9)
(7,2) (7,9)
(8,3) (8,8)
(10,2) (10,9)
(Punto al Infinito)
Ingresa un punto para determinar si es generador
Ingresa x: 3
Ingresa y: 5
Vamos a doblar el punto
x3= 8 y3= 3
Vamos a sumar los puntos
x3= 5 y3= 9
Vamos a sumar los puntos
x3= 7 y3= 9
Vamos a sumar los puntos
x3= 2 y3= 7
Vamos a sumar los puntos
x3= 10 y3= 9
Vamos a sumar los puntos
x3= 10 y3= 2
Puntos generados 6
es punto generador: true
--------------------------------------------------------------------------------
```

Conclusión:

En conclusión, la suma y el doblado de puntos en curvas elípticas son operaciones fundamentales que desempeñan un papel clave en la criptografía de clave pública y en otros campos de la matemática aplicada. Estas operaciones permiten la creación de sistemas de cifrado asimétricos robustos y eficientes, y también tienen importantes aplicaciones en la geometría algebraica y la teoría de números.

Además, la suma y el doblado de puntos en curvas elípticas tienen propiedades matemáticas interesantes, como la asociatividad y la conmutatividad, lo que las hace útiles en una amplia variedad de aplicaciones. También se ha demostrado que estos algoritmos son computacionalmente difíciles de invertir, lo que los convierte en una herramienta valiosa en la protección de la privacidad y la seguridad de la información.

En resumen, la suma y el doblado de puntos en curvas elípticas son operaciones matemáticas fundamentales con una amplia gama de aplicaciones prácticas. Su estudio y desarrollo continuo seguirá siendo importante en el avance de la criptografía y en otros campos de la matemática aplicada en el futuro.