UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

Álgebra conmutativa: tarea 1

Fecha de entrega: 8 de febrero, 2023

EJERCICIO 1

Cuando un elemento $d \in \mathbb{F}_p$ es un cuadrado distinto de cero, decimos que d es un residuo cuadrático módulo p. Listar los residuos cuadráticos de $\mathbb{F}_p$ para los siguientes casos $p = 3, 5, 7, 11, 13, 17, 163$.

EJERCICIO 2

Considerar $p \in \mathbb{Z}$ un primo impar y $d \in \mathbb{Z}$ primo relativo con p. Definimos $\left(\frac{d}{p}\right)$, el *símbolo de Legendre* como sigue:

$$\left(\frac{d}{p}\right) = 1 \quad \text{si } d \text{ es residuo cuadrático} \mod p$$

y

$$\left(\frac{d}{p}\right) = -1 \quad \text{si } d \text{ no es residuo cuadrático} \mod p.$$

Para los primos p del ejercicio (1), verificar que el símbolo de Legendre es multiplicativo:

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right),$$

con $a, b \in \mathbb{F}_p$.

TEOREMA DE RECIPROCIDAD CUADRÁTICA[1]

Considerar p, q cualesquiera enteros primos distintos del ejercicio (1). Verificar las igualdades del teorema de reciprocidad cuadrática:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4} \quad \text{ó} \quad \left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$$

donde $\left(\frac{p}{q}\right)$ denota el símbolo de Legendre. El teorema se puede consultar en [1, página 78].

EJERCICIO 4

Asumir el teorema de reciprocidad cuadrática del ejercicio anterior. Mostrar que un primo $p \in \mathbb{Z}$ impar se puede escribir como suma de dos cuadrados

$$p = a^2 + b^2,$$

donde $a, b \in \mathbb{Z}$ si y sólo si $p \equiv 1 (\text{mod } 4)$.

EJERCICIO 5

Asumir el teorema de reciprocidad cuadrática. ¿Cuál de las siguientes ecuaciones es soluble?

1. $x^2 - 5 = 0 \mod 227$
2. $x^2 - 3 = 0 \mod 163$
3. $x^2 - 13 = 0 \mod 7919$

EJERCICIO 6

Asumiendo la propiedad multiplicativa del símbolo de Legendre y el teorema de reciprocidad cuadrática del ejer (3), mostrar que un primo $p \in \mathbb{Z}$ impar se puede descomponer como la suma de un cuadrado y el triple de un cuadrado

$$p = a^2 + 3b^2,$$

con $a, b \in \mathbb{Z}$, si y sólo si $p \equiv 1 \pmod 3$ ó $p = 3$.

REFERENCES

[1] Pierre Samuel: Algebraic Theory of Numbers. Dover 1970.

[1] Este es un teorema famoso atribuido a C.F. Gauss.