Ayudantía 8

Teoría de Números
Profesor: Yves Martín G.
Ayudante: Valentina Moreno V.

Segundo Semestre 2024

1. Hasta ahora, hemos estudiado como computar una $k-$ésima raíz de b módulo m, pero ¿qué pasaría si b tiene más de una $k-$ésima raíz?

   a) Demuestre que si a es una raíz cuadrada de b módulo m, entonces $-a$ tambien lo es.

   b) Sean a y b enteros tales que satisfacen:

   $$gcd(b, m) = 1$$

   $$gcd(k, \phi(m)) = 1.$$

   Pruebeles que b tiene exactamente una $k-$ésima raíz módulo m.

   c) Haga una conjetura acerca de la cantidad de raíces $k-$ésimas de b si es que

   $$gcd(k, \phi(m)) > 1.$$

2. Pruebe que si m es libre de cuadrados, entonces $x \equiv b^u (mod m)$ siempre es una solución de $x^k \equiv b(mod m)$ (incluso si $gcd(b, m) > 1$. Donde u corresponde a uno de los enteros que satisfacen la ecuación

   $$ku - \phi(m)v = 1.$$

3. Haga una lista de todos los residuos cuadráticos y los no residuos módulo 19.

4. Para cada primo impar p, considere los siguientes números:

   $A =$ suma de todos los $1 \leq a < p$ tal que a es un residuo cuadrático módulo p.

   $B =$ suma de todos los $1 \leq a < p$ tal que a no es es residuo cuadrático módulo p.

   a) Realice un ejemplo módulo 11.

   b) Haga una lista de A y B para todos los primos impares menores a 20.

   c) ¿Que puede conjeturar acerca de $A + B$? Demuestre su conjetura.

5. Un número es llamado un residuo cúbico módulo p si es congruente a un cubo módulo p.

   a) Haga una lista de todos los residuos cúbicos modulo 5, 7 y 11.

   b) conjeture cosas para la próxima ayudantía.