Demostraciones por reducción al absurdo

Se basa en la siguiente equivalencia lógica:

$$[p \Rightarrow q] \Leftrightarrow [p \wedge \neg q \Rightarrow \text{absurdo}]$$

1) Irracionalidad de raíz de 2

Supongamos, por reducción al absurdo, que $\sqrt{2} \in \mathbb{Q}$. Entonces,

$$\sqrt{2} = \frac{p}{q} \text{ con } p, q \in \mathbb{Z} \text{ primos entre sí y } q \neq 0$$

y elevando al cuadrado:

$$2 = \frac{p^2}{q^2} \Rightarrow 2q^2 = p^2$$

La última igualdad nos dice que p^2 es múltiplo de 2 y, por tanto, $p = 2k$ con $k \in \mathbb{Z}$. Sustituyendo, resulta:

$$2q^2 = (2k)^2 \Rightarrow q^2 = 2k^2$$

Es decir, q^2 es múltiplo de 2, y como consecuencia, q también es múltiplo de 2, lo que contradice el hecho de que p y q sean primos entre sí.

2) Infinitud de los números primos

Euclides, proposición 20 del libro IX de los Elementos[1].
Supongamos, por reducción al absurdo, que solo hay un número finito de primos $p_1, p_2, ..., p_n$ y los ordenamos $p_1 < p_2 < ... < p_n$. Consideramos el número natural $N = p_1 \cdot p_2 \cdot ... \cdot p_n + 1$, que puede ser primo o no.
Si es primo, tendríamos un número primo que no está en la lista, lo que constituye una contradicción.
Si N no es primo, entonces tiene que ser divisible por algún número primo. Entonces, para cada primo p_k que divida a N, se tiene que $N = c_k p_k + 1$ con $c_k \geq 1$ y , como consecuencia, el resto de dividir N entre p_k es siempre 1. Por tanto, este primo p_k que divide a N, no puede ser ninguno de la lista de los primos iniciales, lo que también es una contradicción.

3) $\sqrt[n]{2} \in \mathbb{I} \quad \forall n \in \mathbb{N},\ n \geq 3$

Supongamos, por reducción al absurdo, que $\sqrt[n]{2} \in \mathbb{Q}$. Entonces, $\exists p, q \in \mathbb{Z}, q \neq 0,\ \text{m.c.d.}(p, q) = 1$ tales que $\sqrt[n]{2} = \frac{p}{q}$. Elevando a n ambos miembros,

$$2 = \frac{p^n}{q^n}$$

y, por tanto,

[1] Enunciado original (Euclides): *Hay más números primos que cualquier cantidad propuesta de números primos.*

$$2q^n = p^n$$

que se puede reescribir como

$$q^n + q^n = p^n$$

lo que contradice el último teorema de Fermat. Así, $\sqrt[n]{2} \in \mathbb{I}$.

4) Si m y n son números enteros tales que $n + n^2 + n^3 = m + m^2$, entonces n es par

Supongamos, por reducción al absurdo, que n es impar. Entonces, n^2 y n^3 son ambos impares, de donde se deduce que $n + n^2 + n^3$ es impar, ya que es la suma de tres números impares, y como consecuencia $m + m^2$ es impar (ya que $n + n^2 + n^3 = m + m^2$).
Sin embargo, $m + m^2$ es siempre par, ya que $m + m^2 = m(m+1)$ y necesariamente alguno de los números m o $m+1$ es par, y por tanto, hemos llegado a una contradicción.

5) $\lim_{n\to\infty} x^n = +\infty$ si $x > 1$

Para demostrar que la sucesión $\{x^n\}$, que es creciente, no está acotada, vamos a suponer, por reducción al absurdo, que $\{x^n\}$ está acotada. Así,

$$\{x^n\} \to \sup\{x^n\} := \alpha$$

y, por tanto,

$$x^{n+1} \le \alpha \quad \forall n \in \mathbb{N}$$

lo que implica que

$$x^n \le \frac{\alpha}{x} < \alpha \quad \forall n \in \mathbb{N}$$

y esto, contradice el hecho de que α sea el supremo.

6) $\log 2 \in \mathbb{I}$

Supongamos que $\log 2 = \frac{m}{n}$ con $m, n \in \mathbb{N}$ y m.c.d.$(m,n) = 1$. Entonces, tomando exponenciales de base e, se tiene que $2 = e^{\frac{m}{n}}$ y, por tanto, que $e = 2^{\frac{m}{n}}$. Ahora bien, eso quiere decir que e es solución de la ecuación polinómica $x^m - 2^n = 0$, lo que es una contradicción, ya que sabemos que el número e es trascendente y, por tanto, no es solución de ninguna ecuación polinómica con coeficientes enteros.

7) Sean $a, b \in \mathbb{N}$ tales que $\nexists m, n \in \mathbb{N}$ que cumplan que $a^m = b^n$. Entonces, $\log_b a \in \mathbb{I}$

Supongamos que $\log_b a = \frac{p}{q}$ con $p, q \in \mathbb{N}$ y tales que $m.c.d.(p,q) = 1$. Entonces,

$$b^{\frac{p}{q}} = a \Rightarrow \sqrt[q]{b^p} = a \Rightarrow b^p = a^q$$

lo que contradice la hipótesis del enunciado.

8) Sea p un número primo. Entonces, $\sqrt{p} \in \mathbb{I}$

Supongamos que $\sqrt{p} = \frac{a}{b}$ con $a, b \in \mathbb{Z}, b \neq 0$ y m.c.d.$(a,b) = 1$. Entonces,

$$p = \frac{a^2}{b^2} \Rightarrow b^2 p = a^2 \qquad [1]$$

esto es, a^2 es múltiplo de p y, por tanto, a también es múltiplo de p.
Por el teorema fundamental de la Aritmética $a = p_1 \cdot ... \cdot p_n$ con p_i primo, luego

$$a^2 = p_1 \cdot ... \cdot p_n \cdot p_1 \cdot ... \cdot p_n = p_1^{\,2} \cdot ... \cdot p_n^{\,2}$$

y como p es un factor de a^2, supongamos que $p = p_1$. Entonces

$$a^2 = p^2 \cdot p_2^{\,2} \cdot ... \cdot p_n^{\,2}$$

Ahora bien, hemos visto que a es múltiplo de p, luego $a = kp$ con $k \in \mathbb{Z}$ y sustituyendo en [1]

$$b^2 p = (kp)^2 \Rightarrow b^2 p = k^2 p^2 \Rightarrow b^2 = k^2 p$$

Esto es, b^2 es múltiplo de p y, por tanto, b también es múltiplo de p !!, ya que entonces p sería un múltiplo común de a y de b.