UNIVERSIDAD AUTÓNOMA "BENITO JUÁREZ" DE OAXACA

Álgebra moderna II: tarea 7

Fecha de entrega: 21 de abril, 2017

EJERCICIO 1

Sea $R = \mathbb{Z}/p\mathbb{Z}$ con p un entero primo. Listar los residuos cuadráticos de R en los casos $p = 3,5,7,11,13,17,19,43,67$. ¿Cómo se distribuyen en el intervalo $[1,p)$? ¿ cuál es la suma de todos ellos?

EJERCICIO 2

Demostrar que -1 es residuo cuadrático mod p si $(p-1)/2$ es par.

EJERCICIO 3

¿Para qué primos del ejercicio (1) es -2 residuo cuadrático mod p?

TEOREMA DE FERMAT (CONTINUACIÓN)

Un entero primo p se puede escribir como

$$p = x^2 + 2y^2$$

con $x, y \in \mathbb{Z}$ si y sólo si -2 es residuo cuadrático mod p y caraterizar los primos con esta propiedad, es decir, caracterizar los enteros primos p, tal que -2 es residuo cuadrático módulo p.

EJERCICIO 5

Si un entero primo p se puede escribir como

$$p = x^2 + qy^2$$

con $x, y \in \mathbb{Z}$, entonces $-q$ es residuo cuadrático mod p. ¿ Es el recíproco cierto para los primos del ejercicio (1)?

EJERCICIO 6

Si $p \in \mathbb{Z}$ primo se puede escribir como

$$p = x^2 + 3y^2$$

con $x, y \in \mathbb{Z}$, entonces $p \equiv 1 \mod 6$. ¿ Es el recíproco cierto para los primos del ejercicio (1)?

EJERCICIO 7

Supongamos que $\mathbb{Z}[\sqrt{-q}]$ es dominio de factorizacón única. Entonces $p \in \mathbb{Z}$ primo se puede escribir como

$$p = x^2 + qy^2$$

con $x, y \in \mathbb{Z}$ si y sólo si $-q$ es residuo cuadrático mod p.