3.7.23. *Hallar los primos p para los cuales la ecuación $x^2 \equiv 5 \ (mod \ p)$ tiene solución*

Solución: Usemos la Ley de Reciprocidad Cuadrática:

$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)(-1)^{\frac{4(p-1)}{4}} = \left(\frac{p}{5}\right)(-1)^{p-1} = 1$

Luego tenemos solución si:

- $\left(\frac{p}{5}\right) = (-1)^{p-1} = -1$
- $\left(\frac{p}{5}\right) = (-1)^{p-1} = 1$

Veamos ambos casos:

- En el primer caso, sabiendo que p es primo y par, tenemos que $p = 2$, para el cual la ecuación anterior tiene solución: $x^2 \equiv 5 \ (mod \ p) \Rightarrow x^2 \equiv 1 \ (mod \ p) \Rightarrow x = 1$.
- En el segundo caso, necesitamos que $\left(\frac{p}{5}\right) = 1 \Rightarrow p$ es residuo cuadrático $mod(5) \Rightarrow p \equiv 1 \ (mod \ 5)$ ó $p \equiv 4 \ (mod \ 5)$, ya que 1 y 4 son los residuos cuadráticos de 5.

Luego $x^2 \equiv 5 \ (mod \ p)$ tiene solución si $p = 2$, $p \equiv 1 \ (mod \ 5)$ ó $p \equiv 4 \ (mod \ 5)$.

Problema escrito por Julio Aroca