Instituto Tecnológico de Estudios Superiores de Monterrey, Campus Guadalajara

MA2006B.401

Actividad Residuos Cuadráticos

Uso de álgebras modernas para seguridad y criptografía

Equipo:
Alberto Cortés
Diego Pérez
Luis Ramírez
Mariana Rizo

21 de Marzo del 2022

Problema 1

¿Qué es un residuo cuadrático?

Existen diferentes definiciones para el residuo cuadrático, las cuales son equivalentes cuando se trabaja con un módulo primo:

I. Se le llama residuo cuadrático módulo m a cualquier entero r tal que $mcd(m, r) = 1$, para el que tenga solución la congruencia:
$$x^2 \equiv r \ (mod\ m)$$

II. Se le llama residuo cuadrático módulo m a cualquier entero r, para el que tenga solución la congruencia:

$$x^2 \equiv r \ (mod\ m)$$

Problema 2

Encuentre los residuos cuadráticos de 11,13 y 15.

1. 11

   Tenemos que:

$$1^2 \equiv 10^2 \equiv 1 \ (mod\ 11)$$
$$2^2 \equiv 9^2 \equiv 4 \ (mod\ 11)$$
$$3^2 \equiv 8^2 \equiv 9 \ (mod\ 11)$$
$$4^2 \equiv 7^2 \equiv 5 \ (mod\ 11)$$
$$5^2 \equiv 6^2 \equiv 3 \ (mod\ 11)$$

   Por lo tanto, $1, 3, 4, 5, 9$ son los residuos cuadráticos módulo 11.

2. 13

   Tenemos que:

$$1^2 \equiv 12^2 \equiv 1 \ (mod\ 13)$$
$$2^2 \equiv 11^2 \equiv 4 \ (mod\ 13)$$
$$3^2 \equiv 10^2 \equiv 9 \ (mod\ 13)$$
$$4^2 \equiv 9^2 \equiv 3 \ (mod\ 13)$$
$$5^2 \equiv 8^2 \equiv 12 \ (mod\ 13)$$
$$6^2 \equiv 7^2 \equiv 10 \ (mod\ 13)$$

   Por lo tanto, $1, 3, 4, 9, 10, 12$ son los residuos cuadráticos módulo 13.

3. 15

   Tenemos que:

$$1^2 \equiv 14^2 \equiv 4^2 \equiv 11^2 \equiv 1 \ (mod\ 15)$$
$$2^2 \equiv 13^2 \equiv 7^2 \equiv 8^2 \equiv 4 \ (mod\ 15)$$
$$3^2 \equiv 12^2 \equiv 9 \ (mod\ 15)$$
$$5^2 \equiv 10^2 \equiv 10 \ (mod\ 15)$$
$$6^2 \equiv 9^2 \equiv 6 \ (mod\ 15)$$

   Por lo tanto, $1, 4$ son los residuos cuadráticos módulo 15 de acuerdo con la definición I y $1, 4, 6, 9, 10$ de acuerdo con la definición II.

Problema 3

Investiga 2 métodos diferentes para encontrar el número de puntos en una curva elíptica sobre Fq.

I. Naive Approach
   Este método consiste en recorrer todos los elementos de $\mathbb{F}_q$, revisando cuáles de ellos satisfacen la forma de Weierstrass de un curva elíptica: $y^2 = x^3 + Ax + B$. De hecho, los ejercicios del problema 2 fueron hechos de esta manera.

II. Schoof's Algorithm
   El algoritmo de Schoof fue el primer algoritmo determinístico capaz de calcular la cardinalidad de una curva elíptica en tiempo polinomial, teniendo como herramientas fundamentales la división de polinomios y el teorema de Hasse junto con el teorema del residuo chino.

   El método se aprovecha del hecho de que el teorema de Hasse establece que existe un rango finito de posibles valores para $\mid E(\mathbb{F}_q) \mid$. Entonces es suficiente calcular la cardinalidad de la curva módulo $N > 4\sqrt{q}$. Esto se hace mediante el cálculo de de la cardinalidad módulo algunos primos, los cuales satisfacen que su producto exceda $4\sqrt{q}$ y después usar el teorema del residuo chino.

   La clave para el algoritmo consiste en utilizar un polinomio de división para calcular de manera eficiente la cardinalidad módulo un primo.