Cap. 3: Principio de Inducción Matemática. Aritmética (divisibilidad)

Rommel Andrés Bustinza Pariona
e-mail: rbustinza at udec.cl

Facultad de Ciencias Físicas y Matemáticas
Universidad de Concepción

6 de mayo de 2024

Sobre el conjunto de los números enteros $\mathbb{Z}$

Se recuerda que $\mathbb{Z}$ está provisto de las operaciones binarias cerradas

- ADICIÓN $+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, tales que $\forall\, (a, b) \in \mathbb{Z} \times \mathbb{Z}\, :\, a + b \in \mathbb{Z}$.
- MULTIPLICACIÓN $\cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, tales que $\forall\, (a, b) \in \mathbb{Z} \times \mathbb{Z}\, :\, a \cdot b \in \mathbb{Z}$.

Propiedades de $+$ y $\cdot$

1. $\forall\, x, y, z \in \mathbb{Z}\, :\, x + (y + z) = (x + y) + z,$ (asociatividad de $+$)
2. $\forall\, x, y \in \mathbb{Z}\, :\, x + y = y + x,$ (conmutatividad de $+$)
3. $\exists\, 0 \in \mathbb{Z}\, :\, \forall x \in \mathbb{Z}\, :\, 0 + x = x,$ (existencia del elemento neutro para $+$)
4. $\forall\, x \in \mathbb{Z}\, :\, \exists (-x) \in \mathbb{Z}\, :\, x + (-x) = 0,$ (existencia del elemento inverso para $+$)
5. $\forall\, x, y, z \in \mathbb{Z}\, :\, x \cdot (y \cdot z) = (x \cdot y) \cdot z,$ ($\cdot$ es asociativa)
6. $\forall\, x, y \in \mathbb{Z}\, :\, x \cdot y = y \cdot x,$ ($\cdot$ es conmutativa)
7. $\exists\, 1 \in \mathbb{Z}\, :\, \forall x \in \mathbb{Z}\, :\, 1 \cdot x = x,$ (existencia del elemento neutro para $\cdot$)
8. $\forall\, x, y, z \in \mathbb{Z}\, :\, x \cdot (y + z) = x \cdot y + x \cdot z.$ (distributividad)
9. $\forall\, x, y \in \mathbb{Z}\, :\, x \cdot y = 0 \quad \to \quad (x = 0 \vee y = 0)$ ($\mathbb{Z}$ no posee divisores de cero)

- DIFERENCIA $- : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, tales que $\forall\, (a, b) \in \mathbb{Z} \times \mathbb{Z}\, :\, a - b := a + (-b) \in \mathbb{Z}$.
- La DIVISIÓN en $\mathbb{Z}$ no está definida (como operación binaria cerrada).
- $\forall\, a, b \in \mathbb{Z}\, :\, a = b \quad \Leftrightarrow \quad a - b = 0.$

Relación de orden en $\mathbb{Z}$

$\forall\,(a,b)\in\mathbb{Z}\times\mathbb{Z}\,:\,a<b\quad\Leftrightarrow\quad a-b<0$

Se lee: "$a\begin{cases}\text{es menor que}\\ \text{antecede a}\end{cases}\quad b$".

PROPIEDADES:

1. $\forall\,a,b\in\mathbb{Z}\,:\,a<b\quad\veebar\quad a=b\quad\veebar\quad b<a$ (tricotomía).
2. $\forall\,a,b\in\mathbb{Z}\,:\,a<b\to(\forall\,c\in\mathbb{Z}\,:\,a+c<b+c)$.
3. $\forall\,a,b,c\in\mathbb{Z}\,:\,\Big(a<b\wedge 0<c\Big)\to ac<bc$.
4. $\forall\,a,b,c\in\mathbb{Z}\,:\,\Big(a<b\wedge b<c\Big)\to a<c$.

OTRAS RELACIONES DERIVADAS:

- $\forall\,(a,b)\in\mathbb{Z}\times\mathbb{Z}\,:\,a\leq b\quad\Leftrightarrow\quad(a<b\quad\vee\quad a=b)$.
- $\forall\,(a,b)\in\mathbb{Z}\times\mathbb{Z}\,:\,a>b\quad\Leftrightarrow\quad b<a$.
- $\forall\,(a,b)\in\mathbb{Z}\times\mathbb{Z}\,:\,a\geq b\quad\Leftrightarrow\quad(a>b\quad\vee\quad a=b)$.
- $\forall\,(a,b)\in\mathbb{Z}\times\mathbb{Z}\,:\,a=b\quad\Leftrightarrow\quad(a\leq b\quad\wedge\quad a\geq b)$.

El Principio del Buen Orden (Teorema de Zermelo)

"Todo subconjunto no vacío A de $\mathbb{Z}_0^+$, posee un primer elemento".
Es decir, si $\emptyset\neq A\subseteq\mathbb{Z}_0^+$, entonces $\exists\,x\in A\,:\,\forall\,y\in A\,:\,x\leq y$.

Aplicaciones de Principio del Buen Orden (PBO)

PROPIEDAD: El primer elemento de $\emptyset \neq A \subseteq \mathbb{Z}_0^+$ es ÚNICO.

Proposición 1

$\forall\, m \in \mathbb{Z}^+ \,:\, m \geq 1.$

Demostración

Por reducción al absurdo. Supongamos que la PROPOSICIÓN ES FALSA, es decir $\exists\, m \in \mathbb{Z}^+ \,:\, 0 < m < 1$. Esto permite definir el conjunto no vacío (¿por qué?)

$$S := \{b \in \mathbb{Z}^+ \,:\, 0 < b < 1\} \subseteq \mathbb{Z}^+ .$$

Invocando el PBO, S admite primer elemento $x \in S$, tal que $\forall\, y \in S \,:\, x \leq y$. Tenemos

$$\begin{aligned} 0 < x < 1 \quad &\Rightarrow \quad 0 \cdot x < x \cdot x \quad \wedge \quad x \cdot x < x \cdot 1 \\ &\Rightarrow \quad 0 < x^2 \quad \wedge \quad x^2 < x \\ &\Rightarrow \quad 0 < x^2 < x < 1 . \end{aligned}$$

De esta manera, resulta que $x^2 = x \cdot x \in \mathbb{Z}^+$, pertenece a S, es distinto de x y antecede a x. Esto último contradice el hecho que x es primer elemento de S. En consecuencia, se cumple $\forall\, m \in \mathbb{Z}^+ \,:\, m \geq 1$, y concluye la demostración. $\square$

Principio de Inducción Matemática (PIM)

Herramienta que permite validar funciones proposicionales sobre $\mathbb{N} = \mathbb{Z}^+$ o algún subconjunto de éste, de cardinalidad infinita.

Problema tipo 1: Demostrar que $\forall\, m \in \mathbb{N} \ : \ q(m)$. Es recomendable definir el llamado Conjunto de Validez de q, $S := \{m \in \mathbb{N} \ : \ q(m)\}$. Así, el objetivo es probar que S es un Conjunto Inductivo, es decir $S = \mathbb{N}$.

Proposición 2 (PIM-primera forma)

Considerando el conjunto S anterior, si se verifica:

- $1 \in S$, es decir $q(1)$ es verdadero,
- $\ell \in S \quad \Rightarrow \quad \ell + 1 \in S$,

entonces $S = \mathbb{N}$.

Demostración

Por reducción al absurdo, suponemos que $S \neq \mathbb{N}$, lo cual significa que $S \subsetneq \mathbb{N}$. Esto asegura $\exists\, a \in \mathbb{N} \ : \ a \notin S$. Así, $a \in S^c$, lo cual permite introducir $T \ := \ S^c \ := \ \{m \in \mathbb{N} \ : \sim \ q(m)\} \subsetneq \mathbb{N}$, el cual es no vacío (¿por qué?). Luego, por el PBO, T admite primer elemento. Sea $x \in T$ su primer elemento. Como $1 \in S$, entonces $x \geq 2$. Luego, $x - 1 \geq 1$. En vista que $x - 1, x \in \mathbb{N}$ y $x - 1$ antecede a x, se debe cumplir $x - 1 \in S$ (¿por qué?). Por Hipótesis, $x = (x - 1) + 1 \in S$ $(\rightarrow\leftarrow)$. De esta forma, se concluye que $S = \mathbb{N}$, y concluye la demostración. $\square$

Ejemplo 1: Demostrar que $\forall\, m \in \mathbb{N} \,:\, 10^{m+1} - 9m - 10$ es divisible por 81.

Sea el conjunto de validez $S := \{m \in \mathbb{N} \,:\, q(m)\}$, donde $q(m) \,:\, 10^{m+1} - 9m - 10 = \overset{\circ}{81}$.
Veamos que $1 \in S \quad \Leftrightarrow \quad 1 \in \mathbb{N} \quad \wedge \quad q(1)$ es V.
Es claro que $1 \in \mathbb{N}$. Verifiquemos que $q(1)$ es verdadero. En efecto

$$10^{1+1} - 9(1) - 10 = 100 - 19 = 81 = (1)(81)\,,\ \text{el cual es múltiplo de 81} \quad \Rightarrow \quad q(1)\ \text{es V.}$$

De esta manera, $1 \in S$.
Hipótesis de Inducción (H.I.): $m \in S \quad \Leftrightarrow \quad m \in \mathbb{N} \quad \wedge \quad q(m)$ es V.
Tesis de Inducción: $m+1 \in S \quad \Leftrightarrow \quad m+1 \in \mathbb{N} \quad \wedge \quad q(m+1)$ es V.
En vista que $m \in \mathbb{N}$, se infiere que $m+1 \in \mathbb{N}$. Resta verificar que se cumple $q(m+1)$.
Tenemos

$$\begin{aligned}
10^{(m+1)+1} - 9(m+1) - 10 &= 10(10^{m+1}) - 9(m+1) - 10 \\
&= 10(10^{m+1} - 9m - 10 + 9m + 10) - 9(m+1) - 10 \\
&= 10(10^{m+1} - 9m - 10) + 10(9m + 10) - 9m - 19 \\
&= 10(10^{m+1} - 9m - 10) + 81m + 81\,.
\end{aligned}$$

Ahora por H.I., $q(m)$ es V, lo cual implica que $10^{m+1} - 9m - 10 = \overset{\circ}{81}$. Así, $\exists\, k \in \mathbb{Z} \,:\, 10^{m+1} - 9m - 10 = 81k$. De esta manera, resulta

$$10^{(m+1)+1} - 9(m+1) - 10 = 10(81k) + 81m + 81 = 81(\overbrace{10k + m + 1}^{\in\mathbb{Z}}) = \overset{\circ}{81}.$$

Así, $q(m+1)$ es V, con lo cual $m+1 \in S$. Finalmente, aplicando el PIM (primera forma), se concluye que $S = \mathbb{N}$, es decir $\forall\, m \in \mathbb{N} \,:\, 10^{m+1} - 9m - 10 = \overset{\circ}{81}$. $\square$

Ejemplo 2: Sea $p \in \mathbb{Z}^+$ impar. Demostrar que $\forall\, m \in \mathbb{N} \,:\, 2^{m+1}$ divide a $p^{2^m} - 1$.
Sea el conjunto de validez $S := \{m \in \mathbb{N} \,:\, q(m)\}$, donde $q(m) \,:\, 2^{m+1}$ divide a $p^{2^m} - 1$.
Otra forma equivalente de definir la proposición abierta es
$q(m) \,:\, p^{2^m} - 1$ es múltiplo de 2^{m+1}.

Veamos que $1 \in S \quad \Leftrightarrow \quad 1 \in \mathbb{N} \quad \wedge \quad q(1)$ es V.

Es claro que $1 \in \mathbb{N}$. Verifiquemos que $q(1)$ es verdadero. En efecto

$$p^{2^1} - 1 = p^2 - 1 = (p+1)(p-1)\,. \tag{1}$$

Como $p \in \mathbb{N}$ es impar, $\exists\, k \in \mathbb{Z}^+ \,:\, p = 2k - 1$. Así, (1) conduce a

$$p^{2^1} - 1 = (2k)((2k-1)-1) = 2^2 k(k-1) = \underbrace{k(k-1)}_{\in \mathbb{Z}}\, 2^{1+1} \quad \Rightarrow \quad q(1) \text{ es V} \quad \Rightarrow \quad 1 \in S$$

Hipótesis de Inducción (H.I.): $m \in S \quad \Leftrightarrow \quad m \in \mathbb{N} \quad \wedge \quad q(m)$ es V.
Tesis de Inducción: $m+1 \in S \quad \Leftrightarrow \quad m+1 \in \mathbb{N} \quad \wedge \quad q(m+1)$ es V.
En vista que $m \in \mathbb{N}$, se infiere que $m+1 \in \mathbb{N}$. Resta verificar que se cumple $q(m+1)$.
Tenemos

$$p^{2^{m+1}} - 1 = p^{2^m \cdot 2} - 1 = \left(p^{2^m}\right)^2 - 1^2 = \left(p^{2^m} + 1\right)\left(p^{2^m} - 1\right) \tag{2}$$

Ahora por H.I., $q(m)$ es V, lo cual implica que $p^{2^m} - 1 = \overset{\circ}{(2^{m+1})}$. Así,
$\exists\, k \in \mathbb{Z} \,:\, p^{2^m} - 1 = k \cdot 2^{m+1}$.

De esta manera, de (2) resulta

$$\begin{aligned} p^{2^{m+1}} - 1 &= (k\cdot 2^{m+1}+1+1)k\cdot 2^{m+1} = k\cdot 2^{m+1}\cdot 2\cdot(k\cdot 2^m+1) \\ &= \underbrace{k(k\cdot 2^m+1)}_{\in\mathbb{Z}}\cdot 2^{(m+1)+1} \quad\Rightarrow\quad q(m+1)\,\text{es V} \quad\Rightarrow\quad m+1\in S\,. \end{aligned}$$

Finalmente, aplicando el PIM (primera forma), se concluye que $S=\mathbb{N}$, es decir $\forall\, m\in\mathbb{N}\,:\,p^{2^m}-1$ es múltiplo de 2^{m+1}, el cual es equivalente a decir $\forall\, m\in\mathbb{N}\,:\,2^{m+1}$ divide a $p^{2^m}-1$. $\square$

Proposición 3 (PIM-segunda forma) $\Leftrightarrow$ (PIM-primera forma)

Considerando el conjunto S anterior, si se verifica:

- $1\in S$, es decir $q(1)$ es VERDADERO,
- Si $\ell\in\mathbb{N}\backslash\{1\}$ es tal que $\forall\, m\in\mathbb{N}\cap[1,\ell)\,:\,m\in S$, entonces $\ell\in S$,

se concluye que $S=\mathbb{N}$.

Demostración

Por reducción al absurdo, supongamos que $S\neq\mathbb{N}$, lo cual nos dice que $S\subsetneq\mathbb{N}$. Definimos ahora el complemento de S, $T\,:=\,S^{c}\,:=\,\{m\in\mathbb{N}\,:\sim\,q(m)\}\subsetneq\mathbb{N}$, el cual es no vacío (¿por qué?). Luego, por el PBO, T admite primer elemento. Sea $x\in T$ su primer elemento. Como $1\in S$, entonces $x>1$. Esto implica que $\forall\, m\in\mathbb{N}\cap[1,x)\,:\,m\in S$. Luego, por HIPÓTESIS, $x\in S$ $(\rightarrow\leftarrow)$. De esta forma, se concluye que $S=\mathbb{N}$, y concluye la demostración. $\square$

EJEMPLO 3: Demostrar que $\forall\, m \in \mathbb{N} \,:\, m^2 - 2m - 1$ no es divisible por 3.

Sea el conjunto de validez $S := \{m \in \mathbb{N} \,:\, q(m)\}$, donde $q(m) \,:\, m^2 - 2m - 1 \neq \overset{\circ}{3}$.

Veamos que $1 \in S \quad \Leftrightarrow \quad 1 \in \mathbb{N} \quad \wedge \quad q(1)$ es V. Tenemos

$$1 \in \mathbb{N} \quad \wedge \quad 1^2 - 2(1) - 1 = -2 \neq \overset{\circ}{3} \quad \Rightarrow \quad q(1) \text{ es V} \quad \Rightarrow \quad 1 \in S\,,$$

$$2 \in \mathbb{N} \quad \wedge \quad 2^2 - 2(2) - 1 = -1 \neq \overset{\circ}{3} \quad \Rightarrow \quad q(2) \text{ es V} \quad \Rightarrow \quad 2 \in S\,,$$

$$3 \in \mathbb{N} \quad \wedge \quad 3^2 - 2(3) - 1 = 2 \neq \overset{\circ}{3} \quad \Rightarrow \quad q(3) \text{ es V} \quad \Rightarrow \quad 3 \in S\,.$$

Sea ahora $\ell \in \mathbb{N}$, con $\ell > 3$. HIPÓTESIS DE INDUCCIÓN (H.I.): $\forall\, m \in \mathbb{N} \cap [1, \ell) \,:\, m \in S$.
TESIS DE INDUCCIÓN: $\ell \in S$. POR REDUCCIÓN AL ABSURDO, suponemos que $\ell \notin S$, es decir $q(\ell)$ es F. En otras palabras: $\ell^2 - 2\ell - 1 = \overset{\circ}{3}$.

Por otro lado, sea $\tilde{m} := \ell - 3 \in \mathbb{Z}$, el cual satisface: $\tilde{m} \geq 1 \quad \wedge \quad \tilde{m} < \ell$. Luego, como $\tilde{m} \in \mathbb{N} \cap [1, \ell)$, se debe cumplir (por H.I.) que $q(\tilde{m})$ es V. Es decir $\tilde{m}^2 - 2\tilde{m} - 1 \neq \overset{\circ}{3}$. Pero

$$\begin{aligned} \tilde{m}^2 - 2\tilde{m} - 1 &= (\ell - 3)^2 - 2(\ell - 3) - 1 = (\ell^2 - 6\ell + 9) - 2\ell + 6 - 1 \\ &= (\ell^2 - 2\ell - 1) - 6\ell + 15 = (\ell^2 - 2\ell - 1) - 3(2\ell - 5)\,. \end{aligned}$$

Como $\ell^2 - 2\ell - 1 = \overset{\circ}{3}$, $\exists\, a \in \mathbb{Z} \,:\, \ell^2 - 2\ell - 1 = 3a$. De esta manera, se tiene

$$\tilde{m}^2 - 2\tilde{m} - 1 = 3a - 3(2\ell - 5) = 3(\underbrace{a - 2\ell + 5}_{\in \mathbb{Z}}) = \overset{\circ}{3} \quad \Rightarrow \quad q(\tilde{m}) \text{ es F } (\rightarrow\leftarrow)$$

De esta forma $\ell \in S$, y se valida la TESIS DE INDUCCIÓN. Luego, aplicando el PIM (segunda forma), se concluye $S = \mathbb{N}$, es decir $\forall\, m \in \mathbb{N} \,:\, m^2 - 2m - 1 \neq \overset{\circ}{3}$. $\square$

PIM Generalizado

Sea $m_0 \in \mathbb{N}$. Se desea probar ahora: $\forall\, m \in \mathbb{N} \;:\; m \geq m_0 \to q(m)$. Para este fin definimos $\mathbb{A} := \mathbb{N} \cap [m_0, +\infty)$, y el conjunto de validez $S := \{m \in \mathbb{A} \;:\; q(m)\}$. El objetivo es probar que $S = \mathbb{A}$.

Proposición 4: (PIM-tercera forma)

Considerando el conjunto S anterior, si se verifica:

- $m_0 \in S$,
- $\forall\, \ell \in \mathbb{A} : \ell \in S \quad \to \quad \ell + 1 \in S$,

entonces $S = \mathbb{N} \cap [m_0, +\infty)$.

Demostración

Por reducción al absurdo, supongamos que $S \neq \mathbb{A}$. Esto asegura que $\exists\, y_0 \in \mathbb{A}$ tal que $y_0 \notin S$. Esto permite definir $T := \{m \in \mathbb{A} : \sim q(m)\} \subseteq \mathbb{A} \subseteq \mathbb{N}$, el cual es no vacío (¿por qué?). Por el PBO, T posee primer elemento, al cual denotamos por $x \in T$. Como $m_0 \in S$, se tiene que $x > m_0$. De esta manera, resulta $m_0 \leq x - 1 < x$, de donde se infiere que $x - 1 \in S$ (¿por qué?). Por HIPÓTESIS, se deduce que $x = (x-1) + 1 \in S$ $(\to\leftarrow)$. De esta forma, se concluye que $S = \mathbb{A}$, y concluye la demostración. $\square$

EJEMPLO 4: Demostrar que $\forall\, m \in \mathbb{N} \cap [5, +\infty) \;:\; 2^m > m^2$.
HINT: Primero demostrar que $\forall\, m \in \mathbb{N} \cap [3, +\infty) \;:\; 2m + 1 < m^2$.

Proposición 5 (PIM-cuarta forma) $\Leftrightarrow$ (PIM-tercera forma)

Considerando los conjuntos $\mathbb{A}$, S anteriores, si se verifica:

- $m_0 \in S$, es decir $q(m_0)$ es VERDADERO,
- Si $\ell \in \mathbb{A} \backslash \{m_0\}$ es tal que $\forall\, m \in \mathbb{A} \cap [m_0, \ell) \,:\, m \in S$, entonces $\ell \in S$,

se infiere que $S = \mathbb{A}$.

EJEMPLO 5: Demostrar que todo entero $m > 7$, se puede expresar de la forma $m = 3a + 5b$, siendo a, b números enteros no negativos. Es decir:
$\forall\, m \in \mathbb{N} \cap [8, +\infty) \,:\, \exists (a, b) \in \mathbb{Z}_0^+ \times \mathbb{Z}_0^+ \,:\, m = 3a + 5b.$

Sumatoria

Sea $\{a_j\}_{j=r}^{m} \subseteq \mathbb{K}$, siendo $\mathbb{K}$ un conjunto de escalares (naturales, enteros, racionales, irracionales, reales...complejos...), $r, m \in \mathbb{Z}$, con $r \leq m$. Para abreviar la expresión de la adición de estos escalares, se suele emplear el símbolo SUMATORIA, como sigue

$$\sum_{j=r}^{m} a_j \ := \ a_r + \cdots + a_m \quad (\text{Usualmente: } r = 0 \quad \vee \quad r = 1)\,.$$

Se lee: "La sumatoria de los a_j, desde $j = r$ hasta $j = m$."

EJEMPLOS:

1. La suma de los $m \in \mathbb{N}$ primeros números naturales se puede denotar como

$$1 + 2 + 3 + \cdots + m = \sum_{j=1}^{m} j \quad (\text{aquí } a_j := j)\,.$$

2. La suma de los cuadrados de los $m \in \mathbb{N}$ primeros números naturales se denota como

$$1^2 + 2^2 + 3^2 + \cdots + m^2 = \sum_{j=1}^{m} j^2 \quad (\text{aquí } a_j := j^2)\,.$$

3. Para la suma de los $m \in \mathbb{N}$ primeros términos de una progresión geométrica de razón q y primer elemento a, resulta

$$a + aq + aq^{+} \cdots + aq^{m-1} = \sum_{k=0}^{m-1} aq^{k} = \sum_{j=1}^{m} aq^{j-1}\,.$$

Propiedades (salvo la primera, se demuestran por PIM):

1. En una sumatoria, el índice de la suma es una "variable muda", es decir puede cambiarse por cualquier "letra" donde aparezca.
$$\sum_{j=1}^{m} a_j = \sum_{k=1}^{m} a_k = \sum_{\ell=1}^{m} a_\ell = a_1 + \cdots + a_m\,.$$
2. Una suma se puede expresar de diversas formas, usando para ello "sumas parciales"
$$\sum_{j=1}^{m} a_j = \sum_{j=1}^{m-1} a_j + a_m = a_1 + \sum_{j=2}^{m} a_j = \sum_{j=1}^{\ell} a_j + \sum_{\ell+1}^{m} a_j\,, \quad \text{donde } 1 < \ell < m$$
$$= \sum_{j=1}^{\ell-1} a_j + a_\ell + \sum_{j=\ell+1}^{m} a_j\,, \quad \text{donde } 1 < \ell < m\,.$$
3. $\forall\, c \in \mathbb{K} : \forall\, m \in \mathbb{N} : \displaystyle\sum_{j=1}^{m} c = c\, m$. Se recalca que la constante c no depende de j.
4. $\forall\, c \in \mathbb{K} : \forall\, m \in \mathbb{N} : \displaystyle\sum_{j=1}^{m} c\, a_j = c \sum_{j=1}^{m} a_j$. De nuevo, la constante c no depende de j.
5. Propiedad Telescópica: $\forall\, m \in \mathbb{N} : \displaystyle\sum_{j=1}^{m} (a_j - a_{j-1}) = a_m - a_0$.

   Segunda Forma: $\forall\, m \in \mathbb{N} : \displaystyle\sum_{j=1}^{m} (a_{j+1} - a_j) = a_{m+1} - a_1$.

Sumas notables

1. $\forall\, m \in \mathbb{N} : \displaystyle\sum_{k=1}^{m} k = \frac{m(m+1)}{2}.$
2. $\forall\, m \in \mathbb{N} : \displaystyle\sum_{k=1}^{m} k^2 = \frac{m(m+1)(2m+1)}{6}.$
3. $\forall\, m \in \mathbb{N} : \displaystyle\sum_{k=1}^{m} k^3 = \left(\frac{m(m+1)}{2}\right)^2.$

Sea $\{a_j\}_{j=r}^{m} \subseteq \mathbb{K}$, siendo $\mathbb{K}$ un conjunto de escalares (naturales, enteros, racionales, irracionales, reales...complejos...), $r, m \in \mathbb{Z}$, con $r \leq m$. Para abreviar la expresión del producto de estos escalares, se suele emplear el símbolo PRODUCTORIA, como sigue

$$\prod_{j=r}^{m} a_j \,:=\, a_r \cdots a_m \quad (\text{Usualmente: } r = 0 \quad \vee \quad r = 1)\,.$$

Se lee: "La productoria de los a_j, desde $j = r$ hasta $j = m$."
EJEMPLO NOTABLE: La productoria de los $m \in \mathbb{N}$ primeros números naturales, se expresa como

$$\prod_{k=1}^{m} k = 1 \cdot 2 \cdots m\,.$$

Este producto se conoce como FACTORIAL DE m, y tiene notación propia $m!$.

Propiedades (salvo la primera, se demuestran por PIM):

1. En una sumatoria, el índice de la suma es una "variable muda", es decir puede cambiarse por cualquier "letra" donde aparezca.

$$\prod_{j=1}^{m} a_j = \prod_{k=1}^{m} a_k = \prod_{\ell=1}^{m} a_\ell = a_1 \cdots a_m \,.$$

2. Una suma se puede expresar de diversas formas, usando para ello "productos parciales"

$$\prod_{j=1}^{m} a_j = \left(\prod_{j=1}^{m-1} a_j\right) \cdot a_m = a_1 \cdot \left(\prod_{j=2}^{m} a_j\right) = \left(\prod_{j=1}^{\ell} a_j\right) \cdot \left(\prod_{\ell+1}^{m} a_j\right) \,, \quad \text{donde } 1 < \ell < m$$

$$= \left(\prod_{j=1}^{\ell-1} a_j\right) \cdot a_\ell \cdot \left(\prod_{j=\ell+1}^{m} a_j\right) \,, \quad \text{donde } 1 < \ell < m \,.$$

3. $\forall\, c \in \mathbb{K} \,:\, \forall\, m \in \mathbb{N} \,:\, \displaystyle\prod_{j=1}^{m} c = c^m$. Se recalca que la constante c no depende de j.

4. $\forall\, c \in \mathbb{K} \,:\, \forall\, m \in \mathbb{N} \,:\, \displaystyle\prod_{j=1}^{m} (c\, a_j) = c^m \prod_{j=1}^{m} a_j$. La constante c no depende de j.

5. Propiedad Telescópica: $\forall\, m \in \mathbb{N} \,:\, \displaystyle\prod_{j=1}^{m} \left(\frac{a_j}{a_{j-1}}\right) = \frac{a_m}{a_0}$.