Pontificia Universidad Católica de Chile
Facultad de Matemáticas
2° semestre 2020

Ayudantía 09

23 de Octubre

MAT2225 - Teoría de Números

1) ¿Es 74 un residuo cuadrático módulo 131?

Solución. Basta calcular $\left(\frac{74}{131}\right)$. Para esto, notar que

$$\left(\frac{74}{131}\right) = \left(\frac{37}{131}\right) \cdot \left(\frac{2}{131}\right)$$

Por reciprocidad cuadrática, tenemos $\left(\frac{37}{131}\right) \cdot \left(\frac{131}{37}\right) = 1$, por lo que $\left(\frac{37}{131}\right) = \left(\frac{131}{37}\right)$. También, $\left(\frac{131}{37}\right) = \left(\frac{20}{37}\right) = \left(\frac{4}{37}\right) \cdot \left(\frac{5}{37}\right)$. Sabemos que $\left(\frac{4}{37}\right) = 1$ (ya que $2^2 = 4$). $\left(\frac{5}{37}\right) \cdot \left(\frac{37}{5}\right) = 1$, por lo que $\left(\frac{5}{37}\right) = \left(\frac{37}{5}\right) = \left(\frac{2}{5}\right) = -1$. Juntando todo, se tiene

$$\begin{aligned}\left(\frac{74}{131}\right) &= \left(\frac{37}{131}\right) \cdot \left(\frac{2}{131}\right) \\ &= \left(\frac{4}{37}\right) \cdot \left(\frac{5}{37}\right) \cdot \left(\frac{2}{131}\right) \\ &= 1 \cdot (-1) \cdot (-1) = 1,\end{aligned}$$

ya que $\left(\frac{2}{131}\right) = (-1)^{(131^2-1)/8}$. Por lo tanto, 74 es un residuo cuadrático módulo 131. ∎

2) ¿Para qué primos $p \geq 5$ se tiene que -3 es un cuadrado módulo p?

Solución. Basta calcular $\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{3}{p}\right)$. Tenemos que $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$. Por reciprocidad cuadrática, $\left(\frac{3}{p}\right) = (-1)^{(p-1)/2} \cdot \left(\frac{p}{3}\right)$. Juntando todo,

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{3}{p}\right) = (-1)^{(p-1)/2} \cdot (-1)^{(p-1)/2} \cdot \left(\frac{p}{3}\right) = \left(\frac{p}{3}\right).$$

Luego, -3 es un cuadrado modulo p ssi p es un cuadrado módulo 3, por lo que funciona para los primos de la forma $3k + 1$. ∎

3) Sea $p \geq 3$ primo. Muestre que

$$\left(\frac{1}{p}\right) + \left(\frac{2}{p}\right) + \ldots + \left(\frac{p-2}{p}\right) + \left(\frac{p-1}{p}\right) = 0$$

Demostración. La suma se puede re-escribir como

$$1 \cdot (\#\text{ residuos}) - 1 \cdot (\#\text{ no-residuos}).$$

Hay $\frac{p-1}{2}$ residuos, por lo que hay $p - 1 - \frac{p-1}{2} = \frac{p-1}{2}$ no-residuos. Reemplazando arriba se tiene que la suma es 0. ∎

4) a) Demuestre que la ecuación $x^2 \equiv_{19} -1$ no tiene soluciones enteras.

Demostración. Supongamos que tiene solución. Luego, $\left(\frac{-1}{19}\right) = 1$. Pero $\left(\frac{-1}{19}\right) = (-1)^{\frac{19-1}{2}} = (-1)^9 = -1$, $\rightarrow\leftarrow$.

Por lo tanto, la ecuación no tiene soluciones enteras. ∎

b) Considere la ecuación $x^2 - dy = -1$. Muestre que si existe un primo tal que $p \equiv_4 3$ y $p \mid d$, entonces la ecuación no tiene soluciones enteras.

Demostración. Supongamos que existe este primo p. Viendo la ecuación módulo p, tenemos $x^2 \equiv_p -1$. Esto pasa ssi $\left(\frac{-1}{p}\right) = 1$. Pero tenemos que

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = (-1)^{\frac{(4k+3)-1}{2}} = (-1)^{2k+1} = -1,$$

$\rightarrow\leftarrow$.

Por lo tanto, si existe un primo cumpliendo las condiciones, la ecuación no tiene soluciones enteras. ∎

c) Muestre que la ecuación $x^2 \equiv -1 \pmod{2450003}$ no tiene soluciones enteras.

Demostración. Lo anterior es equivalente a probar que la ecuación $x^2 - 2450003y = -1$ no tiene solución. Como $2450003 \equiv_4 3$, existe un divisor primo de la forma $4k + 3$, por lo que por parte b) la ecuación no tiene soluciones enteras. ∎