Reto 5

Carlos Quesada

1. Solución

La ecuación:

$$x^4 = y^2 + p \qquad \text{con } p \in \mathbb{P} \tag{1}$$

Tiene solución si y sólo si $\frac{p+1}{2}$ es un cuadrado. En ese caso hay 4 soluciones:

$$x = \sqrt{\frac{p+1}{2}} \qquad y = \frac{p-1}{2}$$

$$x = \sqrt{\frac{p+1}{2}} \qquad y = -\frac{p-1}{2}$$

$$x = -\sqrt{\frac{p+1}{2}} \qquad y = \frac{p-1}{2}$$

$$x = -\sqrt{\frac{p+1}{2}} \qquad y = -\frac{p-1}{2}$$

2. Demostración

Demostrarlo no es muy complicado. Tenemos que si x_0 e y_0 son soluciones de la ecuación (1), entonces también han de serlo de la misma ecuación módulo p. Así tenemos:

$$x^4 \equiv y^2 \; mod(p) \Rightarrow x^2 \equiv \pm y \; mod(p)$$

Por tanto sólo soluciones de esta forma podrán ser soluciones de la ecuación original. Pero esto no quiere decir que todas estas soluciones lo sean también en la principal. Veamos cuales de ellas lo son verdaderamente. Llamemos

$a = x^2$, entonces $a = \pm y + k \cdot p$ donde y tiene queser entero. Hagamos primero el caso $y > 0$. Lo dividimos en dos partes, el caso $a = y + k \cdot p$:

$(y + kp)^2 = y^2 + p$
$y^2 + 2ykp + (kp)^2 = y^2 + p$
$2y = \frac{p}{pk} - pk$
Como $2y \in \mathbb{Z}$ y $pk \in \mathbb{Z} \Rightarrow$
$\frac{p}{pk} \in \mathbb{Z} \Rightarrow k = \pm 1$
Además $k = 1$no puede ser ya que daria 'positivo' $= 1 - p \Rightarrow$
$y = \frac{p-1}{2} \Rightarrow$
$x = \pm\sqrt{a} = \pm\sqrt{\frac{p-1}{2} - p} = \pm\sqrt{-\frac{p+1}{2}}$

Este resultado es imposible ya que obtendríamos números complejos. Veamos ahora el resultado tomando $a = -y + kp$:

$(-y + k \cdot p)^2 = y^2 + p$
$y^2 - 2ykp + (kp)^2 = y^2 + p$
$2y = -\frac{p}{pk} + pk$
Como $2y \in \mathbb{Z}$ y $pk \in \mathbb{Z} \Rightarrow$
$\frac{p}{pk} \in \mathbb{Z} \Rightarrow k = \pm 1$
Además $k = -1$no puede ser ya que daria 'positivo' $= 1 - p \Rightarrow$
$y = \frac{-1+p}{2} \Rightarrow$
$x = \pm\sqrt{a} = \pm\sqrt{-\frac{-1+p}{2} + p} = \pm\sqrt{\frac{p+1}{2}}$

Veamoslo ahora para $y < 0$. El razonamiento es el mismo, para el caso $a = -y + k \cdot p$:

$(-y + k \cdot p)^2 = y^2 + p$
$y^2 - 2ykp + (kp)^2 = y^2 + p$
$2y = -\frac{p}{pk} + pk$
Como $2y \in \mathbb{Z}$ y $pk \in \mathbb{Z} \Rightarrow$
$\frac{p}{pk} \in \mathbb{Z} \Rightarrow k = \pm 1$
Además $k = 1$no puede ser ya que daria 'negativo' $= -1 + p \Rightarrow$
$y = \frac{1-p}{2} \Rightarrow$
$x = \pm\sqrt{a} = \pm\sqrt{-\frac{1-p}{2} - p} = \pm\sqrt{-\frac{1+p}{2}}$

Este resultado es imposible ya que obtendríamos números complejos. Veamos ahora el resultado tomando $a = y + kp$:

$(y + kp)^2 = y^2 + p$
$y^2 + 2ykp + (kp)^2 = y^2 + p$
$2y = \frac{p}{pk} - pk$
Como $2y \in \mathbb{Z}$ y $pk \in \mathbb{Z} \Rightarrow$
$\frac{p}{pk} \in \mathbb{Z} \Rightarrow k = \pm 1$
Además $k = -1$no puede ser ya que daria 'negativo' $= -1 + p \Rightarrow$
$y = \frac{1-p}{2} \Rightarrow$
$x = \pm\sqrt{a} = \pm\sqrt{\frac{1-p}{2} + p} = \pm\sqrt{\frac{p+1}{2}}$

Sin embargo nos piden soluciones enteras, así que de entre las soluciones anteriores, sólo valen aquellas en las que x es entero, esto es, cuando $\sqrt{\frac{p+1}{2}}$ es entero. Así tenemos, que solo si $\frac{p+1}{2}$ es un cuadrado hay soluciones enteras para la ecuación y éstas son:

$$x = \sqrt{\frac{p+1}{2}} \qquad y = \frac{p-1}{2}$$

$$x = \sqrt{\frac{p+1}{2}} \qquad y = -\frac{p-1}{2}$$

$$x = -\sqrt{\frac{p+1}{2}} \qquad y = \frac{p-1}{2}$$

$$x = -\sqrt{\frac{p+1}{2}} \qquad y = -\frac{p-1}{2}$$