Matemática Discreta

Tema 1: Lógica

$x^2 - 5x + 6 = 0$

$$x = \frac{5 \pm \sqrt{25 - 4 \cdot 6}}{2 \cdot 1} \begin{cases} \frac{5-1}{2} = 3 \\ \frac{5-1}{2} = 2 \end{cases}$$

Nota: $ax^2 + bx + c = 0$

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

- Proposiciones

Sentencia enunciada de la que se puede decir si es verdad o miente:

→ Está lloviendo 0 (Falso)

→ La sangre es roja 1(Verdadero)

- Proposiciones simples

Las proposiciones se escriben con letras minúsculas: $p, q, r, s, t, \ldots$

Operaciones básicas lógicas:

- Disyunción $\vee$ "o"
- Conjunción $\wedge$ "y"
- Negación $\neg$ "no"

- Tablas de verdad

p	q	$p \vee q$
1	1	1
1	0	1
0	1	1
0	0	0

p	q	$p \wedge q$
1	1	1
1	0	0
0	1	0
0	0	0

p	$\neg p$
1	0
0	1

Nota: Dos proposiciones on lógicamente similares cuando tienen el mismo cambio de unidad.

Orden de prioridad

1) Negación

2) Conjunción

3) Disyunción

Ejemplo

$(p \vee q) \wedge r \not\equiv p \vee q \wedge r$

p	q	r	$p \vee q$	$(p \vee q) \wedge r$	$q \wedge r$	$p \vee q \wedge r$
1	1	1	1	1	1	1
1	1	0	1	0	0	1
1	0	1	1	1	0	1
1	0	0	1	0	0	1
0	1	1	1	1	1	1
0	1	0	1	0	0	0
0	0	1	0	0	0	0
0	0	0	0	0	0	0

$\neg p \vee qr \not\equiv \neg(p \vee q)$

p	q	$\neg p$	$\neg p \vee q$	$p \vee q$	$\neg(p \vee q)$
1	1	0	1	1	0
1	0	0	0	1	0
0	1	1	1	1	0
0	0	1	1	0	1

$\neg(p \vee q) \equiv \neg p \vee \neg p$

p	q	$\neg p$	$\neg q$	$\neg p \vee \neg q$	$\neg p \wedge \neg q$
1	1	0	0	1	0
1	0	0	1	0	0
0	1	1	0	1	0
0	0	1	1	1	1

- Tautología: La tabla de verdad tiene todo 1 $(p \vee \neg p)$
- Contradicción: La tabla de verdad tiene todo 0 $(p \wedge \neg p)$

- Álgebra de porposiciones

p	0	$p \vee 0$
1	0	1
0	0	0

p	1	$p \vee 1$
1	1	1
0	1	1

$p \vee 0 \equiv p$	$p \wedge 1 \equiv p$	
$p \vee 1 \equiv 1$	$p \wedge 0 \equiv 0$	Leyes de identidad
$p \vee p \equiv p$	$p \wedge p \equiv p$	
$p \vee (q \vee r) \equiv (p \vee q) \vee r$	$p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r$	Leyes asociativas
$p \vee q \equiv q \vee p$	$p \wedge q \equiv q \wedge p$	Leyes conmutativas
$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$	$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	Leyes distributivas
$\neg\neg p \equiv p$		Ley de doble negación
$\neg 1 \equiv 0 \quad p \vee \neg p \equiv 1$	$\neg 0 \equiv 1 \quad p \wedge \neg p \equiv 0$	Leyes de los complementos
$\neg(p \vee q) \equiv \neg p \wedge \neg q$	$\neg(p \wedge q) \equiv \neg p \vee \neg q$	Leyes de DeMorgan

- Demostración

$\neg(p \vee q) \vee (\neg p \wedge q) \equiv \neg p$

$(\neg p \wedge \neg q) \vee (\neg p \wedge q)$

$\neg p \wedge (\neg q \vee q)$

$\neg p \wedge 1$

$\neg p$

- Proposiciones

$p \to q$

$p \leftrightarrow q$

$(p \to q) \wedge (q \to p)$

$(\neg p \vee q) \wedge (\neg q \vee p)$

p	q	$p \to q$	$p \leftrightarrow q$
1	1	1	1
1	0	0	0
0	1	1	0
0	0	1	1

$p \to q \equiv \neg p \vee q$

p	q	$\neg p$	$\neg p \vee q$
1	1	0	1
1	0	0	0
0	1	1	1
0	0	1	1

$p \to q \equiv \neg q \to \neg p$

p	q	$\neg p$	$\neg q$	$\neg p \to \neg q$
1	1	0	0	1
1	0	0	1	0
0	1	1	0	1
0	0	1	1	1

- Deducciones lógicas

Si n es natural entonces $2n$ es par.

Si $a, b, c \in \mathbb{R}$ y $a \neq 0$ entonces la solución de $ax`2 + bx + c = 0$ es $x = \dfrac{-b \pm \sqrt{b^2 - 4ac}}{2a}$

$\{p_1, p_2, p_4\} \to q$

$\{p_1, p_2, \ldots, p_n\} \to q \qquad p_1 \wedge p_2 \wedge \cdots \wedge p_n \to q$ es tautología, si no es una falacia.

$\{p \to q, p\} \to q$

p	q	$p \to q$	$(p \to q) \wedge p$	$((p \to q) \wedge p) \to q$
1	1	1	1	1
1	0	0	0	1
0	1	1	0	1
0	0	1	0	1

$\{p \to q, q\} \to p$

p	q	$p \to q$	$(p \to q) \wedge q$	$((p \to q) \wedge q) \to p$
1	1	1	1	1
1	0	0	0	1
0	1	1	1	0
0	0	1	0	1

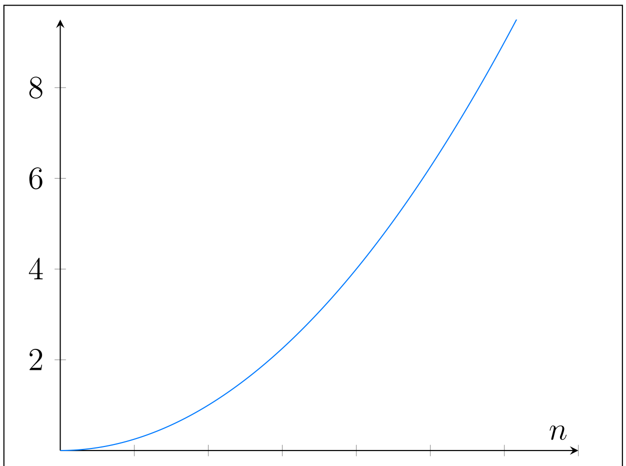
$\{p \to q, q \to r\} \to (p \to r)$

p	q	r	$p \to q$	$q \to r$	$(p \to q) \wedge (q \to r)$	$p \to r$	$((p \wedge q) \wedge (q \to r)) \to (p \to r)$
1	1	1	1	1	1	1	1
1	1	0	1	0	0	0	1
1	0	1	0	1	0	1	1
1	0	0	0	1	0	0	1
0	1	1	1	1	1	1	1
0	1	0	1	0	0	1	1
0	0	1	1	1	1	1	1
0	0	0	1	1	1	1	1

- Lógica de propiedades

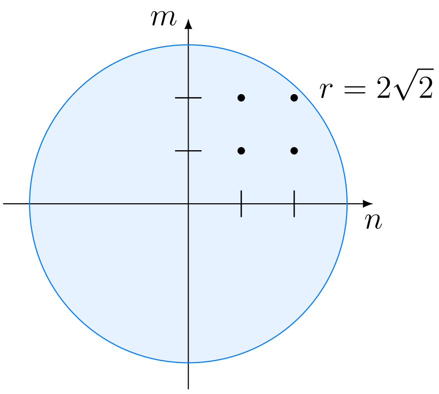
Si $n \geq 3$ entonces $n^2 > 4$.

$$\mathbb{N} = \{1, 2, 3, \ldots\} \qquad P(n) = n^2 > 4 \begin{cases} P(1) = 1 > 4 & 0 \\ P(2) = 4 > 4 & 0 \\ P(3) = 9 > 4 & 1 \end{cases}$$



– Conjunto de verdad: conjunto de elementos que verifica $P(n)$.

$P(n,m) \qquad T_P = \{(1,1),(1,2),(2,1),(2,2)\}$



$n, m \in \mathbb{N}, \quad P(n) \quad n^2 < 4 \qquad T_P = \{1\}$

$Q(m), \ 2m \geq 3 \qquad T_Q = \{2, 4, \ldots\}$

$[\exists n P(n)] \land [\forall m Q m]$ es 0

$[\exists n P(n)] \lor [\forall m Q m]$ es 1

$\neg\, [\exists n P(n)] \land [\forall m Q m]$ es 0

$$\boxed{\begin{array}{l} \neg\,(\exists n P(n)) \equiv \forall n \neg P(n) \\[1em] \neg\,(\forall n P(n)) \equiv \exists n \neg P(n) \end{array}}$$

$\exists n \exists m P(n,m)$ es 1 $\qquad \forall n \forall m \neg\,(P(n,m)) \equiv \neg\,(\exists n \exists m P(n,m))$

$\forall n \forall m P(n,m)$ es 0 $\qquad \exists n \exists m \neg\,(P(n,m)) \equiv \neg\,(\forall n \forall m P(n,m))$

$\exists n \forall m P(n,m)$ es 0 $\qquad \forall n \exists m \neg\,(P(n,m)) \equiv \neg\,(\exists n \forall m P(n,m))$

$\forall n \exists m P(n,m)$ es 1 $\qquad \exists n \forall m \neg\,(P(n,m)) \equiv \neg\,(\forall n \exists m P(n,m))$

- Ejercicios 26/09/23

17) $[(p \land q) \longleftrightarrow (\lor \neg r)] \lor p$

$$(\neg p \lor q) \land (\neg q \lor p) \equiv ((\neg p \lor q) \land \neg q) \lor ((\neg p \lor q) \land p) \equiv \overbrace{(\neg p \land \neg q \lor \underbrace{q \land \neg q}_{0})}^{\neg p \land \neg q \equiv \neg(p \lor q)} \lor (\overbrace{\underbrace{\neg p \land p}_{0} \lor p \land q}^{p \land q})$$

p	q	r	$\neg r$	$p \land q$	$p \lor \neg r$	$(p \land q) \longleftrightarrow (p \lor \neg r)$	$[(p \land q) \longleftrightarrow (p \lor \neg r)] \lor p$
1	1	1	0	1	1	1	1
1	1	0	1	1	1	1	1
1	0	1	0	0	1	0	1
1	0	0	1	0	1	0	1
0	1	1	0	0	1	0	0
0	1	0	1	0	0	1	1
0	0	1	0	0	1	0	0
0	0	0	1	0	0	1	1

Tema 2: Conjuntos

Un conjunto es una colección de objetos (elementos).

$a \in A$

$\mathbb{N} = \{1, 2, \ldots\}$	$A = \{1, 2, 3\} = \{n \in \mathbb{N} : n < 4\}$
$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$	$B = \{n \in \mathbb{N} : n > 4\} = \{5, 6, \ldots\}$

Dados A y B conjuntos:

$A \subseteq B$ si $\forall\ a \in A$ se cumple que $a \in B$

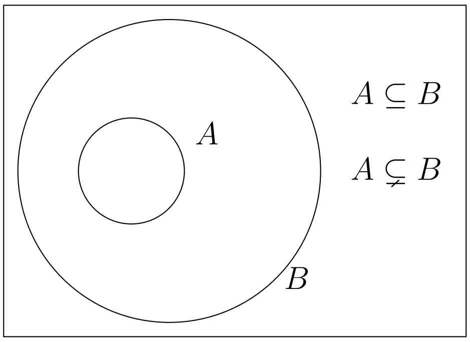
$A = B$ si $A \subseteq B$ y $B \subseteq A$

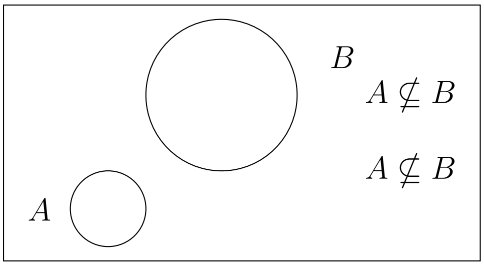
$A \subsetneq B$ (no está contenido).

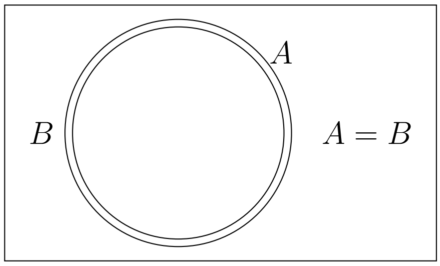
$A \neq B$ (es distinto de).

Si $A \subseteq B$ y $A \neq B \longrightarrow A \subsetneq B$

Diagrama de Venn.



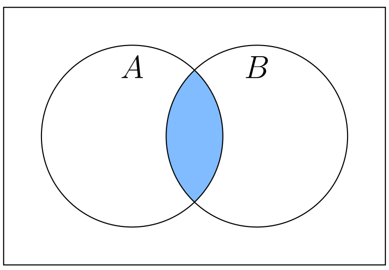




Operaciones

- Intersección: $A \cap B = \{x : x \in A \wedge x \in B\}$
- Unión: $A \cup B = \{x : x \in A \vee x \in B\}$
- Complementario: $A^c = \{x \in \mathrm{U} : \underbrace{x \notin A}_{\neg(x \in A)}\}$

$A \cup B = \varnothing \qquad A \cup \mathrm{U}$ Conjunto universal $= A$

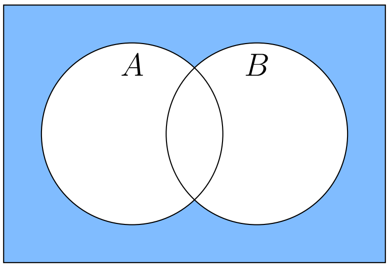


$A \cup \varnothing = A$

$A \cap \varnothing = \varnothing$

Álgebra de conjuntos

- Leyes idempotentes $\quad A \cup A = A \quad A \cap A = A$
- Leyes asociativas $\quad A \cup (B \cup C) = (A \cup B) \cup C \quad A \cap (B \cap C) = (A \cap B) \cap C$
- Leyes conmutativas $\quad A \cup B = B \cup A \quad A \cap B = A \cap B$
- Leyes distributivas $\quad A \cup (B \cap C) = (A) \cap B) \cup (A \cap C) \quad A \cap (B \cup C) = (A) \cup B) \cap (A \cup C)$
- Leyes de identidad $\quad A \cup \varnothing = A \quad A \cup \mathrm{U} = \mathrm{U} \quad A \cap \varnothing = \varnothing \quad A \cap \mathrm{U} = A$
- Leeys de involución $\quad (A^c)^c = A$
- Leyes de complementos $\quad A \cup A^c = \mathrm{U} \quad \mathrm{U}^c = 0 \quad A \cap A^c = \varnothing \quad \varnothing^c = \mathrm{U}$
- Leyes de DeMorgan $\quad (A \cup B)^c = A^c \cap B^c \quad (A \cap B)^c = A^c \cup B^c$



$(A \cup B)^c = A^c \cap B^c$

$(A \cup B)^c = A^c \cap B^c$

$A^c \cap B^c \subseteq (A \cup B)^c$

$x \in (A{\cup}B)^c \rightarrow x \notin A{\cup}B \rightarrow x \notin A{\wedge}x \notin B \equiv x \in A^c,\ x \in B^c \rightarrow x \in A^c{\cap}B^c$

Diferencia

$A \backslash B = \{x \in \mathrm{U} : x \in A \wedge x \notin B\} \equiv A \cap B^c$

$A^C = \mathrm{U} \backslash A$

$A = \{1, 2\}$

$B = \{2, 3\}$

$\underset{\{4\}}{A \backslash B} \neq \underset{\{3\}}{B \backslash A}$

$a, A, \subseteq, =, \cap, \cup, \backslash, A^c$

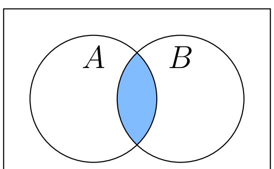
Principio de inducción-exclusión

Dado A conjunto, $|A|$ es el número de elementos de A.

Si $A,\ B$ son finitos, entonces $|A \cup B| = |A| - |B| - |A \cap B|$

- Demostración

Caso 1. $A \cap B = \varnothing \longrightarrow |A \cup B| = |A| + |B|$



$$\text{Caso 2. } A \cap B \neq \varnothing \qquad A \cup B = \begin{matrix} A \cup (B \backslash A) \\ A \cap (B \backslash A) = \varnothing \end{matrix} \longrightarrow |A \cup B| = |A| + |B \backslash A|$$

- Ejemplo

50 alumnos

28 tienen IPHONE $|A| = 28 \qquad |A \cap B| = 28 + 33 - 50 = 5$

20 tiene el MALO CARO $|B| = 20$

13 tienen el MALO BARATO $|C| = 13 \qquad |A \cup B \cup C| = 50$

$|A \cap B \cap C| = ?$

$$\begin{aligned} |(A \cup B) \cup C| &= |A \cup B| + |C| - |(A \cup B) \cap C| \\ &= |A| + |B| - |A \cap B| + |C| - (|A \cap C| + |B \cap C| - |\overbrace{A \cap \underbrace{C \cap B \cap C}_{C \cap C = C}}^{A \cap B \cap C}|) \\ &= |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C| = |A \cup B \cup C| \\ &50 = 28 + 20 + 13 - 7 - 5 - 4 + |A \cap B \cap C| \longrightarrow |A \cap B \cap C| = 5 \end{aligned}$$

Relaciones

$A,\ B \longrightarrow$ producto cartesiano

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

$A = \{1, 2\}$

$B = \{3, 4\}$

$R = \{(1,3), (1,4), (2,3), (2,4)\}$

Si A y B son finitos $\longrightarrow |A \times B| = |A| \cdot |B|$

Si $A = B \longrightarrow A \times A = A^2$

Una relación $\sim$ es un subconjunto de $A \times B$.

Si $A = B, \ \sim$ es una relación sobre A.

- Ejemplos

$R = \{(2,3).(2,4)\}$

$2 \sim 3$

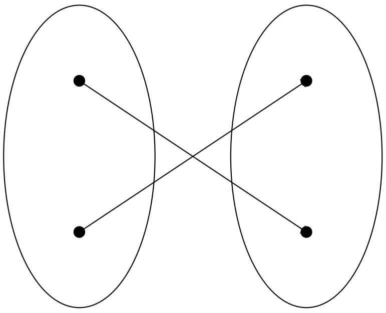
$1 \nsim 3$

$R^2 = R \times R$

$f(x) = x^2$

Una función es una relación R en $A \times B$ de manera que que $\forall a \in A$

$\exists$ un único $b \in B$ tal que $\underset{a \sim b}{(a,b) \in R} \longleftrightarrow$ Si $(a,b_1) \in R$ y $(a,b_2) \in R \longrightarrow b_1 = b_2$



Sea R relación sobre A. $(R \subseteq A \times A)$

R puede ser:

1) Reflexiva si $a \sim a \quad \forall a \in A$.

2) Simétrica si $\forall a_1, a_2 \in A$ tal que $a_1 \sim a_2$ se cumple que $a_2 \sim a_1$.

3) Antisimétria si $\forall a_1, a_2 \in A$ tal que $a_1 \sim a_2$ $(a_1 \sim a : 2 \wedge a_2 \sim a_1 \longrightarrow a_1 = a_2)$ se cumple que $a_2 \nsim a_1$

4) Transitiva si $\forall a_1, a_2, a_3 \in A$ tal que $a_1 \sim a_2$ y $a_2 \sim a_2$ tal que $a_1 \sim a_3$.

Relación de equivalencia

Una relación R sobre un conjunto $A \neq \varnothing$ es de equivalencia si es:

- Reflexiva $a \sim a \; \forall a \in A$

- Simétrica si $a \sim b \to b \sim a \; \forall a, b \in A$

- Transitiva si $a \sim b$ y $b \sim c \to a \sim c \; \forall a, b, c \in A$

- Ejemplos

1) $\mathbb{N}$ $n \sim m$ si $n - m$ es par

Reflexiva $n \sim n \quad n - n = 0$ es par

Simétrica $n \sim m \to n - m$ es par $\to m - n$ es par $\to m \sim n$.

Transitiva $\quad n \sim m \to n - m$ es par $\qquad \underbrace{n - m} + \underbrace{m - \tilde{n}} = n - \tilde{n}$ es par $\to n \sim \tilde{n}$

$m \sim \tilde{n} \to m - \tilde{n}$ es par

- Clases de equivalencia

$a \in A \qquad [a] := \{b \in A : a \sim b\}$

1) Teorema

R relación de equivalencia entre $A \neq 0$ $\forall a, b \in A$ o bien $\underbrace{[a] = [b]}_{a \sim b}$ o bien $\underbrace{[a] \cap [b] = \varnothing}_{a \nsim b}$.

- Demostración

Sea $a, b \in A,\ a \neq b \begin{cases} a \sim b \\ a \nsim b \end{cases}$

$a \sim b \to ?`[a] = [b]?$

$[a] \subseteq [b]$. Sea $x \in [a] \to \left.\begin{matrix} a \sim c \\ b \sim a \end{matrix}\right\} \to b \sim c \to c \in [b]$

$a \nsim b$ Reducción al absurdo. $(p \to q \equiv \neg q \to \neg p)$

Sea $c \in [a] \cap [b] \neq \varnothing \to \left.\begin{matrix} c \in [a] \to a \sim c \\ c \in [b] \to b \sim c \to c \sim b \end{matrix}\right\} \to a \sim b$

Relación de Orden

Una relación R sobre $A \neq \varnothing$ se dice de orden si cumple.

- Relación reflexiva
- Relación transitiva
- Relación antisimétrica. Si $a \sim b \to b \nsim a$ $\forall a, b \in A$.

- Ejemplo

$\mathbb{N}$ $\quad n \leq m$ si n divide m. $(n|m) \leftrightarrow \exists k \in \mathbb{N}$ tal que $n \cdot k = m$

- Reflexiva: $n \cdot 1 = n \to n|n \to n \leq n$.

- Antisimétrica: $\quad n \leq m \to n|m \to \exists k_1 \in \mathbb{N}$ tal que $n \cdot k_1 = m$

  $m \leq n \to m|n \to \exists k_2 \in \mathbb{N}$ tal que $m \cdot k_2 = n$

  $m \cdot k_1 \cdot k_2 = m \to k_1, k_2 = 1 \to k_1 = k_2 = 1$

- Transitiva: $\left.\begin{matrix} n \leq m \to \exists k_1 \in \mathbb{N} \text{ tal que } n \cdot k_1 = m \\ n \leq \tilde{n} \to \exists k_2 \in \mathbb{N} \text{ tal que } m \cdot k_2 = \tilde{n} \end{matrix}\right\} \to n\underbrace{(k_1 \cdot k_2)}_{\in \mathbb{N}} = \tilde{n} \to n|\tilde{n} \to n \leq \tilde{n}$

Relación de orden parcial

$(\mathbb{N}, \underset{\text{orden usual}}{\leq})$ Relación de orden total

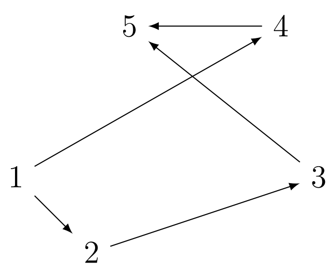
$n \leq m \leftrightarrow \exists k \in \mathbb{N} \cup \{0\}$ tal que $n + k = m$

Una relación R sobre $A \neq \varnothing$ y A finito.

Diagramas de Hasse

$A = \{1, 2, 3, 4, 5\}$

$R = \{(1,1), (1,2)^{(1,3)};(1,4)^{(1,5)};(2,2), (2,3)^{(2,5)};(3,3), (3,5), (4,4), (5,5), (4,5)\}$



$$\left.\begin{array}{l} 1 \leq 2 \\ 2 \leq 3 \end{array}\right\} \to 1 \leq 3$$

Relación de orden sobre $A \neq \varnothing$ $\quad B \subseteq A$

$a \in A$

a es supremo de B si $b \leq a$ $\forall b \in B$

a es cota inferior de B si $a \leq b$ $\forall b \in B$

a es supremo de B si es la menor cota superior

a es ínfimo de B si es la myor cota inferior

a es máximo de B si es supremo de B y $a \in B$ a es mínimo de B si es ínfimo de B y $a \in B$

$A = \{1, 2, 3, 4, 5, 6, 9, 12\}$ $n \leq m$ si $n | m$

$B = \{1, 2, 3\}$

Cota superior $= \{6, 12\}$

$b \in B$ es maximal si

$\nexists a \in B$ tal que $b \leq a$ $\leftarrow$ Elemento maximal $\to \boxed{\text{C.S}} \to S \to$ max

$b \in a$ es minimal si

$\nexists a \in B$ tal que $a \leq b$

Principio de inducción

$1 + 3 + 5 + \cdots + 2n - 1 = n^2$

1

$1+1=2$

$2+1=3$

$3+1=4$

$\vdots$

$= n$

$n+1$

$\mathbb{N} = P(n) = \{n \in \mathbb{N} : 1+3+5+\cdots+2n-1 = n^2 \text{ es V}\}$

- $1 \in P(m)$. $\quad 1 = 1^2$
- Si $n \in P(m) \to n+1 \in P(m)$ $\quad$ ¿$1+3+\cdots+\underbrace{2n+1}_{2(n+1)-1} = (n+1)^2$?

$\underbrace{1+3+5+\cdots+2n-1}+2n+1 = n^2+2n+1 = (n+1)^2$

- Ejercicios 27/09/2023

28)

$X = \{1,2,3,4,5\}$

a) $(\exists x(x+3=18)) \equiv \forall x(x+3 \neq 10)$

b) $\forall x(x+3<10)$ es 1

c) $\exists x(x+3<10)$ es 1

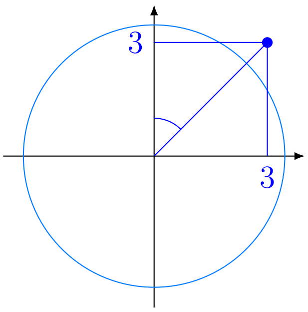
d) $\forall x(x+3 \leq 7)$ es 0 $\exists x(x+3>7)$ es 1

29)

$X = \{1,2,3\}$

a) $\exists x \forall y(x^2 < y+1)$ $\quad x=1$ $\quad 1 < y+1$

b) $\forall x \exists y(x^2+y^2<12)$



c) $\neg(\forall x \forall y(x^2+y^2<12)) \equiv \exists x \exists y(x^2+y^2<12)$

31) $\exists x P(x) \wedge Q(x)$

a) $\forall x P(x) \longleftrightarrow Q(x)$ es 1 $\quad \nearrow \ \forall x \neg P(x) \wedge \neg Q(x)$ $\quad$ ($P(x)$ y $Q(x)$ sean falsa)

$\searrow \ \exists x P(x) \wedge Q(x)$

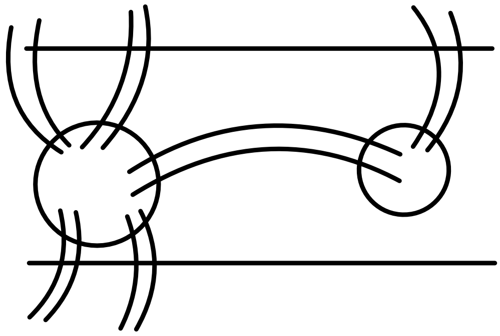
b) $P(a) \vee Q(b) \equiv \exists a \exists b \quad P(a) \vee Q(b)$

32) $\exists x Q(x) \equiv \forall x Q(x)$

a) $\forall x \exists y P(y) \rightarrow Q(x)$

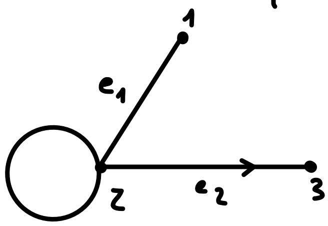
b) $P(a) \vee Q(b)$

Tema 3: Teoría de grafos



Konisberg

Un grafo $G=(V,E)$ es un par de conjuntos, V vértices y E aristas de forma que cada arista une un par de vértices

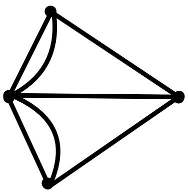


$V=\{1,2,3\}$

$E=\{e_1,e_2\}$

Orden de G es $|V|$

- **Tipos de grafos:**
  - Multigrafos
  - Grafo simple
  - Pseudografo
  - Grafos dirigidos
  - Grafos no dirigidos !!



(*) =
$$\begin{array}{r} \deg(1)=1 \\ +\ \deg(3)=1 \\ \deg(2)=4 \\ \hline 6=2|E| \end{array}$$

$v\in V$, se llama grado de v al número de aristas, que salen o entran en v.

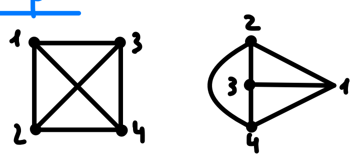
$\deg(v)$ (*)

- **Teorema (Apretón de manos)**

Dado un grafo $G=(V,E)$, se cumple que

$$\sum_{v\in G} \deg(v) = 2|E|$$

Ejemplo



Son el mismo grafo

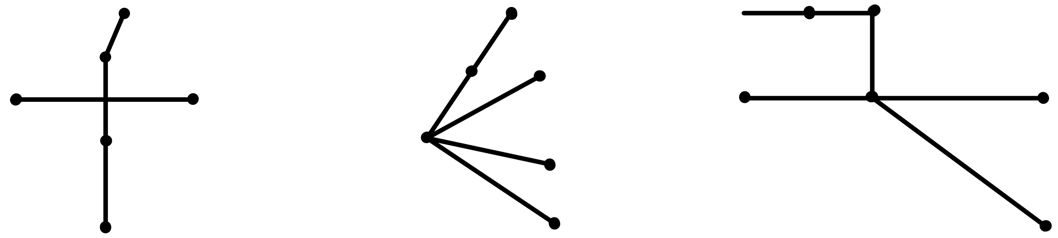
Isomorfo

(1,3)	(2,3)		(1,2)	(2,4)
(1,4)	(2,4)	≡	(1,3)	(2,3)
(1,2)	(3,4)		(1,4)	(3,4)

Dos grafos $G=(V,E)$ y $G'=(V',E')$ se dicen **isomorfos** si existe una aplicación biyectiva $f: V \longrightarrow V'$ de forma que para cada par $u,v\in V$, $f(u), f(v) \in V'$ son unidos por el mismo número de aristas.

Dado un grafo $G=(V,E)$, un subgrafo de G es un grafo $G'=(V',E')$ tal que $V'\subseteq V$ y $E'\subseteq E$.

Dos grafos $G=(V,E)$ y $G'=(V',E')$ se dicen **homeomorfo** si se construyen a partir de un mismo grafo añadiendo vértices en sus aristas.

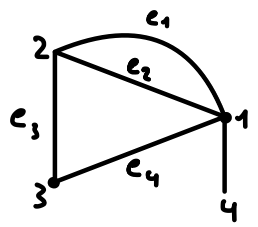


Dos vértices u, v son adyacentes si existe una arista que los una.

Un camino es una sucesión

$$u_1, e_1, u_2, e_2, \ldots, u_k, e_k, u_{k+1} \qquad u_i \in V \quad i=\{1,2,\ldots,k+1\}$$

→ La longitud del camino es el nº de aristas. $\qquad e_i \in E \quad i=\{1,2,\ldots,k\}$



$1, e_1, 2, e_3, 3, \ldots$

$3, e_4, 1, e_2, 2, \ldots$

→ Un camino es **simple** cuando no se repite ningún vértice.

→ Camino simple y cerrado: **ciclo**

→ Si no se repite ninguna arista: **recorrido**

$G=(V,E)$ aristas

vértices

$v_1, e_1, v_2, e_2, \ldots, v_n, e_n, v_{n+1}$ camino

- Cerrado $(v_1 = v_{n+1})$

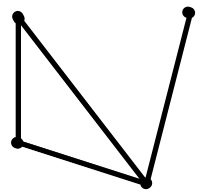
⊕ Simple si $v_i \neq v_j \quad i\neq j$

- Cerrado y simple: **ciclo**

⊕ Recorrido si $e_i \neq e_j \quad i \neq j$

Un grafo es conexo si:

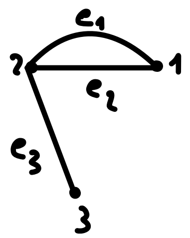
- $\forall u, v \in V$ existe un camino que los une



- Si el grafo no es conexo, se llama componente conexa a un subgrafo conexo que no está contenido en ningún subgrafo mayor que él.

- **Propiedad:**

Sea $G = (V, E)$ un grafo y sean $u, v \in V$ unidos por un camino. Entonces existe un camino simple que los une



$1, e_1, 2, \underbrace{e_2, 1, e_1, 2,}\, e_3, 3$

$1, e_1, 2, e_3, 3$

- **Demostración**

Sea $u = v_1, e_1, v_2, e_2, \dots, v_{n-1}, e_{n-1}, v_n = v$ un camino

1) Es simple. FIN

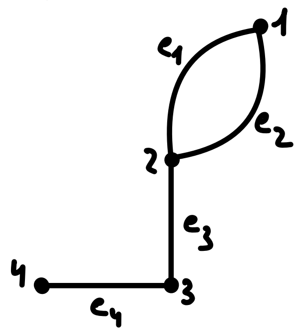
2) No es simple:

 - Sea $i := \min\{K \in \{1, \dots, n\} : v_i = v_j \text{ para algún } j > i\}$
 - Sea $\ell := \max\{K \in \{i+1, \dots, n\} : V_K = V_i\}$

$u, \dots, e_{i-1}, v_i, \cancel{\boxed{e_i, v_{i+1}, \dots, v_\ell,}}\ e_\ell, \dots, v$

- **Puentes y puntos de corte**

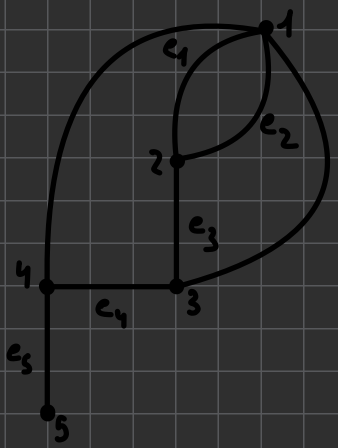
Un puentes es una arista e de forma que $G' = \{V, E \setminus \{e\}\}$ no es conexo.



Un punto de corte es un vértice $u \in V$ tal que que el subgrafo $G' = \{V \setminus \{u\}, E \setminus E_u\}$ no es conexo, donde

$E \setminus E_u$: {Conjunto de vértices que no acaban ni terminan en u.}

El diámetro es la mayor distancia entre 2 vértices (diam(G))



$d(1,3) = 1$

$d(1,5) = 2$

- Grafos Eulerianos

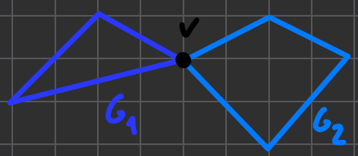
Un grafo conexo $G(V,E)$ es Euleriano si existe un recorrido cerrado de longitud $|E|$.

- Lema

Sea $G(V,E)$ un grafo conexo compuesto por dos subgrafos Eulerianos con al menos un vértice en común y que no compartan aristas. Entonces G es euleriano.

- Demostración

Sea v un vértice común. G_1 y G_2 los dos subgrafos



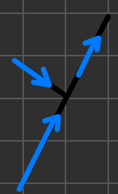
- Teorema de Euler

Sea $G=(V,E)$ un grafo conexo. G es euleriano si y solo si

$$\deg(v) = \text{par} \ \forall v \in V$$

- Demostración

Si $\deg(V)$ es impar por algún $v \in V$, no puede ser euleriano



Suponemos que $\deg(v)$ es par $\forall v \in V$

$$v_1, e_1, \ldots, v_n, e_n, v_{n+1} = v_1$$

Tema 4: Aritmética (modular)

$(\mathbb{Z}, +, \cdot)$ Anillo

$+$ Asociativa, comunicativa, elemento neutro (0), elemento $\overset{\text{inverso}}{\text{simétrico}}$ $(n + \overset{n-n}{(-n)} = 0)$

$\cdot$ Asociativa, comunicativo, elemento neutro (1), distributivo respecto de la suma $n \cdot (m + \tilde{n}) = n \cdot m + n \cdot \tilde{n}$

$n \cdot 0 = 0$

$n \cdot 0 + \cancel{n \cdot 0} = n \cdot (0 + 0) = \cancel{n \cdot 0}$

Divisibilidad

- Algoritmos de la división

Dados $p, 1 \in \mathbb{N} \backslash \{0\}$. Existe d y r, $r < q$, $d, r \in \mathbb{N}$, únicos de forma que $p = q \cdot d + r$

- Demostración

$d = \max\{n \in \mathbb{N} : q \cdot n \leq p\} \to q \cdot d \leq p < q(d+1)$

$p < qd + q \to \exists \underset{r<q}{r \text{ tal que}}\ p = q \cdot d + r$

Suponemos que $\exists d_1, d_2, \underbrace{r_1, r_2}_{<q}$ tal que:

$$\begin{matrix} p = d_1 \cdot q + r_1 \\ p = d_2 \cdot q + r_2 \end{matrix} \longrightarrow \underset{>0}{q} \underset{\geq 0}{(d_1 - d_2)} = r_2 - r_1 \to r_2 \geq r_1$$

1) $d_1 = d_2 \to r_2 = r_1$

2) $d_1 > d_2 \to d_1 - d_2 \geq 1 \to \left.\begin{matrix} r_2 - r_1 \geq q \\ r_1 < q \end{matrix}\right\} \longrightarrow r_2 < q$ Contradicción

Si $r = 0$ se dice que p divide a q, $p|q$.

p es divisor de q.

$$\begin{matrix} p|q & 2|4 \\ \updownarrow & 3\not|4 \\ \exists d \text{ tal que} & p = q \cdot d \end{matrix}$$

- Proposición

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

a) Si $a|b \to a|b \cdot c$

b) Si $a|b$ y $b|c \to a|c$

c) Si $a|b$ y $a|c \to a|b \cdot x + c \cdot y\ \forall x, y \in \mathbb{Z}$

d) Si $a, b \in \mathbb{N}\backslash\{0\}$ y $a|b \to a \leq b$

e) Si $a|b$ y $b|a \to a = b$ ó $a = -b$

- Demostración

a) $a|b \to \exists d \in \mathbb{Z}$ tal que $a \cdot d = b \to a \cdot (d \cdot c) = b \cdot c \to a|b \cdot c$

b) $\left.\begin{array}{l} a|b \to \exists d_1 \in \mathbb{Z} \text{ tal que } a \cdot d_1 = b \\ b|c \to \exists d_2 \in \mathbb{Z} \text{ tal que } b \cdot d_2 = c \end{array}\right\} \to a\,\underbrace{d_1 \cdot d_2}_{\in\mathbb{Z}} = c \to a|c$

c) $\left.\begin{array}{l} a|b \to \exists d_1 \in \mathbb{Z} \text{ tal que } a \cdot d_1 = b \\ a|c \to \exists d_2 \in \mathbb{Z} \text{ tal que } a \cdot d_2 = c \end{array}\right\} \to \begin{array}{c} a \cdot d_1 \cdot x = bx \\ a \cdot d_2 \cdot y = cy \end{array}$

$a(d_1x + d_2y) = bx + cy \to a|bx + cy$

d) $a|b \to \exists d \in \mathbb{N}$ tal que $a \cdot d = b$

$d \geq 1 \to a \cdot d \geq a$

e) $a|b \to \exists d_1 \in \mathbb{Z}$ tal que $a \cdot d_1 = b$

$b|a \to \exists d_2 \in \mathbb{Z}$ tal que $b \cdot d_2 = a$

- Algoritmo de Euclides

$d = \gcd(a, b)$ si d es el mayor número natural tal que $d|a$ y $d|b$

$\gcd(16, 6) = 2$

$$\begin{array}{r|l} 16 & 2 \\ 8 & 2 \\ 4 & 2 \\ 2 & 2 \\ 1 & \end{array} \qquad \begin{array}{r|l} 6 & 2 \\ 3 & 3 \\ 1 & \end{array}$$

- Proposición

$a, b \in \mathbb{N},\ a < b (a \lneq b)$ y sean d y $r,\ r < a$ tales que $b = a \cdot d + r$. Entonces $\gcd(a, b) = \gcd(r, a)$

$$\begin{array}{ll} \gcd(868,747) & 868 = 747 \cdot 1 + 121 \\ \gcd(747,121) & 747 = 121 \cdot 6 + 21 \\ \gcd(121,21) & 121 = 21 \cdot 5 + 16 \\ \gcd(21,16) & 21 = 16 \cdot 1 + 5 \\ \gcd(16,5) & 16 = 5 \cdot 3 + 1 \\ \gcd(5,1) & 5 = 1 \cdot 5 + 0 \end{array}$$

- Demostración

$$\text{Sea } d_1 \to \left.\begin{array}{l} d_1|a \\ d_1|b \end{array}\right\} \to d_1|b + (-d) \cdot a = r \to \gcd(a,r) \geq d_1$$

$$\text{Sea } d_2 = \gcd(a,r) \to \left.\begin{array}{l} d_2|a \\ d_2|r \end{array}\right\} \to a \cdot d + r = b \to d_2 \leq \gcd(a,b)$$

Teorema de Bezout

Sean $a, b \in \mathbb{Z} \backslash \{0\}$ y $d = \gcd(a,b)$. Entonces d es el menor enterio positivo tal que $d = a \cdot x + b \cdot y,\ x, y \in \mathbb{Z}$.

- Demostración

$a, b \in \mathbb{N} \backslash \{0\}$

$$\underset{M \neq \varnothing}{M} = \{\underset{a \in M}{m \in \mathbb{N} \backslash \{0\}}; \exists x, y \in \mathbb{Z} \text{ tal que } \underset{a = a \cdot 1 + b \cdot 0}{m = a \cdot x + b \cdot y}\} \subseteq \mathbb{N}$$

$$\begin{array}{l} d = \min M \\ c = \gcd(a,b) \end{array} \quad ¿c = d?$$

1) $d|a$ (y $d|b$)

Suponemos que $d \nmid a \to \exists p \in \mathbb{Z}$ y $0 < r < d$ tal que $\begin{array}{c} a = p \cdot d + r \\ d = a \cdot x + b \cdot y \end{array}$

$$r = a - p \cdot d = a - p(a \cdot x + b \cdot y) = a \underbrace{(1 - px)}_{\in \mathbb{Z}} - b \cdot \underbrace{p \cdot y}_{\in \mathbb{Z}} \to \begin{array}{c} r \in M \\ r < d \\ d = \min M \end{array}$$

$$\left.\begin{array}{l} d|a \\ d|b \end{array}\right\} c \geq d$$

$$¿c \leq d? \qquad \left.\begin{array}{l} c|a \\ c|b \end{array}\right\} \to c|ax + by = d \to \left.\begin{array}{l} c \leq d \\ c \geq d \end{array}\right\} \to c = d$$

$$\begin{aligned} \gcd(134,298) &\quad 298 = 134\cdot 2 + 30 \\ \gcd(30,134) &\quad 134 = 30\cdot 4 + 14 \\ \gcd(14,30) &\quad 30 = 14\cdot 2 + 2 \\ \gcd(2,14) &\quad 14 = 2\cdot 7 + 0 \end{aligned}$$

$\exists x, y \in \mathbb{Z}, \quad 2 = 134\cdot x + 298\cdot y$

$$\begin{aligned} 2 &= 30 - 2\cdot 14 \\ &= 30 - 2\cdot(134 - 4\cdot 30) \\ &= (-2)\cdot 134 + 9\cdot 30 \\ &= (-2)\cdot 134 + 9\cdot(298 - 2\cdot 134) \\ &= \underset{y}{9}\cdot 928 + (\underset{x}{-20})\cdot 134 = 2 \end{aligned}$$

Algoritmo de Euclides Extendido

$\gcd(a,b)$

$a < b$

$$\left(\begin{array}{c|cc} a & 1 & 0 \\ b & 0 & 1 \end{array}\right) \xrightarrow{F_2 - F_1\cdot d} \left(\begin{array}{c|cc} a & 1 & 0 \\ V & d & 1 \end{array}\right) \xrightarrow{F_1 \times F_2} \left(\begin{array}{c|cc} V & d & 1 \\ a & 1 & 0 \end{array}\right)$$

$b = a\cdot d + r$ $\qquad$ 1) $r = 0 \qquad a = \gcd(b,a)$

$$\left(\begin{array}{c|cc} 134 & 1 & 0 \\ 298 & 0 & 1 \end{array}\right) \xrightarrow{F_2 - 2\cdot F_1} \left(\begin{array}{c|cc} 134 & 1 & 0 \\ 30 & -2 & 1 \end{array}\right) \xrightarrow{F_1 \times F_2} \left(\begin{array}{c|cc} 30 & -2 & 1 \\ 134 & 1 & 0 \end{array}\right) \xrightarrow{F_2 - 4\cdot F_1} \left(\begin{array}{c|cc} 30 & -2 & 1 \\ 14 & 9 & -4 \end{array}\right) \xrightarrow{F_1 \times F_2}$$

$$\left(\begin{array}{c|cc} 14 & 9 & -4 \\ 30 & -2 & 1 \end{array}\right) \xrightarrow{F_2 - 2F_1} \left(\begin{array}{c|cc} 14 & 9 & -4 \\ 2 & -20 & 9 \end{array}\right) \xrightarrow{F_1 \times F_2} \left(\begin{array}{c|cc} 2 & -20 & 9 \\ 14 & 9 & -4 \end{array}\right) \xrightarrow{F_2 - 7F_1} \left(\begin{array}{c|cc} 2 & -20 & 9 \\ 0 & - & -\,- \end{array}\right)$$

- Propiedad

$a \sim b \longleftrightarrow$ Los restos resultatnes de dividir a y b por m son iguales

- Demostración

$a \sim b \longrightarrow m|a-b \longrightarrow \exists p$ tal que $m \cdot p = a - b$

$$\begin{array}{r} a = mp_1 + r_1 \\ b = mp_2 + r_2 \\ \hline a - b = m\underbrace{(p_1 - p_2)}_{p} + \underbrace{(r_1 - r_2)}_{0 \to r_1 = r_2} \end{array} \qquad \begin{array}{c} a = mp_1 + r \\ b = mp_2 + r \\ \hline \end{array}$$

$$\begin{array}{c} \mathbb{Z}_m \\ \overline{a}, \overline{b} \end{array} \left\} \begin{array}{l} \overline{a} + \overline{b} = \overline{a+b} \\ \overline{a} \cdot \overline{b} = \overline{a \cdot b} \end{array} \right.$$

En $\mathbb{Z}_{16}$

$$\overline{7} + \overline{10} = \overline{17} = \overline{1}$$

$$\overline{7} \cdot \overline{10} = \overline{70} = \overline{6}$$

- Propiedad

En $\mathbb{Z}_n$ $+$ y $\cdot$ están bien definidas

- Demostración

$$\left. \begin{array}{l} a = mp_1 + r_1 \\ b = mp_2 + r_2 \\ \hline a + b = m \cdot (p_1 + p_2) + (r_1 + r_2) \end{array} \right\} \longrightarrow a \cdot b = \begin{array}{l} a \cdot b \sim r_1 \cdot r_2 \\ m(p_1p_2 + p_1r_2 + p_2r_1) + r_1r_2 \end{array}$$

$\mathbb{Z}_2$

$+$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$

$\cdot$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$

$\mathbb{Z}_3$

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

$\mathbb{Z}_4$

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

$m \in \mathbb{N}\backslash\{0,1\}$

$a \sim b \longleftrightarrow m|a-b \rightarrow \mathbb{Z}_m$

$\mathbb{Z}_4 \quad 2\cdot 2 = 0$

$a \in \mathbb{Z}_m$ es invertible si existe $a^{-1} \in \mathbb{Z}_m$ tal que $a \cdot a^{-1} = 1$.

- Teorema

Dado $m \in \mathbb{N}\backslash\{0,1\}$, entonces:

1) a es invertible en $\mathbb{Z}_m$ si y sólo si $\gcd(m,a) = 1$ a no es invertible en $\mathbb{Z}_m$ si y sólo si $\exists b \in \mathbb{Z}_m\backslash\{0\}$ tal que $a \cdot b = 0$

- Demostración

1) " $\Longrightarrow$ " $\exists a^{-1} \in \mathbb{Z}_m$ tal que $a \cdot a^{-1} = 1(\mod m) \longrightarrow m|aa^{-1}-1 \longrightarrow \exists k \in \mathbb{Z}$ tal que $aa^{-1-1=m\cdot k}$
$\longrightarrow a\,a^{-1} - m\,k = 1 \longrightarrow \gcd(a,m) = 1$ Teorema de Bezout

" $\Longleftarrow$ " $1 = ap + mp \longrightarrow m|ap-1 \longrightarrow ap \equiv 1(\mod m) \longrightarrow p = a^{-1}$

- Función de Euler

$$m \in \mathbb{N}\backslash\{0,1\} \qquad \varphi(m) = |A \cdot m|$$

$$A_m = \{n \in \{1,\ldots,m-1\} : \gcd(n,m) = 1\}$$
$$= \{n \in \{1,\ldots,m-1\} : n \text{ es invertible en } \mathbb{Z}_m\}$$

- Proposición

1) Si p es primo $\varphi(p) = p-1$

2) Si p es primo, $\varphi(p^k) = p^k - p^{k-1}$

3) Si $\gcd(n,m) = 1$, entonces $\varphi(n \cdot m) = \varphi(n)\cdot\varphi(m)$

- Demostración

1)

2)

3) $|A_n \cdot m| = |A_n| \cdot |A_m| = |A_n \times A_m|$

$f : A_{n\cdot m} \longrightarrow A_n \times A_m$ biyectiva

$k \in A_{n\times m}$

$k_1 \equiv k \pmod n \quad k_1 < n \quad \gcd(k_1, n) = 1?$

$k_2 \equiv k \pmod m \quad k_2 < m \quad \gcd(k_2, m) = 1?$

$f(k) = (k_1, k_2)$

- f bien definida.

  Supongo que:

  $$\gcd(k, n) = d > 1 \xrightarrow[\text{Th. Bezout}]{} \exists\, a, b \in \mathbb{Z} \text{ tal que } d = a \cdot k_1 + b \cdot k_2 = \{k_1 = k + c \cdot n,\ c \in \mathbb{Z}\}$$
  $$= a(k + cn) + bn = a \cdot k + (ac + b)n$$
  $$= \gcd(k, n) \neq 1$$

$$\left.\begin{array}{l} k_1 \equiv k \pmod n \\ k_1 \equiv l \pmod n \end{array}\right\} \longrightarrow k \equiv l \pmod n \longrightarrow n | k - l$$

$$\left.\begin{array}{l} k_2 \equiv k \pmod m \\ k_2 \equiv l \pmod m \end{array}\right\} \longrightarrow k \equiv l \pmod m \longrightarrow m | k - l$$

$\gcd(n, m) = 1 \longrightarrow n \cdot m | k - l$

$k \equiv l \pmod{n \cdot m} \longrightarrow l = k$

- f subinyectiva

  $$\forall\, (k_1, k_2) \in A_n \times A_m \quad \exists\, k \in A_{n\cdot m} \text{ tal que } \begin{array}{l} k \equiv k_1 \pmod n \\ k \equiv k_2 \pmod m \end{array}$$

  $\gcd(n, m) = 1$

  [Teorema chino de los restos]

  $$\exists\, k \text{ tal que } \left\{\begin{array}{l} k \equiv k_1 \pmod n \\ k \equiv k_2 \pmod m \end{array}\right\} \longrightarrow \exists \text{ un único } k < n \cdot m \text{ soluciones de este sistema.}$$

  Suponemos que $\gcd(k, n \cdot m) = d > 1$

  $\gcd(n, m) = \{\text{Algoritmo de Euclídes}\} = \gcd(k, n)$

Sean $a, m \in \mathbb{N} \backslash \{0, 1\}$ tales que $\gcd(a, m) = 1$

Entonces $a^{-1} \equiv a^{\varphi(m)-1} (\operatorname{mod} m)$

- Demostración

En $\mathbb{Z}_m$, $\quad \begin{aligned} A_m &= \{m_1, m_2, \ldots, m_{\varphi(m)}\} \\ B_m &= \{a \cdot m_1, a \cdot m_2, \ldots, a \cdot m_{\varphi(m)}\} \end{aligned}$