Métodos de demostración

Clase 06

IIC 1253

Prof. Cristian Riveros

¿qué es una demostración?

Definición

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

¿qué **afirmaciones matemáticas** conocen?

Afirmaciones matemáticas

Ejemplos

1. Todo número natural cumple que
   si es par, entonces su sucesor es impar.

   $$\forall x.\ x \text{ es par} \rightarrow \text{el sucesor de } x \text{ es impar}$$

2. Todo número natural cumple que
   es par si, y solo si, el número al cuadrado es par.

   $$\forall x.\ x \text{ es par} \leftrightarrow x^2 \text{ es par}$$

3. Existe una cantidad infinita de números primos.

   ?

afirmación matemática $\approx$ proposición en lógica de predicados

Tipos de afirmaciones matemáticas

- Teorema.
- Proposición.
- Definición.
- Axioma.
- Lemma.
- Corolario.
- Conjetura.
- Problema abierto.

¿qué es un teorema?

Definición

Un **teorema** es
una afirmación matemática que es **verdadera** y **demostrable**.

- ¿qué es un **lema**?
- ¿qué es una **proposición**?
- ¿qué es un **corolario**?

¿qué es un axioma?

Definición

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

¿qué axiomas conocen?

¿qué es una conjectura?

Definición

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

¿qué conjetura conocen?

Ejemplos

*"todo número mayor a 2 puede ser escrito como
la suma de dos primos."*

Conjetura de Goldbach

*"Si n es mayor 2, entonces NO existen números positivos
x, y, z, tal que $x^n + y^n = z^n$."*

(ex) Conjetura de Fermat

¿qué es un problema abierto?

Definición

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

¿qué problema abierto conocen?

¿cuál es el problema abierto mas importante en CS?

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

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

Wikipedia.

¿cuál es el problema abierto mas importante en CS?

Uno de los 7 "Millennium Prize Problems":

1. Yang–Mills and Mass Gap
2. Riemann Hypothesis
3. **P vs NP Problem**
4. Navier–Stokes Equation
5. Hodge Conjecture
6. ~~Poincaré Conjecture~~
7. Birch and Swinnerton-Dyer Conjecture

propuestos por *The Clay Mathematics Institute*.

¿cuál es el problema abierto mas importante en CS?

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

US$ 1 millón a quien lo resuelva.

"Aside from being an important problem in computational theory, a proof either way would have **profound implications** *for mathematics, cryptography, algorithm research, artificial intelligence, game theory, multimedia processing, philosophy, economics and many other fields."*

Wikipedia.

¿qué es una demostración?

Definición

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

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

- axiomas.
- hipótesis o supuestos (si existe).
- afirmaciones previamente demostradas.

Cada argumento en la secuencia de argumentos esta conectado con el anterior por una **regla de inferencia** (consecuencia lógica).

El **último paso** de la secuencia establece la verdad de la afirmación.

¿qué NO es una demostración?

- Una secuencia de símbolos.
- Una secuencia disconexa de argumentos.

IMPORTANTE

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

¿cómo encontramos una secuencia de argumentos para demostrar un teorema?

1. Experiencia.
2. Intuición.
3. Creatividad.
4. Perseverancia.
5. **Métodos de demostración**.

Outline

Outline

Demostración directa

Supongan que queremos demostrar una afirmación como:

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

Método directo

Suponemos que $P(n)$ es verdadero para un n **cualquiera** (genérico) y demostramos que $Q(n)$ también es verdadero.

¿qué sucede cuando $P(n)$ es **falso**?

Ejemplo de una demostración directa

Definición

- Un entero n en $\mathbb{Z}$ se dice **par** si existe k en $\mathbb{Z}$ tal que $n = 2k$.
- Un entero n en $\mathbb{Z}$ se dice **impar** si existe k en $\mathbb{Z}$ tal que $n = 2k + 1$.

Teorema

Si n es un entero impar, entonces n^2 es impar.

Demostración

Suponemos que n es impar.
Por definición, existe un $k \in \mathbb{Z}$ tal que $n = 2k + 1$.

$$\begin{array}{rcll} n^2 & = & (2k+1)^2 & \text{(definición de } n\text{)} \\ & = & 4k^2 + 4k + 1 & \text{(multiplicación } (2k+1)(2k+1)\text{)} \\ & = & 2 \cdot (2k^2 + 2k) + 1 & \text{(factorización por 2)} \end{array}$$

Si definimos k' como $k' = 2k^2 + 2k$, entonces se tiene que $n^2 = 2k' + 1$.
Por definición de un número impar, concluimos que n^2 es impar. $\square$

Outline

Demostración por contrapositivo

Supongan que queremos demostrar:

$$\forall x. P(x) \rightarrow Q(x) \;\equiv\; \forall x.\, \neg Q(x) \rightarrow \neg P(x)$$

Método por contrapositivo

Suponemos que $Q(n)$ es **falso** para un n cualquiera (genérico) y demostramos que $P(n)$ también es **falso**.

Ejemplo de demostración por contrapositivo

Teorema

Suponga a y b son positivos. Si $n = ab$, entonces $a \leq \sqrt{n}$ o $b \leq \sqrt{n}$.

¿es posible hacer una demostración directa?

Demostración (por contrapositivo)

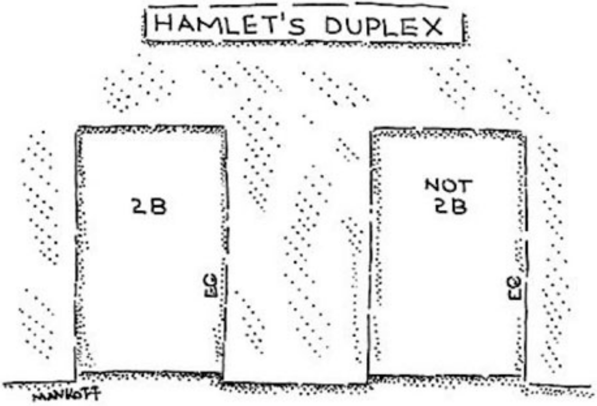
PD: Si $a > \sqrt{n}$ y $b > \sqrt{n}$, entonces $n \neq ab$.

Suponga que $a > \sqrt{n}$ y $b > \sqrt{n}$ con n positivo.

$$\begin{array}{rcll} n & = & \sqrt{n} \cdot \sqrt{n} & \\ & < & a \cdot \sqrt{n} & \text{(por } a > \sqrt{n}\text{)} \\ & < & a \cdot b & \text{(por } b > \sqrt{n}\text{)} \end{array}$$

Entonces, $n < a \cdot b$ y, por lo tanto, $n \neq ab$. □

¿cuál método ocupar? ¿directo o contrapositivo?



Outline

Demostración por contradicción

Supongan que queremos demostrar una afirmación R, pero demostramos:

$$(\neg R) \rightarrow (S \wedge \neg S)$$

donde S es una afirmación cualquiera.

¿qué implica esto?

Metodó por contradicción

Suponemos que $\neg R$ es verdadero y inferimos una **contradicción**.

Si esto sucede, entonces R debe ser **verdadero**.

Demostración por contradicción (versión alternativa)

Supongan que queremos demostrar:

$$R \ := \ \forall x. \ P(x) \rightarrow Q(x)$$

Metodó por contradicción

$$\neg R \ := \ \exists x. \ P(x) \wedge \neg Q(x)$$

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

> *"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).

Ejemplo de una demostración por contradicción

Definiciones

- Un número r en $\mathbb{R}$ se dice **racional** si existen enteros p y q tal que:

$$r = \frac{p}{q}$$

  con $q \neq 0$ y p, q no tienen divisores en común exceptuando el 1.

- Un número $r \in \mathbb{R}$ se dice **irracional** si no es racional.

Teorema

$\sqrt{2}$ es un número irracional.

Ejemplo de una demostración por contradicción

Demostración ($\sqrt{2}$ es un número irracional)

Suponga que $\sqrt{2}$ es racional.
Entonces, existen p y q en $\mathbb{Z}$, sin divisores en común, tal que $\sqrt{2} = \frac{p}{q}$.

$$\begin{array}{rcl} \sqrt{2} & = & \frac{p}{q} \\ 2 \cdot q^2 & = & p^2 \end{array}$$

Por lo tanto, p^2 es par y, entonces, p **es par** (¿por qué?).
Como p es par, entonces $p = 2k$ para algún k en $\mathbb{Z}$.

$$\begin{array}{rcl} 2 \cdot q^2 & = & p^2 \\ 2 \cdot q^2 & = & (2k)^2 \\ q^2 & = & 2 \cdot k^2 \end{array}$$

Por lo tanto, q^2 es par y, entonces, q **es par**.

Contradicción! (¿por qué?)

$\square$

Ejemplo de una demostración por contradicción

Definición

Un número entero p es un número **primo** si
los únicos número que lo dividen son el 1 y p.

Teorema

Existe una cantidad infinita de números primos.

Ejercicio! (demostración clásica)

Outline

Demostración por análisis de casos

Supongan que queremos demostrar:

$$\forall x \in D.\, P(x)$$

Metodó de análisis de casos

Dividimos el dominio de posibilidades D a una cantidad **finita de casos** $D_1, D_2, \ldots, D_k$ tal que:

$$D \ = \ D_1 \cup D_2 \cup \ldots \cup D_k$$

Por último, demostramos para todo subdominio D_i se cumple:

$$\forall x \in D_i.\, P(x)$$

con i desde 1 hasta k.

Ejemplo de una demostración por casos

Teorema

Para todo entero n se cumple que $n^2 \geq n$.

Demostración

1. Si $n = 0$, entonces $0^2 = 0$. Por lo tanto, $0^2 \geq 0$.
2. Si $n \geq 1$, entonces:

$$\begin{array}{rcll} n & \geq & 1 & \\ n^2 & \geq & n & \text{(multiplicando ambos lados por } n > 0\text{)} \end{array}$$

3. Si $n \leq -1$, como $n^2 \geq 0$ entonces se tiene que $n^2 \geq n$.

$\square$

¿cuál es la ventaja de demostrar por casos?

Recomendación

"Cuando todos los métodos anteriores han fallado y no se sabe por donde empezar, una "estrategia" es empezar demostrando casos simples para así **ganar intuición** *en la demostración general. "*

Outline

Demostración de **doble implicación**

Supongan que queremos demostrar una afirmación como:

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

Demostración para doble-implicación

Debemos demostrar dos afirmaciones (**ambas direcciones**):

$$\forall x.\, P(x) \rightarrow Q(x) \quad \text{y} \quad \forall x.\, P(x) \leftarrow Q(x)$$

Ejemplo de una demostración de **doble-implicación**

Teorema

Para todo número natural n,
se tiene que n es impar si, y solo si, n^2 es impar.

Demostración

($\Rightarrow$) Si n es impar, entonces n^2 es impar. ✓

($\Leftarrow$) Si n^2 es impar, entonces n es impar.

PD: Si n es par, entonces n^2 es par.

...

Ejercicio: termine la demostración.

Outline

Demostración por **contra-ejemplo**

Supongan que deseamos demostrar que la siguiente afirmación es falsa:

$$\forall x.\, P(x)$$

Demostración por contra-ejemplo

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

Ejemplo de una demostración por **contra-ejemplo**

Teorema

Es falso que todo número mayor a 1 es la suma de dos cuadrados perfectos.

Demostración

Probamos con los primeros números mayor a 1:

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

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

¿cómo buscar/encontrar el contra-ejemplo?

Recomendaciones

1. Probar primero los ejemplos más "**pequeños**".
2. Seguir con los ejemplos más "**comunes**".
3. Intentar con muchos ejemplos.

Outline

Demostración **existencial**

Supongan que queremos demostrar:

$$\exists x.\, P(x)$$

Demostración de existencia

Debemos demostrar que **existe** un elemento n tal que $P(n)$ es **verdadero**.
Notese que NO es estrictamente necesario mostrar n explicitamente.

Ejemplo de una demostración **existencial**

Teorema

Existen dos números irracionales a y b tal que a^b es racional.

Demostración

Como $\sqrt{2}$ es irracional considere $\sqrt{2}^{\sqrt{2}}$.

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 considere $a = \sqrt{2}^{\sqrt{2}}$ y $b = \sqrt{2}$.

$$\begin{aligned}
\left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} &= \sqrt{2}^{\sqrt{2}\cdot\sqrt{2}} \\
&= \sqrt{2}^{2} \\
&= 2
\end{aligned}$$

   Por lo tanto, a^b es racional.

$\square$

¿cuál método de demostración ocupar?

No existe un método infalible para demostrar!

Recomendaciones

1. Probar con distintos métodos.
2. Ganar intución intentando con casos o ejemplos mas sencillos.
3. Revisar demostraciones similares.
4. Sean creativos.