

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

20 de junio de 2024



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

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

- ADICIÓN $+$: $\mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$, tales que $\forall (a, b) \in \mathbb{Z} \times \mathbb{Z} : a + b \in \mathbb{Z}$.
- MULTIPLICACIÓN \cdot : $\mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$, 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 $\forall x, y \in \mathbb{Z} : x + y = y + x$, (comutatividad 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 comutativa)
- 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 $\forall x, y \in \mathbb{Z} : x \cdot y = 0 \rightarrow (x = 0 \vee y = 0)$ (\mathbb{Z} no posee divisores de cero)

- DIFERENCIA $-$: $\mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$, 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).
- $\forall a, b \in \mathbb{Z} : a = b \Leftrightarrow a - b = 0$.



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

Relación de orden en \mathbb{Z}

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

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

PROPIEDADES:

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

OTRAS RELACIONES DERIVADAS:

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

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

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

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. □

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-primeras formas)

Considerando el conjunto S anterior, si se verifica:

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

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. □

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 $q(m) : 10^{m+1} - 9m - 10 = 81$.

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

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

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

De esta manera, $1 \in S$.

HIPÓTESIS DE INDUCCIÓN (H.I.): $m \in S \Leftrightarrow m \in \mathbb{N} \wedge q(m)$ es V.

TESIS DE INDUCCIÓN: $m + 1 \in S \Leftrightarrow m + 1 \in \mathbb{N} \wedge q(m + 1)$ 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 $10^{m+1} - 9m - 10 = 81$. Así,

$\exists k \in \mathbb{Z} : 10^{m+1} - 9m - 10 = 81k$. De esta manera, resulta

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

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 $\forall m \in \mathbb{N} : 10^{m+1} - 9m - 10 = 81$.



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

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

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

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

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

HIPÓTESIS DE INDUCCIÓN (H.I.): $m \in S \Leftrightarrow m \in \mathbb{N} \wedge q(m)$ es V.

TESIS DE INDUCCIÓN: $m + 1 \in S \Leftrightarrow m + 1 \in \mathbb{N} \wedge q(m + 1)$ 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

$$p^{2^{m+1}} - 1 = p^{2^m \cdot 2} - 1 = (p^{2^m})^2 - 1^2 = (p^{2^m} + 1)(p^{2^m} - 1) \quad (2)$$

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

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

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 $p^{2^m} - 1$.

□

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 $\ell \in \mathbb{N} \setminus \{1\}$ 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 $q(m) : m^2 - 2m - 1 \not\equiv 3$.

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

$$1 \in \mathbb{N} \wedge 1^2 - 2(1) - 1 = -2 \not\equiv 3 \Rightarrow q(1) \text{ es V} \Rightarrow 1 \in S,$$

$$2 \in \mathbb{N} \wedge 2^2 - 2(2) - 1 = -1 \not\equiv 3 \Rightarrow q(2) \text{ es V} \Rightarrow 2 \in S,$$

$$3 \in \mathbb{N} \wedge 3^2 - 2(3) - 1 = 2 \not\equiv 3 \Rightarrow q(3) \text{ es V} \Rightarrow 3 \in S.$$

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: $\ell^2 - 2\ell - 1 \stackrel{\circ}{=} 3$.

Por otro lado, sea $\tilde{m} := \ell - 3 \in \mathbb{Z}$, el cual satisface: $\tilde{m} \geq 1 \wedge \tilde{m} < \ell$. Luego, como $\tilde{m} \in \mathbb{N} \cap [1, \ell)$, se debe cumplir (por H.I.) que $q(\tilde{m})$ es V. Es decir $\tilde{m}^2 - 2\tilde{m} - 1 \not\equiv 3$. 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 $\ell^2 - 2\ell - 1 \stackrel{\circ}{=} 3$, $\exists a \in \mathbb{Z} : \ell^2 - 2\ell - 1 = 3a$. De esta manera, se tiene

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

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 $\forall m \in \mathbb{N} : m^2 - 2m - 1 \not\equiv 3$.



PIM Generalizado

Sea $m_0 \in \mathbb{N}$. Se desea probar ahora: $\forall m \in \mathbb{N} : m \geq m_0 \rightarrow q(m)$. 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:

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

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 $x = (x - 1) + 1 \in S$ ($\rightarrow \leftarrow$). 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 $\ell \in \mathbb{A} \setminus \{m_0\}$ 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 (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”

$$\begin{aligned}\sum_{j=1}^m a_j &= \sum_{j=1}^{m-1} a_j + a_m = a_1 + \sum_{j=2}^m a_j = \sum_{j=1}^{\ell} a_j + \sum_{j=\ell+1}^m a_j, \quad \text{donde } 1 < \ell < m \\ &= \sum_{j=1}^{\ell-1} a_j + a_\ell + \sum_{j=\ell+1}^m a_j, \quad \text{donde } 1 < \ell < m.\end{aligned}$$

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



Sea $\{a_j\}_{j=r}^m \subseteq \mathbb{K}$, siendo \mathbb{K} un conjunto de escalares (reales, ... complejos ...), $r, m \in \mathbb{Z}$, con $r \leq m$. Para abbreviar 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”

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

- 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 $\{a_j\} \subseteq \mathbb{K} \setminus \{0\}$.



El algoritmo de división de Euclides

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

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

Demostración (Existencia)

Sean $a \in \mathbb{Z}_0^+$, $d \in \mathbb{Z}^+$ fijos, pero arbitrarios. Consideraremos 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

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

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, en vista que $d > 0$, resulta $\tilde{r} < r$. Por otro lado,

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

De esta forma, $\tilde{r} \in S$ antecede (en forma estricta) al 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 $a = dq + r = d\tilde{q} + \tilde{r}$. Esto conduce a

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

Por la TRICOTOMÍA EN \mathbb{Z} , puede suceder: $\tilde{r} > r \quad \vee \quad r > \tilde{r} \quad \vee \quad \tilde{r} = r$.

Analizando cada caso (para concluir que $\tilde{r} = r$):

- 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 $d = d \cdot 1 \leq d(q - \tilde{q}) = \tilde{r} - r \stackrel{(r \geq 0)}{\leq} \tilde{r} < d$. Se infiere así que $d < d$ ($\rightarrow \leftarrow$).
- 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 ($d < d$).
- 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)

$\forall (a, d) \in \mathbb{Z} \times \mathbb{Z} \setminus \{0\} : \exists! (q, r) \in \mathbb{Z} \times \mathbb{Z} : a = dq + r$, 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: $b | a$.

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

Por ejemplo: $3 | 6$, pero $3 \nmid 7$. También, $-2 | 6$, $5 | -45$, $-4 | -48$.

Proposición 8 (Primeras propiedades)

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

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

Proposición 9 (Más propiedades)

7) $\forall (a, b) \in (\mathbb{Z} \setminus \{0\})^2 : b | a \Rightarrow |b| \leq |a|.$

8) $\forall (a, b) \in (\mathbb{Z} \setminus \{0\})^2 : b | a \wedge a | b \Rightarrow |b| = |a|.$

9) $\forall (a, b) \in \mathbb{Z}^2 : \forall c \in \mathbb{Z} \setminus \{0\} : (c | a \wedge c | b) \Rightarrow (c | (a + b) \wedge c | (a - b)).$

Definición: MÁXIMO COMÚN DIVISOR (MCD)

Consideremos 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, \dots, a_m , si verifica las condiciones:

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

NOTACIÓN: $d := \text{mcd}(a_1, \dots, a_m)$.

OBSERVACIÓN: El MCD de un conjunto de números es único.

En efecto, si d, \tilde{d} son $\text{mcd}(a_1, \dots, a_m)$, 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: $\text{mcd}(12, 18, 30) = 6$; $\text{mcd}(7, 13, 27, 100) = 1$.



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

Sean $a, b \in \mathbb{Z} \setminus \{0\}$, y sea $d := \text{mcd}(a, b)$. Entonces $\exists (x, y) \in \mathbb{Z}^2 : ax + by = d$.

Demostración

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

$$S := \{z \in \mathbb{Z}^+ \mid \exists (x, y) \in \mathbb{Z}^2 : z = ax + by\} \subseteq \mathbb{Z}^+ \subseteq \mathbb{Z}_0^+,$$

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 $d \in S$, $\exists (x_0, y_0) \in \mathbb{Z}^2 : d = ax_0 + by_0$.

RESTA PROBAR QUE $d = \text{mcd}(a, b)$. Para ello:

- Veamos que $d \mid a$. En efecto, por el ALGORITMO DE LA DIVISIÓN DE EUCLIDES, $\exists !(q, r) \in \mathbb{Z}^2$, con $0 \leq r < d$, tales que $a = qd + r$. 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, $d \mid a$.
- Veamos que $d \mid b$. (invocar 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 $d = \text{mcd}(a, b)$. □

Ejemplo:

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

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

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

Proposición 10

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

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 $\text{mcd}(a, b) = \text{mcd}(b, r)$.

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 $d = mcd(b, r)$. \square

Proposición 12 (Algoritmo del MCD) (Algoritmo de Euclides)

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

$$(q_1, r_1) \in \mathbb{Z} \times \mathbb{Z}_0^+ : a = bq_1 + r_1, \quad 0 < r_1 < b$$

$$(q_2, r_2) \in \mathbb{Z} \times \mathbb{Z}_0^+ : b = r_1 q_2 + r_2, \quad 0 < r_2 < r_1$$

$$(q_3, r_3) \in \mathbb{Z} \times \mathbb{Z}_0^+ : r_1 = r_2 q_3 + r_3, \quad 0 < r_3 < r_2$$

.....

$$(q_m, r_m) \in \mathbb{Z} \times \mathbb{Z}_0^+ : r_{m-2} = r_{m-1} q_m + r_m, \quad 0 < r_m < r_{m-1}$$

$$(q_{m+1}, r_{m+1}) \in \mathbb{Z} \times \mathbb{Z}_0^+ : r_{m-1} = r_m q_{m+1}, \quad (r_{m+1} = 0).$$

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

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

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



OBSERVACIÓN: Del ALGORITMO DEL MCD, se desprende que los residuos inducidos $\{r_j\}$ forman una sucesión estrictamente decreciente en \mathbb{Z}_0^+ , por lo que su último término es CERO. Esto asegura que este algoritmo siempre termina en un número finito de pasos.

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

Aplicando el ALGORITMO DEL MCD resulta

$$2024 = (1972)(1) + 52 \quad (4)$$

$$1972 = (52)(37) + 48 \quad (5)$$

$$52 = (48)(1) + 4 \quad (6)$$

$$48 = (4)(12) + 0 \quad (7)$$

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.

Del paso (6), tenemos $4 = 52 - (48)(1)$.

Ahora, eliminamos 48 del paso (5), y reemplazamos en la expresión anterior. Nos queda

$$4 = 52 - (1972 - (52)(37))(1) = (1972)(-1) + (52)(38) \quad (8)$$

Ahora eliminamos 52 del paso (4). Resulta

$$\begin{aligned} 4 &= (1972)(-1) + (2024 - (1972)(1))(38) = (2024)(38) + (1972)(-39) \\ \Rightarrow 2024(38) + 1972(-39) &= 4. \end{aligned}$$

Proposición 13

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

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

Proposición 14

Sean $a, b \in \mathbb{Z} \setminus \{0\}$. 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

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

Proposición 15

Sea $\{a_j\}_{j=1}^3 \subseteq \mathbb{Z}$. Si $d_2 := mcd(a_1, a_2)$ y $d_3 := mcd(d_2, a_3)$, entonces $d_3 = mcd(a_1, a_2, a_3)$.

Demostración

De la definición de d_3 , tenemos que $d_3|d_2$ y $d_3|a_3$. Como $d_3|d_2$, se infiere que $d_3|a_1$ y $d_3|a_2$. Ahora sea $\tilde{d} \in \mathbb{Z}^+$ tal que $\forall j \in \{1, 2, 3\} : \tilde{d}|a_j$. Resulta $\tilde{d}|d_2$, y como $\tilde{d}|a_3$, entonces $\tilde{d}|d_3$. En consecuencia, $d_3 = mcd(a_1, a_2, a_3)$. \square

La generalización de la propiedad anterior (cuya demostración requiere invocar PIM), se enuncia a continuación:

Proposición 16 (Estrategia para determinar MCD de un conjunto de más de dos enteros)

Para cualquier $m \in \mathbb{Z} \setminus \{1\}$, consideremos $\{a_j\}_{j=1}^m \subseteq \mathbb{Z}$. Si $d_2 := mcd(a_1, a_2)$, $d_3 := mcd(d_2, a_3)$, ..., y $d_m := mcd(d_{m-1}, a_m)$, entonces $d_m = mcd(a_1, a_2, \dots, a_m)$.

Ejemplo: Determinar $mcd(40, 60, 100)$

Tenemos: $d_2 = mcd(40, 60) = 20$, $d_3 := mcd(d_2, 100) = mcd(20, 100) = 20$. Luego, invocando la Proposición 15, se concluye que $mcd(40, 60, 100) = d_3 = 20$.

Definición: Mínimo Común Múltiplo (MCM)

Considere el conjunto $C := \{a_j\}_{j=1}^m \subseteq \mathbb{Z} \setminus \{0\}$. Se dice que $k \in \mathbb{Z}^+$ es MÍNIMO COMÚN MÚLTIPLO de a_1, \dots, a_m , si verifica las condiciones:

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

Es decir, el MCM de $\{a_j\}_{j=1}^m$ es el menor entero positivo que es múltiplo de todos los números $\{a_j\}_{j=1}^m$.

NOTACIÓN: $k := mcm(a_1, \dots, a_m)$.

EJEMPLOS: $mcm(40, 60, 100) = 600$, $mcm(-150, 625) = 3750$.



Proposición 17: $\forall (a, b) \in \mathbb{Z}^+ \times \mathbb{Z}^+ : mcd(a, b) \cdot mcm(a, b) = a \cdot b$.

DEMOSTRACIÓN: Sea $(a, b) \in \mathbb{Z}^+ \times \mathbb{Z}^+$ fijo, pero arbitrario. Como $a | mcm(a, b)$, $\exists c \in \mathbb{Z}^+ : mcm(a, b) = ac$. Por otro lado, $b | mcm(a, b)$. En consecuencia, la división entre ac y b es EXACTA.

Consideremos ahora $d := mcd(a, b)$. Esto implica que

$\exists (a_1, b_1) \in \mathbb{Z}^+ \times \mathbb{Z}^+ : a = a_1 d \wedge b = b_1 d$. Además, $mcd(a_1, b_1) = 1$ (*¿por qué?*).

Tenemos así: $\frac{ac}{b} = \frac{a_1 d c}{b_1 d} = \frac{a_1 c}{b_1} \in \mathbb{Z}^+$. De esta manera, se infiere que $b_1 | c$, con lo cual

$\exists k \in \mathbb{Z}^+ : c = b_1 k = \frac{b}{d} k$. Esto conduce a $mcm(a, b) = ac = \frac{ab}{d} k$, con $\frac{ab}{d} \in \mathbb{Z}^+$.

Notamos que $\frac{ab}{d}$ es un múltiplo de a y de b . Por definición de MCM, $mcm(a, b) | \frac{ab}{d}$. Esto asegura que $\exists \ell \in \mathbb{Z}^+ : \frac{ab}{d} = mcm(a, b) \ell = \frac{ab}{d} k \ell$. De aquí se desprende que $k \ell = 1$.

Siendo $k, \ell \in \mathbb{Z}^+$, la única posibilidad es: $k = \ell = 1$. De esta forma, resulta

$\frac{ab}{d} = mcm(a, b)$, es decir $mcd(a, b) \cdot mcm(a, b) = a \cdot b$.

FINALMENTE, como $(a, b) \in \mathbb{Z}^+ \times \mathbb{Z}^+$ es fijo pero arbitrario, queda establecida la validez de la propiedad. □

Corolario 18: $\forall (a, b) \in \mathbb{Z}^+ \times \mathbb{Z}^+ : mcd(a, b) = 1 \Rightarrow mcm(a, b) = a \cdot b$.

EN GENERAL: $\forall (a, b) \in (\mathbb{Z} \setminus \{0\}) \times (\mathbb{Z} \setminus \{0\}) : mcd(a, b) \cdot mcm(a, b) = |ab|$.

Definición (Números coprimos)

Sean $a, b \in \mathbb{Z} \setminus \{0\}$. Se dice que a y b son PRIMOS RELATIVOS, COPRIMOS o PRIMOS ENTRE SÍ (PESI), si $mcd(a, b) = 1$.

Proposición 19

Sea $\{a_j\}_{j=1}^3 \subseteq \mathbb{Z}^+$. Si $k_2 := mcm(a_1, a_2)$ y $k_3 := mcm(k_2, a_3)$, entonces $k_3 = mcm(a_1, a_2, a_3)$.

Demostración:

De la definición de k_3 , tenemos que $k_2|k_3$ y $a_3|k_3$. Como $k_2|k_3$, se infiere que $a_1|k_3$ y $a_2|k_3$. Ahora sea $\tilde{k} \in \mathbb{Z}^+$ tal que $\forall j \in \{1, 2, 3\} : a_j|\tilde{k}$. Resulta $k_2|\tilde{k}$, y como $a_3|\tilde{k}$, entonces $k_3|\tilde{k}$. En consecuencia, $k_3 = mcm(a_1, a_2, a_3)$. \square

La generalización de la propiedad anterior (cuya demostración requiere invocar PIM), se enuncia a continuación:

Proposición 20: (Estrategia para determinar MCM de un conjunto de más de dos enteros)

Para cualquier $m \in \mathbb{Z} \setminus \{1\}$, consideremos $\{a_j\}_{j=1}^m \subseteq \mathbb{Z}^+$. Si $k_2 := mcm(a_1, a_2)$, $k_3 := mcm(k_2, a_3)$, ..., y $k_m := mcm(k_{m-1}, a_m)$, entonces $k_m = mcm(a_1, a_2, \dots, a_m)$.



... hacia el Teorema Fundamental de la Aritmética

Definición: Número primo y número compuesto

Decimos que $p \in \mathbb{N} \setminus \{1\}$ 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 $\exists m_1, m_2 \in \mathbb{N} \setminus \{1, m\} : m = m_1 m_2$.

Ejemplos

Números primos: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, ...

Números compuestos: 4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20, 22, 24, 25, 26, 27, 28, 30, ...

Proposición 21: Caracterización de números primos

$\forall p \in \mathbb{N} \setminus \{1\} : p$ es primo si y sólo si $\forall (a, b) \in \mathbb{Z}^+ \times \mathbb{Z}^+ : p|ab \Rightarrow (p|a \vee p|b)$.

Demostración:

Sea $p \in \mathbb{N} \setminus \{1\}$ fijo, pero arbitrario.

(\Rightarrow) HIPÓTESIS: p es primo.

Ahora, consideremos $(a, b) \in \mathbb{Z}^+ \times \mathbb{Z}^+$ fijo, pero arbitrario, tal que $p|ab$.

- Caso: $p|a$ o $p|b$, no hay más nada que probar.

Demostración (continuación)

- Caso: $p \nmid a$. Se infiere que $\text{mcd}(p, a) = 1$. Luego, invocando el Lema de Bézout, $\exists (\alpha, \beta) \in \mathbb{Z} \times \mathbb{Z} : \alpha p + \beta a = 1$. Multiplicando por b , resulta $\alpha pb + \beta ab = b$. Como $p|\alpha pb$ y $p|\beta ab$, se deduce que $p|(\alpha pb + \beta ab)$, es decir $p|b$.
- Caso: $p \nmid b$. Se procede de manera similar al caso anterior. Por tanto, se concluye que $p|a$.

En vista que $(a, b) \in \mathbb{Z}^+ \times \mathbb{Z}^+$ es fijo pero arbitrario, se establece

$$\forall (a, b) \in \mathbb{Z}^+ \times \mathbb{Z}^+ : p|ab \Rightarrow (p|a \vee p|b).$$

(\Leftarrow) HIPÓTESIS: $\forall (a, b) \in \mathbb{Z}^+ \times \mathbb{Z}^+ : p|ab \Rightarrow (p|a \vee p|b)$.

Sea $a \in \mathbb{Z}^+$ un factor de p . Luego, $\exists b \in \mathbb{Z}^+ : p = ab$. Como $p|ab$, resulta (por hipótesis) que $p|a \vee p|b$.

- Caso: $p|a$. Como $a|p$, resulta $|p| = |a|$, es decir $a = p$. De esta manera, se deduce que $b = 1$. Es decir, los únicos factores enteros positivos de p son 1 y p . Por tanto, p es un número primo.
- Caso: $p|b$. Luego, $\exists c \in \mathbb{Z}^+ : b = pc$. De esta manera,

$$p = ab = apc \Leftrightarrow ac = 1 \Leftrightarrow a = 1 = c.$$

Así, se deduce que $b = p$. Es decir, los únicos factores enteros positivos de p son 1 y p . Por tanto, p es un número primo.

Finalmente, como ambos casos conducen a la misma conclusión, se completa la demostración. □

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 22 (Teorema Fundamental de la Aritmética)

$\forall m \in \mathbb{N} \setminus \{1\}$: m es primo ó m se puede descomponer como multiplicación de números primos (con posibles repeticiones de algunos de ellos como factores). Esta descomposición es única, salvo por el orden de los factores.

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).



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 $\mathbb{A} := \mathbb{N} \setminus \{1\}$ 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 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, con posible repetición), 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 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 (4ta forma), $S = \mathbb{A}$, y concluye la demostración. □

Demostración...la unicidad, salvo el orden de los factores

Sea $m \in \mathbb{A}$ fijo, pero arbitrario.

- Caso m es un número primo. Inmediato.
- Caso m es un número compuesto. Supongamos que existen conjuntos de números primos $\{p_1, \dots, p_r\}$ y $\{q_1, \dots, q_s\}$ (con posibles repeticiones), tales que $m = p_1 \cdots p_r = q_1 \cdots q_s$. Sin pérdida de generalidad, supondremos que $r \leq s$, y que los conjuntos de primos dados, están ordenados en forma no decreciente. Como p_1 es un factor primo de m , $p_1 | q_1 \cdots q_s$. Siendo q_1 el menor de los factores primos de m , se infiere que necesariamente $p_1 = q_1$. Esto conduce a la igualdad $p_2 \cdots p_r = q_2 \cdots q_s$. Repitiendo el proceso, se deduce que $\forall j \in \{1, \dots, r\} : p_j = q_j$ y también que $r = s$. En caso contrario, la igualdad nos quedaría $1 = q_{r+1} \cdots q_s$. Esto implica que $q_{r+1} = \cdots = q_s = 1$ ($\rightarrow \leftarrow$). Esto nos conduce a decir que la factorización de m (fijado el orden de los factores primos), es única.
Finalmente, como $m \in \mathbb{A}$ es fijo pero arbitrario, se concluye la unicidad referida.



Corolario 23 (inmediato)

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

Teorema 24 (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 22** y

COROLARIO 23 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 $\forall j \in \{1, \dots, m_0\} : z > p_j$. 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, $\exists j_0 \in \{1, \dots, m_0\} : p_{j_0} | z$. Luego, $p_{j_0} | \left(z - \prod_{j=1}^{m_0} p_j \right)$, 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

El griego Eratóstenes dió una sencilla pero eficaz regla para determinar los primos comprendidos entre 2 y un número positivo $n > 1$. En lo que sigue introducimos $\mathbb{P} := \{q \in \mathbb{Z}^+ : q \text{ es primo}\}$. Recordar $2, 3, 5, 7, 11, 13, 17, 19 \in \mathbb{P}$.

Proposición 25 (Criba de Eratóstenes)

$$\forall n \in \mathbb{N} \setminus \{1, 2\} : n \text{ es un número compuesto si y sólo si } \exists p \in \mathbb{P} \cap (1, \sqrt{n}] : p|n.$$

Demostración:

Sea $n \in \mathbb{N} \setminus \{1, 2\}$ fijo, pero arbitrario.

(\Rightarrow) HIPÓTESIS: n es compuesto. Invocando el TEOREMA FUNDAMENTAL DE LA ARITMÉTICA, n puede descomponerse como multiplicación de factores primos. Sea $p \in \mathbb{P}$ el menor factor primo de n . Luego, $\exists q \in \mathbb{Z}^+ : n = pq \wedge p \leq q$.

Relación de orden en \mathbb{R} : $\sqrt{n} < p \vee p \leq \sqrt{n}$.

- Caso: $\sqrt{n} < p$. Tenemos: $n < p^2 = p \cdot p \leq p \cdot q = n$. Esto implica que $n < n$, lo que es una contradicción.
- Por Descartes, se debe cumplir $p \leq \sqrt{n}$, y se concluye la TESIS.

(\Leftarrow) HIPÓTESIS: $\exists p \in \mathbb{P} \cap (1, \sqrt{n}] : p|n$.

Se infiere en forma inmediata que n admite un factor primo $p < n$. Esto conduce a decir que n es un número compuesto.

Finalmente, como $n \in \mathbb{N} \setminus \{1, 2\}$ es fijo pero arbitrario, se concluye la validez de la propiedad.



A continuación, unos ejemplos de aplicación:

- Veamos si $n = 31$ es un número primo o no. Tenemos $\{p \in \mathbb{P} : p \leq \sqrt{31} < \sqrt{36} = 6\} = \{2, 3, 5\}$. Resulta

$$31 = (2)(15) + 1$$

$$31 = (3)(10) + 1$$

$$31 = (5)(6) + 1.$$

En consecuencia, $n = 31$ no es número compuesto, es decir 31 es un número primo.

- Veamos si $n = 313$ es un número primo o no. Tenemos $\{p \in \mathbb{P} : p \leq \sqrt{313} < \sqrt{324} = 18\} = \{2, 3, 5, 7, 11, 13, 17\}$. Resulta

$$313 = (2)(156) + 1$$

$$313 = (3)(104) + 1$$

$$313 = (5)(62) + 3$$

$$313 = (7)(44) + 5$$

$$313 = (11)(28) + 5$$

$$313 = (13)(24) + 1$$

$$313 = (17)(18) + 7.$$

En consecuencia, $n = 313$ no es número compuesto, es decir 313 es un número primo.



Determinando mcd y mcm de dos números (regla práctica)

Sean $a, b \in \mathbb{Z}^+$. Por el TEOREMA FUNDAMENTAL DE LA ARITMÉTICA, tenemos que $\exists \{p_j\}_{j=1}^r \subseteq \mathbb{P}$ (subconjunto de números primos todos distintos entre sí) tales que

$$\exists \{m_j\}_{j=1}^r \subseteq \mathbb{Z}_0^+ : a = \prod_{j=1}^r p_j^{m_j},$$

$$\exists \{n_j\}_{j=1}^r \subseteq \mathbb{Z}_0^+ : b = \prod_{j=1}^r p_j^{n_j}.$$

Entonces

$$mcd(a, b) = \prod_{j=1}^r p_j^{\alpha_j}, \text{ donde } \forall j \in \{1, \dots, r\} : \alpha_j := \min(m_j, n_j),$$

$$mcm(a, b) = \prod_{j=1}^r p_j^{\beta_j}, \text{ donde } \forall j \in \{1, \dots, r\} : \beta_j := \max(m_j, n_j).$$

Ejemplo

$$\begin{cases} 600 = \dots = 2^3 \cdot 3 \cdot 5^2 = 2^3 \cdot 3^1 \cdot 5^2 \cdot 7^0 \\ 315 = \dots = 3^2 \cdot 5 \cdot 7 = 2^0 \cdot 3^2 \cdot 5^1 \cdot 7^1. \end{cases} \Rightarrow \begin{cases} mcd(600, 315) = 2^0 \cdot 3^1 \cdot 5^1 \cdot 7^0 = 15 \\ mcm(600, 315) = 2^3 \cdot 3^2 \cdot 5^1 \cdot 7^2 = 12600. \end{cases}$$

Problemas de aplicación de MCD y MCM

- 1 En la tienda de Manuel hay una caja con 12 naranjas y otra con 18 peras. Manuel quiere distribuir las frutas en cajas más pequeñas de forma que:
- todas las cajas tienen el mismo número de frutas,
 - cada caja sólo puede tener peras o naranjas y
 - las cajas deben contener la mayor cantidad de frutas posible.

¿Cuántas frutas deben haber en cada caja? ¿Cuántas cajas se requerirán?

- 2 Carolina quiere coser una colcha collage con retales de tela cuadrados del mayor tamaño posible y que tengan el mismo tamaño (longitud medida en \mathbb{Z} , en [cm]). Si la colcha tiene que medir 180 cm. de alto y 100 cm. de ancho, ¿cuánto deben medir los retales? ¿Cuántos retales se tienen que recortar para coser la colcha?
- 3 En una calle se están instalando dos semáforos: uno de ellos se pondrá en verde cada 3 minutos y el otro, cada 5 minutos. Una vez se conectan los semáforos en simultáneo, ¿cada cuánto tiempo tardarán en ponerse en verde al mismo tiempo?
- 4 Juan y Marta van a correr alrededor de una urbanización de su ciudad, partiendo siempre juntos del mismo lugar. Juan tarda 16 minutos en dar una vuelta completa y Marta tarda 24 minutos. Cuando coincidan en el punto de partida por primera vez, ¿cuántas vueltas habrá dado cada uno?



Ecuaciones Diofánticas Lineales (Diofanto de Alejandría - siglo III - IV)

Sean $a, b, c \in \mathbb{Z}$ dados. Interesa estudiar la ECUACIÓN DIOFÁNTICA LINEAL:
Determinar $(x, y) \in \mathbb{Z}^2 : ax + by = c$.

Proposición 26

La ecuación diofántica planteada tiene soluciones enteras si y sólo si $mcd(a, b) | c$.

Resolviendo Ecuaciones Diofánticas Lineales Homogéneas

Sean $a, b \in \mathbb{Z}$, no nulos a la vez, con los cuales se plantea la ECUACIÓN DIOFÁNTICA LINEAL HOMOGÉNEA: Determinar $(x, y) \in \mathbb{Z}^2 : ax + by = 0$.

Considerando $d := mcd(a, b)$, se puede deducir que el conjunto solución de esta ecuación viene dado por $C.S. = \left\{ (x, y) = \left(\frac{b}{d}m, -\frac{a}{d}m \right) \in \mathbb{Z}^2 \mid m \in \mathbb{Z} \right\}$.

Resolviendo Ecuaciones Diofánticas Lineales No Homogéneas

Sean $a, b \in \mathbb{Z}$, no nulos a la vez, y $c \in \mathbb{Z} \setminus \{0\}$, con los cuales se plantea la ECUACIÓN DIOFÁNTICA LINEAL NO HOMOGÉNEA: Determinar $(x, y) \in \mathbb{Z}^2 : ax + by = c$.

Supongamos que la ecuación diofántica planteada es soluble, y $(x_0, y_0) \in \mathbb{Z}^2$ es una solución de ésta. Considerando $d := mcd(a, b)$, se puede deducir que el conjunto solución de esta ecuación viene dado por $C.S. = \left\{ (x, y) = \left(x_0 + \frac{b}{d}m, y_0 - \frac{a}{d}m \right) \in \mathbb{Z}^2 \mid m \in \mathbb{Z} \right\}$.

Otras ecuaciones diofánticas

Determinar $(w, x, y, z) \in (\mathbb{Z}^+)^4 : w^3 + x^3 = y^3 + z^3$

Solución no trivial más pequeña: $12^3 + 1^3 = 9^3 + 10^3 = 1729$ (número de Ramanujan-Hardy, 1917)

Se ha demostrado que tiene un número infinito de soluciones no triviales.

Determinar $(x, y, z) \in (\mathbb{Z}^+)^3 : x^2 + y^2 = z^2$...la tripleta de Pitágoras

Se sabe/conocen que tiene infinitas soluciones no triviales.

Dado $n \in \mathbb{Z} \setminus \{1, 2\}$, determinar $(x, y, z) \in (\mathbb{Z}^+)^3 : x^n + y^n = z^n$...el último teorema de Fermat o la conjetura de Fermat (1637)...quien afirmó que no tiene solución, pero la demostración nunca fue encontrada

Andrew Wiles (matemático inglés) demostró en 1995 que este problema no tiene solución.



Algunos resultados acerca de la distribución de los números primos

Fórmula que genera todos los números primos

- El polinomio $g(m) := m^2 - m + 41$ entrega números primos para $m \in \{0, 1, 2, \dots, 40\}$. Sin embargo, $g(41) = 41^2$.
- CONJETURA DE LOS NÚMEROS DE FERMAT: $\forall m \in \mathbb{Z}_0^+ : F_m := 2^{2^m} + 1$ es primo. $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ y $F_4 = 65537$ son primos. Euler probó que $F_5 = (641)(6700417)$, con lo cual la conjetura es FALSA. F_6, \dots, F_{32} son compuestos. Hasta mediados de 2015, el número de Fermat más pequeño que no se sabe si es primo o compuesto es F_{33} . El número compuesto de Fermat más grande que se conoce es F_{332980} , que es divisible por $(193)(2^{3329782} + 1)$. Esto da pie a otras conjeturas: ¿Sólo existen cinco números primos de Fermat? ¿Existen infinitos números primos de Fermat?

Recordando que \mathbb{P} denota el conjunto de todos los números primos.

Postulado de Joseph Bertrand (matemático francés) (en 1845)

$$\forall m \in \mathbb{N} \setminus \{1\} : \exists p \in \mathbb{P} : m < p < 2m.$$

- Bertrand verificó su certeza para $2 \leq m \leq 3000000$.
- En 1850, Chebyshev demostró la conjetura, dando lugar al TEOREMA DE BERTRAND-CHEBYSHEV o TEOREMA DE CHEBYSHEV.

Otro problema abierto y algunos resultados recientes sobre los primos

Teorema de los números primos

Sea $x \in \mathbb{R}^+$, y designemos por $\pi(x)$ la cantidad de números primos $\leq x$. Entonces $\pi(x) \sim \frac{x}{\ln(x)} \Leftrightarrow \lim_{x \rightarrow +\infty} \frac{\pi(x)}{x/\ln(x)} = 1$.

- Conjeturado por Legendre en 1798.
- Demostrado en 1896, en forma paralela, por Jacques Hadamard y Charles Jean de la Vallée Poussin, usando ideas de Bernhard Riemann (la función zeta de Riemann).

Los primos gemelos

Sean p, q números primos. Se dice que p y q son PRIMOS GEMELOS si $|p - q| = 2$. Por ejemplo, 3 y 5, 5 y 7, 11 y 13, 17 y 19, 29 y 31, etc.

¿Existen infinitas parejas de primos gemelos?

Formulado ya por los griegos, es uno de los problemas más antiguos de la Matemática que, sin embargo, todavía espera su solución.

Conjetura

La sucesión de números primos contiene progresiones aritméticas arbitrariamente largas.

Teorema (B. Green, T. Tao, 1998)

$\forall m \in \mathbb{N} \setminus \{1, 2\}$: existen m números primos en progresión aritmética.

En una carta dirigida a Euler (matemático suizo) en 1742, Goldbach (matemático prusiano) afirmó haber observado:

- Todo entero par mayor que 2 es la suma de dos primos (Conjetura fuerte - problema binario de Goldbach).
- Todo entero impar mayor que 5 es la suma de tres primos (Conjetura débil - problema ternario de Goldbach).

...sobre el problema binario de Goldbach

Se cree que los métodos actuales son insuficientes para resolverla. Sólo se ha podido comprobar con la ayuda de computadores para todos los números pares menores que 10^{18} .

...sobre el problema ternario de Goldbach

- Vinogradov (matemático ruso) demostró en 1937 que todo entero impar mayor que la constante $C_1 = 10^{300}$ se puede expresar como la adición de tres números primos. Pero la gran magnitud de C_1 hace impracticable comprobar la conjetura para los impares menores que C_1 , aún con la ayuda del computador (o todos los computadores posibles del mundo).
- En 2013, Harald Helfgott (matemático peruano) pudo reducir dicha constante a $C_2 = 10^{30}$, con lo cual sí fue factible validar la conjetura para los números enteros impares menores que dicho valor....le tomó 3 meses con la ayuda de potentes computadores. Así, quedó demostrada la CONJETURA DÉBIL DE GOLDBACH.

Magnitud del mayor factor primo de enteros de la forma $m^2 + 1$

Para cada $k \in \mathbb{Z} \setminus \{0\}$, denotamos por $\mathcal{P}(k)$ el mayor factor primo de k . Por convención $\mathcal{P}(\pm 1) = 1$.

PROBLEMA: dado $m \in \mathbb{Z}^+$, interesa conocer cuán grande puede ser $\mathcal{P}(m^2 + 1)$.

- En 1934, Chowla demostró que $\exists C > 0 : \forall m \in \mathbb{Z}^+ : \mathcal{P}(m^2 + 1) \geq C \log_2(m)$.
- En 1976, Sorey and Tijdeman demostraron que
 $\exists C > 0 : \forall m \in \mathbb{Z}^+ : \mathcal{P}(m^2 + 1) \geq C \left(\frac{\log_3(m)}{\log_4(m)} \right) \log_2(m).$
- En 2024 (*Inventiones mathematicae* (2024) 236:373-385), Héctor Pastén (matemático chileno, ex-UdeC, actualmente profesor PUC), demostró que
 $\exists C > 0 : \forall m \in \mathbb{Z}^+ : \mathcal{P}(m^2 + 1) \geq C \frac{(\log_2(m))^2}{\log_3(m)}.$

