Métodos de demostración

Clase 08

IIC 1253

Prof. Pedro Bahamondes

Outline

Métodos de demostración

Epílogo

Definición

Una demostración es un argumento válido para establecer la verdad de una afirmación matemática.

¿Qué tipos de afirmaciones matemáticas conocemos?

- Definición
- Axioma
- Teorema
- Proposición
- Lema
- Corolario
- Conjetura
- Problema abierto

Definición

Una **afirmación matemática** es una sentencia sobre objetos matemáticos que puede ser verdadera o falsa.

Definición

Una afirmación matemática es una sentencia sobre objetos matemáticos que puede ser verdadera o falsa.

Observación

Todo predicado o fórmula es una afirmación matemática.

Definición

Una afirmación matemática es una sentencia sobre objetos matemáticos que puede ser verdadera o falsa.

Observación

Todo predicado o fórmula es una afirmación matemática.

Ejemplos

- Todo número natural cumple que si es par, entonces su sucesor es impar.
- Existe un número natural tal que todo número es mayor a él.

Axiomas

Definición

Un **axioma** es una afirmación matemática que se considera evidente y se acepta sin requerir demostración previa.

¿Qué axiomas conocemos?

Axiomas

Axiomatización de Peano

```
■ 0 ∈ N

■ \forall x(x = x)

■ \forall x \forall y(x = y \rightarrow y = x)

■ \forall x \forall y \forall z(x = y \land y = z \rightarrow x = z)

■ \forall x \forall y(x = y \land y \in \mathbb{N} \rightarrow x \in \mathbb{N})

■ \forall x(x \in \mathbb{N} \rightarrow S(x) \in \mathbb{N})

■ \forall x \forall y(x = y \leftrightarrow S(x) = S(y))

■ \neg (\exists x(S(x) = 0))
```

Definición

Un teorema es una afirmación matemática verdadera y demostrable.

Definición

Un teorema es una afirmación matemática verdadera y demostrable.

Ejemplos

- Teorema de Pitágoras.
- Teorema fundamental del álgebra.
- Teorema de los 4 colores.
- Teoremas de incompletitud de Gödel.

Definición

Un lema es un resultado menor cuyo fin es ayudar en la demostración de un teorema.

Definición

Un lema es un resultado menor cuyo fin es ayudar en la demostración de un teorema.

Definición

Una **proposición** es un resultado interesante, pero de menor importancia que un teorema.

Definición

Un lema es un resultado menor cuyo fin es ayudar en la demostración de un teorema.

Definición

Una **proposición** es un resultado interesante, pero de menor importancia que un teorema.

Definición

Un corolario es una afirmación matemática cuya demostración se deriva casi directamente de un teorema.

Conjeturas

Definición

Una conjetura es una afirmación matemática que se cree que es verdad pero ${\bf NO}$ se ha demostrado.

Conjeturas

Definición

Una conjetura es una afirmación matemática que se cree que es verdad pero **NO** se ha demostrado.

Ejemplo

"Todo número par mayor a 2 puede ser expresado como suma de dos primos"

Conjetura de Goldbach

Conjeturas

Definición

Una conjetura es una afirmación matemática que se cree que es verdad pero **NO** se ha demostrado.

Ejemplo

"Todo número par mayor a 2 puede ser expresado como suma de dos primos"

Conjetura de Goldbach

$$\forall x \forall y \forall z \forall n (n > 2 \rightarrow x^n + y^n \neq z^n)$$

(ex) Conjetura de Fermat

Problemas abiertos

Definición

Un **problema abierto** es una afirmación matemática la cual no se sabe si es verdadera o falsa, y para la cual todavía no se conoce una solución o demostración.

Problemas abiertos

Definición

Un **problema abierto** es una afirmación matemática la cual no se sabe si es verdadera o falsa, y para la cual todavía no se conoce una solución o demostración.

¿Cuál es el problema abierto más importante en ciencia de la computación?

$$\mathsf{P} = \mathsf{NP}$$

¿Cuál es el problema abierto más importante en ciencia de la computación?

$$P \stackrel{?}{=} NP$$

"If the solution to a problem can be quickly verified by a computer, can the computer also solve that problem quickly?"

Wikipedia

.

Definición

Una demostración es un argumento válido para establecer la verdad de una afirmación matemática.

Definición

Una demostración es un argumento válido para establecer la verdad de una afirmación matemática.

Un argumento válido es una secuencia de argumentos que puede estar compuesta por:

- Axiomas
- Hipótesis (si existen)
- Afirmaciones previamente demostradas

Cada argumento en la secuencia de argumentos está conectado con el anterior por una regla de inferencia. El último paso de la secuencia establece la verdad de la afirmación.

Definición

Una demostración es un argumento válido para establecer la verdad de una afirmación matemática.

Un argumento válido es una secuencia de argumentos que puede estar compuesta por:

- Axiomas
- Hipótesis (si existen)
- Afirmaciones previamente demostradas

Cada argumento en la secuencia de argumentos está conectado con el anterior por una regla de inferencia. El último paso de la secuencia establece la verdad de la afirmación.

Se parece a algo que ya vimos, ¿no?

- Una secuencia de símbolos
- Una secuencia disconexa de argumentos

- Una secuencia de símbolos
- Una secuencia disconexa de argumentos

IMPORTANTE

La secuencia de argumentos debe ser lo más clara, precisa y completa posible. La demostración debe convencer al lector u oyente sin dejarle ninguna duda sobre la correctitud de la demostración.

- Experiencia
- Intuición
- Creatividad
- Perseverancia

- Experiencia
- Intuición
- Creatividad
- Perseverancia
- Métodos de demostración

- Experiencia
- Intuición
- Creatividad
- Perseverancia
- Métodos de demostración

Supongamos que tenemos una afirmación como la siguiente:

$$\forall x (P(x) \rightarrow Q(x))$$

¿Qué métodos de demostración podemos ocupar?

Métodos de demostración

$$\forall x (P(x) \rightarrow Q(x))$$

- Directa
- Contrapositivo
- Contradicción
- Por análisis de casos
- Otros tipos de demostración

También se conoce del latin *modus ponendo ponens* ("la forma en que se afirma afirmando").

También se conoce del latin *modus ponendo ponens* ("la forma en que se afirma afirmando"). Por demostrar:

$$\forall x (P(x) \to Q(x))$$

Método directo

Suponemos que P(n) es verdadero para un n arbitrario y demostramos que Q(n) también es verdadero.

También se conoce del latin *modus ponendo ponens* ("la forma en que se afirma afirmando"). Por demostrar:

$$\forall x (P(x) \rightarrow Q(x))$$

Método directo

Suponemos que P(n) es verdadero para un n arbitrario y demostramos que Q(n) también es verdadero.

Ejercicio

Un entero $n \in \mathbb{Z}$ se dice un **cuadrado perfecto** si existe un $k \in \mathbb{Z}$ tal que $n = k^2$. Demuestre que si n y m son cuadrados perfectos, entonces $n \cdot m$ también lo es.

También se conoce del latin *modus ponendo ponens* ("la forma en que se afirma afirmando"). Por demostrar:

$$\forall x (P(x) \rightarrow Q(x))$$

Método directo

Suponemos que P(n) es verdadero para un n arbitrario y demostramos que Q(n) también es verdadero.

Ejercicio

Un entero $n \in \mathbb{Z}$ se dice un **cuadrado perfecto** si existe un $k \in \mathbb{Z}$ tal que $n = k^2$. Demuestre que si n y m son cuadrados perfectos, entonces $n \cdot m$ también lo es

Ejercicio

Sea $n \in \mathbb{N}$. Demuestre que si n es impar, entonces n^2 es impar.

También se conoce del latin *modus tollendo tollens* ("el camino que niega al negar").

También se conoce del latin *modus tollendo tollens* ("el camino que niega al negar").Por demostrar:

$$\forall x (P(x) \rightarrow Q(x))$$

Método por contrapositivo

Suponemos que Q(n) es falso para un n arbitrario y demostramos que P(n) también es falso.

También se conoce del latin *modus tollendo tollens* ("el camino que niega al negar").Por demostrar:

$$\forall x (P(x) \rightarrow Q(x))$$

Método por contrapositivo

Suponemos que Q(n) es falso para un n arbitrario y demostramos que P(n) también es falso.

Ejercicio

Sea $n \in \mathbb{N}$. Demuestre que si 3n + 2 es impar, entonces n es impar.

También se conoce del latin *modus tollendo tollens* ("el camino que niega al negar").Por demostrar:

$$\forall x (P(x) \rightarrow Q(x))$$

Método por contrapositivo

Suponemos que Q(n) es falso para un n arbitrario y demostramos que P(n) también es falso.

Ejercicio

Sea $n \in \mathbb{N}$. Demuestre que si 3n + 2 es impar, entonces n es impar.

Ejercicio

Sea $a, b \in \mathbb{Z}^+$. Demuestre que si $n = a \cdot b$ entonces $a \le \sqrt{n}$ o $b \le \sqrt{n}$.

"Reductio ad absurdum, which Euclid loved so much, is one of a mathematician's finest weapons. It is a far finer gambit than any chess play: a chess player may offer the sacrifice of a pawn or even a piece, but a mathematician offers the game."

A mathematician's apology (G. H. Hardy).

Por demostrar:

$$\forall x (P(x) \rightarrow Q(x))$$

Método por contradicción

Suponemos que existe un n tal que P(n) es verdadero y Q(n) es falso e inferimos una contradicción.

¿A qué se parece?

Por demostrar:

$$\forall x (P(x) \rightarrow Q(x))$$

Método por contradicción

Suponemos que existe un n tal que P(n) es verdadero y Q(n) es falso e inferimos una contradicción.

¿A qué se parece?

Ejercicio

Demuestre que $\sqrt{2}$ es irracional.

Ejercicio

Demuestre que $\sqrt{2}$ es irracional.

Por contradicción suponemos que $\sqrt{2}$ es racional, por lo que puede escribirse de la forma $\sqrt{2} = \frac{a}{b}$ con $a, b \in \mathbb{Z}$ sin factores en común y $b \neq 0$.

Ejercicio

Demuestre que $\sqrt{2}$ es irracional.

Por contradicción suponemos que $\sqrt{2}$ es racional, por lo que puede escribirse de la forma $\sqrt{2} = \frac{a}{b}$ con $a,b \in \mathbb{Z}$ sin factores en común y $b \neq 0$. Notemos que al no tener factores en común, no pueden ser ambos pares.

Ejercicio

Demuestre que $\sqrt{2}$ es irracional.

Por contradicción suponemos que $\sqrt{2}$ es racional, por lo que puede escribirse de la forma $\sqrt{2}=\frac{a}{b}$ con $a,b\in\mathbb{Z}$ sin factores en común y $b\neq 0$. Notemos que al no tener factores en común, no pueden ser ambos pares. Desarrollando la igualdad:

$$\sqrt{2} = \frac{a}{b}$$

$$2 = \frac{a^2}{b^2}$$
 (Elevamos al cuadrado)
$$a^2 = 2b^2$$

Ejercicio

Demuestre que $\sqrt{2}$ es irracional.

Por contradicción suponemos que $\sqrt{2}$ es racional, por lo que puede escribirse de la forma $\sqrt{2}=\frac{a}{b}$ con $a,b\in\mathbb{Z}$ sin factores en común y $b\neq 0$. Notemos que al no tener factores en común, no pueden ser ambos pares. Desarrollando la igualdad:

$$\sqrt{2} = \frac{a}{b}$$

$$2 = \frac{a^2}{b^2}$$
(Elevamos al cuadrado)
$$a^2 = 2b^2$$

Entonces, a^2 es par y por lo tanto (\bigstar) a también es par: a = 2k.

Ejercicio

Demuestre que $\sqrt{2}$ es irracional.

Entonces, a^2 es par y por teorema anterior a también es par: a = 2k.

Ejercicio

Demuestre que $\sqrt{2}$ es irracional.

Entonces, a^2 es par y por teorema anterior a también es par: a = 2k. Reemplazando en la igualdad anterior:

$$a^{2} = 2b^{2}$$
$$(2k)^{2} = 2b^{2}$$
$$4k^{2} = 2b^{2}$$
$$b^{2} = 2k^{2}$$

Entonces, b^2 es par.

Ejercicio

Demuestre que $\sqrt{2}$ es irracional.

Entonces, a^2 es par y por teorema anterior a también es par: a = 2k. Reemplazando en la igualdad anterior:

$$a^{2} = 2b^{2}$$
$$(2k)^{2} = 2b^{2}$$
$$4k^{2} = 2b^{2}$$
$$b^{2} = 2k^{2}$$

Entonces, b^2 es par. Por teorema anterior b también es par. Esto es una contradicción, ya que entre a y b alguno debe ser un número impar.

Ejercicio

Demuestre que $\sqrt{2}$ es irracional.

Entonces, a^2 es par y por teorema anterior a también es par: a = 2k. Reemplazando en la igualdad anterior:

$$a^{2} = 2b^{2}$$
$$(2k)^{2} = 2b^{2}$$
$$4k^{2} = 2b^{2}$$
$$b^{2} = 2k^{2}$$

Entonces, b^2 es par.Por teorema anterior b también es par. Esto es una contradicción, ya que entre a y b alguno debe ser un número impar. Concluimos entonces que $\sqrt{2}$ no puede ser racional y por lo tanto es irracional.

Por demostrar:

$$\forall x (P(x) \rightarrow Q(x))$$

Método por contradicción

Suponemos que existe un n tal que P(n) es verdadero y Q(n) es falso e inferimos una contradicción.

¿A qué se parece?

Ejercicio

Demuestre que $\sqrt{2}$ es irracional.

Ejercicio

Demuestre que existe una cantidad infinita de números primos.

Por demostrar:

$$\forall x (P(x) \to Q(x))$$

Por demostrar:

$$\forall x (P(x) \rightarrow Q(x))$$

Dividimos el dominio de la interpretación \mathcal{I} con que trabajamos en una cantidad finita de casos $C_1,...,C_n$, tal que:

$$\mathcal{I}(dom) = \bigcup_{i=1}^n C_i$$

Por demostrar:

$$\forall x (P(x) \rightarrow Q(x))$$

Dividimos el dominio de la interpretación \mathcal{I} con que trabajamos en una cantidad finita de casos $C_1, ..., C_n$, tal que:

$$\mathcal{I}(dom) = \bigcup_{i=1}^n C_i$$

Método por casos

Para cada subdominio C_1, \ldots, C_n demostramos que:

$$\forall x (P(x) \to Q(x))$$

Por demostrar:

$$\forall x (P(x) \rightarrow Q(x))$$

Dividimos el dominio de la interpretación \mathcal{I} con que trabajamos en una cantidad finita de casos $C_1, ..., C_n$, tal que:

$$\mathcal{I}(dom) = \bigcup_{i=1}^n C_i$$

Método por casos

Para cada subdominio C_1, \ldots, C_n demostramos que:

$$\forall x (P(x) \to Q(x))$$

Ejercicio

Sea $n \in \mathbb{Z}$. Demuestre que $n^2 \ge n$.

Ejercicio

Sea $n \in \mathbb{Z}$. Demuestre que $n^2 \ge n$.

Ejercicio

Sea $n \in \mathbb{Z}$. Demuestre que $n^2 \ge n$.

Sea $n \in \mathbb{Z}$. Tenemos 3 casos:

1. n = 0: es claro que se cumple la propiedad.

Ejercicio

Sea $n \in \mathbb{Z}$. Demuestre que $n^2 \ge n$.

Sea $n \in \mathbb{Z}$. Tenemos 3 casos:

- 1. n = 0: es claro que se cumple la propiedad.
- 2. n > 0: como $n \in \mathbb{Z}$ tenemos que $n \ge 1$. Si multiplicamos por n a ambos lados, obtenemos que $n^2 \ge n$.
- 3. n < 0: si multiplicamos por n (negativo) a ambos lados: $n^2 > 0 \Rightarrow n^2 > n \Rightarrow n^2 \ge n$.

Ejercicio

Sea $n \in \mathbb{Z}$. Demuestre que $n^2 \ge n$.

Sea $n \in \mathbb{Z}$. Tenemos 3 casos:

- 1. n = 0: es claro que se cumple la propiedad.
- 2. n > 0: como $n \in \mathbb{Z}$ tenemos que $n \ge 1$. Si multiplicamos por n a ambos lados, obtenemos que $n^2 \ge n$.
- 3. n < 0: si multiplicamos por n (negativo) a ambos lados: $n^2 > 0 \Rightarrow n^2 > n \Rightarrow n^2 > n$

Ya que no existen más casos, concluimos que la propiedad se cumple para todo $n \in \mathbb{Z}$. \square

Otros tipos de demostración

- Demostración por doble implicación
- Demostración por contra-ejemplo
- Demostración existencial

Demostración por doble implicación

Por demostrar:

$$\forall x (P(x) \leftrightarrow Q(x))$$

Demostración por doble implicación

Se deben demostrar ambas direcciones por separado. En términos formales:

$$\forall x (P(x) \to Q(x)) \land \forall x (Q(x) \to P(x))$$

Demostración por doble implicación

Por demostrar:

$$\forall x (P(x) \leftrightarrow Q(x))$$

Demostración por doble implicación

Se deben demostrar ambas direcciones por separado. En términos formales:

$$\forall x (P(x) \rightarrow Q(x)) \land \forall x (Q(x) \rightarrow P(x))$$

Ejercicio

Sea $n \in \mathbb{N}$. Demuestre que n es impar si y sólo si n^2 es impar.

Por demostrar:

$$\neg(\forall x(P(x)))$$

Método por contra-ejemplo

Encontrar un elemento n (cualquiera) tal que P(n) es falso.

Por demostrar:

$$\neg(\forall x(P(x)))$$

Método por contra-ejemplo

Encontrar un elemento n (cualquiera) tal que P(n) es falso.

Ejercicio

Demuestre que es falso que todo número entero es suma de dos cuadrados perfectos.

Por demostrar:

$$\neg(\forall x(P(x)))$$

Método por contra-ejemplo

Encontrar un elemento n (cualquiera) tal que P(n) es falso.

Ejercicio

Demuestre que es falso que todo número entero es suma de dos cuadrados perfectos.

Probamos con los primeros números mayores a 1:

Por demostrar:

$$\neg(\forall x(P(x)))$$

Método por contra-ejemplo

Encontrar un elemento n (cualquiera) tal que P(n) es falso.

Ejercicio

Demuestre que es falso que todo número entero es suma de dos cuadrados perfectos.

Probamos con los primeros números mayores a 1:

$$\begin{array}{rcl}
2 & = & 1^2 + 1^2 \\
3 & \neq & 1^2 + 1^2 \\
& \neq & 2^2 + 1^2
\end{array}$$

Por demostrar:

$$\neg(\forall x(P(x)))$$

Método por contra-ejemplo

Encontrar un elemento n (cualquiera) tal que P(n) es falso.

Ejercicio

Demuestre que es falso que todo número entero es suma de dos cuadrados perfectos.

Probamos con los primeros números mayores a 1:

$$\begin{array}{rcl}
2 & = & 1^2 + 1^2 \\
3 & \neq & 1^2 + 1^2 \\
& \neq & 2^2 + 1^2
\end{array}$$

Por lo tanto, 3 no es la suma de dos cuadrados perfectos.

Por demostrar:

 $\exists x (P(x))$

Por demostrar:

$$\exists x (P(x))$$

Método por existencia

Debemos demostrar que existe un elemento n tal que P(n) es verdadero. (Nótese que NO es estrictamente necesario mostrar n explícitamente.)

Por demostrar:

$$\exists x (P(x))$$

Método por existencia

Debemos demostrar que existe un elemento n tal que P(n) es verdadero. (Nótese que NO es estrictamente necesario mostrar n explícitamente.)

Ejercicio

Demuestre que existen a, b irracionales tal que a^b es racional.

Ejercicio

Demuestre que existen a, b irracionales tal que a^b es racional.

Ejercicio

Demuestre que existen a, b irracionales tal que a^b es racional.

Como sabemos que $\sqrt{2}$ es irracional, considere $\sqrt{2}^{\sqrt{2}}$. Tenemos dos casos:

Ejercicio

Demuestre que existen a, b irracionales tal que a^b es racional.

Como sabemos que $\sqrt{2}$ es irracional, considere $\sqrt{2}^{\sqrt{2}}$. Tenemos dos casos:

1. Si $\sqrt{2}^{\sqrt{2}}$ es **racional**, entonces $a = \sqrt{2}$ y $b = \sqrt{2}$ es suficiente.

Ejercicio

Demuestre que existen a, b irracionales tal que a^b es racional.

Como sabemos que $\sqrt{2}$ es irracional, considere $\sqrt{2}^{\sqrt{2}}$. Tenemos dos casos:

- 1. Si $\sqrt{2}^{\sqrt{2}}$ es **racional**, entonces $a = \sqrt{2}$ y $b = \sqrt{2}$ es suficiente.
- 2. Si $\sqrt{2}^{\sqrt{2}}$ es **irracional**, entonces consideremos $a = \sqrt{2}^{\sqrt{2}}$ y $b = \sqrt{2}$:

Ejercicio

Demuestre que existen a, b irracionales tal que a^b es racional.

Como sabemos que $\sqrt{2}$ es irracional, considere $\sqrt{2}^{\sqrt{2}}$. Tenemos dos casos:

- 1. Si $\sqrt{2}^{\sqrt{2}}$ es racional, entonces $a = \sqrt{2}$ y $b = \sqrt{2}$ es suficiente.
- 2. Si $\sqrt{2}^{\sqrt{2}}$ es **irracional**, entonces consideremos $a = \sqrt{2}^{\sqrt{2}}$ y $b = \sqrt{2}$:

$$(\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^{\sqrt{2} \cdot \sqrt{2}}$$
$$= \sqrt{2}^{2}$$
$$= 2$$

Ejercicio

Demuestre que existen a, b irracionales tal que a^b es racional.

Como sabemos que $\sqrt{2}$ es irracional, considere $\sqrt{2}^{\sqrt{2}}$. Tenemos dos casos:

- 1. Si $\sqrt{2}^{\sqrt{2}}$ es racional, entonces $a = \sqrt{2}$ y $b = \sqrt{2}$ es suficiente.
- 2. Si $\sqrt{2}^{\sqrt{2}}$ es **irracional**, entonces consideremos $a = \sqrt{2}^{\sqrt{2}}$ y $b = \sqrt{2}$:

$$\left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2} \cdot \sqrt{2}}$$

$$= \sqrt{2}^2$$

$$= 2$$

Por lo tanto, a^b es racional. \Box

Outline

Métodos de demostración

Epílogo

Objetivos de la clase

- □ Identificar equivalencia lógica en predicados
- □ Comprender consecuencia lógica en predicados
- Conocer métodos de demostración
- □ Relacionar los métodos con fórmulas en predicados

