Álgebra I

Contenidos

1. Lógica y teoría de conjuntos . . . 3
   - Conectores lógicos . . . 3
   - Teoría de conjuntos elemental . . . 3
   - Operaciones de conjuntos . . . 4
2. Relaciones y funciones . . . 6
   - Relaciones de orden . . . 6
   - Relaciones de equivalencia . . . 6
   - Funciones . . . 7
   - Inyecciones, suryecciones y biyecciones . . . 9
   - Coordinabilidad de conjuntos . . . 9
3. Inducción . . . 10
   - Teorema de inducción . . . 10
   - Principio de inducción y principio de inducción generalizada . . . 10
   - Sumatorias y productorias . . . 11
   - Progresiones aritméticas y geométricas . . . 11
   - Principio de buena ordenación . . . 13
   - Principio de inducción global o inducción fuerte . . . 13
   - Cardinalidad y conjuntos finitos e infinitos . . . 14
   - Principio del palomar . . . 15
   - Principio de inclusión-exclusión . . . 16
4. Combinatoria . . . 18
   - Principio multiplicativo . . . 18
   - Variaciones, permutaciones y combinaciones . . . 19
   - Números combinatorios . . . 20
   - Fórmula binomial de Newton . . . 21
   - Probabilidad . . . 23
5. Teoría de números elemental . . . 24
   - Divisibilidad . . . 24
   - Algoritmo de división entera . . . 25
   - Congruencia módulo n . . . 26
   - Máximo común divisor . . . 27
   - Algoritmo de Euclides . . . 27
   - Combinaciones lineales y números coprimos . . . 27
   - Lema de Euclides . . . 29
   - Ecuaciones lineales diofánticas y la identidad de Bézout . . . 30

Ecuaciones lineales de congruencia 30
Números primos 32
Teorema fundamental de la aritmética 33
Mínimo común múltiplo 34
Teorema chino del resto 35
Pequeño teorema de Fermat 35
Orden multiplicativo 36
6. El cuerpo de números complejos $\mathbb{C}$ 37
La unidad imaginaria i 37
Distancia en $\mathbb{C}$ y conjugados 38
Forma trigonométrica 40
Fórmula de de Moivre 40
Raíces n-ésimas de un complejo no nulo 41
El grupo G_n de raíces de la unidad 41
Raíces primitivas de la unidad 43
6. Polinomios 45
Suma y producto de polinomios 45
Algoritmo de la división en $\mathbb{K}[x]$ 46
Especialización de polinomios y el teorema del resto 47
Multiplicidad de raíces 49
Polinomio derivado 49
Criterio de raíces racionales de Gauss 50
Apéndice: Sucesión de Fibonacci 51

1. Lógica y teoría de conjuntos

Definición 1.1. Dada una proposición p, entendemos por $v(p)$ al valor de verdad de p.

Definición 1.2. Dadas las proposiciones p y q, definimos los siguientes conectores lógicos:
(1) *Negación* ($\sim$): $\sim p$ se cumple si no se cumple p
(2) *Conjunción* ($\wedge$): $p \wedge q$ se cumple si se cumplen tanto p como q
(3) *Disyunción* ($\vee$): $p \vee q$ se cumple si se cumple p o bien se cumple q
(4) *Condicional* ($\Rightarrow$): $p \Rightarrow q$ se cumple siempre y cuando no ocurra el hecho de que se cumple p pero no q simultáneamente
(5) *Bicondicional* ($\iff$): $p \iff q$ se cumple siempre que $v(p) = v(q)$

Definición 1.3. Entendemos por *conjunto* a una colección de objetos, a la que llameremos *elementos*. Si x es un elemento de un conjunto A, notamos $x \in A$.
Decimos que un conjunto A es un *subconjunto* de un conjunto B, o bien que A está *contenido* en B si $(x \in A) \Rightarrow (x \in B)$ y lo notamos $A \subseteq B$.

Definición 1.4. Dado un conjunto A, p se dice *predicable sobre* A si posee un valor de verdad para todo $x \in A$

Proposición 1.1. Dados los conjuntos A y B, $A = B$ si y sólo si $(A \subseteq B) \wedge (B \subseteq A)$, o equivalentemente, $(x \in A) \iff (x \in B)$.

Dem. $(A \subseteq B) \wedge (B \subseteq A)$ es equivalente a $\big((x \in A) \Rightarrow (x \in B)\big) \wedge \big((x \in B) \Rightarrow (x \in A)\big)$ por definición. Entonces $(x \in A) \iff (x \in B)$. Es fácil ver que, si esto se cumple, $A = B$ ya que, en caso contrario, debería existir $x \in A$ tal que $x \notin B$ o viceversa, violando las hipótesis planteadas. Recíprocamente, $A = B$ implica $(x \in A) \iff (x \in B)$. □

Definición 1.5. Definimos un conjunto $\mathcal{U}$, denominado *conjunto universal* o *conjunto de referencia*, como el conjunto del cual todo otro conjunto con el que estemos trabajando sea un subconjunto (para así poder evitar contradicciones como la paradoja de Rusell).

Definición 1.6. Llamamos *conjunto vacío* a aquel conjunto que no posee ningún elemento, y lo notamos $\emptyset$

Definición 1.7. Dado un conjunto A, definimos al *conjunto de partes de* A (también llamado *conjunto de potencias de* A), al que notamos $\mathcal{P}(A)$, como:

$$\mathcal{P}(A) = \{X : X \subseteq A\}$$

Definición 1.8. Dado un conjunto A, definimos al *complemento de* A, al que notamos A^c o bien A', como:

$$A^c = \{x \in \mathcal{U} : x \notin A\}$$

Operaciones de conjuntos

Definición 1.9. Dados los conjuntos A y B, definimos a la *intersección de A y B*, a la que notamos $A \cap B$, como:

$$A \cap B = \{x \in \mathcal{U} : (x \in A) \wedge (x \in B)\}$$

Si $A \cap B = \emptyset$ decimos que A y B son *disjuntos*.

Propiedades. Dados $A, B, C \subseteq \mathcal{U}$, se verifica que:

(1) $(A \cap B) \cap C = A \cap (B \cap C)$ (asociatividad)
(2) $A \cap B = B \cap A$ (conmutatividad)
(3) $(A \cap B) \subseteq A$ y $(A \cap B) \subseteq B$
(4) $\big((A \cap B) = A\big) \iff (A \subseteq B)$
(5) $(A \cap A) = A$
(6) $(A \cap A^c) = \emptyset$
(7) $(A \cap \emptyset) = \emptyset$
(8) $(A \cap \mathcal{U}) = A$

Definición 1.10. Dados los conjuntos A y B, definimos a la *unión de A y B*, a la que notamos $A \cup B$, como:

$$A \cup B = \{x \in \mathcal{U} : (x \in A) \vee (x \in B)\}$$

Propiedades. Dados $A, B, C \subseteq \mathcal{U}$, se verifica que:

(1) $(A \cup B) \cup C = A \cup (B \cup C)$ (asociatividad)
(2) $A \cup B = B \cup A$ (conmutatividad)
(3) $A \subseteq (A \cup B)$ y $B \subseteq (A \cup B)$
(4) $\big((A \cup B) = B\big) \iff (A \subseteq B)$
(5) $(A \cup A) = A$
(6) $(A \cup A^c) = \mathcal{U}$
(7) $(A \cup \emptyset) = A$
(8) $(A \cup \mathcal{U}) = \mathcal{U}$

Leyes de DeMorgan. Dados $A, B, C \subseteq \mathcal{U}$, se verifica que:

(1) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
(2) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
(3) $(A \cap B)^c = (A^c \cup B^c)$
(4) $(A \cup B)^c = (A^c \cap B^c)$

Definición 1.11. Dados los conjuntos A y B, definimos a la *diferencia entre A y B*, a la que notamos $A - B$, como:

$$A - B = \{x \in \mathcal{U} : (x \in A) \wedge (x \notin B)\}$$

Propiedades. Dados $A, B \subseteq \mathcal{U}$, se verifica que:

(1) $(A - B) \subseteq A$
(2) $\big((A - B) = A\big) \iff \big((B - A) = B\big) \iff A$ y B son disjuntos
(3) $\big((A - B) = \emptyset\big) \iff (A \subseteq B)$
(4) $(A - A) = \emptyset$
(4) $(A - A^c) = A$
(6) $(A - \emptyset) = A$
(7) $(A - \mathcal{U}) = \emptyset$
(8) $(A - B) = (A \cap B^c)$

Definición 1.12. Dados los conjuntos A y B, definimos a la *diferencia simétrica entre A y B*, a la que notamos $A \triangle B$, como:

$$A \triangle B = \{x \in \mathcal{U} : (x \in A - B) \vee (x \in B - A)\} = (A - B) \cup (B - A)$$

Propiedades. Dados $A, B, C \subseteq \mathcal{U}$, se verifica que:

(1) $(A \triangle B) \triangle C = A \triangle (B \triangle C)$ (asociatividad)
(2) $A \triangle B = B \triangle A$ (conmutatividad)
(3) $A \triangle B = (A \cup B) - (A \cap B)$
(4) $\big((A \triangle B) = (A \cup B)\big) \iff A$ y B son disjuntos
(5) $A \cap (B \triangle C) = (A \cap B) \triangle (A \cap C)$
(6) $(A \triangle A) = \emptyset$
(7) $(A \triangle A^c) = \mathcal{U}$
(8) $(A \triangle \emptyset) = A$
(9) $(A \triangle \mathcal{U}) = A^c$

Definición 1.13. Dada una familia $(\mathcal{A}_i)_{i \in I}$ de conjuntos, definimos su *intersección*, notada $\bigcap_{i \in I}$, como:

$$\bigcap_{i \in I} = \{x \in \mathcal{U} : (\forall i \in I) x \in \mathcal{A}_i\}$$

y su *unión*, notada $\bigcup_{i \in I}$, como:

$$\bigcup_{i \in I} = \{x \in \mathcal{U} : (\exists i \in I) x \in \mathcal{A}_i\}$$

Definición 1.14. Dados los conjuntos A y B, definimos a su *producto cartesiano*, notado $A \times B$, como:

$$A \times B = \{(a, b) : a \in A, b \in B\}$$

Más generalmente, dados los conjuntos $A_1, A_2, \ldots, A_n$ (con $n \in \mathbb{N}$), su producto cartesiano $A_1 \times A_2 \times \cdots \times A_n$ es el conjunto de todas las n-uplas $(m_1, m_2, \ldots, m_n)$ donde $m_1 \in A_1, m_2 \in A_2, \ldots, m_n \in A_n$ respectivamente.

2. Relaciones y funciones

Definición 2.1. Dados A y B conjuntos, llamamos *relación de A en B* a cualquier subconjunto $\mathcal{R}$ de $A \times B$.
Si $(a, b) \in \mathcal{R}$, notamos $a\mathcal{R}b$ y decimos que *a está relacionado con b*.
Si $\mathcal{R}$ es una relación de A en A, simplemente decimos que $\mathcal{R}$ es una *relación en A*.

Definición 2.2. Dada una relación $\mathcal{R}$ de A en B, definimos al *dominio de $\mathcal{R}$*, notado $\mathrm{Dom}(\mathcal{R})$, como:

$$\mathrm{Dom}(\mathcal{R}) = \{x \in A : (\exists y \in B) \text{ tal que } x\mathcal{R}y\}$$

y al *codominio de $\mathcal{R}$*, notado $\mathrm{Cod}(\mathcal{R})$, como:

$$\mathrm{Cod}(\mathcal{R}) = \{x \in B : (\exists y \in A) \text{ tal que } y\mathcal{R}x\}$$

Observación. Para cualquier relación $\mathcal{R}$ de A en B, $\mathrm{Dom}(\mathcal{R}) \subseteq A$ y $\mathrm{Cod}(\mathcal{R}) \subseteq B$.
Además, $\mathrm{Dom}(\mathcal{R}) = \emptyset$ y $\mathrm{Cod}(\mathcal{R}) = \emptyset$ si y sólo si $\mathcal{R} = \emptyset$

Definición 2.3. Dada una relación $\mathcal{R}$ en A en B, decimos que $\mathcal{R}$ es:
(1) *reflexiva* si $(\forall x \in A)x\mathcal{R}x$
(2) *simétrica* si $x\mathcal{R}y \iff y\mathcal{R}x$, con $x, y \in A$
(3) *transitiva* si $(x\mathcal{R}y \wedge y\mathcal{R}z) \Rightarrow x\mathcal{R}z$, con $x, y, z \in A$
(4) *antisimétrica* si $(x\mathcal{R}y \wedge y\mathcal{R}x) \iff x = y$

Definición 2.4. Una relación reflexiva, antisimétrica y transitiva $\mathcal{R}$ en un conjunto A se dice una *relación de orden*. Dicho orden se dice *total* si se cumple la ley de tricotomía, es decir, para todo $x, y \in A$ se cumple que $x\mathcal{R}y$ o bien $y\mathcal{R}x$.

Observación. La relación $\geq$ es un orden total sobre $\mathbb{R}$; la relación $\subseteq$ es un orden no total sobre $\mathcal{P}(X)$

Dem. Es fácil ver que, para todo $x, y, z \in \mathbb{R}$, se verifica que:
(1) $x \geq x$
(2) $(x \geq y \wedge y \geq x) \iff x = y$
(3) $(x \geq y \wedge y \geq z) \Rightarrow x \geq y$
(4) $x \geq y$ o bien $y \geq x$
Entonces $\geq$ es un orden total sobre $\mathbb{R}$

Para todo $A, B, C \in \mathcal{P}(X)$ se verifica que:
(1) $A \subseteq A$
(2) $(A \subseteq B \wedge B \subseteq A) \iff A = B$
(3) $(A \subseteq B \wedge B \subseteq C) \Rightarrow A \subseteq C$
(4) Puede darse el caso que $A \not\subseteq B$ y $B \not\subseteq A$, por lo que no se cumple la ley de tricotomía.
Entonces $\subseteq$ es un orden no total sobre $\mathcal{P}(X)$ □

Definición 2.5. Una relación reflexiva, simétrica y transitiva $\mathcal{R}$ en un conjunto A se dice una *relación de equivalencia*.

Observación. La relación $=$ es una relación de equivalencia sobre cualquier conjunto.

Dem. Es fácil ver que, para todo $x, y, z \in A$, se verifica que:
(1) $x = x$
(2) $x = y \iff y = x$
(3) $(x = y \wedge y = z) \Rightarrow x = y$
Entonces $=$ es una relación de equivalencia sobre A □

Definición 2.6. Dados una relación de equivalencia $\mathcal{R}$ sobre A y un elemento $x \in A$, llamamos *clase de equivalencia de* x (o en breve *clase de* x) y notamos $\mathrm{Cl}(x)$ al conjunto definido como:

$$\mathrm{Cl}(x) = \{y \in A : x\mathcal{R}y\}$$

Propiedades. Dados una relación de equivalencia $\mathcal{R}$ sobre A y los elementos $x, y \in A$, se verifica que:

(1) $(\forall x \in A) x \in \mathrm{Cl}(x)$
(2) $(\forall x \in A)\mathrm{Cl}(x) \neq \emptyset$
(3) $\bigcup_{x \in A} \mathrm{Cl}(x) = A$
(4) $(\forall x, y \in A)\mathrm{Cl}(x) = \mathrm{Cl}(y)$ o bien $\mathrm{Cl}(x) \cap \mathrm{Cl}(y) = \emptyset$
(5) $\big(\mathrm{Cl}(x) = \mathrm{Cl}(y)\big) \iff x\mathcal{R}y$
(6) A es expresable como unión disjunta de sus clases de equivalencia.

Definición 2.7. Llamamos *partición de un conjunto* A a una familia $(A_i)_{i \in I}$ de subconjuntos de A que satisfacen las siguientes propiedades:
(1) $\bigcup_{i \in I} A_i = A$
(2) $(\forall i, j \in I$ tal que $i \neq j) A_i \cap A_j = \emptyset$
(3) $(\forall i \in I) A_i \neq \emptyset$
o bien, equivalentemente, que $(\forall x \in A)(\exists! i \in I)$ tal que $x \in A_i$

Proposición 2.1. Toda relación de equivalencia $\mathcal{R}$ induce unívocamente una partición sobre A, y recíprocamente toda partición de A induce unívocamente una relación de equivalencia $\mathcal{R}'$.

Dem. Veamos primero que $\mathcal{R}$ induce unívocamente una partición sobre A, a la que llamaremos $(A_{\mathcal{R}_i})$. Definimos $(A_{\mathcal{R}_i})$ de modo que $(x \in A_{\mathcal{R}_i}) \wedge (y \in A_{\mathcal{R}_i}) \iff \mathrm{Cl}(x) = \mathrm{Cl}(y)$. Es fácil ver que $(A_{\mathcal{R}_i})$ es una partición debido a las propiedades de las clases de equivalencia mencionadas anteriormente.
Recíprocamente, una partición (A_i) de A define una relación de equivalencia $\mathcal{R}'$ sobre A tal que $x\mathcal{R}'y \iff (x \in A_i \wedge y \in A_i)$. Es fácil ver que $\mathcal{R}'$ es una relación de equivalencia, ya que se verifica:
(1) $x\mathcal{R}'x \iff (x \in A_i \wedge x \in A_i)$, lo cual se cumple porque todo x pertence a un único A_i
(2) $(x \in A_i \wedge y \in A_i) \iff (y \in A_i \wedge x \in A_i)$
(3) $(x \in A_i \wedge y \in A_i) \wedge (y \in A_i \wedge z \in A_i) \Rightarrow (x \in A_i \wedge z \in A_i)$

□

Definición 2.8. Dada una relación $\mathcal{R}$ de A en B, decimos que $\mathcal{R}$ es una *función de A en B* si para todo $a \in A$ existe un único $b \in B$ tal que $a\mathcal{R}b$. Normalmente notamos funciones con las letras f, g, h, etc. Para notar que f es una función de A en B, decimos $f : A \to B$, y si $(a, b) \in f$ notamos $f(a) = b$.

Definición 2.9. Si una función $f : A \to B$ verifica que $f(x) = c$ para todo $x \in A$ con $c \in B$, decimos que f es *constante*.

Definición 2.10. Dado un conjunto A, la función $f : A \to A$ que verifica que $f(x) = x$ para todo $x \in A$ es llamada *función indentidad de A* y se nota I_A

Observación. Si f y g son funciones de A en B, $f = g$ es equivalente a $(f \subseteq g) \wedge (g \subseteq f)$ y a $(\forall x \in A) f(x) = g(x)$

Definición 2.11. Sean $f : A \to B$ y $g : B' \to C$, con $B \subseteq B'$, definimos *la función composición de f y g*, que notaremos $g \circ f$, de modo que:

$$g \circ f : A \to C \text{ tal que } (\forall x \in A)(g \circ f)(x) = g(f(x))$$

Observación. Para cualquier función f de A en B, $f \circ I_A = f$ e $I_B \circ f = f$

Definición 2.12. Si f es una función de A en B, decimos que f es *inversible* o que f *admite inversa* si existe una función $g : B \to A$ tal que $g \circ f = I_A$ y $f \circ g = I_B$

Observación. Si f es una función inversible, posee una única inversa, a la cual notaremos f^{-1}. Además, para cualquier f inversible se verifica que $(f^{-1})^{-1} = f$

Dem. Supongamos que existen dos inversas diferentes de f, llamémoslas f^{-1} y $f^{-1'}$. Ya que son distintas, entonces existe x tal que:

$$a = f^{-1}(x) \neq f^{-1'}(x) = b$$

Pero si ambas son inversas de f, tenemos que:

$$(f \circ f^{-1})(x) = f(f^{-1}(x)) = f(a) = x = f(b) = f(f^{-1'}(x)) = (f \circ f^{-1'})(x)$$

Pero si $f(a) = f(b)$ con $a \neq b$, f no es inversible, ya que en caso de existir una inversa f^{-1}, se debería cumplir que:

$$a = (f^{-1} \circ f)(a) = f^{-1}(f(a)) = f^{-1}(f(b)) = (f^{-1} \circ f)(b) = b$$

Por lo tanto, no pueden existir dos inversas diferentes de f.

Además, $(f^{-1})^{-1} = f$ es obvio ya que f verifica que $f \circ f^{-1} = I_{\text{Dom}(f^{-1})}$ y $f^{-1} \circ f = I_{\text{Cod}(f^{-1})}$. □

Definición 2.13. Si f es una función de A en B, la *imagen de f*, notada $\text{Im}(f)$ es el conjunto definido como:

$$\text{Im}(f) = \{b \in B : (\exists a \in A) \text{ tal que } b = f(a)\}$$

Observación. $\text{Im}(f) \subseteq \text{Cod}(f)$ para cualquier función f

Definición 2.14. Si f es una función de A en B, decimos que f es:

(1) *inyectiva* si para todo $a, a' \in A$ se cumple que $a \neq a' \Rightarrow f(a) \neq f(a')$, o equivalentemente $f(a) = f(a') \Rightarrow a = a'$
(2) *suryectiva* o *sobreyectiva* si $\text{Im}(f) = B = \text{Cod}(f)$, o equivalentemente si para todo $b \in B$ existe $a \in A$ tal que $b = f(a)$
(3) *biyectiva* si f es inyectiva y suryectiva, o equivalentemente si para todo $b \in B$ existe un único $a \in A$ tal que $b = f(a)$

Teorema. Una función f es inversible si y sólo si es biyectiva.

Dem. $(\Rightarrow)$ Ya demostramos que f debe ser inyectiva para ser inversible como parte de la demostración de la unicidad de las inversas. Falta ver que f debe ser suryectiva. Si f no es suryectiva, existe un $y \in \text{Cod}(f)$ tal que $y \neq f(x)$ para todo $x \in \text{Dom}(f)$. Pero $y = (f \circ f^{-1})(y) = f(f^{-1}(y))$, lo cual es absurdo, por lo tanto f debe ser suryectiva.

$(\Leftarrow)$ Si f es biyectiva, para todo $b \in \text{Cod}(f)$ existe un único $a \in \text{Dom}(f)$ tal que $b = f(a)$. Entonces definimos g tal que $g(b) = a$. Es fácil ver entonces que $g \circ f = I_{\text{Dom}(f)}$ y $f \circ g = I_{\text{Cod}(f)}$ □

Definición 2.15. Si dados los conjuntos A y B existe una biyección f de A en B decimos que son *coordinables* y lo notamos $A \approx B$

Observación. $\approx$ define una relación de equivalencia sobre un conjunto universal $\mathcal{U}$

Dem. Es fácil ver que, para todo $A, B, C \in \mathcal{U}$, se verifica que:
(1) $A \approx A$, dado que $I_A : A \to A$ es biyectiva
(2) $A \approx B \iff B \approx A$, ya que en caso de existir una biyección $f : A \to B$, entonces $f^{-1} : B \to A$ también lo es
(3) $(A \approx B \wedge B \approx C) \Rightarrow A \approx C$, ya que en caso de existir biyecciones $f : A \to B$ y $g : B \to C$, entonces $g \circ f : A \to C$ también lo es

Entonces $\approx$ es una relación de equivalencia sobre $\mathcal{U}$ □

3. Inducción

Definición 3.1. Dados un conjunto A, una función $f : \mathbb{N} \to A$ se dice una *sucesión de elementos de A* (o bien una *secuencia de elementos de A*). Notaremos a $f(n)$ como x_n, y a la sucesión como $(x_n)_{n\in\mathbb{N}} = \{x_1, x_2, \dots\}$, donde x_n es el enésimo término de la sucesión. También llamaremos sucesión a funciones $f : \mathbb{N}_0 \to A$, donde $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$

Definición 3.2. Un conjunto $A \subseteq \mathbb{R}$ se dice *inductivo* si $1 \in A$ y si para todo $x \in A$ se cumple que $(x + 1) \in A$

Definición 3.3. Llamamos *conjunto de números naturales*, y notamos $\mathbb{N}$ a la intersección de todos los conjuntos inductivos, es decir:

$$\mathbb{N} = \bigcap_{A \text{ inductivo}} A$$

Teorema de inducción. Si el conjunto $A \subseteq \mathbb{N}$ es inductivo, entonces $A = \mathbb{N}$

Dem. Para que $A = \mathbb{N}$ se debe cumplir que $A \subseteq \mathbb{N}$ y $\mathbb{N} \subseteq A$. Ahora bien, $A \subseteq \mathbb{N}$ se cumple por hipótesis, y por la definición de $\mathbb{N}$ sabemos que $\mathbb{N} = A \cap X$, con X la intersección de todos los otros conjuntos inductivos. Se deduce entonces que $x \in \mathbb{N} \Rightarrow x \in A$, o sea $\mathbb{N} \subseteq A$ □

Principio de inducción. Dada una proposición p que verifique, para todo $n \in \mathbb{N}$, que:

(1) Se cumple $p(1)$
(2) Si se cumple $p(n)$, entonces también se cumple $p(n + 1)$

Entonces se cumple $p(n)$ para todo $n \in \mathbb{N}$

Dem. Definimos $A = \{x \in \mathbb{N} : \text{se cumple } p(x)\}$. Ahora bien, $A \subseteq \mathbb{N}$ y, por hipótesis, es inductivo; entonces, por el teorema de inducción, $A = \mathbb{N}$ □

Definición 3.4. Notamos $\mathbb{Z}_{\geq r}$ al conjunto definido como:

$$\mathbb{Z}_{\geq r} = \{k \in \mathbb{Z} : k \geq r\}$$

Principio de inducción generalizada. Dados $r \in \mathbb{Z}$ y una proposición p predicable sobre $\mathbb{Z}_{\geq r}$ tal que:

(1) Se cumple $p(r)$
(2) Para todo $n \in \mathbb{Z}_{\geq r}$, si se cumple $p(n)$, entonces también se cumple $p(n + 1)$

Entonces se cumple $p(n)$ para todo $n \in \mathbb{Z}_{\geq r}$

Dem. Definimos la proposición q de modo que $q(n) = p(n + r - 1)$. Entonces se cumple $q(1) = p(r)$ y además $q(k) \Rightarrow q(k+1)$ ya que $p(n+r-1) \Rightarrow p(n+r)$ y $(n+r-1), (n+r) \in \mathbb{Z}_{\geq r}$. Por lo tanto se cumple $q(n)$ para todo $n \in \mathbb{N}$, y consecuentemente se cumple $p(n)$ para todo $n \in \mathbb{Z}_{\geq r}$ □

Definición 3.5. Definimos por inducción al *factorial de n*, notado $n!$, de acuerdo a la siguiente recurrencia:

$$0! = 1$$
$$(n+1)! = n!(n+1)$$

Definición 3.6. Dada una sucesión $(a_i)_{i\in\mathbb{N}}$ de reales, definimos por inducción a la *sumatoria* de los primeros k términos de la sucesión, de acuerdo a la siguiente recurrencia:

$$x_1 = a_1$$
$$x_{k+1} = x_k + a_{k+1}$$

El término k-ésimo de la sumatoria es notado $\sum_{i=1}^{k} a_i$
Análogamente definimos a la *productoria* de los primeros k términos de la sucesión, de acuerdo a la siguiente recurrencia:

$$x'_1 = a_1$$
$$x'_{k+1} = x'_k(a_{k+1})$$

El término k-ésimo de la productoria es notado $\prod_{i=1}^{k} a_i$

Propiedades. Dados $k \in \mathbb{R}$ y $(a_i)_{i\in\mathbb{N}}, (b_i)_{i\in\mathbb{N}}$ sucesiones de reales, se verifica que:

(1) $\sum_{i=1}^{n}(a_i + b_i) = \sum_{i=1}^{n} a_i + \sum_{i=1}^{n} b_i$
(2) $\sum_{i=1}^{n} ka_i = k\sum_{i=1}^{n} a_i$
(3) $\sum_{i=1}^{n} k = kn$
(4) $\prod_{i=1}^{n}(a_i b_i) = (\prod_{i=1}^{n} a_i)\,(\prod_{i=1}^{n} b_i)$
(5) $\prod_{i=1}^{n} ka_i = k^n \prod_{i=1}^{n} a_i$
(6) $\prod_{i=1}^{n} k = k^n$

Definición 3.7. Dada una sucesión $(a_i)_{i\in\mathbb{N}_0}$ de reales, extendemos la notación de sumatorias y productorias:

$$\sum_{i=0}^{n} a_i = \sum_{j=1}^{n+1} a_{j-1} \text{ y } \prod_{i=0}^{n} a_i = \prod_{j=1}^{n+1} a_{j-1}$$

Dado $r \in \mathbb{N}$:

$$\sum_{i=r}^{n} a_i = \sum_{i=1}^{n} a_i - \sum_{i=1}^{r} a_i = \sum_{i=0}^{n-r} a_{r+i} \text{ y } \prod_{i=r}^{n} a_i = \prod_{i=0}^{n-r} a_{r+i}$$

Dado $s \in \mathbb{N}$ tal que $s < r$:

$$\sum_{i=r}^{s} a_i = 0 \text{ y } \prod_{i=r}^{s} a_i = 1$$

Definición 3.8. La sucesión $(a_i)_{i\in\mathbb{N}_0}$ de reales se dice una *progresión aritmética* si se cumple que, para todo $k \in \mathbb{N}_0$, $a_{k+1} = a_k + c$ con $c \in \mathbb{R}$.
A su vez, decimos que es una *progresión geométrica* si se cumple que, para todo $k \in \mathbb{N}_0$, $a_{k+1} = c(a_k)$ con $c \in \mathbb{R}$

Observación. Si la sucesión $(a_i)_{i\in\mathbb{N}_0}$ es aritmética, $a_i = a_0 + qi$
Si la sucesión $(a_i)_{i\in\mathbb{N}_0}$ es geométrica, $a_i = a_0 \cdot q^i$
Llamamos a q la *razón* de la sucesión.

Dem. Por inducción, tenemos que:

Si (a_i) es aritmética:
(1) $a_0 = a_0 + q \cdot 0$
(2) Si $a_k = a_0 + qk$ entonces $a_{k+1} = a_0 + qk + k = a_0 + q(k+1)$
Entonces $a_i = a_0 + qi$ para todo $i \in \mathbb{N}_0$

Si (a_i) es geométrica:
(1) $a_0 = a_0 \cdot q^0$
(2) Si $a_k = a_0 \cdot qk$ entonces $a_{k+1} = a_0 \cdot q^k \cdot k = a_0 \cdot q^{k+1}$
Entonces $a_i = a_0 \cdot q^i$ para todo $i \in \mathbb{N}_0$ □

Proposición 3.1. Si la sucesión $(a_i)_{i\in\mathbb{N}_0}$ es aritmética:

$$\sum_{i=0}^{n} a_i = (n+1)\left(a_0 + \frac{qn}{2}\right)$$

Si la sucesión $(a_i)_{i\in\mathbb{N}_0}$ es geométrica:

$$\sum_{i=0}^{n} a_i = \frac{a_0(q^{n+1}-1)}{q-1} \text{ si } q \neq 1$$

En ambos casos, q es la razón de la sucesión.
Si $q = 1$ en una sucesión geométrica, el caso se reduce a una sucesión aritmética de razón 0.

Dem. Demostramos primero la identidad para sucesiones aritméticas. Por lo demostrado en la observación anterior, $a_i = a_0 + qi$, por lo tanto tenemos que:

$$\begin{aligned}
\sum_{i=0}^{n} a_i &= \sum_{i=0}^{n} (a_0 + qi) \\
&= \sum_{i=0}^{n} a_0 + \sum_{i=0}^{n} qi \\
&= (n+1)(a_0) + q\sum_{i=0}^{n} i \\
&= (n+1)(a_0) + q\left(\frac{n(n+1)}{2}\right) \\
&= (n+1)\left(a_0 + \frac{qn}{2}\right)
\end{aligned}$$

Ahora, para sucesiones geométricas tenemos que $a_i = a_0 \cdot q^i$. Notaremos $S_n = \sum_{i=0}^{n} a_i$. Consideremos el producto $q \cdot S_n$:

$$q \cdot S_n = q\sum_{i=0}^{n} a_i = q\sum_{i=0}^{n} (a_0 \cdot q^i) = \sum_{i=0}^{n} (a_0 \cdot q^{i+1}) = \sum_{i=1}^{n+1} (a_0 \cdot q^i)$$

Entonces:

$$\begin{aligned} q \cdot S_n - S_n &= \sum_{i=1}^{n+1} (a_0 \cdot q^i) - \sum_{i=0}^{n} (a_0 \cdot q^i) \\ \iff S_n(q-1) &= a_0 \cdot q^{n+1} - a_0 \cdot q^0 = a_0(q^{n+1} - 1) \\ \iff S_n &= \frac{a_0(q^{n+1}-1)}{q-1} \end{aligned}$$

□

Principio de buena ordenación de $\mathbb{N}$. Todo conjunto $A \subseteq \mathbb{N}$ no vacío tiene mínimo; es decir, existe $a \in A$ tal que $(\forall x \in A) a \leq x$

Dem. Consideremos la proposición $p(n) = (A \subseteq \mathbb{N} \wedge n \in A) \Rightarrow \exists \min(A)$. Basta demostrar que $p(n)$ vale para todo $n \in \mathbb{N}$ para demostrar el principio de buena ordenación.

Por inducción:
(1) $p(1)$ se cumple, ya que $\min(\mathbb{N}) = 1$ y $A \subseteq \mathbb{N}$, por lo que $\min(A) = 1$
(2) $p(k) \Rightarrow p(k+1)$. Si $k \in A$, existe un mínimo por hipótesis inductiva. Si $k \notin A$, consideremos el conjunto $A' = A \cup \{k\}$. A' tiene mínimo por hipótesis inductiva; llamémoslo m. Si $m \neq k$, entonces $m \in A$, y dado que $A \subseteq A'$, también es mínimo de A. Si $m = k$, se deduce que $k+1$ es mínimo de A ya que $k < n$ para todo $n \in A$ y no existe $k' \in \mathbb{N}$ tal que $k < k' < k+1$ □

Teorema. El principio de buena ordenación de $\mathbb{N}$ implica el principio de inducción.

Dem. Sea p una proposición predicable en $\mathbb{N}$ tal que:

(1) Se verifica $p(1)$
(2) $p(k) \Rightarrow p(k+1)$

Ahora bien, consideremos el conjunto $A = \{n \in \mathbb{N} : \text{no se cumple } p(n)\}$. Si $A \neq \emptyset$, existe $m = \min(A)$ debido al principio de buena ordenación. Por hipótesis, $m \neq 1$ ya que $1 \notin A$. Por lo tanto, $m - 1 \in \mathbb{N}$ y $m - 1 \notin A$ (de lo contrario m no sería mínimo). Entonces, se cumple $p(m-1)$, y por hipótesis, $p(m)$ también, lo cual es una contradicción ya que $m \in A$. Se deduce entonces que no existe mínimo de A, por lo tanto $A = \emptyset$ y la proposición vale para todo $n \in \mathbb{N}$ □

Principio de inducción global (o inducción fuerte). Dada una proposición p predicable en $\mathbb{Z}_{\geq r}$ tal que:

(1) Se cumple $p(r)$
(2) Si se cumple $p(j)$ para todo $j \leq k$, se cumple entonces $p(k+1)$

Entonces se cumple $p(n)$ para todo $n \in \mathbb{Z}_{\geq r}$

Dem. Supongamos que $p(n)$ no se cumple para todo $n \in \mathbb{Z}_{\geq r}$. Entonces, definimos $m = \min\{n \in \mathbb{Z}_{\geq r} : \text{no se cumple } p(n)\}$. Es claro que m existe por el principio de buena ordenación (el cual vale para $\mathbb{Z}_{\geq r}$ porque lo podemos considerar como $\mathbb{N}$ desplazado por una constante r). Entonces, por hipótesis, si no se cumple $p(m)$, entonces existe algún $j < m$ tal que no se cumple $p(j)$ (ya que $m \neq r$), pero esto es absurdo porque entonces m no seria el mínimo valor para el cual la proposición no se cumple. Por lo tanto, se cumple $p(n)$ para todo $n \in \mathbb{Z}_{\geq r}$ □

Definición 3.9. Dado $n \in \mathbb{N}$, notamos $\mathbb{I}_n$ al conjunto definido como:

$$\mathbb{I}_n = \{k \in \mathbb{N} : 1 \leq k \leq n\}$$

Un conjunto de este tipo es llamado una *sección de* $\mathbb{N}$

Definición 3.10. Un conjunto A se dice *finito* si existe $n \in \mathbb{N}$ tal que $\mathbb{I}_n$ y A son coordinables. En este caso, decimos que A tiene n elementos o que su *cardinalidad* es n, y notamos $\#A = n$
Un conjunto A se dice *infinito* si no es finito, es decir, si no existe $n \in \mathbb{N}$ tal que $\mathbb{I}_n$ y A sean coordinables.

Observación. # define una relación de equivalencia sobre un conjunto universal $\mathcal{U}$.

Dem. La igualdad de cardinales entre dos conjuntos es equivalente a la coordinabilidad de ambos, lo cual ya demostramos es una relación de equivalencia sobre $\mathcal{U}$. □

Proposición 3.2. Para cualquier conjunto finito A se verifica que:

$$\#\mathcal{P}(A) = 2^{\#A}$$

Dem. Notaremos $\{0,1\}^n$ al conjunto de n-uplas binarias, o equivalentemente, al producto cartesiano:

$$\prod_{i=1}^{n} \{0,1\}$$

Es fácil ver, por combinatoria, que $\#\{0,1\}^n = 2^n$.

Dado que A es finito, podemos disponer de sus elementos indexándolos con una sección de $\mathbb{N}$, de modo que $A = \{a_1, a_2, \ldots, a_n\}$, donde $n = \#A$.

Consideremos entonces la función $f : \mathcal{P}(A) \to \{0,1\}^{\#A}$ definida tal que:

$$f(B) = (b_1, b_2, \ldots, b_n)$$

donde $b_i = 1$ si $a_i \in B$ y $b_i = 0$ si $a_i \notin B$.

Ahora bien, consideremos la función $g : \{0,1\}^{\#A} \to \mathcal{P}(A)$ definida tal que:

$$g(x_1, x_2, \ldots, x_n) = \{a_i : x_i = 1\}$$

Es fácil ver que $f \circ g = I_{\{0,1\}^{\#\mathcal{P}(A)}}$ y $g \circ f = I_{\mathcal{P}(A)}$, o sea f y g son inversas entre sí, y consecuentemente, biyecciones. Entonces:

$$\#\mathcal{P}(A) = \#\{0,1\}^{\#A} = 2^{\#A}$$

□

Principio de Dirichlet (o del palomar). Dados A, B conjuntos finitos, si $\#A > \#B$ entonces no existe una inyección de A en B

Dem. Consideremos la siguiente proposición predicable en $\mathbb{N}$:

$$p(n) : m > n \implies \nexists \text{ inyección } f : \mathbb{I}_m \to \mathbb{I}_n$$

Veamos que $p(n)$ se verifica para todo $n \in \mathbb{N}$ por inducción:

(1). $p(1)$ se verifica, ya que, si $f : \mathbb{I}_m \to \{1\}$, $f(k) = 1$ para todo $k \in \mathbb{I}_m$

(2). Veamos que, si se cumple $p(n)$, entonces también lo hace $p(n+1)$, suponiendo una función $f : \mathbb{I}_m \to \mathbb{I}_{n+1}$ con $m > n+1$.

Si $n+1 \notin \text{Im}(f)$, entonces f es una función de $\mathbb{I}_m$ en $\mathbb{I}_n$ y, por hipótesis, no es inyectiva.

Si $n+1 \in \text{Im}(f)$, supongamos que $f(m) = n+1$. En ese caso, la restricción de f a $\mathbb{I}_{m-1}$ produce una función de $\mathbb{I}_{m-1}$ en $\mathbb{I}_n$, por lo que se deduce, por hipótesis, que f no es inyectiva.

Por último, si $f(x) = n+1$ con $1 \leq x < m$, consideremos la función $g : \mathbb{I}_m \to \mathbb{I}_m$ definida de modo que:

$$g(y) = \begin{cases} y & \text{si } y \neq x \wedge y \neq m \\ m & \text{si } y = x \\ x & \text{si } y = m \end{cases}$$

Claramente, g es biyectiva. Entonces, si f es inyectiva, $f \circ g$ también lo es; pero $(f \circ g)(m) = n+1$, reduciéndolo al caso anterior. Por lo tanto, f no es inyectiva.

□

Proposición 3.3. Dados $m, n \in \mathbb{N}$ tal que $m \neq n$, no existe una biyección entre $\mathbb{I}_m$ y $\mathbb{I}_n$

Dem. Ya que no existen inyecciones de una sección de $\mathbb{N}$ mayor a una menor (por el principio del palomar), es claro que no existen biyecciones entre diferentes secciones. □

Proposición 3.4. Si A es finito y $S \subseteq A$, entonces S es finito y $\#A \geq \#S$. Más aún, $\#A = \#S$ si y sólo si $A = S$

Dem. Dado que A es finito, podemos disponer de sus elementos indexándolos con una sección de $\mathbb{N}$, de modo que $A = \{a_1, a_2, \ldots, a_n\}$, donde $n = \#A$. Si $S \subseteq A$, entonces podemos elegir la forma de indexar A de modo que $S = A - \{a_m, a_{m+1}, \ldots, a_{n-1}, a_n\}$, donde los términos sustraídos son aquellos $a \in A$ tales que $a \notin S$. De este modo, $S = \{a_1, \ldots, a_{n-m}\}$ y consecuentemente es biyectable con $\mathbb{I}_{n-m}$, es decir, finito. Es fácil ver que $\#A = \#S$ sólo si no sustraigo ningún término de A, por lo que se deduce que $S = A$. □

Proposición 3.5. Sean $A_1, A_2, \ldots, A_r$ (con $r \in \mathbb{N}$) conjuntos finitos tales que $A_i \cap A_j = \emptyset$ si $i \neq j$, entonces:

$$\bigcup_{i \in \mathbb{I}_r} A_i \text{ es finita, y } \#\bigcup_{i \in \mathbb{I}_r} A_i = \sum_{i=1}^{r} \#A_i$$

Dem. Llamemos B a la unión de los conjuntos A_i. Podemos ver que B es indexable con $\mathbb{I}_c$, donde c es la suma de las cardinalidades de los conjuntos A_i, ya que es posible definir dicho índice de modo que:

$$B = \{b_1, \ldots, b_c\}$$

Para crear este índice, primero definiremos la r-upla $p = (p_1, \ldots, p_r)$ tal que:

$$p_i = \sum_{j=1}^{i} \#A_j$$

Entonces, dado $i \leq c$, definimos $m = \min\{j : p_j \geq i\}$ y construimos el índice de B tal que:

$$b_i = A_{m_{i-p_{m-1}}}$$

Por lo tanto, la unión es finita, y de cardinalidad c. □

Proposición 3.6 (Principio de inclusión-exclusión)**.** Sean A, B conjuntos finitos, entonces:

$$\#(A \cup B) = \#A + \#B - \#(A \cap B)$$

Dem. Es fácil ver que:

$$A \cup B = (A - B) \cup (A \cap B) \cup (B - A)$$

Como dicha unión es disjunta, por lo probado en la proposición anterior, tenemos que:

$$\#(A \cup B) = \#(A - B) + \#(A \cap B) + \#(B - A)$$

Además:

$$\#A = \#(A - B) + \#(A \cap B) \text{ y } \#B = \#(B - A) + \#(A \cap B)$$

Sumando estos dos términos:

$$\begin{gathered} \#A + \#B = \#(A - B) + \#(B - A) + 2\#(A \cap B) \\ \iff \#A + \#B - \#(A \cap B) = \#(A - B) + \#(B - A) + \#(A \cap B) = \#(A \cup B) \end{gathered}$$

□

Proposición 3.7. Dados A, B conjuntos finitos, si $\#A < \#B$ entonces no existe una suryección de A en B

Dem. Sea f una función de A en B y sea $A_b = \{x \in A : f(x) = b\}$, es decir, la preimagen de b en f. Es fácil ver que la familia de todos los conjuntos A_b es disjunta y su unión es A; por lo tanto:

$$\#A = \sum_{b \in B} \#A_b$$

Si f es suryectiva, $A_b \neq \emptyset$, entonces, para todo $b \in B$, $\#A_b \geq 1$, y por lo tanto:

$$\#A = \sum_{b \in B} \#A_b \geq \sum_{b \in B} 1 = \#B$$

lo cual es absurdo; por lo tanto f no es suryectiva. □

Proposición 3.8. Sean $A_1, A_2, \ldots, A_r$ (con $r \in \mathbb{N}$) conjuntos finitos, entonces:

$$A_1 \times A_2 \times \cdots \times A_n \text{ es finito, y } \#(A_1 \times A_2 \times \cdots \times A_n) = \prod_{i=1}^{r} \#A_i$$

Dem. Para cada $a \in A_1$, definimos:

$$L_a = \{z \in (A_1 \times A_2) : z = (a, b) \text{ con } b \in A_2\}$$

Es fácil ver que la familia de conjuntos L_a es una partición de $A_1 \times A_2$ y que $\#L_a = \#A_2$, por lo tanto:

$$\#(A_1 \times A_2) = \# \bigcup_{a \in A_1} L_a = \sum_{a \in A_1} \#L_a = (\#A_1)(\#A_2)$$

El resultado es generalizable a productos de familias finitas de conjuntos por inducción. □

4. Combinatoria

Principio multiplicativo. Dada una experiencia que puede arrojar m resultados posibles, y por cada uno de ellos, una sgeunda experiencia que pueda arrojar n resultados posibles, la realización conjunta de ambas puede arrojar mn resultados.

Más generalmente, dadas r experiencias $E_1, \ldots, E_r$ tales que E_i puede arrojar m_i resultados, la realización conjunta de todas puede arrojar la siguiente cantidad de resultados:

$$\prod_{i=1}^{r} m_i$$

Definición 4.1. Dados A, B conjuntos finitos, utilizaremos la siguiente notación:

(1). B^A denotará al conjunto de todas las funciones de A en B
(2). $\text{Iny}(A, B)$ denotará al conjunto de todas las inyecciones de A en B
(3). $\text{Biy}(A, B)$ denotará al conjunto de todas las biyecciones de A en B

Lema 4.1. Sea f una función entre dos conjuntos finitos y coordinables A y B, de cardinalidad n. Entonces son equivalentes:

(1). f es inyectiva
(2). f es suryectiva
(3). f es biyectiva

Dem. (1). Supongamos que f es inyectiva. Sea $f' : A \to \text{Im}(f)$ definida de modo tal que $f(x) = f'(x)$ para todo $x \in A$. Es inmediato que f' es biyectiva. Entonces, $\#B = \#A = \#\text{Im}(f)$ (ya que, por el principio del palomar, no puede haber biyecciones entre conjuntos de distinta cardinalidad, ya que no habrá inyecciones del mayor al menor), por lo que f es suryectiva, y por lo tanto, también biyectiva.

(2). Supongamos que f es suryectiva. Sea $A_b = \{x \in A : f(x) = b\}$, es decir, la preimagen de b en f. Es fácil ver que la familia de todos los conjuntos A_b es disjunta y su unión es A; por lo tanto:

$$\#A = \sum_{b \in B} \#A_b$$

Si f es suryectiva, $A_b \neq \emptyset$, entonces, para todo $b \in B$, $\#A_b \geq 1$, y por lo tanto:

$$\#A = \sum_{b \in B} \#A_b \geq \sum_{b \in B} 1 = \#B$$

de lo cual deducimos que:

$$\sum_{b \in B} \#A_b = \sum_{b \in B} 1$$

por lo tanto f es inyectiva, y por lo tanto, también biyectiva.

(3). Por definición, si f es biyectiva, también es inyectiva y suryectiva.

□

Proposición 4.1. Dados A, B conjuntos finitos, se verifica que:

(1).
$$\#(B^A) = \#B^{\#A}$$

(2).
$$\#(\mathrm{Iny}(A,B)) = \begin{cases} 0 & \text{si } \#A > \#B \\ \prod_{i=0}^{\#A-1} \#B - i = \frac{(\#B)!}{(\#B-\#A)!} & \text{si } \#A \leq \#B \end{cases}$$

(3).
$$\#(\mathrm{Biy}(A,B)) = \begin{cases} 0 & \text{si } \#A \neq \#B \\ (\#A)! & \text{si } \#A = \#B \end{cases}$$

Dem. (1). Dado que una función de A en B asigna todo elemento de A a un elemento de B, entonces tenemos $\#A$ experiencias que pueden arrojar $\#B$ resultados; entonces, por el principio multiplicativo:
$$\#(B^A) = \prod_{i=1}^{\#A} \#B = \#B^{\#A}$$

(2). Si $\#A > \#B$, entonces no hay inyecciones de A en B por el principio del palomar. Ahora bien, si $\#A \geq \#B$, una inyección de A en B consiste en asignar diferentes elementos de B a cada elemento de A; por lo tanto, tendremos $\#A$ experiencias, en las que cada una puede arrojar un resultado menos que la anterior, partiendo desde $\#B$ resultados, es decir:
$$\#(\mathrm{Iny}(A,B)) = \prod_{i=1}^{\#A} \#B - i + 1 = \prod_{i=0}^{\#A-1} \#B - i = \frac{(\#B)!}{(\#B-\#A)!}$$

(3). Si $\#A \neq \#B$, o bien no existen inyecciones de A en B, o no existen inyecciones de B en A, debido al principio del palomar. Consecuentemente no hay biyecciones entre A y B. Ahora bien, si $\#A = \#B$, por lo demostrado en el Lema 4.1, si f es una inyección de A en B también es una biyección (y es obvio que toda biyección es una inyección), entonces:
$$\#(\mathrm{Biy}(A,B)) = \#(\mathrm{Iny}(A,B)) = \frac{(\#B)!}{(\#B-\#A)!} = (\#B)! = (\#A)!$$

□

Definición 4.2. Dados $m, n \in \mathbb{N}$, definimos los siguientes conceptos:

(1). Si $m \leq n$, cualquier elección ordenada de m elementos distintos elegidos en un conjunto de n elementos es llamada una *variación m-aria de n elementos*. Notamos V_m^n a la cantidad de dichas variaciones. Además:
$$V_m^n = \#(\mathrm{Iny}(\mathbb{I}_m, \mathbb{I}_n)) = \frac{n!}{(n-m)!}$$

(2). Cualquier elección ordenada de m elementos no necesariamente distintos elegidos en un conjunto de n elementos es llamada una *variación m-aria con repetición de n elementos*. Notamos VR_m^n a la cantidad de dichas variaciones. Además:
$$VR_m^n = \#\left(\mathbb{I}_n^{\mathbb{I}_m}\right) = n^m$$

(3). Cualquier elección ordenada de n elementos distintos elegidos en un conjunto de n elementos es llamada una *permutación n-aria*. Notamos P_n a la cantidad de dichas permutaciones. Además:

$$P_n = \#(\mathrm{Iny}(\mathbb{I}_n, \mathbb{I}_n)) = \#(\mathrm{Biy}(\mathbb{I}_n, \mathbb{I}_n)) = n!$$

(4). Si $m \leq n$, cualquier elección no ordenada de m elementos distintos elegidos en un conjunto de n elementos es llamada una *combinación m-aria de n elementos*. Notamos C_m^n, o más frecuentemente $\binom{n}{m}$ a la cantidad de dichas combinaciones. Además:

$$\binom{n}{m} = \frac{n!}{m!(n-m)!}$$

Esto se debe a que:

$$V_m^n = \binom{n}{m} m!$$

Observación. $\binom{n}{m}$ es el número de subconjuntos de cardinalidad m que admite un conjunto de n elementos. Esto se deduce inmediatamente de la definición de combinación.

Definición 4.3. Llamamos a $\binom{n}{m}$ el *número combinatorio n m*, y extendemos su definición de modo que, si $m < 0$ o $n < m$:

$$\binom{n}{m} = 0$$

De este modo $\binom{n}{m}$ está bien definido para todo $n, m \in \mathbb{N}$

Proposición 4.2. Para todo $n, k \in \mathbb{N}$, se verifican las siguientes identidades:

(1).
$$\binom{n}{0} = 1$$

(2).
$$\binom{n}{1} = n$$

(3).
$$\binom{n}{k} = \binom{n}{n-k}$$

(4).
$$\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}$$

Dem. (1).
$$\binom{n}{0} = \frac{n!}{0!(n-0)!} = \frac{n!}{n!} = 1$$

(2).
$$\binom{n}{1} = \frac{n!}{1!(n-1)!} = \frac{n!}{(n-1)!} = n$$

(3).
$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n!}{(n-(n-k))!(n-k)!} = \binom{n}{n-k}$$

(4). Dado que $\binom{n+1}{k}$ es el número de subconjuntos de cardinalidad k que admite un conjunto de $n+1$ elementos, observamos que, si no utilizamos un elemento x del conjunto de $n+1$ elementos, tenemos $\binom{n}{k}$ subconjuntos posibles; por otro lado, si lo utilizamos, tenemos $\binom{n}{k-1}$ subconjuntos posibles (ya que ya hemos elegido el primer elemento). Se deduce entonces que:
$$\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}$$

□

Fórmula binomial de Newton. Dados $a, b \in \mathbb{R}$ y $n \in \mathbb{N}_0$, se verifica que:
$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$$

Dem. Por inducción:

(1).
$$(a+b)^0 = 1 = \sum_{k=0}^{0} \binom{0}{k} a^{0-k} b^k = \binom{0}{0} a^{0-0} b^0$$

(2). Veamos que:
$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k \implies (a+b)^{n+1} = \sum_{k=0}^{n+1} \binom{n+1}{k} a^{n+1-k} b^k$$

Por hipótesis:
$$\begin{aligned}
(a+b)^{n+1} &= (a+b)(a+b)^n \\
&= (a+b) \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k \\
&= a \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k + b \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k \\
&= \sum_{k=0}^{n} \binom{n}{k} a^{n+1-k} b^k + \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^{k+1}
\end{aligned}$$

Es fácil ver que, por una sustitución de índices, vale que:
$$\sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^{k+1} = \sum_{k=1}^{n+1} \binom{n}{k-1} a^{n+1-k} b^k$$

Entonces, tenemos que:

$$(a+b)^{n+1} = \sum_{k=0}^{n} \binom{n}{k} a^{n+1-k} b^k + \sum_{k=1}^{n+1} \binom{n}{k-1} a^{n+1-k} b^k$$

Ahora bien, vale que:

$$\sum_{k=0}^{n} \binom{n}{k} a^{n+1-k} b^k = \sum_{k=0}^{n+1} \binom{n}{k} a^{n+1-k} b^k$$

ya que el término $(n+1)$-ésimo es $\binom{n}{n+1} a^{n+1-(n+1)} b^{n+1} = 0 \cdot 1 \cdot b^{n+1} = 0$

Además, también vale que:

$$\sum_{k=1}^{n+1} \binom{n}{k-1} a^{n+1-k} b^k = \sum_{k=0}^{n+1} \binom{n}{k-1} a^{n+1-k} b^k$$

ya que el término 0 es $\binom{n}{0-1} a^{n+1-1} b^0 = 0 \cdot a^n \cdot 1 = 0$

Por lo tanto, tenemos que:

$$\begin{aligned}
(a+b)^{n+1} &= \sum_{k=0}^{n+1} \binom{n}{k} a^{n+1-k} b^k + \sum_{k=0}^{n+1} \binom{n}{k-1} a^{n+1-k} b^k \\
&= \sum_{k=0}^{n+1} \binom{n}{k} a^{n+1-k} b^k + \binom{n}{k-1} a^{n+1-k} b^k \\
&= \sum_{k=0}^{n+1} \left(\binom{n}{k} + \binom{n}{k-1} \right) (a^{n+1-k} b^k) \\
&= \sum_{k=0}^{n+1} \binom{n+1}{k} (a^{n+1-k} b^k)
\end{aligned}$$

□

Observación. Dado $n \in \mathbb{N}_0$, se verifica que:

$$\sum_{k=0}^{n} \binom{n}{k} = (1+1)^n = 2^n = \#\mathcal{P}(\mathbb{I}_n)$$

Esto se debe a que $\binom{n}{k}$ representa al número de subconjuntos de k elementos de n, por lo cual su suma desde $k = 0$ hasta n representa el total de los subconjuntos de n.

Observación. Dado $n \in \mathbb{N}_0$, se verifica que:

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} = (1-1)^n = 0^n = 0$$

Además, esto implica que:

$$\sum_{\substack{k=0 \\ k \text{ par}}}^{n} \binom{n}{k} = \sum_{\substack{k=0 \\ k \text{ impar}}}^{n} \binom{n}{k}$$

lo cual implica a su vez que todo conjunto tiene igual cantidad de subconjuntos de cardinalidad par e impar.

Definición 4.4. Dado un experimento de resultado aleatorio, llamamos *espacio de resultados* al conjunto de todos los resultados posibles del experimento. Un *suceso (o evento) aleatorio* es un subconjunto del espacio de resultados.

Definición 4.5. Dado un espacio de resultados E de un cierto experimento aleatorio, llamamos *función de probabilidad* a una función $p : \mathcal{P}(E) \to [0,1]$ tal que:

(1). $p(E) = 1$
(2). p es aditiva; es decir, dados $S, T \subseteq E$ disjuntos, $p(S \cup T) = p(S) + p(T)$

Si E es finito, es decir, $E = \{x_1, x_2, \ldots, x_n\}$, tenemos que:

$$\sum_{i=1}^{n} p\left(\{x_i\}\right) = 1$$

ya que la unión de cada elemento de un conjunto equivale al conjunto. Usaremos la notación p_i para referirnos a $p\left(\{x_i\}\right)$. Por lo tanto, basta elegir n números que sumen 1 para definir una función de probabilidad sobre un espacio de resultados finito.

Para ello, normalmente se realizan N instancias del experimento, y luego, notando f_i la cantidad de veces que tenemos un resultado x_i, se asignan las probabilidades de modo que:

$$p_i = \frac{f_i}{N}$$

Observación. Dada una función de probabilidad p sobre un espacio de resultados E y un suceso aleatorio S, se verifica que $p(S) = 1 - p(S^c)$, ya que $E = S \cup S^c$, $p(E) = 1$ y p es aditiva.

Definición 4.6. Dada una función de probabilidad p sobre un espacio de resultados E de cardinalidad $n \in \mathbb{N}$, se dice que sus resultados son *equiprobables* si $p_i = p_j$ para todo $i, j \in \mathbb{I}_n$. Además resulta evidente que $p_i = \frac{1}{n}$ y $p(S) = \frac{\#S}{n}$, donde S es un suceso aleatorio.

5. Teoría de números elemental

Definición 5.1. Dados $a, b \in \mathbb{Z}$, decimos que *a divide* a b, a es *divisor* de b, o b es *múltiplo* de a si existe $c \in \mathbb{Z}$ tal que $b = ac$. En tal caso, notamos $a \mid b$; si no existiera dicho c, notamos $a \nmid b$.

Propiedades. Dados $a, b \in \mathbb{Z}$, se verifican las siguientes propiedades:

(1). $a \mid 0$

(2). $1 \mid b$

(3). $0 \mid b \iff b = 0$

(4). Si $a \mid b$ y $a \neq 0$, entonces $\frac{b}{a} \in \mathbb{Z}$

(5). La relación de divisibilidad entre dos enteros es reflexiva y transitiva.

(6). $a \mid b \iff |a| \mid |b|$

(7). Si $a \mid b$ y $b \neq 0$, entonces $|a| \leq |b|$

(8). Si $a \neq 0$, entonces a tiene un número infinito de múltiplos.

(9). Si $b \neq 0$, entonces b tiene un número finito de divisores.

(10). $(a \mid b \wedge b \mid a) \iff |a| = |b| \iff a = \pm b$

(11). Si $a \mid b_i$ para todo $i \in \mathbb{I}_n$, entonces $a \mid \sum_{i=1}^{n} x_i b_i$ con $x_i \in \mathbb{Z}$

(12). Si $a \mid b_i$ para todo $i \in \mathbb{I}_{n-1}$ y $a \mid \sum_{i=1}^{n} b_i$, entonces $a \mid b_n$

Dem. (1). $0 = a \cdot 0$

(2). $b = 1 \cdot b$

(3). $b = 0 \cdot c = 0$

(4). Si $a \mid b$ y $a \neq 0$, entonces existe $c \in \mathbb{Z}$ tal que $c = \frac{b}{a}$

(5). La relación de divisibilidad entre dos enteros es reflexiva, ya que $a \mid a$ debido a que $a = a \cdot 1$, y transitiva, dado que si $a \mid b$ y $b \mid c$, tenemos que $b = ax$ y entonces $c = (ax)y$, de lo que se deduce que $a \mid c$ ya que $c = a(xy)$.

(6). $a \mid b$ implica que $b = ac$, entonces $\pm b = (\pm a)(\pm c)$ tomando signos apropiadamente, por lo que $|a| \mid |b|$

(7). Si $a \mid b$ y $b \neq 0$, entonces $|a| \mid |b|$, por lo que $|b| = |c| \cdot |a| \geq |a|$ si $c \neq 0$.

(8). El conjunto $A = \{na : n \in \mathbb{Z}\}$ está conformado por múltiplos de a y es claramente infinito.

(9). Dado que si $a \mid b$ y $b \neq 0$, entonces $|a| \leq |b|$, el conjunto de divisores de b está contenido en el conjunto $B = \{\pm n : n \in \mathbb{I}_{|b|}\}$, el cual es claramente finito.

(10). Si $(a \mid b \wedge b \mid a)$ entonces $b = ax$ y $a = by$, por lo tanto $b = (by)x$, lo cual se cumple si y sólo si $|x| = |y| = 1$, por lo que se deduce que $|a| = |b|$

(11). Si $a \mid b_1$ y $a \mid b_2$, entonces $a \mid x_1 b_1 \pm x_2 b_2$, ya que, si $b_1 = ay$ y $b_2 = az$, entonces:

$$x_1 b_1 \pm x_2 b_2 = x_1 ay \pm x_2 az = a(x_1 y \pm x_2 z)$$

El resultado es generalizable por inducción a sumatorias de términos finitos.

(12). Si $a \mid b_1$ y $a \mid b_1 + b_2$, entonces $a \mid b_2$, ya que $b_2 = (b_1 + b_2) - b_1$. Por lo visto en el item anterior, las sumas de múltiplos de a son múltiplos de a.

□

Teorema 5.1 (Existencia del algoritmo de división entera)**.** Dados $a, b \in \mathbb{Z}$ con $a \neq 0$, existe un único par $(q, r) \in \mathbb{Z}^2$ tal que $b = qa + r$ con $0 \leq r < |a|$. Al dividir b por a, llamaremos *divisor* a a, *dividendo* a b, *cociente* a q y *resto* a r. Notaremos $r_a(b)$ al resto obtenido al dividir b por a.

Dem. Supongamos $b \geq 0$. Sean $A = \{b - ka : k \in \mathbb{Z}\}$ y $B = A \cap \mathbb{N}_0$. Es evidente que $B \neq \emptyset$ (por ejemplo, $b \in B$ pues $b = b - 0 \cdot a$). Por lo tanto, por el principio de buena ordenación, existe $r = \min B$. Ahora bien, $r \geq 0$ dado que $r \in B$, y además existe $q \in \mathbb{Z}$ tal que $r = b - qa$, es decir $b = qa + r$, ya que $r \in A$. Sea $|a| = \sigma a$, donde $\sigma = \pm 1$; entonces:

$$r - |a| = b - qa - |a| = b - qa - \sigma a = b - (q + \sigma)a$$

Por lo tanto, $r - |a| \in A$ y además $r - |a| \notin B$ (en caso de pertenecer a B, $r - |a| < r = \min B$, lo cual sería absurdo). De esto deducimos que $r - |a| \notin \mathbb{N}_0$; por lo tanto, $r < |a|$.

De este modo el par (q, r) cumple lo pedido. Ahora mostraremos que dicho par es único. Supongamos que $(q', r') \in \mathbb{Z}^2$ también verifica lo pedido. Entonces:

$$0 = (q - q')a + r - r' \iff (q - q')a = r' - r$$

Es evidente que $r' = r \iff q' = q$ puesto que $a \neq 0$. Supongamos entonces que $r' \neq r$. Asumimos sin pérdida de generalidad que $r' > r$; entonces, dado que $a \mid r' - r$ y $r' - r \neq 0$, tenemos que:

$$|a| \leq |r' - r| = r' - r \leq r' < |a|$$

lo cual es obviamente absurdo; por lo tanto queda demostrada la unicidad del par (q, r).

En el caso en que $b < 0$ y $a > 0$, sabemos que existe un par $(t, s) \in \mathbb{Z}^2$ tal que $-b = ta + s$ con $0 \leq s < a$. Si $s = 0$, entonces $(-t, 0)$ cumple lo pedido; si $s > 0$, entonces $b = -ta - s + a - a = (-t - 1)a + a - s$, donde $0 \leq a - s < a$, por lo que el par $(-t - 1, a - s)$ cumple lo pedido.

Finalmente, si $b < 0$ y $a < 0$ sabemos que existe un par $(t, s) \in \mathbb{Z}^2$ tal que $-b = t(-a) + s$ con $0 \leq s < -a$. Si $s = 0$, entonces $(t, 0)$ cumple lo pedido; si $s > 0$, entonces $b = ta - s + a - a = (t + 1)a - a - s$, donde $0 \leq -a - s < -a = |a|$, por lo que el par $(t + 1, -a - s)$ cumple lo pedido. □

Corolario. Dados $n \in \mathbb{N}$, $x \in \mathbb{Z}$, se verifica que:

$$n \mid x \iff r_n(x) = 0$$

Lema 5.1. Dados $n \in \mathbb{N}$, $x, y \in \mathbb{Z}$ se verifica que:

$$r_n(x) = r_n(y) \iff n \mid y - x$$

Dem. ($\Rightarrow$) Si $r_n(x) = r_n(y)$, entonces $x = qn + r$ e $y = q'n + r$, por lo tanto $y - x = (q' - q)n$; entonces, $n \mid y - x$.

($\Leftarrow$) Si $n \mid y - x$, entonces $y - x = qn$, por lo tanto $y = qn + x$. Por el algoritmo de división, tenemos que $x = q'n + r$, por lo tanto, $y = qn + q'n + r$, o sea, $y = (q + q')n + r$, de lo que se deduce que $r_n(x) = r_n(y)$ □

Definición 5.2. Dados $n \in \mathbb{N}$, $x, y \in \mathbb{Z}$, decimos que x e y son *congruentes módulo n* si $r_n(x) = r_n(y)$ (o, equivalentemente, si $n \mid y - x$). En este caso notaremos $x \equiv y \pmod{n}$, o simplemente $x \equiv y \ (n)$.

Observación. La congruencia módulo n define una relación de equivalencia sobre $\mathbb{Z}$, y sus diferentes clases de equivalencia son llamadas *clases de congruencia*.

Dem. Es fácil ver que la congruencia módulo n es reflexiva, puesto que $r_n(x) = r_n(x)$, simétrica, dado que $r_n(x) = r_n(y) \iff r_n(y) = r_n(x)$ y transitiva, puesto que $(r_n(x) = r_n(y) \wedge r_n(y) = r_n(z)) \Rightarrow r_n(x) = r_n(z)$. □

Propiedades. Dados $n \in \mathbb{N}$, $x, y \in \mathbb{Z}$, se verifican las siguientes propiedades:

(1).
$$\sum_{i=1}^{k} x_i \equiv \sum_{i=1}^{k} r_n(x_i) \pmod{n}$$

(2).
$$\prod_{i=1}^{k} x_i \equiv \prod_{i=1}^{k} r_n(x_i) \pmod{n}$$

(3).
$$x^y \equiv r_n(x)^y \pmod{n}$$

Dem. Demostraremos (1) y (2) para sumas y productos de dos términos, pero el resultado es fácilmente generalizable a sumas y productos de términos finitos por inducción.

(1). Tenemos $x = qn + r_n(x)$ e $y = tn + r_n(y)$; por lo tanto:
$$x + y = (q + t)n + r_n(x) + r_n(y)$$
Entonces $x + y \equiv r_n(x) + r_n(y) \pmod{n}$ pues $n \mid x + y - (r_n(x) + r_n(y))$

(2).
$$\begin{aligned} xy &= qtn + r_n(x)tn + r_n(y)qn + r_n(x)r_n(y) \\ &= (qt + r_n(x)t + r_n(y)q)n + r_n(x)r_n(y) \end{aligned}$$
Entonces $xy \equiv r_n(x)r_n(y) \pmod{n}$ pues $n \mid xy - r_n(x)r_n(y)$

(3).
$$x^y = \prod_{i=1}^{y} x \equiv r_n(x)^y \pmod{n}$$

□

Proposición 5.1. Dada una *terna pitagórica* $a, b, c \in \mathbb{Z}$ (es decir, a, b, c tales que $a^2 + b^2 = c^2$), a o b (o ambos) deben ser pares.

Dem. Dado $x \in \mathbb{Z}$, es fácil ver que, si x es par, $x^2 \equiv 0 \pmod{4}$, puesto que $x^2 = (2k)^2 = 4k^2$. En caso contrario, $x^2 \equiv 1 \pmod{4}$, dado que $x^2 = (2k-1)^2 = 4k^2 - 4k + 1 = 4(k^2 - k) + 1$. Por lo tanto, si a y b son impares, entonces $a^2 + b^2 = c^2 \equiv 2 \pmod{4}$, lo cual es absurdo. □

Definición 5.3. Dados $a, b \in \mathbb{N}$, el *máximo común divisor* de a y b, notado $(a : b)$ es el mayor de los divisores comunes a ambos enteros. Formalmente:

$$(a : b) = \max A \cap B$$

donde A y B son los conjuntos cuyos elementos son los divisores de a y b respectivamente.

Extendemos la definición a $\mathbb{Z}$ de modo que, dados $x, y \in \mathbb{Z}$:

$$(x : y) = \begin{cases} (|x| : |y|) & \text{si } x \neq 0 \wedge y \neq 0 \\ |y| & \text{si } x = 0 \end{cases}$$

Observación. Dados $a, b \in \mathbb{Z}$, $(a : b) = a$ si y sólo si $a \mid b$.

Dem. Es obvio que $(a : b) = a$ implica $a \mid b$; el converso se demuestra considerando que todo divisor de a es también divisor de b si $a \mid b$, por lo que basta tomar al mayor divisor de a, el cual es a. □

Lema 5.2. Dados $a, b, k \in \mathbb{Z}$, se verifica que $(a : b) = (kb + a : b)$

Dem. Para demostrar este hecho basta con probar que ambos pares tienen los mismos divisores comunes. Dado un $c \in \mathbb{Z}$ tal que $c \mid a$ y $c \mid b$, entonces $c \mid kb + a$ por propiedades de la divisibilidad.

Consideremos entonces $d \in \mathbb{Z}$ tal que $d \mid kb + a$ y $d \mid b$. Como $d \mid b$, entonces $d \mid kb$, de lo que se deduce que $d \mid a$. □

Proposición 5.2. Dados $a, b \in \mathbb{Z}$, se verifica que $(a : b) = (a : r_a(b))$

Dem. $b = qa + r_a(b)$, por lo que $r_a(b) = b - qa$. Por el lema anterior, se verifica que $(a : b) = (a : b - qa)$ □

Algoritmo de Euclides. Sean $r_{-1}, r_0 \in \mathbb{N}$, con $r_{-1} \geq r_0$. A partir de estos valores, construiremos dos secuencias (q_i) y (r_i) de modo que

$$r_k = q_{k+2}\, r_{k+1} + r_{k+2}$$

Es claro que q_{k+2} y r_{k+2} quedan determinados por el algoritmo de la división, así que basta con nuestros valores iniciales para construir las sucesiones. Ahora bien, la sucesión de restos es una sucesión estrictamente decreciente de términos enteros no negativos, así que eventualmente llegará al 0. Ahora bien, es obvio que $(r_{-1} : r_0) = (r_j : r_{j+1})$ por la proposición anterior; de este modo es posible calcular $(r_{-1} : r_0)$ fácilmente aún con números de gran tamaño.

Definición 5.4. Dados $a, b, m \in \mathbb{Z}$ decimos que m es *combinación lineal* de a y b si existen $x, y \in \mathbb{Z}$ de modo que $m = ax + by$.

Lema 5.3. Dados $a, b \in \mathbb{Z}$, $(a : b)$ es combinación lineal de a y b.

Dem. Supongamos $a, b > 0$ (el caso en el que alguna variable es nula es trivial, y el caso negativo es análogo al que demostraremos). Sea r_n la primer entrada nula de la sucesión (r_i) construida en la utilización del algoritmo de Euclides sobre a y b.

Por inducción en n:
Si $n = 1$, entonces $a \mid b$ y entonces $(a : b) = 1 \cdot a + 0 \cdot b$.
Supongamos que la afirmación es válida para $n - 1$, con $n > 1$. Entonces $(a : b) = (a : r_1)$, y $(a : r_1)$ requiere $n - 1$ pasos en el algoritmo de Euclides, por lo que es combinación lineal de a y b por hipótesis inductiva. □

Proposición 5.3. Dados $a, b \in \mathbb{Z}$, solamente los múltiplos de $(a : b)$ pueden expresarse como combinación lineal de a y b.

Dem. Llamaremos $d = (a : b)$. Por el lema anterior, $d = ax_0 + by_0$. Si $d \mid m$, entonces:

$$m = dk = (ax_0 + by_0)k = a(x_0k) + b(y_0k)$$

Por lo tanto cualquier múltiplo de d es combinación lineal de a y b.

Ahora bien, supongamos que n es combinación lineal de a y b. Entonces, $n = au + bv$, pero $d \mid a$ y $d \mid b$, por lo que $d \mid au + bv = n$. Por lo tanto, cualquier combinación lineal de a y b es necesariamente un múltiplo de d. □

Proposición 5.4. Dados $a, b \in \mathbb{Z}$, si $d = (a : b)$, entonces d satisface que:

(1). $d \mid a$ y $d \mid b$
(2). $t \mid d$ para todo t divisor común de a y b

Ademas, d y $-d$ son los únicos enteros que satisfacen (1) y (2)

Dem. (1) es inmediato por la definición de d. Como $d = ax + by$, entonces, si $t \mid a$ y $t \mid b$, entonces $t \mid ax + by = d$, demostrando (2).

Supongamos ahora que d' también cumple (1) y (2). Entonces $d \mid d'$, puesto que $t \mid d'$ para todo divisor común t, pero también $d' \mid d$ por los mismos motivos. Se deduce entonces que $|d| = |d'|$ □

Definición 5.5. Dados $a, b \in \mathbb{Z}$, decimos que son *coprimos* si $(a : b) = 1$. En este caso notamos $a \perp b$.

Observación. $a \perp a + 1$ puesto que $1 = (-1)\, a + 1(a + 1)$

Proposición 5.5. Dados $a, b, d \in \mathbb{Z}$, entonces son equivalentes las siguientes afirmaciones:

(1). $d = (a : b)$
(2). $d \mid a, d \mid b$ y $\frac{a}{d} \perp \frac{b}{d}$
(3). $d \mid a, d \mid b$ y d es combinación lineal de a y b

Dem. $(1 \Rightarrow 2)$ Es claro que $d \mid a$ y $d \mid b$. Dado que d es combinación lineal de a y b, existen $x, y \in \mathbb{Z}$ de modo que $d = ax + by$. Pero entonces $1 = \frac{a}{d}x + \frac{b}{d}y$, de lo que deducimos que $\frac{a}{d}$ y $\frac{b}{d}$ son coprimos.

$(2 \Rightarrow 3)$ Por hipótesis, existen $x, y \in \mathbb{Z}$ tales que $1 = \frac{a}{d}x + \frac{b}{d}y$, por lo que, multiplicando por d, tenemos que $d = ax + by$.

$(3 \Rightarrow 1)$ Por hipótesis, sabemos que $d \mid a$ y $d \mid b$, por lo que existen $x, y \in \mathbb{Z}$ tales que $d = ax + by$. Dado un divisor común t de a y b, se deduce que $t \mid ax + by = d$, por lo que $d = (a : b)$ □

Proposición 5.6 (Lema de Euclides)**.** Dados $a, b, c \in \mathbb{Z}$, si $a \mid bc$ y $a \perp b$, entonces $a \mid c$.

Dem. Dado que $a \perp b$, existen $x, y \in \mathbb{Z}$ tales que $1 = ax + by$. Entonces $c = acx + bcy$. Dado que $a \mid bcy$ por hipótesis, y además $a \mid acx$, entonces $a \mid acx + bcy = c$. □

Proposición 5.7. Dados $a, b \in \mathbb{Z}$, si $a \perp b$, entonces $a^k \perp b^n$ para todo $n, k \in \mathbb{N}$

Dem. Dado que $a \perp b$, existen $x, y \in \mathbb{Z}$ tales que $1 = ax + by$. Entonces:

$$\begin{aligned} 1 = 1^n &= \sum_{k=0}^{n} \binom{n}{k} (ax)^{n-k} (by)^k \\ &= (by)^n + \sum_{k=0}^{n-1} \binom{n}{k} (ax)^{n-k} (by)^k \\ &= b^n y^n + a \left(\sum_{k=0}^{n-1} \binom{n}{k} a^{n-k-1} x^{n-k} (by)^k \right) \end{aligned}$$

Por lo tanto, $a \perp b^n$. Repitiendo el mismo argumento, concluimos que $a^k \perp b^n$ □

Proposición 5.8. Dados $a, b \in \mathbb{Z}$, $k \in \mathbb{N}$, se verifica que $(ka : kb) = k(a : b)$

Dem. Llamemos $d = (a : b)$. Es claro que $kd \mid ka$ y $kd \mid kb$; además, existen $x, y \in \mathbb{Z}$ tales que $d = ax + by$. Multiplicando por k, tenemos que $kd = (ka)x + (kb)y$, por lo que $(ka : kb) = kd$. □

Proposición 5.9. Dados $a, b \in \mathbb{Z}$, $n \in \mathbb{N}$, se verifica que $(a^n : b^n) = (a : b)^n$

Dem. Llamemos $d = (a : b)$. Entonces:

$$(a^n : b^n) = \left(d^n \frac{a^n}{d^n} : d^n \frac{b^n}{d^n} \right) = d^n \left(\frac{a^n}{d^n} : \frac{b^n}{d^n} \right)$$

Dado que $\frac{a}{d} \perp \frac{b}{d}$, por la proposición anterior tenemos que $\frac{a^n}{d^n} \perp \frac{b^n}{d^n}$, por lo que $(a^n : b^n) = d^n$ □

Proposición 5.10. Dados $a, b \in \mathbb{Z}$, $n \in \mathbb{N}$, $a^n \mid b^n$ si y sólo si $a \mid b$.

Dem. ($\Rightarrow$) $(a:b)^n = (a^n : b^n) = a^n$ dado que $a^n \mid b^n$. Es inmediato entonces que $a = (a:b)$, por lo que $a \mid b$.

($\Leftarrow$) Si $a \mid b$, entonces $b = ka$. Por lo tanto, $b^n = k^n a^n$, y es obvio que $a^n \mid k^n a^n$ □

Identidad de Bézout. Dados $a, b, c \in \mathbb{Z}$ con $ab \neq 0$, la *ecuación lineal diofántica* (o *diofantina*) $ax + by = c$ posee infinitas soluciones $(x, y) \in \mathbb{Z}^2$ siempre que $(a:b) \mid c$; de lo contrario no existen soluciones.

Dem. Supongamos que $d = (a:b) \mid c$; de lo contrario, no existen soluciones, dado que toda combinación lineal de a y b es múltiplo de c. Entonces, $c = dk$. Sabemos que existen $\alpha, \beta \in \mathbb{Z}$ tales que $a\alpha + b\beta = d$. Multiplicando por k, tenemos que $a(\alpha k) + b(\beta k) = dk = c$. Por lo tanto, existe al menos una solución, de la forma $(\alpha k, \beta k)$.

Si (x_0, y_0) es una solución puntual, supongamos una solución genérica cualquiera (x, y). Entonces:

$$\begin{aligned} & ax + by = c = ax_0 + by_0 \\ \iff & a(x - x_0) + b(y - y_0) = 0 \\ \iff & \frac{a}{d}(x - x_0) = \frac{b}{d}(y_0 - y) \end{aligned}$$

Dado que $\frac{a}{d} \mid \frac{b}{d}(y_0 - y)$ y $\frac{a}{d} \perp \frac{b}{d}$, por el Lema de Euclides, tenemos que $\frac{a}{d} \mid y_0 - y$. Utilizando un razonamiento simétrico, concluimos que también $\frac{b}{d} \mid x - x_0$. Por lo tanto, $y_0 - y = \frac{a}{d}k$ y $x - x_0 = \frac{b}{d}t$. Reemplazando en la igualdad anterior, se verifica que:

$$\frac{ab}{d^2}k = \frac{ba}{d^2}t$$

Por lo tanto, $k = t$. Finalmente, tenemos que una solución genérica a la ecuación tiene la siguiente forma:

$$(x, y) = \left(x_0 + \frac{b}{d}k, y_0 - \frac{a}{d}k\right)$$

para cualquier $k \in \mathbb{Z}$. Es fácil ver que, de hecho, (x, y) es solución, dado que:

$$a\left(x_0 + \frac{b}{d}k\right) + b\left(y_0 - \frac{a}{d}k\right) = ax_0 + by_0 = c$$

□

Definición 5.6. Llamamos *ecuación lineal de congruencia* a cualquier ecuación de la forma:

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

donde $a, b, m, x \in \mathbb{Z}$.

Es claro que, si x es solución de la ecuación, entonces toda la clase de congruencia módulo m

de x también lo es. Por otra parte, si x es solución, existe $k \in \mathbb{Z}$ de modo que $ax + mk = b$; por lo tanto, la ecuación $ax \equiv b \ (m)$ es resoluble si y sólo si la ecuación diofántica $ax + mk = b$ es resoluble; es decir, si $(a : m) \mid b$.

Suponiendo que esta última condición se cumple, sea x_0 una solución (que corresponde con una solución (x_0, k_0) de la ecuación diofántica $ax + mk = b$). En tal caso, todas las soluciones de la ecuación lineal de congruencia son de la forma $x_0 + \frac{m}{d}t$, donde $d = (a : b)$ y $t \in \mathbb{Z}$. Llamemos $x_t = x_0 + \frac{m}{d}t$. Utilizando el algoritmo de la división, dividimos t por d; entonces $t = qd + r$, con $0 \leq r < d$. Luego:

$$x_t = x_0 + \frac{m}{d}t = x_0 + \frac{m}{d}(qd + r) = x_0 + mq + \frac{m}{d}r \equiv x_0 + \frac{m}{d}r = x_r \pmod{m}$$

Por lo tanto, la ecuación lineal de congruencia admite a lo sumo d soluciones módulo m, a saber, las clases de congruencia de x_0, $x_0 + \frac{m}{d}$, $x_0 + 2\frac{m}{d}$, $\cdots$, $x_0 + (d-1)\frac{m}{d}$.

Veamos finalmente que todas estas soluciones son diferentes módulo m. Suponiendo lo contrario, existen índices $i, j \in \mathbb{Z}$ distintos tales que $0 \leq i < j \leq d - 1$ y:

$$x_i = x_0 + i\frac{m}{d} \equiv x_0 + j\frac{m}{d} = x_j \pmod{m}$$

Pero entonces existe $h \in \mathbb{Z}$ tal que:

$$\begin{aligned} \left(x_0 + j\frac{m}{d}\right) - \left(x_0 + i\frac{m}{d}\right) &= mh \\ \iff (j-i)\frac{m}{d} &= mh \\ \iff j - i &= dh \end{aligned}$$

lo cual implica $d \mid j - i$, lo cual es absurdo puesto que $0 < j - i \leq d - 1$.

Como una ecuación lineal de congruencia presenta d soluciones módulo m, al hablar de soluciones nos referiremos a clases de congruencia y no a enteros en particular.

Corolario. Dados $a, m \in \mathbb{Z}$, a posee inversa módulo m (es decir, existe b tal que $ab \equiv 1 \pmod{m}$) si y sólo si $a \perp m$, es decir, $(a : m) = 1$ (para garantizar la resolubilidad de la ecuación lineal de congruencia).

Proposición 5.11. Dados $a, b, m, x \in \mathbb{Z}$, si $ax \equiv b \ (m)$ y d es divisor común de a, b y m, entonces:

$$\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$$

Dem. Si $ax \equiv b \ (m)$, existe $k \in \mathbb{Z}$ tal que $ax + bk = m$, entonces:

$$\frac{a}{d}x + \frac{b}{d}k = \frac{m}{d} \iff \frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$$

□

Proposición 5.12. Dados $a, b, c, m \in \mathbb{Z}$, si $ac \equiv bc \pmod{m}$ y $c \perp m$, entonces $a \equiv b \pmod{m}$.

Dem. Si $ac \equiv bc \pmod{m}$, entonces $m \mid ac - bc = (a-b)c$. Dado que $c \perp m$, entonces $m \mid a - b$, es decir, $a \equiv b \pmod{m}$. □

Definición 5.7. Decimos que $a \in \mathbb{Z}$ es *primo* si admite exactamente 4 divisores $(a, -a, 1, -1)$. Si $|a| \neq 1$ y a no es primo, decimos que a es *compuesto*. Notamos $\mathbb{P}$ al conjunto de números primos.

A pesar de que $a \in \mathbb{P} \iff -a \in \mathbb{P}$, normalmente nos referimos a primos positivos al hablar de un primo genérico. Cabe destacar que 1 y -1 no son primos (ni compuestos).

Observación. Si $a \in \mathbb{P}$, sus únicas factorizaciones son $a = 1\,a = (-1)(-a)$; mientras que si a es compuesto, admite al menos una factorización no trivial, es decir, $a = bc$ donde $1 < b, c < a$ (asumiendo a positivo).

Proposición 5.13. Todo entero $a > 1$ es divisible por algún primo.

Dem. Sea $D = \{n \in \mathbb{N} : (n \mid a) \wedge (n > 1)\}$, es decir, el conjunto de divisores mayores a 1 de a. Es claro que $D \neq \emptyset$ pues $a \in D$. Entonces, por el principio de buena ordenación, existe $p = \min D$. Ahora bien, si p fuera compuesto, admitiría una factorización tal que $p = xy$ con $1 < x, y < p$. En ese caso, $x \mid p$, pero $p \mid a$; entonces, por transitividad, $x \mid a$. Entonces $x \in D$, pero $x < p$, lo cual es absurdo. Concluimos entonces que p es primo y divide a a. □

Corolario (Teorema de Euclides)**.** El conjunto $\mathbb{P}$ es infinito.

Dem. Sean $p_1, p_2, \ldots, p_r$ un conjunto finito de primos. Consideremos el número $A = 1 + \prod_{i=1}^{r} p_i$. Como $A > 1$, existe $q \in \mathbb{P}$ tal que $q \mid A$. Dado que $q \nmid 1$, entonces $q \nmid \prod_{i=1}^{r} p_i$ y consecuentemente $q \nmid p_j$ para cualquier $j \leq r$. □

Corolario (Criterio de Eratóstenes)**.** Si $n \in \mathbb{N}$ es compuesto, existe $p \in \mathbb{P}$ tal que $p \mid n$ y $p \leq \sqrt{n}$

Dem. Como n es compuesto, admite una factorización no trivial $n = xy$. Podemos suponer sin pérdida de generalidad que $x \leq \sqrt{n} \leq y$, dado que si tanto x como y son menores a $\sqrt{n}$, entonces $xy < \sqrt{n}^2 < n$ (si ambos son mayores, el razonamiento es análogo). Por la proposición anterior, existe un primo p tal que $p \mid x$, y por transitividad $p \mid n$. □

Proposición 5.14. Todo $n \in \mathbb{N}$ mayor a 1 es producto de números primos.

Dem. Por inducción global en n:
Es claro que 2 es producto de primos, ya que 2 es primo. Supongamos $n > 2$ y que el resultado es válido para todo m tal que $1 < m < n$. Si n es primo, no hay nada que demostrar. Si n es compuesto, entonces $n = xy$ con $1 < x, y < n$. Pero por hipótesis inductiva, x e y son productos de primos; por lo tanto n también lo es. □

Proposición 5.15. Sean $a, b \in \mathbb{Z}$, $p \in \mathbb{P}$. Se verifican las siguientes propiedades:

(1). $p \mid a$ o bien $p \perp a$

(2). $p \mid ab$ implica que $p \mid a$ o bien $p \mid b$

(3). Generalizando el resultado anterior, $p \mid \prod_{i=1}^{r} x_i$ implica $p \mid x_j$ para algún $j \leq r$

Dem. (1). Es claro que $(a : p) = p$ o bien $(a : p) = 1$, por lo tanto $p \mid a$ o $p \perp a$.

(2). Dado $p \mid ab$, supongamos $p \nmid a$. Por la propiedad anterior, $p \perp a$; entonces $p \mid b$ por el lema de Euclides.

(3). La generalización se obtiene fácilmente por inducción en r sobre el resultado anterior. □

Teorema fundamental de la aritmética. Todo número natural n posee una única factorización (obviando permutaciones de factores) de la forma:

$$n = \prod_{i=1}^{n} p_i^{\alpha_i}$$

donde $r \in \mathbb{N}_0$, $p_1, p_2, \ldots, p_r \in \mathbb{P}$ tal que $p_i > 0$ y $p_i \neq p_j$ si $i \neq j$ y $\alpha_i \in \mathbb{N}$.

Dem. Ya hemos demostrado que todo número $n \in \mathbb{N}$ admite una factorización prima; falta demostrar su unicidad.

Supongamos que $n = p_1^{\alpha_1} \ldots p_r^{\alpha_r} = q_1^{\beta_1} \ldots q_s^{\beta_s}$ donde q_i y β_i satisfacen las mismas condiciones de la hipótesis. Ahora bien, dado i tal que $1 \leq i \leq r$, es claro que $p_i \mid n = q_1^{\beta_1} \ldots q_s^{\beta_s}$. Dado que $p_i \in \mathbb{P}$ entonces existe j tal que $p_i \mid q_j^{\beta_j}$, pero como también $q_j \in \mathbb{P}$ entonces $p_i \mid q_j$, pero esto sólo es posible si $p_i = q_j$, dado que ambos son primos. Por lo tanto, $\{p_i\}_{i \leq r} = \{q_j\}_{j \leq r}$ (la doble contención es probada por un razonamiento simétrico, lo cual también implica la igualdad $r = s$).

Resta entonces demostrar que $\alpha_i = \beta_i$ para todo $i \leq r$. Supongamos que existe cierto i tal que $\alpha_i \neq \beta_i$. Asumimos sin pérdida de generalidad $\alpha_i < \beta_i$. Entonces:

$$np_i^{-\alpha_i} = p_1^{\alpha_1} \ldots p_{i-1}^{\alpha_{i-1}} p_{i+1}^{\alpha_{i+1}} \ldots p_r^{\alpha^r} = p_1^{\beta_1} \ldots p_i^{\beta_i - \alpha_i} \ldots p_r^{\beta_r}$$

Como $\beta_i - \alpha_i > 0$, entonces $p_i \mid p_1^{\beta_1} \ldots p_i^{\beta_i - \alpha_i} \ldots p_r^{\beta_r} = p_1^{\alpha_1} \ldots p_{i-1}^{\alpha_{i-1}} p_{i+1}^{\alpha_{i+1}} \ldots p_r^{\alpha^r}$. Por lo tanto, existe $k \neq i$ tal que $p_i \mid p_k^{\alpha_k}$, pero del mismo modo que la demostración anterior, esto implica $p_i = p_k$ lo cual es absurdo. Se deduce entonces que $\alpha_i = \beta_i$ para todo $i \leq r$. □

Enunciaremos una serie de corolarios del teorema fundamental de la aritmética. Para ellos, definimos $a \in \mathbb{N}$, que presentará una factorización prima a la que notaremos $a = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$

Corolario 5.1. $\{p_1, \ldots, p_r\}$ es el conjunto de divisores primos de a.

Dem. Es claro que $p_i \mid a$ para todo $i \leq r$. Recíprocamente, supongamos $q \in \mathbb{P}$ tal que $q \mid a$; entonces $q \mid p_1^{\alpha_1} \ldots p_r^{\alpha_r}$ y por lo tanto $q = p_i$ para algún i, hecho que se deduce con la misma técnica usada en la demostración del teorema. □

Corolario 5.2. $\alpha_k = \max\{n \in \mathbb{N} : p_k^n \mid a\}$

Dem. Es claro que $p_k^{\alpha_k} \mid a$. Suponiendo $p_k^{\alpha_{k+1}} \mid a$, entonces $a = p_k^{\alpha_{k+1}} b$ con $b \in \mathbb{Z}$. Si divimos por esta expresión por $p_k^{\alpha_k}$, tenemos:

$$p_1^{\alpha_1} \dots p_{k-1}^{\alpha_{k-1}} p_{k+1}^{\alpha_{k+1}} \dots p_r^{\alpha^r} = p_k b$$

Pero entonces $p_k \mid p_1^{\alpha_1} \dots p_{k-1}^{\alpha_{k-1}} p_{k+1}^{\alpha_{k+1}} \dots p_r^{\alpha^r}$, y entonces $p_k = p_i$ para algún $i \leq r$, lo cual es absurdo. □

Corolario 5.3. Si $b \in \mathbb{N}$ entonces $a \mid b$ si y sólo si $p_i^{\alpha_i} \mid b$ para todo $i \leq r$

Dem. ($\Rightarrow$) $p_i^{\alpha_i} \mid a$ y $a \mid b$, entonces $p_i^{\alpha_i} \mid b$ por transitividad.

($\Leftarrow$) Si $p_i^{\alpha_i} \mid b$ para todo $i \leq r$, entonces, por los corolarios anteriores, la factorización prima de b será de forma:

$$b = p_1^{\alpha_1'} \dots p_r^{\alpha_r'} q_1^{\beta_1} \dots q_s^{\beta_s}$$

con $\alpha_i' \geq \alpha_i$ y q_j distintos de los p_i. Esto es:

$$b = q_1^{\beta_1} \dots q_s^{\beta_s} p_1^{\alpha_1} \dots p_r^{\alpha_r} p_1^{\alpha_1'-\alpha_1} \dots p_r^{\alpha_r-\alpha_r'} = q_1^{\beta_1} \dots q_s^{\beta_s} a p_1^{\alpha_1'-\alpha_1} \dots p_r^{\alpha_r-\alpha_r'}$$

Por lo tanto, $a \mid b$ □

Corolario 5.4. Dados $m, n \in \mathbb{N}$, $m \mid n$ si y sólo si todo primo en la factorización de m aparece también en la de n con mayor o igual exponente. La demostración es inmediata a partir del corolario anterior.

Corolario 5.5. *a posee exactamente $\prod_{i=1}^{r}(\alpha_i + 1)$ divisores positivos.*

Dem. Todo divisor positivo de a es de la forma $d = p_1^{\alpha_1'} \dots p_r^{\alpha_r'}$ donde $0 \leq \alpha_i' \leq \alpha_i$. Luego, el resultado se deduce por combinatoria, aplicando el principio multiplicativo. □

Corolario 5.6. Sean $b_1, \dots, b_n$ divisores de a tales que son coprimos entre sí. Entonces $\prod_{i=1}^{n} a_i \mid b$.

Dem. Dado que los divisores son coprimos, no poseen ningún primo en común en todas sus factorizaciones; por lo tanto, al multiplicarlos entre sí no se da lugar a algún crecimiento de exponentes sobre ningún factor primo, y dado que todos dividen a a, entonces el producto también lo hace. □

Corolario 5.7. Sean $a, b \in \mathbb{N}$ con factorizaciones primas $a = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ y $b = p_1^{\beta_1} \dots p_r^{\beta_r}$ (admitiendo $\alpha_i, \beta_i = 0$). Entonces:

$$(a : b) = \prod_{i=1}^{r} p_i^{\min\{\alpha_i, \beta_i\}}$$

Definición 5.8. Dados $a, b \in \mathbb{N}$, el *mínimo común múltiplo* de a y b, al cual notaremos $[a : b]$, es $m \in \mathbb{N}$ tal que $a \mid m$, $b \mid m$ y, si t es un múltiplo común de a y b, entonces $m \mid t$. La noción es extensible a $\mathbb{Z}$ del mismo modo que se generalizó el máximo común divisor.

Podemos demostrar que dicho número existe; más aún, vale la fórmula

$$[a : b] = \frac{ab}{(a : b)}$$

para todo $a, b \in \mathbb{N}$; demostremos este hecho. Llamemos $m = [a : b]$ y $d = (a : b)$. Es claro que $m = a\frac{b}{d} = b\frac{a}{d}$ por lo que $m \mid a$ y $m \mid b$. Si $t = \alpha a = \beta b$, es decir, es un múltiplo común de a y b, entonces:

$$\frac{t}{d} = \frac{a}{d}\alpha = \frac{b}{d}\beta$$

Entonces $\frac{a}{d} \mid \frac{b}{d}\beta$, pero entonces $\frac{a}{d} \mid \beta$ pues $\frac{a}{d} \perp \frac{b}{d}$. Por lo tanto:

$$t = \frac{a}{d}kb = \frac{ab}{d}k = mk$$

Teorema chino del resto. Sean $m_1, m_2, \ldots, m_r \in \mathbb{N}$ coprimos dos a dos, y sea $m = \prod_{i=1}^{r} m_i$, entonces, dados $a_1, a_2, \ldots, a_r \in \mathbb{Z}$ cualesquiera, existe $x \in \mathbb{Z}$ tal que $x \equiv a_i \pmod{m_i}$ para todo i tal que $1 \leq i \leq r$, y además, dicha solución x es única módulo m.

Dem. Para cada índice i, definimos M_i tal que:

$$M_i = \prod_{\substack{j=1 \\ j \neq i}}^{r} m_j = \frac{m}{m_i}$$

Es claro que $M_i \perp m_i$, dado que M_i es un producto de factores coprimos a m_i. Luego, la ecuación $M_i\nu \equiv 1 \pmod{m_i}$ es resoluble. Sea entonces ν_i una solución para el índice i. Entonces, definimos $x = \sum_{k=1}^{r} M_k\nu_k a_k$. x satisface lo pedido, dado que:

$$x = \sum_{k=1}^{r} M_k\nu_k a_k \equiv M_i\nu_i a_i \equiv a_i \pmod{m_i}$$

Demostramos ahora la unicidad de la solución, módulo m. Si $y \equiv x \pmod{m}$, entonces $y \equiv x \pmod{m_i}$ para todo i, dado que $m \mid y - x$ implica $m_i \mid y - x$ por transitividad. Por lo tanto y también es solución.

Recíprocamente, supongamos que x' es otra solución. Entonces $x' \equiv x \pmod{m_i}$ para todo i, por lo que $m_i \mid x - x'$. Dado que los m_i son coprimos dos a dos, esto implica que $m \mid x - x'$, es decir $x' \equiv x \pmod{m}$. □

Pequeño teorema de Fermat. Sean $a \in \mathbb{Z}$ y p un primo tal que $p \nmid a$. Entonces $a^{p-1} \equiv 1 \pmod{p}$.

Dem. Suponiendo sin pérdida de generalidad p positivo, consideremos el intervalo $\mathbb{I}_{p-1}$. Si $k \in \mathbb{I}_{p-1}$, entonces $p \nmid ka$, pues $p \nmid k$ dado que $k < p$ y p es primo, y $p \nmid a$ por hipótesis. Por lo tanto, $ka \equiv x_k \pmod{p}$, con $x_k \in \mathbb{I}_{p-1}$. Ahora bien, $x_i \neq x_j$ si $i \neq j$, puesto que, en caso contrario:

$$ia \equiv x_i = x_j \equiv ja \pmod{p}$$

Dado que $a \perp p$, esto implica $i \equiv j \pmod{p}$ lo cual es claramente absurdo.

Por lo tanto, por el principio del palomar, concluimos que $\{x_1, \ldots, x_{p-1}\} = \mathbb{I}_{p-1}$, es decir, los x_i forman una permutación de $\mathbb{I}_{p-1}$. Ahora bien, multiplicando las congruencias $ka \equiv x_k \pmod{p}$, obtenemos la identidad:

$$a^{p-1}(p-1)! \equiv \prod_{i=1}^{p-1} x_i \pmod{p}$$

Pero es claro que $(p-1)! = \prod_{i=1}^{p-1} x_i$, dado que los factores de cada producto son los mismos, obviando la permutación. Además, $(p-1)! \perp p$, pues $(p-1)!$ es un producto de factores coprimos a p. Podemos entonces cancelar ambos términos de la congruencia, obteniendo:

$$a^{p-1} \equiv 1 \pmod{p}$$

Este resultado es equivalente a claramente equivalente a $a^p \equiv a \pmod{p}$; sin embargo, este último vale incluso cuando $p \mid a$, ya que en dicho caso la identidad se reduce a $a^p \equiv 0 \equiv a \pmod{p}$. □

Definición 5.9. Sea $a \in \mathbb{Z}$ y p primo tales que $p \nmid a$. Definimos entonces el *orden multiplicativo de a módulo p* de modo que:

$$\operatorname{ord}_p(a) = \min\left\{k \in \mathbb{N} : a^k \equiv 1 \pmod{p}\right\}$$

La existencia de dicho mínimo está garantizada por el principio de buena ordenación, puesto que el conjunto es no vacío (en particular, el teorema de Fermat garantiza la pertenencia de $p-1$).

Proposición 5.16. Sea $m = \operatorname{ord}_p(a)$, entonces $m \mid p-1$. Más aún, para cualquier $t \in \mathbb{N}$, $a^t \equiv 1 \pmod{p}$ si y sólo si $m \mid t$.

Dem. Sea $r = r_m(p-1)$, es decir, $p-1 = qm + r$, con $0 \leq r < m$. Luego, por el teorema de Fermat:

$$1 \equiv a^{p-1} \equiv a^{qm} a^r \equiv (a^m)^q a^r \equiv a^r \pmod{p}$$

Es evidente entonces que $r = 0$, por lo tanto, $m \mid p-1$. El mismo razonamiento demuestra que $a^t \equiv 1 \pmod{p}$ implica $m \mid t$.

Además, si $m \mid t$, entonces $t = km$ con $k \in \mathbb{Z}$. Entonces:

$$a^t \equiv a^{km} \equiv (a^m)^k \equiv 1 \pmod{p}$$

□

6. El cuerpo de números complejos $\mathbb{C}$

Definición 6.1. Definimos sobre $\mathbb{R}^2$ dos operaciones, a las que llamaremos de modo génerico *suma* $(+)$ y *producto* $(\cdot)$, de modo que, si $z, w \in \mathbb{R}^2$ tales que $z = (a, b)$, $w = (c, d)$:

$$z + w = (a + c,\ b + d)$$
$$zw = (ac - bd,\ ad + bc)$$

Propiedades. Enunciamos algunas propiedades sobre estas operaciones:

(1). La suma y el producto son operaciones asociativas y conmutativas.
(2). $(0, 0)$ es el elemento neutro de la suma; $(1, 0)$ es el elemento neutro del producto.
(3). Dado $z = (a, b) \in \mathbb{R}^2$, existe $w \in \mathbb{R}^2$ tal que $z + w = (0, 0)$. En efecto, basta tomar $w = (-a, -b)$. w será notado $-z$ y lo llamaremos el *inverso aditivo de* z.
(4). Dado $z = (a, b) \in \mathbb{R}^2$ tal que $z \neq (0, 0)$, existe $w \in \mathbb{R}^2$ tal que $zw = (1, 0)$. En efecto, basta tomar $w = \left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right)$. w será notado z^{-1} y lo llamaremos el *inverso multiplicativo de* z.
(5). El producto es distributivo respecto de la suma.

En consecuencia, $\mathbb{R}^2$ es, respecto de estas operaciones, un cuerpo, al cual llamaremos *cuerpo de números complejos* y notaremos $\mathbb{C}$.

Definición 6.2. A partir de la suma y el producto, podemos definir otras dos operaciones: la *diferencia* $(-)$ y el *cociente* $(\div)$, de modo que, si $z, w \in \mathbb{C}$ tales que $z = (a, b)$, $w = (c, d)$:

$$z - w = z + (-w)$$
$$\frac{z}{w} = zw^{-1}$$

Observación 6.1. Consideremos la función $\phi : \mathbb{R} \to \mathbb{C}$ definida por $\phi(x) = (x, 0)$. Es claro que ϕ es inyectiva; entonces, a partir de ahora identificaremos a $\mathbb{R}$ como $\mathrm{Im}(\phi) = \{(a, b) \in \mathbb{C} : b = 0\}$, permitiendo el abuso de notación para referirnos al par $(x, 0)$ como simplemente x y afirmar que vale la inclusión $\mathbb{R} \subseteq \mathbb{C}$. Es inmediato entonces verificar las siguientes propiedades (válidas para todo $a, b \in \mathbb{R}$):

(1). $\phi(a + b) = (a + b, 0) = (a, 0) + (b, 0) = \phi(a) + \phi(b)$
(2). $\phi(ab) = (ab, 0) = (a, 0)(b, 0) = \phi(a)\phi(b)$
(3). $\phi(0) = (0, 0)$ y $\phi(1) = (1, 0)$, por lo tanto los elementos neutros de $\mathbb{R}$ se corresponden con sus contrapartes de $\mathbb{C}$.
(4). $\phi(-a) = (-a, 0) = -(a, 0)$
(5). $\phi(a^{-1}) = (a^{-1}, 0) = (a, 0)^{-1}$ siempre que $a \neq 0$

Definición 6.3. Sea $(a, b) \in \mathbb{C}$. Tenemos entonces:

$$(a, b) = (a, 0) + (0, b) = (a, 0) + (b, 0)(0, 1) = a + b(0, 1)$$

Notaremos $i = (0,1)$, a la cual llamaremos la *unidad imaginaria*. De este modo, $(a,b) = a + bi$, expresión a la que llamaremos *forma binómica de* (a,b). Por lo tanto, $\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\}$ y $\mathbb{R} = \{a + bi \in \mathbb{C} : b = 0\}$. Podemos verificar que la forma binómica concuerda con el modo en el cual definimos la suma y el producto, puesto que:

$$(a + bi) + (c + di) = (a + c) + (b + d)i$$
$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i$$

Además, dado $z = (a,b) \in \mathbb{C}$, decimos que a es la *parte real* y b la *parte imaginaria* de z, notadas $a = \mathrm{Re}(z)$ y $b = \mathrm{Im}(z)$ respectivamente. Si $\mathrm{Re}(z) = 0$, decimos que z es *imaginario puro*. Es claro además que $z = w$ si y sólo si sus partes reales e imaginarias son iguales.

Proposición 6.1. Se verifica que $i^2 = -1$. Además, $i^n = i^{r_4(n)}$. para todo $n \in \mathbb{N}$.

Dem. La primera identidad es inmediata pues:

$$i^2 = (0,1)(0,1) = (-1,0) = -1$$

Luego,

$$i^4 = \left(i^2\right)^2 = (-1)^2 = 1$$

Entonces, dado un natural $n = 4q + r_4(n)$:

$$i^n = i^{4q + r_4(n)} = \left(i^4\right)^q i^{r_4(n)} = 1^q i^{r_4(n)} = i^{r_4(n)}$$

Más aún:

$$i^n = \begin{cases} 1 & \text{si } n \equiv 0 \pmod 4 \\ i & \text{si } n \equiv 1 \pmod 4 \\ -1 & \text{si } n \equiv 2 \pmod 4 \\ -i & \text{si } n \equiv 3 \pmod 4 \end{cases}$$

Definiendo i^{-n} como $(i^n)^{-1}$, la fórmula anterior sigue siendo válida para exponentes negativos. □

Observación 6.2. A partir del hecho de que $i^2 = -1$, se deduce que todo real x negativo admite (dos) raíces cuadradas en $\mathbb{C}$; a saber, $\pm\sqrt{|x|}i$.

Definición 6.4. Dado $z = a + bi \in \mathbb{C}$, definimos a la función *módulo*, notada $|\cdot| : \mathbb{C} \to \mathbb{R}_{\geq 0}$, de modo que $|z| = \sqrt{a^2 + b^2}$. Esta definición surge naturalmente a partir de la interpretación geométrica de $\mathbb{C}$ como un plano aplicando el teorema de Pitágoras. Cabe destacar también que podemos pensar esta función como una extensión de la función módulo real y que induce una métrica sobre $\mathbb{C}$ suponiendo $d(z,w) = |z - w|$.

Definición 6.5. Dado $z = a + bi \in \mathbb{C}$, definimos a su *conjugado*, notado $\overline{z}$, de modo que $\overline{z} = a - bi$.

Propiedades. Enunciamos algunas propiedades del módulo y los conjugados. Sean $z = a + bi, w = c + di \in \mathbb{C}$:

(1). $\overline{(\overline{z})} = z$
(2). $\overline{z+w} = \overline{z} + \overline{w}$
(3). $\overline{zw} = \overline{z} \cdot \overline{w}$
(4). $\overline{z^n} = \overline{z}^n$ con $n \in \mathbb{Z}, z \neq 0$
(5). $z + \overline{z} = 2\,\mathrm{Re}(z)$
(6). $z - \overline{z} = 2i\,\mathrm{Im}(z)$
(7). $z \cdot \overline{z} = (a+bi)(a-bi) = a^2 + b^2 = |z|^2$
(8). $z^{-1} = \frac{\overline{z}}{|z|^2}$ con $z \neq 0$ (se deduce de la propiedad anterior)
(9). $|z| \geq 0$. Más aún, $|z| = 0$ si y sólo si $z = 0$
(10). $|zw| = |z| \cdot |w|$
(11). $|z^n| = |z|^n$ con $n \in \mathbb{Z}, z \neq 0$

Proposición 6.2. Se verifica para todo $z, w \in \mathbb{C}$ la siguiente desigualdad, conocida como *desigualdad triangular:*

$$|z+w| \leq |z| + |w|$$

Dem.

$$\begin{aligned}
|z+w|^2 &= (z+w)\overline{(z+w)} \\
&= (z+w)(\overline{z}+\overline{w}) \\
&= z\overline{z} + z\overline{w} + w\overline{z} + w\overline{w} \\
&= |z|^2 + |w|^2 + z\overline{w} + \overline{z}w \\
&= |z|^2 + |w|^2 + \overline{\overline{z}w} + \overline{z}w \\
&= |z|^2 + |w|^2 + 2\,\mathrm{Re}\,(\overline{z}w) \\
&\leq |z|^2 + 2\,|\mathrm{Re}\,(\overline{z}w)| + |w|^2 \\
&\leq |z|^2 + 2\,|\overline{z}w| + |w|^2 \\
&= |z|^2 + 2|z| \cdot |w| + |w|^2 \\
&= (|z| + |w|)^2
\end{aligned}$$

Por lo tanto, dado que $|x| \geq 0$, deducimos que $|z+w| \leq |z| + |w|$. □

Proposición 6.3. Todo $z \in \mathbb{C}$ no nulo admite exactamente dos raíces cuadradas, es decir, existen exactamente dos $w \in \mathbb{C}$ tal que $z = w^2$.

Dem. Supongamos $z \notin \mathbb{R}$ (este resultado ya fue probado anteriormente), es decir, $z = a + bi$ con $b \neq 0$. Supongamos que $w = c + di$ es una posible solución. Esto es, $a + bi = (c+di)^2 = c^2 - d^2 + 2cdi$. Además, $|z| = |w|^2$, por lo que $c^2 + d^2 = |z|$, por lo que obtenemos el siguiente sistema de ecuaciones:

$$\begin{cases} c^2 - d^2 &= a \\ 2cd &= b \\ c^2 + d^2 &= |z| \end{cases}$$

Despejando, obtenemos:

$$c = \pm\sqrt{\frac{|z| + a}{2}}$$
$$d = \pm\sqrt{\frac{|z| - a}{2}}$$

Debido a que $2cd = b$, debemos elegir c y d de modo que su producto tenga el mismo signo que b, de modo que tenemos dos maneras de hacerlo (c y d del mismo signo si $b > 0$, de signos opuestos si $b < 0$). □

Definición 6.6. Sea $z = a + bi \in \mathbb{C}$ no nulo, observando que $\left|\frac{z}{|z|}\right| = 1$, resulta que $\frac{a}{|z|} + \frac{b}{|z|}i$ es un punto de la circunferencia unitaria centrada al origen. Por lo tanto, existe un único $\theta \in [0, 2\pi)$ de modo que:

$$\begin{cases} \frac{a}{|z|} & = \cos\theta \\ \frac{b}{|z|} & = \operatorname{sen}\theta \end{cases}$$

En consecuencia, $z = |z|\,(\cos\theta + i\operatorname{sen}\theta)$. Llamamos a esta última expresión la *forma trigonométrica* (o *forma polar*) de z. El número real θ es llamado el *argumento principal* de z, y es notado $\theta = \arg(z)$. Notaremos, para facilitar la escritura, $\mathbb{C}^* = \mathbb{C} - \{0\}$.

Definición 6.7. Dados $z = a + bi \in \mathbb{C}^*$ y $\alpha = \arg(z)$, debido a la periodicidad de las funciones seno y coseno, tenemos, para cualquier $k \in \mathbb{Z}$:

$$z = |z|\,(\cos(\alpha + 2k\pi) + i\operatorname{sen}(\alpha + 2k\pi))$$

Esto motiva la introducción del concepto de *congruencia módulo* 2π, de modo similar a la congruencia entera. Dados $x, y \in \mathbb{R}$, decimos que x es congruente con y módulo 2π si existe $k \in \mathbb{Z}$ tal que $y - x = 2k\pi$. En tal caso notamos $x \equiv y \pmod{2\pi}$. Cabe destacar que, dado $x \in \mathbb{R}$, existe un único $y \in [0, 2\pi)$ tal que $x \equiv y \pmod{2\pi}$.

Proposición 6.4. Dados $z, w \in \mathbb{C}^*$, donde $z = r(\cos x + i\operatorname{sen} x)$ y $w = s(\cos y + i\operatorname{sen} y)$ con $r, s \in \mathbb{R}_{>0}$ y $x, y \in \mathbb{R}$, entonces $z = w$ si y sólo si $r = s$ y $x \equiv y \pmod{2\pi}$.

Fórmula de de Moivre. Dados $z, w \in \mathbb{C}^*$, entonces $\arg(zw) \equiv \arg(z) + \arg(w) \pmod{2\pi}$. Más precisamente:

$$\arg(zw) = \begin{cases} \arg(z) + \arg(w) & \text{si } \arg(z) + \arg(w) < 2\pi \\ \arg(z) + \arg(w) - 2\pi & \text{si } \arg(z) + \arg(w) \geq 2\pi \end{cases}$$

Dem. Sean $\alpha = \arg(z)$ y $\beta = \arg(w)$. Entonces:

$$\begin{aligned} zw &= |z|\,(\cos\alpha + i\operatorname{sen}\alpha)\,|w|\,(\cos\beta + i\operatorname{sen}\beta) \\ &= |zw|\,(\cos\alpha\cos\beta - \operatorname{sen}\alpha\operatorname{sen}\beta + i(\cos\alpha\operatorname{sen}\beta + \operatorname{sen}\alpha\cos\beta)) \\ &= |zw|\,(\cos(\alpha + \beta) + i\operatorname{sen}(\alpha + \beta)) \end{aligned}$$

□

Corolario. Dado $z \in \mathbb{C}^*$, se verifica que $\arg(\overline{z}) = \arg\left(z^{-1}\right) = -\arg(z)$.

Dem. $0 = \arg(1) = \arg\left(z^{-1}z\right) \equiv \arg(z) + \arg\left(z^{-1}\right) \pmod{2\pi}$. El mismo razonamiento demuestra el caso de $\overline{z}$ pues el producto $z\overline{z}$ es real, y consecuentemente de argumento 0. □

Proposición 6.5. Dado $z \in \mathbb{C}^*$, se verifica que $\arg(z^n) \equiv n\arg(z) \pmod{2\pi}$ para todo $n \in \mathbb{Z}$.

Dem. Demostraremos primero la proposición para $n \in \mathbb{N}_0$. Por inducción en n: vemos que la proposición se cumple para $n = 0$, pues $\arg\left(z^0\right) = \arg(1) = 0 = 0\arg(z)$. Ahora, suponiendo que la proposición vale para n, veamos que también vale para $n+1$:

$$\arg\left(z^{n+1}\right) \equiv \arg(z^n) + \arg(z) \equiv n\arg(z) + \arg(z) = (n+1)\arg(z) \pmod{2\pi}$$

La proposición vale también para enteros negativos, puesto que, para $n \in \mathbb{N}$:

$$\arg\left(z^{-n}\right) = \arg\left(\left(z^n\right)^{-1}\right) \equiv -\arg(z^n) \equiv -n\arg(z) \pmod{2\pi}$$

□

Teorema 6.1. Todo $z \in \mathbb{C}^*$ admite exactamente n raíces n-ésimas en $\mathbb{C}^*$; en otras palabras, la ecuación $x^n = z$ tiene exactamente n soluciones.

Dem. Sea $z = |z|(\cos\alpha + i\,\mathrm{sen}\,\alpha)$ y sea $w = |w|(\cos\beta + i\,\mathrm{sen}\,\beta)$ una posible raíz n-ésima de z, es decir, $w^n = z$. Por lo tanto, tenemos el siguiente sistema de ecuaciones:

$$\begin{cases} |w|^n & = |z| \\ n\beta & \equiv \alpha \pmod{2\pi} \end{cases}$$

Equivalentemente:

$$\begin{cases} |w| & = \sqrt[n]{|z|} \\ \beta & = \frac{\alpha + 2k\pi}{n} \end{cases}$$

para algún $k \in \mathbb{Z}$. Por lo tanto, tenemos una raíz w_k por cada valor entero k, definidas de modo que:

$$w_k = \sqrt[n]{|z|}\left(\cos\left(\frac{\alpha + 2k\pi}{n}\right) + i\,\mathrm{sen}\left(\frac{\alpha + 2k\pi}{n}\right)\right)$$

Ahora bien, dado $k \in \mathbb{Z}$, sea $r = r_n(k)$, es decir, $k = qn + r$, con $0 \leq r < n$. Entonces:

$$\arg(w_k) \equiv \frac{\alpha + 2k\pi}{n} = \frac{\alpha + 2r\pi}{n} + q(2\pi) \equiv \frac{\alpha + 2r\pi}{n} \equiv \arg(w_r) \pmod{2\pi}$$

En consecuencia, $w_k = w_r$. Por lo tanto, hay a lo sumo n raíces $w_0, \ldots, w_{n-1}$ (tantas como clases de congruencia módulo n). Es fácil ver que estas raíces son diferentes entre sí, pues difieren en menos de 2π entre sí. □

Definición 6.8. Dado $n \in \mathbb{N}$, indicaremos por G_n al conjunto de raíces n-ésimas de 1, es decir:

$$G_n = \left\{ \cos\left(\frac{2k\pi}{n}\right) + i\,\text{sen}\left(\frac{2k\pi}{n}\right) : k \in \{0, \ldots, n-1\} \right\} = \{u_0, \ldots, u_{n-1}\}$$

Cabe destacar que los elementos de G_n son los vértices de un polígono regular de n lados inscripto en la circunferencia unitaria, con un vértice en 1.

Lema 6.1. Sean $z, w \in \mathbb{C}^*$ de modo que w es una raíz n-ésima de z. Entonces $\{u_0 w, \ldots, u_{n-1} w\}$ es el conjunto de raíces n-ésimas de z, donde u_k es una raíz n-ésima de la unidad.

Dem. Es claro que el conjunto anterior está conformado por n números diferentes (de lo contrario, basta multiplicar por w^{-1} y llegamos a un absurdo, pues esto implicaría que existen menos de n raíces n-ésimas de la unidad). Entonces:

$$(u_k w)^n = u_k^n w^n = w^n = z$$

Dado que el conjunto contiene n elementos, abarca todas las raíces de z. □

Proposición 6.6. Enunciaremos algunas propiedades de G_n:

(1). $1 \in G_n$. Esto es inmediato pues $1^n = 1$ para cualquier n.
(2). Si $z \in G_n$ entonces $|z| = 1$. Esto es una consecuencia de la fórmula de de Moivre.
(3). Si $z \in G_n$ entonces $\overline{z} = z^{-1} \in G_n$. En primer lugar, $z^{-1} = \frac{\overline{z}}{|z|^2} = \overline{z}$. Luego, $\left(z^{-1}\right)^n = \left(z^n\right)^{-1} = 1^{-1} = 1$.
(4). Si $z, w \in G_n$ entonces $zw \in G_n$, pues $(zw)^n = z^n w^n = 1$.
(5). Como corolario de (4), si $z \in G_n$ entonces $z^k \in G_n$ para cualquier $k \in \mathbb{Z}$.

Entonces, G_n conforma un grupo junto con el producto usual en $\mathbb{C}$, dado que posee a su elemento neutro, el producto es asociativo, el inverso de cada elemento está contenido en G_n y está cerrado bajo el producto. Más aún, $(G_n, \cdot)$ es un grupo cíclico (y por ende abeliano).

Proposición 6.7. Dados $n, m \in \mathbb{N}$, se verifica que $G_n \cap G_m = G_{(n:m)}$

Dem. Sean $d = (n : m)$ y $z \in G_d$. Supongamos $n = dk$, $m = dh$. Entonces:

$$z^n = z^{dk} = \left(z^d\right)^k = 1^k = 1$$
$$z^m = z^{dh} = \left(z^d\right)^h = 1^h = 1$$

Por lo tanto, $z \in G_d$ implica $z \in G_n \cap G_m$. Veamos entonces el converso de esta implicación. Supongamos $z \in G_n \cap G_m$. Por las propiedades del máximo común divisor, existen $a, b \in \mathbb{Z}$ de modo que $d = an + bm$. Entonces:

$$z^d = z^{an+bm} = z^{an} z^{bm} = \left(z^n\right)^a \left(z^m\right)^b = 1^a 1^b = 1$$

Concluimos entonces que $z \in G_n \cap G_m$ implica $z \in G_d$. □

Corolario. Dados $n, m \in \mathbb{N}$, $G_n \subseteq G_m$ si y sólo si $n \mid m$.

Dem. $G_n \subseteq G_m$ si y sólo si $G_n = G_n \cap G_m = G_{(n:m)}$. Por lo tanto, $G_n \subseteq G_m$ si y sólo si $n = (n : m)$, es decir $n \mid m$. □

Definición 6.9. Dados $n \in \mathbb{N}$ y $z \in G_n$, decimos que z es una raíz n-ésima *primitiva* de la unidad si todo elemento de G_n puede expresarse como una potencia de z; es decir, para todo $u \in G_n$ existe $k \in \mathbb{Z}$ de modo que $z^k = w$. De manera equivalente, z es raíz primitiva si $G_n = \{z^0, \ldots, z^{n-1}\}$, ya que $u = z^k$ con $k = qn + r$, por lo tanto $u = z^{qn+r} = z^r$ con $0 \leq r < n$. Diremos que z es una *primitiva de orden* n si es primitiva de G_n. Además, considerando G_n como grupo cíclico, es claro ver que cualquier raíz primitiva es un generador de G_n.

Observación 6.3. u_1 siempre es primitiva de G_n.

Dem. Dado $u_k \in G_n$, tenemos que:

$$\begin{aligned} w &= \cos\left(\frac{2k\pi}{n}\right) + i\,\mathrm{sen}\left(\frac{2k\pi}{n}\right) \\ &= \left(\cos\left(\frac{2\pi}{n}\right) + i\,\mathrm{sen}\left(\frac{2\pi}{n}\right)\right)^k \\ &= u_1^k \end{aligned}$$

□

Proposición 6.8. Dado $z \in G_n$, son equivalentes las siguientes afirmaciones:

(1). z es primitiva de G_n
(2). $n = \min\{t \in \mathbb{N} : z^t = 1\}$, es decir, $z \notin G_m$ si $m < n$
(3). $z = u_k$ con $k \perp n$

Dem. $(1 \Rightarrow 2)$ Supongamos que existe $k < n$ de modo que $z^k = 1$. Entonces, dado $t \in \mathbb{Z}$, $z^t = z^{r_k(t)}$, por lo que existen a lo sumo k potencias diferentes de z, lo cual es absurdo pues z es primitiva de G_n.

$(2 \Rightarrow 3)$ Dado que $z \in G_n$, tenemos:

$$z = \cos\left(\frac{2k\pi}{n}\right) + i\,\mathrm{sen}\left(\frac{2k\pi}{n}\right)$$

Sea $d = (k : n)$. Consideremos entonces la siguiente igualdad:

$$z^{\frac{n}{d}} = \cos\left(\frac{n}{d}\frac{2k\pi}{n}\right) + i\,\mathrm{sen}\left(\frac{n}{d}\frac{2k\pi}{n}\right) = \cos\left(\frac{2k\pi}{d}\right) + i\,\mathrm{sen}\left(\frac{2k\pi}{d}\right) = 1$$

Esto se debe a que $\frac{k}{d} \in \mathbb{Z}$ y por lo tanto el argumento de la expresión es 0. Ahora bien, como la mínima potencia de z que vale 1 es n, tenemos $\frac{n}{d} \geq n$, por lo tanto, $d = 1$.

$(3 \Rightarrow 1)$ Una vez más, dado $z = u_k \in G_n$:

$$z = \cos\left(\frac{2k\pi}{n}\right) + i\,\text{sen}\left(\frac{2k\pi}{n}\right)$$

Supongamos $w \in G_n$:

$$w = \cos\left(\frac{2m\pi}{n}\right) + i\,\text{sen}\left(\frac{2m\pi}{n}\right)$$

Ahora bien, dado que $k \perp n$, la ecuación lineal de congruencia $kx \equiv m \pmod{n}$ es resoluble pues $1 \mid m$ para todo m. Por lo tanto, basta resolver dicha ecuación (que presentará una única solución, módulo n) para obtener x tal que $z^x = w$, pues:

$$z^x = \cos\left(\frac{2kx\pi}{n}\right) + i\,\text{sen}\left(\frac{2kx\pi}{n}\right) = \cos\left(\frac{2m\pi}{n}\right) + i\,\text{sen}\left(\frac{2m\pi}{n}\right) = w$$

ya que $\frac{2kx\pi}{n} \equiv \frac{2m\pi}{n} \pmod{2\pi}$. Por lo tanto, z es primitiva de G_n. □

6. Polinomios

En este capítulo, la letra $\mathbb{K}$ designará a cualquiera de los conjuntos $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.

Definición 6.1. Un *polinomio f con coeficientes en* $\mathbb{K}$ es una expresión del tipo:

$$\sum_{j=0}^{n} a_j x^j$$

donde $n \in \mathbb{N}_0$, $a_i \in \mathbb{K}$ para todo $i \leq n$ y x es un símbolo llamado *indeterminada*. Los a_i se dicen los *coeficientes* de f y a_k será el coeficiente *de grado k*. El conjunto de polinomios con coeficientes en $\mathbb{K}$ será notado $\mathbb{K}[x]$. Naturalmente, tenemos que:

$$\mathbb{Z}[x] \subseteq \mathbb{Q}[x] \subseteq \mathbb{R}[x] \subseteq \mathbb{C}[x]$$

Definición 6.2. Sean $f, g \in \mathbb{K}[x]$, $f = \sum_{j=0}^{m} a_j x^j$, $g = \sum_{j=0}^{n} b_j x^j$. Suponiendo $m \geq n$, decimos que $f = g$ si $a_j = b_j$ para todo $j \leq m$ y $b_j = 0$ para todo $j > m$.

Alternativamente, podemos suponer que un polinomio está dado por una secuencia infinita $a_0, a_1, \ldots$ de coeficientes, con la condición de que $a_k = 0$ para todo k a partir de cierto $k_0 \in \mathbb{N}_0$. De acuerdo con esta definición alternativa, decimos que $f = g$ si ambos polinomios tienen la misma secuencia de coeficientes. En general, escribiremos el polinomio hasta su último coeficiente no nulo.

Definición 6.3. El polinomio que corresponde a la secuencia nula se llama el *polinomio nulo* y lo notaremos simplemente 0.

Definición 6.4. Sean $f \in \mathbb{K}[x]$ no nulo y $(a_i)_{i \in \mathbb{N}_0}$ la secuencia de sus coeficientes. Definimos entonces el *grado* de f (notado $\mathrm{gr}(f)$) como el máximo $k \in \mathbb{N}_0$ de modo que $a_k \neq 0$. Formalmente:

$$\mathrm{gr}\,(f) = \max\{k \in \mathbb{N}_0 : a_k \neq 0\}$$

Definición 6.5. Dados $f, g \in \mathbb{K}[x]$, $f = \sum_{j=0}^{n} a_j x^j$, $g = \sum_{j=0}^{n} b_j x^j$, definimos la *suma de f y g*, notada $f + g$, de modo que:

$$f + g = \sum_{j=0}^{n} (a_j + b_j) x^j$$

Propiedades. Dados $f, g, h \in \mathbb{K}[x]$, se verifican las siguientes propiedades:

(1). $f + g \in \mathbb{K}[x]$
(2). $(f + g) + h = f + (g + h)$
(3). $f + g = g + f$
(4). $f + 0 = f$
(5). Dado f, existe $(-f) \in \mathbb{K}[x]$ de modo que $f + (-f) = 0$ (en particular, si $f = \sum_{j=0}^{n} a_j x^j$, entonces $(-f) = \sum_{j=0}^{n} (-a_j) x^j$)

Definición 6.6. Un polinomio de la forma ax^r (es decir, que posee un único coeficiente no nulo) se dice un *monomio*.

Observación 6.1. Sea $f \in \mathbb{K}[x]$ con $f = \sum_{j=0}^{n} a_j x^j$. Consideremos los monomios $f_j = a_j x^j$. Es claro entonces que $f = \sum_{j=0}^{n} f_j$. Por lo tanto, todo polinomio es expresable como una suma de monomios.

Definición 6.7. Dados $f, g \in \mathbb{K}[x]$, $f = \sum_{j=0}^{m} a_j x^j$, $g = \sum_{j=0}^{n} b_j x^j$, definimos el *producto entre f y g*, notado fg, de modo que:

$$fg = \sum_{i,j} a_i b_j x^{i+j} = \sum_{k=0}^{m+n} \left(\sum_{i+j=k} a_i b_j \right) x^k = \sum_{k=0}^{m+n} \left(\sum_{i=0}^{m} a_i b_{k-i} \right) x^k$$

En la última equivalencia, pueden darse términos negativos $k - i$; en tal caso, definimos $b_{k-i} = 0$ si $k - i < 0$. En particular, si $f = c$ (donde $c \in \mathbb{K}$), entonces:

$$fg = \sum_{j=0}^{m} (cb_j) x^j$$

Proposición 6.1. Dados $f, g \in \mathbb{K}[x]$ no nulos:

(1). Si $\mathrm{gr}(f) \neq \mathrm{gr}(g)$, entonces $\mathrm{gr}(f+g) = \max\{\mathrm{gr}(f), \mathrm{gr}(g)\}$
(2). Si $\mathrm{gr}(f) = \mathrm{gr}(g)$ y $f + g \neq 0$, entonces $\mathrm{gr}(f+g) \leq \max\{\mathrm{gr}(f), \mathrm{gr}(g)\}$
(3). $fg \neq 0$. Más aún, $\mathrm{gr}(fg) = \mathrm{gr}(f) + \mathrm{gr}(g)$

Definición 6.8. En un polinomio no nulo, llamamos *coeficiente principal* al que acompaña al exponente que corresponde al grado del polinomio. Si el coeficiente principal de un polinomio es 1, decimos que dicho polinomio es *mónico*.

Observación 6.2. En $\mathbb{K}[x]$ vale la propiedad distributiva del producto respecto de la suma; es decir, dados $f, g \in \mathbb{K}[x]$, $f(g+h) = fg + fh$. Por lo tanto, $\mathbb{K}[x]$ conforma junto a la suma y el producto un anillo conmutativo.

Proposición 6.2. Si $\mathbb{K} = \mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$ y $f \in \mathbb{K}[x]$ no nulo, entonces f es inversible (es decir, existe $g \in \mathbb{K}[x]$ tal que $fg = 1$) si y sólo si $\mathrm{gr}(f) = 0$.

Dem. ($\Leftarrow$) Si $\mathrm{gr}(f) = 0$, digamos $f = a$ con $a \in \mathbb{K}$ no nulo. Basta entonces tomar $g = a^{-1}$ ($a^{-1} \in \mathbb{K}$ existe debido a que $\mathbb{K}$ es un cuerpo) para garantizar $fg = 1$.

($\Rightarrow$) Supongamos f inversible y que $fg = 1$ con $g \in \mathbb{K}[x]$. Ahora bien:

$$0 = \mathrm{gr}(1) = \mathrm{gr}(fg) = \mathrm{gr}(f) + \mathrm{gr}(g)$$

y esto es posible si y sólo si $\mathrm{gr}(f) = \mathrm{gr}(g) = 0$. □

Algoritmo de la división en $\mathbb{K}[x]$. Sean $f, g \in \mathbb{K}[x]$ con $f \neq 0$. Entonces, existen únicos $h, r \in \mathbb{K}[x]$ tales que $g = hf + r$ y $\mathrm{gr}(r) < \mathrm{gr}(f)$ o bien $r = 0$. Llamaremos a h el *cociente* de la división de g por f y r se dirá el *resto*, al cual notaremos $r = r_f(g)$.

Dem. Si $g = 0$ o $\text{gr}(g) < \text{gr}(f)$ entonces basta tomar $h = 0$ y $r = g$. En caso contrario, es decir, $\text{gr}(g) \geq \text{gr}(f)$, escribamos $f = \sum_{i=0}^{m} a_i x^i$ y $g = \sum_{i=0}^{n} b_i x^i$, donde $n \geq m$. Podemos reescribir a g como:

$$g = \frac{b_n}{a_m} x^{n-m} f + \left(g - \frac{b_n}{a_m} x^{n-m} f \right)$$

Llamemos $g_1 = g - \frac{b_n}{a_m} x^{n-m} f$. Si $g_1 = 0$ o $\text{gr}(g_1) < \text{gr}(f)$, entonces basta tomar $h = \frac{b_n}{a_m} x^{n-m}$ y $r = g_1$. De lo contrario, observemos que $\text{gr}\left(\frac{b_n}{a_m} x^{n-m} f \right) = n$ y su coeficiente principal es b_n (el mismo del polinomio g). Por lo tanto $\text{gr}(g_1) < n$. Aplicando entonces un argumento inductivo sobre $n - m$ resulta que existen polinomios h_1 y r_1 tales que $g_1 = h_1 f + r_1$, donde $r_1 = 0$ o bien $\text{gr}(r_1) < \text{gr}(f_1)$. Luego:

$$g = \frac{b_n}{a_m} x^{n-m} f + h_1 f + r_1 = \left(\frac{b_n}{a_m} x^{n-m} + h_1 \right) f + r_1$$

y entonces basta tomar $h = \left(\frac{b_n}{a_m} x^{n-m} + h_1 \right)$ y $r = r_1$, y así inductivamente.

Demostremos entonces la unicidad de dichos polinomios. Supongamos un par de polinomios h' y r' que también verifican lo pedido. Es evidente que $h = h'$ si y sólo si $r = r'$; entonces, supongamos $r' \neq r$. Ahora bien, $\text{gr}(r') \neq \text{gr}(r)$ (de lo contrario, $\text{gr}(h) = \text{gr}(h')$ y si $f = hg + r$, entonces $h'g$ diferirá de hg en algún coeficiente de grado mayor a $\text{gr}(r')$). Entonces, supongamos sin pérdida de generalidad $\text{gr}(r) > \text{gr}(r')$. Observando que $0 = (h - h')g + r - r'$, deducimos que $(h' - h)g = r - r' \neq 0$. Pero eso implica:

$$\text{gr}(g) \leq \text{gr}(r - r') = \text{gr}(r) < \text{gr}(g)$$

lo cual es claramente absurdo. □

Definición 6.9. Dados $f, g \in \mathbb{K}[x]$, dedcimos que f *divide a* g si existe $h \in \mathbb{K}[x]$ de modo que $g = fh$. En dicho caso notaremos $f \mid g$, de manera análoga a los enteros. Es claro que $f \mid g$ si y sólo si $r_f(g) = 0$.

Definición 6.10. Dado $f = \sum_{i=0}^{n} a_i x^i \in \mathbb{K}[x]$, queda inducida una función (que también notaremos f) $f : \mathbb{K} \to \mathbb{K}$ definida por $f(z) = \sum_{i=0}^{n} a_i z^i$. Dicha función es llamada la *especialización de f en z*.

Observación 6.3. Dados $f, g \in \mathbb{K}[x]$ y $z \in \mathbb{K}$, entonces $(f + g)(z) = f(z) + g(z)$ y $(fg)(z) = f(z)g(z)$

Definición 6.11. Si $f \in \mathbb{K}[x]$ y $z \in \mathbb{K}$, decimos que z es una *raíz* de f si $f(z) = 0$.

Teorema del resto. Sean $f \in \mathbb{K}[x]$ y $z \in \mathbb{K}$. Entonces $r_{x-z}(f) = f(z)$.

Dem. Aplicando el algoritmo de la división, tenemos que $f = (x - z)h + r$ donde $r \in \mathbb{K}$. Luego, especializando en z:

$$f(z) = \left((x - z)h + r \right)(z) = ((x - z)h)(z) + r(z) = (z - z)h + r = r$$

□

Corolario. Dados $f, g \in \mathbb{K}[x]$ y $z \in \mathbb{K}$, z es raiz de f si y sólo si $(x - z) \mid f$.

Propiedades. Enunciaremos algunas propiedades de las raíces y las especializaciones. Sean $f, g, h \in \mathbb{K}[x]$ y $z \in \mathbb{K}$, entonces:

(1). Si $f \mid g$, entonces toda raíz de f es raíz de g.

(2). Sea $f = \prod_{i=1}^{n} f_i$; entonces z es raíz de f si y sólo si z es raíz de f_k para algún índice k.

(3). Si $\mathrm{gr}(f) = n$, entonces f tiene a lo sumo n raíces distintas en $\mathbb{K}$.

(4). $f = g$ si y sólo si $f(z) = g(z)$ para todo $z \in \mathbb{K}$.

Dem. (1). Suponiendo z raíz de f, especializando en z tenemos:

$$g(z) = (fh)(z) = f(z)h(z) = 0\,h(z) = 0$$

(2). Especializando en z:

$$f(z) = \left(\prod_{i=1}^{n} f_i\right)(z) = \prod_{i=1}^{n} f_i(z) = 0$$

Entonces $f(z) = 0$ si y sólo si algún $f_i(z) = 0$.

(3). Por inducción en n: es claro que, si $\mathrm{gr}(f) = 1$, digamos $f = ax + b$ presenta una única raíz: $\frac{-b}{a}$. Supongamos que el hecho se cumple para todo $m < n$, con $n > 1$. Supongamos también que f admite alguna raiz en $\mathbb{K}$ a la que llamaremos z_1 (el resultado es inmediato si f no admite raíces). Entonces, podemos factorizar a f de la forma $f = (x - z_1)f_1$, donde $f_1 \in \mathbb{K}[x]$ y $\mathrm{gr}(f_1) = n - 1$. Ahora bien, por hipótesis inductiva, f_1 tiene a lo sumo $n - 1$ raíces distintas en $\mathbb{K}$, y como toda raíz de f distinta de z_1 es raíz de f_1, se deduce que f tiene a lo sumo tantas raíces como su grado.

(4). Es inmediato ver que $f = g$ implica $f(z) = g(z)$. Demostremos el converso: supongamos $f(z) = g(z)$ para todo $z \in \mathbb{K}$ pero $f \neq g$. Entonces $f - g \neq 0$, y entonces $\mathrm{gr}(f - g) = n$. Especializando en $w \in \mathbb{K}$:

$$(f - g)(w) = f(w) - g(w) = 0$$

Por lo tanto, cualquier $w \in \mathbb{K}$ es raíz, pero $f - g$ tiene a lo sumo n raíces distintas, por la propiedad anterior. Entonces $f = g$.

□

Proposición 6.3. Si $f \in \mathbb{K}[x]$ y $z_1, \ldots, z_r$ son raíces distintas de f, entonces:

$$\left(\prod_{i=1}^{r}(x - z_i)\right) \mid f$$

Dem. Por inducción en r: si $r = 1$ el resultado sigue por el teorema del resto. Supongamos $r > 1$ y que el resultado vale para todo $r' < r$. Entonces, por el teorema del resto existe $g \in \mathbb{K}[x]$ tal que $f = g(x - z_1)$. Si $i > 1$, resulta que $0 = f(z_i) = (z_i - z_1)g(z_i)$, y esto implica $g(z_i) = 0$. Entonces, una vez más, por el teorema del resto existe $h \in \mathbb{K}[x]$ tal que $g = h\prod_{i=2}^{r}(x - z_i)$. Finalmente:

$$f = (x - z_1)h\prod_{i=2}^{r}(x - z_i) = h\prod_{i=1}^{r}(x - z_i)$$

□

Definición 6.12. Dados $f \in \mathbb{K}[x]$ no nulo y $z \in \mathbb{K}$ raíz de f, decimos que z es una raíz de *multiplicidad* n de f, con $n \in \mathbb{N}$ si $(x-z)^n \mid f$ y $(x-z)^{n+1} \nmid f$. En este caso notaremos $\text{mult}(z, f) = n$.
Equivalentemente:

$$\text{mult}(z, f) = \max\left\{k \in \mathbb{N} : (x-z)^k \mid f\right\}$$

Si z es una raíz de multiplicidad 1, se dirá una *raíz simple;* si posee mayor multiplicidad, se dirá una *raíz múltiple*. Además, extendemos la definición de la manera que, si z no es raíz de f, $\text{mult}(z, f) = 0$.

Lema 6.1. Sea $f \in \mathbb{K}[x]$ no nulo y $z \in \mathbb{K}$, entonces $\text{mult}(z, f) = n$ si y sólo si f se factoriza de modo que $f = (x-z)^n g$ con $g(z) \neq 0$.

Dem. ($\Rightarrow$)I Supongamos $\text{mult}(z, f) = n$, entonces existe $g \in \mathbb{K}[x]$ de modo que $f = (x-z)^n g$ con $g(z) \neq 0$, dado que si $g(z) = 0$ entonces $\text{mult}(z, f) = n + 1$.

($\Leftarrow$) Supongamos $f = (x-z)^n g$ con $g(z) \neq 0$. Suponiendo que $(x-z)^{n+1} \mid f$, afirmamos que existe $t \in \mathbb{K}[x]$ tal que $f = (x-z)^{n+1}t$. Entonces, $(x-z)^{n+1}t = (x-z)^n g$. Por lo tanto, $(x-z)^n((x-z)t - g) = 0$. Dado que $(x-z)^n \neq 0$ por hipótesis, tenemos que $(x-z)t - g = 0$, y por lo tanto $(x-z)t = g$, lo cual es claramente absurdo pues z no es raíz de g. □

Definición 6.13. Sea $f = \sum_{i=0}^{n} a_i x^i \in \mathbb{K}[x]$. Entonces, el *polinomio derivado* de f, notado f' es:

$$f' = \sum_{i=1}^{n} i a_i x^{i-1}$$

Lema 6.2. Dados $f \in \mathbb{K}[x]$ no nulo y $z \in \mathbb{K}$ una raíz de f. Entonces, $\text{mult}(z, f') = \text{mult}(z, f) - 1$.

Dem. Por la caracterización presentada anteriormente, $f = (x-z)^n g$ con $g(z) \neq 0$. Derivando:

$$f' = n(x-z)^{n-1}g + (x-z)^n g' = (x-z)^{n-1}(ng + (x-z)g')$$

Llamemos $h = ng + (x-z)g'$. Especializando h en z obtenemos:

$$h(z) = ng(z) + (z-z)g'(z) = ng(z) \neq 0$$

Por lo tanto, por el lema anterior, $\text{mult}(z, f') = n - 1$. □

Corolario. Bajo las mismas hipótesis del lema, $\text{mult}(z, f) = n \geq 1$ si y sólo si $f^{(i)}(z) = 0$ para todo $i \leq n - 1$.

Proposición 6.4. Sean $z_1, \ldots, z_r$ raíces distintas de $f \in \mathbb{K}[x]$ no nulo, de modo que $\text{mult}(z_i, f) = n_i$. Entonces:

$$\left(\prod_{i=1}^{r}(x-z_i)^{n_i}\right) \mid f$$

Dem. Por inducción en r: si $r = 1$ el resultado sigue por la definición de multiplicidad. Suponiendo $r > 1$, tenemos $t \in \mathbb{K}[x]$ de modo que $f(x - z_1)^{n_1} t$ y $t(z_1) \neq 0$. Además, si $i > 1$ tenemos que $f(z_i) = 0$, por lo tanto $t(z_i) = 0$. Sigue entonces que $\text{mult}(z_i, f) = \text{mult}(z_i, t)$. Por razonamiento inductivo, tenemos que $(\prod_{i=2}^{r}(x - z_i)^{n_i}) \mid t$; por lo tanto $f = h\prod_{i=1}^{r}(x - z_i)^{n_i}$ □

Corolario. Sea $f \in \mathbb{K}[x]$ de grado n, entonces, f admite a lo sumo n raíces en $\mathbb{K}$, aún contando cada una de ellas con su correspondiente multiplicidad.

Dem. Sean $z_1, \ldots, z_r$ raíces distintas de f y $n_1, \ldots, n_r$ sus respectivas multiplicidades. Vale decir entonces que f tiene, considerando multiplicidad, $\sum_{i=1}^{r} n_i$ raíces en $\mathbb{K}$. De acuerdo con la proposición anterior, existe $g \in \mathbb{K}[x]$ de modo que $f = g\prod_{i=1}^{r}(x - z_i)^{n_i}$. Tomando grados:

$$n = \text{gr}\left(g\prod_{i=1}^{r}(x - z_i)^{n_i}\right) = \sum_{i=1}^{r} n_i + \text{gr}(g) \geq \sum_{i=1}^{r} n_i$$

□

Propiedades. Sea $\mathbb{K} = \mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$. Si $f, g \in \mathbb{K}[x]$, entonces:

(1). Si $a \in \mathbb{K}$ es no nulo, entonces $a \mid g$ y $ag \mid g$ para cualquier $g \in \mathbb{K}[x]$.
(2). Si $f \mid g$ y $g \mid f$, entonces $\text{gr}(f) = \text{gr}(g)$ (o equivalentemente, existe $a \in \mathbb{K}$ no nulo de modo que $g = af$). En este caso, los polinomios se dicen *asociados*.
(3). Todo polinomio f es asociado a un único polinomio mónico.

Criterio de raíces racionales de Gauss. Sea $f = \sum_{j=1}^{n} a_j x^j \in \mathbb{Q}[x]$; si $\frac{p}{q} \in \mathbb{Q}$ es raíz de f, entonces $p \mid a_0$ y $q \mid a_n$.

Dem. Supongamos que $\frac{p}{q}$ es raíz de f; entonces $0 = q^n f\left(\frac{p}{q}\right) = a_n p^n + q\left(\sum_{j=1}^{n-1} a_j \frac{p^j}{q^{j-1}}\right)$. Por lo tanto, $q \mid a_n p^n$ y debido a que $p \perp q$, $q \mid a_n$. El resultado para p se deduce de manera análoga. □

Apéndice: Sucesión de Fibonacci

Definición. Llamamos *sucesión de Fibonacci* a la sucesión dada por la recurrencia:

$$\begin{aligned} F_0 &= 0 \\ F_1 &= 1 \\ F_{n+2} &= F_n + F_{n+1} \end{aligned}$$

Proposición. Dado el polinomio $x^2 - x - 1$, podemos ver que $\varphi = \frac{1+\sqrt{5}}{2}$ y $\psi = \frac{1-\sqrt{5}}{2}$ son sus raíces. Se verifica entonces que:

$$F_n = \frac{\varphi^n - \psi^n}{\varphi - \psi} = \frac{\varphi^n - \psi^n}{\sqrt{5}}$$

Dem. Cabe destacar que se puede extender la definición de la sucesión para incluir términos de índice negativo, de modo que siga satisfaciendo la recurrencia; por ejemplo, $F_{-1} = 1$, $F_{-2} = -1$, *ad infinitum*.

Para demostrar la proposición, probaremos primero la identidad:

$$\varphi^n = F_n\varphi + F_{n-1}$$

Por inducción global:

(1). Se verifica para el caso $n = 0$ y $n = 1$, ya que:

$$\begin{aligned} 1 = \varphi^0 &= F_0\varphi + F_{-1} = 0 \cdot \varphi + 1 \\ \varphi = \varphi^1 &= F_1\varphi + F_0 = 1 \cdot \varphi + 0 \end{aligned}$$

(2). Para el paso inductivo, queremos demostrar que, si se verifica para todo $j \leq k$ que:

$$\varphi^j = F_j\varphi + F_{j-1}$$

entonces también se verifica que:

$$\varphi^{k+1} = F_{k+1}\varphi + F_k$$

Ahora bien, teniendo en cuenta que $\varphi^2 = \varphi + 1$ ya que φ es raíz de $x^2 - x - 1$, tenemos que:

$$\begin{aligned} \varphi^{k+1} &= \varphi^{k-1}\varphi^2 \\ &= \varphi^{k-1}(\varphi + 1) \\ &= \varphi^k + \varphi^{k-1} \\ &= (F_k\varphi + F_{k-1}) + (F_{k-1}\varphi + F_{k-2}) \\ &= F_{k+1}\varphi + F_k \end{aligned}$$

Ahora bien, este mismo razonamiento es también aplicable a ψ ya que también es raíz de $x^2 - x - 1$; por lo tanto:

$$\psi^n = F_n\psi + F_{n-1}$$

Pero entonces, es claro que:

$$\varphi^n - \psi^n = F_n\varphi - F_n\psi = F_n(\varphi - \psi)$$

de lo que se deduce inmediatamente que:

$$F_n = \frac{\varphi^n - \psi^n}{\varphi - \psi} = \frac{\varphi^n - \psi^n}{\frac{1+\sqrt{5}}{2} - \frac{1-\sqrt{5}}{2}} = \frac{\varphi^n - \psi^n}{\sqrt{5}}$$

□

Proposición. Se verifica que:

$$\frac{\varphi^n - \psi^n}{\sqrt{5}} \simeq \frac{\varphi^n}{\sqrt{5}}$$

Por lo tanto, $F_n \simeq \frac{\varphi^n}{\sqrt{5}}$, y además:

$$\frac{F_{n+1}}{F_n} \xrightarrow[n\to\infty]{} \varphi$$

Dem. Dado que $\psi = \frac{1-\sqrt{5}}{2} \simeq -0,618... \in (-1, 0)$, es fácil ver que $|\psi^n|$ tiende a 0, por lo cual el término $-\psi^n$ resulta poco significante para n suficientemente grande.

Entonces, es fácil ver que:

$$\frac{F_{n+1}}{F_n} = \frac{\frac{\varphi^{n+1} - \psi^{n+1}}{\sqrt{5}}}{\frac{\varphi^n - \psi^n}{\sqrt{5}}} = \frac{\varphi^{n+1} - \psi^{n+1}}{\varphi^n - \psi^n} \xrightarrow[n\to\infty]{} \frac{\varphi^{n+1}}{\varphi^n} = \varphi$$

□

Proposición. Si dado $n \in \mathbb{N}$, m es el menor natural tal que $n \mid F_m$, entonces $n \mid F_{km}$ para todo $k \in \mathbb{N}$