Introducción

En la clase de hoy, empezaremos viendo otro ejemplo de una demostración de la equivalencia de tres proposiciones matemáticas.

A continuación, introduciremos los conceptos de teorema, lema, corolario y axioma.

Por último, trataremos las demostraciones de existencia y unicidad, que aparecen frecuentemente en Matemáticas.

Empezamos recordando el método "circular" que vimos al final de la última clase para demostrar que varias proposiciones matemáticas son equivalentes.

Demostración de la equivalencia de varias proposiciones

En ocasiones, queremos demostrar que tres o más proposiciones matemáticas son equivalentes. Entonces, para demostrar que n proposiciones $P_1,\ldots,P_n$ donde $n \geq 3$ son equivalentes se demuestra lo siguiente:

$P_1 \Rightarrow P_2$,

$P_2 \Rightarrow P_3$,

$\vdots$

$\vdots$

$P_{n-1} \Rightarrow P_n$,

$P_n \Rightarrow P_1$.

Es decir, se hace una demostración "circular" de la equivalencia de las n proposiciones.

Ejemplo

Proposición 1

Sean $m, n \in \mathbb{Z}$. Entonces, son equivalentes las siguientes condiciones:

(1) n y m son pares o n y m son impares.

(2) $n + m$ es par

(3) $n - m$ es par.

Demostración de la Proposición 1

Supongamos que $m, n \in \mathbb{Z}$. Tenemos que demostrar que $(1) \Rightarrow (2)$, $(2) \Rightarrow (3)$ y $(3) \Rightarrow (1)$.

En primer lugar, demostramos que $(1) \Rightarrow (2)$. Supongamos que o bien n y m son pares o bien n y m son impares.

Caso 1. n y m son pares.

Entonces, existen $k, l \in \mathbb{Z}$ tales que $n = 2k$ y $m = 2l$. Por tanto,

$$n + m = 2k + 2l = 2(k + l).$$

Entonces, como $k + l \in \mathbb{Z}$, tenemos que $n + m$ es par.

Demostración de la Proposición 1

Caso 2. n y m son impares.

Entonces, existen $k, l \in \mathbb{Z}$ tales que $n = 2k + 1$ y $m = 2l + 1$. Por tanto,

$$n + m = 2k + 2l + 2 = 2(k + l + 1).$$

Entonces, como $k + l + 1 \in \mathbb{Z}$, tenemos que $n + m$ es par.

A continuación, demostramos que $(2) \Rightarrow (3)$. Supongamos que $n + m$ es par. Existe entonces $k \in \mathbb{Z}$ tal que $n + m = 2k$. Por tanto,

$$n - m = n + m - 2m = 2k - 2m = 2(k - m).$$

Por tanto, $n - m$ es par.

Demostración de la Proposición 1

Por último, demostramos que $(3) \Rightarrow (1)$. Supongamos que $n - m$ es par. Entonces, existe un $k \in \mathbb{Z}$ tal que $n - m = 2k$.
Distinguimos entonces los siguientes casos:

Caso 1. n es par.

Sea $l \in \mathbb{Z}$ tal que $n = 2l$. Por tanto:

$$m = n - (n - m) = 2l - 2k = 2(l - k).$$

Por consiguiente, m es par. En consecuencia, m y n son pares, y por tanto se cumple (1).

Demostración de la Proposición 1

Caso 2. n es impar

Sea $l \in \mathbb{Z}$ tal que $n = 2l + 1$. Por tanto:

$$m = n - (n - m) = 2l + 1 - 2k = 2(l - k) + 1.$$

Por consiguiente, m es impar. En consecuencia, m y n son impares, y por tanto si cumple (1). $\square$

Teoremas, lemas, corolarios y axiomas

A las proposiciones verdaderas que son relevantes en Matemáticas se les llama teoremas. El término "teorema" se reserva para los resultados matemáticos de mayor interés.

Un lema es un resultado auxiliar en el proceso de una demostración de un teorema o de una proposición. Hay ocasiones en las que la demostración de un teorema es muy extensa, en cuyo caso es conveniente dividir dicha demostración en una serie de lemas.

Un corolario es una proposición que se deduce con facilidad de un teorema. En muchas ocasiones, los corolarios son casos particulares importantes de los teoremas.

Por último, un axioma es una proposición verdadera evidente, que se considera que no necesita demostración. Un ejemplo de un axioma es la proposición "por dos puntos distintos del plano pasa exactamente una recta".

Un teorema sobre números primos

Recordemos que un número natural n es primo, si tiene exactamente dos divisores.

Teorema 1

Sea n un número natural mayor que 1. Si $2^n - 1$ es primo, entonces n es primo.

Para demostrar este teorema, utilizaremos el siguiente lema:

Lema 1

Si a es un número real y x es un número natural no nulo, entonces

$$a^x - 1 = (a-1)(a^{x-1} + a^{x-2} + \cdots + a + 1).$$

Demostración del Lema 1

Tenemos que

$$(a-1)(a^{x-1}+a^{x-2}+\cdots+a+1)=$$
$$a\cdot(a^{x-1}+a^{x-2}+\cdots+a+1)-(a^{x-1}+a^{x-2}+\cdots+a+1)=$$
$$a^x+a^{x-1}+a^{x-2}\cdots+a-a^{x-1}-a^{x-2}-\cdots-a-1=a^x-1.\ \square$$

Demostración del Teorema 1

Demostramos el Teorema 1 por el contrarrecíproco. Es decir, vamos a demostrar que

$$n \text{ no es primo } \Rightarrow 2^n - 1 \text{ no es primo.}$$

Supongamos entonces que n no es primo. Por tanto, existen números naturales p y q tales que $p, q > 1$ y $p, q < n$ de manera que $n = p \cdot q$. Tenemos entonces que

$$2^n - 1 = 2^{p \cdot q} - 1 = (2^p)^q - 1.$$

Aplicamos ahora el Lema 1, tomando $a = 2^p$ y $x = q$. Obtenemos entonces:

Demostración del Teorema 1

$2^n - 1 = (2^p)^q - 1 = a^q - 1 = (a-1)(a^{q-1} + a^{q-2} + \cdots + a + 1) = (2^p - 1)((2^p)^{q-1} + (2^p)^{q-2} + \cdots + 2^p + 1)$.

Ahora, nos fijamos en el factor $2^p - 1$ de la expresión anterior.. Por un lado, como tenemos que $n = p \cdot q$ y $q > 1$, deducimos que $p < n$, y por tanto $2^p < 2^n$, y por consiguiente $2^p - 1 < 2^n - 1$.

Por otra parte, como $p > 1$, inferimos que $3 < 2^p$, y por tanto $1 < 2^p - 1$.

Así pues, hemos demostrado que $1 < 2^p - 1 < 2^n - 1$. Entonces, como $2^p - 1$ es un divisor de $2^n - 1$, deducimos que $2^n - 1$ no es primo. $\square$

Demostraciones de existencia y unicidad

En muchas ocasiones queremos demostrar proposiciones del tipo "existe un único elemento de un dominio D que satisface una propiedad $P(x)$", lo cual formalmente se escribe como $\exists! x \in D P(x)$. Obsérvese que esta última expresión la podemos escribir como:

$$(\exists x \in D P(x)) \wedge (\forall x \in D \forall y \in D (P(x) \wedge P(y) \rightarrow x = y)).$$

Para demostrar la existencia, tenemos que encontrar un elemento del dominio que estemos considerando que satisfaga la propiedad. Y para demostrar la unicidad, o bien demostramos de manera directa que si tenemos dos elementos que cumplen la propiedad, entonces esos dos elementos han de ser iguales; o bien procedemos por reducción al absurdo, suponiendo que existen dos elementos distintos que cumplen la propiedad, y entonces llegamos a una contradicción.

Ejemplos

Proposición 2

La ecuación $x^2 - 1 = 0$ tiene una única solución entera positiva.

Demostración de la existencia. Tomemos $x = 1$. Como $1 \in \mathbb{Z}$, $1 > 0$ y $1^2 - 1 = 0$, queda demostrada la existencia.

Demostración de la unicidad. Sean $m, n \in \mathbb{Z}$ tales que $m, n > 0$. Supongamos que $m^2 - 1 = 0$ y $n^2 - 1 = 0$. Entonces, $m^2 - 1 = n^2 - 1$. Por tanto, $m^2 = n^2$. Como $m^2 = n^2$, deducimos que $m = n$ o $m = -n$. El caso $m = -n$ es imposible, ya que m y n son números positivos. Por tanto, $m = n$. Así pues, hemos demostrado la unicidad.$\square$

Ejemplos

Proposición 3

La ecuación $27x^3 - 8 = 0$ tiene una única solución en los números reales.

En este caso, podemos demostrar la existencia y unicidad de la siguiente manera. Sea a un número real arbitrario. Tenemos entonces:

$$27a^3 - 8 = 0 \Leftrightarrow 27a^3 = 8 \Leftrightarrow a^3 = \frac{8}{27} \Leftrightarrow a = \frac{2}{3}.$$

Por tanto:

$$27a^3 - 8 = 0 \Leftrightarrow a = \frac{2}{3}.$$

Obsérvese que la implicación de derecha a izquierda demuestra la existencia, y la implicación de izquierda a derecha demuestra la unicidad. $\square$

Ejemplos

Proposición 4

Existe una única solución de la ecuación $x^2 + y^2 = z^2$ en enteros positivos consecutivos.

Demostración de la existencia. Tomemos $x = 3$, $y = 4$ y $z = 5$ Claramente, se tiene que $3^2 + 4^2 = 5^2$.

Demostración de la unicidad. Tenemos que demostrar que la única solución de la ecuación $x^2 + y^2 = z^2$ en enteros positivos consecutivos es $x = 3$, $y = 4$ y $z = 5$. Sean x, y, z tres números enteros positivos consecutivos que satisfacen la ecuación $x^2 + y^2 = z^2$. Como x, y, z son enteros positivos consecutivos, existe un número natural $n > 1$ tal que $x = n - 1$, $y = n$ y $z = n + 1$. Así pues, tenemos que

$$(n-1)^2 + n^2 = (n+1)^2.$$

Ejemplos

Por tanto,

$$n^2 - 2n + 1 + n^2 = n^2 + 2n + 1.$$

Luego,

$$n^2 - 4n = 0.$$

Así pues,

$$n(n-4) = 0.$$

Entonces, la única solución de $n(n-4) = 0$ con $n > 1$ es $n = 4$.

Por tanto, tenemos que $x = n - 1 = 3$, $y = n = 4$ y $z = n + 1 = 5$. $\square$

Ejemplos

Teorema del Algoritmo de la División

Sean $a, b \in \mathbb{N}$ tales que $b > 0$. Entonces, existen números naturales q y r tales que $a = b \cdot q + r$ y de manera que $0 \leq r < b$. Además, q y r son únicos.

Demostración de la existencia. Sea bq el mayor múltiplo de b que es menor o igual que a. Entonces,

$$bq \leq a < b(q+1).$$

Sea $r = a - bq$. Como $bq \leq a$, deducimos que $r \geq 0$. Por otra parte, tenemos:

$$r = a - bq < b(q+1) - bq = b.$$

Por tanto, $r < b$. Y como antes hemos demostrado que $r \geq 0$, tenemos que $0 \leq r < b$.
Por otra parte, como tenemos que $r = a - bq$, deducimos que $a = bq + r$. Así pues, queda demostrada la existencia.

Demostración de la Unicidad

Para demostrar la unicidad, procedemos por reducción al absurdo. Supongamos entonces que existen $r_1, q_1, r_2, q_2 \in \mathbb{N}$ tales que se cumplen las siguientes condiciones:

(1) $a = bq_1 + r_1 = bq_2 + r_2$.

(2) $0 \leq r_1 < b$ y $0 \leq r_2 < b$.

(3) $r_1 \neq r_2$.

Obsérvese que, como $bq_1 + r_1 = bq_2 + r_2$, tenemos que $r_1 - r_2 = b(q_2 - q_1)$. Vamos a demostrar que $b \leq |r_1 - r_2|$. Para ello, consideramos los siguientes dos casos:

Demostración de la Unicidad

Caso 1. $r_2 < r_1$.

Como $b(q_2 - q_1) = r_1 - r_2$, $b > 0$ y $r_1 - r_2 > 0$, deducimos que $q_2 - q_1 > 0$. Por tanto, b es un divisor de $r_1 - r_2$. Así pues, $b \leq r_1 - r_2 = |r_1 - r_2|$.

Caso 2. $r_1 < r_2$.

Obsérvese que como $b(q_2 - q_1) = r_1 - r_2$, $b > 0$ y $r_1 - r_2 < 0$, tenemos que $q_2 - q_1 < 0$. Entonces como $b(q_2 - q_1) = r_1 - r_2$, deducimos que $b(q_1 - q_2) = r_2 - r_1$. Por tanto, b es un divisor de $r_2 - r_1$. Así pues, $b \leq r_2 - r_1 = |r_1 - r_2|$.

Así pues, hemos demostrado por casos que $b \leq |r_1 - r_2|$.

Demostración de la Unicidad

Sin embargo, como tenemos que $0 \leq r_1 < b$ y $0 \leq r_2 < b$, podemos deducir que $|r_1 - r_2| < b$ considerando otra vez los dos casos de antes:

Caso 1. $r_2 < r_1$.

Tenemos que $|r_1 - r_2| = r_1 - r_2$. Entonces, como $r_1 < b$ y $r_2 \geq 0$, deducimos que $|r_1 - r_2| = r_1 - r_2 < b$.

Caso 2. $r_1 < r_2$.

Tenemos que $|r_1 - r_2| = r_2 - r_1$. Entonces, como $r_2 < b$ y $r_1 \geq 0$, deducimos que $|r_1 - r_2| = r_2 - r_1 < b$.

Así pues, hemos demostrado por casos que $|r_1 - r_2| < b$.

Entonces, hemos demostrado que $b \leq |r_1 - r_2|$ y que $|r_1 - r_2| < b$, y por tanto hemos llegado a una contradicción. $\square$