4.3.11. *Demostrar que la única solución en enteros positivos de la ecuación* $y^2 = x^3 - 1$ *es* $y = 0, x = 1$.

Solución: Antes de empezar probamos lo siguiente:

$$\text{Si } a \in \mathbb{Z}, \text{ entonces } a^2 \equiv 0, 1 \pmod 4. \tag{1}$$

Si $a \in \mathbb{Z}$, se puede expresar en una de las siguientes formas: $4k, 4k+1, 4k+2, 4k+3$, con $k \in \mathbb{Z}$. Entonces,

$$\begin{aligned} a^2 &= (4k)^2 && \equiv 0 \pmod 4 \\ &= (4k+1)^2 && \equiv 1 \pmod 4 \\ &= (4k+2)^2 && \equiv 0 \pmod 4 \\ &= (4k+3)^2 && \equiv 1 \pmod 4 \end{aligned}$$

Empezamos con la prueba: podemos expresar la igualdad de la forma $y^2+1 = x^3$. Como $\mathbb{Z}[i]$ es un dominio de factorización única, podemos expresar esta igualdad de forma única como

$$y^2 + 1 = (y+i) \cdot (y-i) = x^3.$$

Sea γ un factor común de $y+i, y-i$. Como γ ha de ser divisor de la suma $(y+i)+(y-i) = 2i$, $N(\gamma)$ divide a $N(2i) = 4$. Por el otro lado, $N(\gamma)$ divide a $N(y+i) = y^2+1 = x^3$, que es impar (si x fuese par, entonces $x^3 - 1 \equiv 3 \pmod 4$, lo cual es imposible (véase (1)) ya que no existe ningún $y \in \mathbb{Z}$ tal que $y^2 \equiv 3 \pmod 4$). Por tanto, $N(\gamma) = 1$, lo que quiere decir que γ es una unidad. Como $y+i$ e $y-i$ son coprimos, los dos números han de ser de la forma

$$(y+i) = (m+ni)^3, \quad (y-i) = (s+ti)^3$$

para algunos $m, n, s, t \in \mathbb{Z}$. Basta con resolver la primera ecuación. Desarrollando obtenemos

$$\begin{aligned} y + i &= (m+ni)(m^2 + 2nmi - n^2) \\ &= m^3 + 2nm^2 i - mn^2 + m^2 ni - 2n^2 m - n^3 i \\ &= (m^3 - 3n^2 m) + i(3nm^2 - n^3) \\ &= m(m^2 - 3n^2) + i(n(3m^2 - n^2)). \end{aligned}$$

En consecuencia, se han de cumplir la igualdad $1 = n(3m^2 - n^2)$. Si $n = 1$, se tiene que satisfacer $3m^2 - 1 = 1$, pero la igualdad $3m^2 = 2$ no tiene solución en $\mathbb{Z}$. Si $n = -1$, entonces $3m^2 - 1 = -1$, lo cual se cumple para $m = 0$. En consecuencia, $y = 0$, y como $x^3 = y^2 + 1 = 1$, obtenemos que $x = 0$.

Problema escrito por Patrizio Guagliardo