3.7.31. *Demostrar que si* $(x, y) = 1$ *entonces* $x^2 + y^2$ *no es divisible por ningún primo* $p \equiv 3$ *(mód 4).*

Vamos a hacerlo por reducción al absurdo. Por tanto, suponemos que existe un primo $p \equiv 3$ (mód 4) tal que $x^2 + y^2 \equiv 0$ (mód p).

Observemos que $x^2 + y^2 \equiv 0$ (mód p) $\Leftrightarrow x^2 \equiv -y^2$ (mód p)

OBSERVACIÓN: Si $y \equiv 0$ (mód p) $\implies x \equiv 0$ (mód p), y esto no puede ser porque (x, y)=1.

La observación anterior se traduce en que $-y^2$ es un residuo cuadrático módulo p $\implies \left(\frac{-y^2}{p}\right) = 1$ (1)

Desarrollamos el símbolo de Legendre:

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

Como y^2 es un cuadrado, resulta evidente que es un residuo cuadrático módulo p. Además, como sabemos $p \equiv 3$ (mód 4):

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

Pero este hecho entra en contradicción con (1). Como consecuencia, el supuesto era falso, lo que prueba que no existe ningún primo $p \equiv 3$ (mód 4) tal que $x^2 + y^2 \equiv 0$ (mód p).

Problema escrito por Jesús de los Nietos Valle.