Restos cuadráticos y Símbolo de Legendre

Kenny J. Tinoco

Octubre de 2024

Definición 1 (Símbolo de Legendre)**.** Sea $p > 2$ un primo y a un entero cualquiera, se tiene que

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{si } p \mid q. \\ 1, & \text{si } p \nmid q \text{ y } a \text{ es resto cuadrático en módulo } p. \\ -1, & \text{si } a \text{ no es resto cuadrático en módulo } p. \end{cases}$$

Lema 1 (Propiedades del símbolo de Legendre)**.** El símbolo de Legendre cumple los siguientes resultados.

i) Si $a \equiv b \pmod{p}$, entonces $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

ii) Si $p \nmid a$, entonces $\left(\frac{a^2}{p}\right) = 1$.

iii) Para todos lo enteros a, b se cumple $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

iv) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$, en concreto $\left(\frac{-1}{p}\right) = 1$ si y solo si $p \equiv 1 \pmod{4}$.

Teorema 1 (Ley de reciprocidad cuadrática)**.** Sean p, q dos primos impares, se cumple que

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

Observación 1.

De la ley de reciprocidad cuadrática, obtenemos que

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right), & \text{si } p \text{ ó } q \equiv 1 \pmod{4} \\ -\left(\frac{q}{p}\right), & \text{si } p \equiv q \equiv 3 \pmod{4} \end{cases}$$

Teorema 2 (Criterio de Euler)**.** Sea $p > 2$ un primo y a un entero cualquiera, entonces se cumple

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Teorema 3. Sea $p > 2$ un primo, entonces se cumple que

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Observación 2.

Del teorema anterior, obtenemos que

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & \text{si } p \equiv 1, 7 \pmod{8} \\ -1, & \text{si } p \equiv 3, 5 \pmod{8} \end{cases}$$

Veamos algunos ejercicios.

Ejercicio 1. Determinar los valores de los siguientes símbolos de Legendre.

1. $\left(\frac{44}{103}\right)$
2. $\left(\frac{-60}{1019}\right)$
3. $\left(\frac{2010}{1019}\right)$
4. $\left(\frac{139}{433}\right)$
5. $\left(\frac{523}{1103}\right)$

Ejercicio 2. Resolver las siguientes congruencias.

1. $x^2 \equiv 196 \pmod{1357}$
2. $x^2 + x \equiv 0 \pmod{13}$
3. $x^2 + 3x + 2 \equiv 0 \pmod{7}$
4. $x^2 + 5x + 13 \equiv 0 \pmod{11}$
5. $x^2 - 3x + 2 \equiv 8 \pmod{17}$
6. $25x^2 + 7x \equiv 7 \pmod{17}$
7. $x^2 + x + 7 \equiv 0 \pmod{189}$