UNIVERSIDAD AUTÓNOMA "BENITO JUÁREZ" DE OAXACA

Álgebra moderna III: tarea 1

Fecha de entrega: 1 de septiembre, 2017

EJERCICIO 1

Listar los residuos cuadráticos de $\mathbb{Z}/p\mathbb{Z}$ para los siguientes casos $p = 3, 5, 7, 11, 13, 17, 163$.

LEY DE LOS SIGNOS

- Si a y b son residuos cuadráticos mod p ¿es ab residuo cuadrático mod p?
- Si a y b no son residuos cuadráticos mod p, ¿es ab residuo cuadrático mod p?
- Si a es residuo y b no es residuo cuadrático mod p ¿es ab residuo cuadrático mod p?

EJERCICIO 3

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

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

y

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

Para los primos del ejercicio (1), verificar:

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

Reciprocidad cuadrática[1]

Sea p, q cualesquiera enteros primos distintos del ejercicio (1). Verificar que

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}.$$

La prueba de este teorema se puede consultar en [1, página 78].

Ejercicio 5

Asumir el teorema de reciprocidad cuadrática del ejercicio anterior. Listar qué primos del ejercicio (1) tienen a 3 y -3 como residuo cuadrático.

Ejercicio 6

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. $x^2 - 13 = 0 \mod 67$

References

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

[1] Este es un teorema famoso debido a Gauss.