UNIVERSIDAD AUTÓNOMA "BENITO JUÁREZ" DE OAXACA

Teoría de números: tarea 3

Fecha de entrega: 17 de septiembre 2018

TEOREMA DE FERMAT[1]

Todo número primo de la forma $p = 4k + 1$ se puede descomponer como la suma de dos cuadrados

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

de forma única.

EJERCICIO 2

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

EJERCICIO 3

¿Para qué primos del ejercicio anterior la ecuación $x^2 + 2 = 0$ tiene solución en $\mathbb{Z}/p$?

ARGUMENTAR A FAVOR O EN CONTRA

La ecuación $x^2 + 1 = 0$ tiene solución en el campo $\mathbb{Z}/p$ si el número $(p-1)/2$ es par.

[1] Disquisitiones Arithmeticae, pág. 148.

EJERCICIO 5

Sea $p \in \mathbb{Z}$ primo tal que se puede escribir como sigue

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

con $x, y \in \mathbb{Z}$. Mostrar que $p \equiv 1 \pmod 3$.

ARGUMENTAR A FAVOR O EN CONTRA

Todo número primo de la forma $p = 3k + 1$ se puede descomponer, de forma única, como la suma de un cuadrado y el triple de un cuadrado. Es decir,

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