Preliminares

Horst H. von Brand
vonbrand@inf.utfsm.cl

Departamento de Informática
Universidad Técnica Federico Santa María

Contenido

Escribir matemáticas

Al escribir matemáticas, particularmente demostraciones, es indispensable expresarse en forma clara y directa. Interesa convencer al lector mediante un argumento lógico. Use notación matemática solo si ayuda a cumplir este objetivo.
Organice el texto en orden lógico. Si usa resultados que no demuestra, indique la fuente de los mismos. Generalmente, bastará lo visto en clases. Si usa resultados que se demuestran más adelante, indíquelo claramente.

Temática

Antes de entrar al tema de demostraciones propiamente tal, discutiremos alguna notación y conceptos ubicuos en matemáticas.

Relaciones

Es común querer describir conexiones entre objetos, diciendo que están *relacionados*.
Formalmente, una *relación* R entre los conjuntos $\mathscr{A}$ y $\mathscr{B}$ no es más que un conjunto de pares ordenados, $R \subseteq \mathscr{A} \times \mathscr{B}$. Si $(a, b) \in R$, se anota $a\,R\,b$, si $(a, b) \notin R$ se anota $a\,\not{R}\,b$. De particular interés son relaciones entre elementos de un conjunto universo $\mathscr{U}$.

Relaciones

Sea R una relación de $\mathscr{U}$ a $\mathscr{U}$. Se dice que R es:

Reflexiva: Para todo $a \in \mathscr{U}$ es $a\,R\,a$.

Transitiva: Para todo $a, b, c \in \mathscr{U}$ si $a\,R\,b$ y $b\,R\,c$ entonces $a\,R\,c$.

Simétrica: Para todo $a, b \in \mathscr{U}$ si $a\,R\,b$ entonces $b\,R\,a$.

Antisimétrica: Para todo $a, b \in \mathscr{U}$ si $a\,R\,b$ y $b\,R\,a$ entonces $a = b$.

Conectada: Para todo $a, b \in \mathscr{U}$ si $a \neq b$ entonces $a\,R\,b$ o $b\,R\,a$.

Relaciones

Relaciones de orden

Un *preorden* es reflexivo y transitivo. Una *relación de orden* es reflexiva, transitiva y antisimétrica. Una *relación de orden total* es reflexiva, transitiva, antisimétrica y conectada.

Ejemplos son $\leq$ sobre $\mathbb{Z}$ (es un orden total) y $\subseteq$ entre conjuntos (no es total). Un ejemplo de preorden es «*no es más alto que*» comparando alturas entre personas.

Relaciones

Relaciones de equivalencia

Una *relación de equivalencia* es reflexiva, transitiva y simétrica.

Ejemplos son la igualdad entre números, similitud entre figuras geométricas y la equivalencia módulo m:

$$a \equiv b \pmod{m}$$

si $m \mid (b - a)$.

Relaciones

Clases de equivalencia

Si R es una relación de equivalencia sobre $\mathscr{U}$, la *clase de equivalencia* de $a \in \mathscr{U}$ es el conjunto:

$$[a] = \{x \in \mathscr{U} : x \, R \, a\}$$

Es simple ver que si $a \, R \, b$ entonces $[a] = [b]$, y que si $a \not R \, b$ entonces $[a] \cap [b] = \varnothing$. Como $a \in [a]$ (por reflexividad), las clases de equivalencia de R *particionan* al conjunto $\mathscr{U}$ (su unión es $\mathscr{U}$, son disjuntas a pares – no hay elementos en común entre ellos).

Conjuntos bien ordenados

Un conjunto $\mathscr{S}$ con una orden total $\preceq$ tal que todo subconjunto no vacío de $\mathscr{S}$ tiene un elemento mínimo se llama *bien ordenado*. Lo anterior implica que $\mathscr{S}$ tiene un único mínimo.
Ejemplos son $\mathbb{N}$ con $\leq$, y $\mathbb{N}\times\mathbb{N}$ con $\preceq$ definido mediante $(u,v)\preceq(x,y)$ si $u<v$ o $u=v\wedge v\leq y$.

Relaciones

Operaciones

Dada una relación R podemos definir relaciones adicionales. Nos interesan particularmente:

Clausura transitiva: La relación R^+ es la mínima relación transitiva que contiene a R. En términos simples, $a\,R^+\,b$ si $a\,R\,b$ o hay $c_1, c_2, \ldots, c_n$ tales que $a\,R\,c_1, c_1\,R\,c_2, \ldots, c_n\,R\,b$. Es decir, podemos llegar de a a b en uno o más pasos de R.

Clausura reflexiva y transitiva: La relación R^* es la mínima relación transitiva y reflexiva que contiene a R. En términos simples, $a\,R^*\,b$ si $a = b$ o $a\,R^+\,b$. Podemos llegar de a a b en cero o más pasos de R.

Relaciones

Operaciones

Consideremos la relación «sucesor de» en $\mathbb{Z}$: $a\,S\,b$ si $b = a+1$.
Entonces:

S^+: Es la relación $<$: $x\,S^+\,y$ significa que $x\,S\,y$ $(y = x+1)$ o hay $c_1, c_2, \ldots, c_n$ con $c_1 = x+1, c_2 = c_1+1, \ldots, y = c_n+1$; es decir $x < y$.

S^*: Es la relación $\leq$: $x\,S^*\,y$ significa que $x = y$ o $x\,S^+\,y$ $(x < y)$, o sea $x \leq y$.

Funciones

Una *función* f es una relación entre $\mathscr{A}$ y $\mathscr{B}$ con la restricción que para cada $a \in \mathscr{A}$ hay un único $b \in \mathscr{B}$ relacionado a a. Se anota $f : \mathscr{A} \to \mathscr{B}$ para indicar que f es una función de $\mathscr{A}$ a $\mathscr{B}$. Se anota $f(a) = b$ si $(a, b) \in f$.

Para un subconjunto $\mathscr{X} \subseteq \mathscr{A}$ la *imagen* de $\mathscr{X}$ es:

$$f(\mathscr{X}) = \{f(x) : x \in \mathscr{X}\}$$

Para un subconjunto $\mathscr{Y} \subseteq \mathscr{B}$ la *preimagen* de $\mathscr{Y}$ es:

$$f^{-1}(\mathscr{X}) = \{x : \exists y \in \mathscr{Y}, f(x) = y\}$$

Funciones

Tipos especiales

Una función $f : \mathscr{A} \to \mathscr{B}$ es:

Inyectiva: Para todo $a, b \in \mathscr{A}$ si $a \neq b$ entonces $f(a) \neq f(b)$.

Sobreyectiva: Para todo $b \in \mathscr{B}$ hay algún $a \in \mathscr{A}$ tal que $f(a) = b$.

Biyectiva: Es inyectiva y sobreyectiva. Para cada $a \in \mathscr{A}$ hay exactamente un $b \in \mathscr{B}$ tal que $f(a) = b$, y viceversa. Solo en este caso hay una función inversa.

Funciones

Tipos especiales

Consideremos funciones de $\mathbb{N}$ a $\mathbb{Z}$:

Inyectiva: $f(x) = 2x$

Sobreyectiva: $g(x) = \begin{cases} x/4 & x \equiv 0 \pmod 4 \\ -(x-1)/4 & x \equiv 1 \pmod 4 \\ (x-2)/4 & x \equiv 2 \pmod 4 \\ -(x-3)/4 & x \equiv 3 \pmod 4 \end{cases}$

Biyectiva: $h(x) = \begin{cases} x/2 & x \text{ par} \\ -(x-1)/2 & x \text{ impar} \end{cases}$

Tenemos $h^{-1}(y) = 2|y| + [y \leq 0]$

Teoremas, corolarios, lemas, proposiciones

Terminología común en matemáticas incluye las siguientes. Todos son resultados verdaderos, que se han demostrado. No tienen una definición precisa, distintos autores los usan en forma diferente.

Teorema: Un resultado central.

Corolario: Un teorema que resulta directamente de un teorema anterior (o de su demostración).

Lema: Un resultado con demostración independiente, usado para demostrar un teorema.

Proposición: Un resultado que se demuestra, pero que no tiene importancia en sí mismo.

Teoremas, corolarios, lemas, proposiciones

Ocasionalmente hallamos:

Conjetura: Un resultado que podría o no ser cierto. La tarea central de las matemáticas es sospechar conjeturas interesantes y demostrarlas (hacerlas teoremas) o refutarlas (demostrar que son falsas).
Hay conjeturas famosas que se sospecha casi universalmente son ciertas, que se usan como punto de partida de demostraciones.

Ejemplos de tipos de demostraciones

Daremos ejemplos de demostraciones usando las distintas técnicas. Los resultados demostrados acá y sus demostraciones son en general muy simples, concéntrese en la estructura general de las demostraciones, trate de ceñirse a ella en su trabajo. Incluso en nuestros ejemplos simples las demostraciones no siempre son puras, usamos técnicas distintas para demostrar resultados auxiliares.

Demostración directa

Es el tipo de demostración más simple. Consiste en razonar desde lo dado hasta llegar a la conclusión.

Demostración directa

Planteo

Proposición

Todo número entero impar puede expresarse como la diferencia de cuadrados.

Por ejemplo, es $55 = 8^2 - 3^2$ y $-63 = 9^2 - 12^2$.

Demostración directa

Trabajo en borrador

Si x es impar, $x = 2a+1$. Lo a demostrar es:

$$x = u^2 - v^2 = (u+v)\cdot(u-v)$$

Puede ser $u - v = 1$, o sea $u = v+1$. Obtenemos:

$$\begin{aligned} x &= (u+v)\cdot(u-v) \\ &= (2v+1)\cdot 1 \end{aligned}$$

Esto es válido incluso si x es negativo.

Demostración directa

Demostración

Demostración.

Sea x un número entero impar, con lo que hay un entero a tal que $x = 2a+1$. Vemos que:

$$\begin{aligned} x &= 2a+1 \\ &= (2a+1)\cdot 1 \\ &= ((a+1)+a)\cdot((a+1)-a) \\ &= (a+1)^2 - a^2 \end{aligned}$$

Así tenemos una representación de x como diferencia de cuadrados. □

Demostración directa

Comentarios

Note que el borrador no tiene mucho en común con la demostración. Contando solo con la demostración, no siempre estaremos en condiciones de reconstruir el razonamiento que llevó allí. El razonamiento del borrador puede extenderse para construir otras representaciones usando la factorización del número, pero con esto basta.
Formalmente solo interesa la demostración, explicar cómo construirla es útil para enseñanza o a la hora de buscar extensiones.

Demostración por casos

Es común que una demostración deba considerar varios casos. Es importante asegurarse de cubrir todos ellos. Muchas veces los casos se parecen, basta indicar los paralelos en vez de repetir la demostración.

Números de Ramsey

En teoría de grafos, al grafo de n vértices conectados cada uno con todos los demás (el grafo *completo*) se le anota K_n. Si tomamos K_n y coloreamos sus arcos de azul y rojo, podemos preguntarnos cuál es el mínimo n para el que todo K_n así decorado contenga un K_r de arcos rojos o un K_s de arcos azules. Este es el *número de Ramsey* $R(r,s)$.

Números de Ramsey

Planteo

Teorema

$R(3, 3) = 6$

Números de Ramsey

Demostración

Demostración.

Demostraremos que $R(3,3) \leq 6$ y aparte que $R(3,3) > 5$, con lo que $R(3,3) = 6$.

Considere K_6 con arcos azules o rojos. Elija un vértice del grafo. Estará conectado mediante arcos del mismo color con al menos tres de los otros cinco vértices. Supongamos que ese color es azul, el caso de color rojo es similar.

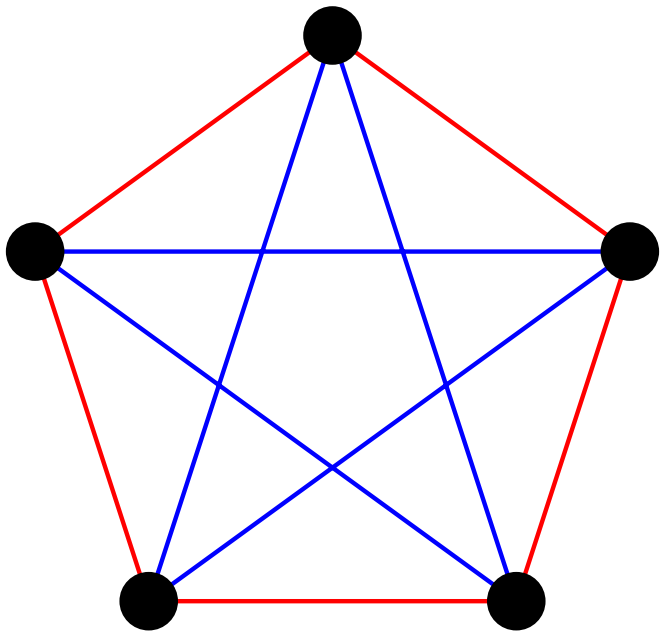
Ahora hay dos casos: Si entre los tres vértices elegidos hay un arco azul, con el vértice original forman un K_3 azul. Si los tres vértices están unidos solo por arcos rojos, forman un K_3 rojo.

Concluimos que $R(3,3) \leq 6$.

Números de Ramsey

Demostración

La figura ilustra un coloreo de arcos de K_5 sin triángulos del mismo color, con lo que $R(3,3) > 5$.



Contrapositivo

Se basa en la identidad lógica $(P \implies Q) \equiv (\neg Q \implies \neg P)$. Esto puede resultar un tanto confuso, anuncie que usará esta estrategia, y plantee $\neg Q \implies \neg P$, posiblemente simplificando esta expresión.

Contrapositivo

Planteo

Proposición

Si $x^2 - 6x + 5$ *es par,* x *es impar.*

Contrapositivo

Demostración

Razonar desde el valor del polinomio al valor de x es incómodo.

Demostración.
Demostramos el contrapositivo: si x no es impar (es par), entonces $x^2 - 6x + 5$ no es par (es impar).
Si x es par, los dos primeros términos del polinomio son pares, sumados al impar 5 el resultado es impar. □

Demostración por contradicción

Para demostrar que P es verdadero, demostramos que $\neg P \implies F$, que es equivalente. Suponemos que P es falso, llegando a una contradicción (algo que sabemos falso; un absurdo, por lo que también se le llama *por reducción al absurdo*).
Debe alertar al lector que empleamos esta estrategia, e indicar claramente la conclusión falsa a la que se llega.

Demostración por contradicción

Planteo

Teorema

El número real $\sqrt{2}$ es irracional.

Demostración por contradicción

Demostración

Demostración.
Lo demostramos por contradicción. Supongamos que $\sqrt{2}$ es un número racional:

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

donde la fracción está en términos mínimos, en particular solo uno de a, b puede ser par.

Demostración por contradicción

Demostración

Entonces:

$$\left(\frac{a}{b}\right)^2 = 2$$
$$a^2 = 2b^2$$

Como a^2 es par, a es par, digamos $a = 2c$. Así:

$$4c^2 = 2b^2$$
$$2c^2 = b^2$$

Demostración por contradicción

Demostración

Como $2c^2$ es par, b^2 y por tanto b son pares, con lo que tanto a como b son pares. Esto contradice la suposición que a/b está en términos mínimos. $\square$

Demostración por contradicción

Comentarios

En general, los pasos intermedios de una demostración pueden usarse: hemos demostrado que son ciertos. Esto no es válido en este caso, estamos partiendo de una premisa falsa para llegar a algo falso, los pasos intermedios serán falsos también.

Equivalencias

Sabemos que $P \iff Q$ es lo mismo que $(P \implies Q) \wedge (Q \implies P)$.
Salvo el caso poco común en que se puede demostrar mediante una cadena de equivalencias, la técnica básica es demostrar implicancia (en una dirección) y su recíproco (en la dirección contraria) .

Equivalencias

Planteo

Usamos antes este resultado.

Teorema

El número entero a^2 es par si y solo si a es par.

Equivalencias

Demostración

Demostración.

Demostramos implicancia en ambas direcciones.

Si a es par, hay un entero c tal que $a = 2c$, con lo que $a^2 = 4c^2 = 2(2c^2)$ que es par.

Para el recíproco, si a^2 es par es par a, demostramos el contrapositivo: si a no es par entonces a^2 no es par. Si a es impar, hay c tal que $a = 2c + 1$. Entonces:

$$\begin{aligned} a^2 &= (2c+1)^2 \\ &= 4c^2 + 4c + 1 \\ &= 2(2c^2 + 2c) + 1 \end{aligned}$$

que es impar. □

Equivalencias

Varias aseveraciones

En caso de que se quiera demostrar que un conjunto de relaciones son equivalentes, suele demostrarse un ciclo de implicancias. Por ejemplo, en álgebra lineal vieron (o verán):

Teorema

Las siguientes son equivalentes para la matriz cuadrada A *de* $n \times n$*:*

(a) La matriz A *tiene inversa.*

(b) La ecuación $A \cdot x = b$ *tiene solución única para* x*.*

(c) La ecuación $A \cdot x = 0$ *solo tiene la solución trivial.*

(d) La forma reducida por filas de A *es* I_n*.*

(e) El determinante $\det(A) \neq 0$*.*

(f) La matriz A *no tiene a* 0 *como valor propio.*

Equivalencias

Varias aseveraciones

La forma tradicional de demostrar esto es cerrar un ciclo:

$$\begin{array}{ccccc} (a) & \Longrightarrow & (b) & \Longrightarrow & (c) \\ \Uparrow & & & & \Downarrow \\ (f) & \Longleftarrow & (e) & \Longleftarrow & (d) \end{array}$$

Claramente cualquier otro entramado que dé un digrafo fuertemente conexo (de todo vértice se puede llegar a todos los demás) es igualmente válido.

Existencia

Muchos teoremas aseveran que existen objetos de ciertas características. La forma obvia de demostrarlos es exhibir uno de ellos, pero eso no siempre es posible.

Existencia

Planteo

Teorema

Hay números irracionales x, y tales que x^y es racional.

Existencia

Demostración no constructiva

Demostración.

Sabemos que $\sqrt{2}$ es irracional. Si $\left(\sqrt{2}\right)^{\sqrt{2}}$ es racional, este es un ejemplo. En caso contrario, $\left(\sqrt{2}\right)^{\sqrt{2}}$ es irracional, y $\left(\left(\sqrt{2}\right)^{\sqrt{2}}\right)^{\sqrt{2}} = \left(\sqrt{2}\right)^2 = 2$ es un ejemplo. □

No fuimos capaces de exhibir un ejemplo, solo demostrar su existencia.

Existencia

Demostración constructiva

Demostración.
Sabemos que $\sqrt{2}$ es irracional. Además, $\log_2 9$ es irracional, cosa que demostramos por contradicción. Supongamos que $\log_2 9$ es racional, o sea hay enteros positivos a, b tales que:

$$\begin{aligned} \log_2 9 &= \frac{a}{b} \\ 9 &= 2^{\log_2 9} \\ &= 2^{a/b} \\ 9^b &= 2^a \end{aligned}$$

Esto es absurdo, el lado izquierdo es impar y el derecho par.

Existencia

Demostración constructiva

Ahora:

$$\begin{aligned}\left(\sqrt{2}\right)^{\log_2 9} &= \left(\sqrt{2}\right)^{2\log_2 3} \\ &= 2^{\log_2 3} \\ &= 3\end{aligned}$$

y 3 ciertamente es racional.
Hemos dado el ejemplo $x = \sqrt{2}$ e $y = \log_2 9$. □

Existencia

Advertencia

Para demostrar existencia basta exhibir un ejemplo. Un ejemplo, o incluso muchos, no es suficiente para demostrar el caso general.

Refutación

Hay veces que necesitamos demostrar que una aseveración (una conjetura) es falsa. Para refutar P, basta demostrar $\neg P$.

Refutación

Muchas aseveraciones implícitamente son universales, se aplican a todos los objetos bajo consideración. Otras aseveran que ciertos objetos existen, son existenciales.
Note que la negación de $\forall x, P(x)$ es $\exists x, \neg P(x)$ (basta hallar un x que hace falso $P(x)$, un *contraejemplo*) y que la negación de $\exists x, P(x)$ es $\forall x, \neg P(x)$.

Refutación

Conjetura

Para todo n entero $p(n) = n^2 - n + 11$ es primo.

Como es una aseveración universal, basta un contraejemplo.

Refutación.

Un contraejemplo es $n = 11$, que da $p(n) = 11 \cdot 11$, un número compuesto. □

Refutación

Conjetura

Hay un número real x tal que $x^4 < x < x^2$.

Esta es una aseveración existencial, un contraejemplo no sirve de nada.

Refutación

Refutación.

Simbólicamente es $\exists x, x^4 < x < x^2$, su negación es $\forall x, \neg(x^4 < x < x^2)$. Demostramos esto por contradicción. Supongamos que tal x existe. Por $x^4 < x$ vemos que $x > 0$. Dividiendo $x^4 < x < x^2$ por x obtenemos:

$$x^3 < 1 < x$$
$$x^3 - 1 < 0 < x - 1$$
$$(x-1)(x^2+x+1) < 0 < x - 1 \qquad (x - 1 > 0)$$
$$x^2 + x + 1 < 0 < 1$$

Esto es absurdo, vimos $x > 0$ por lo que el lado izquierdo es positivo. □

Demostraciones con conjuntos

Los conjuntos son básicos en matemáticas. Lo básico es demostrar que un elemento pertenece (o no) a un conjunto. Lo siguiente es demostrar que $\mathscr{A} \subseteq \mathscr{B}$, que se hace demostrando que $x \in \mathscr{A} \implies x \in \mathscr{B}$. Para demostrar $\mathscr{A} = \mathscr{B}$ demostramos $\mathscr{A} \subseteq \mathscr{B}$ y $\mathscr{B} \subseteq \mathscr{A}$.

Demostraciones con conjuntos

Usamos la notación $2^{\mathscr{A}}$ para denotar el conjunto de subconjuntos del conjunto $\mathscr{A}$.

Proposición

$$2^{\mathscr{A}} \cup 2^{\mathscr{B}} \subseteq 2^{\mathscr{A} \cup \mathscr{B}}$$

Demostraciones con conjuntos

Demostración.
Si $\mathscr{X} \in 2^{\mathscr{A}} \cup 2^{\mathscr{B}}$ es que $\mathscr{X} \subseteq \mathscr{A}$ o $\mathscr{X} \subseteq \mathscr{B}$.
Consideremos $\mathscr{X} \subseteq \mathscr{A}$, el otro caso es similar. En tal caso $\mathscr{X} \subseteq \mathscr{A} \cup \mathscr{B}$, con lo que $\mathscr{X} \in 2^{\mathscr{A} \cup \mathscr{B}}$. □

Inducción

Para demostrar que para todo $n \in \mathbb{N}$ se cumple $P(n)$ podemos usar inducción: Demostramos que $P(1)$ es cierto (el *caso base*) y que para todo n se cumple $P(n) \Longrightarrow P(n+1)$ (el *paso de inducción*). Variantes son tomar un caso base diferente y lo que a veces se llama *inducción fuerte*, usar que $P(k)$ vale para $1 \leq k \leq n$ (usar todos los casos anteriores o algunos de ellos) para demostrar $P(n+1)$. Usar $P(k)$ para $k \leq n$ en la demostración de $P(n+1)$ es *usar la hipótesis de inducción*, que suele abreviarse *por inducción*.

Inducción

Lo mismo es aplicable a conjuntos bien ordenados $\mathscr{S}$: El caso base es demostrar que $P(m$ vale para el mínimo m de $\mathscr{S}$, la inducción es demostrar que si para todo $u \prec x$ (o sea, $u \preceq x$ pero $x \npreceq u$) se cumple $P(u)$ entonces $P(x)$.

Inducción

Planteo

Teorema

Para todo $n \geq 0$*:*

$$\sum_{1 \leq k \leq n} k = \frac{n(n+1)}{2}$$

Inducción

Demostración

Demostración.

Por inducción sobre n desde $n = 0$.

Base: Para $n = 0$ lo aseverado se reduce a $0 = 0$ (la suma vacía es 0). Se cumple.

Inducción: Supongamos que vale hasta $n = m$, consideremos:

$$\begin{aligned}
\sum_{1 \le k \le m+1} k &= \sum_{1 \le k \le m} k + m + 1 && \text{Definición de sumatoria} \\
&= \frac{m(m+1)}{2} + m + 1 && \text{Por inducción} \\
&= \frac{(m+1)(m+2)}{2} && \text{Lo solicitado}
\end{aligned}$$

Inducción fuerte

Planteo

Proposición

Toda cantidad mayor a 7 puede entregarse solo con monedas de 3 y 5.

Inducción fuerte

Demostración

Demostración.

Por inducción fuerte sobre n. Agregar una moneda de 3 aumenta la cantidad entregada en 3, necesitamos $P(n-2)$ para demostrar $P(n+1)$.

Bases: Tenemos $8 = 5+3$, $9 = 3+3+3$ y $10 = 5+5$.

Inducción: Si podemos entregar todas las cantidades hasta n, podemos entregar $n-2$ y también $(n-2)+3 = n+1$.

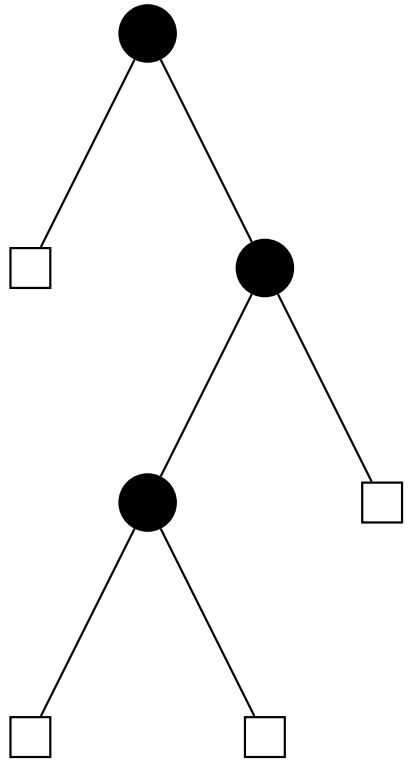
Por inducción vale para todo $n \geq 8$. □

Inducción estructural

En el caso de estructuras definidas recursivamente habrá casos base sobre los que se construyen estructuras más complejas. Es natural demostrar propiedades de tales estructuras por inducción siguiendo la definición, que suele llamarse *inducción estructural*.
Definimos *árboles binarios* como el *árbol vacío* que solo consta de un nodo externo o un nodo raíz con subárboles binarios izquierdo y derecho.

Inducción estructural

(a) El árbol vacío



(b) Tres nodos internos

Mínimo contraejemplo

En un conjunto bien ordenado $\mathscr{S}$, para demostrar que $P(x)$ es verdadero para todo $x \in \mathscr{S}$ suponemos $m \in \mathscr{S}$ mínimo que es un contraejemplo y llegamos a una contradicción, típicamente hallando un contraejemplo menor.

Mínimo contraejemplo

Lema

Todo entero es un producto de primos.

Demostración.

Sabemos que 2 es un producto de (un solo) primo. Sea m el mínimo entero que no es un producto de primos. Si m es primo es un producto de primos. Por lo tanto m es compuesto, $m = a \cdot b$ con $a, b \neq 1$. Pero como $a, b < m$, son productos de primos, $a = p_1 \cdot p_2 \cdots p_r$ y $b = q_1 \cdot q_2 \cdots q_s$, y:

$$m = a \cdot b = (p_1 \cdot p_2 \cdots p_r) \cdot (q_1 \cdot q_2 \cdots q_s)$$

un producto de primos. Contradicción. □

Inducción estructural

Teorema

Un árbol binario que tiene n nodos internos tiene $n+1$ nodos externos.

Inducción estructural

Demostración.

Por inducción estructural.

Base: El árbol binario vacío no tiene nodos internos y tiene un nodo externo. Cumple.

Inducción: Sea un árbol binario no vacío, con lo que tiene un nodo raíz y dos subárboles binarios, digamos que de r y s nodos internos. El árbol tiene $r+s+1$ nodos internos, y por inducción $(r+1)+(s+1)=(r+s+1)+1$ nodos externos, que es lo que asevera la hipótesis.

Por inducción vale para todos los árboles binarios. □

La paradoja del inventor

Planteo

A veces resulta más fácil resolver un problema más general.
Calcule la suma:

$$\sum_{k\geq 0} \frac{k^2}{2^k}$$

La paradoja del inventor

Desarrollo

Es el caso particular $z = 1/2$ de la suma:

$$\sum_{k\geq 0} k^2 z^k$$

Sabemos que si $|z| < 1$ es:

$$\frac{1}{1-z} = \sum_{k\geq 0} z^k$$

De acá:

$$\begin{aligned}\sum_{k\geq 0} k^2 z^k &= z\frac{\mathrm{d}}{\mathrm{d}z}\left(z\frac{\mathrm{d}}{\mathrm{d}z}\sum_{k\geq 0} z^k\right)\\ &= \frac{z^2+z}{(1-z)^3}\end{aligned}$$

La paradoja del inventor

Desarrollo

Como $1/2$ está en el rango de convergencia de la serie, basta substituir:

$$\sum_{k\geq 0} \frac{k^2}{2^k} = \frac{(1/2)^2 + 1/2)}{(1-1/2)^3}$$
$$= 6$$

La paradoja del inventor

Resolver el caso particular parecía imposible, resolvimos infinitos casos en forma simple.

La paradoja del inventor

Planteo

Teorema

$$1+\frac{1}{4}+\frac{1}{9}+\cdots+\frac{1}{n^2}<2$$

La paradoja del inventor

Desarrollo

Sumar un nuevo término a ambos lados destruye lo buscado. Es común en demostraciones por inducción demostrar una hipótesis más fuerte, ya que da más con que trabajar.
Buscamos una diferencia d_n que dé:

$$2 - d_n + \frac{1}{(n+1)^2} \leq 2 - d_{n+1}$$

Resulta que $d_n = 1/n$ funciona.

La paradoja del inventor

Demostración

Demostración.
Por inducción demostramos algo más fuerte:

$$\sum_{1 \leq k \leq n} \frac{1}{k^2} \leq 2 - \frac{1}{n}$$

Base: El caso $n = 1$ es obvio.

La paradoja del inventor

Demostración

Inducción: Suponiendo que se cumple para n:

$$\begin{aligned}\sum_{1\le k\le n+1}\frac{1}{k^2} &\le 2-\frac{1}{n}+\frac{1}{(n+1)^2}\\ &= 2-\frac{n^2+n+1}{n(n+1)^2}\\ &< 2-\frac{n^2+n}{n(n+1)^2}\\ &= 2-\frac{1}{n+1}\end{aligned}$$

La paradoja del inventor

Demostración

Por inducción vale para todo $n \geq 1$. □

Resumen

- Cómo escribir matemáticas.
- Relaciones y funciones. Propiedades, clasificación, operaciones.
- Tipos de demostraciones.