Cuerpos cuadráticos

1 La ecuación $x^2 - Dy^2 = 1$

1.1 Un ejemplo

¿Qué significa resolver la ecuación

$$z^2 = 2 \; ? \tag{1}$$

Desde un punto de vista geométrico, la solución de (1) "es" la longitud de la diagonal de un cuadrado de lados de longitud 1. La ecuación (1) no tiene soluciones racionales. El argumento se puede separar en dos partes. Por un lado, el conjunto

$$\{y \in \mathbb{Z} \, : \, y \geq 0, \, z = x/y \text{ cumple } (1)\}$$

tiene un primer elemento, o bien es vacío. Por otro, si $z = x/y$ cumple (1), entonces, por Factorización única, $2 \mid x$, $4 \mid 2y^2$ y $2 \mid y$, y, así, $z = x'/y'$, con $x' = x/2$ e $y' = y/2$. Pero, entonces, $|y'| < |y|$.

Aunque (1) no tenga soluciones racionales, podemos buscar aproximaciones a una solución. En primer lugar, la resolubilidad de la ecuación (1) con $z \in \mathbb{Q}$, equivale a la resolubilidad de

$$x^2 = 2y^2 \tag{2}$$

con $x, y \in \mathbb{Z}$ ($y \neq 0$). En el plano cartesiano real, (2) describe dos rectas: $x = y\sqrt{2}$ y $x = -y\sqrt{2}$, que se cortan en $(0, 0)$. La ecuación

$$x^2 - 2y^2 = 1 \tag{3}$$

describe una hipérbola que tiene a la recta $x = y\sqrt{2}$ como asíntota. En particular, los pares (x, y) que verifican (3) se pueden interpretar como aproximaciones a $\sqrt{2}$: si $x, y > 0$ son soluciones a (3), entonces

$$(x/y)^2 - 2 = 1/y^2 \; .$$

Así, con $y \to \infty$, el valor $z = x/y$ tiende a $\sqrt{2}$. La ventaja de (3) por sobre (2) es que admite soluciones $x, y \in \mathbb{Z}$.

Una solución a (3) es $(x, y) = (1, 0)$. Otra solución es $(x, y) = (3, 2)$. Toda otra solución se puede "deducir" de esta última. Esto sugiere que debería haber cierta estructura en el conjunto de soluciones a (3) que explique este fenómeno. Se verifica la siguiente identidad:

$$(uU + 2vV)^2 - 2\,(uV + vU)^2 = \left(u^2 - 2v^2\right)\left(U^2 - 2V^2\right) \; , \tag{4}$$

de lo que se deduce que, si (u, v) y (U, V) resuelven (3),[1] entonces podemos construir una nueva solución:

$$(u, v) \cdot (U, V) \;=\; \big(uU + 2vV, uV + vU\big) \;. \tag{5}$$

Es decir, $(x, y) := (u, v) \cdot (U, V)$ también es solución de (3).[2] La operación (5) verifica:

$$\begin{aligned}
(u, v) \cdot (U, V) &= (U, V) \cdot (u, v) \;, \\
(1, 0) \cdot (U, V) &= (U, V) \;, \\
(u, v) \cdot (1, 0) &= (u, v) \;, \\
(x, y) \cdot \big((u, v) \cdot (U, V)\big) &= \big((x, y) \cdot (u, v)\big) \cdot (U, V) \quad \text{y} \\
(3, 2) \cdot (3, -2) &= (1, 0) \;.
\end{aligned}$$

Teorema 1.1. *Sea $(x_1, y_1) = (3, 2)$ y, para $n > 1$, definimos $(x_n, y_n) = (3, 2) \cdot (x_{n-1}, y_{n-1})$.*

(i) Dados enteros $u, v > 0$ tales que $u^2 - 2v^2 = 1$, existe $n \geq 1$ tal que $(u, v) = (x_n, y_n)$.

(ii) La sucesión (x_n, y_n) verifica

$$\begin{bmatrix} x_n \\ y_n \end{bmatrix} \;=\; \begin{bmatrix} 3 & 4 \\ 2 & 3 \end{bmatrix}^n \begin{bmatrix} 1 \\ 0 \end{bmatrix} \;.$$

(iii) La sucesión (x_n, y_n) verifica

$$x_n + y_n\sqrt{2} \;=\; (3 + 2\sqrt{2})^n \;.$$

(iv) Dados enteros $x, y > 0$ tales que $x^2 - 2y^2 = 1$, se cumple

$$\left| \frac{x}{y} \,-\, \sqrt{2} \right| \;<\; \frac{1}{2\sqrt{2}y^2} \;.$$

(v) Dados enteros $x, y > 0$ tales que $|x/y - \sqrt{2}| < 1/2y^2$, se cumple $|x^2 - 2y^2| = 1$. Recíprocamente, si $|x^2 - 2y^2| = 1$, entonces $|x/y - \sqrt{2}| < 1/2y^2$.

Demostración. En cuanto a (i), notamos que no hay soluciones con $v = 1$ y que, con $v = 2$, la solución en enteros positivos es $(3, 2)$. Si (u, v) es solución con $u > 0$ y $v > 2$, entonces

$$(3, -2) \cdot (u, v) \;=\; (3u - 4v, 3v - 2u) \;.$$

Pero,

$$3v - 2u \;=\; \frac{9v^2 - 4u^2}{3v + 2u} \;=\; \frac{v^2 - 4}{3v + 2u}$$

muestra que $0 < 3v - 2u < v$ y $u^2 = 2v^2 + 1$ implica $u > v\sqrt{2}$, con lo que $3u - 4v > (3\sqrt{2} - 4)\, v > 0$. Inductivamente, $(3, -2) \cdot (u, v) = (3, 2)^n$. □

[1] Notar que no estamos diciendo nada acerca de "dónde" pueden tomar valores las incógnitas u, v, U y V.

[2] Además, las coordenadas x, y son funciones bilineales de las coordenadas u, v y U, V.

El ítem Teorema 1.1 (v) sugiere estudiar también la ecuación

$$x^2 - 2y^2 = -1 \ . \tag{6}$$

Se puede ver que $(1, 1)$ es solución de (6).

Teorema 1.2. *Dados enteros $u, v > 0$ tales que $|u^2 - 2v^2| = 1$, existe $n \geq 1$ tal que $(u, v) = (1, 1)^n$.*

Demostración. Se puede comprobar que $(3, 2) = (1, 1)^2$. □