Reto 5

Mohamed Khalifi

1. Solución

Las soluciones de la ecuación diofantica:

$$x^4 = y^2 + p$$

Son de la forma

$$\begin{cases} x_1 = \pm\sqrt{(1+p)/2} \\ y_1 = (p-1)/2 \\ \text{o} \\ x_2 = \pm\sqrt{(1+p)/2} \\ y_2 = (1-p)/2 \end{cases}$$

Para algún primo impar p talque

$$p = 2a^2 - 1 \qquad a \in \mathbb{Z} - \{0\}$$

2. Demostración

Para la demostración volvemos a la ecuación (1) y factorizamos

$$x^4 = y^2 + p \iff x^4 - y^2 = p \iff (x^2 - y)(x^2 + y) = p$$

Como p es primo la última igualdad solo se cumple cuando se da alguno de los siguientes casos:

a) $x^2 - y = 1$ y $x^2 + y = p$
b) $x^2 - y = p$ y $x^2 + y = 1$
c) $x^2 - y = -1$ y $x^2 + y = -p$
d) $x^2 - y = -p$ y $x^2 + y = -1$

Descartamos los casos **c** y **d** ya que al resolver ambos sistemas obtenemos $x = \pm\sqrt{-(1+p)/2}$ valores complejos cuando solo estamos interesados en soluciones enteras.

Para el caso **a** resolvemos el sistema:

$$\begin{cases} x^2 - y = 1 \\ x^2 + y = p \end{cases}$$

Y obtenemos el primer par de soluciones:

$$[x_1 = \pm\sqrt{(1+p)/2}\ ;\ y_1 = (p-1)/2] \qquad (1)$$

Como queremos las soluciones enteras tenemos que imponer las siguientes condiciones sobre el primo p

1º $\dfrac{1+p}{2} = a^2 \iff p = 2a^2 - 1 \quad a \in \mathbb{Z} - \{0\}$

2º $\dfrac{1+p}{2} = n \iff p = 2n - 1 \iff p \equiv 1 \mod 2$

En realidad la segunda condición es redundante ya que si 'p' cumple la primera condición es obvio que es impar.

Resolviendo el sistema del caso **b**

$$\begin{cases} x^2 - y = p \\ x^2 + y = 1 \end{cases}$$

Obtenemos el segundo par de soluciones

$$[x_2 = \pm\sqrt{(1+p)/2}\ ;\ y_2 = (1-p)/2] \qquad (2)$$

Para las que tenemos que imponer las mismas condiciones sobre p que en el primer par de soluciones.