Capítulo 1

Conjuntos, Relaciones y Funciones.

Definición 1.1.1. (informal de conjunto y elementos.)

Un conjunto es una colección de objetos, llamados *elementos*, que tiene la propiedad que dado un objeto cualquiera, se puede decidir si ese objeto es un elemento del conjunto o no.

Se dice que cada elemento a de un conjunto A *pertenece* al conjunto A, y se nota $a \in A$. Si un objeto b no pertenece al conjunto A, se nota $b \notin A$.

Definición 1.1.3. (Subconjuntos e Inclusión.)

Sea A un conjunto. Se dice que un conjunto B *está contenido en* A, y se nota $B \subseteq A$ (o también $B \subset A$), si todo elemento de B es un elemento de A. En ese caso decimos también que B *está incluído en* A, o que B es un *subconjunto* de A. Si B no es un subconjunto de A se nota $B \not\subseteq A$ (o $B \not\subset A$).

$B \subseteq A$ si $\forall x,\ x \in B \Rightarrow x \in A$, $B \not\subseteq A$ si $\exists x \in B : x \notin A$.

$A = B \iff A \subseteq B$ y $B \subseteq A$.

Definición 1.1.5. (Conjunto de partes.)

Sea A un conjunto. El *conjunto de partes* de A, que se nota $\mathcal{P}(A)$, es el conjunto formado por todos los subconjuntos de A, o sea el conjunto cuyos *elementos* son los subconjuntos de A. Es decir

$$\mathcal{P}(A) = \{B : B \subseteq A\} \quad \text{o también} \quad B \in \mathcal{P}(A) \iff B \subseteq A.$$

- Cualquiera sea el conjunto A, $\emptyset \in \mathcal{P}(A)$, $A \in \mathcal{P}(A)$.
- $\mathcal{P}(\emptyset) = \{\emptyset\}$, o sea el conjunto que tiene como único elemento al conjunto vacío.

1.1.2 Operaciones entre conjuntos.

Complemento ^{c}: Sea A subconjunto de un conjunto referencial U. El *complemento* de A (en U) es el conjunto de los elementos de U que no pertenecen a A, que se suele notar con A' o A^c (aquí usaremos la notación A^c que es la que aparece en la práctica). Es decir

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

Unión $\cup$: Sean A, B subconjuntos de un conjunto referencial U. La *unión* de A y B es el conjunto $A \cup B$ de los elementos de U que pertenecen a A o a B. Es decir

$$A \cup B = \{x \in U : x \in A \text{ o } x \in B\}.$$

Intersección $\cap$. Sean A, B subconjuntos de un conjunto referencial U. La *intersección* de A y B es el conjunto $A \cap B$ de los elementos de U que pertenecen tanto a A como a B. Es decir

$$A \cap B = \{x \in U : x \in A \text{ y } x \in B\}.$$

Cuando $A \cap B = \emptyset$, se dice que A y B son conjuntos *disjuntos*.

Proposición 1.1.6. (Leyes de De Morgan y distributivas.)

Sean A, B, C *conjuntos dentro de un conjunto referencial* U. *Entonces*

Leyes de De Morgan

$(A \cup B)^c = A^c \cap B^c \quad y \quad (A \cap B)^c = A^c \cup B^c.$

Leyes distributivas*:*

$A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \quad y \quad A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$

Diferencia $-$**:** $A - B := A \cap B^c$, es decir

$$x \in A - B \iff x \in A \text{ y } x \in B^c \iff x \in A \text{ y } x \notin B.$$

Es decir, $A - B$ es el conjunto de los elementos de A que no son elementos de B:

$$A - B = \{a \in A : a \notin B\}.$$

Diferencia simétrica $\triangle$**:** $A \triangle B$ es el conjunto de los elementos de U que pertenecen a A o a B pero no a los dos a la vez. Es decir

$$A \triangle B = \{c \in U : (c \in A \text{ y } c \notin B) \text{ o } (c \in B \text{ y } c \notin A)\}.$$

Vale

$$A \triangle B = (A - B) \cup (B - A) = (A \cap B^c) \cup (B \cap A^c) = (A \cup B) - (A \cap B).$$

- Siempre $A \triangle B = B \triangle A$ (simetría), $A \triangle \emptyset = A$, $A \triangle U = A^c$, $A \triangle A = \emptyset$, $A \triangle A^c = U$.

Tablas de verdad de los conectores lógicos:

Sean p, q proposiciones, es decir afirmaciones que son o bien verdaderas o bien falsas, como por ejemplo "hoy es domingo", o "$\forall\, n \in \mathbb{N}, n \geq 3$", o "los perros son mamíferos". Las tablas de verdad de los conectores lógicos son las siguientes:

p	$\neg p$
V	F
F	V

p	q	$p \vee q$
V	V	V
V	F	V
F	V	V
F	F	F

p	q	$p \wedge q$
V	V	V
V	F	F
F	V	F
F	F	F

p	q	$p \veebar q$
V	V	F
V	F	V
F	V	V
F	F	F

p	q	$p \Rightarrow q$
V	V	V
V	F	F
F	V	V
F	F	V

p	q	$p \Leftrightarrow q$
V	V	V
V	F	F
F	V	F
F	F	V

.

(La definición formal de $p \Rightarrow q$ es $\neg p \vee q$.)

Tablas de verdad de las operaciones de conjuntos:

- *Complemento:* El complemento A^c de A en U se corresponde con $\neg p$.
- *Unión:* La unión $A \cup B$ se corresponde con $p \vee q$.
- *Intersección:* La intersección $A \cap B$ se corresponde con $p \wedge q$.
- *Diferencia simétrica:* La diferencia simétrica $P \triangle Q$ se corresponde con $p \veebar q$.
- *Inclusión:* La inclusión $A \subseteq B$ se corresponde con $p \Rightarrow q$.
- *Igualdad:* La igualdad $A = B$ se corresponde con $p \Leftrightarrow q$.

A	A^c
V	F
F	V

A	B	$A \cup B$
V	V	V
V	F	V
F	V	V
F	F	F

A	B	$A \cap B$
V	V	V
V	F	F
F	V	F
F	F	F

A	B	$A \triangle B$
V	V	F
V	F	V
F	V	V
F	F	F

A	B	$A \subseteq B$
V	V	V
V	F	F
F	V	V
F	F	V

A	B	$A = B$
V	V	V
V	F	F
F	V	F
F	F	V

.

- La tabla de la diferencia $A - B$ se obtiene de la definición $A - B = A \cap B^c$:

A	B	B^c	$A \cap B^c = A - B$
V	V	F	F
V	F	V	V
F	V	F	F
F	F	V	F

.

Definición 1.1.7. (Producto cartesiano.)

Sean A, B conjuntos. El producto cartesiano de A con B, que se nota $A \times B$, es el conjunto de *pares ordenados*

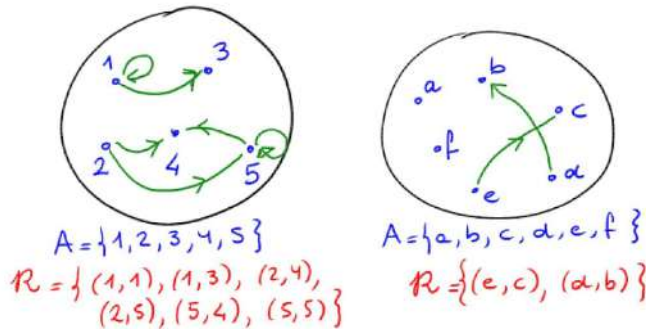
$$A \times B := \{(x, y) : x \in A, y \in B\}.$$

Definición 1.2.1. (Relación.)

Sean A y B conjuntos. Una *relación* $\mathcal{R}$ *de* A *en* B es un subconjunto cualquiera $\mathcal{R}$ del producto cartesiano $A \times B$. Es decir $\mathcal{R}$ es una relación de A en B si $\mathcal{R} \in \mathcal{P}(A \times B)$.

Sin embargo, cuando el conjunto A es finito (como en este caso), una relación $\mathcal{R}$ en A se puede representar también por medio de un *grafo dirigido*, o sea un conjunto de puntos (llamados *vértices*, que son los elementos del conjunto A) y un conjunto de *flechas* entre los vértices, que se corresponden con los elementos relacionados: se pone una flecha (que parte de x y llega a y) para cada elemento $(x, y) \in \mathcal{R}$, es decir cada vez que $x \mathcal{R} y$.

Ejemplos:



Definición 1.2.3. (Relación reflexiva, simétrica, antisimétrica y transitiva.)

Sean A un conjunto y $\mathcal{R}$ una relación en A.

- Se dice que $\mathcal{R}$ es *reflexiva* si $(x, x) \in \mathcal{R}, \forall x \in A$ (dicho de otra manera, $x \mathcal{R} x, \forall x \in A$). En términos del grafo de la relación, $\mathcal{R}$ es reflexiva si en cada vértice hay una flecha que es un "bucle", es decir que parte de él y llega a él.

- Se dice que $\mathcal{R}$ es *simétrica* si cada vez que un par $(x, y) \in \mathcal{R}$, entonces el par "simétrico" $(y, x) \in \mathcal{R}$ también (dicho de otra manera, $\forall x, y \in A,\ x \mathcal{R} y \Rightarrow y \mathcal{R} x$). En términos del grafo de la relación, $\mathcal{R}$ es simétrica si por cada flecha que une dos vértices en un sentido, hay una flecha (entre los mismos vértices) en el sentido opuesto.

- Se dice que $\mathcal{R}$ es *antisimétrica* si cada vez que un par $(x, y) \in \mathcal{R}$ con $x \neq y$, entonces el par $(y, x) \notin \mathcal{R}$ (dicho de otra manera, $\forall x, y \in A,\ x \mathcal{R} y$ e $y \mathcal{R} x \Rightarrow x = y$). En términos del grafo de la relación, $\mathcal{R}$ es antisimétrica si no hay ningún par de flechas en sentidos opuestos que unen dos vértices distintos.

- Se dice que $\mathcal{R}$ es *transitiva* si para toda terna de elementos $x, y, z \in A$ tales que $(x, y) \in \mathcal{R}$ e $(y, z) \in \mathcal{R}$, se tiene que $(x, z) \in \mathcal{R}$ también (dicho de otra manera, $\forall x, y, z \in A,\ x \mathcal{R} y$ e $y \mathcal{R} z \Rightarrow x \mathcal{R} z$). En términos del grafo de la relación, $\mathcal{R}$ es transitiva si hay un "camino directo" por cada "camino con paradas".

Definición 1.2.4. (Relación de equivalencia y relación de orden.)

Sean A un conjunto y $\mathcal{R}$ una relación en A.

- Se dice que una relación $\mathcal{R}$ en un conjunto A es una *relación de equivalencia* cuando es una relación reflexiva, simétrica y transitiva.
- Se dice que una relación $\mathcal{R}$ en un conjunto A es una *relación de orden* cuando es una relación reflexiva, antisimétrica y transitiva.

Definición 1.2.5. (Clases de equivalencia.)

Sean A un conjunto y $\sim$ una relación de equivalencia en A. Para cada $x \in A$, la *clase de equivalencia de* x es el conjunto

$$\overline{x} = \{y \in A : y \sim x\} \subseteq A.$$

Proposición 1.2.6. (Propiedad fundamental de las clases de equivalencia.)

Sean A un conjunto y $\sim$ una relación de equivalencia en A. Sean $x, y \in A$. Entonces, o bien $\overline{x} \cap \overline{y} = \emptyset$, o bien $\overline{x} = \overline{y}$.

Una relación de equivalencia sobre un conjunto induce una partición del mismo, es decir, un conjunto en el que se ha definido una relación de equivalencia puede ser dividido en varios subconjuntos de elementos equivalentes entre sí y tales que la reunión de esos subconjuntos coincide con el conjunto entero.

1.3 Funciones.

Sean A y B conjuntos, y sea $\mathcal{R}$ una relación de A en B. Se dice que $\mathcal{R}$ es una *función* cuando todo elemento $x \in A$ está relacionado con algún $y \in B$, y este elemento y es único. Es decir:

$$\forall\, x \in A,\ \exists!\, y \in B :\ x\,\mathcal{R}\,y.$$

Aquí el símbolo "$\exists!$" significa "existe un único", es decir:

$$\begin{aligned}&\forall\, x \in A,\ \exists\, y \in B \text{ tal que } x\,\mathcal{R}\,y,\\ &\text{y si } y, z \in B \text{ son tales que } x\,\mathcal{R}\,y \text{ y } x\,\mathcal{R}\,z,\ \text{entonces } y = z.\end{aligned}$$

Como a cada $x \in A$ le corresponde un $y \in B$ y este y es único, se le puede dar un nombre que hace notar que y depende de x: se dice que y es la *imagen* de x por f, y se suele notar "$y = f(x)$", que es la forma usual en la que conocemos a las funciones; se nota "$f : A \to B$" a una función del conjunto A en el conjunto B.

Definición 1.3.2. (Igualdad de funciones.)

Sean $f, g : A \to B$ funciones. Se tiene

$$f = g \iff f(x) = g(x),\ \forall\, x \in A.$$

Dada una función $f : A \to B$, el conjunto A se llama el *dominio* de la función f, y el conjunto B se llama el *codominio* de la función f. Como se ve de los ejemplos anteriores, todos los elementos del dominio tienen que estar involucrados en una función, o sea tienen que tener al menos una imagen y con $y = f(x)$, pero puede ocurrir que haya elementos y del codominio que no estén involucrados, que no tengan preimagen x tal que $f(x) = y$

Definición 1.3.3. (Imagen de una función.)

Sea $f : A \to B$ es una función. La *imagen* de f, que se nota $\mathrm{Im}(f)$, es el subconjunto de elementos de B que están relacionados con algún elemento de A. Es decir

$$\mathrm{Im}(f) = \{y \in B :\ \exists\, x \in A \text{ tal que } f(x) = y\}.$$

Definición 1.3.4. (Funciones inyectivas, sobreyectivas y biyectivas.)

Sea $f : A \to B$ una función. Se dice que

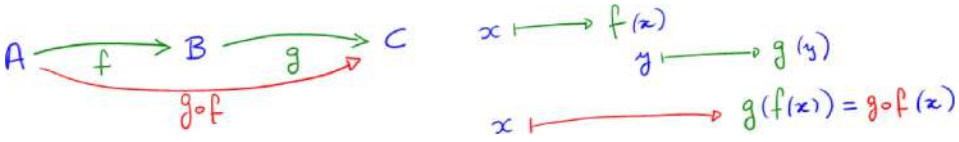
- f es *inyectiva* si *para todo* elemento $y \in B$ existe *a lo sumo un* elemento $x \in A$ para el cual $f(x) = y$. Dicho de otra manera, f es inyectiva si para todo $x, x' \in A$ tales que $f(x) = f(x')$ se tiene que $x = x'$.
- f es *sobreyectiva* si *para todo* elemento $y \in B$ existe *al menos un* elemento $x \in A$ para el cual $f(x) = y$. Dicho de otra manera, f es sobreyectiva si $\mathrm{Im}(f) = B$.
- f es *biyectiva* si es a la vez inyectiva y sobreyectiva, es decir *para todo* elemento $y \in B$ existe *exactamente un* elemento $x \in A$ para el cual $f(x) = y$.

Definición 1.3.5. (Composición de funciones.)

Sean A, B, C conjuntos, y $f : A \to B$, $g : B \to C$ funciones. Entonces la *composición* de f con g, que se nota $g \circ f$, definida por

$$g \circ f(x) = g\big(f(x)\big), \ \forall x \in A$$

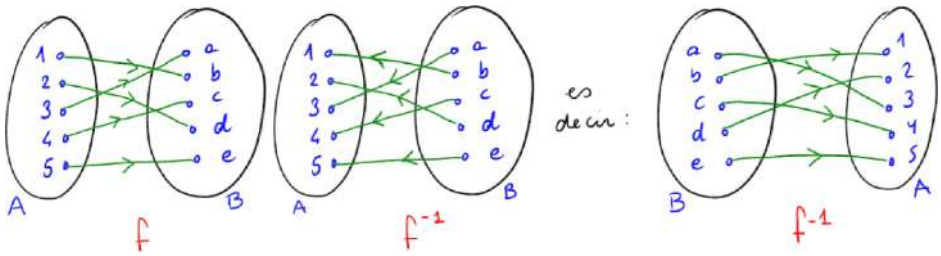
resulta ser una función de A en C. Esto se visualiza mejor en el diagrama:



1.3.1 Funciones biyectivas y función inversa.

función inversa de f. Está definida
únicamente cuando la función f es biyectiva. Se tiene que $f^{-1} : B \to A$ es la función que satisface para todo $y \in B$:

$$f^{-1}(y) = x \iff f(x) = y.$$



Proposición 1.3.6. (Biyectividad y función inversa.)

Sea $f : A \to B$ una función.

- *Si f es biyectiva, entonces $f^{-1} \circ f = \mathrm{id}_A$ y $f \circ f^{-1} = \mathrm{id}_B$.*
- *Si existe una función $g : B \to A$ tal que $g \circ f = \mathrm{id}_A$ y $f \circ g = \mathrm{id}_B$, entonces f es biyectiva y $f^{-1} = g$.*

- La función inversa de la función

$$f_6 : \mathbb{N} \to \mathbb{Z}, \ f_6(n) = \begin{cases} \dfrac{n-1}{2} & \text{si} \quad n \text{ es impar} \\ -\dfrac{n}{2} & \text{si} \quad n \text{ es par} \end{cases}$$

es la función $f_6^{-1} : \mathbb{Z} \to \mathbb{N}$ dada por

$$f_6^{-1}(k) = \begin{cases} 2k+1 & \text{si} \quad k \geq 0 \\ -2k & \text{si} \quad k \leq -1. \end{cases}$$

Números Naturales e Inducción.

2.1.1 La suma de Gauss.

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$$

$\forall\, n \in \mathbb{N}: \quad 1+2+\cdots+(n-1)+n = \dfrac{n(n+1)}{2}.$

2.1.2 La serie geométrica.

$$\sum_{i=0}^{n} q^i = 1+q+\cdots+q^n = \begin{cases} \frac{q^{n+1}-1}{q-1} & \text{si} \quad q \neq 1 \\ n+1 & \text{si} \quad q = 1. \end{cases}, \ \forall\, n \in \mathbb{N}.$$

2.2.1 Sumatoria.

Sea $n \in \mathbb{N}$. La notación $\sum_{i=1}^{n} a_i$, que se lee la *sumatoria* para i de 1 a n de a_i, representa la suma de los n primeros términos de la sucesión $(a_i)_{i\in\mathbb{N}}$:

$$\sum_{i=1}^{n} a_i = a_1 + \cdots + a_n,$$

que se define formalmente *por recurrencia*, para evitar los puntos suspensivos:

$$\sum_{i=1}^{1} a_i = a_1 \quad \text{y} \quad \sum_{i=1}^{n+1} a_i = \sum_{i=1}^{n} a_i \ + a_{n+1}\ , \ \forall\, n \in \mathbb{N}.$$

La sumatoria satisface las dos propiedades siguientes para todo $n \in \mathbb{N}$, para todo par de sucesiones $(a_i)_{i\in\mathbb{N}}$, $(b_i)_{i\in\mathbb{N}}$ en A y para todo $c \in A$:

- $\Big(\sum_{i=1}^{n} a_i\Big) + \Big(\sum_{i=1}^{n} b_i\Big) = \sum_{i=1}^{n} (a_i + b_i)\,.$
- $c \cdot \sum_{i=1}^{n} a_i = \sum_{i=1}^{n} c \cdot a_i\,.$

Así por ejemplo, $\sum_{k=1}^{n^2}(k+n) = \Big(\sum_{k=1}^{n^2} k\Big) + \Big(\sum_{k=1}^{n^2} n\Big) = \dfrac{n^2(n^2+1)}{2} + n^3\,.$

2.2.2 Productoria.

Sea $n \in \mathbb{N}$. La notación $\prod_{i=1}^{n} a_i$, que se lee la *productoria* para i de 1 a n de a_i, representa el producto de los n primeros términos de la sucesión $(a_i)_{i\in\mathbb{N}}$:

$$\prod_{i=1}^{n} a_i = a_1 \cdots a_n,$$

que se define formalmente *por recurrencia*, para evitar los puntos suspensivos:

$$\prod_{i=1}^{1} a_i = a_1 \quad \text{y} \quad \prod_{i=1}^{n+1} a_i = \Big(\prod_{i=1}^{n} a_i\Big) \cdot a_{n+1}\ , \ \forall\, n \in \mathbb{N}.$$

- $\prod_{i=1}^{n} i = 1 \cdot 2 \cdots (n-1) \cdot n$ se nota $n!$,

- $\prod_{i=1}^{n} c = c^n$, $\forall\, c \in A$, $\forall\, n \in \mathbb{N}$.

La productoria satisface la propiedad siguiente para todo $n \in \mathbb{N}$ y sucesiones $(a_i)_{i\in\mathbb{N}}$, $(b_i)_{i\in\mathbb{N}}$ en A:

- $\Big(\prod_{i=1}^{n} a_i\Big) \cdot \Big(\prod_{i=1}^{n} b_i\Big) = \prod_{i=1}^{n} (a_i \cdot b_i)$.

Teorema 2.3.2. (Principio de inducción.)

Sea $p(n)$, $n \in \mathbb{N}$, una afirmación sobre los números naturales. Si p satisface

- (Caso base) *$p(1)$ es Verdadera,*
- (Paso inductivo) *$\forall\, h \in \mathbb{N}$, $p(h)$ Verdadera $\Rightarrow$ $p(h+1)$ Verdadera,*

entonces $p(n)$ es Verdadero, $\forall\, n \in \mathbb{N}$.

Aquí la hipótesis "$p(h)$ Verdadero" para un h dado se denomina la *hipótesis inductiva* (HI).

Teorema 2.3.3. (Principio de inducción "corrido".)

Sea $n_0 \in \mathbb{Z}$ y sea $p(n), n \geq n_0$, una afirmación sobre $\mathbb{Z}_{\geq n_0}$. Si p satisface

- (Caso base) *$p(n_0)$ es Verdadera,*
- (Paso inductivo) *$\forall\, h \geq n_0$, $p(h)$ Verdadera $\Rightarrow$ $p(h+1)$ Verdadera,*

entonces $p(n)$ es Verdadero, $\forall\, n \in \mathbb{N}$.

2.4 Sucesiones definidas por recurrencia.

Una sucesión definida de esta manera, como aquí:

$$a_1 = 1, \quad a_{n+1} = 2a_n + 1, \ \forall\, n \in \mathbb{N}$$

es una sucesión definida *por recurrencia*, ya que para calcular un término necesitamos conocer el anterior. Además de necesitar conocer el caso base $n = 1$ obviamente, sino no sabríamos por donde empezar.

2.5.3 Sucesiones de Lucas.

Una *sucesión de Lucas* es una sucesión $(a_n)_{n\in\mathbb{N}_0}$ definida recursivamente por

$$a_0 = a,\ a_1 = b, \quad a_{n+2} = c\,a_{n+1} + d\,a_n,\ \forall\, n \in \mathbb{N}_0,$$

donde $a, b, c, d \in \mathbb{C}$ son números dados.

Consideremos la ecuación $X^2 - cX - d = 0$ asociada a la sucesión de Lucas (que se obtiene de la expresión $a_2 - c\,a_1 - d\,a_0 = 0$ y luego reemplazando a_2 por X^2, a_1 por X y a_0 por 1).

Supongamos que estamos en el caso en que $X^2 - cX - d$ tiene dos raíces distintas r y $\overline{r}$. Observemos que estas dos raíces r y $\overline{r}$ satisfacen las relaciones

$$r^2 = c\,r + d \quad \text{y} \quad \overline{r}^2 = c\,\overline{r} + d. \tag{2.3}$$

Existe una única sucesión $(\gamma_n)_{n\in\mathbb{N}_0} = (\alpha\, r^n + \beta\,\overline{r}^n)_{n\in\mathbb{N}_0}$ que satisface las condiciones iniciales $\gamma_0 = a$, $\gamma_1 = b$.

Esto es cierto pues para ello hay que resolver el sistema lineal

$$\begin{cases} \alpha & + & \beta & = & a \\ \alpha\, r & + & \beta\,\overline{r} & = & b \end{cases}$$

que tiene solución y es única pues $r \neq \overline{r}$ por hipótesis: se obtiene

$$\alpha = \frac{b - a\,\overline{r}}{r - \overline{r}} \quad \text{y} \quad \beta = \frac{a\,r - b}{r - \overline{r}}.$$

Se concluye que esta sucesión $(\gamma_n)_{n\in\mathbb{N}_0} = (\alpha\, r^n + \beta\,\overline{r}^n)_{n\in\mathbb{N}_0}$ coincide con la sucesión de Lucas original $(a_n)_{n\in\mathbb{N}_0}$, ya que satisface las mismas condiciones iniciales y la misma recurrencia. Por lo tanto el término general de la sucesión $(a_n)_{n\in\mathbb{N}_0}$ es

$$a_n = \alpha\, r^n + \beta\,\overline{r}^n,\ \forall n \in \mathbb{N}_0.$$

Teorema 2.5.7. (Principio de inducción completa.)

Sea $p(n)$, $n \in \mathbb{N}$, una afirmación sobre los números naturales. Si p satisface

- (Caso base) *$p(1)$ es Verdadera,*
- (Paso inductivo) *$\forall\, h \in \mathbb{N}$, $p(1), \ldots, p(h)$ Verdaderas $\Rightarrow$ $p(h+1)$ Verdadera,*

entonces $p(n)$ es Verdadero, $\forall\, n \in \mathbb{N}$.

(El paso inductivo en este caso también suele escribirse en la forma: $\forall\, h \in \mathbb{N}$, $p(k)$ Verdadera para $1 \leq k \leq h \ \Rightarrow\ p(h+1)$ Verdadera.)

Ejemplo: Sea $(a_n)_{n\in\mathbb{N}}$ la sucesión definida por recurrencia como

$$a_1 = 1, \quad a_{n+1} = 1 + \sum_{k=1}^{n} a_k, \ \forall\, n \in \mathbb{N}.$$

Probar que el término general de la sucesión es $a_n = 2^{n-1}$, $\forall\, n \in \mathbb{N}$.

Demostración. Aplicaremos aquí (por necesidad) el principio de inducción completa enunciado en el Teorema 2.5.7.

$$p(n): \quad a_n = 2^{n-1}.$$

- Caso base: ¿$p(1)$ V? Sí, pues $2^0 = 1 = a_1$.
- Paso inductivo: Dado $h \in \mathbb{N}$, ¿$p(1), \ldots, p(h)$ Verdaderas $\Rightarrow$ $p(h+1)$ Verdadera?
  - HI: $a_1 = 2^0 \quad, \ldots, a_h = 2^{h-1}$, o sea $a_k = 2^{k-1}$ para $1 \le k \le h$.
  - Qpq $a_{h+1} = 2^h$.

  Pero por definición de la sucesión, para $h \ge 1$ se tiene

  $$a_{h+1} \underset{def}{=} 1 + \sum_{k=1}^{h} a_k \underset{HI}{=} 1 + \sum_{k=1}^{h} 2^{k-1} \underset{\text{cambio de variable}}{=} 1 + \sum_{i=0}^{h-1} 2^i = 1 + (2^h - 1) = 2^h$$

  (usa suma geométrica)

  como se quería probar.

Es decir hemos probado tanto los casos base como el paso inductivo. Se concluye que $p(n)$ es Verdadero, $\forall\, n \in \mathbb{N}$. $\square$

Combinatoria de conjuntos, relaciones y funciones.

Definición 3.1.1. (Cardinal de un conjunto.)

Sea A un conjunto, se llama *cardinal de* A a la cantidad de elementos *distintos* que tiene A, y se nota $\#A$. Cuando el conjunto no tiene un número finito de elementos, se dice que es *infinito*, y se nota $\#A = \infty$.

Observación 3.1.2. (Cardinal de un subconjunto.)

Sea A es un conjunto finito y sea $B \subseteq A$. Entonces $\#B \leq \#A$

Observación 3.1.3. (Cardinal de la unión y del complemento.)

Sean A, B conjuntos finitos dentro de un conjunto referencial U.

- Si A y B son conjuntos disjuntos, entonces $\#(A \cup B) = \#A + \#B$.
- En general $\#(A \cup B) = \#A + \#B - \#(A \cap B)$.
- Si U es un conjunto finito, entonces $\#(A^c) = \#U - \#A$.

Se deduce por ejemplo

$$\#(A - B) = \#A - \#(A \cap B) \quad \text{y} \quad \#(A \triangle B) = \#A + \#B - 2\#(A \cap B).$$

Proposición 3.1.4. (Cardinal del producto cartesiano y del conjunto de partes.)

1. *Sean A y B conjuntos finitos. Entonces $\#(A \times B) = \#A \cdot \#B$.*
2. *Sean $AA_1, \ldots, A_n, A$ conjuntos finitos. Entonces*

$$\#(A_1 \times \cdots \times A_n) = \#A_1 \cdots \#A_n = \prod_{i=1}^{n} \#A_i,$$
$$\#(A^n) = (\#A)^n.$$

3. *Sea A un conjunto finito, entonces $\#(\mathcal{P}(A)) = 2^{\#A}$.*

Proposición 3.1.5. (Cantidad de relaciones.)

Sean A_m y B_n conjuntos finitos, con m y n elementos respectivamente. Entonces la cantidad de relaciones que hay de A_m en B_n es igual a $2^{m \cdot n}$.

Proposición 3.1.6. (Cantidad de funciones.)

Sean A_m y B_n conjuntos finitos, con m y n elementos respectivamente. Entonces la cantidad de funciones f que hay de A_m en B_n es igual a n^m.

Proposición 3.1.7. (Cardinal de conjuntos y funciones.)

Sean A y B conjuntos finitos.

- *Sea $f : A \to B$ una función* inyectiva. *Entonces $\#A \leq \#B$.*
- *Sea $f : A \to B$ una función* sobreyectiva. *Entonces $\#A \geq \#B$.*
- *Sea $f : A \to B$ una función* biyectiva. *Entonces $\#A = \#B$.*

Definición 3.2.1. (El factorial, o la cantidad de funciones biyectivas.)

Sea $n \in \mathbb{N}$. El *factorial* de n, que se nota $n!$, es el número natural definido como

$$n! = n \cdot (n-1) \cdots 2 \cdot 1 = \prod_{i=1}^{n} i,$$

que coincide con la cantidad de funciones biyectivas que hay entre dos conjuntos con n elementos, o con la cantidad de permutaciones de elementos en un conjunto de n elementos.
Esta definición se extiende a $\mathbb{N}_0$ definiendo $0! = 1$.

Proposición 3.2.2. (Cantidad de funciones inyectivas.)

Sean A_m y B_n conjuntos finitos, con m y n elementos respectivamente, donde $m \leq n$. Entonces la cantidad de funciones inyectivas $f : A_m \to B_n$ que hay es

$$n \cdot (n-1) \cdots (n-m+1) = \frac{n!}{(n-m)!}.$$

Teorema 3.3.4. (Número combinatorio.)

Sea $n \in \mathbb{N}_0$ y sea A_n un conjunto con n elementos. Para $0 \leq k \leq n$, la cantidad de subconjuntos con k elementos del conjunto A_n (o equivalentemente, la cantidad de maneras que hay de elegir k elementos en el conjunto A_n) es igual a

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

Observación 3.3.2.

- $\binom{n}{0} = \binom{n}{n} = 1$ pues el único subconjunto de A_n con 0 elementos es el conjunto $\emptyset$, y el único subconjunto de A_n con n elementos es A_n mismo.

- $\binom{n}{1} = n$ pues los subconjuntos de A_n con 1 elemento son los subconjuntos
$$\{a_1\}, \{a_2\}, \ldots, \{a_{n-1}\}, \{a_n\}.$$

- Podemos darnos cuenta que $\binom{n}{n-1} = n$ también ya que dar un subconjunto de A_n con $n-1$ elementos es lo mismo que elegir cuál elemento a_i quedó afuera del subconjunto: por ejemplo el subconjunto $\{a_1, \ldots, a_{n-1}\}$ es el que corresponde a haber dejado a_n afuera.

- Con el mismo razonamiento, $\binom{n}{k} = \binom{n}{n-k}$, $\forall\, k, 0 \leq k \leq n$, ya que a cada subconjunto B_k de A_n con k elementos, podemos asignarle el subconjunto complemento B_k^c que tiene $n-k$ elementos, y esta asignación es una función biyectiva... O lo que es lo mismo, cada vez que elegimos k elementos en A_n estamos dejando de elegir los $n-k$ elementos complementarios.

- Más aún, dado que $\binom{n}{k}$, $0 \leq k \leq n$, cuenta la cantidad de subconjuntos con k elementos en el conjunto A_n con n elementos, y que sabemos que la cantidad total de subconjuntos que hay en A_n es 2^n, se tiene:

$$2^n = \binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n-1} + \binom{n}{n} = \sum_{k=0}^{n} \binom{n}{k}, \quad \forall n \in \mathbb{N}_0.$$

3.3.3 El Binomio de Newton.

$$(x+y)^n = x^n + \binom{n}{1}x^{n-1}y + \binom{n}{2}x^{n-2}y^2 + \cdots + \binom{n}{n-1}xy^{n-1} + y^n$$
$$= \sum_{k=0}^{n}\binom{n}{k}x^{n-k}y^k, \ \forall\, n \in \mathbb{N}_0,$$

o lo que es lo mismo, ya que los números combinatorios son simétricos ($\binom{n}{k} = \binom{n}{n-k}$)*:*

$$(x+y)^n = \sum_{k=0}^{n}\binom{n}{k}x^{k}y^{n-k}, \ \forall\, n \in \mathbb{N}_0.$$

Enteros – Primera parte.

Definición 4.2.1. (Divisibilidad.)

Sean $a, d \in \mathbb{Z}$ con $d \neq 0$. Se dice que d *divide* a a, y se nota $d \mid a$, si existe un elemento $k \in \mathbb{Z}$ tal que $a = k \cdot d$ (o sea si el cociente $\frac{a}{d}$ es un número entero). También se dice en ese caso que a es divisible por d, o que a es múltiplo de d. O sea:

$$d \mid a \iff \exists\, k \in \mathbb{Z} : a = k \cdot d.$$

En caso contrario, se dice que d no divide a a, y se nota $d \nmid a$. Eso es cuando el cociente $\frac{a}{d} \notin \mathbb{Z}$, o sea no existe ningún entero $k \in \mathbb{Z}$ tal que $a = k \cdot d$.

El conjunto de los divisores positivos y negativos de un entero a se notará por $\mathrm{Div}(a)$ y el de los divisores positivos por $\mathrm{Div}_+(a)$.

Propiedades 4.2.2. (De la divisibilidad.)

- Todo número entero $d \neq 0$ satisface que $d \mid 0$ pues $0 = 0 \cdot d$ (aquí $k = 0$). Así el 0 tiene infinitos divisores : $\mathrm{Div}\,(0) = \mathbb{Z} \setminus \{0\}$.
- $d \mid a \Leftrightarrow -d \mid a$ (pues $a = k \cdot d \Leftrightarrow a = (-k) \cdot (-d)$).

  De la misma manera $d \mid a \Leftrightarrow d \mid -a \Leftrightarrow -d \mid -a$.

  Se concluye que $d \mid a \Leftrightarrow |d| \mid |a|$ (donde $|x|$ denota el módulo o valor absoluto de x).

  En particular a cada divisor negativo de a le corresponde un divisor positivo.
- Si $a \neq 0$, $d \mid a \Rightarrow |d| \leq |a|$ (pues $|a| = k|d|$ con $|a| \neq 0$ implica k es un entero no nulo y positivo, es decir $k \geq 1$; por lo tanto, $|a| = k|d| \geq |d|$).

  En particular, todo número entero a *no nulo* tiene sólo un número finito de divisores, todos pertenecientes al conjunto

  $$\{-|a|, \ldots, -1, 1, \ldots, |a|\}.$$

  O sea $\mathrm{Div}_+\,(a) \subset \{1, \ldots, |a|\}$.

  Además, por la observación del inciso anterior, el número total de divisores de a es el doble del número de divisores positivos.
- $d \mid a$ y $a \mid d \Leftrightarrow a = \pm d$ (pues $a = k \cdot d$ y $d = j \cdot a$ implica que $a = (k \cdot j) \cdot a$, por lo tanto k y j son dos números enteros que satisfacen $k \cdot j = 1$, o sea, $k = \pm 1$).
- Para todo $a \in \mathbb{Z}$, se tiene $1 \mid a$ y $-1 \mid a$, y también $a \mid a$ y $-a \mid a$.

  Así, si $a \neq \pm 1$, a tiene por lo menos 4 divisores distintos $(\pm 1, \pm a)$, o 2 divisores positivos distintos $(1, |a|)$.

Definición 4.2.3. (Números primos y compuestos.)

- Se dice que $a \in \mathbb{Z}$ es un número *primo* si $a \neq 0, \pm 1$ y tiene únicamente 4 divisores (o 2 divisores positivos). Por ejemplo $\pm 2, \pm 3, \pm 5, \pm 7, \pm 11$.

  (En general los números primos se notan con las letras p, q,...)
- Se dice que a es un número *compuesto* si $a \neq 0, \pm 1$ y tiene más que 4 divisores (o más que 2 divisores positivos). Por ejemplo $\pm 4, \pm 6, \pm 8, \pm 9$.

  Se observa que a es compuesto si y sólo si tiene un divisor positivo d que satisface $2 \leq d \leq |a| - 1$ (pues ya vimos que $\mathrm{Div}_+\,(a) \subset \{1, \ldots, |a|\}$ y si a tiene más que 2 divisores positivos, tiene que haber uno en "algún lugar en el medio").

Propiedades 4.2.4. (De la divisibilidad.)

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

- $d \mid a$ y $d \mid b \Rightarrow d \mid a+b$.

  (Pues si $a = k \cdot c$ y $b = j \cdot c$ con $k, j \in \mathbb{Z}$, entonces $a+b = (k+j) \cdot c$, donde $k+j \in \mathbb{Z}$.)
- $d \mid a$ y $d \mid b \Rightarrow d \mid a-b$.
- $d \mid a+b$ no implica que $d \mid a$ y $d \mid b$: Por ejemplo, $6 \mid 4+8$ pero $6 \nmid 4$ y $6 \nmid 8$.
- Sin embargo si $d \mid a+b$ y *se sabe que* $d \mid a$, entonces $d \mid b$.

  (Pues $d \mid (a+b)-a$.)
- $d \mid a \Rightarrow d \mid c \cdot a$, $\forall\, c \in \mathbb{Z}$.
- $d \mid a \Rightarrow d^2 \mid a^2$ y $d^n \mid a^n$, $\forall\, n \in \mathbb{N}$.

  (Pues si $a = k \cdot d$, entonces $a^2 = k^2 \cdot d^2$ y $a^n = k^n \cdot d^n$.)

  Veremos más adelante que vale la recíproca también: si $d^2 \mid a^2$ entonces $d \mid a$, etc.)
- $d \mid a \cdot b$ no implica $d \mid a$ o $d \mid b$: Por ejemplo, $6 \mid 3 \cdot 4$ pero $6 \nmid 3$ y $6 \nmid 4$.

Definición 4.2.5. (Congruencia.)

Sea $d \in \mathbb{Z}$, $d \neq 0$. Dados $a, b \in \mathbb{Z}$, se dice que a *es congruente a* b *módulo* d si $d \mid a-b$.

Se nota $a \equiv b \pmod{d}$ o también $a \equiv b\ (d)$. O sea:

$$a \equiv b \pmod{d} \iff d \mid a-b.$$

En caso contrario se nota $a \not\equiv b \pmod{d}$ o $a \not\equiv b\ (d)$.

Proposición 4.2.6. (La congruencia es una relación de equivalencia.)

Sea $d \in \mathbb{Z}$, $d \neq 0$. *Sea* $\mathcal{R}$ *la relación en* $\mathbb{Z}$ *dada por*

$$a\ \mathcal{R}\ b \iff a \equiv b \pmod{d}, \quad \forall\, a, b \in \mathbb{Z}.$$

Entonces $\mathcal{R}$ *es una relación de equivalencia.*

Demostración.

- *Reflexividad :* Para todo $a \in \mathbb{Z}$, $a \equiv a \pmod{d}$ pues $d \mid a-a$.
- *Simetría :* Hay que probar que para todo $a, b \in \mathbb{Z}$ tales que $a \equiv b \pmod{d}$, entonces $b \equiv a \pmod{d}$. Pero $a \equiv b \pmod{d}$ significa que $d \mid a-b$, y por lo tanto $d \mid -(a-b) = b-a$, luego $b \equiv a \pmod{d}$.
- *Transitividad :* Hay que probar que para todo $a, b, c \in \mathbb{Z}$ tales que $a \equiv b \pmod{d}$ y $b \equiv c \pmod{d}$ entonces $a \equiv c \pmod{d}$. Pero $a \equiv b \pmod{d}$ significa que $d \mid a-b$, y $b \equiv c \pmod{d}$ significa que $d \mid b-c$. Por lo tanto $d \mid (a-b)+(b-c) = a-c$, es decir $a \equiv c \pmod{d}$.

Proposición 4.2.7. (Propiedades de la congruencia.)

Sea $d \in \mathbb{Z}$, $d \neq 0$. *Entonces :*

1. *Para todo* $n \in \mathbb{N}$, $a_1, \ldots, a_n, b_1, \ldots, b_n \in \mathbb{Z}$,

$$\begin{cases} a_1 \equiv b_1 \pmod{d} \\ \quad \vdots \\ a_n \equiv b_n \pmod{d} \end{cases} \implies a_1 + \cdots + a_n \equiv b_1 + \cdots + b_n \pmod{d}.$$

2. $\forall\, a, b, c \in \mathbb{Z}$,

$$a \equiv b \pmod{d} \implies c\,a \equiv c\,b \pmod{d}.$$

5. *Para todo* $n \in \mathbb{N}$, $a_1, \ldots, a_n, b_1, \ldots, b_n \in \mathbb{Z}$,

$$\begin{cases} a_1 \equiv b_1 \pmod{d} \\ \quad \vdots \\ a_n \equiv b_n \pmod{d} \end{cases} \implies a_1 \cdots a_n \equiv b_1 \cdots b_n \pmod{d}.$$

6. $\forall\, a, b \in \mathbb{Z}$, $n \in \mathbb{N}$,

$$a \equiv b \pmod{d} \Rightarrow a^n \equiv b^n \pmod{d}.$$

Teorema 4.3.1. (Algoritmo de división.)

Dados $a, d \in \mathbb{Z}$ *con* $d \neq 0$, existen $k, r \in \mathbb{Z}$ *que satisfacen*

$$a = k \cdot d + r \quad \text{con} \quad 0 \leq r < |d|.$$

Además, k *y* r *son* únicos *en tales condiciones.*

Se dice que k es el *cociente* y r es el *resto* de la división de a por d (a es el *dividendo* y d el *divisor*). Al resto r lo notaremos $r_d(a)$ para especificar que es el "resto de a al dividir por d".

Observación 4.3.3. (Divisibilidad y resto.)

Sean $a, d \in \mathbb{Z}$, $d \neq 0$. Entonces

$$r_d(a) = 0 \iff d \mid a \iff a \equiv 0 \pmod{d}.$$

Proposición 4.3.4. (Congruencia y resto.)

Sea $d \in \mathbb{Z}$, $d \neq 0$. *Entonces*

1. $a \equiv r_d(a) \pmod{d}$, $\forall\, a \in \mathbb{Z}$.
2. $a \equiv r \pmod{d}$ *con* $0 \leq r < |d| \Rightarrow r = r_d(a)$.
3. $r_1 \equiv r_2 \pmod{d}$ *con* $0 \leq r_1, r_2 < |d| \Rightarrow r_1 = r_2$.
4. $a \equiv b \pmod{d} \iff r_d(a) = r_d(b)$.

Corolario 4.3.5. (Tablas de Restos.)

Sean $a, b, d \in \mathbb{Z}$, $d \neq 0$. *Entonces*

- $r_d(a+b) = r_d\big(r_d(a) + r_d(b)\big)$.
- $r_d(a \cdot b) = r_d\big(r_d(a) \cdot r_d(b)\big)$.
- $r_d(a^n) = r_d\big(r_d(a)^n\big)$, $\forall\, n \in \mathbb{N}$.

Demostración.

$$\begin{cases} a \equiv r_d(a) \pmod d \\ b \equiv r_d(b) \pmod d \end{cases} \implies \begin{cases} a+b \equiv r_d(a)+r_d(b) \pmod d \\ a \cdot b \equiv r_d(a) \cdot r_d(b) \pmod d \\ a^n \equiv r_d(a)^n \pmod d,\ \forall\, n \in \mathbb{N}. \end{cases}$$

Definición 4.5.1. (Máximo común divisor.)

Sean $a, b \in \mathbb{Z}$, no ambos nulos. El *máximo común divisor* entre a y b, que se nota $(a : b)$, es el mayor de los divisores comunes de a y b. Es decir:

$$(a:b) \mid a,\ (a:b) \mid b \quad \text{y si} \quad d \mid a \text{ y } d \mid b, \text{ entonces } \ d \leq (a:b).$$

- Probar que los únicos valores posibles para $(a^2+8 : a+1)$, $\forall\, a \in \mathbb{Z}$, son 1, 3 o 9, y mostrar con ejemplos que se realizan todos.

Para ello miramos quiénes son los posibles divisores comunes de a^2+8 y $a+1$:

$$\begin{cases} d \mid a^2+8 \\ d \mid a+1 \end{cases} \implies \begin{cases} d \mid a^2+8 \\ d \mid (a-1)(a+1) = a^2-1 \end{cases} \implies d \mid 9,$$

restando. Por lo tanto en principio los posibles valores para el máximo común divisor son únicamente los divisores positivos de 9: 1, 3 o 9. Efectivamente, para $a = 0$ se consigue $(a^2+8 : a+1) = (8:1) = 1$, para $a = 2$ se consigue $(a^2+8 : a+1) = (12:3) = 3$ y para $a = -1$ se consigue $(a^2+8 : a+1) = (9:0) = 9$.

Proposición 4.5.2. *Sean $a, b \in \mathbb{Z}$ no ambos nulos, y sea $k \in \mathbb{Z}$, entonces:*

$$\begin{aligned} &\mathrm{DivCom}(\{a,b\}) = \mathrm{DivCom}(\{b, a-k\cdot b\}),\ y \\ &\mathrm{DivCom}_+(\{a,b\}) = \mathrm{DivCom}_+(\{b, a-k\cdot b\}). \end{aligned}$$

En particular, para todo $k \in \mathbb{Z}$, $\quad (a:b) = (b : a-k\cdot b)$.

Aplicando esto a $r_b(a) = a - k\cdot b$, se obtiene que $(a:b) = (b : r_b(a))$.

Ejemplo: Cálculo de $(120 : -84)$:

Como $(120 : -84) = (120 : 84)$, calculamos este último para simplificar las divisiones (esto no es esencial para el algoritmo). Se tiene

$$\begin{array}{rcl} 120 &=& 1\cdot 84 + 36 \implies (120:84) = (84:36) \\ 84 &=& 2\cdot 36 + 12 \implies (84:36) = (36:12) \\ 36 &=& 3\cdot 12 + 0 \implies (36:12) = (12:0). \end{array}$$

Pero $(12:0) = 12$, luego $(120 : -84) = 12$ ya que

$$(120:-84) = (120:84) = (84:36) = (36:12) = (12:0) = 12.$$

Teorema 4.5.5. (Mcd y combinación entera.)

Sean $a, b \in \mathbb{Z}$, *no ambos nulos. Entonces existen* $s, t \in \mathbb{Z}$ *tales que*

$$(a : b) = s \cdot a + t \cdot b.$$

Observación 4.5.6. (Combinaciones enteras de a y b.)

Sean $a, b \in \mathbb{Z}$ no ambos nulos, y $c \in \mathbb{Z}$.

$$c = s' \cdot a + t' \cdot b \text{ para } s', t' \in \mathbb{Z} \quad \Longleftrightarrow \quad (a : b) \mid c.$$

La observación anterior nos dice que el máximo común divisor $(a : b)$ es el número *natural más chico* que se puede escribir como combinación entera de a y b y que todas las demás combinaciones enteras de a y b son divisibles por él.

El Teorema 4.5.5 tiene otra consecuencia importantísima que no es obvia a primera vista: el máximo común divisor no solo es el más grande de los divisores comunes sino que también es divisible por todos los divisores comunes.

Proposición 4.5.7. (Mcd y divisores comunes.)

Sean $a, b \in \mathbb{Z}$, *no ambos nulos y sea* $d \in \mathbb{Z}$, *con* $d \neq 0$. *Entonces*

$$d \mid a \;\; y \;\; d \mid b \iff d \mid (a : b).$$

Proposición 4.5.8. (Mcd de múltiplo común de dos números.)

Sean $a, b \in \mathbb{Z}$, *no ambos nulos, y sea* $k \in \mathbb{Z}$ *con* $k \neq 0$. *Entonces*

$$(k\,a : k\,b) = |k| \cdot (a : b).$$

Teorema 4.5.9. (Equivalencias del mcd.)

Sean $a, b \in \mathbb{Z}$, *no ambos nulos, y sea* $d \in \mathbb{N}$. *Son equivalentes:*

1. $d \mid a,\ d \mid b$ *y si* $c \mid a \;\; y \;\; c \mid b$, *entonces* $c \leq d$.
2. $d \mid a,\ d \mid b$ *y existen* $s, t \in \mathbb{Z}$ *tales que* $d = sa + tb$.
3. $d \mid a,\ d \mid b$ *y si* $c \mid a \;\; y \;\; c \mid b$, *entonces* $c \mid d$.

Un número $d \in \mathbb{N}$ *que cumple cualquiera de esas 3 propiedades es el máximo común divisor* $(a : b)$.

Definición 4.5.10. (Números coprimos.)

Se dice que $a, b \in \mathbb{Z}$ no ambos nulos son *coprimos* si y solo si $(a : b) = 1$, es decir si y solo si los únicos divisores comunes de a y b son ± 1.

$$a \perp b \iff (a : b) = 1$$

- Para $a, b \in \mathbb{Z}$ coprimos, los distintos valores que puede tomar $(2a+b : 3a-2b)$ son exactamente el 1 y el 7:

– Sea d un divisor común entre $2a+b$ y $3a-2b$,

$$\begin{cases} d \mid 2a+b \\ d \mid 3a-2b \end{cases} \implies \begin{cases} d \mid 3(2a+b) \\ d \mid 2(3a-2b) \end{cases}$$
$$\implies \begin{cases} d \mid 6a+3b \\ d \mid 6a-4b \end{cases} \implies d \mid 7b.$$

De la misma manera:

$$\begin{cases} d \mid 2a+b \\ d \mid 3a-2b \end{cases} \implies \begin{cases} d \mid 2(2a+b) \\ d \mid 3a-2b \end{cases}$$
$$\implies \begin{cases} d \mid 4a+2b \\ d \mid 3a-2b \end{cases} \implies d \mid 7a.$$

Luego $d \mid 7a$ y $d \mid 7b$. Aplicando las Proposiciones 4.5.7 y 4.5.8 y el hecho que $a \perp b$, se tiene

$$d \mid (7a : 7b) = 7(a : b) = 7 \implies d \mid 7.$$

Se concluye que el máximo común divisor, que es el mayor de estos d posibles, es o bien 1 o 7 como se quería probar (además efectivamente ya mostramos que había casos en que es 1 y casos en que es 7).

Observación 4.5.11. (Coprimos y combinación entera.)

Sean $a, b \in \mathbb{Z}$ no ambos nulos. Entonces

$$a \perp b \iff \exists\, s, t \in \mathbb{Z} \;:\; 1 = s\,a + t\,b.$$

Proposición 4.5.12. (Propiedades esenciales de divisibilidad con coprimalidad.)

Sean $a, b, c, d \in \mathbb{Z}$ con $c \neq 0$ y $d \neq 0$. Entonces

1. $c \mid a,\ d \mid a$ y $c \perp d \implies c\,d \mid a$.
2. $d \mid a\,b$ y $d \perp a \implies d \mid b$.

Ejemplo: Cálculo de los $a, b \in \mathbb{Z}$ coprimos tales que $\dfrac{2}{a} + \dfrac{a}{b}$ es entero.

$$\frac{2}{a} + \frac{a}{b} = \frac{2b + a^2}{ab} \in \mathbb{Z} \iff ab \mid 2b + a^2.$$

Pero al ser $a \perp b$, $ab \mid 2b + a^2 \Leftrightarrow a \mid 2b + a^2$ y $b \mid 2b + a^2$.

Pero, dado que $a \mid a^2$, $a \mid 2b + a^2 \Leftrightarrow a \mid 2b$, y, dado que $a \perp b$, $a \mid 2b \Leftrightarrow a \mid 2$. Es decir, $a \in \{\pm 1, \pm 2\}$.

De la misma forma, dado que $b \mid 2b$, $b \mid 2b + a^2 \Leftrightarrow b \mid a^2$, y, dado que $b \perp a^2$ (pues $a \perp b$), $b \mid a^2 \cdot 1 \Leftrightarrow b \mid 1$, o sea $b \in \{\pm 1\}$.

Se obtienen luego los 8 pares $a = \pm 1, b = \pm 1$ y $a = \pm 2, b = \pm 1$.

Proposición 4.5.13. ("Coprimizando")

Sean $a, b \in \mathbb{Z}$, *no ambos nulos. Entonces*

$$\frac{a}{(a:b)} \perp \frac{b}{(a:b)}.$$

Por lo tanto

$$a = (a:b)\,a' \quad y \quad b = (a:b)\,b'$$

donde los números enteros $a' = \dfrac{a}{(a:b)}$ *y* $b' = \dfrac{b}{(a:b)}$ *son coprimos.*

Ejemplos:

- Sean $a, b \in \mathbb{Z}$ no ambos nulos tales que $(a:b) = 6$. ¿Cuáles son los posibles valores de $(6a + 12b : 6\,a - 6\,b)$?

  Coprimizando, se tiene $a = 6\,a'$, $b = 6\,b'$ con $a' \perp b'$, luego

  $$\begin{aligned}(6a + 12b : 6a - 6b) &= (36a' + 72b : 36a' - 36b') \\ &= (36'(a' + 2b') : 36(a' - b')) \\ &= 36(a' + 2b : a' - b').\end{aligned}$$

  Para concluir falta averiguar quiénes son los posibles valores de $(a' + 2b' : a' - b')$ si $a' \perp b'$.

  Sea entonces d un divisor común:

  $$\begin{cases} d \mid a' + 2b' \\ d \mid a' - b' \end{cases} \implies d \mid 3b',$$

  $$\begin{cases} d \mid a' + 2b' \\ d \mid a' - b' \end{cases} \implies \begin{cases} d \mid a' + 2b' \\ d \mid 2a' - 2b' \end{cases} \implies d \mid 3a'.$$

  Obtuvimos $d \mid 3a'$ y $d \mid 3b'$. Luego $d \mid (3a' : 3b') = 3(a' : b') = 3$.

  Por lo tanto, los posibles valores de $(a' + 2b' : a' - b')$ si $a' \perp b'$ son en principio 1 y 3. Efectivamente si por ejemplo $a' = 1$ y $b' = 0$, $(a' + 2b' : a' - b') = 1$ mientras que si $a' = b' = 1$, $(a' + 2b' : a' - b') = (3:0) = 3$.

  Por lo tanto hemos probado que si $(a:b) = 6$, los valores que puede tomar

  $$(6a + 12b : 6\,a - 6\,b) = 36(a' + 2b : a' - b')$$

  son $36 \cdot 1 = 36$ o $36 \cdot 3 = 108$.

- Sea $a \in \mathbb{Z}$ tal que $(a:8) = 4$. ¿Cuáles son los posibles valores de $(a^2 + a + 32 : 16)$?

  La condición $(a:8) = 4$ implica en particular que $4 \mid a$, o sea $a = 4\,a'$. Por lo tanto,

  $$4 = (a:8) = (4a' : 4 \cdot 2) = 4(a' : 2) \implies 1 = (a' : 2),$$

  o sea a' impar. Luego,

  $$\begin{aligned}(a^2 + a + 32 : 16) &= (16\,a'^2 + 4\,a' + 32 : 16) = \big(4\,(4\,a'^2 + a' + 8) : 4 \cdot 4\big) \\ &= 4\,(4a'^2 + a' + 8 : 4),\end{aligned}$$

  donde a' es impar. Ahora bien, $(4a'^2 + a' + 8 : 4) \in \{1, 2, 4\}$ pues tiene que ser un divisor positivo de 4. Como claramente $2 \nmid 4a'^2 + a' + 8$ pues a' es impar, 2 no es un divisor común (no divide al mcd). Luego $(4a'^2 + a' + 8 : 4) = 1$. Por lo tanto $(a^2 + a + 32 : 16) = 4$.

Observación 4.5.14. Sean $a, b \in \mathbb{Z}$, no ambos nulos. Sea $d \in \mathbb{N}$ un número que satisface que

$$d \mid a,\ d \mid b \quad \text{y} \quad \frac{a}{d} \perp \frac{b}{d}.$$

Entonces $d = (a : b)$.

(Esto vale por ejemplo porque $\frac{a}{d} \perp \frac{b}{d} \Leftrightarrow \exists\, s, t \in \mathbb{Z}$ con $1 = s\frac{a}{d} + t\frac{b}{d}$, lo que implica que $d = sa + tb$, la caracterización (2) del Teorema 4.5.9.)

4.6 Primos y factorización.

Recordemos que un número $p \in \mathbb{Z}$ es *primo* si y solo si es $\neq 0, \pm 1$ y tiene únicamente 4 divisores, o, lo que es lo mismo, si y solo si tiene únicamente 2 divisores positivos. También, que un número $a \in \mathbb{Z}$ es *compuesto* si y solo si es $\neq 0, \pm 1$ y existe $d \in \mathbb{Z}$ con $1 < d < |a|$ tal que $d \mid a$.

Proposición 4.6.1. (Todo número entero $\neq 0, \pm 1$ es divisible por algún primo.)

Sea $a \in \mathbb{Z}$, $a \neq 0, \pm 1$. Entonces existe un número primo (positivo) p tal que $p \mid a$.

Corolario 4.6.2. (Cantidad de primos.)

Existen infinitos primos (positivos) distintos.

Digresión sobre Complejidad (1) Dado un número a, hay un algoritmo muy natural para establecer si a es primo o no: simplemente se divide a a por todos los números d menores que él (o por todos los primos menores que él, produciéndolos por ejemplo con la criba, o en realidad alcanza con dividirlo por todos los primos menores que $\sqrt{a}$, como se comentó arriba). Si nunca da resto 0, es que a es primo.

4.6.1 La propiedad fundamental de los números primos.

Si p es un número primo (positivo), y $a \in \mathbb{Z}$ es cualquiera, entonces $\mathrm{Div}_+(p) = \{1, p\}$ y por lo tanto $\mathrm{DivCom}_+(\{p, a\}) \subset \{1, p\}$: es igual a $\{1, p\}$ cuando $p \mid a$ y es igual a $\{1\}$ cuando $p \nmid a$. Por lo tanto el máximo común divisor entre p y a, es igual a p cuando $p \mid a$ y es igual a 1 cuando $p \nmid a$:

$$(p : a) = \begin{cases} p & \text{si} \quad p \mid a \\ 1 & \text{si} \quad p \nmid a \end{cases}, \qquad \text{y por lo tanto} \qquad p \perp a \ \Leftrightarrow\ p \nmid a.$$

(En particular, observemos que si p y q son primos positivos distintos, entonces $p \perp q$.)

Teorema 4.6.3. (Propiedad fundamental de los números primos.)

Sea p un primo y sean $a, b \in \mathbb{Z}$. Entonces

$$p \mid a \cdot b \implies p \mid a \quad o \quad p \mid b.$$

Demostración. La Proposición 4.5.12 (2) dice que si $p \mid a \cdot b$ y $p \perp a$ entonces $p \mid b$. Por lo visto arriba, la condición $p \perp a$ es equivalente a $p \nmid a$. Luego la Proposición 4.5.12 (2) dice que si $p \mid a \cdot b$ y $p \nmid a$ entonces $p \mid b$. Esto es claramente lo mismo que decir que si $p \mid a \cdot b$ entonces $p \mid a$ o $p \mid b$, pues si $p \mid a \cdot b$, hay dos posibilidades: Si $p \mid a$, ya está. Y si $p \nmid a$, entonces $p \mid b$. □

p es primo si y solo si cada vez que p divide a un producto divide a alguno de los factores.

Proposición 4.6.4. *Sea p un número primo y sean $a_1, \ldots, a_n \in \mathbb{Z}$, con $n \geq 2$. Entonces*

$$p \mid a_1 \cdots a_n \implies p \mid a_i \text{ para algún } i,\ 1 \leq i \leq n.$$

En particular, dado $a \in \mathbb{Z}$, si $p \mid a^n$ entonces $p \mid a$.

Teorema 4.6.5. (Teorema fundamental de la aritmética.)

Sea $a \in \mathbb{Z}$, $a \neq 0, \pm 1$. Entonces a se escribe en forma única como producto de primos (positivos)*, (o se factoriza en forma única como producto de primos (positivos),) es decir:*

- $\forall\, a \in \mathbb{Z},\ a \neq 0, \pm 1$, *existe* $r \in \mathbb{N}$ *y* existen *primos positivos* $p_1, \ldots, p_r$ *distintos y* $m_1, \ldots, m_r \in \mathbb{N}$ *tales que*

$$a = \pm\, p_1^{m_1} \cdot p_2^{m_2} \cdots p_r^{m_r}.$$

- *Esta escritura es* única *salvo permutación de los primos.*

<u>*Ejemplo:*</u> Sean $a = 84 = 2^2 \cdot 3 \cdot 7$ y $b = 188650 = 2 \cdot 5^2 \cdot 7^3 \cdot 11$. Entonces

$$a \cdot b = 2^3 \cdot 3 \cdot 5^2 \cdot 7^4 \cdot 11 \quad \text{y} \quad a^9 = 2^{18} \cdot 3^9 \cdot 7^9$$

Observación 4.6.6. (Primos de productos y potencias.)

Sean $a, b \in \mathbb{Z}$ no nulos de la forma

$$a = \pm\, p_1^{m_1} \cdots p_r^{m_r} \ \text{ con } \ m_1, \ldots, m_r \in \mathbb{N}_0,$$
$$b = \pm\, p_1^{n_1} \cdots p_r^{n_r} \ \text{ con } \ n_1, \ldots, n_r \in \mathbb{N}_0.$$

Entonces

- $a \cdot b = \left(\pm\, p_1^{m_1} \cdots p_r^{m_r} \right) \cdot \left(\pm\, p_1^{n_1} \cdots p_r^{n_r} \right) = \pm\, p_1^{m_1+n_1} \cdots p_r^{m_r+n_r}$.

  Es decir $a \cdot b$ tiene exactamente los primos de a y de b en su factorización y los exponentes se suman.

- $a^n = \left(\pm\, p_1^{m_1} \cdots p_r^{m_r} \right)^n = (\pm 1)^n\, p_1^{m_1 n} \cdots p_r^{m_r n}$ es la factorización en primos de a^n, para todo $n \in \mathbb{N}$.

  Es decir a^n tiene exactamente los mismos primos que a en su factorización, y los exponentes van multiplicados por n.

<u>*Nota:*</u> Otro hecho que se desprende de este (y que de hecho aparece en la demostración de la unicidad de la factorización) es que $p \mid a$ si y solo si p aparece en la factorización en primos de a.

- Sea $d \mid 2^3 \cdot 5^4$. ¿Cómo puede ser d?

  Está claro que si $k \cdot d = 2^3 \cdot 5^4$, entonces en k y en d no pueden aparecer más que los primos 2 y 5 (por la unicidad de la factorización). Además si $d = 2^i \cdot 5^j$ con $0 \leq i, j$ para que $d \in \mathbb{Z}$, y $k = 2^{i'} \cdot 5^{j'}$ con $0 \leq i', j'$ para que $k \in \mathbb{Z}$, tiene que satisfacerse

$$2^3 \cdot 5^4 = k \cdot d = 2^{i'} \cdot 5^{j'} \cdot 2^i \cdot 5^j = 2^{i'+i} \cdot 5^{j'+j}.$$

  Así, $i' + i = 3$ y $j' + j = 4$. Esto implica, dado que $i' \geq 0$ y $j' \geq 0$, que $0 \leq i \leq 3$ y $0 \leq j \leq 4$.
  Así, si $d \mid 2^3 \cdot 5^4$, la factorización en primos de d es

$$d = 2^i \cdot 5^j, \quad \text{con } \ 0 \leq i \leq 3,\ 0 \leq j \leq 4.$$

  Luego $\mathrm{Div}(2^3 5^4) = \{\, \pm 2^i 5^j,\ 0 \leq i \leq 3, 0 \leq j \leq 4 \,\}$.

  Por lo tanto, $2^3 5^4$ tiene $(3+1)(4+1) = 20$ divisores positivos distintos, y $2 \cdot 20 = 40$ divisores enteros, positivos y negativos.

Proposición 4.6.7. (Divisores de un número y cantidad.)

Sea $a \in \mathbb{Z}$, $a \neq 0, \pm 1$, *y sea* $a = \pm p_1^{m_1} \cdots p_r^{m_r}$ *la factorización en primos de* a. *Entonces*

1. $d \mid a \iff d = \pm p_1^{n_1} \cdots p_r^{n_r}$ *con* $0 \leq n_1 \leq m_1, \ldots, 0 \leq n_r \leq m_r$.
2. $\#\mathrm{Div}_+(a) = (m_1+1)\cdots(m_r+1)$ *y* $\#\mathrm{Div}(a) = 2(m_1+1)\cdots(m_r+1)$.

- ¿Cuál es el menor número natural n con 12 divisores positivos?

  $a = 1$ tiene únicamente 1 divisor positivo. O sea $a \geq 2$. Sea $a = p_1^{m_1} \cdots p_r^{m_r}$ con $m_1, \ldots, m_r \in \mathbb{N}$ la factorización en primos de a. Sabemos que entonces la cantidad de divisores positivos de a es $(m_1+1)\cdots(m_r+1)$. Observemos que como $m_i \geq 1$, entonces $m_i + 1 \geq 2$, $\forall\, i$. Luego, la condición $12 = (m_1+1)\cdots(m_r+1)$ implica $12 \geq 2^r$, o sea $r \leq 3$: a tiene a lo sumo 3 primos distintos. Por lo tanto a es de una de las siguientes formas:

  $$a = p^m \quad \text{o} \quad a = p_1^{m_1} \cdot p_2^{m_2} \quad \text{o} \quad a = p_1^{m_1} \cdot p_2^{m_2} \cdot p_3^{m_3}.$$

  - Caso $a = p^m$: En ese caso a tiene $m+1$ divisores positivos. Si se quiere que sean 12, entonces $m+1 = 12$ implica $m = 11$: $a = p^{11}$, y el más chico de ellos es claramente $a = 2^{11} = 2048$.
  - Caso $a = p_1^{m_1} \cdot p_2^{m_2}$: En ese caso a tiene $(m_1+1)(m_2+1)$ divisores positivos. Si se quiere que sean 12, entonces $(m_1+1)(m_2+1) = 12 = 6 \cdot 2 = 4 \cdot 3$ implica $m_1+1 = 6, m_2+1 = 2$ o $m_1+1 = 4, m_2+1 = 3$ (o cambiando el rol de m_1 y m_2). Así se obtiene $m_1 = 5, m_2 = 1$ o $m_1 = 3, m_2 = 2$. Luego $a = p_1^5 \cdot p_2$ o $a = p_1^3 \cdot p_2^2$. Claramente los más chicos de éstos son $a = 2^5 \cdot 3 = 96$ y $a = 2^3 \cdot 3^2 = 72$.
  - Caso $a = p_1^{m_1} \cdot p_2^{m_2} \cdot p_3^{m_3}$: En ese caso a tiene $(m_1+1)(m_2+1)(m_3+1)$ divisores positivos. Si se quiere que sean 12, entonces $(m_1+1)(m_2+1)(m_3+1) = 12 = 3 \cdot 2 \cdot 2$ implica $m_1+1 = 3, m_2+1 = 2$ y $m_3+1 = 2$ (o cambiando el rol de m_1, m_2 y m_3). Así se obtiene $m_1 = 2, m_2 = 1, m_3 = 1$. Luego $a = p_1^2 \cdot p_2 \cdot p_3$. Claramente el más chico de éstos es $a = 2^2 \cdot 3 \cdot 5 = 60$.

- Calcular la suma de los divisores positivos de 10^{10}: Se tiene

  $$\mathrm{Div}_+(10^{10}) = \mathrm{Div}_+(2^{10} \cdot 5^{10}) = \{2^i 5^j,\ 0 \leq i \leq 10, 0 \leq j \leq 10\}.$$

  Por lo tanto

  $$\sum_{d>0, d \mid 10^{10}} d = \sum_{0 \leq i,j \leq 10} 2^i 5^j = \sum_{i=0}^{10} (\sum_{j=0}^{10} 2^i 5^j) = \sum_{i=0}^{10} (2^i \sum_{j=0}^{10} 5^j)$$
  $$= (\sum_{j=0}^{10} 5^j)(\sum_{i=0}^{10} 2^i) = \frac{5^{11}-1}{5-1} \cdot \frac{2^{11}-1}{2-1} = (2^{11}-1)\frac{5^{11}-1}{4}.$$

Proposición 4.6.9. (Máximo común divisor y factorización.)

Sean $a, b \in \mathbb{Z}$ *no nulos de la forma*

$$a = \pm p_1^{m_1} \cdots p_r^{m_r} \quad con \quad m_1, \ldots, m_r \in \mathbb{N}_0,$$
$$b = \pm p_1^{n_1} \cdots p_r^{n_r} \quad con \quad n_1, \ldots, n_r \in \mathbb{N}_0.$$

Entonces

$$(a : b) = p_1^{\min\{m_1, n_1\}} \cdots p_r^{\min\{m_r, n_r\}}.$$

Corolario 4.6.10. (Mcd de potencias.)

Sean $a, b \in \mathbb{Z}$ *no nulos.*

1. *Sean* $a, b \neq 0, \pm 1$ *con factorización en primos* $a = \pm p_1^{m_1} \cdots p_r^{m_r}$, $m_1, \ldots, m_r \in \mathbb{N}$, *y* $b = \pm q_1^{n_1} \cdots q_s^{n_s}$, $n_1, \ldots, n_s \in \mathbb{N}$. *Entonces*

$$(a : b) = 1 \iff p_i \neq q_j, \ \forall\, i, j.$$

2. $(a : b) = 1$ *y* $(a : c) = 1 \iff (a : bc) = 1$.

3. $(a : b) = 1 \iff (a^m : b^n) = 1, \ \forall\, m, n \in \mathbb{N}$.

4. $(a^n : b^n) = (a : b)^n, \ \forall\, n \in \mathbb{N}$.

   ¡Ojo que para esta 4ta propiedad tiene que ser la misma potencia n*!*

<u>*Ejemplos:*</u>

- Calcular $(2^n + 3^n : 2^n - 2 \cdot 3^n)$, para todo $n \in \mathbb{N}$.

  Sea d un posible divisor común:

$$\left\{ \begin{array}{l} d \mid 2^n + 3^n \\ d \mid 2^n - 2 \cdot 3^n \end{array} \right. \implies d \mid 3^n + 2 \cdot 3^n \implies d \mid 3 \cdot 3^n.$$

  De la misma manera:

$$\left\{ \begin{array}{l} d \mid 2^n + 3^n \\ d \mid 2^n - 2 \cdot 3^n \end{array} \right. \implies \left\{ \begin{array}{l} d \mid 2 \cdot 2^n + 2 \cdot 3^n \\ d \mid 2^n - 2 \cdot 3^n \end{array} \right. \implies d \mid 2 \cdot 2^n + 2^n \implies d \mid 3 \cdot 2^n.$$

  Pero

$$d \mid 3 \cdot 3^n \text{ y } d \mid 3 \cdot 2^n \implies d \mid (3 \cdot 3^n : 3 \cdot 2^n) = 3\,(3^n : 2^n) = 3 \cdot 1 = 3.$$

  Por lo tanto, $(2^n + 3^n : 2^n - 2 \cdot 3^n) = 1$ o 3.

  Pero se ve claramente que 3 no puede ser un divisor común ya que $3 \nmid 2^n + 3^n$ (pues si lo dividiera, se tendría que $3 \mid 2^n$, absurdo!). Por lo tanto el 3 queda descartado como posible mcd, y se concluye que $(2^n + 3^n : 2^n - 2 \cdot 3^n) = 1$, $\forall\, n \in \mathbb{N}$.

- Sean $a, b \in \mathbb{Z}$ no ambos nulos tales que $(a : b) = 6$.
  Calcular $(a\,b : 6\,a - 6\,b)$.

  "Coprimizando", se tiene $a = 6\,a'$, $b = 6\,b'$ con $a' \perp b'$, luego

$$\begin{aligned}(a\,b : 6\,a - 6\,b) &= (36\,a'b' : 36a' - 36b') = (36\,a'b' : 36(a' - b')) \\ &= 36(a'b' : a' - b').\end{aligned}$$

  Para concluir falta calcular los posibles valores de $(a'b' : a' - b')$ cuando $a' \perp b'$:

  Sea d un divisor común:

$$\left\{\begin{array}{l} d \mid a'b' \\ d \mid a' - b' \end{array}\right. \implies \left\{\begin{array}{l} d \mid a'b' \\ d \mid a'(a' - b') \end{array}\right. \implies \left\{\begin{array}{l} d \mid a'b' \\ d \mid a'^2 - a'b' \end{array}\right. \implies d \mid a'^2$$

  De la misma manera:

$$\left\{\begin{array}{l} d \mid a'b' \\ d \mid a' - b' \end{array}\right. \implies \left\{\begin{array}{l} d \mid a'b' \\ d \mid b'(a' - b') \end{array}\right. \implies \left\{\begin{array}{l} d \mid a'b' \\ d \mid a'b' - b'^2 \end{array}\right. \implies d \mid b'^2$$

  Obtuvimos $d \mid a'^2$ y $d \mid b'^2$. Luego $d \mid (a'^2 : b'^2)$. Pero, como vimos arriba, $a' \perp b' \Rightarrow a'^2 \perp b'^2$, es decir $(a'^2 : b'^2) = 1$. O sea $d \mid 1$. Así se prueba que los únicos divisores comunes de $a'b'$ y $a' - b'$ son ± 1, luego $a'b' \perp a' - b'$, y se concluye

$$(a\,b : 6\,a - 6\,b) = 36(a'b' : a' - b') = 36.$$

4.6.3 Mínimo común múltiplo.

Definición 4.6.11. (Mínimo común múltiplo.)

Sean $a, b \in \mathbb{Z}$, no nulos. El *mínimo común múltiplo* entre a y b, que se nota $[a : b]$, es el menor número natural que es un múltiplo común de a y b.

Ejemplo: Como todos ya "saben", para $a = 588 = 2^2 \cdot 3 \cdot 7^2$ y $b = 188650 = 2 \cdot 5^2 \cdot 7^3 \cdot 11$, el mínimo común múltiplo $[a : b]$ es el producto de todos los primos que aparecen en a y en b a la máxima potencia a la que aparecen, o sea $[a : b] = 2^2 \cdot 3 \cdot 5^2 \cdot 7^3 \cdot 11$. Probemos este hecho en general.

Proposición 4.6.12. (Mínimo común múltiplo y factorización.)

Sean $a, b \in \mathbb{Z}$ no nulos de la forma

$$\begin{aligned} a &= \pm\, p_1^{m_1} \cdots p_r^{m_r} \quad \textit{con} \quad m_1, \ldots, m_r \in \mathbb{N}_0, \\ b &= \pm\, p_1^{n_1} \cdots p_r^{n_r} \quad \textit{con} \quad n_1, \ldots, n_r \in \mathbb{N}_0. \end{aligned}$$

Entonces

$$[a : b] = p_1^{\max\{m_1, n_1\}} \cdots p_r^{\max\{m_r, n_r\}}.$$

Corolario 4.6.13. (Mcm y múltiplos comunes.)

Sean $a, b \in \mathbb{Z}$, *no ambos nulos y sea* $m \in \mathbb{Z}$, *con* $m \neq 0$. *Entonces*

$$a \mid m \;\; y \;\; b \mid m \iff [a : b] \mid m.$$

Ejemplo: Observemos que para $a = 2^2 \cdot 3^1 \cdot 7^2$ y $b = 2^1 \cdot 5^2 \cdot 7^3 \cdot 11^1$, teníamos $(a : b) = 2^1 \cdot 7^2$ y $[a : b] = 2^2 \cdot 3^1 \cdot 5^2 \cdot 7^3 \cdot 11^1$. Luego

$$\begin{aligned}(a : b) \cdot [a : b] &= (2^1 \cdot 7^2) \cdot (2^2 \cdot 3^1 \cdot 5^2 \cdot 7^3 \cdot 11^1) \\ &= 2^{1+2} \cdot 3^{0+1} \cdot 5^{0+2} \cdot 7^{2+3} \cdot 11^{0+1} \\ &= 2^{2+1} \cdot 3^{1+0} \cdot 5^{0+2} \cdot 7^{2+3} \cdot 11^{0+1} \\ &= (2^2 \cdot 3^1 \cdot 7^2) \cdot (2^1 \cdot 5^2 \cdot 7^3 \cdot 11^1) \;=\; a \cdot b.\end{aligned}$$

Es inmediato probar que este resultado vale en general.

Proposición 4.6.14. (Producto mcd y mcm.)

Sean $a, b \in \mathbb{Z}$, *no nulos, entonces* $|a \cdot b| = (a : b) \cdot [a : b]$.

En particular, si $a \perp b$, *entonces* $[a : b] = |a \cdot b|$.

Esto da una alternativa para calcular el mínimo común múltiplo cuando uno no conoce la factorización de los números. De hecho esta forma de calcular el mínimo común múltiplo es para números grandes más veloz que factorizar los números para luego aplicar la Proposición 4.6.14, ya que calcular el máximo común divisor por el algoritmo de Euclides es para números grandes más veloz que factorizar.

Ejemplo: Determinar todos los pares de números $a, b \in \mathbb{N}$ que satisfacen que

$$(a : b) = 2^2 \cdot 3 \cdot 17 \quad \text{y} \quad [a : b] = 2^5 \cdot 3 \cdot 5^2 \cdot 17^2.$$

¡Nunca olvidar que "coprimizar" en general ayuda!

Sabemos que $a = (a : b)\, a'$ y $b = (a : b)\, b'$ con $a' \perp b'$. Luego

$$(a : b)[a : b] = a\, b = (a : b)^2 a'\, b'.$$

Es decir

$$a'b' = \frac{[a : b]}{(a : b)} = \frac{2^5 \cdot 3 \cdot 5^2 \cdot 17^2}{2^2 \cdot 3 \cdot 17} = 2^3 \cdot 5^2 \cdot 17, \text{ con } a' \perp b'.$$

Al ser $a' \perp b'$ no puede aparecer un mismo primo simultáneamente en a' y b', y por lo tanto las posibilidades son (eligiendo cuáles son los primos que aparecen en a' y luego los restantes estarán en b'):

$$\begin{array}{ll} a' = 1,\; b' = 2^3 \cdot 5^2 \cdot 17 & a' = 2^3,\; b' = 5^2 \cdot 17 \\ a' = 5^2,\; b' = 2^3 \cdot 17 & a' = 17,\; b' = 2^3 \cdot 5^2 \\ a' = 2^3 \cdot 5^2,\; b' = 17 & a' = 2^3 \cdot 17,\; b' = 5^2 \\ a' = 5^2 \cdot 17,\; b' = 2^3 & a' = 2^3 \cdot 5^2 \cdot 17,\; b' = 1. \end{array}$$

Multiplicando estos números por $(a : b) = 2^2 \cdot 3 \cdot 17$ se obtienen todos los pares (a, b).