INTRODUCCION. INDUCCION

¿Cómo demostramos que un programa funciona correctamente y produce los resultados buscados? La intuición o probar que funciona adecuadamente en algunos casos no es aceptable. Para demostrar algo es necesario un razonamiento formal que consiste en un proceso que comienza con afirmaciones que sabemos que son ciertas y las conecta con otras, también ciertas, mediante inferencias lógicas. Finalmente el proceso termina cuando obtenemos el enunciado que queremos demostrar y que será el último de los enunciados encadenados.

Vamos a desarrollar aquellas matemáticas que son necesarias para razonar sobre programas en computación.

Una de las técnicas más importantes en el razonamiento matemático es la generalización, ya que una proposición será aplicable en más casos y además es más fácil comprender por qué es cierta, dejando de lado detalles no importantes. Por ejemplo, la proposición:

No existe ningún triángulo cuyos lados sean de longitud 1,2 y 6.

puede ser generalizada a:

No existe ningún triángulo con lados de longitudes a, b y c si $a + b \leq c$.

En este caso se pone de manifiesto que es importante la relación entre las longitudes de los lados y que en el primer enunciado pasa más desapercibido.

En este curso vamos a aprender a hacer demostraciones matemáticas y vamos a trabajar con cantidades no continuas. Por ello introducimos los sistemas numéricos.

Antes de introducirlos, vamos a ver un ejemplo de una demostración matemática. Queremos demostrar que el cuadrado de un entero cualquiera es impar si el entero es impar y viceversa. Lo primero es formularlo en lenguaje más matemático:

- <u>Teorema</u>

  Para todo entero n, n^2 es impar si y sólo si n es impar.

  Conviene destacar lo siguiente:

  - Utilizamos una variable n para referirnos al elemento bajo discusión y así podemos utilizarlo en otras partes del enunciado para referirnos a dicho elemento. (El nombre que usamos es irrelevante pero muchas veces se utiliza p para números primos, x para reales, que ayudan a entender la proposición.)
  - Aunque el nombre de la variable sugiera cierto significado es imprescindible especificar el mismo. n podría ser también un entero positivo.
  - Utilizamos un cuantificador: *Para todo* para subrayar que la propiedad es cierta para *cualquier* entero.
  - En realidad "n^2 es impar si y sólo si n es impar"son dos afirmaciones en una:
    1. "n^2 es impar si n es impar". En otras palabras, si n es impar entonces n^2 es impar.
    2. "n^2 es impar sólo si n es impar". En otras palabras, si n^2 es impar entonces n es impar.

Para abreviar, si llamamos $p \equiv n^2$ es impar y $q \equiv n$ es impar, "p sólo si q"significa lo mismo que " si p entonces q". Cuando p es cierto, q tiene que serlo también. Y "p si q"es lo mismo que " si q entonces p".

Una afirmación del tipo "p si y sólo si q"es verdadera sólo cuando "p sólo si q", "p si q"son ambas ciertas o lo que es lo mismo cuando " si p entonces q", " si q entonces p"son ciertas las dos.

También decimos que p y q son equivalentes y podemos escribir p sii q.

Demostración.

1. Si n es impar entonces n^2 es impar. (Demostración directa)
   Si n es impar $n = 2k + 1$ donde k es algún entero.
   $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1.$
   Tomando $j = 2k^2 + 2k$ entonces $n^2 = 2j + 1$, luego n^2 es impar.
2. Si n^2 es impar entonces n es impar. (Demostración por contradicción)
   Supongamos que no es cierto para todo n, entonces existe algún n tal que n^2 es impar pero n no es impar, en consecuencia es par. Por tanto, si demostramos que si n es par entonces n^2 es par estaríamos demostrando que no existe ningún n par con n^2 impar.
   Si n es par $n = 2k$ donde k es algún entero.
   $n^2 = (2k)^2 = 4k^2 = 2(2k^2).$
   Tomando $j = 2k^2$ entonces $n^2 = 2j$, luego n^2 es par.

Si una demostración es larga y consta de varios pasos, alguno de éstos puede ser demostrado independientemente del teorema y si su principal interés es en el contexto del teorema, lo denominamos *lema*.

Resultados interesantes, fáciles de demostrar tras demostrar un teorema se llaman corolarios.

- <u>Corolario</u>

  Si n es impar, entonces n^4 es impar.

  Dem.

  $n^4 = (n^2)^2$

  Si n es impar, por el teorema n^2 es impar y si n^2 es impar, de nuevo por el teorema $(n^2)^2 = n^4$ es impar.

  Otras técnicas incluyen la distinción de casos...

  Si queremos demostrar que una propiedad es cierta para todo número natural n podríamos demostrarlo distinguiendo casos. Por ejemplo:

  Caso 1: $n = 0$

  Caso 2: n par y $n > 0$.

  Caso 3: n impar

  Pasamos, a continuación a introducir los sistemas numéricos.

SISTEMAS NUMERICOS.

- Números Naturales.

  Cuando contamos objetos les asignamos los números 1,2,3 .... Denotamos $\mathbb{N} = \{0, 1, 2, \ldots\}$. Fijamos 0 como el primer número natural.

  Una de las principales propiedades de los números naturales es que todo elemento de $\mathbb{N}$ se puede obtener aplicando reiteradamente la función sucesor s $(s(n) = n + 1)$ a cero. Decimos que es una **función generadora**:

  0
  $1 = s(0)$
  $2 = s(s(0))$
  $3 = s(s(s(0)))\ldots$

  Utilizaremos este hecho para demostrar muchas propiedades de los números naturales.

  El conjunto de los números naturales $\mathbb{N}$ es un conjunto ordenado:

  $m \leq n \iff m = n$ ó $n = s(...(s(m))...)$

- Números Enteros

  Consideramos la ecuación $m - n = x \qquad m < n$ $(m \leq n$ y $m \neq n)$.

  Para resolverla necesitamos considerar números negativos

  $$\mathbb{Z} = \mathbb{N} \cup \{-1, -2, -3, \ldots\}$$

  Ahora ya no podemos obtener cualquier número entero aplicando repetidamente la función sucesor a 0. Necesitamos otra función generadora que nos permitirá obtener los números negativos. La denotamos la función predecesor p. $p(n) = n - 1$.:

  Funciones Generadoras: la función sucesor s $(s(n) = n + 1)$ y la función predecesor p
  $p(n) = n - 1$.

  0
  $1 = s(0) \qquad -1 = p(0)$
  $2 = s(s(0)) \qquad -2 = p(p(0))$
  $3 = s(s(s(0))) \qquad -3 = p(p(p(0)))$
  .
  .
  .

  La relación entre ambas funciones es la siguiente:

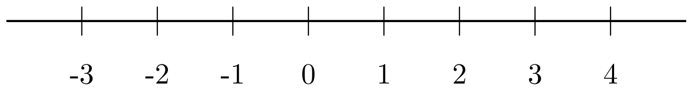
  $s(p(n) = n \quad p(s(n)) = n$

  Luego

  $s(-2) = s(p(p(0))) = p(0) = -1$

  $p(3) = p(s(s(s(0)))) = s(s(0)) = 2$

$p(p(3)) = p(p(s(s(s(0))))) = p(s(s(0))) = s(0) = 1$



Hay huecos entre los enteros, eso nos lleva a decir que $\mathbb{Z}$ es discreta.

En Análisis el paso al límite es fundamental y, en algunos casos es imprescindible considerar sistemas numéricos continuos.

- <u>Números Racionales</u>

  $\mathbb{N} \subsetneq \mathbb{Z} \subsetneq \mathbb{Q}$

  Si consideramos la ecuación
  $m = nx \quad n \neq 0 \; m \neq t \cdot n, \; t \in \mathbb{Z} \quad \Longrightarrow \quad x = \dfrac{m}{n} \in \mathbb{Q}$. No tiene solución entera.

  $\mathbb{Q} = \left\{ \dfrac{m}{n} \middle| \; m, n \in \mathbb{Z} \right\}$

  Sabemos que todo número racional tiene un desarrollo decimal finito o periódico.

  Ejemplos:
  $\dfrac{1}{5} = 0.2 \qquad \dfrac{1}{3} = 0.3333...$
  $\dfrac{17}{6} = 2.8333... \qquad \dfrac{41}{3330} = 0.0123123...$
  Sin embargo, es fácil considerar números con un desarrollo decimal no periódico por lo que vemos que hay otros números además de los racionales ya introducidos.

  8.101001000100001... el número de 0s entre los 1s aumenta $\Longrightarrow$ desarrollo decimal no periódico Estos son los números irracionales. Otros irracionales son:

  $\pi = 3.14159265358979323846 26...$

  $\sqrt{2} = 1.4142135623730950488016887242097....$

  $\sqrt{3}, \quad \sqrt{5}, \ldots$

- <u>Números Reales</u>

  $\mathbb{R} = \mathbb{Q} \cup \mathbb{I}$

  Pasamos a adoptar un punto de vista distinto y podemos distinguir entre números **algebraicos** y **trascendentes**.

  Un número real es algebraico si es solución de una ecuación polinómica.

  $$a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n = 0 \quad a_0 \neq 0, a_i \; \in \mathbb{Z} \quad n > 0$$

  Todo número racional es un número algebraico:
  $q = \dfrac{m}{n} \quad \Longrightarrow \quad q$ es solución de $\; nx - m = 0$

  $p \in \mathbb{I} \;\not\Longrightarrow\;$ número algebraico:

$\sqrt{2}$ es un irracional pero sí es un número algebraico ya que es solución de $x^2 - 2 = 0$

$\pi = 3{,}1415...$ $\quad e = 2{,}71828...$ son irracionales y son números trascendentes. No son números algebraicos.

- Números Complejos

  Sea la ecuación $x^2 + 1 = 0$ no tiene solución real. Luego tenemos que considerar una clase más amplia de números: los números complejos.

  $\mathbb{R} \subseteq \mathbb{C} \qquad \mathbb{C} = \{a + ib | a, b \in \mathbb{R}\} \qquad i = \sqrt{-1}$

  $\mathbb{C}$ verifica que todo polinomio con coeficientes en $\mathbb{C}$ tiene solución en $\mathbb{C}$. (Teorema Fundamental del Algebra)

  $\mathbb{N} \subsetneq \mathbb{Z} \subsetneq \mathbb{Q} \subsetneq \mathbb{R} \subsetneq \mathbb{C}$

  Este proceso algebraico que nos ha obligado a ir extendiendo nuestros sistemas numéricos termina con los complejos debido al Teorema Fundamental.

- Axiomas de Peano. Principio de Inducción.

  Vamos a describir los números naturales. Los siguientes axiomas caracterizan $\mathbb{N}$.

  1. P1 Existe un elemento de $\mathbb{N}$ que llamamos 0. (Primer natural).
  2. P2 Existe la función sucesor $s : \mathbb{N} \longrightarrow \mathbb{N}$ tal que $\forall n \in \mathbb{N} \;\; s(n) \in \mathbb{N}$.
  3. P3 $\forall m, n \in \mathbb{N} \;\; s(m) = s(n) \implies m = n$.
  4. P4 $\forall n \in \mathbb{N} \;\; s(n) \neq 0$.
  5. P5 Principio de Inducción

  Antes de enunciar este principio lo ilustramos con el siguiente ejemplo:

  Supongamos que tenemos una sucesión de bloques en una mesa numerados 0,1,2,... y que algunos bloques están marcados con una X.

  Supongamos que:

  (S1) El bloque 0 está marcado.

  (S2) Si los bloques que preceden al bloque (n+1) están marcados, entonces el bloque (n+1) también está marcado.

  Si admitimos que este principio es verdadero, entonces demostraremos que todo bloque está marcado.

  (S1) explícitamente dice que el bloque 0 está marcado.

  Consideramos el bloque 1. Todos los bloques que preceden el bloque 1, en este caso sólo el 0, están marcados, luego por (S2) podemos afirmar que el bloque 1 está marcado.

  Consideramos el bloque 2. Todos los bloques que preceden el bloque 2, en este caso el 0 y el 1, ya hemos visto que están marcados, luego por (S2) podemos afirmar que el bloque 2 también está marcado.

  Procediendo de esta forma demostraremos que todos los bloques están marcados.

  Por ejemplo, supongamos que hemos verificado que los bloques 0...5 están marcados, para demostrar que el bloque 6 también lo está, bastará con aplicar (S2) ya que todos los anteriores están marcados.

P5 Principio de Inducción.

Supongamos que para todo número natural n tenemos un enunciado S(n) que es verdadero o falso. Si

> Paso Base: S(0) es verdadero.
>
> Paso Inductivo:
> Para todo $k \in \mathbb{N}$, si S(k) es verdadero entonces S(k+1) también es verdadero.

Entonces S(n) es verdadero para todo número natural n.

- EJEMPLOS

- Ej.1
Supongamos que $Suma_n$ denota la suma de los n primeros enteros positivos

$$Suma_n = 0 + 1 + 2 + 3 + \dots n$$

Afirmamos $\quad (*) \ \ S(n) \equiv Suma_n = \dfrac{n(n+1)}{2} \quad$ para $n = 0, 1, \dots$

Realmente tenemos una sucesión de enunciados:

$S(0) \equiv Suma_0 = \dfrac{0 \cdot 1}{2} = 0$

$S(1) \equiv Suma_1 = \dfrac{1 \cdot 2}{2} = 1$

$S(2) \equiv Suma_2 = \dfrac{2 \cdot 3}{2} = 3$

.

.

La demostración por inducción consta de dos pasos:

- Base: $n = 0$, $\ S(0)$ es verdadero.

  $S(0) \equiv \ Suma_0 = \dfrac{0 \cdot 1}{2} = 0$

  $\qquad\quad Suma_0 = 0$

- Suponemos que el enunciado para $n = k$, $S(k)$ es verdadero (Hipótesis de Inducción(HI)), y tenemos que demostrar que el enunciado para $n = k + 1$ es verdadero: $(S(k) \Longrightarrow S(k+1))$ (Paso Inductivo)

  $S(k) \equiv \ Suma_k = \dfrac{k(k+1)}{2}$

  $\qquad\quad Suma_k = 0 + 1 + 2 + \dots + k = \dfrac{k(k+1)}{2}$

  Tenemos que demostrar que $\quad Suma_{k+1} = \dfrac{(k+1)(k+2)}{2} \quad$ es verdadero.

  Por la definición $\quad Suma_{k+1} = 0 + 1 + 2 + \dots + k + (k+1) = Suma_k + (k+1)$

  Por la Hipótesis de Inducción $\ Suma_k = \dfrac{k(k+1)}{2}\ $ luego

  $Suma_{k+1} = Suma_k + (k+1) = \dfrac{k(k+1)}{2} + (k+1) = \dfrac{k(k+1)}{2} + \dfrac{2(k+1)}{2} = \dfrac{k(k+1) + 2(k+1)}{2} = \dfrac{(k+2)(k+1)}{2} = \dfrac{(k+1)(k+2)}{2}$

Hemos visto que se verifica la Base y el Paso Inductivo, luego el Principio de Inducción nos dice que $S(n)$ se cumple para todo $n \in \mathbb{N}$.

- Ej.2

$\forall k \in \mathbb{N}\ 3^{2k} + 4^{k+1}$ es múltiplo de 5 $\Longleftrightarrow \forall k \in \mathbb{N}\ 3^{2k} + 4^{k+1} = 5 \cdot t$ para algún $t \in \mathbb{N}$

Base $S(0) \equiv 3^0 + 4^1 = 5 = 5 \cdot 1 = 5 \cdot t$ para $t = 1$

Paso Inductivo $S(k) \Longrightarrow S(k+1)$

(HI) $S(k) \equiv 3^{2k} + 4^{k+1} = 5 \cdot t_1$ para algún $t_1 \in \mathbb{N}$

$S(k+1) \equiv 3^{2(k+1)} + 4^{(k+1)+1} = 3^{2k} \cdot 3^2 + 4^{k+1} \cdot 4 = 3^{2k} \cdot 9 + 4^{k+1} \cdot 4 = 3^{2k}(5 + 4) + 4^{k+1} \cdot 4 = 3^{2k} \cdot 5 + 4(3^{2k} + 4^{k+1}) \underset{\substack{\uparrow \\ (\text{H.I. } S(k))}}{=} 3^{2k} \cdot 5 + 4(5t_1) = 5(3^{2k} + 4t_1) = 5t_2$

- Ej.3

$\left(1 + \frac{1}{3}\right)^n \geq 1 + \frac{n}{3} \qquad n = 0, 1, \ldots.$

Base $S(0) \equiv \left(1 + \frac{1}{3}\right)^0 \geq 1 + \frac{0}{3} = 1$

$\left(1 + \frac{1}{3}\right)^0 = 1 = 1 + \frac{0}{3}$

Paso Inductivo $S(k) \Longrightarrow S(k+1)$

Suponemos $S(n)$ cierto para $n = k$

(HI) $S(k) \equiv \left(1 + \frac{1}{3}\right)^k \geq 1 + \frac{k}{3}$

Tenemos que probar

$S(k+1) \equiv \left(1 + \frac{1}{3}\right)^{k+1} \geq 1 + \frac{k+1}{3}$

$S(k+1) \equiv \left(1 + \frac{1}{3}\right)^{k+1} = \left(1 + \frac{1}{3}\right)^k \left(1 + \frac{1}{3}\right) \underset{\substack{\uparrow \\ (\text{HI. } S(k))}}{\geq} \left(1 + \frac{k}{3}\right)\left(1 + \frac{1}{3}\right) = \left(1 + \frac{k}{3}\right) +$

$\left(1 + \frac{k}{3}\right)\left(\frac{1}{3}\right) = 1 + \frac{k}{3} + \frac{1}{3} + \frac{k}{9} \underset{\substack{\uparrow \\ \left(\frac{k}{9} \geq 0\right)}}{\geq} 1 + \frac{k}{3} + \frac{1}{3} = 1 + \frac{k+1}{3}$

Algunas veces no podemos aplicar directamente el principio de inducción y necesitamos una versión más fuerte que se conoce como el Principio de Inducción Completa. No obstante es equivalente al principio de inducción ya estudiado.

- **Principio de Inducción Completa**

  Supongamos que para todo número natural n tenemos un enunciado S(n) que es verdadero o falso. Si

  Paso Base: S(0) es verdadero.

  Paso Inductivo:

  Para todo $k \in \mathbb{N}$, si S(j) es cierto para todo $0 \leq j < k$ entonces S(k) también es cierto

Entonces podemos concluir que S(n) es cierto para todo número natural n.

Si S(0) no está definido pero queremos demostrar que los enunciados siguientes son verdaderos

$$S(n_0), S(n_0+1), S(n_0+2), \ldots \quad \text{donde} \quad n_0 \neq 0$$

parece que si modificamos la Base a $S(n_0)$ *es cierto*, en vez de $S(0)$ *es cierto*? tendremos un principio de inducción similar. En efecto es así. Podemos enunciar un Principio de Inducción más general. Para ello, primero definimos $\mathbb{Z}_m$, un segmento de $\mathbb{Z}$.

- <u>$\mathbb{Z}_m$ y el Principio de Inducción.</u>

  Sea $m \in \mathbb{Z}$. Definimos $\mathbb{Z}_m = \{m, s(m), s(s(m)), \ldots\}$

  Podemos ya definir el Principio de Inducción y el Principio de Inducción Completo para $\mathbb{Z}_m$.

- Principio de Inducción

  Supongamos que para todo $n \in \mathbb{Z}_m$ tenemos un enunciado S(n) que es verdadero o falso. Si

  Paso Base: S(m) es verdadero, $m \in \mathbb{Z}$

  Paso Inductivo:
  Para todo $k \in \mathbb{Z}_m$, si S(k) es cierto entonces S(k+1) también lo es

  Entonces S(n) es cierto para todo número $n \in \mathbb{Z}_m$.

- Nota: Necesitamos un valor inicial, i_0 tal que $S(i_0)$ es cierto. $S(k) \Longrightarrow S(k+1)$ puede ser cierto , pero falso $S(k)$.
  Si no existe un entero i_0 tal que $S(i_0)$ es cierto, la conclusión de que $S(n)$ es cierto para todo $n \geq i_0$ sería falsa.

  El paso base, aunque muchas veces trivial, es fundamental incluirlo en la demostración.

- <u>Ej.</u>
  $S(n) \equiv 2 + 2 \cdot 2 + \ldots 2 \cdot n = (n-1)(n+2) \quad n = 1, 2 \ldots.$

  Paso Inductivo $S(k) \Longrightarrow S(k+1)$

  (HI) $S(k) \equiv 2 + 2 \cdot 2 + \ldots 2 \cdot k = (k-1)(k+2)$

  $S(k+1) \equiv 2 + 2 \cdot 2 + \ldots 2 \cdot k + 2 \cdot (k+1) = (k-1)(k+2) + 2 \cdot (k+1) = k^2 - k + 2k - 2 + 2k + 2 = k(k+3)$

  El paso inductivo es cierto, sin embargo la afirmación es falsa para todo entero positivo:

  $2 + 2 \cdot 2 + \ldots 2 \cdot n = 2(1 + 2 + \ldots n) = 2\dfrac{n(n+1)}{2} =$
  $= n(n+1)$
  $(n-1)(n+2) = n(n+1) \implies -2 = 0$

- Principio de Inducción Completa

  Supongamos que para todo $n \in \mathbb{Z}_m$ tenemos un enunciado S(n) que es verdadero o falso. Si

  Paso Base: S(m) es verdadero.

  Paso Inductivo:
  Para todo $k \in \mathbb{Z}_m$, si S(j) es cierto para todo $m \leq j < k$ entonces S(k) también es cierto

  Entonces S(n) es cierto para todo número $n \in \mathbb{Z}_m$.

- <u>Ej.</u>
  $n! \geq 2^{n-1} \quad n = 1, 2, \ldots$

  Base: $S(1) \equiv 1! = 1 = 2^{1-1} = 2^0 = 1$

  Paso Inductivo $\forall k \in \mathbb{Z}_1 \quad S(k) \Longrightarrow S(k+1)$

  (IH) $\quad S(k) \equiv k! \geq 2^{k-1}$

  Tenemos que demostrar

  $S(k+1) \equiv (k+1)! \geq 2^{(k+1)-1} = 2^k$

  $$S(k+1) \equiv (k+1)! = (k+1)k! \underset{\substack{\uparrow \\ (\text{HI. } S(k))}}{\geq} (k+1)2^{k-1} \underset{\substack{\uparrow \\ (k+1) \geq 2}}{\geq} 2 \cdot 2^{k-1} = 2^k$$

- <u>Ej.</u>
  $\forall n \geq 4 \quad 2^n < n!$

  Base $\;S(4) \equiv 2^4 < 4! \iff 16 < 24 = 4!$

  Paso Inductivo $\forall k \in \mathbb{Z}_4 \quad S(k) \Longrightarrow S(k+1)$

  (HI) $\quad S(k) \equiv 2^k < k!$

  Tenemos que demostrar

  $S(k+1) \equiv 2^{k+1} < (k+1)!$

  $$2^{k+1} = 2 \cdot 2^k \underset{\substack{\uparrow \\ (\text{HI. } S(k))}}{<} 2 \cdot k! \underset{\substack{\uparrow \\ 2 < (k+1) \;\; (\text{ya que } \; k \geq 4)}}{<} (k+1)k! = (k+1)!$$

- <u>Ejemplo de Inducción Completa.</u>
  Si $n > 1$ entonces n se puede escribir como producto de primos.

  Base $\;S(2) \equiv 2$ is prime

  Paso Inductivo $\forall n \geq 2 \quad$ si $S(k)$ es cierto para todo $2 \leq k < n \quad$ entonces $S(n)$ es cierto.

  - n es primo $\Longrightarrow S(n)$ es trivial.

- n is compuesto $\implies$ $n = a \cdot b$ $2 \leq a \leq b < n$.
  Por la HI $S(a)$, $S(b)$ se cumplen, $\implies$
  $a = p_1 \cdot \ldots \cdot p_r$ $\quad b = p'_1 \cdot \ldots \cdot p'_s$
  $n = a \cdot b = p_1 \cdot \ldots \cdot p_r \cdot p'_1 \cdot \ldots \cdot p'_s$

- Ej.
  Demuestra por inducción que cualquier franqueo postal $\geq 4c$, se puede completar con sellos de 2c o 5c.

  Base: $S(4) \equiv$ dos sellos de 2.

  Paso Inductivo $\forall n \geq 4$ si $S(k)$ es cierto para todo $4 \leq k < n$ entonces $S(n)$ es cierto.

  $n = (n-2) + 2$. HI. $\implies n - 2 = t_1 \cdot 2 + t_2 \cdot 5$

  $n = (n-2) + 2 = t_1 \cdot 2 + t_2 \cdot 5 + 2 = 2(t_1 + 1) + 5t_2 \implies S(n)$ es cierto.

  Nota: Hay un pequeño problema. Sólo consideramos franqueos de 4 o más céntimos, luego si $n = 5 \implies n - 2 = 3$ pero 3 no es un valor posible y no podemos suponer $S(3)$ cierto. Esto sólo ocurre para $n = 5$, luego si comprobamos explícitamente $S(4)$ y $S(5)$ (como caso **base**) solucionamos el problema.

  Ya hemos comprobado $S(4)$

  $S(5) \equiv 5 = 1 \cdot 5$ Un sello de 5c.

Este ejemplo nos lleva a considerar el **Principio de Inducción Completa para Z_m con varios casos base**

Sea S un enunciado definido para números enteros.

Base: S(m) ... S(l) $l \geq m$ son ciertos.

Paso Inductivo Completo:
Para cualquier $k > l$, si S(j) $\forall m \leq j < k$ es cierto, entonces S(k) es cierto

Podemos concluir que S(n) se verifica para todo $n \in \mathbb{Z}_m$.

No se puede aplicar a $\mathbb{Z}$. Necesitamos **Inducción Estructural**.

Sea S un enunciado definido para números enteros.

1. P1 $S(0)$ es cierto.
2. P2 $\forall k \in \mathbb{N}$ si $S(k)$ es cierto $\implies$ $S(s(k)) = S(k+1)$ es cierto, donde s es el sucesor.
3. P3 $\forall k \in \mathbb{N}$ si $S(k)$ es cierto $\implies$ $S(p(k)) = S(k-1)$ es cierto, donde p es el predecesor.

Entonces $\forall n \in \mathbb{Z}$, $S(n)$ es cierto.

- <u>Ej.</u>
  Sea $a, m \in \mathbb{Z} \quad a \neq 0$

  $\forall n \in \mathbb{Z} \quad a^{m+n} = a^m \cdot a^n$

  1. P1 $\;S(0) \equiv a^{m+0} = a^m = a^m \cdot 1 = a^m \cdot a^0$
  2. P2 (HI) $S(k) \equiv a^{m+k} = a^m \cdot a^k$

     $S(s(k)) = S(k+1) = a^{m+(k+1)} = a^{(m+k)+1} = a^{m+k} \cdot a \underset{\substack{\uparrow \\ \text{(HI. } S(k))}}{=} a^m \cdot a^k \cdot a =$

     $= a^m \cdot (a^k \cdot a) = a^m \cdot a^{k+1}$
  3. P3 (HI) $S(k) \equiv a^{m+k} = a^m \cdot a^k$

     $S(p(k)) = S(k-1) = a^{m+(k-1)} = a^{(m+k)-1} = \dfrac{a^{m+k}}{a} \underset{\substack{\uparrow \\ \text{(HI. } S(k))}}{=} \dfrac{a^m \cdot a^k}{a} = a^m \cdot \dfrac{a^k}{a} =$

     $= a^m \cdot a^{k-1}$