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

27 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).
- $\forall\, a,b \in \mathbb{Z} \,:\, a = b \quad \Leftrightarrow \quad a-b = 0$.

... sobre $\mathbb{Z}$ ...

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 $\begin{cases}\text{es menor que}\\ \text{antecede a}\end{cases}$ 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

$10^{1+1} - 9(1) - 10 = 100 - 19 = 81 = (1)(81)$, el cual es múltiplo de 81 $\quad \Rightarrow \quad q(1)$ 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 $\forall\, m \in \mathbb{N} \,:\, 10^{m+1} - 9m - 10 \overset{\circ}{=} 81$.

□

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

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

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 $p^{2^m} - 1$. □

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. □

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 $\forall\, m \in \mathbb{N} \,:\, m^2 - 2m - 1 \neq \overset{\circ}{3}$.

□

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 $q \neq 0$ y primer elemento $b \in \mathbb{R}$, resulta
$$b + bq + bq^2 + \cdots + bq^{m-1} = \sum_{j=1}^{m} bq^{j-1} \quad (\text{aquí } a_j := bq^{j-1})\,.$$

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

1. En una sumatoria, el índice es una "variable muda": $\sum_{j=1}^{m} a_j = \sum_{k=1}^{m} a_k = \sum_{\ell=1}^{m} a_\ell$.
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. $\forall\, m \in \mathbb{N} : \sum_{j=1}^{m}(a_j + b_j) = \sum_{j=1}^{m} a_j + \sum_{j=1}^{m} b_j$.
4. $\forall\, c \in \mathbb{K} : \forall\, m \in \mathbb{N} : \sum_{j=1}^{m} c = c\, m$. Se recalca que la constante c no depende de j.
5. $\forall\, c \in \mathbb{K} : \forall\, m \in \mathbb{N} : \sum_{j=1}^{m} c\, a_j = c \sum_{j=1}^{m} a_j$. De nuevo, la constante c no depende de j.
6. Propiedad Telescópica: $\forall\, m \in \mathbb{N} : \sum_{j=1}^{m}(a_j - a_{j-1}) = a_m - a_0$.

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

Sumas notables

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

Productoria

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: $m!$
Por convención $0! = 1$.

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

1. En una productoria, el índice de la productoria 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 productoria 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. $\forall\, c \in \mathbb{K} : \forall\, m \in \mathbb{N} : \prod_{j=1}^{m} c = c^m$. Se recalca que la constante c no depende de j.

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

5. Propiedad Telescópica: $\forall\, m \in \mathbb{N} : \prod_{j=1}^{m} \left(\frac{a_j}{a_{j-1}}\right) = \frac{a_m}{a_0}$, siendo $\{a_j\} \subseteq \mathbb{K}\backslash\{0\}$.

El algoritmo de división de Euclides

Proposición 6 (Algoritmo de la división de Euclides - versión clásica)

$\forall\,(a,d)\in\mathbb{Z}_0^+\times\mathbb{Z}^+\,:\,\exists\,!\,(q,r)\in\mathbb{Z}\times\mathbb{Z}\,:\,a=d\,q+r$, con $0\leq r<d$.

Demostración (Existencia)

Sean $a\in\mathbb{Z}_0^+$, $d\in\mathbb{Z}^+$ fijos, pero arbitrarios. Consideremos los casos:
Caso 1: $a=0$. Aquí consideramos $q=0$, $r=0<d$.
Caso 2: $a=d=1$. Tomamos $q=1$ y $r=0<d$.
Caso 3: $a\,d>1$. Definimos el conjunto

$$S:=\{x\in\mathbb{Z}_0^+\,|\,\exists\,m\in\mathbb{Z}_0^+\,:\,x=a-d\,m\}\subseteq\mathbb{Z}_0^+\,,$$

el cual es no vacío, pues $a=a-d\cdot 0\in S$. Luego, por el Principio del Buen Orden, S tiene un primer elemento, al cual denotaremos por r. Dado que $r\in S$, $\exists\,q\in\mathbb{Z}_0^+\,:\,r=a-d\,q$. Así, $a=d\,q+r$, con $r\geq 0$.
Resta probar que $r<d$: Por Reducción al absurdo, suponemos que $r\geq d$. Luego, $\tilde{r}:=r-d\geq 0$. Además

$$\tilde{r}=a-d\,q-d=a-d\,(q+1)<r\overset{(\tilde{m}:=q+1\in\mathbb{Z}_0^+)}{\Rightarrow}\tilde{r}\in S\quad\wedge\quad\tilde{r}<r\,.$$

De esta forma, $\tilde{r}$ es el primer elemento de S $(\rightarrow\leftarrow)$. Así, se concluye que $r<d$. □

... Demostración (Unicidad)

Por Reducción al Absurdo, supongamos que $\exists\, q, \tilde{q}, r, \tilde{r} \in \mathbb{Z}^+$, con $0 \leq r, \tilde{r} < d$, tales que $a = d\,q + r = d\,\tilde{q} + \tilde{r}$. Esto conduce a

$$d\,q + r = d\,\tilde{q} + \tilde{r} \quad \Rightarrow \quad d(q - \tilde{q}) = \tilde{r} - r\,. \tag{3}$$

Afirmación: $\tilde{r} = r$.
En efecto, analizando los (otros) casos posibles.

- Caso $\tilde{r} > r$. De (3), se tiene $d(q - \tilde{q}) = \tilde{r} - r > 0$. Como $d > 0$, resulta $q - \tilde{q} \in \mathbb{N}$. Luego, $q - \tilde{q} \geq 1$, y por tanto $d = d \cdot 1 \leq d(q - \tilde{q}) = \tilde{r} - r < d$, de donde $d < d$ $(\rightarrow\leftarrow)$.
- Caso $\tilde{r} < r$. De (3), se tiene (luego de multiplicar por -1) $d(\tilde{q} - q) = r - \tilde{r} > 0$. Razonando como en el caso anterior, se llega también a una contradicción.
- Luego, por Descartes (gracias a la tricotomía de los números enteros), se concluye que $\tilde{r} = r$.

Así, de (3) se infiere que $q = \tilde{q}$, y concluimos la unicidad. □

El resultado anterior puede generalizarse a todo $\mathbb{Z}$

Proposición 7 (Algoritmo de la división de Euclides - versión generalizada)

$\forall\,(a, d) \in \mathbb{Z} \times \mathbb{Z}\backslash\{0\} \,:\, \exists!\,(q, r) \in \mathbb{Z} \times \mathbb{Z} \,:\, a = d\,q + r$, con $0 \leq r < |d|$.

Divisibilidad

Definición:

Sean $a, b \in \mathbb{Z}$, con $b \neq 0$. Se dice que $\begin{cases} b \text{ divide a } a \\ b \text{ es un factor/divisor de } a \end{cases}$ si $\exists\, c \in \mathbb{Z}$ (necesariamente único) tal que $a = bc$.

NOTACIÓN: $b \mid a$.

OBSERVACIÓN: $b \mid a$ también se puede leer como: "a es divisible por b", o "a es un múltiplo de b".

Por ejemplo: $3 \mid 6$, pero $3 \nmid 7$.

Proposición 8 (Primeras propiedades)

1. $\forall\, a \in \mathbb{Z}\backslash\{0\} \,:\, a \mid a$, pues $\exists 1 \in \mathbb{Z} \,:\, a = a \cdot 1$ (factor único).
2. $\forall\, a \in \mathbb{Z}\backslash\{0\} \,:\, a \mid 0$.
3. $\forall\, a \in \mathbb{Z} \,:\, 1 \mid a \quad \wedge \quad -1 \mid a$, pues $a = 1 \cdot a = (-1) \cdot (-a)$. Se dice que 1 y -1 son divisores universales.
4. $\forall\, a, b \in \mathbb{Z}\backslash\{0\} \,:\, \forall\, c \in \mathbb{Z} \,:\, \Big(a \mid b \wedge b \mid c\Big) \Rightarrow a \mid c$.
5. $\forall\, a, b \in \mathbb{Z} \,:\, \forall\, d \in \mathbb{Z}\backslash\{0\} \,:\, \Big(d \mid (a+b) \wedge d \mid a\Big) \Rightarrow d \mid b$.
6. $\forall\, a \in \mathbb{Z} \,:\, \forall\, b \in \mathbb{Z}\backslash\{0\} \,:\, b \mid a \Leftrightarrow (-b) \mid a \Leftrightarrow b \mid (-a) \Leftrightarrow (-b) \mid (-a)$.

OBSERVACIÓN: La última propiedad nos dice que para cuestiones de divisibilidad, podemos ignorar el signo de los números involucrados.

Proposición 9 (Más propiedades)

7. $\forall\, a, b \in \mathbb{Z}\backslash\{0\} \,:\, b \,|\, a \quad \Rightarrow \quad |b| \leq |a|.$
8. $\forall\, a, b \in \mathbb{Z}\backslash\{0\} \,:\, b \,|\, a \,\wedge\, a \,|\, b \quad \Rightarrow \quad |b| = |a|.$
9. $\forall\, a, b \in \mathbb{Z} \,:\, \forall\, c \in \mathbb{Z}\backslash\{0\} \,:\, \Big(c \,|\, a \,\wedge\, c \,|\, b\Big) \quad \Rightarrow \quad \Big(c \,|\, (a+b) \,\wedge\, c \,|\, (a-b)\Big).$

Definición: Máximo Común Divisor (MCD)

Considere el conjunto $C := \{a_j\}_{j=1}^{m} \subseteq \mathbb{Z}$. Se dice que $d \in \mathbb{Z}^+$ es MÁXIMO COMÚN DIVISOR de $a_1, ..., a_m$ si verifica las condiciones:

- $\forall\, j \in \{1, ..., m\} \,:\, d \,|\, a_j$,
- Si $\tilde{d} \in \mathbb{Z}^+$ es otro número tal que $\forall\, j \in \{1, ..., m\} \,:\, \tilde{d} \,|\, a_j$, entonces $\tilde{d} \,|\, d$.

Es decir, el MCD de $\{a_j\}_{j=1}^{m}$ es el mayor entero positivo que divide a todos los números de $\{a_j\}_{j=1}^{m}$.
NOTACIÓN: $d := mcd(a_1, ..., a_m)$.

OBSERVACIÓN: El MCD de un conjunto de números es único.
En efecto, si $d, \tilde{d}$ son $mcd(a_1, ..., a_m)$, resulta $\tilde{d} \,|\, d \,\wedge\, d \,|\, \tilde{d}$. Luego, por PROPOSICIÓN 9 (PROPIEDAD 8): $|d| = |\tilde{d}|$. Como el mcd es positivo, se concluye $\tilde{d} = d$.
EJEMPLO: $mcd(12, 18, 30) = 6$; $mcd(7, 13, 27, 100) = 1$.

Lema de Bézout (Identidad de Bézout) (versión clásica)

Sean $a, b \in \mathbb{Z}\backslash\{0\}$, y sea $d := mcd(a, b)$. Entonces $\exists\, x, y \in \mathbb{Z} : ax + by = d$.

Demostración

Definimos el conjunto de las combinaciones lineales enteras de a y b:

$$S := \{z \in \mathbb{Z}^+ : (\exists\, x, y \in \mathbb{Z}) : (z = ax + by)\} \subseteq \mathbb{Z}^+ \subseteq \mathbb{Z}_0^+ ,$$

el cual es no vacío pues $z = |a| \in S$ (para $x = 1$, $y = 0$, si $a > 0$; $x = -1$, $y = 0$, si $a < 0$). Por el Principio del Buen Orden, S posee primer elemento, al que denotaremos por d. Como $d \in S$, $\exists\, x_0, y_0 \in \mathbb{Z} : d = ax_0 + by_0$.
Resta probar que $d = mcd(a, b)$. Para ello:

- $d \mid a$. En efecto, por el Algoritmo de la División de Euclides, $\exists\, q, r \in \mathbb{Z}$, con $0 \leq r < d$, tales que $a = q\,d + r$. Notamos que $0 \leq r = a - qd = a - q(ax_0 + by_0) = (1 - qx_0)a + (-qy_0)b$. En vista que $1 - qx_0, -qy_0 \in \mathbb{Z}$, se infiere que $r \in S \cup \{0\}$. Pero, $r \notin S$, pues sino r sería el primer elemento de S $(r < d)$. En consecuencia, $r = 0$ y así, $d \mid a$.
- $d \mid b$. (Se demuestra con argumentos análogos a los dados en el caso anterior).
- Sea $\tilde{d} \in \mathbb{Z}^+$ otro divisor común de a y de b. Esto asegura la existencia de $\alpha, \beta \in \mathbb{Z} : a = \alpha\tilde{d}$ y $b = \beta\tilde{d}$. Luego, $d = ax_0 + by_0 = \alpha\tilde{d}x_0 + \beta\tilde{d}y_0 = \tilde{d}(\alpha x_0 + \beta y_0)$. En vista que $\alpha x_0 + \beta y_0 \in \mathbb{Z}$, se infiere que $\tilde{d} \mid d$.

Finalmente, se concluye que $d = mcd(a, b)$. □

Ejemplo:

$$\begin{aligned} mcd(12,42) = 6 &= 12(-3) + 42(2) \\ &= 12(4) + 42(-1) \\ &= 12(11) + 42(-3) \\ &= 12(18) + 42(-5) \\ &= \cdots \end{aligned}$$

Lema de Bézout (Identidad de Bézout) (versión generalizada)

Sean $\{a_j\}_{j=1}^m \subseteq \mathbb{Z}\backslash\{0\}$, y $d := mcd(a_1, ..., a_m)$. Entonces $\exists\, \{x_j\}_{j=1}^m \subseteq \mathbb{Z} : \sum_{j=1}^{m} a_j x_j = d$.

Proposición 10

$\forall\, a \in \mathbb{Z} : \forall\, b \in \mathbb{Z}^+ : b \mid a \quad \Rightarrow \quad b = mcd(a, b)$.

Proposición 11

Sean $a, b \in \mathbb{Z}$, con $b \neq 0$. Considere $q, r \in \mathbb{Z}$ el cuociente y resto (respectivamente) que resulta de aplicar el Algoritmo de la División de Euclides a a y b: $a = bq + r$. Entonces $mcd(a, b) = mcd(b, r)$.

Demostración

Sea $d = mcd(a, b)$. Probaremos que $d = mcd(b, r)$. Tenemos

- $d \mid a \wedge d \mid b$. Luego, $d \mid (a - bq)$, es decir $d \mid r$. Recordar también que $d \mid b$.
- Sea $\tilde{d} \in \mathbb{Z}^+$ con $\tilde{d} \mid b \wedge \tilde{d} \mid r$. Así, $\tilde{d} \mid (bq + r)$, es decir $\tilde{d} \mid a$. Como $\tilde{d} \mid b$, resulta $\tilde{d} \mid d$.

De esta manera, se concluye que $d = mcd(b, r)$. □

Proposición 12 (Algoritmo del MCD)

Dados $a, b \in \mathbb{Z}^+$, con $a > b$ y b no es factor de a. Sean

$$
\begin{aligned}
(q_1, r_1) \in \mathbb{Z} \times \mathbb{Z}_0^+ &: a = bq_1 + r_1\,, \quad 0 < r_1 < b \\
(q_2, r_2) \in \mathbb{Z} \times \mathbb{Z}_0^+ &: b = r_1 q_2 + r_2\,, \quad 0 < r_2 < r_1 \\
(q_3, r_3) \in \mathbb{Z} \times \mathbb{Z}_0^+ &: r_1 = r_2 q_3 + r_3\,, \quad 0 < r_3 < r_2 \\
&\cdots\cdots \\
(q_m, r_m) \in \mathbb{Z} \times \mathbb{Z}_0^+ &: r_{m-2} = r_{m-1} q_m + r_m\,, \quad 0 < r_m < r_{m-1} \\
(q_{m+1}, r_{m+1}) \in \mathbb{Z} \times \mathbb{Z}_0^+ &: r_{m-1} = r_m q_{m+1}\,, \quad (r_{m+1} = 0)\,.
\end{aligned}
$$

Entonces $r_m = mcd(a, b)$.

PROOF: Invocando la Proposición 11 reiteradamente, y la Proposición 10 al final, resulta

$$mcd(a, b) = mcd(b, r_1) = mcd(r_1, r_2) = \cdots = mcd(r_{m-1}, r_m) = r_m\,. \qquad \square$$

Ejemplo: Determinar $mcd(2024, 1972)$.

Aplicando el ALGORITMO DEL MCD resulta

$$2024 = 1972(1) + 52 \tag{4}$$
$$1972 = 52(37) + 48 \tag{5}$$
$$52 = 48(1) + 4 \tag{6}$$
$$48 = 4(12) + 0 \tag{7}$$

De donde se deduce que $mcd(2024, 1972) = 4$.
Notar que los residuos generados son: $52 > 48 > 4 > 0$.
Ahora determinemos una combinación lineal entera de {2024,1972}, que nos de su MCD.
Eliminamos 48 de (5), usando (6). Nos queda

$$1972 = 52(37) + 52 - 4 = 52(38) - 4 \tag{8}$$

Ahora, eliminamos $52 \cdot 38$ de 38(4), usando (8). Resulta

$$2024(38) = 1972(38) + 1972(1) + 4 \quad \Rightarrow \quad 2024(38) + 1972(-39) = 4\,.$$

Proposición 13

$\forall\, c \in \mathbb{N} : \forall\, a, b \in \mathbb{Z}\backslash\{0\} : mcd(ca, cb) = c \cdot mcd(a, b)$.

PROOF: Consecuencia inmediata de la PROPOSICIÓN 12 (multiplicar todo por c). □

Proposición 14

Sean $a, b \in \mathbb{Z}\backslash\{0\}$. Si $\tilde{d} \in \mathbb{Z}^+$ es un divisor común de a y de b, entonces

$$mcd\left(\frac{a}{\tilde{d}}, \frac{b}{\tilde{d}}\right) = \frac{mcd(a, b)}{\tilde{d}}.$$

Demostración

$$mcd(a, b) = mcd\left(\frac{a}{\tilde{d}}\tilde{d}, \frac{b}{\tilde{d}}\tilde{d}\right) = \tilde{d}\, mcd\left(\frac{a}{\tilde{d}}, \frac{b}{\tilde{d}}\right) \quad \Rightarrow \quad mcd\left(\frac{a}{\tilde{d}}, \frac{b}{\tilde{d}}\right) = \frac{mcd(a, b)}{\tilde{d}}\,. \quad \square$$

Definición: Número primo y número compuesto

Decimos que $p \in \mathbb{N}\backslash\{1\}$ es Número Primo, cuando sus únicos divisores (en $\mathbb{N}$) son 1 y p. Por otro lado, los números naturales mayores que 1, que no son primos, se llaman Números Compuestos. Dicho de otra manera, $m \in \mathbb{N}$ es número compuesto si $\exists\, m_1, m_2 \in \mathbb{N}\backslash\{1, m\} \ : \ m = m_1 m_2$.

Ejemplos

Números primos: 2, 3, 5, 7, 11, 13, 17, 19, 23, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, ...
Números compuestos: 4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20, 22, 24, 25, 26, 27, 28, 30, ...

La importancia de los números primos radica en que de alguna forma se pueden ver como los "átomos" o "bloques" con los que se generan los demás números.

Teorema 1

$\forall\, m \in \mathbb{N}\backslash\{1\}$: m es primo o m se puede descomponer como multiplicación de números primos.

Ejemplos

- 2, 3 son números primos.
- $60 = 4 \cdot 15 = 2 \cdot 2 \cdot 3 \cdot 5$. Luego 60, que no es primo, se descompone como multiplicación de números primos (2, 2, 3 y 5 en este caso).

Demostración

Para cada $m \in \mathbb{N}$, definimos los enunciados abiertos:

- $p(m)$: m es número primo,
- $q(m)$: m se puede descomponer como multiplicación de números primos.

Definimos ahora $\mathbb{A} := \mathbb{N}\backslash\{1\}$ y el conjunto de validez

$$S := \{m \in \mathbb{A} : p(m) \vee q(m)\}.$$

Notamos que $2, 3 \in S$, por ser ambos números primos. También, $4 \in S$, pues $4 > 1$ y $4 = 2 \cdot 2$, lo cual indica que $q(4)$ es $\mathtt{V}$. Esto exhibe que $S \neq \emptyset$.
Hipótesis de inducción (H.I.): Sea $\ell \in \mathbb{A}$, con $\ell > 4$ tal que $\forall\, k \in \mathbb{A} \cap (1, \ell) : k \in S$.
Veamos que $\ell \in S$.

- Caso 1: ℓ es número primo. Automáticamente, $\ell \in S$.
- Caso 2: ℓ es número compuesto. Esto implica que $\exists\, a, b \in \mathbb{N} \cap (1, \ell) : \ell = ab$. Por H.I. , $(p(a) \vee q(a)) \wedge (p(b) \vee q(b))$.
  Si $q(a) \wedge q(b)$, entonces $\exists\, \{a_i\}_{i=1}^{r}, \{b_j\}_{j=1}^{s}$ (todos ellos números primos), tales que $a = \prod_{i=1}^{r} a_i$ y $b = \prod_{j=1}^{s} b_j$. Esto implica que $\ell = ab = \prod_{i=1}^{r} a_i \prod_{j=1}^{s} b_j$, y se concluye que $q(\ell)$ es $\mathtt{V}$, es decir $\ell \in S$.
  Cualquiera de las otras tres opciones posibles, permite concluir también (Verificarlo) que $\ell \in S$.

Luego, por el PIM generalizado, $S = \mathbb{A}$, y concluye la demostración. $\square$

Corolario 1 (inmediato)

$\forall\, m \in \mathbb{N}\backslash\{1\}$: Si m no es primo, entonces m es divisible por un número primo.

Teorema 2 (Euclides)

Existen infinitos números primos.

Demostración

Por reducción al absurdo, supongamos que hay una cantidad finita de números primos, digamos $m_0 \in \mathbb{N}$. Sean éstos los elementos del conjunto $\{p_j\}_{j=1}^{m_0}$. En seguida, generamos el número natural $z := \prod_{j=1}^{m_0} p_j + 1$. Siendo $z > 1$, e invocando el Teorema 1 y Corolario 1 anterior, se tiene que z es un número primo o z es divisible por un número primo. Analizando cada caso ahora:

- Caso 1: z es un número primo. Como $z > \prod_{j=1}^{m_0} p_j$, se desprende que $\forall\, j \in \{1, ..., m_0\} \,:\, z > p_j$. Ello implica que $z \notin \{p_j\}_{j=1}^{m_0}$ (z no pertenece al conjunto de todos los primos) $(\rightarrow\leftarrow)$.
- Caso 2: z es divisible por un número primo, del conjunto de todos los primos $\{p_j\}_{j=1}^{m_0}$. Es decir, $\exists\, j_0 \in \{1, ..., m_0\} \,:\, p_{j_0} \,|\, z$. Luego, $p_{j_0} \,|\, (z - \prod_{j=1}^{m_0} p_j)$, es decir $p_{j_0} \,|\, 1$. Como $1 \,|\, p_{j_0}$, entonces (Propos. 9, propiedad 8) $|p_{j_0}| = |1|$. Por tanto, $p_{j_0} = 1$ $(\rightarrow\leftarrow)$

De esta manera, se concluye que existe una cantidad infinita de números primos. $\square$