

Fundamentos Matemáticos

<https://github.com/AdriCri22/Fundamentos-Matematicos-FM-FIB>

1. Lógica y demostraciones

Lógica proposicional

Las fórmulas de lógica proposicional se constituyen con los siguientes símbolos:

- Letras proposicionales: $p, q, r, s \dots$ (átomos o fórmulas atómicas)
- Conectivas lógicas:
 - Binarias:

\wedge	\vee	\rightarrow	\leftrightarrow
y	o	Si ..., entonces ...	Si y solo si ..., entonces ...

- Unarias:
 - \neg (no)

Significado de las conectivas (Tablas de la verdad):

Asignación		φ	$\neg\varphi$
		0	1
		1	0

φ	ψ	$\varphi \wedge \psi$	$\varphi \vee \psi$	$\varphi \rightarrow \psi$	$\varphi \leftrightarrow \psi$
0	0	0	0	1	1
0	1	0	1	1	0
1	0	0	1	0	0
1	1	1	1	1	1

Tipos de fórmulas importantes:

- Tautología: fórmula siempre cierta (La tabla de la verdad siempre da 1)
- Insatisficible / Contradicción: fórmula siempre falsa (La tabla de la verdad siempre da 0)
- Satisfacible: fórmula que es cierta para alguna asignación (La tabla de la verdad contiene algún 1)

Equivalencia de fórmulas

La siguiente tabla muestra propiedades básicas a partir de las que podemos ir de una fórmula a otra para poder demostrar que dos fórmulas son equivalentes.

Distributiva	$\varphi \wedge (\psi \vee \theta) \equiv (\varphi \wedge \psi) \vee (\varphi \wedge \theta)$	$\varphi \vee (\psi \wedge \theta) \equiv (\varphi \vee \psi) \wedge (\varphi \vee \theta)$
De Morgan	$\neg(\varphi \wedge \psi) \equiv \neg\varphi \vee \neg\psi$	$\neg(\varphi \vee \psi) \equiv \neg\varphi \wedge \neg\psi$
Absorción	$\varphi \wedge (\varphi \vee \psi) \equiv \varphi$	$\varphi \vee (\varphi \wedge \psi) \equiv \varphi$
Idempotencia	$\varphi \wedge \varphi \equiv \varphi$	$\varphi \vee \varphi \equiv \varphi$
Conmutativa	$\varphi \wedge \psi \equiv \psi \wedge \varphi$	$\varphi \vee \psi \equiv \psi \vee \varphi$

Asociativa	$\varphi \wedge (\psi \wedge \theta) \equiv (\varphi \wedge \psi) \wedge \theta$	$\varphi \vee (\psi \vee \theta) \equiv (\varphi \vee \psi) \vee \theta$
Neutra	$\varphi \wedge 1 \equiv \varphi$	$\varphi \vee 0 \equiv \varphi$
	$\varphi \vee 1 \equiv 1$	$\varphi \wedge 0 \equiv 0$
Complementaria	$\varphi \vee \neg\varphi \equiv 1$	$\varphi \wedge \neg\varphi \equiv 0$
Doble negación	$\neg\neg\varphi \equiv \varphi$	
	$\neg 1 \equiv 0$	$\neg 0 \equiv 1$
Traducción de la \rightarrow	$\varphi \rightarrow \psi \equiv \neg\varphi \vee \psi$	$\neg(\varphi \rightarrow \psi) \equiv \varphi \wedge \neg\psi$
Traducción de la \leftrightarrow	$\varphi \leftrightarrow \psi \equiv (\varphi \rightarrow \psi) \wedge (\psi \rightarrow \varphi)$ $\varphi \leftrightarrow \psi \equiv (\varphi \wedge \psi) \vee (\neg\varphi \wedge \neg\psi)$	$\neg(\varphi \leftrightarrow \psi) \equiv (\varphi \wedge \neg\psi) \vee (\neg\varphi \wedge \psi)$

Lógica de predicados

Para tener una relación hay que disponer de un “dominio de individuos” y una propiedad de estos individuos, cada individuo del dominio tiene o no una propiedad. El número de individuos se representa mediante el término aridad, es decir, una relación de aridad 1, significa que esta relación es una propiedad que depende de 1 individuo.

Una relación de aridad 2 tiene dos argumentos:

- Es una propiedad que depende de dos individuos.
- La propiedad es del conjunto o relaciona a los individuos entre ellos.
- Cada pareja de individuos tiene o no tiene la propiedad.

Ejemplos (Dominio \mathbb{Z}):

- Las relaciones: “ser par”, “ser un cuadrado”, “ser múltiple de 4” son relaciones de aridad 1.
- Las relaciones: “ser menor que ($x < y$)”, “ser igual que ($x = y$)”, “ser congruente módulo 5 ($x \equiv y \pmod{5}$)” son relaciones de aridad 2.
- Las relaciones: “ x está entre y y z ”, “ x es congruente con y módulo z ” son relaciones de aridad 3.

Para representar una relación de aridad n se usa la siguiente fórmula atómica: $R(x_1, x_2, \dots, x_n)$, en casos de relaciones binarias (aridad 2) se puede escribir xRy en vez de $R(x, y)$

Cuantificadores:

- $\forall x\varphi \equiv$ Todos los individuos x del dominio cumplen φ .
- $\exists x\varphi \equiv$ Existe algún (al menos un) individuo x del dominio que cumpla φ .

Equivalencia

$\neg\forall x\varphi \equiv \exists x\neg\varphi$	$\neg\exists x\varphi \equiv \forall x\neg\varphi$
$\forall x\forall y\varphi \equiv \forall y\forall x\varphi$	$\exists x\exists y\varphi \equiv \exists y\exists x\varphi$
$\forall x(\varphi \wedge \psi) \equiv \forall x\varphi \wedge \forall x\psi$	$\exists x(\varphi \vee \psi) \equiv \exists x\varphi \vee \exists x\psi$

La equivalencia $\forall x\exists y\varphi$ y $\exists y\forall x\varphi$ no es cierta. Por ejemplo, si el dominio son los nombres naturales $\forall x\exists y(x < y)$ es cierta, en cambio $\exists y\forall x(x < y)$ es falsa.

Tampoco son ciertas las equivalencias $\forall x(\varphi \vee \psi) \equiv \forall x\varphi \vee \forall x\psi$ ni $\exists x(\varphi \wedge \psi) \equiv \exists x\varphi \wedge \exists x\psi$. Por ejemplo: $x \in \mathbb{N}$, $P(x)$ es “ x es par”, $I(x)$ es “ x es impar”, $\forall x(P(x) \vee I(x))$ es cierta, en cambio $\forall xP(x) \vee \forall xI(x)$ es falsa.

Formalización

Consiste en expresar en un lenguaje “formal” un enunciado. Consistirá en encontrar una fórmula de la lógica de predicados. Al formalizar con cuantificadores se presuponen:

- Un dominio (o universo) de individuos.
- Unas relaciones entre individuos.

Hay dos patrones que aparecen de manera habitual:

1. $\forall x(A(x) \rightarrow B(x))$ Todos los individuos de tipo A (que tienen la propiedad A) tienen la propiedad B.
2. $\exists x(A(x) \wedge B(x))$ Hay individuos de tipo A que tienen la propiedad B.

Nota: para expresar que x cumple las propiedades A y B no se puede expresar de esta manera $A(B(x))$, la forma correcta es $A(x) \wedge B(x)$.

Veracidad y cuantificadores

Para justificar que un enunciado es cierto dependerá de su “forma”.

- Demostración de un existencial $\exists xP(x)$
Basta con dar un elemento a del dominio que cumple la propiedad P , es decir, basta con dar un ejemplo que sea cierto
- Demostración de un universal $\forall xP(x)$
Se hace a partir de una “demostración”.

Cuantificadores mezclados

Queremos demostrar	Que hay que hacer
$\exists x \in A \ P(x)$ Cierto	Dar un ejemplo: Dar $a \in A$ tal que $P(a)$
$\forall x \in A \ P(x)$ Falso	Dar un contraejemplo: Dar $a \in A$ tal que $\neg P(a)$
$\exists y \in A \ \forall x \in A \ P(x, y)$ Cierto	Dar $a \in A$ tal que $\forall x \in A \ P(x, a)$ ¹
$\forall x \in A \ \exists y \in A \ P(x, y)$ Cierto	Por cada $x \in A$ dar $y = E(x)$ tal que $\forall x \in A \ P(x, E(x))$ ²

1. La y no puede depender de la x : es constante
2. La y acostumbra a depender de x , aunque en alguna ocasión puede ser constante

Demostraciones

En el lenguaje semiformal (fura de las fórmulas) se usan: *i*, *o*, *no*, \Rightarrow , \Leftrightarrow , en vez de: \wedge , \vee , \neg , \rightarrow , \leftrightarrow .

$A \Rightarrow B \equiv A$ implica $B \equiv$ si A entonces $B \equiv A$ es la **hipótesis** y B la **Tesis**

Ejemplo: Queremos demostrar que: “por todo entero n , si n es impar entonces $n^2 + 4n - 1$ es par”.

1. Escribimos el enunciado de esta forma (que n es un entero se sobreentiende):

$$n \text{ impar} \Rightarrow n^2 + 4n - 1 \text{ par}$$

2. Lo formalizamos:

$$\forall x(I(x) \rightarrow P(x^2 + 4x - 1))$$

Dónde $I(x)$ formaliza “ x es impar”, $P(x)$ formaliza “ x es par” i el dominio son los enteros

Pasos lógicos (sirven para que en cualquier momento de una demostración puedan ser usados):

Pasos lógicos			Tautologías
A, B	\Rightarrow	A	$(p \wedge q) \rightarrow p$
A	\Rightarrow	$A \text{ o } B$	$p \rightarrow (p \vee q)$
$A \text{ o } B, \text{ no } A$	\Rightarrow	B	$((p \vee q) \wedge \neg p) \rightarrow q$
$A, A \Rightarrow B$	\Rightarrow	B	$(p \wedge (p \rightarrow q)) \rightarrow q$
$\text{no } B, A \Rightarrow B$	\Rightarrow	$\text{no } A$	$(\neg q \wedge (p \rightarrow q)) \rightarrow \neg p$
<i>ABSURDO</i>	\Rightarrow	A	$0 \rightarrow p$
$A \Rightarrow B, B \Rightarrow C$	\Rightarrow	$A \Rightarrow C$	$((p \rightarrow q) \wedge (q \rightarrow r)) \rightarrow (p \rightarrow r)$

Nota: la coma se usa como si fuera \wedge (una conjunción)

Pasos básicos de la igualdad (a, b, c, \dots son números reales)

- $a = a$ (reflexiva)
- $a = b \Rightarrow b = a$ (simétrica)
- $a = b, b = c \Rightarrow a = c$ (transitiva)
- $a = b \Rightarrow E(a) = E(b)$ ($E(x)$ es una expresión dónde aparece x)
- $a = b \Rightarrow a + c = b + c$
- $a = b \Rightarrow ac = bc$
- $a = b \Rightarrow a^2 = b^2$
- $a = b, a' = b' \Rightarrow a + a' = b + b'$
- $a = b, a' = b' \Rightarrow aa' = bb'$

Propiedades básicas de la suma y el producto (a, b, c, \dots son números reales)

- $a + (b + c) = (a + b) + c$ (Asociativa de la suma)
- $a + b = b + a$ (Conmutativa de la suma)
- $a + 0 = a$ (0 es el neutro de la suma)
- $a + (-a) = 0$ ($-a$ es el inverso de a de la suma)
- $a(bc) = (ab)c$ (Asociativa del producto)
- $ab = ba$ (Conmutativa del producto)
- $a \times 1 = a$ (1 es el neutro del producto)
- $a \neq 0 \Rightarrow a \times (1/a) = 1$ ($1/a$ es el inverso de a del producto)
- $a(b + c) = ab + ac$ (distributiva)

Pasos básicos del orden (a, b, c, \dots son números reales)

- $a \leq a$
- $a \leq b, b \leq a \Rightarrow a = b$
- $a \leq b, b \leq c \Rightarrow a \leq c$
- $a \leq b \text{ o } b \leq a$
- $a \leq b \Rightarrow a + c \leq b + c$
- $a \leq b, c \geq 0 \Rightarrow ac \leq bc$
- $a \leq b, c \leq d \Rightarrow a + c \leq b + d$
- $a \leq b \Rightarrow -b \leq -a$
- $a^2 \geq 0$
- $0 \leq a \leq b \Rightarrow a^2 \leq b^2$
- $a \leq b \Rightarrow a^2 \leq b^2$
- $a \leq b \Rightarrow a^3 \leq b^3$
- $(n \text{ natural par}) \quad 0 \leq a \leq b \Rightarrow a^n \leq b^n$

Otros

1. a natural, b natural $\Rightarrow a + b$ natural, ab natural
2. a entero, b entero $\Rightarrow -a$ entero, $a + b$ entero, ab entero
3. a racional, b racional $\Rightarrow -a$ racional, $a + b$ racional, ab racional
4. b racional, $b \neq 0$ $\Rightarrow 1/b$ racional
5. a racional, b racional, $b \neq 0$ $\Rightarrow a/b$ racional

Nota: Podemos definir natural de la siguiente manera: 0 es natural i si a es natural, $a + 1$ es natural. No hay más naturales que los que se constituyen aplicando un nombre finito de veces estas reglas.

Prueba directa

Salimos de la hipótesis A i llegamos a la tesis B . Esto se hace mediante pequeñas implicaciones que han de ser muy claras, estas implicaciones pueden ser, por ejemplo, los pasos anteriores.

Queremos demostrar $A \Rightarrow B$
$A \Rightarrow A' \Rightarrow A'' \Rightarrow \dots \Rightarrow B$

Prueba del contrarrecíproco

Se basa en: $p \rightarrow q \equiv \neg q \rightarrow \neg p$

Queremos demostrar $A \Rightarrow B$
$\neg B \Rightarrow \dots \Rightarrow \neg A$

Reducción al absurdo

Se basa en: $p \equiv \neg p \rightarrow 0$

Queremos demostrar A
$\neg A \Rightarrow \dots \Rightarrow \text{Contradicción}$

Reducción al absurdo II

Se basa en: $p \rightarrow q \equiv (p \wedge \neg q) \rightarrow 0$

Queremos demostrar $A \Rightarrow B$
$A, \neg B \Rightarrow \dots \Rightarrow \text{Contradicción}$

Prueba de una disyunción

Se basa en: $(q \vee r) \equiv (\neg q \rightarrow r)$

Queremos demostrar $B \vee C$
$\neg B \Rightarrow \dots \Rightarrow C$

En caso de más disyuntandos: $p_1 \vee \dots \vee p_n \equiv (\neg p_1 \vee \dots \vee \neg p_{n-1}) \rightarrow p_n$

Queremos demostrar $B_1 \vee \dots \vee B_n$
$\neg B_1, \neg B_2, \dots, \neg B_{n-1} \Rightarrow \dots \Rightarrow B_n$

Disyunción al consecuente

Se basa en: $p \rightarrow (q \vee r) \equiv (p \wedge \neg q \rightarrow r)$

Queremos demostrar $A \Rightarrow (B \vee C)$
$A, \neg B \Rightarrow \dots \Rightarrow C$

Con más disyuntandos: $p \rightarrow (q_1 \vee \dots \vee q_n) \equiv (p \wedge \neg q_1 \wedge \dots \wedge \neg q_{n-1}) \rightarrow q_n$

Queremos demostrar $A \Rightarrow (B_1 \vee \dots \vee B_n)$
$A, \neg B_1, \neg B_2, \dots, \neg B_{n-1} \Rightarrow \dots \Rightarrow B_n$

Prueba por casos

Se basa en la tautología: $(p_1 \vee \dots \vee p_n) \rightarrow (p \leftrightarrow (p_1 \rightarrow p) \wedge \dots \wedge (p_n \rightarrow p))$

Queremos demostrar B , distinguimos los casos A_1, \dots, A_n
<p><u>Caso 1:</u> A_1</p> <p style="text-align: right;">$A_1 \Rightarrow \dots \Rightarrow B$</p> <p>...</p> <p><u>Caso n:</u> A_n</p> <p style="text-align: right;">$A_n \Rightarrow \dots \Rightarrow B$</p>

Nota: hay que hacerlo con todos los casos

Disyunción al antecedente

Se basa en: $(q \vee r) \rightarrow p \equiv (q \rightarrow p) \wedge (r \rightarrow p)$

Es equivalente a hacer una prueba por casos (distinguimos según B o C).

Queremos demostrar $(B \vee C) \Rightarrow A$
<p style="text-align: right;">$B \Rightarrow \dots \Rightarrow A$</p> <p style="text-align: right;">$C \Rightarrow \dots \Rightarrow A$</p>

Cuando hay más casos:

Queremos demostrar $(B_1 \vee \dots \vee B_n) \Rightarrow A$
<p style="text-align: right;">$B_1 \Rightarrow \dots \Rightarrow A$</p> <p style="text-align: right;">...</p> <p style="text-align: right;">$B_n \Rightarrow \dots \Rightarrow A$</p>

Demostración de una equivalencia

Se basa en: $p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$

Queremos demostrar $A \leftrightarrow B$
<p style="text-align: right;">$A \Rightarrow B$</p> <p style="text-align: right;">$B \Rightarrow A$</p>

Cuando hay más casos:

Queremos demostrar que A_1, A_2, \dots, A_n son equivalentes (dos a dos)
$A_1 \Rightarrow A_2$ $A_2 \Rightarrow A_3$ \dots $A_{n-1} \Rightarrow A_n$ $A_n \Rightarrow A_1$

Nota: Se puede cambiar el orden de los enunciados A_1, A_2, \dots, A_n

Demostración por unicidad

Cuando decimos que “hay como mucho una x que satisface $P(x)$ ” o bien “si hay una x que satisface $P(x)$ este es único”, estamos expresando: $\forall x, y (P(x) \wedge P(y) \rightarrow x = y)$

Queremos ver que hay como mucho una x tal que $P(x)$.
$P(x), P(y) \Rightarrow \dots \Rightarrow x = y$

Nota: No afirmamos que el elemento x exista, sólo que no hay dos diferentes o, mejor dicho, que hay como mucho uno (puede ser que no haya ninguno).

Nota: Cuando queramos ver que “hay una única x tal que $P(x)$ ” habrá que ver dos cosas: que existe el elemento x y que es único.

2. Inducción

Inducción simple

Se usa cuando la variable n depende de una infinidad de enteros (una sucesión de números).

Se basa en: $\forall n \geq n_0 \ P(n) \equiv P(n_0) \wedge \forall n > n_0 (P(n-1) \rightarrow P(n))$

Queremos demostrar $\forall n \geq n_0 \ P(n)$
$P(n_0)$ $\forall n > n_0 (P(n-1) \rightarrow P(n))$

Se presenta así:

- Paso base $P(n_0)$ | Si es necesario más de un caso inicial: $P(n_0), \dots, P(n_i)$
- Paso inductivo Sea $n > n_0$:
 - Hipótesis de inducción: $P(n-1)$

Queremos ver (tesis): $P(n)$ Procedemos:

Ejemplo: $\sum_{i=1}^n \frac{1}{i(i+1)} = \frac{n}{n+1}$ para $n \geq 1$

Queremos demostrar: $\forall n \geq 1 \sum_{i=1}^n \frac{1}{i(i+1)} = \frac{n}{n+1}$

- Paso base: $n = 1$

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

- Paso inductivo $n > 1$:
 - H.I. sustituimos n por $n-1$ $\frac{n-1}{(n-1)+1} = \frac{n-1}{n}$

Queremos ver: $\sum_{i=1}^n \frac{1}{i(i+1)} = \frac{n}{n+1}$

Procedemos:

Identidad notable: $(a+b)(a-b) = a^2 - b^2$

$$\begin{aligned} \sum_{i=1}^n \frac{1}{i(i+1)} &= \sum_{i=1}^{n-1} \frac{1}{i(i+1)} + \frac{1}{n(n+1)} = \frac{n-1}{n} + \frac{1}{n(n+1)} = \frac{(n-1)(n+1) + 1}{n(n+1)} = \frac{n^2 - 1^2 + 1}{n(n+1)} = \\ &= \frac{n^2}{n(n+1)} = \frac{n}{n+1} \end{aligned}$$

Inducción completa

Se usa cuando queremos demostrar un rango de valores

Se basa en: $\forall n \geq n_0 \ P(n) \equiv P(n_0) \wedge \forall n > n_0 (P(n_0) \wedge \dots \wedge P(n-1) \rightarrow P(n))$

Queremos demostrar $\forall n \geq n_0 \ P(n)$
$P(n_0)$ $\forall n > n_0 (P(n_0) \wedge \dots \wedge P(n-1) \rightarrow P(n))$

Se presenta así:

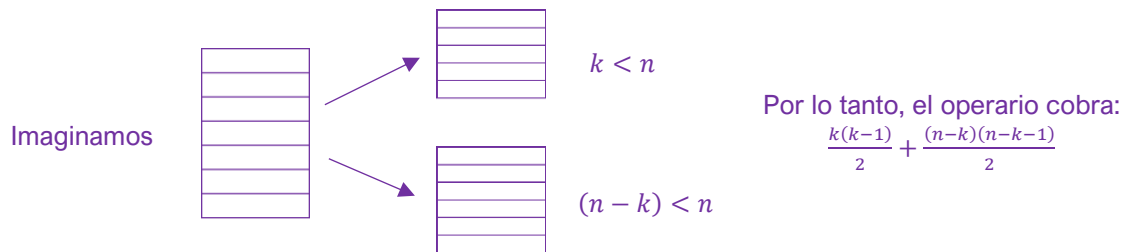
- Paso base: $P(n_0)$ | Si es necesario más de un caso inicial: $P(n_0), P(n_0 + 1), \dots, P(n_i)$
- Paso inductivo: para $n > n_0$:
 - H.I. $P(n_0), P(n_0 + 1), \dots, P(n - 1)$
 - Queremos ver: $P(n)$

Ejemplo: El problema de las pilas. Tenemos una pila de n cajas y queremos convertir en n pilas de 1 caja. Esto lo haremos subdividiendo cada pila de k cajas en dos pilas r y s caja, donde $r + s = k$, $r, s > 0$. Le pediremos al operario que efectúe esta tarea y cada vez que divida una pila de $r + s$ cajas en dos pilas de r y s cajas le pagamos rs euros. Demuestra que al final, independientemente de la estrategia del operario, si al principio hay n cajas, le pagaremos $n(n - 1) / 2$ euros.

- Paso base: $n = 2$ (Ha de haber mínimo 2 cajas para separarlas en 2 pilas)

Si hay 2 cajas, las separamos en 2 pilas de 1 caja ($r = s = 1$), por lo tanto, el operario cobra $rs = 1 * 1 = 1$ euros, es equivalente a $2 * (2 - 1) / 2 = 1$.

- Paso inductivo $n > 2$:



Con n cajas tenemos una 1ª división de $k(n - k)$ cajas que se paga a $k(n - k)$ € y después para $k < n$ y $(n - k) < n$ aplicaremos H.I.

Por lo tanto, basta ver que: $k(n - k) + \frac{k(k-1)}{2} + \frac{(n-k)(n-k-1)}{2} = \frac{n(n-1)}{2} \Leftrightarrow \frac{2k(n-k) + k(k-1) + (n-k)(n-k-1)}{2} = \frac{n^2 - n}{2} \Leftrightarrow 2nk - 2k^2 + k^2 - k + n^2 - nk - n - nk + k^2 + k = n^2 - n \Leftrightarrow n^2 - n = n^2 - n$.

Ejemplo: El juego de las cerillas. Hay dos montones con el mismo número de cerillas y dos jugadores. Cada jugador escoge una pila de cerillas y retira de esta pila mínimo una cerilla. Juegan alternativamente. El juego acaba cuando no quedan cerillas i gana el último que saca alguna cerilla del montón. Demuestra que, si el segundo jugador quita cada vez el mismo número de cerillas del montón que el primer jugador, gana.

- Paso base: $n = 2$

Indiferentemente de si el primer jugador coge 1 o 2 cerillas del montón, el segundo jugador al imitarlo ganará.

- Paso inductivo $n > 2$:

El primer jugador quita k cerillas $k > 0$
El segundo jugador quita k cerillas $k > 0$ } Quedan $n - k < n$ cerillas

Formalizar diferentes definiciones:

- n es par $n = 2k$
- n es impar $n = 2k + 1$
- a divide b $a|b$ o $b = ac$

Definiciones y recordatorios:

- Es primo si los únicos divisores positivos son 1 y p
- $\log_b a = c \Leftrightarrow b^c = a$
- Residuo (r) = dividendo (x) – divisor (y) \times cuociente (q) $\equiv x \bmod y$
- Que un número acabe en cierto dígito, **por ejemplo 9, se representa:** $10k + 9 \quad \forall k \geq 0$
- **Que por ejemplo el residuo de dividir x entre 6 sea 4 se representa:** $n = 6k + 4 \quad k \in \mathbb{Z}$
- Números naturales $\mathbb{N} = \{1, 2, 3, \dots\}$
- Números enteros $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3\}$
- Números racionales $\mathbb{Q} = \left\{\frac{p}{q} \mid p, q \in \mathbb{Z} \wedge q \neq 0\right\}$
- Números irracionales (\mathbb{I}) son números decimales infinitos no periódicos
- Nombres reales $\mathbb{R} = \mathbb{Q} \cup \mathbb{I}$

3. Conjuntos y relaciones

Los conjuntos son como un tipo de “bolsa” que contienen ciertos objetos en el interior, de manera desordenada. Sólo importa que objetos están dentro y cuáles no. También podemos pensar en una especie de lista donde no importa el orden y no pueden haber repeticiones. No podemos “llamar” al primer elemento, sólo podemos pedir si un determinado objeto está o no (esto es un booleano, que se llama “función característica”).

Cuando un objeto x está en el conjunto A diremos que x **pertenece a A** o que **x es un elemento de A** . Lo **denotamos como $x \in A$** .

Cuando un objeto x no está en el conjunto A diremos que x **no pertenece a A** o que **x no es un elemento de A** . Lo **denotamos como $x \notin A$** .

Los elementos pueden ser de cualquier tipo (números, conjuntos, fórmulas, listas, ...).

Existen dos formas de representar un conjunto:

- Por **extensión**: damos la “lista” (no importa el orden y no hay repeticiones) de sus elementos $A = \{1, 3, 5, 7, 9\}$
- Por **compresión**: Damos una propiedad $P(x)$ que caracteriza sus elementos ($P(x)$ es una propiedad que todos los elementos del conjunto cumplen y ninguno más)

$$A = \{x \mid P(x)\}$$

Igualdad de conjuntos

Dos conjuntos A, B son iguales si y sólo si tienen los mismos elementos: $A = B \Leftrightarrow \forall x(x \in A \leftrightarrow x \in B)$

Conjunto vacío

Conjunto que no tiene elementos, se denota como: $\emptyset = \{ \} = \{x \mid x \neq x\}$

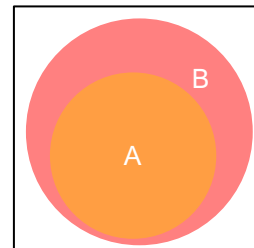
Inclusión entre conjuntos (\subseteq)

A contiene “algunos elementos” (pueden ser todos) de B :

$$A \subseteq B \Leftrightarrow \forall x(x \in A \rightarrow x \in B)$$

Propiedades:

- 1- $\emptyset \subseteq A$.
- 2- $A \subseteq A$.
- 3- $A \subseteq B$ i $B \subseteq C$ implica $A \subseteq C$.



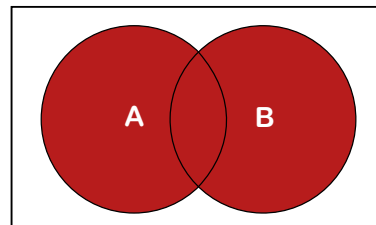
Operaciones entre conjuntos

Unión

Se puede expresar de dos formas:

$$A \cup B = \{x \mid x \in A \vee x \in B\}$$

$$x \in A \cup B \Leftrightarrow x \in A \vee x \in B$$



Propiedades:

1. $A \cup A = A$
2. $A \cup \emptyset = A$
3. $A \cup B = B \cup A$
4. $A \cup (B \cup C) = (A \cup B) \cup C$
5. $A \subseteq A \cup B, B \subseteq A \cup B$

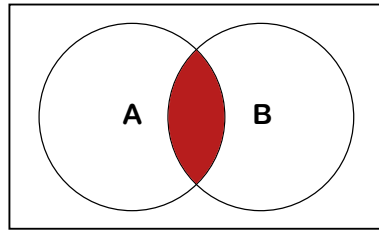
6. $A \subseteq B \Leftrightarrow A \cup B = B$
7. $A \cup B \subseteq C \Leftrightarrow A \subseteq C, B \subseteq C$

Intersección

Se puede expresar de dos formas:

$$A \cap B = \{x \mid x \in A \wedge x \in B\}$$

$$x \in A \cap B \Leftrightarrow x \in A \wedge x \in B$$



Propiedades:

1. $A \cap A = A$
2. $A \cap \emptyset = \emptyset$
3. $A \cap B = B \cap A$
4. $A \cap (B \cap C) = (A \cap B) \cap C$
5. $A \cap B \subseteq A, A \cap B \subseteq B$
6. $A \subseteq B \Leftrightarrow A \cap B = A$
7. $C \subseteq A \cap B \Leftrightarrow C \subseteq A \wedge C \subseteq B$

Cuando dos conjuntos A, B no tienen elementos comunes se dice que son disjuntos:

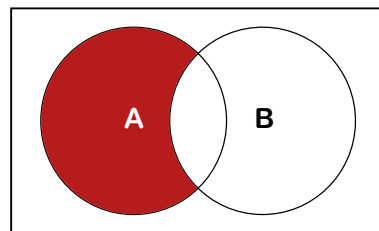
$$A \text{ y } B \text{ son disjuntos} \Leftrightarrow A \cap B = \emptyset$$

Diferencia

Se puede expresar de dos formas:

$$A - B = \{x \mid x \in A \wedge x \notin B\}$$

$$x \in A - B \Leftrightarrow x \in A \wedge x \notin B$$



Propiedades:

1. $A - A = \emptyset$
2. $A - \emptyset = A$
3. $\emptyset - A = \emptyset$
4. $A - B \subseteq A$
5. $(A - B) \cap B = \emptyset$
6. $A \subseteq B \Leftrightarrow A - B = \emptyset$
7. $C \subseteq A - B \Leftrightarrow C \subseteq A \wedge C \cap B = \emptyset$

Otras propiedades:

1. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C), A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ (distributiva)
2. $A \cap (A \cup B) = A, A \cup (A \cap B) = A$
3. $A - (B \cup C) = (A - B) \cap (A - C)$
4. $A \cup B = (A - B) \cup (B - A) \cup (A \cap B)$ y la unión es disjunta (los conjuntos $(A - B), (B - A), (A \cap B)$ son disjuntos 2 a 2).

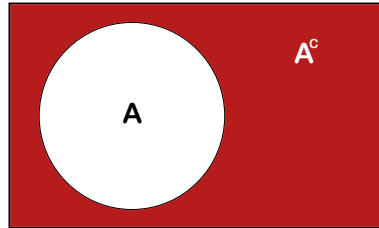
Complementario

Suponemos que hay un conjunto *grande* o *universo* Ω que engloba a todos los elementos.

Se puede expresar de dos formas:

$$A^c = \Omega - A = \{x \in \Omega \mid x \notin A\}$$

$$x \in A^c \Leftrightarrow x \in \Omega \wedge x \notin A$$



Propiedades:

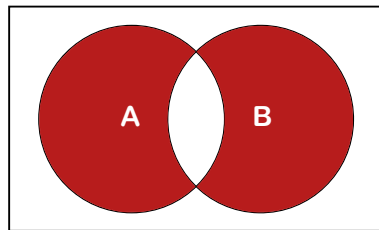
1. $(A^c)^c = A$
2. $\emptyset^c = \Omega, \Omega^c = \emptyset$
3. $A \cap A^c = \emptyset, A \cup A^c = \Omega$
4. $(A \cup B)^c = A^c \cap B^c, (A \cap B)^c = A^c \cup B^c$ (De Morgan)
5. $A - B = A \cap B^c$
6. $B = A^c \Leftrightarrow A \cap B = \emptyset, A \cup B = \Omega$
7. $A \subseteq B \Leftrightarrow B^c \subseteq A^c \Leftrightarrow A \cap B^c = \emptyset \Leftrightarrow A^c \cup B = \Omega$
8. $A \subseteq B^c \Leftrightarrow B \subseteq A^c \Leftrightarrow A \cap B = \emptyset \Leftrightarrow A^c \cup B^c = \Omega$
9. $A^c \subseteq B \Leftrightarrow B^c \subseteq A \Leftrightarrow A^c \cap B^c = \emptyset \Leftrightarrow A \cup B = \Omega$

Diferencia simétrica

Se puede expresar de dos formas:

$$A \triangle B = \{x \mid (x \in A \wedge x \notin B) \vee (x \in B \wedge x \notin A)\}$$

$$x \in A \triangle B \Leftrightarrow (x \in A \wedge x \notin B) \vee (x \in B \wedge x \notin A)$$



Propiedades:

1. $A \triangle B = (A - B) \cup (B - A)$
2. $A \triangle B = (A \cup B) - (A \cap B)$

Partes de un conjunto

Dado un conjunto A definimos el conjunto de las partes (o conjunto potencia) de A así:

$$P(A) = \{x \mid x \subseteq A\}$$

$$x \in P(A) \Leftrightarrow x \subseteq A$$

Ejemplos:

- $P(\emptyset) = \{\emptyset\}$
- $P(\{1\}) = \{\emptyset, \{1\}\}$
- $P(\{1,2\}) = \{\emptyset, \{1\}, \{2\}, \{1,2\}\}$
- $P(\{1,2,3\}) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$

Nota: el número de elementos de un conjunto A recibe el nombre de cardinal de A y se denota como $|A|$. Tenemos: $|P(A)| = 2^{|A|}$

Propiedades:

1. $\emptyset \in P(A)$
2. $A \in P(A)$

Producto cartesiano

Pareja ordenada

Idea: la pareja ordenada es como una lista (o vector) de longitud 2 puesta entre paréntesis (a, b)

$$(a, b) = (c, d) \Leftrightarrow a = c, \quad b = d$$

Producto cartesiano

Dados dos conjuntos A, B definimos el conjunto producto cartesiano de A por B así:

$$A \times B := \{x \mid x = (a, b) \text{ por unos ciertos } a \in A \text{ i } b \in B\} \quad \Bigg| \quad A \times B := \{(a, b) \mid a \in A, b \in B\}$$

Ejemplo:

$$\{1, 2, 3, 4\} \times \{a, b\} = \{(1, a), (2, a), (3, a), (4, a), (1, b), (2, b), (3, b), (4, b)\}$$

Demostraciones con conjuntos

Demostraciones de igualdad entre conjuntos (1ª manera)

Queremos demostrar $A = B$
Sea x cualquiera: $x \in A \Leftrightarrow \dots \Leftrightarrow \dots \Leftrightarrow x \in B$

Demostraciones de una inclusión entre conjuntos

Queremos demostrar $A \subseteq B$
Sea x cualquiera: $x \in A \Rightarrow \dots \Rightarrow \dots \Rightarrow x \in B$

Demostración de igualdad entre conjuntos (2ª manera)

Queremos demostrar $A = B$
Demostraremos dos cosas: $A \subseteq B, B \subseteq A$

Demostración que un conjunto es vacío

Queremos demostrar $A = \emptyset$
Por reducción al absurdo: $\exists x \in A \Rightarrow \dots \Rightarrow \dots \Rightarrow \text{Absurdo}$

Demostración dónde interviene que un conjunto es vacío

En este tipo de demostraciones una buena estrategia es usar contrarrecíproco o reducción al absurdo por tal de que la condición “ser vacío” aparezca negada.

Notamos que:

- $A \neq \emptyset \Leftrightarrow \exists x \ x \in A$
- $A \not\subseteq B \Leftrightarrow \exists x (x \in A \wedge x \notin B)$
- $A \neq B \Leftrightarrow \exists x (x \in A \wedge x \notin B) \vee \exists x (x \notin A \wedge x \in B)$

Relaciones de equivalencia

Idea: una relación binaria en un conjunto A “relaciona” parejas de elementos de A . Cada pareja de elementos de A pueden estar o no estar relacionados. Determinar la relación consiste en indicar que parejas están relacionadas y cuáles no.

Sea $x, y \in A$. Si están relacionados por una relación R lo escribiremos así:

$$xRy$$

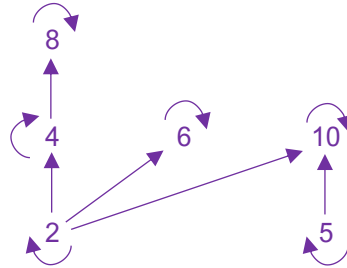
Cuando no están relacionados lo denotaremos por:

$$x \not R y$$

Ejemplo: $A = \{2, 4, 5, 6, 8, 10\}$

$R = \{(2, 2), (2, 4), (2, 6), (2, 10), (4, 4), (4, 8), (5, 5), (5, 10), (6, 6), (8, 8), (10, 10)\}$

Esto quiere decir, por ejemplo, que $2R4$ (2 está relacionado con 4, ya que la pareja $(2, 4) \in R$) en cambio 2 no está relacionado con 3 porque la pareja $(2, 3) \notin R$. También se pueden representar las relaciones mediante diagramas de Venn con flechas: cada flecha representa una pareja relacionada



En todo conjunto A siempre hay las relaciones siguientes:

- La identidad en A (o igualdad), definida por: $xI_A y \Leftrightarrow x = y : I_A = \{(x, y) \in A \times A \mid x = y\} = \{(x, x) \mid x \in A\}$
- La relación vacía (ninguno está relacionado con ninguno): $R = \emptyset$
- La relación total (todos están relacionados con todos): $R = A \times A$

Propiedades importantes que pueden tener las relaciones

Reflexiva	$\forall x \in A \quad xRx$
Simétrica	$\forall x, y \in A \quad (xRy \rightarrow yRx)$
Transitiva	$\forall x, y, z \in A \quad (xRy \wedge yRz \rightarrow xRz)$
Antisimétrica	$\forall x, y \in A \quad (xRy \wedge yRx \rightarrow x = y)$

Una **relación de equivalencia** es una relación binaria que es reflexiva, simétrica y transitiva.

Ejemplo: Tenemos un conjunto A de pelotas de colores

- Reflexiva: una pelota $x \in A$ tiene el mismo color que sí misma.
- Simétrica: siendo $x, y \in A$ y x tiene el mismo color que y entonces, y tiene el mismo color que x .
- Transitiva: siendo $x, y, z \in A$, si x tiene el mismo color que y y y tiene el mismo color que z entonces, x tiene el mismo color que z .

Ejemplo: Consideramos $\mathbb{R} \times \mathbb{R}$ la relación siguiente: $(x, y)R(z, t) \Leftrightarrow |x| + |y| = |z| + |t|$

- Reflexiva: $(x, y)R(x, y) \quad |x| + |y| = |x| + |y|$
- Simétrica: $(x, y)R(z, t) \Rightarrow (z, t)R(x, y)$
 $(x, y)R(z, t) \Rightarrow |x| + |y| = |z| + |t| \Leftrightarrow |z| + |t| = |x| + |y| \Rightarrow (z, t)R(x, y)$
- Transitiva: $\left. \begin{matrix} (x, y)R(z, t) \\ (z, t)R(u, v) \end{matrix} \right\} \Rightarrow |x| + |y| = |z| + |t| = |u| + |v| \Leftrightarrow (x, y)R(u, v)$

Clases de equivalencia y conjunto cociente

Si R es una relación de equivalencia en A i $a \in A$ la clase de a se define así:

$$\bar{a} = \{x \in A \mid xRa\}$$

Por lo tanto, dados $a, b \in A$ tenemos:

$$b \in \bar{a} \Leftrightarrow bRa$$

El **conjunto cociente**, que denotamos por A/R , es el conjunto de todas las clases:

$$A/R = \{x \mid x = \bar{a} \text{ por un cierto } a \in A\} = \{\bar{a} \mid a \in A\}$$

Notamos que:

1. Cada clase de equivalencia es un subconjunto del dominio A .
2. El conjunto cociente A/R es un subconjunto de $P(A)$.

Propiedades:

1. $x \in \bar{x}$
2. Si $x \in \bar{y}$ entonces $\bar{x} = \bar{y}$
3. Si $x \notin \bar{y}$ entonces $\bar{x} \cap \bar{y} = \emptyset$
4. Las clases forman una “partición” de A , es decir:
 - a. Cada clase es no vacía (ya que $x \in \bar{x}$).
 - b. Dos clases diferentes son disjuntas: $\forall x, y \in A \ (\bar{x} \neq \bar{y} \rightarrow \bar{x} \cap \bar{y} = \emptyset)$
 - c. La reunión de todas las clases es A .

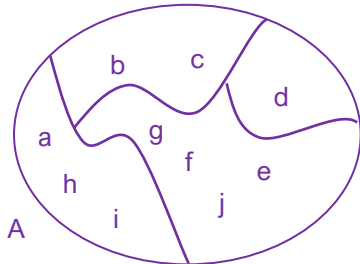
Particiones

Idea: tenemos un conjunto A y lo rompemos (o repartimos) en trozos.

Definición: una partición P de A es un conjunto de subconjuntos no vacíos de A , disjuntos 2 a 2 y tal que su reunión es total. Más precisamente: P es una partición de A si:

- $\forall B \in P \ B \subseteq A$ (de manera equivalente: $P \subseteq P(A)$)
- $\forall B \in P \ B \neq \emptyset$
- $\forall B \in P \ \forall C \in P \ (B \neq C \rightarrow B \cap C = \emptyset)$
- Si $P = \{A_1, A_2, \dots, A_n\}$ entonces $A = A_1 \cup A_2 \cup \dots \cup A_n$
($\forall x \in A \ \exists B \in P \ x \in B$ si la partición no es finita)

Ejemplos:



En el dibujo hemos roto el conjunto $A = \{a, b, c, d, e, f, g, h, i, j\}$ en 4 trozos: $\{b, c\}, \{d\}, \{e, f, g, j\}, \{a, h, i\}$. El conjunto formado por estas 4 partes es una partición de A : $\{\{b, c\}, \{d\}, \{e, f, g, j\}, \{a, h, i\}\}$

- $\{\{1\}, \{2, 3\}, \{4\}, \{5, 6, 7\}\}$ es una partición de $\{1, 2, 3, 4, 5, 6, 7\}$
- $\{\{1, 3, 5\}, \{2, 3\}, \{4\}, \{5, 6, 7\}\}$ **no** es una partición de $\{1, 2, 3, 4, 5, 6, 7\}$
- $\{\{1\}, \{2, 3\}, \{4\}, \{6, 7\}\}$ **no** es una partición de $\{1, 2, 3, 4, 5, 6, 7\}$

Hemos visto que si R es una relación de equivalencia a A , entonces A/R es una partición de A .

Si P es una partición de A , cada elemento x de A pertenece a una única “parte” (elemento de P). Es decir, por cada $x \in A$ hay un único $B \in P$ tal que $x \in B$. Entonces definimos la relación R así:

$$xRy \Leftrightarrow x \text{ y } y \text{ pertenecen al mismo } B \in P$$

Es fácil ver que es una relación de equivalencia. Entonces, si $x \in B \in P$ resulta que $\bar{x} = B$. Por lo tanto, el conjunto cociente $A/R = P$.

4. Funciones

Una función (o aplicación) f consta de un conjunto “origen” A , un conjunto de “destino” B y una “regla” que asocia a cada elemento $x \in A$ a un **único** elemento $y \in B$. Formalmente la “regla” es una relación $R \subseteq A \times B$ que satisface:

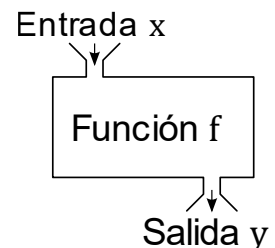
- $\forall x \in A \exists y \in B (x, y) \in R$
- $\forall x \in A \forall y, y' \in B ((x, y) \in R \wedge (x, y') \in R \rightarrow y = y')$

A la única $y \in B$ tal que $(x, y) \in R$ la llamamos **imagen** del elemento x y lo denotamos (a la imagen) cómo $f(x)$. De esta manera podemos expresar las dos propiedades anteriores como:

- $\forall x \in A f(x) \in B$ Para toda entrada A hay una salida B
- $\forall x, x' \in A (x = x' \rightarrow f(x) = f(x'))$ Para la misma entrada siempre se ha de dar la misma salida

Cuando estas dos condiciones se cumplen decimos que f **está bien definida**.

Idea: la “regla” es como una especie de programa, A es un conjunto de entradas posibles y B es un conjunto que contiene todas las salidas posibles (el conjunto de entradas puede ser más grande que el conjunto de todas las salidas). A corresponde a una especificación de la entrada del programa: A es el conjunto de objetos que satisfacen la precondition del programa. B correspondería a una “especificación” de la salida: B es el conjunto de objetos que satisfacen la postcondición del programa.



Notación:

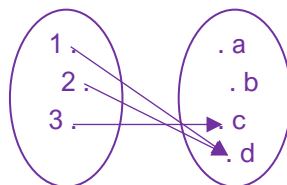
$$f: A \rightarrow B, \quad x \rightarrow f(x)$$

Terminología:

- El conjunto A recibe el nombre de **dominio** o más formalmente conjunto de origen, mientras que B recibe el nombre de **codominio** (informalmente hablamos de conjunto de destino o llegada). Intentaremos evitar la palabra “salida” porque se puede referir tanto al dominio como al codominio.
- $f(x)$ es la imagen de x .
- Si $f(x) = y$, x es una **antiimagen** de y , y es la **imagen** de x .
- Cuando decimos que $f: A \rightarrow B$ **está bien definida** queremos decir que se cumplen las dos condiciones de la definición: Cada $x \in A$ tiene una única imagen $f(x)$ y esta pertenece a B .

Ejemplos:

- $f: \mathbb{Z} \rightarrow \mathbb{N}$ definida por $f(x) = |x|$
- $f: \mathbb{Q} \rightarrow \mathbb{Q}$ definida por $f(x) = \frac{3x-5}{4}$
- $f: \{1, 2, 3\} \rightarrow \{a, b, c, d\}$ definida por $f(1) = d$, $f(2) = d$, $f(3) = c$.



Igualdad entre aplicaciones

Dos aplicaciones son iguales cuando:

- Tienen el mismo dominio y el mismo codominio
- La misma “regla”, es decir, con las mismas entradas corresponden las mismas salidas.

Dadas $f, g: A \rightarrow B$

$$f = g \quad \text{sí y sólo si} \quad \forall x \in A \quad f(x) = g(x)$$

Ejemplos:

- Las funciones $f : \mathbb{R} \rightarrow \mathbb{R}$ definida por $f(x) = x^2 + 1$, $g : \mathbb{Z} \rightarrow \mathbb{Z}$ definida por $g(x) = x^2 + 1$ y $h : \mathbb{Z} \rightarrow \mathbb{R}$ definida por $h(x) = x^2 + 1$ son las tres diferentes.
- Las funciones $f, g : \{1, 2\} \rightarrow \mathbb{Z}$ definidas por $f(x) = x^2$ y $g(x) = 3x - 2$ son iguales (son la misma función).

Propiedades importantes que pueden tener las aplicaciones $f : A \rightarrow B$

- **Inyectiva** $\forall x, x' \in A \ (f(x) = f(x') \rightarrow x = x')$ Cada vez que cogen dos elementos del dominio que tienen la misma imagen los dos elementos son equivalentes
- **Exhaustiva** $\forall y \in B \ \exists x \in A \ f(x) = y$ Por cada elemento del codominio hay como mínimo un elemento del dominio
- **Biyectiva** inyectiva y exhaustiva

Notamos que:

- f es inyectiva \Leftrightarrow todo $y \in B$ tienen como mucho una antiimagen.
- f es exhaustiva \Leftrightarrow todo $y \in B$ tiene como mínimo una antiimagen.
- f es biyectiva \Leftrightarrow todo $y \in B$ tiene una única antiimagen.

Función inversa

Para que una función sea “inversa” de una aplicación, esta ha de ser biyectiva.

Si $f : A \rightarrow B$ es biyectiva, sabemos que todo elemento $y \in B$ tiene una única antiimagen. Entonces **la función inversa** de f , que denotamos por f^{-1} , es la aplicación que va de B a A y que todo $y \in B$ le hacen corresponder su única antiimagen.

$$f : A \rightarrow B \text{ biyectiva}$$

$$f^{-1} : B \rightarrow A$$

$$f^{-1}(y) := \text{la única antiimagen de } y = \text{la única } x \in A \text{ tal que } f(x) = y$$

Notamos que:

- f ha de ser biyectiva, si no la inversa no existe
- $f^{-1}(y) = x \Leftrightarrow f(x) = y$

Propiedad:

Si f es biyectiva entonces f^{-1} también es biyectiva y $(f^{-1})^{-1} = f$.

Imagen y antiimagen de un conjunto

Dados $f : A \rightarrow B$, $X \subseteq A$ $Y \subseteq B$ definimos:

- El conjunto imagen de X :

$$f(X) = \{y \in B \mid \exists x \in X \ f(x) = y\} = \{f(x) \mid x \in X\}$$

$$y \in f(X) \Leftrightarrow \exists x \in X \ f(x) = y$$

- El conjunto antiimagen de Y :

$$f^{-1}(Y) = \{x \in A \mid f(x) \in Y\}$$

$$\text{Si } x \in A: \ x \in f^{-1}(Y) \Leftrightarrow f(x) \in Y$$

Notamos que:

- $f(X)$ es un subconjunto de B (el conjunto de todas las imágenes de los elementos de X).
- $f^{-1}(Y)$ es un subconjunto de A (el conjunto de todas las antiimágenes de los elementos de Y).

Composición de aplicaciones

Dadas $f : A \rightarrow B$ y $g : B \rightarrow C$ definimos la composición de f con g , que llamaremos f compuesta con g y denotemos por $g \circ f$, así:

$$g \circ f : A \rightarrow C, \quad (g \circ f)(x) = g(f(x))$$

Notaremos que:

- No siempre se puede componer, sólo cuando el codominio de la primera aplicación es la misma que (o este contenido en) el dominio de la segunda.
- Decimos f compuesta con g , pero lo denotamos $g \circ f$.

Propiedades:

- $f : A \rightarrow B$, $g : B \rightarrow C$, $h : C \rightarrow D$ entonces $h \circ (g \circ f) = (h \circ g) \circ f$ (Asociativa)
- Si $f : A \rightarrow B$, entonces $I_B \circ f = f \circ I_A = f$

Propiedades de la composición, inyectividad y exhaustividad:

- La composición de aplicaciones inyectivas es inyectiva.
- Si $g \circ f$ es inyectiva entonces f es inyectiva.
- La composición de aplicaciones exhaustivas es exhaustiva.
- Si $g \circ f$ es exhaustiva entonces g es exhaustiva.
- La composición de aplicaciones biyectivas es biyectiva.
- Si $g \circ f$ es biyectiva entonces f es inyectiva y g es exhaustiva.

Propiedades de la composición y la inversa:

- Si $f : A \rightarrow B$ es biyectiva, entonces $f^{-1} \circ f = I_A$ y $f \circ f^{-1} = I_B$
- Si $f : A \rightarrow B$ y $g : B \rightarrow A$ satisfacen $g \circ f = I_A$ y $f \circ g = I_B$, entonces las dos son biyectivas y cada una es la inversa de la otra: $g = f^{-1}$ y $f = g^{-1}$

Demostraciones con funciones

Demostración que $f : A \rightarrow B$ es inyectiva

Sean $x, x' \in A$ cualquiera: $f(x) = f(x') \Rightarrow \dots \Rightarrow x = x'$

Demostración que $f : A \rightarrow B$ NO es inyectiva

Dado $x, x' \in A$ satisfaciendo: $x \neq x'$, $f(x) = f(x')$ (un contraejemplo)

Demostración que $f : A \rightarrow B$ es exhaustiva

Sea $y \in B$ cualquiera. Tenemos que dar alguna $x \in A$ tal que $f(x) = y$

Demostración que $f : A \rightarrow B$ NO es exhaustiva

Tenemos que dar $y \in B$ que no tenga ninguna antiimagen (por la que la "ecuación" $f(x) = y$ no tiene ninguna solución $x \in A$).

Demostración que $f : A \rightarrow B$ es biyectiva

1ª manera: f es inyectiva y exhaustiva

2ª manera: Sea $y \in B$ cualquiera. Tenemos que ver que hay un único $x \in A$ tal que $f(x) = y$.

Demostración que las aplicaciones $f, g : A \rightarrow B$ son iguales ($f = g$)

Dada $x \in A$, tenemos que ver $f(x) = g(x)$

5. Divisibilidad

Dados dos enteros a, b definimos: $a \mid b \Leftrightarrow$ existe un entero q tal que $b = aq$

$a \mid b$ se lee a divide b . También decimos que a es un divisor de b o que b es un múltiplo de a .

Ejemplos: $2 \mid 6, 6 \mid 6, 6 \mid -12, -4 \mid 12$.

Notamos que:

- No es exactamente lo mismo $a \mid b$ que $b/a \in \mathbb{Z}$.
- Si $a \neq 0$ si que es equivalente: $a \mid b \Leftrightarrow b/a \in \mathbb{Z}$.
- $a \mid b \Leftrightarrow (a = b = 0) \vee (a \neq 0 \wedge b/a \in \mathbb{Z})$.

Propiedades: Para todo a, b, c, u, v enteros:

1. $1 \mid a$
2. $a \mid 0$
3. $a \mid a$ (Reflexiva)
4. $a \mid b, b \mid c \Rightarrow a \mid c$ (Transitiva)
5. $a \mid b \Rightarrow ac \mid bc$
6. Si $c \neq 0, ac \mid bc \Rightarrow a \mid b$ (Simplificación)
7. $a \mid b \Rightarrow a \mid bc$
8. $a \mid b \Leftrightarrow a \mid -b \Leftrightarrow -a \mid b \Leftrightarrow -a \mid -b \Leftrightarrow |a| \mid |b|$ (No depende del signo)
9. Si $b \neq 0, a \mid b \Rightarrow |a| \leq |b|$
10. $a \mid b, b \mid a \Rightarrow |a| = |b|$
11. $a \mid b, a \mid c \Rightarrow a \mid ub + vc$ (Linealidad)

Ejemplo: Queremos encontrar a todos los enteros divisores de 6 y 15 a la vez. Si $a \mid 6$ y $a \mid 15$, por linealidad, $a \mid 15 - 2 \cdot 6 = 3$. Recíprocamente, $a \mid 3$ por la propiedad 7, $a \mid 3 \cdot 5 = 15$ y $a \mid 3 \cdot 2 = 6$. Así, los divisores comunes de 6 y 15 son los enteros a tales que $a \mid 3$, es decir, $\pm 1, \pm 3$.

Números primos

Dado un número entero p : p es primo $\Leftrightarrow p \geq 2$ y los únicos divisores positivos de p son 1 y p

Notamos que:

- Los números primos son positivos y el 1 no es primo.
- Si $n \geq 2$, y no es primo (recibe el nombre de compuesto) entonces $n = rs$ para ciertos enteros r, s con $2 \leq r < n, 2 \leq s < n$.
- Los números 1, -1 no tienen divisores primos.

Resultados:

- Todo número entero $n \geq 2$ es primo o es producto de números primos.
- Todo número entero $n \geq 2$ tiene algún divisor primo p . Si además n no es primo, podemos escoger algún divisor primo $p \leq \sqrt{n}$.
- Hay infinitos números primos

Test de primalidad: Para verificar que un número n es primo, basta con verificar que no tiene ningún divisor primo $\leq \sqrt{n}$.

Máximo común divisor (mcd)

El máximo común divisor de los enteros a_1, a_2, \dots, a_n es el más grande de todos los divisores comunes de a_1, a_2, \dots, a_n si alguno de estos valores no es 0. Los divisores comunes de $0, 0, \dots, 0$ son todos los enteros y por lo tanto no hay un máximo. En este caso se toma el 0 como mcd por definición. El máximo común divisor de a_1, a_2, \dots, a_n lo denotamos como $mcd(a_1, a_2, \dots, a_n)$. Esto lo podemos expresar así:

$$mcd(0, 0, \dots, 0) = 0$$

- Si algún $a_i \neq 0$, $\text{mcd}(a_1, a_2, \dots, a_n)$ es el único entero d que verifica las dos propiedades siguientes:
 - $d \mid a_i$ por cada i
 - Si $d' \mid a_i$ por cada i entonces $d' \leq d$.

Propiedades: Por cualquier entero a, b, u tenemos que:

- Si $a \mid b$ entonces $\text{mcd}(a, b) = |a|$
- $\text{mcd}(a, 0) = |a|$
- Si p es primo y no divide b , entonces $\text{mcd}(p, b) = 1$
- El mcd no depende del signo: $\text{mcd}(a, b) = \text{mcd}(a, -b) = \text{mcd}(-a, b) = \text{mcd}(-a, -b)$
- $\text{mcd}(a, b) = \text{mcd}(a + ub, b)$ **(Teorema de Euclides)**

a y b son **primos entre sí** $\Leftrightarrow \text{mcd}(a, b) = 1$ El máximo común divisor es 1 o -1

Primos entre sí o **relativamente primos**

Observación: a y b son primos entre sí \Leftrightarrow no tienen ningún divisor primo común

División euclidiana

Dados a, b enteros siendo $b \neq 0$, existen unos únicos enteros q, r tales que:

$$a = bq + r \quad 0 \leq r < |b|$$

$$\begin{array}{r} a \text{ } \overline{) b} \\ r \text{ } q \end{array}$$

q es el cociente y r el residuo de la división de a por b

Algoritmo de Euclides

Queremos calcular $\text{mcd}(a, b)$. Como que el mcd no depende del signo podemos empezar suponiendo que $a \geq b > 0$. Para calcular el mcd usamos esta tabla de referencia:

q		q_1	q_2		q_{n-1}		
r	$r_0 = a$	$r_1 = b$	r_2	...	r_{n-1}	r_n	0

Ejemplo: $\text{mcd}(14001, 279) = \text{mcd}(279, 51) = \text{mcd}(51, 24) = \text{mcd}(24, 3) = 3$

q		50	5	2		
r	14001	279	51	24	3	0

Identidad de Bézout

Dados a, b enteros cualesquiera, existen x, y enteros tales que $\text{mcd}(a, b) = ax + by$. Es básicamente otra de plasmar el apartado anterior.

Una forma sistemática de calcular esta identidad:

x	1	0	x_2	x_3	...	x_{n-1}	x_n	
y	0	1	y_2	y_3	...	y_{n-1}	y_n	
q		q_1	q_2	q_3	...	q_{n-1}		
r	$r_0 = a$	$r_1 = b$	r_2	r_3	...	r_{n-1}	r_n	0

Aplicando el ejemplo anterior:

x	1	0	1	-5	11	
y	0	1	-50	251	-552	
q		50	5	2		
r	14001	279	51	24	3	0

$$3 = 14001(11) + 279(-552)$$

Notamos que: Las identidades de Bézout no son nunca únicas. Siempre podemos y restar múltiplos de $\frac{ab}{\text{mcd}(a,b)}$:

$$ax + by = a \left(x + t \frac{b}{\text{mcd}(a,b)} \right) + b \left(y - t \frac{a}{\text{mcd}(a,b)} \right)$$

Consecuencias de Bézout

Lema de Gauss Si $a \mid bc$ y $\text{mcd}(a, b) = 1$ entonces $a \mid c$

Lema de Euclides Si p es primo y $p \mid bc$ entonces $p \mid b$ o $p \mid c$

Descomposición en factores primos

Unicidad de la descomposición en factores primos

Todo entero $n \geq 2$ tiene una descomposición única de la siguiente forma: $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$, donde cada p_i es primo y cada $e_i > 0$.

Esto quiere decir que el k , los p_1, \dots, p_k y los e_1, \dots, e_k son los únicos (sin considerar la permutación).

Ejemplo: $84 = 2^2 \times 3^1 \times 7^1$ $90 = 2^1 \times 3^2 \times 5^1$

Descomposición en factores primos con signo y exponentes posiblemente nulos

Todo entero $n \neq 0$ tiene una descomposición de la siguiente forma: $n = \varepsilon p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$, donde $\varepsilon = \pm 1$, cada p_i es primo y cada $e_i \geq 0$.

Notamos que: en esta última factorización tanto ε como los exponentes son únicos. Pero ni la k ni los p_1, \dots, p_k son únicos, ya que siempre podemos añadir un nuevo primo con exponente 0.

Por ejemplo: $-28 = (-1) \times 2^2 \times 7^1 = (-1) \times 2^2 \times 3^0 \times 5^0 \times 7^1 \times 11^0$

Gracias a eso siempre podemos suponer que aparecen los mismos números primos en la misma factorización de distintos números.

Por ejemplo: $84 = 2^2 \times 3^1 \times 5^0 \times 7^1 \times 11^0$, $-90 = (-1) \times 2^1 \times 3^2 \times 5^1 \times 7^0 \times 11^0$,
 $-264 = (-1) \times 2^3 \times 3^1 \times 5^0 \times 7^0 \times 11^1$

Cálculo del mcd a partir de la factorización y consecuencias

Divisibilidad y cálculo del mcd a partir de la factorización

Si expresamos $a = \varepsilon_1 p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$ y $b = \varepsilon_2 p_1^{f_1} p_2^{f_2} \dots p_k^{f_k}$ con $e_i, f_i \geq 0$, $\varepsilon_i = \pm 1$ y cada p_i primo entonces tenemos:

1. $a \mid b \Leftrightarrow e_i \leq f_i$ por cada i
2. $\text{mcd}(a, b) = p_1^{\min(e_1, f_1)} p_2^{\min(e_2, f_2)} \dots p_k^{\min(e_k, f_k)}$
3. La fórmula del mcd también vale con 2 o más números cogiendo el mínimo de los distintos exponentes.
4. Los divisores positivos de a son todos los números de la forma $p_1^{g_1} p_2^{g_2} \dots p_k^{g_k}$ con $0 \leq g_i \leq e_i$
5. El número de divisores positivos de a es $(e_1 + 1)(e_2 + 1) \dots (e_k + 1)$

Ejemplo: $\text{mcd}(84, -90, -264) = 2^1 \times 3^1 \times 5^0 \times 7^0 \times 11^0$

Consecuencias de la factorización

1. **Todo divisor común de a , b divide $\text{mcd}(a, b)$. De hecho:** $d \mid a \wedge d \mid b \Leftrightarrow d \mid \text{mcd}(a, b)$
2. $\text{mcd}(\text{mcd}(a, b), c) = \text{mcd}(a, \text{mcd}(b, c)) = \text{mcd}(a, b, c)$ (Asociatividad mcd)
3. $\text{mcd}(ca, cb) = |c| \text{mcd}(a, b)$
4. $\text{mcd}(a/\text{mcd}(a, b), b/\text{mcd}(a, b)) = 1$ (Si $\text{mcd}(a, b)$ no es nulo)
5. Todas las propiedades anteriores valen también con 3 o más enteros.

Nota: El cálculo eficiente de $\text{mcd}(a_1, a_2, \dots, a_n)$ se puede hacer aplicando la asociatividad del mcd y en cada paso, calcular el mcd de dos números mediante el algoritmo de Euclides.

Ecuaciones diofánticas

Las ecuaciones diofánticas son ecuaciones a coeficientes enteros de los cuales buscamos soluciones enteras.

Ejemplo: $6x - 10y = 4$

$$\text{mcd}(6x, -10) = 2 \quad \frac{c}{\text{mcd}(a,b)} = \frac{4}{\text{mcd}(6,-10)} = 2$$

x	1	0	1	-1	2	
y	0	1	0	1	-1	
q		0	1	1	2	
r	6	-10	-6	4	2	0

Resolución de ecuaciones diofánticas

- La ecuación diofántica $ax + by = c$ tiene solución $\Leftrightarrow \text{mcd}(a, b) \mid c$
- Las soluciones particulares se obtienen multiplicando una identidad de Bézout de (a, b) por $\frac{c}{\text{mcd}(a, b)}$ en ambos lados.
- Si x_0, y_0 es una solución particular de la ecuación anterior, todas las soluciones son de la forma:

$$x = x_0 + \frac{b}{\text{mcd}(a, b)} t, \quad y = y_0 - \frac{a}{\text{mcd}(a, b)} t \quad \text{para un cierto entero } t.$$

Mínimo común múltiple

El mínimo común múltiple de los enteros a_1, a_2, \dots, a_n es el más pequeño de todos los múltiplos comunes positivos (> 0) de a_1, a_2, \dots, a_n , si hay. Esto pasa cuando todos los a_i son $\neq 0$. Si alguno de los $a_i = 0$ el único múltiple común es 0. El mínimo común múltiple de los números enteros a_1, a_2, \dots, a_n lo denotamos como $\text{mcm}(a_1, a_2, \dots, a_n)$.

Definición:

- Si algún $a_i = 0$, $\text{mcm}(a_1, a_2, \dots, a_n) = 0$
- Si todo $a_i \neq 0$, el $\text{mcm}(a_1, a_2, \dots, a_n)$ es el único entero m que verifica las dos propiedades siguientes:
 - $m > 0$ y $a_i \mid m$ por cada i
 - Si $m' > 0$ y $a_i \mid m'$ por cada i entonces $m \leq m'$

Propiedades:

1. Si $a \mid b$ entonces $\text{mcm}(a, b) = |b|$
2. El mcm no depende del signo: $\text{mcm}(a, b) = \text{mcm}(a, -b) = \text{mcm}(-a, b) = \text{mcm}(-a, -b)$

Cálculo del mcm a partir de la factorización y consecuencias

Cálculo del mcm a partir de la factorización

Si expresamos $a = \varepsilon_1 p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$ y $b = \varepsilon_2 p_1^{f_1} p_2^{f_2} \dots p_k^{f_k}$ con $e_i, f_i \geq 0$, $\varepsilon_i = \pm 1$ y cada p_i primo entonces tenemos:

$$mcm(a, b) = p_1^{\max(e_1, f_1)} p_2^{\max(e_2, f_2)} \dots p_k^{\max(e_k, f_k)}$$

Esta fórmula también vale con 3 o más números cogiendo el máximo de los distintos exponentes.

Ejemplo: $84 = 2^2 \times 3^1 \times 5^0 \times 7^1 \times 11^0$, $-90 = (-1) \times 2^1 \times 3^2 \times 5^1 \times 7^0 \times 11^0$,
 $-264 = (-1) \times 2^3 \times 3^1 \times 5^0 \times 7^0 \times 11^1$

$$mcm(84, -90, -264) = 2^3 \times 3^2 \times 5^1 \times 7^1 \times 11^1$$

Consecuencias:

1. **Cálculo eficiente del mcm:** $mcd(a, b) \times mcm(a, b) = |ab| \Rightarrow mcm(a, b) = \frac{|ab|}{mcd(a, b)}$
(sólo con 2 números)
2. **Todo múltiplo común de a, b es múltiplo de $mcm(a, b)$.** De hecho: $a \mid m \wedge b \mid m \Leftrightarrow mcm(a, b) \mid m$
3. $mcm(mcm(a, b), c) = mcm(a, mcm(b, c)) = mcm(a, b, c)$ **(Asociatividad mcm)**
4. Todas las propiedades anteriores valen también con 3 o más enteros excepto la propiedad 1.

6. Congruencias

La relación binaria siguiente a \mathbb{Z} recibe el nombre de congruencia. Hay una por cada $m \geq 1$. El nombre m recibe el nombre de módulo de la congruencia.

Definición:

Dada $m \geq 1$

$$\begin{aligned} a \equiv b(\text{mod } m) &\Leftrightarrow m \mid b - a \\ &\Leftrightarrow b = a + km \text{ para una cierta } k \\ &\Leftrightarrow a \text{ i } b \text{ tienen el mismo residuo al dividir por } m \end{aligned}$$

Cuando $a \equiv b(\text{mod } m)$ se dice que a es congruente con b módulo m

Ejemplos:

1. $7 \equiv 15(\text{mod } 4)$ $15 - 7$ es múltiple de 4
2. $7 \not\equiv 12(\text{mod } 4)$ $12 - 7$ no es múltiple de 4
3. $a \equiv b(\text{mod } 1)$ $a - b$ cualquier número es múltiplo de 1
4. $a \equiv b(\text{mod } 2) \Leftrightarrow a \text{ es par}$
5. $a \equiv 1(\text{mod } 2) \Leftrightarrow a \text{ es impar}$
6. $a \equiv b(\text{mod } 2) \Leftrightarrow a \text{ i } b \text{ tiene la misma paridad}$

Propiedad 1 La congruencia módulo m es una relación de equivalencia

Clases modulares

La clase de a por la relación de congruencia módulo m se denota por \bar{a} y el conjunto cociente se denota como \mathbb{Z}_m .

Ejemplo: $m = 5$. Como que hay 5 residuos posibles al dividir por 5, habrá cinco clases de módulo 5:

- $\bar{0} = \{x \in \mathbb{Z} : x \equiv 0(\text{mod } 5)\} = \{5k : k \in \mathbb{Z}\}$
- $\bar{1} = \{x \in \mathbb{Z} : x \equiv 1(\text{mod } 5)\} = \{1 + 5k : k \in \mathbb{Z}\}$
- $\bar{2} = \{x \in \mathbb{Z} : x \equiv 2(\text{mod } 5)\} = \{2 + 5k : k \in \mathbb{Z}\}$
- $\bar{3} = \{x \in \mathbb{Z} : x \equiv 3(\text{mod } 5)\} = \{3 + 5k : k \in \mathbb{Z}\}$
- $\bar{4} = \{x \in \mathbb{Z} : x \equiv 4(\text{mod } 5)\} = \{4 + 5k : k \in \mathbb{Z}\}$

El conjunto cociente es entonces: $\mathbb{Z}_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$

Hechos:

- A \mathbb{Z}_m : $\bar{a} = \{x \in \mathbb{Z} : x \equiv a(\text{mod } m)\} = \{a + mk : k \in \mathbb{Z}\}$
- $\bar{a} = \bar{b}$ a $\mathbb{Z}_m \Leftrightarrow a \equiv b(\text{mod } m)$ Tienen la misma clase si y sólo si son congruentes
- $\mathbb{Z}_m = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{m-1}\}$

Propiedad 2
$$\begin{array}{l} a \equiv a'(\text{mod } m) \\ b \equiv b'(\text{mod } m) \end{array} \Rightarrow \begin{array}{l} a + b \equiv a' + b'(\text{mod } m) \\ ab \equiv a'b'(\text{mod } m) \end{array}$$

Ejemplo 1: Calcular el residuo de dividir 58×79 módulo 11

$$\begin{array}{l} 58 \equiv 3(\text{mod } 11) \\ 79 \equiv 2(\text{mod } 11) \end{array} \Rightarrow 58 \times 79 \equiv 3 \times 2(\text{mod } 11) \Rightarrow 58 \times 79 \equiv 3 \times 2 = 6$$

Ejemplo 2: Calcular las últimas cifras de $2^{1\,000\,000}$ a mano

Trabajaremos con módulo 100. Empezamos calculando los residuos de las primeras potencias de 2:

$$2^2 = 4, \quad 2^3 = 8, \quad 2^4 = 16, \quad 2^5 = 32, \quad 2^6 = 64,$$

$$2^7 = 128 \equiv 28(\text{mod } 100),$$

$$2^8 = 2 \times 2^7 \equiv 2 \times 28 \equiv 56(\text{mod } 100),$$

$$2^9 = 2 \times 2^8 \equiv 2 \times 56 \equiv 112 \equiv 12(\text{mod } 100),$$

$$2^{10} = 2 \times 2^9 \equiv 2 \times 12 \equiv 24(\text{mod } 100),$$

$$2^{11} = 2 \times 2^{10} \equiv 2 \times 24 \equiv 48 \equiv 48(\text{mod } 100),$$

$$2^{12} = 2 \times 2^{11} \equiv 2 \times 48 \equiv 96 \equiv -4(\text{mod } 100),$$

$$2^{13} = 2 \times 2^{12} \equiv 2 \times (-4) \equiv -8(\text{mod } 100),$$

...

$$2^{20} \equiv -24(\text{mod } 100),$$

$$2^{21} \equiv -48(\text{mod } 100),$$

$$2^{22} \equiv 4(\text{mod } 100) \equiv 2^2(\text{mod } 100).$$

Aquí observamos el primer valor que se repite

Por lo tanto, también tenemos que: $2^2 \equiv 2^2 2^{20} \equiv 2^2 2^{20} 2^{20} \equiv 2^2 2^{20} 2^{20} 2^{20} \equiv \dots \equiv 2^{2+20k}(\text{mod } 100)$

Así que: $1\,000\,000 = 18 + 2 + 20 \times 49\,999 \Rightarrow 2^{1\,000\,000} \equiv 2^{2+20 \times 49\,999} 2^{18} \equiv 2^2 2^{18} \equiv 2^{20} \equiv -24 \equiv 76$

Por lo tanto, las últimas dos cifras de $2^{1\,000\,000}$ son 76.

Otras propiedades de las congruencias

1. Si $a \equiv b(\text{mod } m)$ y $d \mid m$ entonces $a \equiv b(\text{mod } d)$ (Se puede reducir el módulo)
2. Si $k > 0$ entonces $ka \equiv kb(\text{mod } km) \Leftrightarrow a \equiv b(\text{mod } m)$ (**Simplificación**)
3. Si $\text{mcd}(k, m) = 1$ entonces: $a \equiv b(\text{mod } m) \Leftrightarrow ka \equiv kb(\text{mod } m)$

Aritmética modular

Podemos definir una aritmética (operaciones de suma y producto) al conjunto \mathbb{Z}_m de la siguiente manera:

- $\bar{a} + \bar{b} = \overline{a + b}$
- $\bar{a} \times \bar{b} = \overline{a \times b}$

Esto está bien definido gracias a la propiedad 2 de las congruencias. Esta propiedad nos dice que: “el resultado no depende del representante”. Expresada en términos de clase:

$$\begin{vmatrix} \bar{a} = \bar{a}' \\ \bar{b} = \bar{b}' \end{vmatrix} \Rightarrow \begin{vmatrix} \bar{a} + \bar{b} \equiv \bar{a}' + \bar{b}' \\ \bar{a}\bar{b} \equiv \bar{a}'\bar{b}' \end{vmatrix}$$

Con estas operaciones es fácil ver que \mathbb{Z}_m **es un anillo**. El neutro de la suma es $\bar{0}$, el neutro del producto es $\bar{1}$ y el inverso por la suma de \bar{a} es $-\bar{a}$.

La propiedad 2 que acabamos de mencionar dice que el resultado nos permite “escoger el representante” que más nos convenga. Siempre es mejor “reducir” antes de operar

Por ejemplo: \mathbb{Z}_{3000} : $\overline{2990} \overline{2995} = \overline{(-10)} \overline{(-5)} = \bar{50}$

Ejemplo: Tabla de la suma de \mathbb{Z}_5 :

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$

Ejemplo: Tabla del producto de \mathbb{Z}_5 :

\times	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Observamos que tanto $\bar{1}$, $\bar{2}$, $\bar{3}$ como $\bar{4}$ tienen el inverso respecto al producto. Es decir, todo elemento no nulo tiene inverso. Cuando esto pasa decimos que el anillo es un **cuerpo**. Así que \mathbb{Z}_5 es cuerpo.

Ejemplo: Tabla del producto de \mathbb{Z}_6 :

\times	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Ahora observamos que las únicas clases que tienen inversa son $\bar{1}$ y $\bar{5}$.

Inversa modular

Buscar una inversa de \bar{a} a \mathbb{Z}_m es buscar un entero x tal que $\bar{a} \times \bar{x} = \bar{1}$. O de manera equivalente, un entero x tal que $ax \equiv 1 \pmod{m}$. Esto último quiere decir que $1 = ax + my$ para un cierto y entero. Todo junto nos dice que \bar{a} tiene inversa a $\mathbb{Z}_m \Leftrightarrow$ la ecuación diofántica $ax + my = 1$ tiene solución. Pero esto pasa si y sólo si $\text{mcd}(a, m) = 1$. Observamos que el inverso se encuentra a partir de una identidad de Bézout por m, a

Acabamos de demostrar que:

Existencia de inversos modulares \bar{a} tiene inverso a $\mathbb{Z}_m \Leftrightarrow \text{mcd}(a, m) = 1$

Ejemplo: Encontrar el inverso modular de $\overline{227}$ a \mathbb{Z}_{2292}

y	0	1	-10	101	-313
q		10	10	3	
r	2292	227	22	7	1

Nota: (Observamos que el valor de x no importa)

Por lo tanto, el inverso de $\overline{227}$ a \mathbb{Z}_{2292} es $\overline{-313} = \overline{1979}$, esto se puede escribir así: $\overline{227}^{-1} = \overline{1979}$

Un cuerpo es anillo cuando, a excepción del 0 (el neutro de la suma), todo elemento es invertible respecto la multiplicación.

Cuando \mathbb{Z}_m es cuerpo \mathbb{Z}_m es un cuerpo $\Leftrightarrow m$ es primo

Sistemas de congruencias

Si tenemos un sistema de dos congruencias: $x \equiv a_1 \pmod{m_1}$, $x \equiv a_2 \pmod{m_2}$, y x es una solución entonces $x = a_1 + m_1y = a_2 + m_2z$ para unos ciertos y, z enteros. Por lo tanto, $m_1y - m_2z = a_2 - a_1$ tiene solución mediante un sistema chino de dos congruencias si y sólo si $\text{mcd}(m_1, m_2) \mid a_2 - a_1$.

En caso de tener todas las soluciones son de la forma: $x = a_1 + m_1y = a_1 + m_1 \left(y_0 + \frac{m_2}{\text{mcd}(m_1, m_2)} t \right) = a_1 + m_1y_0 + \frac{m_1m_2}{\text{mcd}(m_1, m_2)} t = x_0 + \text{mcm}(m_1, m_2)t$ donde x_0 es una solución particular del sistema. Es decir, si el sistema tiene solución, todas las soluciones son de la forma:

$$x \equiv x_0 \pmod{\text{mcm}(m_1, m_2)}$$

Última propiedad de las congruencias

$$a \equiv b \pmod{m_1}, \dots, a \equiv b \pmod{m_n} \Leftrightarrow a \equiv b \pmod{\text{mcm}(m_1, \dots, m_n)}$$

Ejemplo: Consideramos el sistema: $x \equiv 0 \pmod{3}$, $x \equiv 1 \pmod{4}$, $x \equiv 2 \pmod{5}$

Como que: $-3 \equiv 0 \pmod{3}$, $-3 \equiv 1 \pmod{4}$, $-3 \equiv 2 \pmod{5}$

Por transitividad el sistema se puede reescribir: $x \equiv -3 \pmod{3}$, $x \equiv -3 \pmod{4}$, $x \equiv -3 \pmod{5}$

Aplicando la propiedad anterior resulta que esto es equivalente a: $x \equiv -3 \pmod{\text{mcm}(3, 4, 5)}$

Por lo tanto, todas las soluciones al sistema son: $x = -3 + 60t$, t entero

El teorema pequeño de Fermat

$$\text{Si } p \text{ es primo y no divide } a \text{ entonces } a^{p-1} \equiv 1 \pmod{p}$$

Esto se puede expresar en clases a \mathbb{Z}_p de la siguiente manera:

$$\text{Si } p \text{ es primo y } a \text{ es invertible entonces } \overline{a^{p-1}} = \overline{1}$$

Ejemplo: Calculamos el residuo de 43^{3221} módulo 13.

Primero reducimos la base: $43^{3221} \equiv 4^{3221} \pmod{13}$

Como que 4 es primo con 13, por Fermat tenemos que $4^{12} \equiv 1 \pmod{13}$. Como que cada 12 factores “desaparecen”, agruparemos los factores en paquetes de 12: haremos la división Euclidiana de 3221 por 12 y obtenemos que $3221 = 268 \times 12 + 5$. Por lo tanto:

$$4^{3221} \equiv 4^{268 \times 12 + 5} \equiv (4^{12})^{268} 4^5 \equiv 1^{268} 4^5 \equiv 4^5 \equiv 10 \pmod{13}$$

Observación Si $n, m \geq 1$ i $n \equiv m \pmod{p-1}$ $\Rightarrow a^n \equiv a^m \pmod{p}$

Ejemplo: Calculamos el residuo de 4^{3141} módulo 137 reduciendo a Fermat

Como que $3141 \equiv 13 \pmod{136}$ tenemos que: $4^{3141} \equiv 4^{13} \equiv 67108864 \equiv 99 \pmod{137}$