

CONJUNTOS:

- Almacenar elementos
- No se consideran repeticiones
- Responde a la pregunta "¿Está el elemento?".
 - ↳ Si
 - ↳ No

PERTENENCIA: Sea X un elemento, decimos que X es miembro de un conjunto A si:

$$\cdot X \in A$$

La relación es de ELEMENTO \in CONJUNTO.

INCLUSIÓN: Sea A un conjunto de los conjuntos.

Decimos que d está incluido en X si y solo si, X posee todos los elementos de d .

- $d \subseteq A$
- se lee:
 - ↳ "d es un subconjunto de A"
 - ↳ "d está incluido en A"
 - ↳ "d está contenido en A"

$$Ej: A = \{1, 2, 3\} \quad d = \{1, 3\}$$

$d \subseteq A$ para $1 \in A$ y $3 \in A$.

Ej: $A = \{1, \{1, 2\}, 3\}$

- $\{1, 2\} \in A$.
- $\{1, 2\} \notin A$ para $1 \in A$ pero $2 \notin A$.

ELEMENTO VACÍO:

- Se representa con \emptyset .
- Esto incluye en todos los conjuntos.

CUANTIFICADORES: Nos permiten hablar de los elementos de los conjuntos

• $\forall x$: "Para todo x "
↳ Para negarla alcanza un solo fallo.

• $\exists x$: "Existe un x "
↳ Para que sea verdadero, alcanza con encontrar un solo verdadero.

Ej: $A = \{2, 4, 6, 8\}$

$\forall x \in A$ se cumple que para que x sea par. ✓

$$\forall x \in A \Rightarrow x = 2k$$

$$A = \{2, 4, 6, 8\}$$

$\exists x \in A$ tal que x es impar. ✓

$$\exists x \in A \wedge x = 2k + 1$$

$$A = \{5, 20, 21\}$$

$\forall x \in A$, todos los x son múltiplos de 5. F, 21 no es múltiplo de 5.

NEGACIONES DEL \wedge & \exists .

OPERACIONES ENTRE CONJUNTOS: Sean A, B conjuntos.

UNIÓN ($A \cup B$): Se unen ambos conjuntos.

De la lógica proposicional, la unión es un "ó" lógico.

- ↳ Si $x \in A \vee x \notin B : V$
- ↳ Si $x \notin A \vee x \in B : V$
- ↳ Si $x \in A \vee x \in B : V$

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

$$A \cup B = B \cup A. \text{ DEMOSTRAR LUEGO DE =}$$

INTERSECCIÓN ($A \cap B$): El nuevo conjunto tiene los elementos que están en ambos conjuntos.

De la lógica proposicional, la intersección es un "y" lógico.

- ↳ Si $x \in A \wedge x \in B : V$
- ↳ Si $x \notin A \wedge x \notin B : F$

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

\neg	$x \in A \wedge x \notin B : F$	V	F
\neg	$x \notin A \wedge x \in B : F$	F	F
\neg	$x \notin A \wedge x \notin B : V$	F	V

COMPLEMENTO: Lo que está en un Conjunto universal V pero no en el Conjunto.

\hookrightarrow De la lógica proposicional, el Complemento es la negación.

- \neg $x \in A : F$
- \neg $x \notin A : V$

A	$\neg A$
V	F
V	F
F	V
F	V

$$A = \{1, 2\} \quad B = \{3, 4, 5\} \quad C = \{3, 9\} \quad V = \{A, B, C\}$$

$$A^c : \{3, 4, 5, 8, 9\}$$

DIFERENCIA ($A - B$): En los mismos que $A \cap B^c$.

En lo que está en A pero No en B .

$\hookrightarrow A - B : x \in A - y \in B : x \in A, \neg x \in B : V$

$$x \in A \wedge y \in B^c : x \in A, \neg x \in B : V.$$

DIFERENCIA SIMÉTRICA ($A \Delta B$): En un Conjunto que tiene a los elementos que están en A ó B pero no en ambos.

En los mismos que:

$\hookrightarrow (A - B) \cup (B - A)$

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

En lógica proposicional: En $P \vee Q$

Y si A y Y si B : F.

Y si A y Y si B : V

Y si A y Y si B : V

Y si A y Y si B : F.

INCLUSIÓN: Sean A, B conjuntos. Se dice que $A \subseteq B$ si todos los elementos de A están en B.

De la lógica proposicional, la " \Rightarrow "

A	B	$A \Rightarrow B$
V	V	V
V	F	F
F	V	V
F	F	V

IGUALDAD: Sean A, B conjuntos no iguales si $A \subseteq B$ y $B \subseteq A$.

En la lógica proposicional corresponde a " \Leftrightarrow ".

A	B	$A \Leftrightarrow B$
V	V	V
V	F	F
F	V	F
F	F	V

IMPLEMENTACIÓN (\Rightarrow): Es falsa si el antecedente es V y consecuente F.

- Para las demostraciones se supone Antecedente V y se trae de ver que Consecuente NO sea falso.

IGUALDAD DE CONJUNTOS: Dos conjuntos son iguales si $A \subseteq B$ y $B \subseteq A$.

LEYES DE DE MORGAN

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

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

PROPIEDADES DE CONJUNTOS:

- DISTRIBUTIVA: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
- COMUTATIVIDAD: $A \cap B = B \cap A$
- CONJUNTOS DISJUNTOS: $A \cap B = \emptyset$

DEMOSTREMOS:

$$\cdot A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

Como es una igualdad ($A=B$) probaremos que $A \subseteq B$ y $B \subseteq A$.

\Rightarrow OBJETIVO: SUPONENDO QUE VALE $A \cap (B \cup C)$

$$x \in [(A \cap B) \cup (A \cap C)] \Rightarrow x \in (A \cap B) \vee x \in (A \cap C) \Rightarrow$$

DIFU DEFI

$$x \in (A \cap B) \vee x \in (A \cap C) \Rightarrow (x \in A \wedge x \in B) \vee (x \in A \wedge x \in C)$$

$$\Rightarrow x \in A \wedge (x \in B \vee x \in C) \Rightarrow A \cap (B \cup C) \Rightarrow A \cap (B \cup C)$$

Distr

\Leftrightarrow OBJETIVO: SUPONGO QUE VALE $[(A \wedge B) \vee (A \wedge C)]$

$$A \wedge (B \vee C) \Rightarrow x \in [A \wedge (B \vee C)] \xrightarrow{\text{DEF } \wedge} x \in [A \wedge (B \vee C)]$$

$$\xrightarrow{\text{DEF } \wedge} x \in [A \wedge (B \vee C)] \xrightarrow{\text{Distr}} x \in [(A \wedge B) \vee (A \wedge C)] \xrightarrow{\text{DEF } \vee}$$

$\text{DEF } \wedge$

$$[(A \wedge B) \vee (A \wedge C)]$$

Probar la igualdad.

CARDINAL DE UN CONJUNTO: Contador de elementos de un conjunto. Se denota $\#(\text{conjunto})$.

Ej: $A = \{1, 2, \{4, 5, 6\}\}$ $\#A = 3$

CONJUNTO DE PARTES: Sea A un conjunto, se llama Conjunto de poder del conjunto A a los subconjuntos de A . Se denota $P(A)$.

- El $\emptyset \in P(A)$.
- $A \in P(A)$
- $\#P(A) = 2^{\#A}$

Ej: $A = \{1, 2, 3, 4\}$

PRODUTO CARTESIANO: Sean dos conjuntos A y B .

El producto cartesiano es el par ordenado (c, d) con $c \in A$ y $d \in B$.

Se denota $A \times B$.

- $A = \{4, 5\}$ $B = \{1, 2\}$ $A \times B = \{(4, 1), (4, 2), (5, 1), (5, 2)\}$
- $A = \text{Cualquier Conjunto}$ $B = \emptyset$ $A \times B = \emptyset$
- $B = \emptyset$ $A = \text{Cualquier Conjunto}$ $B \times A = \emptyset$
- $A \times B \neq B \times A$
- $\#A \cdot \#B = \#AB$

RELACIONES: Sean A y B conjuntos. Una relación de A en B es un subconjunto cualquiera R de $A \times B$.

Ej: $A = \{1, 2\}$ $B = \{3, 4\}$ $A \times B = \{(1, 3), (1, 4), (2, 3), (2, 4)\}$

$R_1 = \{(1, 1), (1, 3), (1, 4), (2, 3)\}$. No es relación de $A \times B$ pues el $1 \notin B$.

$R_2 = \{(1, 3), (2, 4)\}$. Es una relación de $A \times B$.

$R_3 = \emptyset$. Es una relación de $A \times B$.

Pone hablar de $(1, 3)$ decimos que $1 R 3$.

Ej: $R_2 \Rightarrow 1 R 3, 2 R 4, 1 \not R 4$

RELACIÓN DE UN CONJUNTO EN SÍ MISMO: Sea A un conjunto. A es relaciones con A se le llama $A \times A$.

Al dice que R es una relación en A cuando $R \subseteq A \times A$.

Ej: $A = \{1, 2\}$ $A \times A = \{(1,1), (1,2), (2,2)\}$ $R = \{(1,1), (2,2)\}$

GRÁFICOS DE RELACIÓN (GRAFO):



PROPIEDADES DE RELACIONES: Algo R es una relación en A .

• REFLEXIVA: $\forall a \in A, aRa$.

• Ej. $R = \{(1,1), (2,2), (2,3), (3,1), (4,4)\}$
No es reflexiva pues $3 \not R 3$

$R = \{(1,1), (3,3), (2,1), (2,2)\}$
Es reflexiva.

$R = \{(1,1), (2,2)\} \Rightarrow$ Es reflexiva. En la relación IDENTIDAD

• SIMÉTRICA: $\forall a, b \in A$, si $aRb \Rightarrow bRa$.

Ej: $R = \{(1,2), (2,2)\}$ No es simétrica pues $2 \not R 1$

Ej: $R = \{(1,1)\}$ Es reflexiva y simétrica

Ej: $R = \{(1,2), (2,1)\}$ Es simétrica

• Si no hay flecha de $i \rightarrow A$ ni de VUELTA es SIMÉTRICA
pues NO se cumple anteriormente.

$$\underbrace{aRb}_{F} \Rightarrow bRa = V$$

- **ANTISIMÉTRICA:** Si $aRb \wedge bRa \Rightarrow a=b$.

- Es difícil que sea simétrica y antisimétrica a la vez (salvo la R identidad)
- Si el "y" no se cumple, es antisimétrica.

Ej: $\{(1,1), (2,2)\}$. Es ^{⑤ y R también} antisimétrica pues $1R1 \wedge 1R1 \Rightarrow 1=1$

Ej: $\{(1,2)\}$. Es antisimétrica. $1R2 \wedge 2R1 \Rightarrow 1=2$

$$V \wedge F \Rightarrow F \\ F \Rightarrow F = V$$

- **TRANSITIVA:** Si $aRb \wedge bRc \Rightarrow aRc$

- Si el "y" no se cumple, es transitiva

Ej: $\{(1,2), (2,1), (1,1)\}$. Es transitiva. $1R2 \wedge 2R1 \Rightarrow 1R1$

Ej: $\{(1,2), (2,3), (1,3)\}$. Es transitiva. $1R2 \wedge 2R3 \Rightarrow 1R3$

- **RELACIÓN TOTAL:** $R = A \times A$

- **RELACIÓN IDENTIDAD:**

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

EJEMPLOS CLAROS DE RELACIONES:

La igualdad ($a=b$): Es R, S, T.

La inclusión ($A \subseteq B$): Es R, A S, T. No es S pues $A \subseteq B$ pero no $B \subseteq A$.

Mayor

menor o igual (\leq, \geq): $\in R, AS, T$.

TIPOS DE RELACIONES:

- EQUIVALENCIA: Si una relación es R, S y T .
↳ No permiten Generar Conjunto disjunto.
- ORDEN: Si una relación es R, AS y T .

CLASES DE EQUIVALENCIA: Sea A un Conjunto
y una relación de equivalencia en A . Pone $x \in A$, lo
Clase de equivalencia de x en el Conjunto:

$$\bar{x} = [x] = \{ y \in A : y Rx \} \subseteq A.$$

Vulgarmente "Con quién se relaciona"

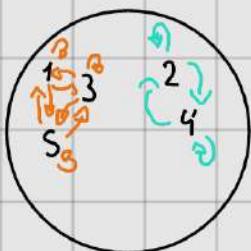
$$Ej: R = \{(1,1), (1,2), (2,1), (3,1), (1,3), (4,5), (5,4), (6,6)\}$$

$$[1] = [2] = [3] = \{1, 2, 3\}$$

$$[4] = [5] = \{4, 5\}$$

$$[6] = \{6\}$$

- PROPIEDAD FUNDAMENTAL: $\bar{x} = \bar{y} \Leftrightarrow \bar{x} \cap \bar{y} = \emptyset$



$$[1] = [3] = [5]$$

$$[4] = [2]$$

$$[2] \cap [1] = \emptyset$$

$$[4] \cap [3] = \emptyset$$

REPRESENTANTE DE CLASE: Cualquier elemento de
una clase de equivalencia representa a la clase.

$[4] = [5] = \{4, 5\}$. Ser el representante de los clúster o el 4.

Calcular la cardinal de clúster de equivalencia
Raíz de la relación $-y^2 + x^2 = -93y + 93x$

1. Plomérs la definición que tiene los clúster de equivalencia.
2. Como x es fijo, delo calcular y en base a él.

* IMPORTANTE: No son dividendo para la función solución $x^2 + x - y = 0$ se indefinen. Por lo tanto, para cada uno los y tienen común.

ii) Delo tomara un $x \in N$, y ver con que y se relaciona.

- \forall que es reflexivo, para todo $x R x$.
- \forall que es simétrico, para tanto, $x R y \Rightarrow y R x \Rightarrow x = y$
¿ Cuál es los clúster de equivalencia?

$$[1] = \{1\}, [2] = \{2\}, [3] = \{3\}$$

$$[x] := \{ y \in A / y R x \}$$

$$= \{ y \in A / -y^2 + x^2 = -93y + 93x \} = \{4, 5\}$$

$$\text{Entidemr} \quad -y^2 + x^2 = -93y + 93x$$

$$(y+x) \cdot (-y+x) = 93(-y+x) \leftarrow$$

$$\underbrace{(y+x)}_{a} \underbrace{(-y+x)}_{c} - \underbrace{93}_{a \cdot c + a \cdot b} \underbrace{(-y+x)}_{b} = 0$$

$$(-y+x) \left((y+x) - 93 \right) = 0$$

$$\begin{aligned} & a \cdot c + a \cdot b \\ & a (\underbrace{c + b}) \end{aligned}$$

Luego, si que para que valga la ecuación;

$$1. (-y+x) = 0 \Rightarrow x = y$$

$$2. (y+x) - 93 = 0 \Rightarrow x+y = 93$$

$$\star = \{ y \in A / x = y \vee x+y = 93 \}$$

$$\mathcal{E}_1: [22] = \{ y \in A / \underbrace{22 = y}_{x, \text{ con } x \in 22, y = 71} \vee 22+y = 93 \}$$

$$[x] = \{ x, 93-x \}$$

$$\mathcal{E}_1: [1] = \{ 1, 92 \}$$

$$\mathcal{E}_2: [2] = \{ 2, 91 \}$$

Es importante verificar siempre.

OTROS: Calcule los
Clases de equivalencia

de $A = \{1, 2, 3\}$

en la relación

$$A \cap B \subseteq A \Delta B \cap \{1, 2, 3\} = \emptyset$$

ii) Hallar la clase de equivalencia de
 $A = \{1, 2, 3\}$

Recordemos que la clase de equivalencia se
da por las relaciones entre los elementos.

Si $A = \{1, 2, 3\}$ tienen los B (en los que se
relaciona (los q. se n marcan) de acuerdo a la definición de equivalencia)

Entonces $\{1, 2, 3\} \cap B \Leftrightarrow (\{1, 2, 3\} \Delta B) \cap \{1, 2, 3\} = \emptyset$
O sea que $B = \{1, 2, 3\}$ para item 1. hace q.
 $(\{1, 2, 3\} \Delta \{1, 2, 3\}) \cap \{1, 2, 3\} = \emptyset$ fuer:

• Si B fuere distinto a $\{1, 2, 3\}$, la intersección
no sería vacía pues $A = \{1, 2, 3\}$

• Si B fuere $\{1, 2, 3, \{1, 2, 3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}\}$ tampoco
la intersección sería vacía pues:
 $(\{1, 2, 3\} \Delta \{1, 2, 3\}) \cap \{1, 2, 3\} = \{2, 3\}$

Concluimos que la clase de equivalencia de A es
 $[A] = \{1, 2, 3\}$

PARTICIÓN: Conjuntos con todos los clústeres de
equivalencia. La unión da



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

FUNCIONES: Una función $A \rightarrow B$ es una relación

$f \subseteq A \times B$ entre A y B que satisface:

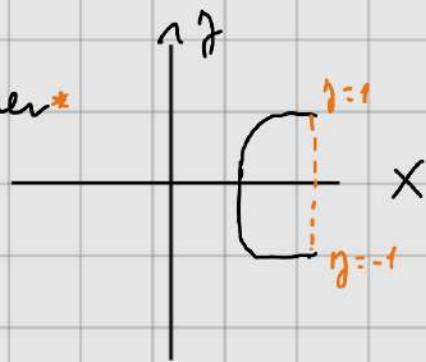
$\forall a \in A, \exists! b \in B / (a, b) \in f \rightarrow$ si mandar $x=1$ devuelvo UN SOLO Y.

• debe ser determinado por a.

$$b = f(a)$$

Ej: $y^2 = x$ no es función pver *

* si $x=1 \left\langle \begin{array}{l} y=-1 \\ y=1 \end{array} \right.$



$\forall a \in A$

$\exists !$

Para ser función debe cumplir criterio de unicidad.

TIPOS DE FUNCIONES:

• **INYECTIVA:** Si para un $a \neq a'$, $f(a) = f(a')$ entonces $a = a'$.

En palabras más simples, dos x deben ir a dos y diferentes.

Si van al mismo, x y x' son iguales

Ej:



No es inyectiva pver $f(1) = f(2)$
 $\Rightarrow 1 \neq 2$.



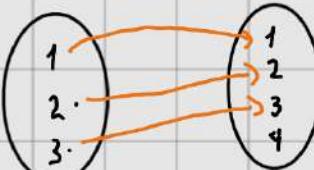
Es inyectiva

• **SOBREYECTIVA:** Si $\forall b \in B, \exists a / f(a) = b$

$$b = f(a)$$

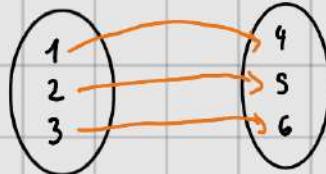
En palabras más simples, si todo y en el codominio recibe alguna x .

Ej:



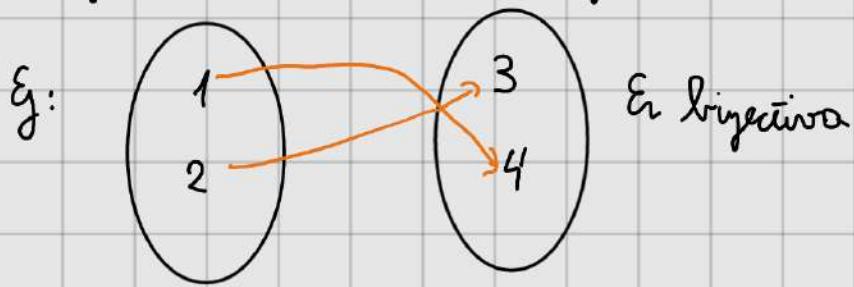
No es sobreyectiva.

Ej:



Es sobreyectiva.

• **BIJECTIVA:** Es bijección si es inyectiva y sobreyectiva



PROBAR INYECTIVIDAD Y SOBREYECTIVIDAD

DE ENCONTRAR CONTRAJEJEMPLOS:

Ej: Sea $f: \mathbb{R} \rightarrow \mathbb{R}$

$$f(x) = \begin{cases} 3x & x \leq 2 \\ x+2 & x > 2 \end{cases}$$

① Sea $x, x' \in \mathbb{R}$, si $f(x) = f(x')$ entonces $x = x'$.

La función tiene dos partes para poner x la tensión, tienen menor valores de x distintos tal que un $b \in \mathbb{R}$ sea el mismo.

Ej: $x=2 \wedge x'=4$

- $x=2$ Col in el primer caso, Oní $f(2)=6$.
- $x=4$ Col in el segundo caso, Oní $f(4)=6$.

¿Podemos un contrajemplo para $x \neq x'$?
sin embargo $f(x) = f(x')$.

f no es inyectiva

(S) Para que sea sobreyectiva, sea $b \in \text{Cofinido}$, $\forall b$ debe existir un $a \in \text{Dominio}$ tal que $b = f(a)$.

Aquí tenemos dos casos.

1) Si $x \leq 2$, $3x$. Por lo tanto el máximo valor hasta ese punto es 6 pues $3 \cdot (2) = 6$

$$y \leq 6$$

2) Si $x > 2$, $x+2$ x los demás al no tener un límite tenemos que $(2; +\infty)$ para elegir $x \geq y$ como $x \in \mathbb{R}$, $x+2$ también pertenecerá a \mathbb{R} .

Por lo tanto $y \in [4; +\infty)$

1) Volviendo a 1, ahora que $1 \vee 2$ cumplen al 5 y al 6 (Por lo que no es inyectiva).

Otro, note que $\forall y \leq 6$ tiene algún X

Ej: $f: \mathbb{Z} \rightarrow \mathbb{Z}$, Pruebe que es Biyectiva.

$$f(m) : \begin{cases} m+1 & m \text{ impar} \\ m-7 & m \text{ par} \end{cases}$$

En este los tengo otra función para ponerlos
 Así si $m \neq m' \Rightarrow m+1 \neq m' \Rightarrow m-7$.
 ya no tenemos un "rango" si es el criterio es: PAR O IMPAR.

I) Sea $m, m' \in \mathbb{Z}$, si $f(m) = f(m')$ entonces $m = m'$.

Repaso x Caren.

- m par, m' impar: Sabemos que es biyección x los totos $m = m'$. En este caso m par y m' impar, por lo tanto definiría un absurdo.

$$\begin{aligned}m - 7 &= m' + 1 \\m &= m' + 8 \quad \text{ABS!}\end{aligned}$$

- m par, m' par:

$$m - 7 = m' - 7$$

$$m = m'$$

- m impar, m' impar:

$$m + 1 = m' + 1$$

$$m = m'$$

Por lo tanto probamos que si m, m' son iguales se cumple $f(m) = f(m') \Rightarrow m = m'$
 f es inyectiva

S) Poros podes, visto el comportamiento.

IMPARES

m	$m+1$
-5	-4
-3	-2
-1	0
1	2 $\cancel{*1}$
3	4 $\cancel{*3}$
5	6

PARES

m	$m-1$
-4	-11
-2	-9
0	-7 $\cancel{*2}$
2	-5 $\cancel{*4}$
4	-3
6	-1
8	

Ver que los IMPARES \Rightarrow Caen en PAR

Ver que los PARES \Rightarrow Caen en IMPARES

CASO IMPAR: $\forall m \in \mathbb{R}$ impone el siguiente que

$b = m+1$ Com b par, x los teoremas, si b es un elemento del dominio $b-1 = m$ donde m es el valor que le corresponde en el dominio

Encontrar b del codominio, ej 3, le corresponderá un par del dominio.

$$f(\underbrace{b-1}_{\text{IMPAR}}) = (\underbrace{b-1}_{\text{IMPAR}}) + 1 = b \quad \checkmark$$

VERIFICO: $b \text{ PAR} = 2, m = 1 \cancel{*1}$

CASO PAR: $\forall m \in \mathbb{R}$ par, se cumple que b es IMPAR

$$b = m - 7 \Rightarrow b + 7 = m$$

$$\text{Dijo, } f(b+7) = \underbrace{(b+7)}_{\text{PAR}} - 7 = b \quad \checkmark$$

f es sobreyectiva

VERIFICAR: Tomar $b, b+7$ en \mathbb{M} .

$$\ast 2 \quad b \text{ IMPAR} : -7, m=0$$

Para verificar, saber que si doy b , me debiera dar el m correspondiente.

IMPORANTE recordar donde estoy parado.

$$m \text{ PAR} \Rightarrow b \text{ IMPAR} \text{ si doy } b \text{ impares debemos ver luego} \\ b+7 \text{ PAR} = m$$

si de $\text{DOM} \rightarrow \text{COD}$ le resto 7, si voy de $\text{COD} \rightarrow \text{DOM}$
le sumo 7

En todos los casos debe quedar igual b .

Como es BIJECTIVA, calcula la inversa. $f^{-1}(m) : \underbrace{\mathbb{Z}}_{\mathcal{B}} \rightarrow \underbrace{\mathbb{Z}}_{\mathcal{A}}$

$$f(m) : \begin{cases} m+1 & m \text{ impar} \\ m-7 & m \text{ par} \end{cases}$$

• Si m impar $\Rightarrow m+1$.

b PAR

Ej: $m=5$, $b=6$. Wieviel zu 6, como mehr o -5?
6-1, oder $m-1$

• Si m par $\Rightarrow m-7$.
 b IMPAR

Ej: $m=6$, $b=-1$. Wieviel zu -1, como mehr o -6?
 $-1+7$, oder $m+7$.

Ahí, $f(b)^{-1} = \begin{cases} b-1 & \text{si } b \text{ PAR} \\ b+7 & \text{si } b \text{ IMPAR} \end{cases}$

Entonces, si manda un b , se suma donde él m corresponda.

• $f(9) = 3$ ~~*3~~ • $f(-5) = 2$ ~~*4~~

Véamon que $f \circ f^{-1}(b) = \text{id}_{\mathbb{Z}}(b) \quad \forall b \in \mathbb{Z}$

$f \circ f^{-1}$, tengo dor dor.

$f(f^{-1}(b)) = \begin{cases} f(\underbrace{b-1}_{\text{IMPAR}}) & \text{si } b \text{ PAR} \\ f(\underbrace{b+7}_{\text{PAR}}) & \text{si } b \text{ IMPAR} \end{cases}$

= $\begin{cases} (b-1)+1 & \text{si } b \text{ PAR} \end{cases}$

$$(b+7)-7 \text{ si } b \text{ IMPAR}$$

$$= \begin{cases} b & \text{si } b \text{ PAR} \\ b-7 & \text{si } b \text{ IMPAR} \end{cases}$$

Otro punto $f^{-1} \circ f(a) = a \quad \forall a \in \mathbb{Z}$

$$f^{-1}(f(a)) = \begin{cases} f^{-1}(a+1) & \text{si } a \text{ IMPAR} \\ f^{-1}(a-7) & \text{si } a \text{ PAR} \end{cases}$$

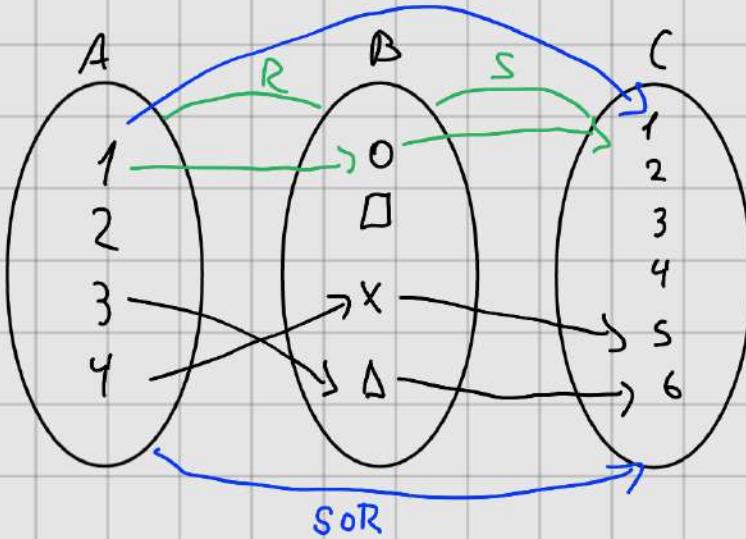
$$= \begin{cases} (a+1)-1 & \text{si } a \text{ IMPAR} \\ (a-7)+7 & \text{si } a \text{ PAR} \end{cases}$$

$$= \begin{cases} a & \text{si } a \text{ IMPAR} \\ a & \text{si } a \text{ PAR} \end{cases}$$

COMPOSICIÓN DE FUNCIONES: $\text{Res-una } R: A \times \bar{B} \rightarrow S = \bar{B} \times A$

La Composición de R y S es la relación de A a C dada por:

$$S \circ R = \{(a, c) \in A \times C \mid \exists b / (a, b) \in R \text{ y } (b, c) \in S\}$$



1 q tiene en A más relaciones con el 1 de C

porque hay alguien en el medio q los convierte.

Lo mismo con $(3, \Delta, 6)$

Si $f: A \rightarrow B \wedge g: B \rightarrow C$ son funciones entonces
 $g \circ f$ también.

Ej: $f: A \rightarrow B$ $g: B \rightarrow C$ $\overset{\text{Cod Dom}}{\sim} g \circ f: A \rightarrow C$

$h: B \rightarrow C$ $k: C \rightarrow D$ $\overset{\text{Cod Dom}}{\sim} h \circ g: B \rightarrow D$

$I_A: A \rightarrow A$

$I_A \circ f = f$

FUNCTION INVERSA: Si $f: A \rightarrow B$, su inversa es $g: B \rightarrow A$

Dicimos que una función f es inversible si hay una función g tal que:

• $f \circ g = I_B$

• $g \circ f = I_A$

Y en ese caso decimos que f es inversa de f .

La función inversa se denota f^{-1} .

Una función es invertible si y solo si es biyectiva.

NÚMEROS NATURALES: Conjunto infinito

- Commutatividad: $m + m = m + m$; $m \cdot m = m \cdot m$
- Asociatividad: $(m+m)+k = m+(m+k)$; $(m \cdot m) \cdot k = m \cdot (m \cdot k)$
- Distributiva: $m(m+k) = mm + mk$

Algunas eran para \Rightarrow DE DOS N
1 es par

1 no 2 no

m m

$m(m+1)$

2

SUMA DE GAUSS: $\forall m \in \mathbb{N}: 1+2+\dots+(m-1)+m =$

Siempre natural

SERIE GEOMÉTRICA: Permite sumar los $m+1$ primeros términos.

$$(q^{m-1} \cdot q = q^{m-1+1} = q^m)$$

$q \in \mathbb{R}$ fijo

$$1+q+q^2+q^3+\dots+q^{m-1}+q^m = Q$$
$$\cdot q = q+q^2+q^3+q^4\dots \underbrace{q^{m-1+1}}_{q^m}+q^{m+1} = qQ$$

$$(q-1)Q = q^{m+1}-1 \Rightarrow Q = \frac{q^{m+1}-1}{q-1} \text{ si } q \neq 1$$

$$Q = \begin{cases} \frac{q^{m+1}-1}{q-1} & \text{Cuando } q \neq 1 \\ \frac{m+1}{1-1} & \text{Cuando } q = 1 \end{cases}$$

$$q=1, Q = 1^0 + 1^1 + 1^2 + 1^3 + \dots + 1^m$$

SUMATORIA: Permite indicar claramente cuantos veces

Hoy que tienen Olga dada.

$$\alpha_1 + \alpha_2 + \alpha_3 + \dots + \alpha_{m-1} + \alpha_m = : \sum_{i=1}^m \alpha_i$$

Ej: $\sum_{i=1}^m i = \frac{m(m+1)}{2}$ ↗ INCLUIDOS m
↘ DESDE 1 INCLUIDOS

Ej 2: $\sum_{i=0}^m q^i$

Ej 3: $\sum_{1 \leq i \leq m} \alpha_i$

Ej 4: $\sum_{i=1}^m 1$: numero m veces el 1.

Ej 5: $\sum_{i=1}^m m^i = m^1 + m^2 + m^m$.

PROPIEDADES DE LA SUMATORIA:

1) $\left(\sum_{k=1}^m a_k \right) + \left(\sum_{k=1}^m b_k \right) = \sum_{k=1}^m (a_k + b_k)$ { 2) $\sum \frac{a+b+c}{d+c} = \sum \frac{a}{d+c} + \sum \frac{b}{d+c} + \sum \frac{c}{d+c}$ ↗ Pueden separar los de arriba.

OJO. Ambas dependen de k, empiezan ^{Y TERMINAN} en el mismo lugar.

3) $\sum_{k=1}^m (c \cdot a_k) = c \sum_{k=1}^m a_k$ | 4) $\sum_{k=1}^m c \cdot a_k + b_k = c \sum_{k=1}^m a_k + \sum_{k=1}^m b_k$

$$\stackrel{m=2}{n^2=4} \Rightarrow 2+2+2+2 = \frac{3}{2} \Rightarrow m^2 \cdot m$$

Ej: $\sum_{k=1}^{m^2} (k+m) = \sum_{k=1}^{m^2} k + \sum_{k=1}^{m^2} m = \frac{m^2(m^2+1)}{2} + m^2 \cdot m$

suma de gauss

5) EXTRAER TÉRMINOS:

$$\sum_{i=0}^{50} i^2 = \sum_{i=0}^{19} i^2 + \sum_{i=20}^{50} i^2$$

$$\sum_{i=0}^{2^{n+1}-2} i^2 = \sum_{i=0}^{2^n \cdot 2} i^2 = \sum_{i=0}^{2^n} i^2 + \sum_{i=2^n+1}^{2^{n+1}} i^2$$

EXTRAJE EL ULTIMO TERmino.

Este me lleva para quedarme con m y poder sacar gauss.

6) RECORDAR: $\sum_{i=1}^{m+1} \alpha_i = \sum_{i=1}^m \alpha_i + \alpha_{m+1}$

7) $\sum_{i=2^{m+1}}^{2^{m+1}} \frac{1}{2^{i-1}}$ =? Como se saca este término?

A medida que i crece, $\frac{1}{2^i}$ va haciéndose más chico.

Jugando con:

$$\cdot \text{Operación más lógica: } \frac{1}{2(q^{n+1})-1} \cdot (q^{n+1} - (q^n + 1))$$

↳ Luego veer el término más rico

8) MOVER INDICE HACIA ATRAS: $\sum_{i=k+1}^m 2i+1 = \left(\sum_{i=k}^m 2i+1 \right) - (2(k+1)+1)$

PRODUCTORIA: Mismo que sumatoria por multiplicación

$$a_1 \cdot a_2 \cdot a_3 \cdot a_{m-1} \cdot a_m = \prod_{i=1}^m a_i$$

$$k!(k+1) = (k+1)!$$

$$\text{Ej: } \prod_{i=1}^m i = 1 \cdot 2 \cdot 3 \cdot 4 \dots (m-1)m = m!$$

$$k(k+1)! / (k+1)!$$

$$\prod_{i=1}^m c = c \cdot c \cdot c = c^m$$

PROPIEDADES DE LA PRODUCTORIA:

$$\cdot \left(\prod_{k=1}^m a_k \right) \cdot \left(\prod_{k=1}^m b_k \right) = \prod_{k=1}^m a_k \cdot b_k = (a_1, b_1) \cdot (a_2, b_2) \cdot (a_3, b_3) \dots$$

• Son iguales inicio y fin.

$$\cdot \prod_{k=1}^m (c a_k) = \left(\prod_{k=1}^m c \right) \cdot \left(\prod_{k=1}^m a_k \right) = c^m \cdot \prod_{k=1}^m a_k$$

$$\cdot \prod a_i \cdot b_i = d(a_1, b_1) \cdot d(a_2, b_2) \cdot d(a_m, b_m) = d^m \left(\prod_{i=1}^m a_i \right) \cdot \left(\prod_{i=1}^m b_i \right)$$

MOVER INDICE HACIA ATRAS:

$$\prod_{i=k+1}^m \frac{1}{i+1} = \left(\prod_{i=k}^m \frac{1}{i+1} \right) \cdot \frac{1}{(k+1)+1}$$

INDUCCIÓN:

Un conjunto inductivo es relativamente IN.

PRINCIPIO DE INDUCCIÓN: Un subconjunto S de IN

es inductivo si:

- $1 \in S$
- $\forall k \in S, k+1 \in S$

Ej: IN es inductivo

INDUCCIÓN SIMPLE: Comienza desde $m=1$ o $m=0$

• Caso base: $P(1)$ se cumple.

• PASO inductivo: $\forall n \in \mathbb{N}$.

• $H_i: P(k)$

• QPQ: $P(k+1)$

$P(k+1)$ vale

si llego a lo que querí^z, $P(k)$ vale y $P(m)$ vale $\forall m \in \mathbb{N}$

INDUCCIÓN CORRIDA: Cuando la inducción implica los $m > 1$.

Ej: Si $m=5$, los elementos valen puer:

$$P(1) \Rightarrow P(2)$$

$$P(3) \Rightarrow P(4)$$

$$P(2) \Rightarrow P(3)$$

$$P(5) \stackrel{?}{\Rightarrow} P(6)$$

Como $P(1), \dots, P(4)$ no tienen la implicación en V puer F = F : V.

A partir de $P(5)$ si vale el Caso base $n=5$, debemos ver que $P(6)$ valga.

$P(7) \dots$ y así puer si vale $P(5)$ pero no $P(6)$ $P(5) \Rightarrow P(6)$
 $V \Rightarrow F = F$.

• Caso base: $P(m)$ con $m > 1$.

• Paso Inductivo: $\forall n \in \mathbb{N}_{\geq m}$

• $H_i: P(k)$

QPQ: $P(k+1)$ vale

• QPQ. Recurrencia
 Al llegar a la que quería, $P(k)$ mole $\rightarrow V_{k \in \mathbb{N}_{>m}}$ y $P(m)$ mole $V_{m \in \mathbb{N}_{>m}}$

SUCESIONES DEFINIDAS POR RECURRENCIA:

Son de la forma:

$$a_1 = x, a_{n+1} = a_n$$

Jue dicen que son por recurrencia para sacar Colgando un término menor del anterior.

$$\text{Ej: } a_1 = 1, a_2 = 3, a_3 = 7, a_4 = 15, a_5 = 31, a_6 = 63.$$

Colgule a_m : $2^1, 2^2, 2^3$
 $2, 4, 8$ le uno menor

$$a_m = 2^m - 1.$$

La sucesión definida por recurrencia:

$$a_1 = 1, a_{n+1} = 2a_n + 1 \quad \text{Sí se cumple: } a_m = 2^m - 1?$$

P(M).

$$P(M) := a_m = 2^m - 1 \quad \forall m \in \mathbb{N}$$

• Caso base: $m=1, a_1 = 2^1 - 1 = 1 = 1 \checkmark$

• Por inducción: $\forall n \in \mathbb{N}$.

• Hi: $a_k = 2^k - 1$

• QPQ: $a_{k+1} = 2^{k+1} - 1$

Pero por la def de la sucesión sabemos que

$$a_{k+1} = 2a_k + 1$$

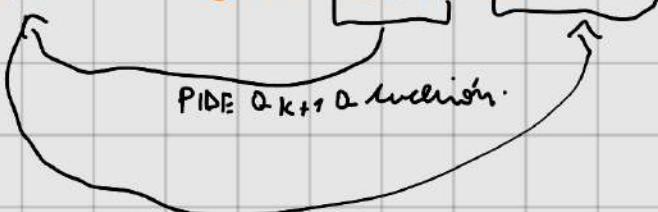
Luego, $a_{k+1} = 2a_k + 1 \stackrel{H_i}{=} 2(2^k - 1) + 1$
 $= 2^{k+1} - 2 + 1$
 $= 2^{k+1} - 1$ Como queríamos probar.

Por lo tanto, probamos el Caso base y para inducir \times la tesis n mole $P(m) \forall m \in \mathbb{N}$

PREGUNTA: Siempre reemplazo el a_{k+1} por la definición en la sucesión, ¿nos luego llegar al QPQ?

$$a_{m+1} = 2a_m + 1$$

$$QPQ: a_{k+1} = 2^{k+1} - 1$$



Luego obtengo QPQ.

Ej 2: Sea la sucesión definida por recurrencia

$$a_1 = 1, a_{m+1} = (\sqrt{a_m} - (m+1))^2 \quad \forall m \in \mathbb{N}$$

O sea $a_2 = 1, a_3 = 4, a_4 = 4, a_5 = 9, a_6 = 9$

$$a_m = \begin{cases} \left(\frac{m+1}{2}\right)^2 & \text{si } m \text{ impar} \\ \left(\frac{m}{2}\right)^2 & \text{si } m \text{ par} \end{cases} \quad P(m)$$

Caso base: $M=1$, Comprobamos $P(1) = 1^2 = 1 = 1 \checkmark$

Paso inducción: sea $k \in \mathbb{N}$.

• Hi: $\alpha_k = \left(\frac{k+1}{2}\right)^2$ si k impar

$$\alpha_k = \left(\frac{k}{2}\right)^2 \text{ si } k \text{ par}$$

• QPQ: $\alpha_{k+1} = \left(\frac{k+2}{2}\right)^2$ si k impar

$$\alpha_{k+1} = \left(\frac{k+1}{2}\right)^2 \text{ si } k \text{ par}$$

Caso k impar: $k+1$ es par.

Se muestra α_{k+1} par de acuerdo a la recursión:

$$\begin{aligned}\alpha_{k+1} &= \left(\sqrt{\alpha_k} - (k+1)\right)^2 \stackrel{\text{Hi}}{=} \left(\sqrt{\left(\frac{k+1}{2}\right)^2} - (k+1)\right)^2 \\ &= \left(\frac{k+1}{2} - (k+1)\right)^2 \\ &= \left(\frac{k+1 - 2(k+1)}{2}\right)^2 \stackrel{\text{Hi}}{=} \left(\frac{-k-1}{2}\right)^2 = \left(\frac{k+1}{2}\right)^2\end{aligned}$$

Caso k par: $k+1$ es impar

Se muestra α_{k+1} impar de acuerdo a la recursión

$$\begin{aligned}\alpha_{k+1} &= \left(\sqrt{\alpha_k} - (k+1)\right)^2 \stackrel{\text{Hi}}{=} \left(\sqrt{\left(\frac{k}{2}\right)^2} - (k+1)\right)^2 \\ &= \left(\left(\frac{k}{2}\right) - (k+1)\right)^2 = \left(\frac{k-2(k+1)}{2}\right)^2 = \left(\frac{k-2k-2}{2}\right)^2 = \left(-\frac{k-2}{2}\right)^2\end{aligned}$$

$$= \left(\frac{k+2}{2} \right)^2 \checkmark$$

Podremos probar el Caso base y el paso inductivo.

Se concluye que $P(m)$ es V, $\forall m \in \mathbb{N}$.

INDUCCIÓN COMPLETA/GLOBAL: Cuando necesitamos que

Múltiples los m Casos Anteriores. $P(1), P(2), \dots, P(n) \vee \Rightarrow P(n+1)$

Ej: $a_1 = 5, a_{m+2} = 5a_{m+1} - 6a_m$

En este ejemplo no podes calcular a_2 para tener a_1 , pero no tienes a_0

$$a_2 \Rightarrow m+2=2, \text{ entonces, } m=0. a_2 = 5a_1 - 6a_0$$

no lo tengo

OBS: En una sucesión dada por recurrencia, si no dan a_1 y a_2 entonces a_n tiene que definir $\forall n \in \mathbb{N}$.

• Caso base: $P(1)$ y $P(2)$ son V.

• Para Inductivo: $\forall k \in \mathbb{N}, P(k) \wedge P(k+1) \vee \Rightarrow P(k+2) \vee$.
brindar $P(m)$ en V, $\forall m \in \mathbb{N}$.

Volvemos al ejemplo anterior... Prueba que el término general de la sucesión

$$a_1 = 5, a_2 = 13, a_{m+2} = 5a_{m+1} - 6a_m \quad \forall m \in \mathbb{N}$$

$$\text{en } \underbrace{a_m = 2^m + 3^m}_{P(m)}$$

• Caso base: $m=1, n=2$.

$$m=1, P(1) = 2^1 + 3^1 = 5 \stackrel{?}{=} 5 \checkmark$$

$$M=2, P(2)=2+3^2=13=13 \vee$$

- Para inducción:海a $k \in \mathbb{N}$ fixo $\vdash P(k) \vee \wedge P(k+1) \vee \Rightarrow P(k+2) \vee?$
- Hi: $a_k = 2^k + 3^k \wedge a_{k+1} = 2^{k+1} + 3^{k+1}$
- QPQ: $a_{k+2} = 2^{k+2} + 3^{k+2}$

Para probarlo de la inducción se tiene que $a_{k+2} = 5a_{k+1} - 6a_k$

$$\begin{aligned}
 a_{k+2} &= 5a_{k+1} - 6a_k \stackrel{\text{Hi}}{=} 5(2^{k+1} + 3^{k+1}) - 6(2^k + 3^k) \\
 &= (3+2)(2^{k+1} + 3^{k+1}) - (3+2)(2^k + 3^k) \\
 &= (3 \cdot 2^{k+1} + 3^{k+2} + 2^{k+2} + 2 \cdot 3^{k+1}) - (3 \cdot 2^k + 3^{k+1} + 2^{k+1} + 2 \cdot 3^k) \\
 &= \underbrace{3 \cdot 2^{k+1} + 3^{k+2} + 2^{k+2} + 2 \cdot 3^{k+1}}_{2^k} - \underbrace{3 \cdot 2^k + 3^{k+1} + 2^{k+1} + 2 \cdot 3^k}_{3^k} \\
 &= 2^k + 3^{k+2} + 2^{k+2} + 3^k - 3^{k+1} - 2^{k+1} \\
 &= 2^k + 3^k \cdot 3^2 + 2^k \cdot 2^2 + 3^k - 3^k \cdot 3 - 2^k \cdot 2 \\
 &= 2^k (2^2 - 2) + 3^k (3^2 + 1 - 3) \\
 &= 2^k (2) + 3^k (7) \\
 &= 2^{k+2} + 3^{k+2} \quad \times \text{obvio en } 3^{k+2}
 \end{aligned}$$

Con probabilidad tiene que para inducción
se concluye que $P(n)$ es V, $\forall n \in \mathbb{N}$

Ej: Numeración tipo $\sum_{i=0}^n a_i$ tiene 1 rebote por here

pero para Ω_1 nos requiere Ω_0 para la
inducción global xf necesita siempre de los n
Términos Anteriores

Ej: Recurrencia que necesita 2 Términos Anteriores

Tiene 2 Casos base xf para Ω_2 necesita $\Omega_1 \wedge \Omega_0$

y la inducción completa xf necesita siempre que
magnor los 3 anteriores

$$P_1 \Rightarrow P_2 \Rightarrow P_3 \Rightarrow P_4 \Rightarrow P_5$$

$$\vee \quad \vee \quad \vee \quad F \quad \vee$$

M_0 función para
 Ω_2 magnor para
 Ω_4 nr.

$$\sum_{K=1}^{\infty} K \cdot K! = (K+1) : \quad \left| \quad \frac{1}{2^K} = \left(\frac{1}{2}\right)^K \right.$$

INDUCCIÓN GLOBAL / COMPLETA CORRIDA:

Sea M_0 un $M > 1$ $\in \mathbb{N}$.

• Caso base: $P(m_0)$ y $P(m_0 + 1)$ son V

• Paso inductivo: $\forall k \geq M_0, P(k) \wedge P(k+1) \rightarrow P(k+2) \text{ V.}$
entonces $P(n)$ en V, $\forall n \in \mathbb{N}_{\geq M_0}$

INDUCCIÓN GLOBAL/COMPLETA CON DESIGUALDADES

Método más complicado.

1) Sea $(a_m)_{m \in \mathbb{N}}$ la sucesión definida por:

$$\begin{cases} a_1 = 3 \\ a_2 = 8 \\ a_m = 5a_{m-1} + 7a_{m-2} \quad \forall m \geq 3. \end{cases}$$

Probar que $a_m < 7^m \quad \forall m \in \mathbb{N}$

Por Composición, voy a necesitar 2 CASOS BASE para

a_m requiere de a_{m-1} y a_{m-2} por global y si siempre

necesito los anteriores se cumplirán.

En el caso que hay menor caso tiene menor mío de una letra, h y k.

• P(M): $a_m < 7^m$

• Caso base:

$$m=1, a_1 < 7^1 \quad / \quad \text{para } 3 < 7$$

• Pase Inducción: $P(1), P(2), \dots, P(h-2), P(h-1) \Rightarrow P(h)$

$$\cdot H_i: Q_{h-1} < 7^{h-1} \quad 0 \leq k \leq h-1$$

$$Q_{h-2} < 7^{h-2}$$

$$\cdot QPQ: Q_h < 7^h \quad \vee \quad 7^h > Q_h$$

$$Q_h = 5Q_{h-1} + 7Q_{h-2} \stackrel{H_i}{<} 5(7^{h-1}) + 7(7^{h-2}) \quad (=)$$

$$7(7^{h-1}) + 7(7^{h-2}) \quad (=) \quad 7^h + 7^{h-1} < 7^h \quad (=) \quad 7^{h-1} < 0 \text{ ABS.}$$

$$\begin{aligned} * 5(7^{h-1}) + 5(7^{h-2}) &\quad (=) \quad 5(7^{h-1} + 7^{h-2}) \quad (=) \quad 5(7^h \cdot 7^{-1} + 7^h \cdot 7^{-2}) \quad (=) \\ 5(7^h (7^{-1} + 7^{-2})) &\quad (=) \quad 5(7^h (\frac{1}{7} + \frac{2}{7})) \quad (=) \quad 5(7^h (\frac{3}{7})) \quad (=) \quad 5 \cdot 7^h \cdot \frac{3}{7} < 7^h \\ \Leftrightarrow 5 \cdot 7^h \cdot 3 &\quad < 7^{h+1} \quad (=) \end{aligned}$$

2) Dado $(a_m)_{m \in \mathbb{N}}$ una sucesión de números reales tales que

$$a_0 = 1$$

$$a_{m+1} = 4 \left(\sum_{k=0}^m a_k \right) - 6m^2 + 13m + 16 \quad m \geq 0 \text{ para } \\ \min \text{ dato } a_0$$

$$\text{Probar que } a_m > 5^m + 3m - 4$$

Abreviatura que nos permite calcular a_{m+1} teniendo los términos anteriores para solo requerir los a_k . En este caso si queremos saber a_0 .

Perls kann hier in der Form lernen.

$$\cdot P(M) = Q_M > S^M + 3M - 4$$

$$\cdot \text{Case here: } M=0, 0 > S^0 + 3 \cdot 0 - 4 > -4 \quad \checkmark \text{ from } 1 > -4.$$

$\cdot P.I.: \text{Also } h \in \mathbb{N} \text{ für } P(0), P(1), \dots, P(R) \rightarrow P(R+1)$

$$\cdot H_i: Q_k > S^k + 3k - 4 \quad 0 \leq k \leq h$$

$$\cdot Q.P.Q: Q_{h+1} > S^{h+1} + 3(h+1) - 4$$

Per Proof:

$$Q_{R+1} = 4 \left(\sum_{k=0}^h Q_k \right) - 6R^2 + 13R + 16$$

$> S^{h+1} - 4$

$$= 4 \left(\sum_{k=0}^h S^k + 3k - 4 \right) - 6R^2 + 13R + 16$$

$$= 4 \left(\left(\sum_{k=0}^h S^k \right) + \left(\sum_{k=0}^h 3k \right) - \left(\sum_{k=0}^h 4 \right) \right) - 6R^2 + 13R + 16$$

$$= \left(4 \underbrace{\left(\sum_{k=0}^h S^k \right)}_1 + 12 \underbrace{\left(\sum_{k=0}^h k \right)}_2 - 16 \underbrace{\left(\sum_{k=0}^h 1 \right)}_3 \right) - 6R^2 + 13R + 16$$

$$\cdot 1: S^k \Rightarrow q = S \text{ bzw. } \frac{S^{h+1} - 1}{S - 1}$$

$$\bullet 2: \frac{h(h+1)}{2} \text{ para } h \in \{0, 1, 2, 3, \dots\}$$

$$\bullet 3: \sum_{k=0}^h 1 = (h+1)$$

$$= 4 \left(5 \frac{s^{h+1}}{4} - 1 \right) + \cancel{12} \cdot \cancel{\frac{h(h+1)}{2}} - 16(h+1) - 6h^2 + 13h + 16$$

$$= 5^{h+1} - 1 + 6h(h+1) - 16(h+1) - 6h^2 + 13h + 16$$

$$= 5^{h+1} + 6h^2 + 6h - 16h - 16 - \cancel{6h^2} + 13h + 16$$

$$= 5^{h+1} - 3h - 1$$

Entonces $a_n > 5^{h+1} + 3(h+1) - 5$ para la
índice nula el P.I

Por lo tanto $P(n) \forall n \in \mathbb{N}$.

2. Conjeturar una fórmula para el término general de la sucesión $(a_n)_{n \in \mathbb{N}_0}$ definida a continuación y probar su validez.

$$a_0 = 3 \quad y \quad a_n = \begin{cases} 2a_{n-1} & \text{si } n \text{ impar} \\ \frac{1}{3}a_{n/2}^2 & \text{si } n \text{ par} \end{cases}, \forall n \geq 1.$$

$$n=1, \quad a_1 = 2a_0 = 6 \quad n=2, \quad a_2 = \frac{1}{3}(a_1)^2 = 12 \quad n=3, \quad a_3 = 2 \cdot 12 = 24$$

$$3, 6, 12, 24$$

$$a_m = 2^m \cdot 3$$

$$CB: a_0 = 2^0 \cdot 3 = 3 \quad \checkmark$$

$$P.I: \forall n \quad n \in \mathbb{N}_0, \text{ queremos que } P(0), P(1), \dots, P(n-1) \Rightarrow P(n) \quad \checkmark$$

$$\cdot H_i: a_k = 2^k \cdot 3$$

$$1 \leq k \leq h$$

$$\cdot QPQ: a_{h+1} = 2^{h+1} \cdot 3$$

Case $h+1$ par:

$$a_{h+1} = \frac{1}{3} \left(a_{\frac{h+1}{2}} \right)^2 \text{ Como nos piden solo } h, \text{ nota que } \frac{h+1}{2} \text{ es impar para } h.$$

$$\frac{h+1}{2} \in \mathbb{Z}, \frac{h+1}{2} \leq h \Leftrightarrow h+1 \leq 2h \Leftrightarrow 1 \leq h, \text{ pero } h \geq 1.$$

$$\begin{aligned} \text{Entonces } h=1, \frac{2}{2}=1. \text{ Por lo tanto, } a_{h+1} &= \frac{1}{3} (a_1)^2 \stackrel{H_i}{=} \frac{1}{3} (3 \cdot 2^{\frac{h+1}{2}})^2 \\ &= \frac{1}{3} (3^2 \cdot (2^{\frac{h+1}{2}})^2) = \frac{1}{3} (9 \cdot 2^{h+1}) = 3 \cdot 2^{h+1} \end{aligned}$$

Case $h+1$ impar: $a_{h+1} = 2 \cdot a_{(h+1)-1} = a_{h+1} = 2a_h \stackrel{H_i}{=} 2 \cdot 2^h \cdot 3 = 2^{h+1} \cdot 3$

DESIGUALDADES:

- Puedes sumar lo que quieras de izq a derecha.
- Los términos tenidos de desigualdad si multiplican por (-1) .
- Siempre debes tener expresiones sencillas o comparar, dg:

$$k^2 + k + 1 \geq k + 1 \text{ es más fácil} \Rightarrow k^2 \geq 0$$

En Inducción, se oírá oír: "Cada vez que haga operación,

puedo reemplazar x lo que quiera mientras no me pase"

$$\text{ej: } 3^n + 5^n \geq 2^{n+2}$$

$$3^k \cdot 3 + 5^k \cdot 5, \text{ Como } 3 \geq 2 \text{ y } 5 \geq 2 \text{ pues "dicho" el}$$

$$\text{CB: } n=1, 3+5 \geq 2^3 = 9 \geq 8 \checkmark \quad 3 \geq 2 \text{ y } 5 \geq 2.$$

$$\cdot H_i: 3^k + 5^k \geq 2^{k+2}$$

$$3^k \cdot 2 + 5^k \cdot 2 \Leftrightarrow 2(3^k + 5^k) \stackrel{H_i}{\geq} 2 \cdot 2^{k+2} > 2^{k+2}$$

$$\cdot QPQ: 3^{k+1} + 5^{k+1} \geq 2^{k+2}$$

$$\text{Entonces, } 2^{k+3} \geq 2^{k+2} \text{ y dg es verdadero.}$$

COMBINATORIA:

- Unión de Conjuntos Disjuntos: $\# A \cup B = \# A + \# B$

• Unión de Conjuntos no disjuntos: $\#A \cup B = \#A + \#B - \#A \cap B$

• Diferencia de Conjunto incluido en otro: $\#A - B = \#A - \#B$


• Diferencia: $\#A - B = \#A - \#A \cap B$

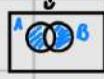
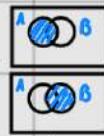
• Total de Combinaciones: $\#(A \times B) = \#A \cdot \#B$

Ej: Pongo $A = \{m \text{ en par}, n \leq 4\}$ $B = \{m \text{ en impar}, m \leq 4\}$

OBS: $-2\#(A \cap B)$ para A más B.

Otro incluye la A y B.

Mismo con B.



¿Cuántas Combinaciones puedes formar?

$$A = \{2, 4\} \quad B = \{1, 3\}$$

Como A ni B tienen condiciones para ser $\left(\begin{array}{c} -, - \\ A \quad B \end{array}\right)$

entonces tengo $\#A \cdot B = \#A \cdot \#B$ Combin.

$$\text{Ej: } \{(2,1), (2,3), (4,1), (4,3)\} \text{ que es } \#A \cdot \#B = 4.$$

• Total de Combinaciones con condiciones para armarse:

$$A = \{1, \dots, 10\} \quad B = \{(Q, 6) \in A \times A, Q \neq 6\}$$

En este caso, Q=6 en 10 Combin. $\{(1,1), (2,2), \dots, (10,10)\}$

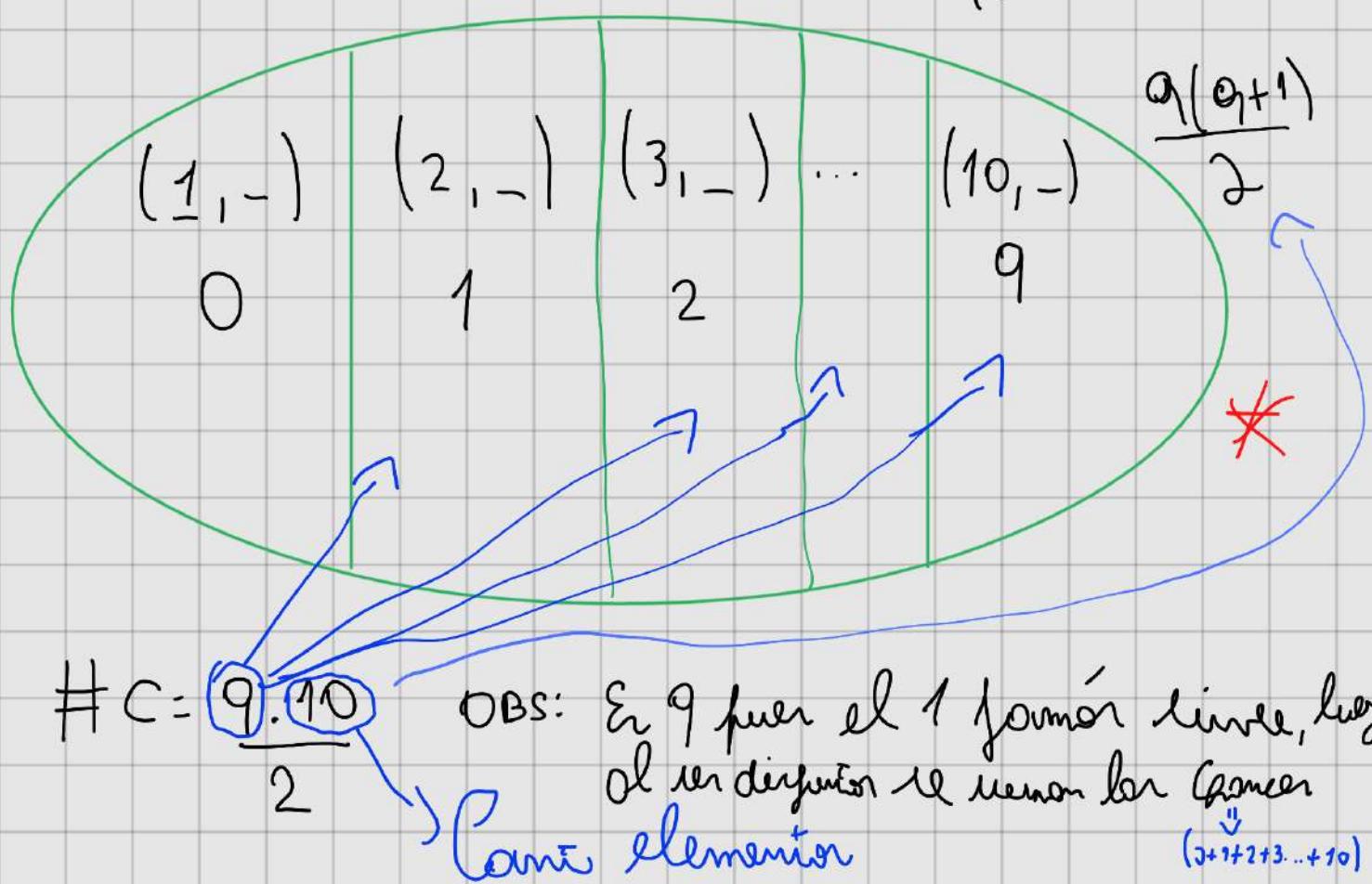
$$\left(\begin{array}{c} -, - \\ 10 \text{ OPS} \quad 9 \text{ OPS} \end{array}\right) = 9 \cdot 10 \Rightarrow \#B = 90$$

Pongo uno, resto del total.

- Tarjetas de Conar, Con condiciones para dormir
dividido en n grupos donde puede haber quien no cumple:

$$C = \{(a, b) \in A \times A; a > b\}$$

$$1+2+3+\dots+n$$



Aquí el Combinador defendió del contexto

Este es el PEOR CASO de COMBINATORIA

- Tarjetas de Conar con repeticiones:

$$A = \{x \in A \text{ de dos elementos}\}$$

$$A = \{1, \dots, 4\} \quad \left\{ \frac{1}{10}, \frac{1}{9} \right\} \text{ pero } \{1, 2\} = \{2, 1\}$$

¿Cuántas posibilidades hay de tener? 2. Entonces tarjetas

háis duplicado los vértices.

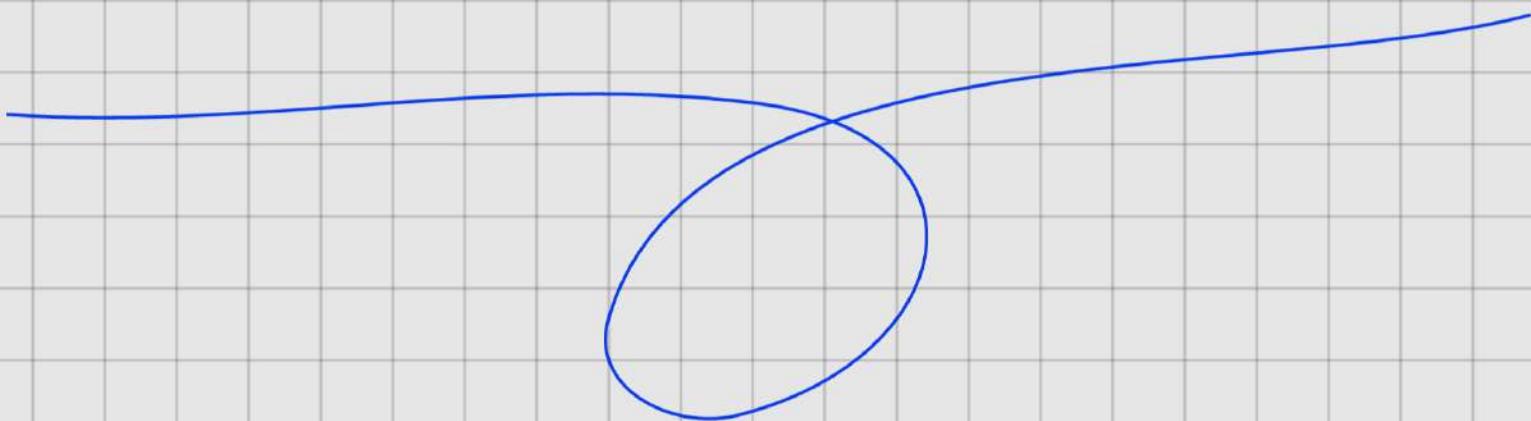
$$\# D = \frac{10 \cdot 9}{2} = 45$$

PRIMER LOGAR → SEGUNDO



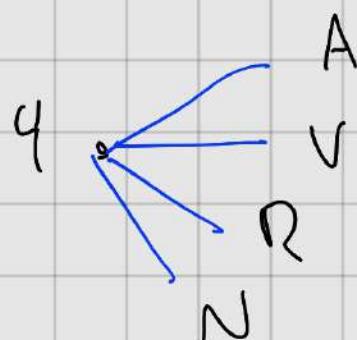
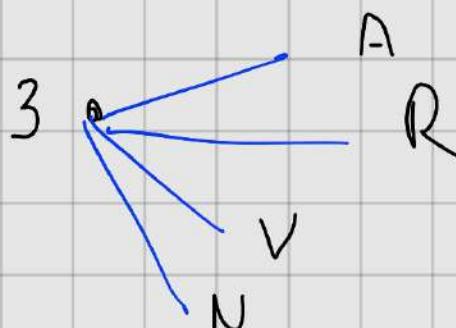
PREGUNTA BIEN: *

Mirá allá! Si los reflejan no tienen
"que vería" la diff de los resultados



Ejemplo Varios:

1) Sean 4 pares, indique de cuántas formas pueden formarse pares. Los colores son A, R, V, N.



Los 4 pares pueden formarse de cualquier de los 4 colores tomados juntos, no hay más que 4.

Condición.

$$4 \cdot 4 \cdot 4 \cdot 4 = 4^4$$

2) lo mismo pero los ordena de menor al mayor.

$$\begin{array}{ccccccc} 4 & & 3 & & 2 & & 1 \\ \hline \uparrow & & \uparrow & & \uparrow & & \uparrow \\ P & & P & & P & & P \end{array} \text{ O sea } 4!$$

No importa qué fuente hay en cada lugar,

los resultados.

P P P P
RVNA
RNVA
RNAV
RVAN
ANVR
AVNR
ARVN
AVRN
NRVA
NVRA
NARV
NAV R
:

PERMUTACIONES: Sea A que tiene n elementos, una
permutación es un conjunto de longit
n ordenado distinto que A.

Ej: $A = \{1, 2, 3\}$

PERMUTACIONES:

$$A' = \{1, 3, 2\} \quad A' = \{2, 3, 1\} \quad A' = \{3, 2, 1\}$$

$$A' = \{3, 1, 2\} \quad A' = \{2, 1, 3\}$$

Un Conjunto de M Elementos Tiene M

permutaciones

PRINCIPIO DE INCLUSIÓN EXCLUSIÓN:

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

Ej: Calcule $\#(A \cup B \cup C)$ a partir del principio de inclusión exclusión

$$\begin{aligned}\#((A \cup B) \cup C) &= \#(A \cup B) + \#C - \#((A \cup B) \cap C) \\&= \underbrace{\#A + \#B - \#(A \cap B)}_{- (\#(A \cap C) \cup \#(B \cap C))} + \#C \\&= \underbrace{\#(A \cap C) + \#(B \cap C)}_{= \#A + \#B - \#(A \cap B) + \#C - (\#(A \cap C) + \#(B \cap C) - \#(A \cap B \cap C))} - (\#(A \cap C) \cup \#(B \cap C)) \\&= \#A + \#B - \#(A \cap B) + \#C - \#(A \cap C) - \#(B \cap C)\end{aligned}$$

$\#(A \cap B \cap C)$

Recuerdo: " \cup " se traduce a " $+$ ". Todo debe estar en intersecciones. No deben quedar uniones porque es más fácil manejar inter. que uniones.

¿Por qué? La unión pide que esté en A o en B o en ambos. 2 CASOS.

La intersección AMBOS a la vez, 1 solo caso.

Fórmula mágica: $(-1)^{m+1}$ da el signo de la operación.

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

ARREGLO: Un arreglo de longitud l de elementos de A es UNA secuencia ordenada de l elementos distintos o iguales.

Si A tiene m elementos, se pueden formar $m!$ arreglos de longitud m.

ANAGRAMA: Permutación de letras que forma otra palabra.

Ej: Calcule la cantidad de anagrama de ABC

$$Rta: 3! \Rightarrow ABC, ACB, BAC, BCA, CAB, CBA.$$

Ej: Calcule la cantidad de anagrama de AABC

4!

2! \Rightarrow PUES ALITO repetido

CARDINAL DEL CONJUNTO DE PARTES:

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

CANTIDAD DE RELACIONES: $\text{Alom } A = \{1, 2, 3\}$ $\text{y } B = \{a, b\}$

La cantidad de relaciones de A en B es $\#(\mathcal{P}(A \times B)) \Theta 2^{m \cdot n}$

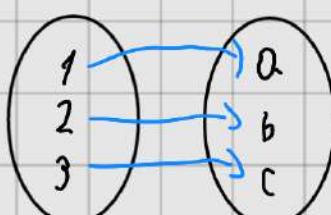
$$A \times B = \{(1, a), (1, b), (1, c), (2, a), (2, b), (2, c), (3, a), (3, b), (3, c)\}$$

$$\begin{aligned} \# \mathcal{P}(A \times B) &= \left\{ \{(1, a), (1, b)\}, \{(1, a), (1, c)\}, \{(2, a), (2, b)\}, \right. \\ &\quad \left. \{(2, a), (2, c)\}, \{(3, a), (3, b)\}, \{(3, a), (3, c)\}, \right. \\ &\quad \left. \{(1, a), (2, b), (1, c)\}, \{(2, a), (2, b), (2, c)\}, \right. \\ &\quad \left. \{(3, a), (3, b), (3, c)\}, \{(1, a), (2, b), (3, c)\} \right\} \end{aligned}$$

Hay $2^{m \cdot n}$ relaciones.

Ej: $\{(1, a), (1, b), (1, c)\}$ es relación pero NO función

Ej: $\{(1, a), (2, b), (3, c)\}$ es relación y función.



y es biyección.

INYECCIVIDAD: si $f(a) = f(a')$ $\Rightarrow a = a'$

SERIA UNA VIDA SI $f(a) = f(a')$

SUBNUEVADAS: $A \in B, \exists: a \in A \Rightarrow a \in B$

CANTIDAD DE FUNCIONES: $\{f\}$ que son subconjuntos de $P(A \times B)$ (llamados R) es función si $\forall a \in \text{Dom}(R)$,

Existencia

$\exists! b \in \text{CoD}(R)$,
diciendo

E decir, $A = \{1, 2, 3\}$ $B = \{a, b\}$, $f: A \rightarrow B$

Así, f : ¿ Es $\{(1, a), (1, b), (2, a)\}$ función? No pues para 2, $\exists! b$.

f : ¿ Es $\{(1, a), (2, b)\}$ función? Sí.

Entonces, ¿ Cuántas funciones existen? $\#B^{\#A}$. En este caso $2^3 = 8$

8 posibles: $\{(1, a), (2, b)\}, \{(1, b), (2, a)\}, \{(1, a), (3, b)\}, \{(3, a), (1, b)\}$

$\{(2, a), (3, b)\}, \{(3, a), (2, b)\}$

Pues para $f(1)$ puede tenerse $a \neq b$

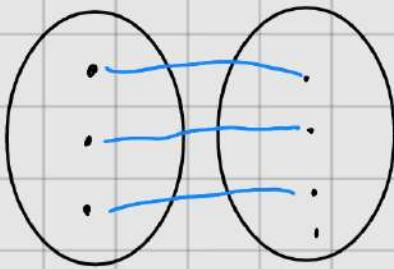
$f(2) \quad " \quad " \quad a \neq b$

$f(3) \quad " \quad " \quad a \neq b$

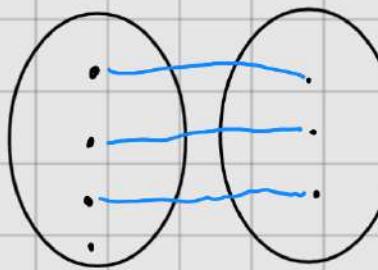
CARDINAL DE FUNCIONES:

• INYECTIVA: $\#A \leq \#B$ pero $\#A > \#B$ algún x debe ir a

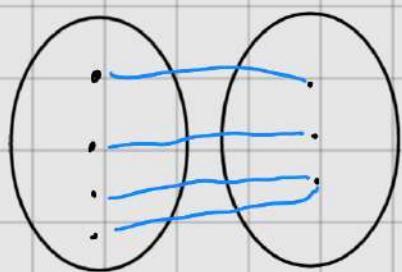
Compartir un γ .



INYECTIVA
 $(\#A \leq \#B)$

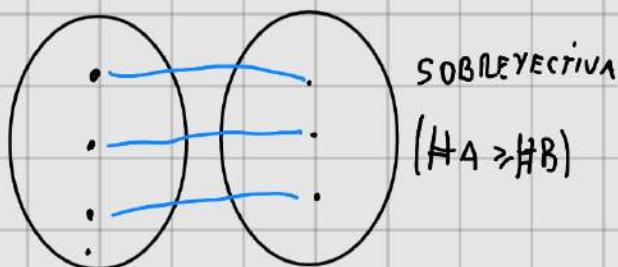


No es
biyectiva

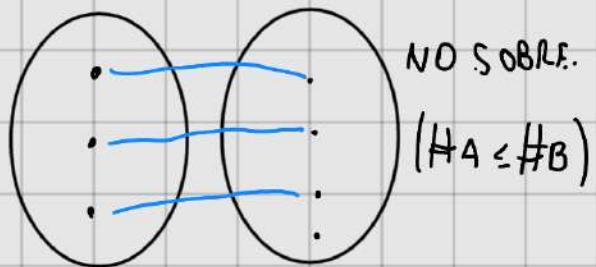


No es
INYECTIVA
 $(\#A > \#B)$

- SOBREYECTIVA: $\#A \geq \#B$ para que llenen B
o bien tener más elementos en A o igual cantidad

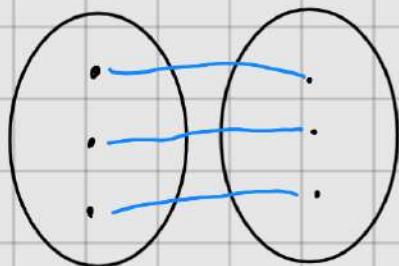


SOBREYECTIVA
 $(\#A \geq \#B)$



NO SOBRE.
 $(\#A \leq \#B)$

- BIYEKTIVA : $\#A = \#B$



CANTIDADES DE FUNCIONES BIYEKTIVAS: M:

Como hablamos de biyectividad té que claves A y B

Ogún y $\#A = \#B$ entonces hay $\#A! \neq \#B!$
funciones distintas.

Ol ver simetría $\#A \neq \#B$ en lo mismo.

Ej: $A = \{1, 2\}$ $B = \{4, 5\}$

Ogún elemento de A (1) y lo conecta
con algún elemento de B (5).

Luego, té que para que sea función
todo elemento de A debe ir en algún B

y también ol ver biyección té que en
sobreyeción por lo tanto todos los elementos de B

salgan idos con algún de A. Ol mismo tiempo,

té que para ser inyectiva el elemento que no

quede en B (9) debe ir con uno que no esté ocupado,

pero se lo contrario no sería inyectiva, pero $f(a) = f(a')$

Así, $f = \{(1,5), (2,4)\}$

O海o, habiendo armado la función π'

que hoy no es posible más que $2! = 2$.

Lo que queda: $f = \{(1,4), (2,5)\}$

Por lo tanto es cierto que $n!$ representa la cantidad de funciones biyectivas distintas.

CANTIDAD DE FUNCIONES INYECTIVAS: $\frac{n!}{(m-n)!}$

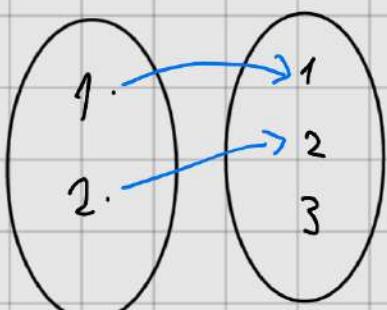
Recordemos que una función es inyectiva si $\forall a \in A \exists! b \in B / f(a) = b$
o sea, si dados $a, a' \in A$ se cumple que $f(a') = f(a) \Rightarrow a = a'$.

En palabras humanas, si dos $x, x' \in A$ dan el mismo B
 $\Rightarrow x \neq x' \Rightarrow$ No es inyectiva

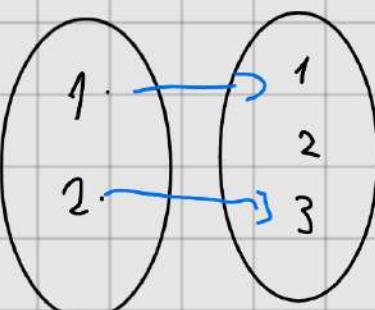
Es inyectiva si $\#A \leq \#B$. Dados $A = \{1,2\} \quad B = \{1,2,3\}$ Calcular
la cantidad de funciones inyectivas $A \rightarrow B$ ($f: A \rightarrow B$)

Vamos a verlos concretos...

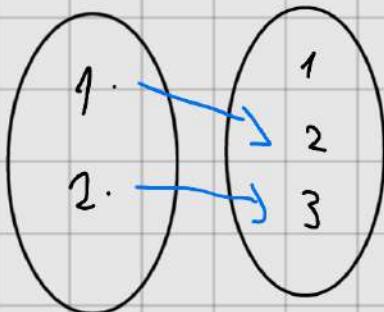
1.



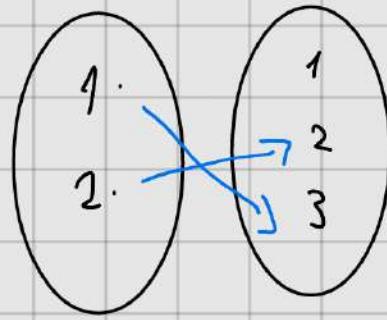
2.



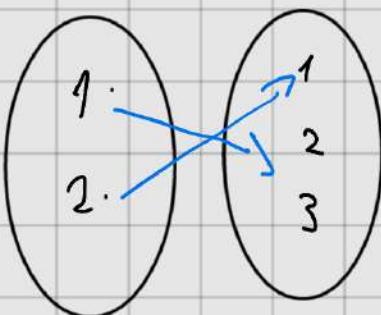
3.



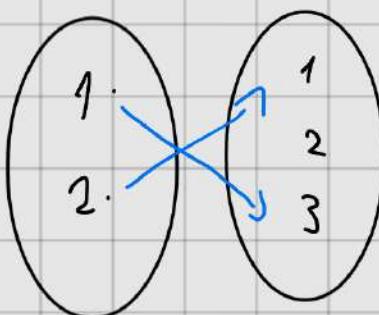
4.



5.



6.



#B:

→ Pueden elementos a tener/mas
en total variando los pares (a,b)

en cada función

$$\frac{(\#B - \#A)!}{(\#B - \#A + 1)!}$$

≥ 0

porque $\#A \leq \#B$

En matemáticas $\frac{3!}{(3-2)!} = 3! = 6$ que son los 6
casos de cambio

PENSAR COMO EL COMPLEMENTO: Deben utilizar el complemento

Opción siempre que no puedan calcular cuantas formas
hay "difícil". En mejor calcular que no pose, y
luego, el total de considerar entre las posibilidades que
no poseen.

10. Sean $A = \{1, 2, 3, 4, 5\}$ y $B = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$. Sea \mathcal{F} el conjunto de todas las funciones $f : A \rightarrow B$.

- ¿Cuántos elementos tiene el conjunto \mathcal{F} ?
- ¿Cuántos elementos tiene el conjunto $\{f \in \mathcal{F} : 10 \notin \text{Im}(f)\}$?
- ¿Cuántos elementos tiene el conjunto $\{f \in \mathcal{F} : 10 \in \text{Im}(f)\}$?
- ¿Cuántos elementos tiene el conjunto $\{f \in \mathcal{F} : f(1) \in \{2, 4, 6\}\}$?

En este ejemplo, A tiene 12 elementos.

El punto ii) nos pide calcular los que en el $\text{Im}(f)$ el 11 $\in \text{Im}(f)$. Esto sucede si el 11 es un elemento que no tiene ningún x . Es decir, como se ve en la lista.

O sea, $11^S, 10 \notin \text{Im}(f)$

En el punto iii) nos piden calcular cuantos $11 \in \text{Im}(f)$

Siendo el más difícil ya q 11 posee tres relaciones

de la forma en la función $f: A \rightarrow B$ dada

Ej: $f: A \rightarrow B = \{(1, 10), (2, 12), \dots\} \cup \{(1, 10), (2, 11)\}$

Si hay más.

Entonces es más fácil calcular cuando $10 \notin \text{Im}(f)$

Si luego deseamos la otra parte:

$$12^S - 11^S$$

En este $10 \notin \text{Im}(f)$

Ejemplo:

• 1) $A = \{1, 2\}$ $B = \{4, 5\}$

¿Cuántas funciones biyectivas existen?

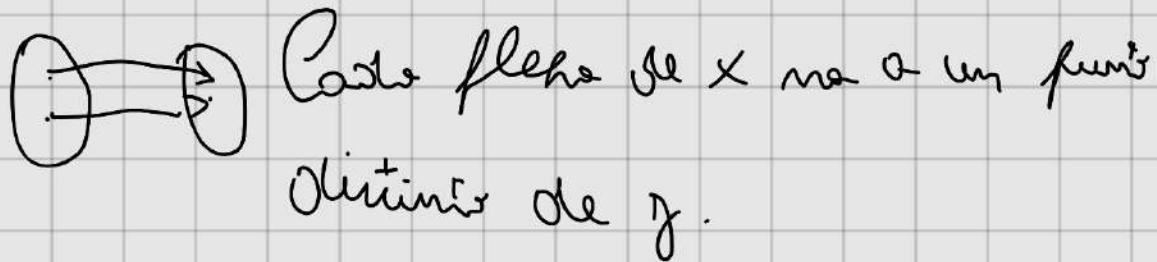
Obtener que una función es biyectiva si $\#A = \#B$.

Entonces debe ser inyectiva y sobreyectiva.

(I): Si tengo un elemento de la $\text{Im}(f)$ debo poder reflejarlo en el Dom.

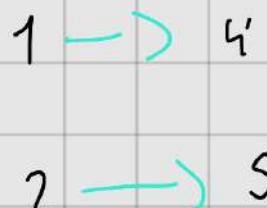
O, del otro lado, si $f(x) = f(x') \Rightarrow x = x'$

(S) Si $\forall b \exists a \in A / f(a) = b$. Entonces la imagen incluye el codominio.



RTA: 3!

PUES:



2 POSIBILIDADES (TOTALES)
DE FUNCIONES BIYECTIVAS

$$2) \text{ No } A = (1, 2) \quad B = (3, 6, +, \%)$$

a. Colule le cani de funzione.

b. " " " " " injection

c. ¿Cuáles funciones tienen que $f(1)$ sea par?

Qd. " " " Que $f(z) \neq 5$ v $f(z) \neq 6$?

Q. Una función del Círculo Interiores y Externos.

$\forall a \in A, \exists ! b \in B.$

Delv culmin taken for a, Como Ma.

RTA: 4^2 . Existen 4^2 funciones (pueden NO SER INY, SOBRE O BIY)

b. Para que las inyecciones solo signifiquen a cada persona en modo local el CDSM.

$$RT_A: \frac{4!}{(4-2)!} = \frac{4!}{2!}$$

C. Revisa los factores para $A=1$, luego que elijas
descuentos y el total.

$$R_{TA} = \frac{1}{2!} \cdot \frac{3!}{2!}$$

• si $f(1) = 6$, but $\frac{3!}{2!}$ incluye el 5,7,8 para $f(2)$

• si $f(1) = 8$, then $\frac{3!}{2!}$ incluye el 5,6,7 para $f(2)$.

d. Calcula cuántas posibilidades hay que $f(2) = 5 \vee f(2) = 6$

$$2^1 \cdot \frac{3!}{2!} \Rightarrow f(2) \text{ es } 5 \text{ o } f(2) \text{ es } 6.$$

Otro-, $\frac{4!}{2!} - \underbrace{\left(2 \cdot \frac{3!}{2!} \right)}_{\text{CANT TOTAL LAS Q } f(2)=5 \text{ O } f(2)=6}$

• 3) Calcula la cantidad de ANAGRAMAS de POLINOMIOS.

a. FORMA 1: $\frac{\text{CANT LETRAS}}{\text{REPETICIONES}}$

$$\frac{10!}{3! 2!} \checkmark$$

b. FORMA 2:

1. PONGO LAS Q.

$$\binom{10}{3}$$

2. PONGO LAS 1

$$\binom{7}{2}$$

3. PONGO LAS DEMÁS

$$\binom{5}{5} = 5!$$

$$\binom{10}{3} \cdot \binom{7}{2} \cdot \binom{5}{5} = \frac{10!}{3! 7!} \cdot \frac{7!}{2! 5!} \cdot 5! \\ = \frac{10!}{3! 2!} \quad \checkmark$$

- 4) Sea $A = \{1, 2, 3, 4, 5, 6, 7\}$ de los números pares armados en conjuntos B tal que tiene máximo 3 impares, B tiene 4 elementos

Impares en $A = \{1, 3, 5, 7\}$

1. Cómo 3 impares de A .

$$\binom{4}{3}$$

2. Cómo cualquier otro elemento (no impar)

$$\binom{3}{1} \rightarrow \#A - \#\text{IMPARES A}$$

$$R_{TA} : \binom{4}{2} \cdot \binom{3}{1}$$

5) Sea $A = \{10, 11, 12, 13, 14, 15, 16\}$ y $B = \{1, 2, 3, 4, 5, 6, 7\}$

¿Cuántas funciones biyectivas tal que $f(\{13, 14, 15\}) = \{2, 3, 4\}$?

1. Reservar para $\{13, 14, 15\}$ los $\{2, 3, 4\}$.

$$\hookrightarrow 3 \cdot 2 \cdot 1 = 3!$$

2. Como quedan solo 4 en $A (10, 11, 12, 16)$ hay 4 libres en $B (1, 5, 6, 7)$.

Deja, 4!

Rta: $3! \cdot 4!$

Recordar que el "!" significa factorial.

¿Cuántas funciones biyectivas tal que $f(\{1, 2\}) = \{1, 2, 3, 4, 5\}$

1 - 5 OPS

2 - 4 OPS

5. 4

Com de $\{1, 2, 3, 4, 5\}$ mén 2, $\#B - 2$ me quedan libres.

5OPS PARA 1 → 4OPS PARA 2

Rta: $5 \cdot 4 \cdot 5! \rightarrow$ El resto

RDO Fórmulas:

#A

B!

FUNCIONES: #B

FUN. INYECTIVAS: $\frac{M!}{(M-m)!} = \frac{M!}{(B-A)!}$

FUN. BIJECTIVAS = A! \odot B!

NRO. COMBINATORIOS: $\binom{M}{k} = \frac{M!}{k!(m-k)!}$

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

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

RD → FASE AYUDANTE: "Combinatorios Ayuda a Comer Caca, pero no nos interesa el elemento en particular"

Ésto frase explica el por qué cuando se eligen

los "pares" primeros x elementos la realidad

faltan los siguientes, los que eventualmente no

interesamos con colocar ESE elemento.

30. Sea $X = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$, y sea \mathcal{R} la relación de equivalencia en $\mathcal{P}(X)$ definida por:

$$A \mathcal{R} B \iff A \cap \{1, 2, 3\} = B \cap \{1, 2, 3\}.$$

¿Cuántos conjuntos $B \in \mathcal{P}(X)$ de exactamente 5 elementos tiene la clase de equivalencia \bar{A} de $A = \{1, 3, 5\}$?

Recordemos def de clase de equivalencia.

$$[A] = \{B \in \mathcal{P}(X) / B \mathcal{R} A\}$$

$$= \{B \in \mathcal{P}(X) / B \cap \{1, 2, 3\} = A \cap \{1, 2, 3\}\}$$

$$= B \cap \{1, 2, 3\} = \{1, 3, 5\} \cap \{1, 2, 3\}$$

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

¿Qué necesita el B para relacionarse con A? Que la igualdad valga, y, por lo B debe tener al {1, 3} y no al 2.

Por lo tanto B ya tiene revisado un elemento, de 9 posibles ya tiene 2 revisados y como uno más es una vez. (1, 1)
Ejemplo: Elije el 1. Elije el 3.

Otros me faltan 3 elementos para completar la combinación. ¿Cuáles?

$$\begin{pmatrix} 7 \\ 3 \end{pmatrix}$$

$$RTA: 1 \cdot 1 \cdot \binom{7}{3} = \binom{7}{3}$$

29. Sea $X = \{1, 2, \dots, 20\}$, y sea \mathcal{R} la relación de orden en $\mathcal{P}(X)$ definida por:

$$A \mathcal{R} B \iff A - B = \emptyset$$

¿Cuántos conjuntos $A \in \mathcal{P}(X)$ cumplen simultáneamente $\#A \geq 2$ y $A \mathcal{R} \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$?

Tomemos 2 condiciones $\#A \geq 2$ y $A \mathcal{R} \{1, 2, 3, \dots, 9\}$

Abremos la segunda, $A \mathcal{R} B \iff A - B = \emptyset$

Esto significa que $A \subseteq B$ siempre porque la diferencia lee vacío.

Si $A \subseteq B$ y $B = \{1, 2, \dots, 9\}$ entonces para que $A \mathcal{R} B$, A debe tener elementos del $\{1, 2, \dots, 9\}$.

¿Cuántas subconjuntos de 9 elementos puede tener el A?

El problema se lleva en que tenemos incluyendo los subconjuntos con 0 y 1 elemento. Así que excluirlos.

$$\binom{9}{0} + \binom{9}{1}$$

Pues los subconjuntos de 0 y 1 no se relacionan. Son diferentes.
ej: $\{3\} \cap \{1\} = \emptyset$.

Ahí, RTA: $2^9 - (\binom{9}{0} + \binom{9}{1})$

Otra forma de pensarla: Los que los subconjuntos que tienen 2 elementos tienen 9.

$$\binom{9}{2} + \binom{9}{3} + \binom{9}{4} + \binom{9}{5} + \binom{9}{6} + \binom{9}{7} + \binom{9}{8} + \binom{9}{9}$$

31. Sean $X = \{n \in \mathbb{N} : n \leq 100\}$ y $A = \{1\}$ ¿Cuántos subconjuntos $B \subseteq X$ satisfacen que el conjunto $A \Delta B$ tiene al sumo 2 elementos?

En este tipo de ejercicios ve la condición que nos piden.

$$\# A \Delta B = 0, \# A \Delta B = 1, \# A \Delta B = 2.$$

Para $\#\{1\} \Delta B = 0$

• B debe ser $\{1\}$. 1OP.

Para $\#\{1\} \Delta B = 1$ $\overset{\# A \Delta B = 0}{\rightarrow}$

• B tiene al 1. $\overset{\# A \Delta B = 1}{\rightarrow}$ con 1 elemento de los 99. $\binom{99}{1}$

• B no tiene al 1. $\overset{\# A \Delta B = 1}{\rightarrow}$ con 1 elemento de los 99. $\binom{99}{0}$.

\hookrightarrow Este caso cae en $\# A \Delta B = 1$.

Para $\#\{1\} \Delta B = 2$ $\overset{\# A \Delta B = 0}{\rightarrow}$

• B tiene al 1. $\overset{\# A \Delta B = 1}{\rightarrow}$ con 2 elementos. $\binom{99}{2}$

$\#A = 1$
• B contiene al 1. Con 1 elemento $\binom{99}{1}$

$$1 + \binom{99}{2} + 2 \binom{99}{1}$$

Ahora $A = \{1, 4, 5, 6\}$ $B = \{8, 9, 10, 11\}$ con $f: A \rightarrow B$ biyectiva.

1. ¿Cuántas funciones $f: A \rightarrow B$ hay? $\#B^{\#A}$. Hay 4⁴ funciones.

2. ¿Cuántas funciones $f: A \rightarrow B$ biyección hay? Hay 4!

3. ¿Cuántas funciones biyección hay tq $f(4) = 10$ y $f(6) = 11$?

1. 1. 2! \Rightarrow Vea: $\{(4, 10), (6, 11), 0\}$ otra: $\{1, 8\} \{5, 9\} \oplus \{5, 9\} \{1, 8\}$

2!

4. ¿Cuántas funciones biyección $f: A \rightarrow B$ hay tq $f(\{1\}) \neq \{8, 9, 10\}$?

3. 3! \Rightarrow Por qe $f(1) = 8 \vee f(1) = 9 \vee f(1) = 10$

Funciones biyección tq qe $f(\{1\}) \neq \{8, 9, 10\}$

$$4! - (3 \cdot 3!) = 24 - 18 = 6$$

Para verificar, fijé el 1 con el 11 y fermé lo demás

$$\{(1, 11)\} \dots \text{luego } f(\{4, 5, 6\}) = \{8, 9, 10\}$$

4	3 OPT
5	2 OPT
6	1 OPT

3! = 6

ENTEROS: A partir de ahora trabajaremos de $n \in \mathbb{Z}$.

Aprendemos el criterio de divisibilidad. Para saber división necesaria multiplicar.

Decimos que un número a es divisible por d si y solo si $\exists q \in \mathbb{Z}$ tal que $a = d \cdot q$.

Se dice " a " divide a " b " y $d \mid a$

Ej: $a = 20$, $d = 5$ Encuentre el cociente (q) de $5 \mid 20$

$$5 \mid 20 \Rightarrow 20 = 5 \cdot q$$

$$\Rightarrow 4 = q$$

Recíprocamente, encuentre a tal que $d = 20$, $q = 4$

$$20 \mid a \Rightarrow a = 20 \cdot q$$

$$\Rightarrow q = 5$$

$$\Rightarrow 20 \mid 20 \quad \checkmark$$

Ej: Encuentre los a , tal que $2 \mid q \cdot 2$. $d = 2$, $a = q \cdot 2$

Debo encontrar los q tales que

$2 = q \cdot 2$ de resto 0.

Los únicos $q \in \mathbb{Z}$ son 0 si a es divisible por 2 para $d = 2$ y $q \cdot 2$ siempre par. $\text{PAR}(\text{MOD } 2) = 0$

Ej: Encuentre los a , tal que $3 \mid q \cdot 2 + 2 \Rightarrow 3 \mid q \cdot 2 + 2 \wedge 3 \nmid 2$; ABS:

Ej: Encuentre los q , tal que $5 \mid q \cdot 2 + 8 \Rightarrow 5 \mid q \cdot 2 + 8 \wedge 5 \nmid 8$; ABS:

OBS: No vale que si $a/b = d/c \Rightarrow d/a \wedge d/b$

Sí vale $a/b \wedge c/d \Rightarrow d/a \wedge b/c$

Ej: Encuentre los q , tal que $d = 10$, $a = 7.2$, $b = 20$

$\frac{7.2}{2}$ para 7.2 debe ser menor a 10 para ser divisores.

$$10 \mid 7.2 \wedge 10 \mid 20 \Rightarrow 10 \mid (7.2) + 20$$

$$q = 15, 10 \mid 30 \wedge 10 \mid 20 \Rightarrow 10 \mid 30 + 20 \Rightarrow 10 \mid 50$$

Vale para todos q múltiplos de 5.

Ej: $d = 5$, $a = 9 - 1$ $b = 5$.

$$5 \mid 9-1 \wedge 5 \mid 5 \Rightarrow 5 \mid (9-1) - 5$$

$$\text{Vale } q = 11, 5 \mid (11-1) - 5 \Rightarrow 5 \mid 5$$

$$\text{Vale } q = 6, 5 \mid (6-1) - 5 \Rightarrow 5 \mid 0$$

$$\text{Vale } q = 16, 5 \mid 15 - 5 \Rightarrow 5 \mid 10$$

Si vale $d \mid a \wedge d \mid b \Rightarrow d \mid a - b$

PROPIEDADES DE LOS ENTEROS: En azul, los compuestos

En verde, los primos

- $d \mid 0$ para cualquier $d \in \mathbb{Z} \setminus \{0\}$. $\frac{0}{d}$ siempre 0.
- $1 \mid d$ para cualquier $d \in \mathbb{Z} \setminus \{0\}$
- $d \mid d$ para cualquier $d \in \mathbb{Z} \setminus \{0\}$. Es reflexiva
- $d \mid a \Leftrightarrow d \mid -a \Leftrightarrow -d \mid a \Leftrightarrow d \mid -a$
- $d \mid a \Rightarrow |d| \leq |a|$

L, si $d \mid a \wedge a \neq 0$ ent $\exists q/a = q.d$. Entonces $|a| = |q||d|$

Si $q \neq 0$: enteros

- Si $a \in \mathbb{Z}$ gan:

. Primo: Tiene 4 divisores. $\{\pm 1, \pm a\}$

. Compuesto: Tiene $2 \leq d \leq |a|-1$ divisores

- $d|a, d|b \Rightarrow d|a \pm b$. Ej: $2|2, 2|4 \Rightarrow 2|6$

(Como a, b son múltiplos de d , $d|ab$)

- $d|a \vee d|b \Rightarrow d|ab$ SOLO VALE EN PRIMOS . Ej: $2|2 \vee 2|5 \Rightarrow 2|10$

- $d|a \Rightarrow d|ca \quad \forall c \in \mathbb{Z}$. Ej: $2|10 \Rightarrow 2|\underline{\underline{2.10}}^{20}$

- $d|ab \Leftrightarrow d|b$ Con $d \perp a$ $5|2 \vee 5|5 \Rightarrow 5|10$

- $P|ab \Rightarrow P|a \vee P|b$ $P = P_{\text{Primos}}$

- $d|a \Leftrightarrow d^m|a^m$. Ej: $2|4 \Rightarrow 2^2|4^2$

- $a|b \wedge b|c \Rightarrow a|c$ Es transitiva

- $d|a \wedge c|a \Leftrightarrow dc|a$ Con $d \perp c$ Ej: $56|13^{2n} \dots 56 = 2 \cdot 7$, luego
 $2^3|13^{2n} \dots \wedge 7|13^{2n} \dots 2 \cdot 7|13^{2n} \dots$

- $c|a+b \wedge c|a \Rightarrow c|b$ (por $c|(a+b)-a \Rightarrow c|b$)

- $a \perp a \Leftrightarrow d \perp a^m \Leftrightarrow d^n \perp a$

Ejemplo:

Mostrar que para $a \in \mathbb{Z}, a \neq 1$ se tiene que $a-1|a^2+5$.

Con la divisibilidad es reflexiva, tenemos que $a-1|a-1$.

$$a-1|a^2+5 \Rightarrow \left\{ \begin{array}{l} (a^2+5) - a(a-1) \Leftrightarrow (a^2+5) + (-a^2+a) \Leftrightarrow (a+5) - (a-1) \\ a-1|a-1 \end{array} \right\} \Leftrightarrow a-1|6$$

Los divisores de $\alpha \in \text{Div}(6) = \{\pm 1; \pm 2; \pm 3; \pm 6\}$

$$\left. \begin{array}{l} \alpha - 1 = -1 \Leftrightarrow \alpha = 0 \in \mathbb{Z} \Rightarrow -1 \mid 5 \checkmark \\ \alpha - 1 = 1 \Leftrightarrow \alpha = 2 \in \mathbb{Z} \Rightarrow 1 \mid 9 \checkmark \\ \alpha - 1 = -2 \Leftrightarrow \alpha = -1 \in \mathbb{Z} \Rightarrow -2 \mid 6 \checkmark \\ \alpha - 1 = 2 \Leftrightarrow \alpha = 3 \in \mathbb{Z} \Rightarrow 2 \mid 19 \checkmark \\ \alpha - 1 = -3 \Leftrightarrow \alpha = -2 \in \mathbb{Z} \Rightarrow -3 \mid 9 \checkmark \\ \alpha - 1 = 3 \Leftrightarrow \alpha = 4 \in \mathbb{Z} \Rightarrow 3 \mid 21 \checkmark \\ \alpha - 1 = -6 \Leftrightarrow \alpha = -5 \in \mathbb{Z} \Rightarrow -6 \mid 30 \checkmark \\ \alpha - 1 = 6 \Leftrightarrow \alpha = 7 \in \mathbb{Z} \Rightarrow 6 \mid 54 \checkmark \end{array} \right\} \begin{array}{l} \text{Los } \alpha \in \mathbb{Z}/0 \cdot 1/\alpha^2 + 5 \text{ son:} \\ \{0, \pm 2, 4, -5, 7, -1, 3\} \end{array}$$

CONGRUENCIAS: Habla de divisibilidad sin cocientes

$a, b \in \mathbb{Z}$ son congruentes módulo m si $m \mid a - b$, y en ese caso escribimos $a \equiv b \pmod{m}$

$$a \equiv b \pmod{m} \Leftrightarrow m \mid a - b$$

$$\text{Ej: } 5 \equiv 3 \pmod{2} \Leftrightarrow 5 \equiv 1 \pmod{2} \Leftrightarrow 4 \equiv 0 \pmod{2}$$

$$\text{Ej: } 13 \equiv 8 \pmod{5} \Leftrightarrow 13 \equiv 3 \pmod{5} \Leftrightarrow 10 \equiv 0 \pmod{5} \quad \text{¿Esto es correcto?}$$

$$5 \mid 13 - 8 \Leftrightarrow 5 \mid 5 \Leftrightarrow 5 \equiv 0 \pmod{5} \quad \text{"}$$

• Dos números a, b son congruentes si el resto de a mod n y b mod n es el mismo

$$a \equiv b \pmod{n} \Leftrightarrow r_n(a) = r_n(b)$$

$$\text{Ej: } n = 2 \quad a = 10 \quad b = 4$$

$$\begin{array}{c} r_2(10) \\ \hline 10 \equiv 0 \pmod{2} \\ \hline r_2(4) \\ \hline 4 \equiv 0 \pmod{2} \end{array} \quad \text{y como } a, b \text{ tienen el}$$

Mismo resto al dividir por 2 \Rightarrow son congruentes.

$$\text{Ej}_2: 7 \equiv 3(4), -1 \equiv 3(4), 7 \equiv 3(4), 15 \equiv 3(4)$$

Existen m clúster de equivalencia MOD m. Una por cada par de restos.

- ↳ Ej: MOD 5 tiene 5 clúster de equivalencia $\bar{0}, \bar{1}, \bar{2}, \bar{3}$ y $\bar{4}$.
- ↳ $10 \in \bar{0}$ pues $10 \bmod 5 = 0$, así todos los $5k \in \bar{0}$
 - ↳ $6 \in \bar{1}$ pues $6 \bmod 5 = 1$, así $5k+1 \in \bar{1}$
 - ↳ ... hasta, $4 \in \bar{4}$ pues $4 \bmod 5 = 4$, así todos $5k+4 \in \bar{4}$ con $k \in \mathbb{Z}$

PROPIEDADES DE LAS CONGRUENCIAS:

- $a \equiv 0(d) \Leftrightarrow d|a$ "si el resto de a mod d es 0, d divide a a (a es divisible por d)"

- Es una relación de equivalencia

$$\textcircled{R} \quad a \equiv a(d) \Leftrightarrow d|a-a \Leftrightarrow d|0 \Leftrightarrow 0 \equiv 0(d)$$

$$\textcircled{S} \quad \text{Si } a \equiv b(d) \text{ y } b \equiv c(d) \Rightarrow a \equiv c(d)$$

$$\frac{d|a-b}{a-b=d} \quad \frac{d|b-c}{b-c=d}$$

$$\frac{a-b=d}{\text{DEBO}} \quad \frac{b-c=d}{\text{LLEGAR}}$$

$$-(a-b)=d$$

||

$$-a+b=d$$

||

$$\frac{d|b-a}{d|b-a}$$

||

$$b \equiv a(d)$$

$$\textcircled{T} \quad a \equiv b(d) \wedge b \equiv c(d) \Rightarrow a \equiv c(d)$$

||

$$d|a-b \wedge d|b-c \Rightarrow d|a-c$$

Como sé que $d|a \wedge d|b \Rightarrow d|a+b$

$$d|(a-b)+(b-c) \Rightarrow d|a-c \text{ Como queríamos probar.}$$

- $a_1 \equiv b_1(d) \wedge a_2 \equiv b_2(d) \Rightarrow a_1 + a_2 \equiv b_1 + b_2(d)$
Esir vale para a_m, b_m .

$$\text{Ej: } 5 \equiv 0(s) \wedge 13 \equiv 3(s) \Leftrightarrow 18 \equiv 3(s)$$

- Sean $a, b, c \in \mathbb{Z}$ vale que: $a \equiv b(d) \Rightarrow c \cdot a \equiv c \cdot b(d)$

$$\text{Ej: } 20 \equiv 10(d) \Rightarrow \underbrace{5}_{c} \cdot \underbrace{4}_{b} \equiv \underbrace{5 \cdot 2}_{c \cdot b}(d)$$

- $a_1 \equiv b_1(d) \wedge a_2 \equiv b_2(d) \Rightarrow a_1 \cdot b_1 \equiv a_2 \cdot b_2(d)$

Esir vale para a_m, b_m

- $a \equiv b(d) \Rightarrow a^m \equiv b^m(d)$

Pruebo $a \equiv b(d) \Rightarrow (a \equiv c(b(a))$

$$\frac{d \mid a-b}{d \mid (a-c(b)) \Leftrightarrow d \mid c(a-b)} \stackrel{\text{es } \mathbb{Z}}{\Rightarrow} d \mid a-b$$

$d \mid ca \stackrel{?}{\Rightarrow} d \mid a \vee d \mid c$

¿Está bien?

Pruebo $a-1 \mid a^n - 1$

$$a-1 \mid a^n - 1 \Leftrightarrow a-1 \mid 0(a-1)$$

* $\Rightarrow a \stackrel{0}{\equiv} 1(a-1) \rightarrow$ Bucle una m. Pasa en 1^m lo que exp.

$$\Rightarrow a^n \equiv 1^m(a-1) \text{ como queríamos probar}$$

$$\Rightarrow a-1 \mid a^n - 1^m \Rightarrow a-1 \mid a^n - 1$$

* $a^m \equiv b^m(c) \Leftrightarrow a \equiv b(c)$

Probar x inducción $64 \mid 49^n + 16n - 1$

$$\underbrace{P(n)}$$

(B: $n=1, 64 \mid 49+16-1 \Rightarrow 64 \mid 64 \checkmark$

P.I: sea $k \in \mathbb{N}$ fijo

. H: $64 \mid 49^k + 16k - 1 \Rightarrow 49^k \equiv -16k + 1(64)$

$\dots \quad 64 \mid 49^{k+1} + 16(k+1) - 1$

..

PREGUNTAR. ¿Por qué solví?

ALGORITMO DE DIVISIÓN:

Si $a \in \mathbb{Z}$ y $b \in \mathbb{N}$, \exists un $q \in \mathbb{Z}$ y $r \in \mathbb{N}$

$$a = q \cdot b + r \rightarrow \text{resto}$$

$0 \leq r < b$

↓ cociente

El resto siempre es positivo y siempre menor al cociente.

Notación: $a \equiv b \pmod m \Leftrightarrow r_m(a) = b$

PROPIEDADES DEL RESTO:

- $a \equiv r_m(a) \pmod m$ $a = 10 \quad m = 2 \quad 10 \equiv 0 \pmod 2$
- $r_m(a+b) = r_m(a) + r_m(b)$
- $r_m(a \cdot b) = r_m(a) \cdot r_m(b)$
- $r_m(a-b) = r_m(a) - r_m(b)$
- $r_m(a^k) = r_m(r_m(a)^k)$

$$\text{Ej 3: } r_5(5^{500}) = r_5(5^{250} \cdot 5^{250}) = r_5(r_5(5^{125}) \cdot r_5(5^{125}) \cdot r_5(5^{125}) \cdot r_5(5^{125}))$$

$$\text{Ej 4: } r_5\left(\underbrace{166}_{1} \cdot \underbrace{4878 + 19999}_{2}\right) = ?$$

$$1. \quad 166^{1328} \cdot 4878 \equiv 1^{1328} \cdot 3 \equiv 3 \pmod 5 \quad 2. \quad 19999 \equiv -1 \equiv 4 \pmod 5$$

$$\text{Entonces, } r_5(166^{1328} \cdot 4878) + r_5(19999) = 7 \equiv 2 \pmod 5$$

↳ Si digo 7 es el mal par

$7 > 5$. 7 no tiene como clave

de equivalencia en 5. El resto debe

ser $0 \leq r < 5$

Ej.: Calcular el resto de dividir $3^{\text{4}^{\text{5}^{25}}}$ por 35.

$$3^{\frac{5}{4}} \stackrel{(35)}{\equiv} (-1)^{\frac{5}{35}} \stackrel{(35)}{\equiv} -1 \stackrel{(35)}{\equiv} 34 \quad \Leftrightarrow \quad \Gamma_{35}(3^{\frac{5}{4}}) = 34 \quad \text{y es válido para } 3^{\frac{5}{4}} < 35.$$

- Calcular el resto de dividir por 35 a $34^{17771} - 6^{1001}$:

Abreus que el 3^{er} le faltó una pora llegan a los 35.
por lo tanto, en lo posible se considera una tasa un -1.

$$34 \stackrel{17777}{=} -6 \stackrel{1001}{=} \begin{matrix} \equiv \\ (35) \end{matrix} -1 -\cancel{6} \stackrel{1001}{=} \begin{matrix} \equiv \\ (35) \end{matrix} -1 -\left(6^2\right) \stackrel{500+1}{=} \begin{matrix} \equiv \\ (35) \end{matrix} -1 -\cancel{1} \cdot \cancel{6} \stackrel{501}{=} \begin{matrix} \equiv \\ (35) \end{matrix} -1 -6 \stackrel{501}{=} \begin{matrix} \equiv \\ (35) \end{matrix} -7 \stackrel{29}{=} 29 \quad (35)$$

Beim 6^2 fangen wir auf.

Ejemplo: Probar que $\forall a \in \mathbb{Z}$ tal que $7 \nmid a$, $r_7(a^3) = 1$ o 6

7: review 0 of 6

Γ	a	a^2	a^3	$a \bmod 7$
0	0	0	0	0
1	1	1	1	1
2	2	4	1	2
3	3	2	6	3
4	4	2	6	4
5	5	4	6	5
6	6	1	6	6

Véase que $r_7(a)$ es largo, los lo elevan al cubo con la
ló más que $r_7(a^3)$.

$$f_7(a) \Rightarrow a=2, f_7(2)=2, f_7(2^3)=9 \text{ MOD } 7 \Rightarrow f_7(2^3)=1$$

↳ PROP: $\text{l}_m(a^k) = \text{l}_m(\text{l}_m(a)) \Rightarrow \text{l}_7(\overbrace{\text{l}_7(2)}^{8})$ / En este caso.

MÁXIMO COMÚN DIVISOR: Sean $a, b \in \mathbb{Z}$ no simultáneamente nulos. Entonces el MCD entre a y b de la forma $(a:b)$.

$$(a:b) = \text{MAX } D(a,b)$$

P: Propiedad

- El MCD es un divisor Común de a y b , y es el Máximo.
- El MCD siempre es un NRO positivo

P: Si a y b son ambos nulos $\Rightarrow (a:b) = 0$

- Si a y b no ambos nulos. Si $(a:0) = |a|$ & si a es nulo $(0:b) = |b|$
- Vale la simetría del MCD, $(a:b) = (b:a)$

- El MCD es siempre menor o igual a $\text{MAX}(a,b)$ O sea,

$$(a:b) \leq \text{max}(a,b)$$

P: Cosa raro importa MCD positivo $(-a:-b) = (a:-b) = (-a:b) = (a:b)$

? P: Al MCD le pides sumar o restar un múltiplo de otro y el MCD seguirá siendo el mismo

ATENCIÓN: Solo UNA OPERACIÓN por vez. $(a+cb:b+a)$ NO vale por $(a+cb:b) \vee (a:b+ca)$ si

P: $\text{MCD}(ac:bc) = \text{MCD}(a:b) \cdot |c|$ (con $a, b, c \in \mathbb{Z}$)

P: $\text{MCD}(a^k:b^k) = \text{MCD}(a:b)^k$

P: $\text{MCD}(a,b) \mid \text{MCD}(a':b')$

P: $a/a \wedge d/b (\Rightarrow d \mid (a:b))$

- Números COPRIMOS: Aquellos a y b no simultáneamente divisibles entre sí que $(a:b) = 1$.

Si a , b y ab son divisibles por su MCD, entonces tienen:

$$\begin{array}{c} a' \text{ y } b' \\ \downarrow a \\ \frac{a}{(a:b)} \end{array} \text{ Números COPRIMOS. Ej: } a:24 \quad b:12 \quad \text{MCD}(a:b)=12$$

$$a' = \frac{24}{12} = 2 \quad b' = \frac{12}{12} = 1 \quad (2:1) = 1$$

PROPIEDADES DE a y b COPRIMOS

- P. $a|bc \Rightarrow a|c$ para a y b COPRIMOS con $(a:b)=1$
- P. $a|c \wedge b|c \Rightarrow ab|c$ para a y b COPRIMOS
- P. $\text{MCD}(a:bc) = \text{MCD}(a:c)$ para a y b COPRIMOS
- P. $\text{MCD}(ab:c) = \text{MCD}(a:c) \cdot \text{MCD}(b:c)$ para a y b COPRIMOS
- P. $\text{MCD}(a^k:b^l)=1$ si a y b COPRIMOS con $k, l \in \mathbb{N}$

! ¿Qué nos dice $(a:b) = |a|$? El MCD es el divisor común máximo entre a y b

Si $(a:b) = |a|$ significa que b es un múltiplo de a , a divide a b

$$\text{Ej: } a=13 \quad b=26 \quad (a:b) = |a|$$

Más tarde, para hacer más rápido factoring los primos.

$$\begin{array}{r} 13 \mid 13 \\ 1 \mid \end{array} \quad \begin{array}{r} 26 \mid 2 \\ 13 \mid 13 \\ 1 \mid \end{array} \Rightarrow (13:26) = 13$$

$$\text{Ej: } a=16 \quad b=32$$

$$\begin{array}{r} 16 \mid 2^4 \\ 8 \mid 2^3 \\ 4 \mid 2^2 \\ 2 \mid 2 \\ 1 \mid \end{array} \quad \begin{array}{r} 32 \mid 2^5 \\ 16 \mid 2^4 \\ 8 \mid 2^3 \\ 4 \mid 2^2 \\ 2 \mid 2 \\ 1 \mid \end{array} \Rightarrow (16:32) = 16 \text{ pues } 16|32 \text{ y } 16|16$$

Luego cumple además que $16 = \text{max}(a,b)$

$$? (a:b) = (a+c, b+c) \vee (a-b, c)$$

$$\text{Ej: } a=4 \quad b=8 \quad (4+8:8) = (12:8+12:8) = (12:32)$$

$$\text{Ej: } a=12 \quad b=24 \quad (\text{y es nro 12})$$

$$(12:24) = (12:24-12:2) = (12:0) = 12.$$

Este que vimos en ² es lo que se llama Algoritmo de Euclides

Algoritmo de Euclides: El peor caso es Fibonacci.

$$\begin{aligned} \text{MCD}(a:b) &= \text{Si } a > b \quad (a - cb:b) \\ &= \text{Si } a > b \quad ((a - cb) - cb:b) \end{aligned}$$

$$\begin{aligned} \text{MCD}(a:b) &= \text{MCD}(r_1:b) \\ &= \text{MCD}(r_1:r_2) \\ &= \text{MCD}(r_3:r_2) \end{aligned}$$

$$a > b > r_1 > r_2 > r_3 > \dots > r_m > r_{m+1}$$

$\frac{\parallel}{\text{MCD}(a:b)}$ $\frac{\parallel}{0}$

Ej: $a = 24 \quad b = 10$

$$24 = 2 \cdot 10 + 4$$

$$10 = 2 \cdot 4 + 2$$

$$4 = 2 \cdot 2 + 0$$

$$\text{MCD}(24:10) = 2 \quad \text{resto} = 0 \quad \text{El MCD del resto anterior } \neq 0$$

$$(24:10) = (10:4) = (4:2) = (2:0) = 2$$

IDENTIDADES DE BEZOUT: ALGORITMO DE EUCLIDES EXTENDIDO

Es lo mismo que Euclides pero le hace IDA y VUELTA.

En la IDA encontramos MCD y resto, en la VUELTA los x y y que nos permiten escribir como combinación lineal $a \alpha + b \beta$.

Buscamos x y y de $(27:8)$

$$27 = 3 \cdot 8 + 3 \quad \text{MCD en 1. los coprimos}$$

$$8 = 2 \cdot 3 + 2$$

$$3 = 1 \cdot 2 + 1$$

$$1 = 1 \cdot 1 + 0$$

Dicho resultado es el algoritmo de Euclides extendido

Resumiendo al revés

$$2 = 1 \cdot 2 + 0 \Rightarrow 0 = 2 - 1 \cdot 2$$

$$3 = 1 \cdot 2 + 1 \quad 0 = 2 - 1(8 - 2 \cdot 3)$$

$$8 = 2 \cdot 3 + 2 \quad 0 = 2 - 1(8 - 2 \cdot 27 - 3 \cdot 8)$$

$$27 = 3 \cdot 8 + 3$$

NÚMEROS PRIMOS: Un número n es primo si tiene exactamente

2 divisores positivos.

Un número es compuesto si es mayor que 1, no es primo y se puede escribir como producto de primos.

Los divisores de un número compuesto siempre son menores o iguales al número n .

- Un número es primo si NO es divisible por un primo menor que él.
- Un número es si es ni primo ni compuesto (≥ 2)

2 es primo, 3 es primo, 4 NO es primo (es divisible como producto de los primos anteriores, o sea $2 \cdot 2$).

- Caracterizar para cada $k \in \mathbb{N}$ el valor que toma: $(12^k - 1 : 12^k + 1286)$.

La idea de este ejercicio es buscar los posibles MCDs y examinar $k \in \mathbb{N}$ que los satisface.

$d = (12^k - 1 : 12^k + 1286)$ y por prop del MCD se tiene que $d | 12^k - 1 \wedge d | 12^k + 1286$.
Entonces, por prop de la divisibilidad se tiene $d | (12^k - 1) + (12^k + 1286)$

$$\text{Entonces, } d | 12^k - 1 - (12^k + 1286) \Rightarrow d | -1287 \Rightarrow d | 1287$$

$$d | 1286(12^k - 1) + (12^k + 1286) \Rightarrow d | 1286 \cdot 12^k + 12^k \Rightarrow d | 12^k(1286 + 1)$$

$$\Rightarrow d | 12^k(1287)$$

$(\text{ca}: \text{cb}) = C(\text{a}: \text{b})$ COPRIMOS pues MCD(a:1)=1.

$$\text{Luego, } d | (12^k(1287) : 1287) \Rightarrow d | 1287 \left(\overbrace{12^k : 1} \right) \Rightarrow d | 1287.$$

Ahora, los posibles MCD con las divisiones de 1287 = {3², 11, 13}

$$3 | (12^k - 1) \wedge 3 | (12^k + 1286) \Rightarrow (12^k - 1) \equiv -1 \pmod{3}$$

$$\Rightarrow (12^k + 1286) \equiv 2 \pmod{3}$$

Luego, $3 | (12^k - 1)$ y $3 | (12^k + 1286)$, pero como decantamos al 9 pues 9 es múltiplo de 3.

Ahora veremos el caso de 11, 13 y 11 · 13.

Caso 11:

$$11 | (12^k - 1) \wedge 11 | (12^k + 1286) \Rightarrow 12^k - 1 \equiv 0 \pmod{11}$$

$$\Rightarrow 12^k + 1286 \equiv 1 + 10 \equiv 0 \pmod{11}$$

Luego, 11 divide $\forall k \in \mathbb{N}$

Caso 13:

$$13 \mid (12^k - 1) \wedge 13 \mid (12^k + 1286) \Rightarrow 12^k - 1 \stackrel{13}{\equiv} (-1)^k - 1 \equiv -2 \equiv 11 \pmod{13}$$

Al poner m divisible $\forall k \in \mathbb{N}$, luego tabla de potencias mod 13.

	0	1	2	3	4	5	6	7	8	9	10	11	12	Mod 13
$(-1)^k - 1$	0	-2	0	0	0	0	0	0	0	0	0	0	0	
$(-1)^k + 1286$	0	$\not\equiv 0$	0	0	0	0	0	0	0	0	0	0	0	

→ Caso $k=2$ satisface $13 \mid (12^k - 1) \wedge 13 \mid (12^k + 1286)$

Caso 13·11: Caso 11 divide $\forall k \in \mathbb{N}$ y 13 divide su LCM por:

RTA:

Caso 13·11: $k=2 \vee k=4 \vee k=6 \dots$ siempre divide el MCD entre 13·11:

$$(12^2 - 1 : 12^2 + 1286) = (143 : 1430) = (0 : 143) = |143| = 143 = 13 \cdot 11.$$

Caso 11: $\forall k$, dg: $k=1$ el MCD entre 11: $(12^1 - 1 : 12^1 + 1286) = (11 : 1298)$
 $= (0 : 11) = |11| = 11$

Preguntón 1: está bien.

- Dibujar todos los divisores del MCD de $(m^3 + 2m^2 - 6m - 21 : m^2 - 9)$ (dibujar uno sobre linea, luego otros 1 comis)

$$d = (m^3 + 2m^2 - 6m - 21 : m^2 - 9) \text{ y por prop del MCD},$$

$$d \mid m^3 + 2m^2 - 6m - 21 \wedge d \mid m^2 - 9 \text{ y por prop de la divisibilidad}$$

$$d \mid m^3 + 2m^2 - 6m - 21 \pm m^2 - 9$$

- $d \mid m^3 + 2m^2 - 6m - 21 - m(m^2 - 9) \Rightarrow d \mid 2m^2 + 3m - 21$
 $\Rightarrow d \mid (2m^2 + 3m - 21) - 2(m^2 - 9) \Rightarrow d \mid 3m - 3$
 $\Rightarrow d \mid 2m(3m - 3) - 3(2m^2 + 3m - 21) \Rightarrow d \mid -15m + 63$
 $\Rightarrow d \mid (-15m + 63) + 5(3m - 3) \Rightarrow d \mid 48$

Per poder d'una divisió de $48 = \{2^4 \cdot 3\}$ que no redueixi en algunes, en el 1.

Case 2:

$$\left. \begin{array}{l} m^3 + 2m^2 - 6m - 21 = m^3 + 1 \\ \quad \quad \quad (2) \end{array} \right\} m^2 - 7 = m^2 + 1$$

Ahora que retomé la exp., table de verificación

M	0	1		MOD 2
$m^3 + 1$	1	0		
$m^2 + 1$	1	0		

$$\rightarrow M \in I(2)$$

2 dívidida entre 3 é IMPAR. Então os $2^2, 2^3$ não valerão em Coss para.

$\text{Cosec } z^2 (4)$:

$$m^3 + 2m^2 - 6m - 21 = m^3 + 2m^2 + 2m + 3 \quad | \quad m^2 - 9 = m^2 + 3$$

Through table of section Mod 4/1000 we can impure

$$\begin{array}{c|ccccc}
 m & \cancel{0} & 1 & \cancel{2} & 3 \\
 \hline
 m^3 + 2m^2 + 2m + 3 & 0 & 2 \\
 m^2 + 3 & 0 & 3
 \end{array}
 \quad \text{mod } 4$$

↳ Divisibility in $M \cong 1(4)$: Euclidean, 2^3 "fakt weder als in $M \cong 1(5)$

$\text{Cos } 2^3 \left(\frac{\pi}{2}\right)$:

$$m^3 + 2m^2 - 6m - 21 \stackrel{(8)}{\equiv} m^3 + 2m^2 + 2m + 3 \quad \left\{ \begin{array}{l} m^2 - 9 \stackrel{(8)}{\equiv} m^2 + 7(8) \end{array} \right.$$

Fractions table de restes:

m	0	1	2	3	4	5	6	7	$\text{mod } 8$
$m^3 + 2m^2 + 2m + 3$	0	$\neq 0$							
$m^2 + 7$	0	0	$\neq 0$						

$$\exists k \in \mathbb{Z}$$

$$8 \text{ divides } m \stackrel{(8)}{\equiv} 1 \quad \text{E.g.: } m^2 - 9 \stackrel{(8)}{\equiv} (8k+1)^2 - 9 \stackrel{(8)}{\equiv} 72 \stackrel{(8)}{\equiv} 0$$

Case 2⁴:

$$m^3 + 2m^2 - 6m - 21 \stackrel{(16)}{\equiv} m^3 + 2m^2 + 10m + 11 \quad \left\{ \begin{array}{l} m^2 - 9 \stackrel{(16)}{\equiv} m^2 + 7(16) \end{array} \right.$$

Fractions table de restes:

m	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	$\text{mod } 16$
$m^3 + 2m^2 + 10m + 11$	11	$\neq 0$															
$m^2 + 7$	7	$\neq 0$															

16 does not divide Mersenne.

Case 3:

$$m^3 + 2m^2 - 6m - 21 \stackrel{(3)}{\equiv} m^3 + 2m^2 \quad \left\{ \begin{array}{l} m^2 - 9 \stackrel{(3)}{\equiv} m^2 \end{array} \right.$$

M	0	1	2	
$m^3 + 2m^2$	0	0	70	
m^2	0	70	70	

Mod 3

3 Divide a m en múltiplos de 3 $\Rightarrow m \equiv 0/3 \Rightarrow m = 3k$

Viendo los 3 casos, ¿El 3 se puede dividir con otros? No, por lo demás todos son impares.

Ejemplos:

MCD = 3 si m es de la forma $3k$ luego los posibles son (ordinales) $(3, 9, 15)$

MCD = 2 si m es IMPAR y $m \equiv 1/2$

MCD = 1 si m es IMPAR y $m \equiv 1/1$

MCD = 1 en cualquier otro caso (par) $(2, 4, 6, 8, \dots)$

Aclaraciones o preguntas en lo que sigue:

- No puedes tomar ningun exponente para los otros,

$$\text{ej: } (2^k + 5^k, 7^k + 2^k) \text{ si } m \neq 1, d=6$$

los posibles MCD son: $\{1, 2, 3, 6\}$ pero al

hacer tabla de residuos.

	0	1	
			Mod 2
$2^k + 5^k$	0	1	
$7^k + 2^k$	0	1	

los tienen que ser iguales.

- Si la congruencia tiene (-1) siempre se divide en: CASO PAR \Rightarrow CASO IMPAR
- per OJO, se defiende de la expresión.

Ej: $(-1)^k - 1 \equiv 0 \pmod{2}$ Muestra que si k es par o impar para

si $k=0$, $(-1)^0 - 1 \equiv 0 \pmod{2}$.

$$\text{si } k=1 \quad (-1)^1 - 1 \equiv -2 \equiv 0 \pmod{2}$$

Ej: $13 \mid 12^k + 1286$ Muestra que si k es par

$$\text{Pues si } k=0, 1287 \equiv 0 \pmod{11}$$

$$\text{si } k=1, 1298 \equiv 2 \pmod{11}$$

- Al hacer inducción por inducción, luego de aplicar la tesis, podes usar " \leq " o " $>$ ".

Ejemplo:

$$\therefore H_i: Q_k > \frac{k-2}{2k}$$

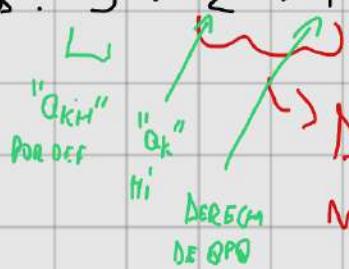
$$\therefore QPQ: Q_{k+1} > \frac{(k-1)}{2k+2}$$

Por def, $Q_{k+1} = \underset{H_i}{\cancel{Q_k^2}} + \frac{1}{4} \stackrel{H_i}{>} \left(\frac{k-2}{2k} \right)^2 + \frac{1}{4}$

Es más que.

Es MENOR que Q_k^2 \downarrow
Como sabemos que
 $\left(\frac{k-2}{2k} \right)^2 + \frac{1}{4} > \frac{(k-1)}{2k+2}$

Ejemplo de pasos: $3 > 2 > 1$



Des igual a la 2da. línea
mientras que el de izq es mayor.

$$5 < 4 \leq 3$$

Llegamos al lf: $\frac{k^2 - 4k + 4}{4k^2} + \frac{1}{4}$ (nos da menor un

$2k+2$ en el denominador (QPQ) multiplicar $\times k^2$ para tener mismo den.

$$\begin{aligned} \frac{k^2 - 4k + 4}{4k^2} + \frac{1}{4} \cdot \frac{k^2}{k^2} &= \frac{k^2 - 4k + 4}{4k^2} + \frac{k^2}{4k^2} \\ = \frac{2k^2 - 4k + 4}{4k^2} &\geq \frac{(k-1)}{2k+2} = (2k+2)(2k^2 - 4k + 4) \geq (k-1) \cdot 4k^2 \\ &= 4k^3 - 8k^2 + 8k + 4k^2 - 8k + 8 \geq 4k^3 - 4k^2 \\ &= 8 \geq 0 \text{ y es en V.} \end{aligned}$$

Por los pasos, $P(1), P(2), \dots, P(k) \vee \Rightarrow P(k+1) \quad \forall k \geq 2$

Luego, $P(n) \vee \forall n \geq 2 \in \mathbb{N}$.

CRÍTICA DE ARISTÓTENES: Basta primos, todos múltiplos, el siguiente NO todos son primos

1 \circlearrowleft 2 \circlearrowleft 3 \circlearrowleft 4 \circlearrowleft 5 \circlearrowleft 6 \circlearrowleft 7 \circlearrowleft 8 \circlearrowleft 9 \circlearrowleft 10 \circlearrowleft 11 \circlearrowleft 12 \circlearrowleft 13 \circlearrowleft

~~15~~ ~~16~~ 17 ~~18~~ 19 ~~20~~ ~~21~~ ~~22~~ 23 ~~24~~

~~25~~ 26 27 ~~28~~ 29 ~~30~~ 31 32 ~~33~~

TEOREMA FUNDAMENTAL DE LA ARITMÉTICA: Múltiplos de números

puede descomponer los números del mismo de la forma de
línica

$$10 = 5 \cdot 2 = 2 \cdot 5$$

$$30 = 2 \cdot 5 \cdot 3 = 5 \cdot 3 \cdot 2 = 2 \cdot 3 \cdot 5 \dots$$

$$4 = 2^2 = 2 \cdot 2$$

Definición: Γ o la cantidad de primos que dividen n en números m enteros positivos.

$$\text{Si } m = 1 \Rightarrow \Gamma = 0$$

$$\text{Ej: } 10, \Gamma = 1 \text{ pues } 5 | 5 \text{ pero } 5 \nmid 2.$$

• Los límites sucesión racionales entre los enteros

• RDO: si P primo $P | ab \Rightarrow P | a \vee P | b$

• Si $P | a_1, a_2, a_3, \dots, a_m \Rightarrow P | a_1 \vee P | a_2 \dots \vee P | a_m$

Ej: 30 es primo (a_1, a_2) $= 2 \cdot 5 \cdot 3 \Rightarrow$ ¿ $5 | 2 \cdot 5 \cdot 3$? \rightarrow sí,

Como s es primo, s divide a alguno de los factores del producto $\Rightarrow s|s \vee s|2 \vee s|3 = V_{\text{primo}}(s)$.

VALUACIÓN DE UN NÚMERO PRIMO: En la cantidad de veces que se repite en número un factor primo.

Ej: $45 = 3 \cdot 5 \cdot 3$ $V_3(45) = 2 \quad V_5(45) = 1$

No tienen soluciones de Nros Compuestos.

Ej: $12 = 4 \cdot 3$ $V_4(12)$ No tiene pares \Rightarrow NO es primo pero si $V_2(12) = 2$.

PROPIEDADES DE VALUACIONES:

- $V_p(a \cdot b) = V_p(a) + V_p(b)$
- $V_p(a^m) = m \cdot V_p(a)$
- $a|b \Leftrightarrow V_p(a) \leq V_p(b)$

CANTIDAD DE DIVISORES DE UN NÚMERO: Multiplicación de

veces que aparece cada exponente + 1.

Ej: $2^3 \cdot 5^2 \cdot 7 \cdot 19 \rightarrow \alpha_1 = 3 \quad \alpha_2 = 2 \quad \alpha_3 = 1 \quad \alpha_4 = 1$

$\left. \begin{array}{l} \alpha_1 = 3+1=4 \\ \alpha_2 = 2+1=3 \\ \alpha_3 = 1+1=2 \\ \alpha_4 = 1+1=2 \end{array} \right\}$ (Ojo con el 0 $\Rightarrow \alpha_1 = 3+1=4$)

$\left. \begin{array}{l} 4 \\ 3 \\ 2 \\ 2 \end{array} \right\}$

El n tiene 9 divisores

Ej: Dado los posibles factorizaciones de un número n tiene 15 divisores.

$$15 = 3 \cdot 5$$

$\underbrace{\quad}_{\times \text{ lo menor}}$

$d_1 \neq d_2$

$$2 \text{ (ASCOS: 1)} d_1 + 1 = 15 \Rightarrow d_1 = 1^4 \text{ o } \boxed{m = p^{14}}$$

$$2) \begin{cases} d_1 + 1 = 3 \Rightarrow d_1 = 2 \\ d_2 + 1 = 5 \Rightarrow d_2 = 4 \end{cases} \quad \vee \quad \begin{cases} d_1 + 1 = 5 \Rightarrow d_1 = 4 \\ d_2 + 1 = 3 \Rightarrow d_2 = 2 \end{cases}$$

$$\Theta: m = p^2 \cdot q^4 \quad \vee \quad m = p^4 \cdot q^2 \quad \text{Gm } p \neq q \text{ PRIMEROS BIS.}$$

Mínimo Común Múltiplo: Sean $a, b \in \mathbb{Z}$ NO simultáneamente nulos.

$\text{MCM}(a, b) \neq 0$ para (a, b) siempre es un posible MCM.

$$\text{MCM}(a, b) = \min M(a, b)$$

• Estudiar las propiedades del MCD entre el MCM.

$$\cdot \text{MCD}(a, b) = p_1^{\min(a_1, b_1)} \cdots p_r^{\min(a_r, b_r)}$$

$$\cdot \text{MCM}(a, b) = p_1^{\max(a_1, b_1)} \cdots p_r^{\max(a_r, b_r)}$$

$$\cdot MCD(a,b) \cdot MCD(a,b) = p_1^{a_1+b_1} \cdots p_r^{a_r+b_r} = ab$$

$$\cdot MCM = \frac{ab}{(a:b)}$$

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

$$\frac{2b+a^2}{ab} \Leftrightarrow ab \mid 2b+a^2 \Rightarrow$$

$ab \mid c \Leftrightarrow a \mid c \wedge b \mid c$

Como $a \perp b$, recuerda propiedades de coprimos.

$$a \mid c \wedge b \mid c \Leftrightarrow ab \mid c$$

$$\text{Ent., } c = 2b+a^2$$

$$\Rightarrow a \mid 2b+a^2 \wedge b \mid 2b+a^2$$

Otro. opción, $a \mid b+c \nmid a \perp b$ entre $a \mid c$

$$\Rightarrow$$
 $a \mid a+b \wedge a \mid a \Rightarrow a \mid b$ $\Rightarrow a \mid a^2 \Rightarrow a \mid 2b$ (pues $a \perp b \Rightarrow a \mid 2$)

$$\Rightarrow a \in \text{Div}(2) = \{1, 2\}$$

$$\text{Como } b \mid 2b \Rightarrow b \mid a^2 \cdot 1 \Rightarrow$$
 $b \perp a \Rightarrow b \perp a^2 \Rightarrow b \mid 1$

$$\Rightarrow b \in \text{Div}(1) = \{1\}$$

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

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

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

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

Ent. Otros nros que para cumplen que es entero,

$$a \in \{\pm 1, \pm 2\} \quad b \in \{\pm 1\} \quad ?^4 \text{ los ?}$$

$$\text{Caso } a=1, b=1 = 3 \checkmark \quad \text{Caso } a=1, b=-1 = 2-1=1 \checkmark$$

Viendo bien, con los enteros x_1 si a fuera menor que b podría no pertenecer a los enteros, pero en este caso $a \in \{\pm 1, \pm 2\}$ tiene que $a > 0$ que $b \in \{\pm 1\}$.

Lo mismo con el $\frac{a}{b}$. Como a siempre es $\leq a_2$, no hay forma que no sea entero.

$$\text{Luego, } 7L + 7L = 7L$$

$$\text{RTA: } a=\pm 1, b=\pm 1 \text{ y } a=\pm 2, b=\pm 1$$

$$\text{OJO: } -2 \cdot 7^{12k+1} \quad \text{No puedo multiplicar } -2 \cdot 7 \text{ x } 7^{\text{potencia distinta}}$$

ECUACIONES DIOFÁNTICAS: Son de la forma

$$ax+by=M \iff ax+by \equiv m(M)$$

→ solución sii $(a:b) \mid M$.

→ Si existe solución entonces COPRIMIZO

Luego, luego:

SOLUCIÓN PARTICULAR → \Rightarrow SOLUCIÓN GENERAL
SOLUCIÓN HOMOGENEA

Es importante recordar que la solución general del sistema tambien verifica la original. No es como cuando el posible MCD lo multiplicamos tipo $2(D')$ y luego $2 \cdot d'$.

Ejemplo:

$$1) 39a - 24b = 6 \quad (39:24) = \left(3.13:3.2^3 \right) = 3$$

¿3|6? Si. Solución.

COPRIMO: IMPORTANTE: si los números a y b NO SON coprimos

$$13a - 8b = 2$$

Solución PARTICULAR:

$$\begin{aligned} a = 2, b = 3 \text{ para } 13(2) - 8(3) &= 2 \\ 2 &= 2 \checkmark \end{aligned}$$

$$\left| \begin{array}{ccccccc} 13 & 26 & 39 & 52 & 65 & 78 \\ 91 & 104 & 117 & & & \\ 8 & 16 & 24 & 32 & 49 & 56 & 64 & 72 \\ 80 & & & & & & & \end{array} \right.$$

SOLUCIÓN HOMOGENEA

$$13a - 8b = 0$$

$$a = 8, b = -13$$

Los homogéneos o tienen iguales a 0

SOLUCIÓN GENERAL / mole k.

$$(2 - 8k; 3 - 13k) \quad k \in \mathbb{Z}$$

2) Determine todos los $(a, b) \in \mathbb{Z}^2$ que satisfacen simultáneamente

$$\cdot 4|a$$

$$\cdot 8|b$$

$$\cdot 33a + 9b = 120$$

Primero, resuelvo la diofántica para $4|a \wedge 8|b$

me dicen datos para obtener que: $4|a \Rightarrow a = 0(4) = a = 4k$

$$8|b \Rightarrow b = 0(8) = b = 8k'$$

Al cumplir de ser los dígitos distintos.

$$\text{Ent, } 33a + 9b = 120 \quad (33:9) = 3$$

$$3 \mid 120 \text{? Si.}$$

Copríncipe

$$11a + 3b = 40$$

SOLUCIÓN PARTICULAR

$$a=5, b=-5$$

SOLUCIÓN HOMOGENEA

$$a=3, b=-11$$

SOLUCIÓN GENERAL:

$$(5+3k; -5-11k) \quad (\text{con } k \in \mathbb{Z})$$

a b

Otro, debe cumplir que $4|a \Rightarrow 8|b$.

$$4 \mid 5+3k \quad ^\wedge \quad 8 \mid -5-11k$$

$$\begin{array}{c} \downarrow \\ 5+3k \equiv 1+3k \equiv 1-k \pmod{4} \\ (4) \end{array}$$

Colo se reto

K	0	1	2	3
1-k	1	0	3	2

Ent 4 divide a 1-k ($\Rightarrow k=1(4)$)

$$8 \mid -5-11k \Leftrightarrow -5-11k \equiv 3+5k \pmod{8}$$

(6)

Colo de reto MOD 8

K	0	1	2	3	4	5	6
---	---	---	---	---	---	---	---

$$8 \mid b \Leftrightarrow k=1(8)$$

$$3+8k \quad | \quad 3 \quad 0 \quad 6 \quad 2 \quad 7 \quad 4 \quad 1$$

Entonces $k \equiv 1(8)$ y $k \equiv 1(4)$. Como $4|8$ y $1 \equiv 1(8)$ entonces $k \equiv 1(4) \subseteq k \equiv 1(8)$. OJO: Existe k si debe ser el menor.

Luego, k tiene la forma $8k+1$.

Vuelvo a solución general: $(5+3(8k+1); -5-11(8k+1))$

$$\Rightarrow (8+24k; -16-88k) /$$

ECUACIONES DE CONGRUENCIA:

Si solución mif $(a:b)|c$ siendo $ax \equiv c(b)$ ($\Leftrightarrow ax+by=c$)

PROPIEDADES:

- $ax \equiv b(c)$ mif $(a:c) \mid b$ ent $\frac{a}{(a:c)}x \equiv \frac{b}{(a:c)}$

Ej: $4x \equiv 16(8)$ ($4:8 = 4$, $4|16$? si)
ent $x \equiv 4(2)$ ($\Leftrightarrow x \equiv 0(2)$)

- $2x \equiv 4(7) \stackrel{2 \cancel{7}}{\Leftrightarrow} x \equiv 2(7)$ Con b mult de a .

$$4x \equiv 2(7) \stackrel{2 \cancel{7}}{\Leftrightarrow} 2x \equiv 1(7) \Leftrightarrow x \equiv 4(7)$$

- $2x \equiv 5(7) \stackrel{4,4,11}{\Leftrightarrow} x \equiv 20(7) \Leftrightarrow x \equiv 6(7)$

$$\text{Ej: } 17x \equiv 3(11) \Leftrightarrow 6x \equiv 3(11) \stackrel{3}{\Leftrightarrow} 2x \equiv 1(11)$$

$$\stackrel{2 \cancel{11}}{\Leftrightarrow} 6x \equiv 1(11)$$

$$\Leftrightarrow 12x \equiv 6(11) \Leftrightarrow x \equiv 6(11) \Rightarrow x = 11k + 6.$$

VERIF: $k=1, x=17$. $17(17) \equiv 289 \equiv 3 \pmod{11}$

- $56x \equiv 28(35)$ $(56:35) = (2^3 \cdot 7 : 7 \cdot 5) = 4$

$\therefore 7|28?$ si. \exists solución

Coprimos, $8x \equiv 4(5) \Leftrightarrow 2x \equiv 1(5) \Leftrightarrow x \equiv 3(5)$

- $78x \equiv 30(12126)$ $(78:12126) = (2 \cdot 3 \cdot 13 : 2 \cdot 3 \cdot 2021) = 6$

$\therefore 6|30?$ si, \exists solución

Coprimos

$$13 \not| 2021$$

$\cdot 156, 156 \not| 2021$

$$13x \equiv 5(2021) \Leftrightarrow 2023x \equiv 980(2021) \Leftrightarrow 7x \equiv 980(2021)$$

$\cdot 289$

$$\Leftrightarrow 2023x \equiv 225420(2021) \Leftrightarrow 2x \equiv 1099(2021)$$

$\cdot 1000$

$$\Leftrightarrow 2000x \equiv 1099000(2021) \Leftrightarrow x \equiv 319(2021)$$

- Hallar todos los $(a,b) \in \mathbb{Z}^2$ tales que

$$\underline{b \equiv 2a(5)} \quad \Rightarrow \quad 28a + 10b = 26$$

Otra vez
2 incógnitas
1º Comprimo

Resuelva simultáneamente: $(28:10) = 2$, $2|26$? si. \exists sol.

Coprimos

$$14a + 5b = 13$$

SOLUCIÓN PARCIAL

$$a = 2, b = -3$$

SOLUCIÓN HOMOGENEA

$$a = 5, b = -14$$

SOLUCIÓN GENERAL

$$\left(\underbrace{2+5k}_a; \underbrace{-3-14k}_b \right) \text{ con } k \in \mathbb{Z}$$

$$b \equiv 2a \pmod{s} \Leftrightarrow -3-14k \equiv 2(2+5k) \pmod{s}$$

$$\Leftrightarrow -24k \equiv 0 \pmod{s}$$

$$\Leftrightarrow k \equiv 0 \pmod{s}$$

$$\text{Luego, } k = s\varphi + 2$$

$$\begin{aligned} \text{Entonces, solución general: } & (2+s(s\varphi+2); -3-14(s\varphi+2)) \\ & = (12+2s\varphi; -31-70\varphi) \\ & \text{Con } \varphi \in \mathbb{Z} \end{aligned}$$

- Hallar todos las soluciones $(x, y) \in \mathbb{Z}^2$ de $110x + 250y = 100$ que satisfagan $37^2 \mid (x-y)^{4321}$.

OBS: $P|ab \Rightarrow P|a \vee P|b$

$$37^2 \mid (x-y)^{4321} \Rightarrow 37 \mid (x-y)^{4321} \Rightarrow 37 \mid (x-y) \cdot (x-y)$$

$$\text{En } 37 \mid (x-y) \Rightarrow 37 \mid (x-y)$$

Resuelvo la desigualdad:

$$(110: 250) = (2 \cdot 5 \cdot 11: 2 \cdot 5^3) = 10$$

¿10|100? Si.

COPRIMIZO

$$11x + 25y = 10$$

11 22 33 44 55 66 77 88 99 110

2 5 10 25 50 100

SOLUCIÓN PARTICULAR

$$x = 10, y = -4$$

SOLUCIÓN HOMOGENEA

$$x = 25, y = -11$$

SOLUCIÓN GENERAL

$$(10+25k; -4-11k) \text{ con } k \in \mathbb{Z}$$

$$\text{Luego } 37((10+25k) - (-4-11k)) \Leftrightarrow 14 + 36k \stackrel{?}{=} 0(37)$$
$$\Leftrightarrow -k \equiv -14(37)$$
$$\Leftrightarrow k \equiv 14(37)$$

$$\text{Entonces } k = 37q + 14 \text{ con } q \in \mathbb{Z}$$

$$\text{Por lo tanto } \rightarrow (10+25(37q+14); -4-11(37q+14)) \checkmark$$

TEOREMA CHINO DEL RESTO:

Los tipos de congruencias de los cuales

Algoritmo de Cínguera.

La idea es tener las soluciones del sistema con modulos coprimos nos add.

PROPIEDADES:

$$m' \leq m.$$

- Si $m'|m$ y $\begin{cases} x \equiv a'(m') \\ x \equiv a(m) \end{cases}$ y $a \equiv a'(m)$ entre el mismo es compatible $\Rightarrow x \equiv a(m)$

Ej: $\begin{cases} x \equiv 1(2) \\ x \equiv 2(8) \end{cases}$ $2|8, 2 \equiv 1(2)$? No, $0 \not\equiv 1(2)$

$$\begin{cases} x \equiv 1(2) \\ x \equiv 1(4) \end{cases} \quad 2|4, 1 \equiv 1(2) \quad \Rightarrow \quad x \equiv 1(4)$$

- Si $m_1, m_2, m_3, \dots, m_n$ son coprimos entre sí entre \exists solución x en $\text{Mod}(m_1, m_2, m_3, \dots, m_n)$ y $x \in m_1, m_2, \dots, m_n$ $x \equiv x_0(m_1, m_2, m_3, \dots, m_n)$. Por el TCR.

- Solo se puede resolver los MOD que tienen divisores primos DIFERENTES.

- Si las ecuaciones tienen mismos divisores pero diferentes MOD, se multiplican los MOD y quita.

Mismo resto. $\Rightarrow \begin{cases} a \equiv 3(7) \\ a \equiv 2(8) \\ a \equiv 3(11) \end{cases} \Rightarrow \begin{cases} a \equiv 3(77) \\ a \equiv 2(8) \end{cases}$

- Solo alfa los MOD en primo si no que solo hace resto con él. Si son coprimos todos no hace resto

Ej: $\begin{cases} a \equiv 1(7) \\ a \equiv 2(11) \\ a \equiv 5(6) \end{cases}$ En 3.2 fuer 6+7+11.

Ej 2: $\begin{cases} a \equiv 1(2) \\ a \equiv 1(6) \end{cases} \Rightarrow$ Acá si xq el 6 es mult de 2.

$$\alpha = 7(11)$$

Ejemplo:

$$\begin{array}{l} \left\{ \begin{array}{l} \alpha \equiv 3(10) \\ \alpha \equiv 2(7) \\ \alpha \equiv 5(9) \end{array} \right. \stackrel{s.1}{\Leftrightarrow} \left\{ \begin{array}{l} \alpha \equiv 3(5) \\ \alpha \equiv 3(2) \Rightarrow \alpha \equiv 1(2) \\ \alpha \equiv 2(7) \\ \alpha \equiv 5(9) \end{array} \right. \\ \text{Leyendo: } \end{array}$$

No se repiten primos iguales

Como tienen los módulos 10, 7 y 9 primos entre sí, entre 3 soluciones mod 630.

Plantea 4 sistema y sumar en solución, luego, x_0 es la suma de las soluciones.

$$(S_1) 126\gamma_1 \equiv 3(5) \Leftrightarrow \gamma_1 \equiv 3(5) \Rightarrow x_1 = 378.$$

$$(S_2) 31\gamma_2 \equiv 3(2) \Leftrightarrow \gamma_2 \equiv 3(2) \Rightarrow x_2 = 945$$

$$(S_3) 90\gamma_3 \equiv 2(7) \Leftrightarrow \gamma_3 \equiv 5(7) \Rightarrow x_3 = 450$$

$$(S_4) 70\gamma_4 \equiv 5(9) \Leftrightarrow \gamma_4 \equiv 5(9) \Leftrightarrow \gamma_4 \equiv 2(9) \Rightarrow x_4 = 140$$

$$\text{Entonces } x_0 = 1913, \quad Q \equiv 1913(630) \Leftrightarrow \alpha \equiv 23(630)$$

$$\begin{array}{l} \left\{ \begin{array}{l} 15\alpha \equiv 10(35) \\ 21\alpha \equiv 15(8) \\ 18\alpha \equiv 24(30) \end{array} \right. \text{Quito los números al lado de los} \\ \text{múltiplos de 3.} \\ (18:30) = (2 \cdot 3^2 : 2 \cdot 3 \cdot 5) \mid 6 \mid 24? \lambda' \end{array}$$

$$\begin{array}{l} \left\{ \begin{array}{l} 3\alpha \equiv 2(7) \\ 5\alpha \equiv 7(1) \\ 3\alpha \equiv 4(5) \end{array} \right. \stackrel{\cdot 2}{\Leftrightarrow} \left\{ \begin{array}{l} 6\alpha \equiv 4(7) \\ 15\alpha \equiv 21(8) \\ 6\alpha \equiv 8(5) \end{array} \right. \\ \stackrel{\cdot 3}{\Leftrightarrow} \end{array}$$

• PLIMERO QUITO LETRAS.

$$\begin{array}{l} \left\{ \begin{array}{l} 3\alpha \equiv 4(5) \\ 5\alpha \equiv 7(1) \\ 6\alpha \equiv 8(5) \end{array} \right. \stackrel{\cdot 2}{\Leftrightarrow} \left\{ \begin{array}{l} -6\alpha \equiv 8(5) \\ -\alpha \equiv 7(1) \end{array} \right. \Leftrightarrow \left\{ \begin{array}{l} \alpha \equiv 3(5) \\ \alpha \equiv 5(7) \end{array} \right. \\ \text{Pero } 3(5) \text{ no } \equiv 5(7) \text{ mod } 23. \\ \text{Por lo tanto, } \alpha \equiv 3(5) \text{ mod } 23. \end{array}$$

Como no hay resto que cumpla no se juntan da en una.

Por el TCR de la 3º solución, es única y es módulo 210.

$$\begin{array}{l} (S_1) 42\gamma_1 \equiv 3(5) \Leftrightarrow 2\gamma_1 \equiv 3(5) \Leftrightarrow 6\gamma_1 \equiv 9(5) \\ \Leftrightarrow \gamma_1 \equiv 4(5) \\ \Rightarrow x_1 = 168 \end{array}$$

$$(S_2) 35\gamma_2 \equiv 2(6) \Leftrightarrow -\gamma_2 \equiv 2(6) \Leftrightarrow \gamma_2 \equiv 4(6) \Rightarrow x_2 = 140$$

$$(S_3) 30\gamma_3 \equiv 5(7) \Leftrightarrow 2\gamma_3 \equiv 5(7) \Leftrightarrow \gamma_3 \equiv 2(7) \Rightarrow \gamma_3 \equiv 6(7) \\ \Rightarrow x_3 = 180$$

$$\text{Luego, } \alpha \equiv 488(210) \Leftrightarrow \alpha \equiv 68(210)$$

Ejercicio ladroner: 13 ladrones roban 1000 monedas. Se reparten y sobran 5.

Luego, llaman a 2 y roban 3.

Luego, llaman a 4 y roban 3.

¿Cuántas monedas perdieron en el camino? El sistema no ayuda

$$\Leftrightarrow \begin{cases} a \equiv 3(7) \\ a \equiv 3(1) \\ a \equiv 3(5) \end{cases} \quad \exists \text{ solución } j_1 \text{ en el.} \\ 7, 8, 5 \text{ óptimas para la sol.}$$

$$(S_1) 40j_1 \equiv 3(7) \Leftrightarrow 5j_1 \equiv 3(7) \xrightarrow{\cdot 3} j_1 \equiv 2(7) \\ x_1 = 80$$

$$(S_2) 35j_2 \equiv 3(1) \Leftrightarrow 3j_2 \equiv 3(8) \xrightarrow{\cdot 3} j_2 \equiv 1(8) \\ x_2 = 35$$

$$(S_3) 56j_3 \equiv 3(5) \Leftrightarrow j_3 \equiv 3(5), x_3 = 168$$

$$x \equiv 283(280) \Leftrightarrow x \equiv 3(280) \quad \checkmark$$

A continuación los módulos que dividirán
en total. #módulos = 1000 - x_0.

$$\left| \begin{array}{l} a \equiv 5(13) \\ a \equiv 3(11) \\ a \equiv 3(7) \end{array} \right\} \Leftrightarrow \left| \begin{array}{l} a \equiv 5(13) \\ a \equiv 3(7) \\ a \equiv r(n, m) \end{array} \right.$$

Como $5 \neq 3$ y $13 \neq 7$ dan a sol,
 \exists solución j en MÓDULO 1001.

Por lo tanto $0 < a \leq 1000$ y $0 \leq a_0 < 1001$

$$(S_1) 77j_1 \equiv 5(13) \Leftrightarrow 12j_1 \equiv 5(13) \Leftrightarrow -j_1 \equiv 5(13) \\ \Leftrightarrow j_1 \equiv -5(13)$$

$$\Leftrightarrow j_1 \equiv 8(13)$$

$$\Rightarrow x_1 = 616$$

$$(S_2) 13j_2 \equiv 3(47) \xrightarrow{6177} 78j_2 \equiv 18(47) \Leftrightarrow j_2 \equiv 18(47) \\ \Rightarrow x_2 = 234$$

$$\text{Luego, } a \equiv 850(1001)$$

Por lo tanto, restaremos $1000 - 850$
módulos en el camino. ✓

PEQUEÑO TEOREMA DE FERMAT: a es P PRIMO POSITIVO y
 $a \in \mathbb{Z}_L$.

$$1) a^P \equiv a(P)$$

$$2) \text{ si } P \nmid a \Rightarrow a^{P-1} \equiv 1(P)$$

OBS: \exists P NO primo que hacen valer $a^P \equiv a(P)$. Entonces se llaman
números de Carmichael.

Los dos son equivalentes:

$$1. a^P \equiv a(P), \text{ si } P \nmid a \xrightarrow{\text{Dividir}} a^{P-1} \equiv 1(P)$$

$$2. a^{P-1} \equiv 1(P) \text{ y } P \nmid a \text{ para } a \nmid P \text{ multi para } a, a^P \equiv a(P)$$

$$3) \bullet P \nmid a \Rightarrow a^m \equiv a^{r_{p-1}(m)}(P) \text{ (con } m \in \mathbb{N}, P \text{ PRIMO, } a \in \mathbb{Z})$$

" a^m es congruente a " a " llevado al resto de $p-1$
 $\text{MOD } m$ "

$$\bullet a = 3, P = 2, m = 2$$

$$3^2 \stackrel{r_1(2)}{\equiv} 3(2) \Leftrightarrow 9 \equiv 3(2) \Leftrightarrow 1 \equiv 1(2) \checkmark$$

$$\bullet (a+b)^P = a^P + b^P$$

$$P = 3, (1+2)^3 = 1^3 + 2^3 \\ 9 = 9$$

$$\bullet a^m \equiv_X (P_1, P_2) = \begin{cases} a^m \equiv_X (P_1) \\ a^m \equiv_X (P_2) \end{cases}$$

$$\bullet \text{si } 0 < a < P \text{ con } P \mid \binom{P}{a}$$

$$a = 3, P = 7 \quad 7 \mid \binom{7}{3} (\Rightarrow 7 \mid \frac{7!}{3!4!} \Leftrightarrow 7 \mid \frac{7 \cdot 6 \cdot 5 \cdot 4}{3!4!})$$

$$\Rightarrow 7 \mid \frac{7 \cdot 6 \cdot 5}{6} \Rightarrow 7 \mid 35 \checkmark$$

$$\bullet a^{\frac{(p-1)(q-1)}{PQ}} \equiv 1(PQ) \text{ si } P, Q \text{ son primos distintos}$$

$$a \nmid PQ$$

$$\bullet \text{Si } m \nmid a, \text{ entonces } a^{P(m)} \equiv 1(m) \text{ (TEOREMA DE EULER, si } m \text{ es primo)}$$

$$\bullet \text{Si } a \perp P^r \text{ entonces } a^{P(r-1)} \equiv 1(P^r) \text{ con } P \text{ PRIMO}$$

Ejemplo:

• Calcular $r_{11}(27^{2154}) = 27^{2154} \equiv ?(11) \Leftrightarrow 5^{2154} \equiv ?(11)$ • $r_{11}(24^{13^{1521}}) \Rightarrow$ Por factor.

¿P/F? entre 11/5? No.

Entonces para la potencia aplicar PTF: si $P/F \Rightarrow a^{P-1} \equiv 1(P)$

$$5^{10} \equiv 1(11)$$

$$\text{Luego, } (5)^{10 \cdot 215+4} \stackrel{\text{PTF}}{\equiv} ((5^1)^{10})^{215+4} \stackrel{\text{PTF}}{\equiv} ((5^1)^{10})^{215} \cdot 5^4 \\ \stackrel{\text{PTF}}{\equiv} 1^{215} \cdot 5^4 \stackrel{\text{PTF}}{\equiv} 9(11)$$

$$r_{10}(2^{154})$$

OBS: $(24^{13})^{1521} \neq 2^{13^{1521}}$

$$2^{13^{1521}}$$

$$13^{1521} \equiv ?(10) \text{ pero } 2^{13^{1521}} \equiv r_{10}(13^{1521})(11)$$

$$13^{1521} \equiv 3^{1521} \equiv (3^2)^{760+1} \stackrel{\text{PTF}}{\equiv} (-1) \cdot 3 \equiv 3(10) \\ \Rightarrow 2^{13^{1521}} \equiv 2^{r_{10}(13^{1521})} \equiv 2^3 \equiv 8(11)$$

• Probar que $V_{0.87}, 7|a^{362} - a^{62} = 0^{362} \equiv 0^{62}(7)$

Porque $7|a \Rightarrow$ Porque $7|a$.

Porque $7|a$.

$$a^6 \equiv 1(P), a^{6 \cdot 60+2} - a^{6 \cdot 10+2} \stackrel{\text{PTF}}{\equiv} a^2 - a^2 \equiv 0(7) \\ \Rightarrow a^{362} \equiv a^{62}(7)$$

Porque $7|a$:

$$a^{362} \equiv 0(7) \text{ pero si } 7|a, a \text{ tiene el } 7$$

$$a^{62} \equiv 0(7) \text{ pero si } 7|a, a \text{ tiene el } 7.$$

Luego, $7|a^{362} - a^{62}$ es porque los divisores.

(6s)

"Mis números de los divisores
por 5 da resto 0, y los
divisores por 9 da 1,
y los divisores por 7 da resto
2, y los divisores por 2 da 1"

$$\begin{cases} m \equiv 0(5) \\ m \equiv 2(7) \Leftrightarrow \\ m \equiv 1(2) \\ \boxed{m \equiv 1(4)} \end{cases} \quad \begin{cases} m \equiv 0(5) \\ m \equiv 2(7) \\ m \equiv 1(4) \end{cases}$$

$$2|4 \quad 7|1 \quad 1 \equiv 1(2) \text{ en } 1|4$$

• Determinar los $m \in \mathbb{N}$ tales que $4^m \equiv 1(7)$

Bueno se buscan los m tales que $4^m \equiv 1(7)$ da resto 1. Como luego de $m=6$ la secuencia se repite.

Tengo

m	0	1	2	3	4	5	6
4^m	1	4	2	1	4	2	1

mod 7

Porque m tales que $m \equiv 0(7), m \equiv 3(7), M \equiv 6(7)$

MAL.

Para tomar los posibles neutros en el exponente:

$$4^m \equiv 1(7) \quad \text{7 es primo} \quad 7 \nmid 4$$

$$\text{entonces para PTF } 4^6 \equiv 1(7)$$

Entonces, el 4^6 me indica que hay

7 casos posibles (restos)

$$M=6k+r \quad \text{con } 0 \leq r < 6$$

$$\text{Luego, } 4^{6k+r} \equiv 1(7)$$

$$\Rightarrow 4^{6k} \cdot 4^r \equiv 1(7) \Rightarrow (4^6)^k \cdot 4^r \equiv 1(7) \Rightarrow 1^k \cdot 4^r \equiv 1(7)$$

Luego, r toma de 0 a 6. (lo en todos los restos x2)

Como los (opuestos) 2 o 2

La tabla me ayuda (número hoy es 20).

$$\Gamma = 0, 4^0 \equiv 1 \equiv 1(7) \checkmark$$

$$\Gamma = 1, 4^1 \equiv 4 \equiv 2(7)$$

$$\Gamma = 2, 4^2 \equiv 2(7)$$

$$\Gamma = 3, 4^3 \equiv 1(7) \checkmark$$

$$\Gamma = 4, 4^4 \equiv 4(7)$$

Entonces Γ me sirve.

$$\Gamma = 0, M = 6k$$

$$\Gamma = 3, M = 6k+3 \quad (\text{MULT } 3 \times \text{residuo})$$

Entonces, si δ hoy (número que me da) $\equiv 1(7)$.

Entonces δ en MOD 140

$$\begin{aligned} S_1 \quad 28\delta_1 &\equiv 0(s) \Leftrightarrow 3\delta_1 \equiv 0(s) \\ &\Rightarrow \delta_1 \equiv 0(s) \\ &\Rightarrow x_1 = 0 \end{aligned}$$

$$\begin{aligned} S_2 \quad 20\delta_2 &\equiv 2(7) \Leftrightarrow -\delta_2 \equiv 2(7) \\ &\Leftrightarrow \delta_2 \equiv 5(7) \\ &\Rightarrow x_2 = 100 \end{aligned}$$

$$\begin{aligned} S_3 \quad 35\delta_3 &\equiv 1(4) \Leftrightarrow 3\delta_3 \equiv 1(4) \\ &\Leftrightarrow -\delta_3 \equiv 1(4) \\ &\Leftrightarrow \delta_3 \equiv 3(4) \\ &\Rightarrow x_3 = 105 \end{aligned}$$

Sigue, $M \equiv 205(140) \Rightarrow M \equiv 65(140)$
cierto!

23. Hallar todos los divisores positivos de 25^{70} que sean congruentes a 2 módulo 9 y a 3 módulo 11.

24. Hallar todos los primos $p \in \mathbb{N}$ que satisfacen:

i) $2p \mid 38^{2p^2-p-1} + 3p + 171$

ii) $3p \mid 5^{p-1} + 3^{p^2+2} + 833$

Enton son ejercicios son difíciles xq hoy que tienen
PROP ENTEROS, PTF, CONGRUENCIAS, TCR, Y MÁS.

El 23 esto se resuelve en guía pero haré' hoy en el 24.

$$24) \text{a)} \quad 2P \mid 38^{2P^2-P-1} + 3P + 171$$

P PRIMO. Veo que el 2 divide si $P=2$ entonces
tendrá el 2 en el 4 divide.

Siempre en el 2 en el 4 divide que P es igual al menor
de los dos, por qué? Porque si P es primo y es divisible de 2
(Primos distintos) nula que $a|c \wedge b|c \Rightarrow a|bc$ con $a \neq b$.

$$\text{Caso } P=2: \quad 4 \mid 38^{8-2-1} + 6 + 171$$

Ver en Congruencias Si DIVIDE. Es en un nro que es divisible.

$$3^8 + 6 + 171 \stackrel{5}{\equiv} 1 + 2 + 3 \stackrel{9}{\equiv} 6 \equiv 2(5) \text{ luego, } 4 \text{ NO divide}$$

Descomposición del 4 (caso posible división).

Otro, pues sea $(m, P) \neq 1 \Rightarrow 2 \mid 3^{\frac{2P^2-P-1}{2}} + 3P + 171$
 $\wedge P \mid 3^{\frac{2P^2-P-1}{2}} + 3P + 171$

Caso 2 | $3^{\frac{2P^2-P-1}{2}} + 3P + 171$:

Hay congruencias MOD 2 para ver si divide

$0 + P + 1 \stackrel{(2)}{\equiv} P+1(2)$ Luego, P primo y todos los primos
 excepto el 2 son impares ($3, 5, 7, 11, 13$)
 enti $P+1$ MOD 4 SIEMPRE 0.

$P+1 \stackrel{(2)}{\equiv} 0(2)$

Luego, 2 divide sabiendo que $P \neq 2$.

Caso $P \mid 3^{\frac{2P^2-P-1}{2}} + 3P + 171: (P \neq 2)$

Algo en Caso.

$\rightarrow 19.2 \rightarrow$ 19.2 debe dividir entre el resto del 19
 Caso $P \mid 3^{\frac{2P^2-P-1}{2}}$ \wedge Caso $P \nmid 3^{\frac{2P^2-P-1}{2}}$: ¿Qué significa? Que si
 P divide entre P es divisor de $3^{\frac{2P^2-P-1}{2}}$ como factor primo, si no
 divide no es divisor primo.

Caso $P \mid 3^{\frac{2P^2-P-1}{2}}$:

$$0 + 3P + 171 \stackrel{(P)}{\equiv} 171(P) \text{ luego, } P \text{ posee divisores}$$

$$171 = 3^2 \cdot 19 \text{ solo puede ser } 19 \times 9$$

$$P \mid 3^{\frac{2P^2-P-1}{2}}$$

Contra P = 19: 38 + 3P + 171 3 no es primo.

$$0 + 0 + 0 \equiv 0(19) \\ (19)$$

Luego, P divide $0 - 38^{2P^2-P-1} + 3P + 171$ más $P = 19$ ($P \mid 38$)

Como $P \nmid 38$: Por el PTF, $a^{p-1} \equiv 1(P)$

Para probar que $2P^2-P-1$

$$\begin{array}{r} & P-1 \\ \overline{P-1} & | \\ 2P+1 & \swarrow \\ \overline{P-1} & | \\ 0 & \end{array}$$

Entonces, $38^{2P^2-P-1} \equiv 1(P)$

$$2P^2-P-1 = (P-1) \cdot (2P+1) + 0$$

$$(38^{P-1})^{2P+1} \cdot 38^0 + 3P + 171 \equiv 172(P) \quad 172 = 2^2 \cdot 43$$

Por lo tanto, como sabemos que 2 no divide a 43.

R9A: Luego, la única posibilidad P son 19 y 43.

En $2P$ tienen 38 y 86 (por el 2 divide a 6 y 18).

• Una PTF cuando hay potencias grandes. Si me hay letra potencia determinar para el PTF con P primo que $P/X \dots$

Ej: $S \mid 3 \cdot 2^{102} + 7 \cdot 2^{1472} - 2 \cdot 5^{200}$

\Rightarrow solo oficio PTF y no reemplazando never.

- Si tengo un PPRIMO que se divide entre el P que divido en 2 casos:
 - P | a
 - P ∤ a.

Entonces los casos determinan que veras que da en todo los exp
 Cuando P es un numero que divide a "a" o no.

$$\text{Ej: } 5 \mid \begin{array}{r} 2470 \\ 2a + 70 \end{array} \quad 100$$

$$\text{Ej: } 5 \mid \begin{array}{r} 2470 \\ \underline{5a} + 60 \\ 0 \end{array} \quad 100$$

Responde

IMPORTANT: Como hay dos resultados a un número grande y
 luego al dividirlos en 2 casos, lo verás solucionado en TCR.

- Usamos el TCR Cuanto pertenece en Módulo los COPRIMOS
) luego debemos expresar la solución en ese Módulo inicial

$$\text{Ej: } 35 \mid \begin{array}{r} 2a^{1400} \\ - 3.5a^{2000} \end{array} \Rightarrow \text{Como } 315 \text{ mole } \text{ que}$$

$$3 \mid \begin{array}{r} 2a^{1400} \\ - 3.5a^{2000} \end{array} \wedge 5 \mid \begin{array}{r} 2a^{1400} \\ - 3.5a^{2000} \end{array}$$

Luego, en base a las soluciones de C/u usamos TCR
 para saber MCD 35.

- En los ejemplos donde la incógnita es el P que divido.
 la idea es usar el PTF haciendo divisiones de polinomios.
- En los ejemplos donde nos dan un MCD y se le pide a que
 un número la idea es factorizar el PTF que nos dan y

ver el MCD. Luego ver que factores NO tienen en el MCD.

Otro factor que felicen numeros & envuelta los崇 de
 $x \mid \dots \wedge x' \mid \dots$ entonces operaciones los崇 son
no divisible. 5.2

$$\text{Ej: } (\alpha^2 - 3 : 10) = 5$$

Entonces los崇 donde 2 divide a los segundos.

$$2 \mid \alpha^2 - 3, \text{ por congruencia } \alpha^2 - 3 \equiv \alpha^2 + 1 \pmod{2}$$

2 divide a $\alpha \equiv 1 \pmod{2}$ pues $1^2 + 1 \equiv 0 \pmod{2}$

entonces necesitamos que $\alpha \equiv 0 \pmod{2}$ pues
entre 2 no divide. Si unímos el de $\alpha \equiv 1 \pmod{2}$ el
MCD tiene 10 y no 5.

- En los ejemplos siguientes hallar el resto se una división en algo divisible. Se dice en reposo los MCD en coprimos.

Reposa los崇 de x simple, x' no simple. Luego

Se tiene una solución MCD $x \pmod{x'}$

se hace un TCR $\text{MCD}(x, x')$

- Cuando el número es muy GRANDE (MCD) tenemos congruencia. Cuando lo a mas grande posible,
lo metemos en otra división y seguimos con resto 0.

(Ejemplo MCD en posterior)

Ej:

a los divisores $\text{Div}(41) = \{1, 41\}$

Caso 41:

$$60 + 9 = 7 \pmod{41} \quad \dots \quad c = 1 \pmod{41} \quad \dots \quad C = 1 \pmod{41}$$

$$5a+3 = ?(41) \Leftrightarrow 5a = -3(41) \Leftrightarrow 5a = 33(41)$$

$$\Leftrightarrow -a = 26(41) \Leftrightarrow a = 23(41)$$

$$\cdot 7a+3 = ?(41) \stackrel{6}{\Leftrightarrow} a = -18(41) \Leftrightarrow a = 23(41)$$

$$a = 41k + 23, k=0, a=23$$

$$7(23) + 3 = 0(41) \quad \wedge \quad 5(23) + b = 0(41)$$

Luego, si $a \equiv 23(41)$ el MCD es 41, si $a \neq 23(41)$ el MCD es 1.

Ej 2: (más visual)

Caso 7:

$$2a-3 \stackrel{4}{\equiv} ?(7) \Leftrightarrow a \equiv -16(7)$$

$$\Leftrightarrow a \equiv 5(7)$$

a	0	1	2	3	4	$\boxed{5}$	6
$2a-3$	4	6	1	2	5	$\boxed{0}$	2
$4a^2+10a-10$	4					$\boxed{0}$	

Mod 7

Luego, 7 divide a $a \equiv 5(7)$.

En este se observa que en la congruencia llegamos a lo mismo que la tabla de restas.

IMPORTANTE: ¿Qué pasaría si x ej., $a \equiv 2(7)$ también valdría? ¿Cómo llegaría solo con congruencias?
↳ La anterioridad del modulado.

COMPLEJOS: $z = a + bi$ con $a, b \in \mathbb{R}$

$$\operatorname{Re}(z) = a \quad \operatorname{Im}(z) = b$$

En Cílico MOD 4 $\Rightarrow \{i^0 = 1, i^1 = i, i^2 = -1, i^3 = -i, i^4 = 1, i^5 = i, \dots\}$
 \Rightarrow ej: $7 \bmod 4 = 3 \Rightarrow i^7 = i^3$

Conclusión.

- $a+ib = a'+ib'$ iiii $a=a'$ y $b=b'$
- $(a+ib) + (c+id) = (a+c) + (ib+id)$
 $= (a+c) + i(b+d)$
- $(a+ib) \cdot (c+id) = ac + aid + ibc + i^2 bd$
 $= (ac - bd) + i(ad + bc)$
- $(0+i0) = \text{elemento neutro}$
- $(a-ib) = \underline{\text{Conjugado}}$ (Caracteriza signo o parte $\text{Im}(z)$)
- $|z| = \sqrt{a^2+b^2}$ Módulo
- $|z^2| = |z|^2 = a^2 + b^2$
- $z^{-1} = \frac{\bar{z}}{|z|^2} = \frac{\bar{z}}{|z|^2}$ INVERSO ($z \cdot z^{-1} = 1$)
- $\bar{z} = \overline{\bar{z}}$ iiii \bar{z} no tiene $\text{Im}(\bar{z})$
- $\bar{z}^k = \overline{z^k}$ iiii $k \neq 0, k \in \mathbb{Z}$
- $\overline{z+w} = \bar{z} + \bar{w}$
- $\overline{z \cdot w} = \bar{z} \cdot \bar{w}$
- $|z| \cdot |w| = |z \cdot w|$
- $z + \bar{z} = 2\text{Re}(z)$
- $z - \bar{z} = 2\text{Im}(z)i$
- $|z \cdot w|^2 = (|z| \cdot |w|)^2$

- $|z+w| \leq |z| + |w|$ desigualdad triangular

Los complejos los tenemos ordenados. De aquí con que deben graficarse.

$\rightarrow \arg(z)$

ARGUMENTO PRINCIPAL: le llamamos comúnmente θ y está entre $[0, 2\pi]$. Lo denotamos "él", a los demás, "un" argumentos

¿Por qué le llamamos principal? Porque un complejo puede tener n argumentos que son múltiplos de $2k\pi$ con $k \in \mathbb{Z}$.

OBS: Cuando nos pidan argumentos, θ debe estar entre $[0, 2\pi]$

Ej: si el argumento es -3.50RAD , le sumo múltiplos de $2k\pi$.

El primer k que nos da argumento positivo es el arg principal

$$\theta = -3.50 + 2\pi = 2.78 \text{ RAD en el arg principal.}$$

Ej: Arg en 12.50RAD ; es el principal? No, pues el MÁXIMO es $2\pi \approx 6.28 \text{ RAD}$ Luego, $\theta = 12.50\text{RAD} - 2\pi = 6.21\text{RAD}$. Luego, 6.21RAD es el argumento principal.

FORMAS DE DESCRIBIR COMPLEJOS:

• BINÓMICA: $a+bi$ con $a, b \in \mathbb{R}$. Usil para sumar.

• POLAR/TRIGONOMÉTRICA: $|z| \cdot (\cos(\theta) + i \sin(\theta))$ con $\theta \in [0, 2\pi]$.
 \hookrightarrow Usil para multiplicar.

• EXPONENCIAL: $|z| \cdot e^{i\theta}$

POLAR A BINÓMICA

$$a = |z| \cdot \cos(\theta)$$

BINÓMICA A POLAR:

$$|z| = \sqrt{a^2 + b^2}$$

$$b = |z| \cdot \operatorname{sen}(\theta)$$

$$\operatorname{Ang}(z) = \operatorname{arctan}\left(\frac{b}{a}\right)$$

(-+)	(++)
180°	0°
180°	360°
(-1)	(+1)

OBS: Luego, opción:

TABLA ÁNGULOS NOTABLES:

θ	0	$\frac{\pi}{6}$	$\frac{\pi}{4}$	$\frac{\pi}{3}$	$\frac{\pi}{2}$
$\operatorname{sen} \theta$	$\frac{\sqrt{0}}{2}$	$\frac{\sqrt{1}}{2}$	$\frac{\sqrt{2}}{2}$	$\frac{\sqrt{3}}{2}$	$\frac{\sqrt{4}}{2}$
$\cos \theta$	1	$\frac{\sqrt{3}}{2}$	$\frac{\sqrt{2}}{2}$	$\frac{1}{2}$	0

θ	0	$\frac{\pi}{6}$	$\frac{\pi}{4}$	$\frac{\pi}{3}$	$\frac{\pi}{2}$
$\operatorname{sen} \theta$	0	$\frac{1}{2}$	$\frac{\sqrt{2}}{2}$	$\frac{\sqrt{3}}{2}$	1
$\cos \theta$	1	$\frac{\sqrt{3}}{2}$	$\frac{\sqrt{2}}{2}$	$\frac{1}{2}$	0

IMAGINARIO PURO: No tiene MÓDULO. Verde lae lo que sea con eye x.

$$\text{ej: } z = -i, \operatorname{Ang}(z) = 270^\circ, \frac{3\pi}{2}$$

$$e^{ib} = (\cos(\theta) + i \operatorname{sen}(\theta))$$

COS es FUNCIÓN PAR $\Rightarrow \cos(-x) = x$

SEN es FUNCIÓN IMPAR $\Rightarrow \operatorname{sen}(-x) = -x$

TODO: Ver más tarde $w^2 = z$

TEOREMA: Siempre existe raíz cuadrada de complejo de orden 2.

* MULTIPLICACIÓN DE COMPLEJOS EN POLAR:

$$w = r_1 (\cos \theta_1 + i \operatorname{sen} \theta_1) \Rightarrow w \cdot z = r_1 r_2 (\cos(\theta_1 + \theta_2) + i \operatorname{sen}(\theta_1 + \theta_2))$$

$$z = r_2 (\cos \theta_2 + i \operatorname{sen} \theta_2)$$

* DIVISIÓN DE COMPLEJOS EN POLAR:

$$w = r_1 (\cos \theta_1 + i \operatorname{sen} \theta_1) \Rightarrow z \cdot w = \frac{r_1}{r_2} (\cos(\theta_1 - \theta_2) + i \operatorname{sen}(\theta_1 - \theta_2))$$

$$z = r \cdot (\cos \alpha + i \sin \alpha) \Rightarrow \frac{w}{z} = \frac{1}{r} \cdot (\cos(\theta - \alpha) + i \sin(\theta - \alpha))$$

* Validez siempre que $\theta \in [0, 2\pi)$

FÓRMULA DE MOIVRE: $z^m = r^m (\cos(m\theta) + i \sin(m\theta))$

PROPIEDADES FUNDAMENTALES:

- $\operatorname{Arg}(z \cdot w) = \operatorname{Arg}(z) + \operatorname{Arg}(w)$ OJO: VER SI ESTÁ ENTRE $[0, 2\pi)$
- $\cos(\theta + \phi) = \cos \theta \cdot \cos \phi - \sin \theta \cdot \sin \phi$
- $\sin(\theta + \phi) = \sin \theta \cdot \cos \phi + \cos \theta \cdot \sin \phi$

OBS: $\theta, \theta + 2\pi$ RAD y $\theta + 2\pi$ RAD tienen el mismo complejo pero difieren en un múltiplo de 2π .

Luego, $z^m = r^m (\cos(m\alpha) + i \sin(m\alpha))$

$$\begin{cases} r^m = r \\ m\alpha - \alpha = 2\pi k \quad k \in \mathbb{Z} \end{cases} \Leftrightarrow \begin{cases} r = \sqrt[m]{r} \\ \theta = \frac{\alpha}{m} + \frac{2\pi k}{m} \quad k \in \mathbb{Z} \end{cases}$$

Entonces,

$$w_k = \sqrt[m]{r} \left(\cos \left(\frac{\alpha}{m} + \frac{2\pi k}{m} \right) + i \sin \left(\frac{\alpha}{m} + \frac{2\pi k}{m} \right) \right)$$

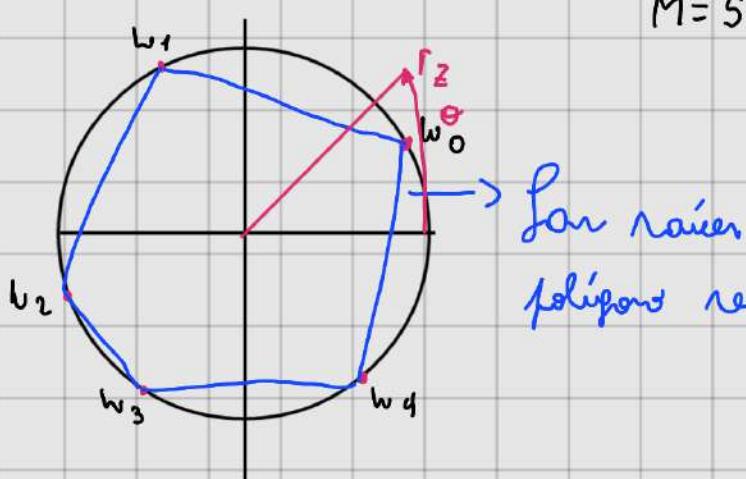
Es una raíz enésima de $z / w^m = z$

OBS: Dos complejos iguales no tienen el mismo módulo si difieren en un ángulo de $2\pi k$ enteros.

$$w_k \equiv w_l \Leftrightarrow k \in l(m)$$

Z tiene exactamente m raíces m -ésimas
 $w_0, w_1, w_2, \dots, w_{n-1}$.

GRÁFICO DE RAÍCES n -ÉSIMAS:



Las raíces m -ésimas forman un polígono regular de m

Vea que w_7 tiene 7 nodos, o sea, w_7 tiene w_2 .
 w_5 tiene 5 nodos, o sea, w_5 tiene w_0 .

RAÍCES PRIMITIVAS DE LA UNIDAD: Si solo las encuentran estas,
solo las encuentran todas. Estas raíces m -ésimas elevadas a la m da de Z .

$$w_k = \cos\left(\frac{2\pi}{m}k\right) + i \sin\left(\frac{2\pi}{m}k\right)$$

Sean x, y dos raíces m -ésimas de $Z \Rightarrow x^m = Z$ y $y^m = Z$

Luego, si dividir 2 raíces m -ésimas, debe dar 1.

$$\left(\frac{x}{y}\right)^m = \frac{x^m}{y^m} = \frac{Z}{Z} = 1$$

Luego, $v = \frac{x}{y}$ es una raíz m -ésima de 1.

DIBS: $(-1)^2 = [(-1) \cdot 1]^2$

$$= (-1)^2 \cdot 1^2 = 1$$

$$\begin{aligned} (-i)^2 &= ((-1) \cdot i)^2 \\ &= (-1)^2 \cdot i^2 \\ &= -1 \end{aligned}$$

• ¿Qué valores MAX de m puede tomar un complejo?

Ej: $(1 - \sqrt{3}i)^m \Rightarrow$ 1. Calcular $|z|$ y $\operatorname{Arg}(z)$ para que esté en el cuadrante inferior y θ esté entre $[0; 2\pi]$ con $0 \leq \theta < 2\pi$.

Luego, ¿Qué m puede tomar?

Primero $m=1, m=2$ haciendo que el Arg sea $\leq 2\pi$. Luego se hace para $m=3, m=4$ etc. el próximo m .

Luego, $m=0, m=1, \dots, m-1$. OJO: m tiene $\geq 2\pi \times$ los ms mds.

$$\text{Ej: } z^m \Rightarrow 2^m \left(\cos\left(\frac{2\pi}{3} \cdot m\right) + i \sin\left(\frac{2\pi}{3} \cdot m\right) \right)$$

Donde, m posee ms paros de 2π , siendo los:

$\rightarrow m_{\max}, m=3$ da $\operatorname{Arg}(z) = 2\pi$ es la més grande

$$m=1, m=2, m=3$$

para el Arg debe ser $0 \leq \frac{2\pi}{3} \cdot m < 2\pi$

Luego, $m=0 \vee m=1 \vee m=2$

$$\text{si } m=0 \Rightarrow 1$$

$$\text{si } m=1 \Rightarrow 2 \left(\cos\left(\frac{2\pi}{3}\right) + i \sin\left(\frac{2\pi}{3}\right) \right)$$

$$\text{si } m=2 \Rightarrow \frac{2\pi}{3} \cdot 2 = \frac{4\pi}{3} \Rightarrow 4 \left(\cos\left(\frac{4\pi}{3}\right) + i \sin\left(\frac{4\pi}{3}\right) \right)$$

CONCLUSIÓN: m no nos impone la otra limitación el que se pone de 2π para determinar M.

$$\text{OJO: } \underline{z^6 = 8+i} \neq \underline{z = (8+i)^6}.$$

MOIVRE

$$0 \leq k < 6$$

RAÍCES n-ASIMAS

MOIVRE PERO

1 sola solución

$$|z|^6 \cdot (\cos(\arg(8+i) \cdot 6) \dots)$$

$$\begin{aligned} &\text{line media} - 2\pi k \theta \\ &+ 2\pi k \end{aligned}$$

$$|z|^6 \cdot (\cos(\arg(8+i) + 2k\pi))$$

$$\frac{1}{M}$$

entre Ojs.

- Si me piden hallar los los $n \in \mathbb{N}$ tales que n-ésima raíz de unidad en la medida que argumento del complejo resulte igual al que se pide.

Raíces n -ésimas de la unidad: $G_n = \{ z \in \mathbb{C} / z^n = 1 \}$

Propiedades de las raíces n -ésimas:

recuerda que el n , si es menor a que n , da 1.

- $z, w \in G_n \Rightarrow z \cdot w \in G_n$
 - $z \in G_n \Rightarrow z^{-1} \in G_n$
 - $1 \in G_n$
 - $(z \cdot w) \cdot v = z \cdot (w \cdot v)$
 - $z \cdot w = w \cdot z$
 - $z^{-1} = \overline{z} = z^{n-1}$
- El producto es asociativo
y Commutativo*

Aquellos que cumplen 1,2,3,4 son llamados "grupos"
y si se cumple el 5º se llama "grupo ABELIANO"

Inverso de un complejo (z) que $z \in G_m$:

$$z^{-1} = \overline{z}$$

$$\overline{\overline{w}} = \overline{w^m}$$

\Downarrow

$$\text{Ej: Si } w \in G_3 \text{ y Tengo } \overline{w}^s \text{ Entonces: } \overline{w}^s = \overline{w^s} = (\overline{w})^s = w^{-s} = w^3$$

Los raíces complejas tienen SIEMPRE DE A PARES, es decir, si $a+bi$ es raíz, $a-bi$ también

Número Geométrico en G_m : Que O si $w \neq 1$, y si $w=1$ da m

$$\sum_{k=0}^m w^k = \begin{cases} 0 \text{ si } w \neq 1 \\ m \text{ si } w=1 \end{cases}$$

Ent, si tenemos $G_7 \sum_{k=0}^6 w^k$ Ent, la suma da O .

Para Cada $w \in G_6$ Calcular:

OBS: En G_m solo le suman los pot en los w. No le hace el MÓDULO en COEFICIENTE.

$$\begin{aligned} & w^1 + w^{-14} + 5 \cdot \overline{w}^4 + w^{39} - 4w^{-28} + w^{2023} \\ &= w^5 + w^4 + 5 \cdot w^4 + w^3 - 4w^2 + w \\ &= w^5 + w^4 + 5(w^4)^{-1} + w^3 - 4w^2 + w \\ &= w^5 + w^4 + 5w^2 + w^3 - 4w^2 + w \end{aligned}$$

$$= w^5 + w^4 + w^3 + w^2 + w^1 = \sum_{k=1}^5 w^k = \left(\sum_{k=0}^5 w^k \right) - w^0$$

1

$$\Rightarrow \begin{cases} \frac{w^6 - 1}{w - 1} & \text{si } w \neq 1 \\ 5 + 1 & \text{si } w = 1 \end{cases}$$

$$\Rightarrow \begin{cases} 0 - 1 = -1 & \text{si } w \neq 1 \\ 6 - 1 = 5 & \text{si } w = 1 \end{cases}$$

Para Cada $w \in G_5$, Calcular $w^{103} + w^{27} + w^{-4} + \overline{w}$

$$w^3 + w^2 + w^{5-4} + w^{-1} \Rightarrow w^3 + w^2 + w + w^4$$

$$\Rightarrow w^4 + w^3 + w^2 + w^1$$

$$\Rightarrow \sum_{k=1}^4 w^k = \left(\sum_{k=0}^4 w^k \right) - w^0 = \begin{cases} 1 & \text{if } w \neq 1 \\ \frac{w^5 - 1}{w - 1} & \text{if } w = 1 \end{cases}$$

$$= \begin{cases} 0 - 1 = -1 & \text{if } w \neq 1 \\ 5 - 1 = 4 & \text{if } w = 1 \end{cases}$$

PROPIEDAD EXPONENTES $z \in G_m \Rightarrow z^k = z^{\Gamma_m(k)}$

Ej: si $w \in w^5$ y w^{10} entonces $w^{10} = w^0, w^{-4} = w^1$

PROPIEDAD DE "INCLUSIÓN" DE G_M : $z \in G_M, d | M \Rightarrow z^d \in G_{\frac{M}{d}}$

Ej: • $z \in G_6, 2 | 6 \Rightarrow z^2 \in G_{\frac{6}{2}} \Rightarrow z^2 \in G_3$

• $z \in G_{12}, 4 | 12 \Rightarrow z^4 \in G_{\frac{12}{4}} \Rightarrow z^4 \in G_3$

Ej: Calcule, en $z \in G_6$, $1 + z^2 + z^4$

MÁS PROPIEDADES:

1. $m | m \Rightarrow G_m \subset G_m$

$$2. G_m \cap G_m \Rightarrow G_{(m:m)}$$

$$3. G_m \subset G_m \Leftrightarrow M \mid m$$

Ej: Sea $Z \in G_6$. Calcular $1 + z^2 + z^4$

$$Z \in G_m \quad d \mid m \Rightarrow z^{\frac{d}{m}} \in G_{\frac{m}{d}}$$

SUMA Y PRODUCTO DE ELEMENTOS DE G_n : si $m > 1$

$$\sum_{w \in G_m} w = 0$$

$$\prod_{w \in G_m} w = \begin{cases} 1 & \text{si } m \text{ impar} \\ -1 & \text{si } m \text{ par} \end{cases}$$

POLINOMIOS: Son de la forma $a_{x^m} + a_{x^{m-1}} + \dots + a_0$.

Viven en un Cuerpo $K[x]$: $\mathbb{Q}, \mathbb{Z}, \mathbb{R}, \mathbb{C}$ y los permiten x vivir en ese Cuerpo K.

POLINOMIO NULO: El polinomio CERO. O sea $P(x) = 0$ es la suma 1 en el producto.

IGUALDAD DE POLINOMIOS: Dos polinomios f y g son iguales si tienen iguales COEFICIENTE a COEFICIENTE.

Ej: $f = x^2 + 4$ $g = (x-2)(x+2)$ $f \neq g$

$$f = x+2 \quad g = x+2 \quad f = g$$

$$f = x^2 + 2 \quad g = x^4 - x^4 + x^2 + 4 - 2 \quad f = g$$

COEFICIENTE PRINCIPAL DE UN POLINOMIO: Es aquel número

jue le corresponde a la x con mayor grado.

Ej: $f = x^2 + 2x^5 + x^4 + 3x^3$ $CP(f) = 2$

POLINOMIOS CONSTANTES: Son números.

Ej: $f = 1, f = 2$

GRADO DE UN POLINOMIO: Existe siempre el polinomio NO nulo. Es la mayor potencia de un x.

Ej: $f = x+1 \quad g_r(f) = 1 \quad f = 1 \quad g_r(f) = 0$

¿Cómo saber el grado?

Siempre es el más grande, pero:

$$f: x^2 + 1 \quad g: -x^2 + 1 \quad g_r(f+g) = 0$$

• Si $g_r(f) \neq g_r(g) \Rightarrow g_r(f+g) = \text{MAX}\{g_r(f), g_r(g)\}$

Ej: $f: x^2 + 4 \quad g: x + 1 \Rightarrow g_r(f+g) = 2$

• Si $g_r(f) = g_r(g)$ pero $CP(f) + CP(g) \neq 0$

$$\Rightarrow g_r(f+g) = g_r(f) = g_r(g)$$

Ej: $f: 2x^2 + 2 \quad g: x^2 - 1$

$$\Rightarrow g_r(f+g) = 2$$

• Si $g_r(f) = g_r(g)$ y $CP(f) + CP(g) = 0$

$$\Rightarrow g_r(f+g) < \text{MAX}\{g_r(f), g_r(g)\}$$

$$\text{Ej: } f: x^2 + 1 \quad g: -x^2 + 2 \quad g_n(f+g) = 0$$

$$\cdot \quad g_n(f+g) \leq \max\{g_n(f), g_n(g)\} \quad \text{SIEMPRE}$$

POLINOMIO MÓNICO: su CP es 1.

Ej: $f = x^5 + 2$ es monico pues el CP que acompaña
al grado mayor es 1.

→ se obtiene haciendo: $\frac{f}{CP(f)}$

TÉRMINO INDEPENDIENTE DE UN POLINOMIO: Es aquel que no
acompaña a la x .

PROPIEDADES DEL GRADO, CP Y T.i.:

- $g_n(f) + g_n(g) = g_n(fg)$
- $CP(fg) = CP(f) \cdot CP(g)$
- $T_i(fg) = T_i(f) \cdot T_i(g)$

IMPORTANCIA DEL CUERPO DE UN POLINOMIO: No permite
que se den las raíces.

$$\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$$

POLINOMIOS INVARIABLES: Si un polinomio es inviable entonces
es un polinomio constante.

$$f \sim g$$

POLINOMIOS ASOCIADOS: Un polinomio f es asociado con g
si cuando multiplicas el polinomio f por un polinomio constante k one de f .

$$\text{Ej: } f: (x^2 + 2x + 1) \quad g: 2x^2 + 4x + 2$$

$$c \cdot f \cdot h = g \quad \text{dado, } h = 2$$

$$f \cdot h = g \Leftrightarrow 2(x^2 + 2x + 1) \Rightarrow 2x^2 + 4x + 2$$

De la mano de esto surge la Divisibilidad de polinomios

Divisibilidad de polinomios: Un polinomio f es divisible por g si existe un polinomio h tq $f = g \cdot h$ y en ese caso $g | f$, $f, g \in K[x]$.

$$\left. \begin{array}{l} \text{Escribimos } f = g(m) \text{ si } m | f \cdot g \\ g | f \Leftrightarrow \exists q \in K[x] / f = q \cdot g \end{array} \right\}$$

Vale la transitoriedad.

Vale la división por múltiplos: $f | g \Rightarrow Cf | g$ con $C \in K$

PROPIEDADES:

- $f | 0, \forall f \in K[x]$
- $g | f \Leftrightarrow \tilde{g} | \tilde{f} \cdot \tilde{q}: g: (x+1) f: (2x+2) \tilde{g}: 2x+2 \tilde{f}: (6x+6)$
SI TIENEN MISMO GRADO Y SE DIVIDEN DIFEREN EN UN K
- $g | f \wedge g | (g \cdot h) = g \cdot (g | h) \Rightarrow g \sim f$
In g divide a f pero multiplicar a g y f por C $\in K$ divierte su igualdad.

POL CONST
Divisores asegurados
 $\therefore C/f \quad c \in K \setminus 0$

2.0
 $\therefore Cf | f \quad c \in K \setminus 0$

$\therefore g | f \Leftrightarrow \frac{g}{f} | f$

g = g(f)
(no asociados)

$C_P(g)$
g monómico

TODO POLINOMIO es PRODUCTO DE POLINOMIOS IRREDUCIBLES

Divisores asegurados de un polinomio: SIEMPRE VALE $A \in K$

C/f : Polinomios constantes (c)

\hookrightarrow Ej: $f: 4x+6$ y $c: 2x+3$ vale.

Cf/f : Polinomios asociados a f .

→ Ej: $f: x+1$ y $c: 3$

Ent $\frac{g}{3x+3}$ es un divisor organo de f

Ora f tiene 2 divisores monicos distintos asegurados:

$$\begin{array}{c} 1 \quad g \\ \hline f \\ (p(f)) \end{array}$$

POLINOMIO IRREDUCIBLE: Se relacionan con el concepto de número primo. Es aquel polinomio f que es divisible por si mismo o el polinomio constante 1.

Es importante considerar el contexto de irreducibilidad: p.ej.
según el cuerpo donde trabaje p.ej. es reducible o no.

Ej: $x^2 + 1$ es irreducible en \mathbb{Z}, \mathbb{R} y \mathbb{Q} pero es reducible en $\mathbb{C}[x]$.

Se dice que f es IRREDUCIBLE si:

- $f \notin K$
- Los únicos divisores de f son los orgános.

POLINOMIO REDUCIBLE: se escribe en base al factor de polinomio irreducibles. Se dice que f es reducible si $\exists g \in K[x] / g | f$ con $0 < q_r(g) < q_r(f)$

ALGORITMO DE DIVISIÓN: Sean $f, g \in K[x]$ con $g \neq 0$, entonces existen únicos $q, r \in K[x]$ tales que $f = q \cdot g + r$ (con $r = 0$ ó $q_r(r) < q_r(g)$)

$$\text{Ej: } x^2 + 2x + 4 \quad |x+2$$

$$-(x^2 + 2x) \quad x$$

4

↓ Como $g_n(r) < g_n(g)$ ent el resto es 4.

$$\text{Luego, } x^2 + 1x + 4 = (x+2) \cdot x + 4$$

POLINOMIOS EN $\mathbb{Z}/p\mathbb{Z}$: Valen las mismas PROPIEDADES que anter.
La diferencia es que p es PRIMO.

Ej: $x^2 + \bar{1} \in \mathbb{Z}/5\mathbb{Z}[x]$ ¿ Es reducible o irreducible?

$$x^2 + \bar{1} \text{ nod } 5 \Rightarrow x^2 - \bar{4} = (x - \bar{2})(x + \bar{2})$$

$$\text{Luego } x - \bar{2} \mid x^2 + \bar{1} \wedge x + \bar{2} \mid x^2 + \bar{1} \Rightarrow (x - \bar{3})(x + \bar{2})$$

Entonces $x^2 + 1$ es REDUCIBLE en $\mathbb{Z}/5\mathbb{Z}$

Ej: $x^2 + \bar{1}$ en $\mathbb{Z}/7\mathbb{Z}$

$$x^2 + \bar{1} \text{ nod } 7 \Rightarrow x^2 - \bar{6} \Rightarrow \text{no se puede.}$$

$$x^2 + 1 = (x + \bar{a})(x + \bar{b}) = x^2 + \underbrace{x\bar{b} + \bar{a}x}_{\substack{1 \rightarrow \text{Expres de res} \\ \text{Expres red}}} - \bar{ab}$$

$$\Rightarrow \bar{ab} = \bar{1}$$

$$\Rightarrow x(\bar{b} + \bar{a}) = \bar{0}$$

$$\Rightarrow \bar{b} = -\bar{a} \quad \text{y} \quad -\bar{a}\bar{a} = \bar{1}$$

!!

$$\frac{y^2}{a^2} = -1$$

Er steht $\overline{-1}$ an den Enden.

$$\begin{array}{c|cccccc} \bar{0} & \bar{0} & \bar{1} & \bar{2} & \bar{3} & \bar{4} & \bar{5} & \bar{6} \\ \hline \bar{0}^2 & \bar{0} & \bar{1} & \bar{4} & \bar{2} & \bar{2} & \bar{9} & \bar{7} \end{array} \quad \neq -\bar{1} = \bar{6}$$

Ora, $x^2 + 1$ è irreducibile su $\mathbb{Z}/7\mathbb{Z}$

- $$\bullet \quad f: x^4 - 1 \quad g: 2x^2 + 3 \text{ en } \mathbb{Z}/5\mathbb{Z}$$

$$\begin{array}{r}
 \begin{array}{l}
 \text{6x}^2 \text{ mds} \\
 x^4 - 1 \quad | \quad \overline{2x^2 + 3} \\
 - (x^4 + \bar{4}x^2) \\
 \hline
 -\bar{4}x^2 - 1 \\
 - (-\bar{4}x^2 - \bar{6}) \\
 \hline
 0
 \end{array}
 \quad
 \left\{
 \begin{array}{l}
 x^4 + \bar{4} \quad | \quad \overline{\bar{2}x^2 + 3} \quad -\frac{1}{2} \notin \mathbb{Z} \\
 - (x^4 + 4x^2) \quad | \quad \bar{3}x^2 - \frac{1}{2} \nearrow \\
 \hline
 x^2 + \bar{4} \\
 - (
 \end{array}
 \right.
 \end{array}$$

¿Dónde para ti ofir el mob en los negocia o no?
¿Debería llegar a la misma? sí

MAXIMO COMUN DIVISOR: Sean $f, g \in K[x]$

el MCD entre f y g es el polinomio monico de mayor grado que divide a ambos en $K[x]$.

PROPIEDADES:

$$\cdot f \neq 0 \Rightarrow (f:0) = \underline{f} \quad \text{!Mópico!}$$

$$\cdot (f: g) = (g: r)^{CP(f)}$$

$$\cdot c \in K^{\times} \Rightarrow (c:g) = 1 \Rightarrow g: c = 3, (3:x^2+1) = 1$$

$$\cdot g|f \Rightarrow (f:g) = \frac{g}{CP(g)} \quad g \neq 0$$

ALGORITMO DE EUCLIDES: El MCD en el ANTEÚLTIMO RESTO.

$$\begin{array}{r} x^{10} - 1 \\ - (x^6 - x^4) \\ \hline x^4 - 1 \end{array} \quad \begin{array}{r} |x^6 - 1 \\ x^4 \end{array} \quad \begin{array}{l} \cdot r_1 = x^6 - 1 \\ \cdot r_2 = x^2 - 1 \end{array}$$

$$\begin{array}{r} x^6 - 1 \\ - (x^6 - x^2) \\ \hline x^2 - 1 \end{array} \quad \begin{array}{r} |x^4 - 1 \\ x^2 \end{array} \quad \begin{array}{l} \cdot r_3 = x^2 - 1 \\ \cdot r_4 = 0 \end{array}$$

$$\begin{array}{r} x^2 - 1 \\ - x^2 - 1 \\ \hline 0 \end{array} \quad \begin{array}{r} |x^2 - 1 \\ 1 \end{array}$$

$$(x^6 - 1 : x^2 - 1) = (x^2 - 1 : 0) = x^2 - 1$$

La ÚNICA FORMA DE HALLAR EL MCD ES USANDO EUCLIDES.

PROPIEDADES ESENCIALES DEL MCD: Sean $f, g \in K[x]$

- $(f:g) \mid f \wedge (f:g) \mid g$
 - $\exists \lambda, \tau \in K[X] \text{ s.t. } (f:g) = \lambda f + \tau g$
 - Si $R \mid f \wedge R \mid g \Rightarrow R \mid (f:g)$
- Ej: $R: x+2 \quad f: 2x+4 \quad g: 3x+6$

$$x+2 \mid 2x+4 \wedge x+2 \mid 3x+6 \Rightarrow (x+2) \mid (2x+4 : 3x+6)$$

$$\begin{array}{r} 3x+6 \mid 2x+4 \\ - (3x+6) \quad \frac{3}{2} \\ \hline 0 \end{array}$$

¿Es esto válido en $K[X]$ o $R[X]$, no?

POLINOMIOS COPRIMOS: Sean $f, g \in K[X]$.

$f \wedge g$ son coprimos si $(f:g)=1$

COPRIMIZAR: $\frac{f}{(f:g)} \wedge \frac{g}{(f:g)}$ son coprimos

PROPIEDADES: Los mismos que los enteros

- $(f:R) = 1 \iff R \mid f \wedge g \iff R \mid f$
- $(f:g) = 1, \quad R \mid f \wedge g \mid f \iff R \mid g$
- Si f es IRREDUCIBLE $\wedge f \mid g \cdot h \iff f \mid g \wedge f \mid h$

Algo $f \in K[X]$ ($f \notin K$) si $g \mid f$ es MÓNICO entónce
 $\exists \lambda \in K \text{ s.t. } g = \underline{f} \lambda$ no es CONSTANTE

Entonces, si $g \in K[X]$ cumplimos

$$(f:g) = \begin{cases} 1 & \text{si } f \nmid g \\ \text{no es constante} & \end{cases}$$

$$\left\{ \begin{array}{l} f \text{ si } f \in \mathbb{F} \\ \frac{f}{CP(f)} \text{ si } f \notin \mathbb{F} \end{array} \right.$$

TFA PARA POLINOMIOS: Sea un polinomio f , hay una única forma de escribirlo como producto de polinomios irreducibles.

$$\text{Ej: } (x^2+1)(x^2-2) \in \mathbb{Q}[x], \mathbb{R}[x] \text{ o en } \mathbb{C}[x].$$

IRREDUCIBLE EN $\mathbb{Q}[x]$.

REDUCIBLE A $(x^2+1)(x-\sqrt{2})(x+\sqrt{2})$ EN $\mathbb{R}[x]$.

REDUCIBLE A $(x-i)(x+i)(x-\sqrt{2})(x+\sqrt{2})$ EN $\mathbb{C}[x]$

EN $\mathbb{Q}[x]$ PUEDEN SER IRREDUCIBLES DE CUALQUIER GRADO

EN $\mathbb{R}[x]$ SON IRREDUCIBLES DE GRADO 1 O 2.

EN $\mathbb{C}[x]$ SON IRREDUCIBLES EN GRADO 1

↳ Vienen de a parar.

RAÍCES DE UN POLINOMIO: Son aquellas α que hacen que la función evaluada en α sea 0.

Para buscar raíces usamos los derivados, $f(\alpha), f'(\alpha) \dots$

→ α es raíz simple $f \Leftrightarrow (x-\alpha) \mid f \text{ y } (x-\alpha)^2 \nmid f$
 $\cdot f(\alpha)=0 \text{ pero } f'(\alpha) \neq 0$

→ α es raíz múltiple de $f \Leftrightarrow (x-\alpha)^m \mid f \text{ y el resto } (x-\alpha)^m \nmid f$
 $(\alpha, f)=m \text{ con } (x-\alpha)^m \mid f \text{ y } (x-\alpha)^{m+1} \nmid f$.

· $f'(\alpha)=0 \text{ y } f''(\alpha)=0 \text{ pero } f^{m+1}(\alpha) \neq 0$.

OBS: $\text{m}(x, f) \leq g(x)$ para no perder más raíces que los de polinomio

PROPIEDADES DE RAÍCES MÚLTIPLES:

$$\cdot (f+g)' = f' + g'$$

$$\cdot (fg)' = f'g + fg'$$

$$\cdot (g \circ f) = g'(f) \cdot f' \Rightarrow m(x-\alpha)^{m-1}$$

$$\cdot f'' = (f')' \in K[x]$$

$$\cdot f^{(m)} = (f^{(m-1)})' \rightarrow f, f', f'', \dots$$

Dadas 1, 2 o n veces se repite en $K[x]$.

Ej: sea $f = 2x^5 + 7x^4 + 2x^3 + 1$ probar q no tiene raíz mult.

Si f tiene raíz múltiple de orden nol q se

$$f(\alpha) = 0 \quad \text{y} \quad f'(\alpha) = 0$$

$$f' = 30x^4 + 49x^6 + 6x^2$$

La única forma q se f' sea 0 es q

$$x = 0.$$

Luego, $f'(0) = 0$ pero $f(0) = 1$ luego,

f no tiene raíces múltiples

Entonces para q $\alpha \in \mathbb{C}$ no sea

$f: x^8 - 2x^4 + a$ tiene raíces múltiples en \mathbb{C}

$$f' = 8x^7 - 8x^3 \Rightarrow 8x^3(x^4 - 1) \Rightarrow x=0 \vee x=1$$

$$f(0) = 0^8 - 2(0)^4 + a \\ = a \Rightarrow a \text{ debe ser } 0$$

$$f(1) = 1^8 - 2(1)^4 + a \\ = 1 - 2 + a \Rightarrow a \text{ debe ser } 1.$$

VERIF:

$$a=0, f = x^8 - 2x^4 + 0$$

$$f' = 8x^7 - 8x^3 \Rightarrow \boxed{x=0} \vee \boxed{x=1}$$

$$f(0) = 0 - 2(0)^4 + 0 = 0, f(1) \text{ no nula.}$$

0 en raíz múltiple si $a=0$

$$a=1, f = x^8 - 2x^4 + 1$$

$$f' = 8x^7 - 8x^3 \Rightarrow \boxed{x=0} \vee \boxed{x=1}$$

$$f(1) = 1^8 - 2(1)^4 + 1 = 0, f(0) \text{ no nula.}$$

1 en raíz múltiple si $a=1$

EVALUACIÓN Y RAÍZ: sea $f \in K[x]$ y $\alpha \in K$, llamamos "evaluación de f en α " al reemplazar la indeterminada x por α .

Ej: $f: 2x+5$ en $\mathbb{Q}[x]$, $\alpha=-5$ es raíz pues $2(-5)+5=0$

PROPIEDADES:

$$\cdot f+g(\alpha) = f(\alpha) + g(\alpha)$$

$$\cdot f \cdot g(\alpha) = f(\alpha) \cdot g(\alpha)$$

$$\cdot f = q \cdot g + r \Rightarrow f(\alpha) = q(\alpha) \cdot g(\alpha) + r(\alpha)$$

OBS OBVIA: Si f es un polinomio constante (C), sea cual sea α , siempre

$$f(\alpha) = C.$$

$$f(x) = 10 \quad x=1, \quad f(1)=10 \quad f(2)=10\dots$$

Polinomio nómico

TEOREMA DEL RESTO: $f \text{ Mod } (x-\alpha) = f(\alpha)$

$$\text{Ej: } x^2 - 4 \Rightarrow 2 \text{ es raíz} \Rightarrow (x-2) \text{ es Raiz}$$

$$\text{Entonces } f(2) = (x^2 - 4) \text{ Mod } (x-2)$$

$$\begin{array}{r} \boxed{x^2 - 4} \\ \underline{- (x^2 - 2x)} \quad |x-2 \\ \hline 2x - 4 \\ \underline{- (2x - 4)} \\ \hline 0 \end{array}$$

↓
0
↓
↓ UAS!

PROPIEDADES:

$$\cdot g/f \wedge g(\alpha) = 0 \text{ entonces } f(\alpha) = 0$$

recordemos que en este caso queremos que g y f difieran en algún múltiplo fuera del dividendo de nuevo 0.

$$\cdot 0 \text{ es raíz de } f \Leftrightarrow a_0 = 0$$

$$\text{Ej: } x(x^2+4) \text{ el t: es } 0, \text{ luego } x=0 \text{ es raíz}$$

$x^2 - 4$ el rango, luego, 0 no es raíz.

- Si f es UN POLINOMIO CONSTANTE no tiene raíces para no hay $x / f(x) = 0$.
- Las raíces son de la forma $(x - \alpha)$
- $f(\alpha) = 0 \wedge f'(\alpha) = 0 \Rightarrow (f \cdot g)(\alpha) = 0$

$$f = 3x - 3 \quad g: 2x - 2 \quad \alpha = 1$$
$$f(1) = 0 \quad g(1) = 0 \quad \checkmark (f \cdot g)(1) = 0$$

Si tienen más de un rango en $f \cdot g$ entonces el MCD entre las funciones es 0 (obvio si las dos se hacen 0)

Algunos trucos:

- $x^6 - x^3 - 2$ y solo tienen raíces complejas, la hacemos cuadrática

$$w = x^3 \Rightarrow w^2 - w - 2$$

Luego, nos piden que $w = 1 \vee w = -2$

Entonces, $x^3 = 1 \quad \wedge \quad x^3 = -2$ y tenemos

de raíces número 6.

$$\begin{array}{r} x^{1000} - x^{500} - x^{25} \\ \hline x^6 - 1 \end{array}$$

Como quieras dividir $\text{tengo } M \in \mathbb{N}^*$

$$x^6 - 1 = 0(x^6 - 1) \quad (\Rightarrow) \quad x^6 = 1(x^6 - 1)$$

$$\text{Entonces } 1000 = 6 \cdot 166 + 4, \quad 500 = 6 \cdot 83 + 2, \quad 20 = 6 \cdot 3 + 2$$

$$\text{fue que } \underbrace{(x^6)}_1^{166} \cdot x^4 - \underbrace{(x^6)}_1^{83} \cdot x^2 - \underbrace{(x^6)}_1^3 \cdot x^2 = x^4 - x^2 - x^2 = \frac{x^4 - 2x^2}{(x^6 - 1)}$$

$$x^4 - 2x^2 \quad \overline{|x^6 - 1} \quad \Rightarrow \text{ como } q_n(x^4 - 2x^2) < x^6 - 1 \text{ en el resto.}$$

- $f(a) = r_{(x-a)}(f)$

Porque, si $x = 2 \quad X = 2$ en $R_{(x-2)} \Rightarrow x - a \approx x - 2$

$$\begin{array}{r} \text{Entonces } f(2) = x - 2 \quad \overline{|x-2} \\ \qquad \qquad \qquad -(x-2) \quad 1 \\ 0 \qquad \qquad \qquad \overrightarrow{=} \end{array}$$

- Si me dan valores de a y el resultado de dividirlos en f y un polinomio tener en cuenta: El grado del polinomio \times el que tengo que dividir. Olvidar dividir siempre por un polinomio el resto tendrá menor grado.

$$f(1) = -2 \quad f(2) = 1 \quad f(-1) = 3 \quad \text{y tengo que calcular el resto para } x^3 - 2x^2 - x + 1$$

$$\text{y que } q_n(r_{(x^3 - 2x^2 - x + 1)}(f)) < 3 \text{ en el resto}$$

$$\text{ent}, f = ax^2 + bx + c$$

ent, $f(1)$ impone que $a \cdot 1^2 + b \cdot 1 + c = 2$

$$\begin{aligned}f(1) &= a(1)^2 + b + c \\&= a + b + c = 2\end{aligned}\quad \left| \begin{aligned}f(2) &= a(2)^2 + b(2) + c \\&= 4a + 2b + c = 1\end{aligned}\right.$$

$$\begin{aligned}f(-1) &= a(-1)^2 + b(-1) + c \\&= a - b + c = 0\end{aligned}$$

entonces resolvemos el sistema para encontrar el polinomio buscando a, b y c .

Hasta aquí, el polinomio tiene el resultado.

- Si se divide entre el MCD, y el resultado es un polinomio constante, el nro es 1.

$$\text{Ej: } 20 \rightarrow \frac{20}{\text{CP}(20)} = \frac{20}{20} = 1.$$

OBS: Un polinomio $f \in \mathbb{R}[x]$ de grado

2 es irreducible si no tiene raíces en \mathbb{R} .

Polinomios Con dos Raíces = El Nulo

TFA DEL ALGEBRA: Los polinomios no constantes

de $\mathbb{C}[X]$ tiene algunas raíces en $\mathbb{C}[X]$.

SIEMPRE QUE TENGA UNA RAÍZ COMPLEJA,
SU CONJUGADA TAMBIÉN ES RAÍZ

LOS POLINOMIOS EN $\mathbb{C}[X]$: solo tienen
intriebles de grado 1.

FACTORIZACIÓN EN IRREDUCIBLES:

$$f = C(x - \alpha_1)^{m_1} (x - \alpha_2)^{m_2} (x - \alpha_3)^{m_3} \dots (x - \alpha_n)^{m_n}$$

Note que $(x - \alpha_2) + (x - \alpha_1)$ y así

con otras más.

POLINOMIOS REALES:

- Si el se grad 2 y no tiene raíces en $\mathbb{R} \Rightarrow$ es intrieble.

$$\Delta(ax^2 + bx + c)$$

- $\Delta > 0$ tiene raíces en \mathbb{R}
- $\Delta = 0$ tiene una raíz doble en \mathbb{R}
- $\Delta < 0$ no tiene raíces en \mathbb{R}

- TODOS Polinomios en $\mathbb{R}[X]$ con $\deg f > 2$ tiene AL MENOS UNA RAÍZ REAL.

Ej: $x^5 - 1 \in \mathbb{R}[X]$

$\hookrightarrow (x-1)$ es Raíz. Luego, las otras son complejas.

- Si el polinomio tiene una raíz compleja también tiene su conjugada (con misma multiplicidad)

\hookrightarrow Es de la forma: $x^2 + 2ax + (a^2 + b^2)$

$$\hookrightarrow (x-z)(x-\bar{z}) \mid f$$

Si $(x-z)^2$ es raíz $\Rightarrow (x-\bar{z})^2$.



\mathbb{R} = VALORES REALES
 \mathbb{C} = CONJUNTOS
 $\mathbb{C} = \mathbb{R} + i\mathbb{R}$
 \hookrightarrow si f tiene
 COEFICIENTES

POLINOMIOS RACIONALES:

- Los irreducibles pueden ser de cualquier grado.
- Teorema de Gauss: Los los polinomios

que $\in \mathbb{Q}[X]$. Si $f = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$

\hookrightarrow CON COEFICIENTES ENTEROS

entonces sus posibles raíces son: $P = \text{Div } \pm \{\mathbb{Q}_0\}$

$Q = \text{Div } \pm \{\alpha\}$

$$\text{Ej: } \frac{1}{4}x^2 + \frac{1}{2}x + 2 \stackrel{4}{\Rightarrow} x^2 + 2x + 8 \text{ y el}$$

polinomio tiene tiene el menor grado.

Recién ahora uno tiene.

OBS: Una vez que tenemos una raíz de la es un múltiple.

la Raíz VALE UN Punto 1.

$$f = \text{TENGO RAÍZ} = f' \quad \begin{cases} \text{1. si NO es raíz IMP - IRRAZ} \\ \text{2. si SI es raíz IMP - IRRAZ} \end{cases}$$

• Si $\sqrt{d} \in \mathbb{Q}$ la raíz entera \Rightarrow la raíz es Entera o IRRAZONAL
Sobre todo la conjugada. Convierte en irracional.

- Si tengo un Polinomio en $\mathbb{Q}[x]$ y tengo UNA RAÍZ $(a+b\sqrt{d})$ con $\sqrt{d} \notin \mathbb{Q} \Rightarrow$ Entonces, su conjugado TAMBIÉN VALE (con misma multiplicidad)

\mathbb{Q}

$\mathbb{R} = \text{VALORES}$
1) Racionales
2) IRRACIONALES
3) NÚMEROS COMPLEJOS

Los números racionales son de la forma:

$(a+b\sqrt{d})$ y su conjugado $(a-b\sqrt{d})$

$$\Leftrightarrow (x-(a+b\sqrt{d})) (x-(a-b\sqrt{d}))$$

$$= x^2 - 2ax + (a^2 - b^2 d)$$

Caso 7L/P 7L: Vale TODOS lo mismo

que en enteros excepto que allí

existe el INVERSO MULTIPLICATIVO

$$ab^{-1} = 1(P).$$

Se consideră că produsul adunării este finit și

nu există niciun element care să coplejeze egalația

$$\cdot [a] + [b] = [a+b]$$

$$\cdot [a] \cdot [b] = [a \cdot b]$$

$$\cdot [a] + ([b] + [c]) = ([a] + [b]) + [c]$$

$$\cdot [0] + [a] = [a]$$

$$\cdot [1] \cdot [a] = [a]$$

$$\cdot [-a] + [a] = [0]$$

$$\cdot [a] ([b] \cdot [c]) = [ab] \cdot [ac]$$

Ej: $x^2 + x + 1 \quad (\pi/2\pi)$

x	$x^2 + x + 1$
0	1
1	1

Deci, este inexistente în $(\pi/2\pi)$

Ej: $x^3 - 1 \quad (\pi/3\pi)$

x	$x^3 - 1$
0	1

Deci, $(x-1)$ este inexistente $\Rightarrow 1$.

$$\begin{array}{r|rr} & 1 & 0 \\ \hline 1 & & 1 \\ \hline 2 & & 1 \end{array}$$

$$\begin{array}{r}
 \begin{array}{r}
 x^3 - 1 \\
 - (x^3 - x^2) \\
 \hline
 x^2 - 1
 \end{array} \\
 - \begin{array}{r}
 x^2 - x \\
 \hline
 x - 1
 \end{array} \\
 - \begin{array}{r}
 x - 1 \\
 \hline
 0
 \end{array}
 \end{array}$$

$$(x-1)(x^2+x+1)$$

$$\begin{array}{r|rr} x & x^2 + x + 1 & \text{MOD } 3 \\ \hline 0 & 1 \\ 1 & 0 \\ 2 & 1 \end{array}$$

für $x = 1$, $(x-1) \equiv 0 \pmod{3}$

$$\begin{array}{r}
 \begin{array}{r}
 x^2 + x + 1 \\
 - (x^2 - x) \\
 \hline
 2x + 1
 \end{array} \\
 - \begin{array}{r}
 2x - 2 \\
 \hline
 3
 \end{array} \\
 \Rightarrow 3 \equiv 0 \pmod{3}
 \end{array}$$

↳ $(x-1)^2(x+2)$ fior $-2 \text{ mod } 3 = 1$

divides $(x-1)^2(x-1) \Rightarrow (x-1)^3$

CONCLUSI^NS

$\mathbb{Q}[x]: (x-\sqrt{2})$ NO VALUE

$(x-\sqrt{2})(x+\sqrt{2})$ NO VALUE

$$(x^2 + 2\alpha x + \dots)$$

• $x^m | f \quad f = q^m \cdot g$

$$x^m | f \Leftrightarrow m \leq m$$

$$x^n | f' \Leftrightarrow m \leq m-1 \quad f' = m \cdot q^{m-1} \cdot g$$

↳ $m+1 \leq m$

• $37^2 | (x-y)^{4321} \Leftrightarrow 37^2 | a^{4321}$

Como 37 en primo

$$37 \mid a^{4321}$$

$$37 \mid a \cdot a \cdot a$$

$$37 \mid a \quad (P|ab \Rightarrow P|a \vee P|b)$$

Si $a \neq 0$

Entonces $37 \mid a$

TIPS VARIOS GENERALES:

- Si estás en la función de G_n , si en el n -ésimo momento la memoria NO vale w^M entonces puedes decir que la memoria vale 1.

3. Para cada $w \in G_{11}$, calcular el valor

$$\sum_{j=0}^{64} w^j \cdot \sum_{j=0}^{64} \bar{w}^j.$$

a) Ej: Sea $w \in G_{11}$

$$\sum_{j=0}^{64} w^j \cdot \sum_{j=0}^{64} \bar{w}^j$$

$w^{10}=1$ para no mole

1 2

$$1) \sum_{j=0}^{6^4} \frac{w^{6^4-1}}{w-1} \text{ si } w \neq 1 \Rightarrow \frac{w^{6^4}-1}{w-1}$$

$$\text{si } w=1 \quad \overline{w}^8 \Rightarrow \overline{w}^n = \overline{w}^m \quad \overline{w} = w^{-1} \text{ en } G_m$$

$$2) \sum_{j=0}^{6^4} \overline{w}^j = \frac{w^{6^4-1}-1}{w-1} \text{ si } w \neq 1 \Rightarrow \frac{w^{6^4}-1}{w^{10}-1}$$

$$\text{si } w=1 \quad \Rightarrow w^{10}=1 \text{ pero } 11 \nmid 10$$

$$\Rightarrow G_{10} \not\subseteq G_{11}$$

Luego, como $(11:10) = 1$

$$\text{entonces } \sum_{j=0}^{6^4} w^j \cdot \sum_{j=0}^{6^4} \overline{w}^j = \begin{cases} 1 \cdot 1 \Rightarrow 1 \text{ si } w \neq 1 \\ 65 \cdot 65 \Rightarrow 4225 \text{ si } w=1 \end{cases}$$

PREG: ¿alguna función si ambas tienen w^{10} en algún lado? ¿xq D4 1?

Algoritmo: Nos piden g trazos de llegar a G_m dato.

Si por casualidad el exp de w que me pides llámenale g:

- Si: $m \mid g$ entonces $G_g \subseteq G_m$ entonces $w^g = 1$. (VER 6)
- Si $M \nmid g$ entonces $(M:g)=1$, y la suma de 1 si $w \neq 1$.

3. Sea $w \in G_{39}$ raíz 39-na primitiva de la unidad. Hallar todos los $n \in \mathbb{N}$ tales que

$$\sum_{j=0}^{5n+1} w^{13j} = 0 \quad \text{y} \quad w^{13} \in G_{3n+7}.$$

(Resumir toda la información obtenida para n en una única ecuación de congruencia).

- Mirando el exp de w , si podes escribir el w y hacer el opuesto el n se G_m unicos podes operarlos.

b) $w^{39} = 1 \Rightarrow G_{39}$

S_{n+1}

$\leq 13^k$

$$\Rightarrow 13^k \geq 13^3 \Rightarrow k \geq 3$$

$$w^{39} \text{ y } 3 \mid 39 \text{ entonces } G_3 \subseteq G_{13}$$

$$\text{entonces } Z = w^{13}$$

$$\langle w \rangle = 0 \Rightarrow (w)$$

$$j=0 \Rightarrow \frac{z^{(s_n+1)+1} - 1}{z - 1}$$

$$\Rightarrow z^{s_n+2}$$

luege s_{n+2} sehe ich multiplikativer Pol QWE?

$$s_{n+2} \equiv 0(3) \Leftrightarrow 2m \equiv -2(3) \Leftrightarrow 2m \equiv 1(3) \Leftrightarrow m \equiv 2(3)$$

Offene, $w^{1s} \in G_{3n+7} \Rightarrow (w^{1s})^{3n+7} = 1$

$$w^{4s_{n+10}5} \Rightarrow 4s_{n+10}5 \equiv 0(39)$$

$$\Rightarrow 6m + 27 \equiv 0(39)$$

$$\Rightarrow 6m \equiv 12(39)$$

$$\Rightarrow 2m \equiv 4(13)$$

$$\stackrel{?}{\Rightarrow} m \equiv 2(13)$$

luege,

$$\left\{ \begin{array}{l} m \equiv 2(13) \\ m \equiv 2(3) \end{array} \right.$$

(S1) $3j_1 \equiv 2(13) \Rightarrow 12j_1 \equiv 8(13) \Leftrightarrow -j_1 \equiv 8(13)$

$$\Leftrightarrow j_1 \equiv 5(13)$$

$$\Rightarrow x_1 = 15$$

$$S_2 \quad 13y_2 \equiv 2(3) \Leftrightarrow y_2 \equiv 2(3) \Rightarrow x_2 = 26$$

Luego, $m \equiv 2(39) \rightarrow m = 39k + 2$

VERIF: $k=0, m=2$

$w_{15} \in G_{13}$ NO. PREGUNTAR.

- Si tengo mismo ltro en dos difñntias:

Ej:

$$1) 7a + 3b = 4 \quad 2) 2b + 11c = 5$$

Coloca el resto de b por 77.

1) Tengo difñntia 1.

2) El resto de b de difñntia 1, lo resto en 2

3) Al B final le quito en 2 lo m&as n&umerico en
1 (VARIABLE)

4) Coloca el resto.

- Si tiene raiz no nula en f, no vale en ninguna entorno

Ej: si -1 es raiz de f, si buscas una raiz no nula a polos con -1

- Multiplicar para cambiar signo o tener con m&as lados

Dividiendo solo en resto (calcular MCD).

- Si no dicen "RAIZ RACIONAL" hablamos de UNA que es la raíz de $\pm\left\{\frac{P}{Q}\right\}$ en su forma más sencilla.
- Si tengo f , y tiene raíz \Rightarrow derivadas para ver si la raíz en $f' \Rightarrow$ si NO es raíz multiplicar a f , si es Raiz calcular f'' ...
- Si $x^2 | f \wedge x^2 | f'$ O es Raiz o MENOS 3 en f .
Pueden FORMAS
ULTIMA MULT. + 1.

Ej: $x^2 | f, x^2 | f'', x^2 | f''' \Rightarrow$ O ALMENOS MULT 4 en f .

- Si tiene en $\mathbb{Q}[x]$ si tiene raíz $(a+b\sqrt{d})$ y $\sqrt{d} \notin \mathbb{Q}$

entonces vale $(a-b\sqrt{d})$. TAMBÍEN VALE CONJUGADA

COMPLEJA. \rightarrow SÓLO SI TIENE COEFS ENTEROS
 \rightarrow CON POL. COEF ENTEROS?

- Si tiene en $\mathbb{R}[x]$ si tiene raíz $(a+b\sqrt{d})$ y $\sqrt{d} \notin \mathbb{Q}$

entonces vale $(a-b\sqrt{d})$. TAMBÍEN VALE CONJUGADA

COMPLEJA. \rightarrow SÓLO SI TIENE COEFS ENTEROS

- Si me piden Polinomios Mónicos No puedo ofrecer

un polinomio constante xf porque se ve monico

- Si tengo otra raíz compleja, los multiplos y

luego dividir el polinomio

$$\text{Ej: } \frac{(x-a)(x-\bar{a})}{(x-i)(x+i)} = a^2 + b^2 = x^2 + 1$$

$$\text{Ej: } (x+\sqrt{2})(x-\sqrt{2}) = a^2 + b^2 = x^2 - 2$$

$$\text{Ej: } (x-(1+\sqrt{2}))(x-(1-\sqrt{2}))$$

$$x^2 - 2x + (a^2 - b^2)$$

$$x^2 - 2x + 1$$

- Si f y g tienen raíces en común \Rightarrow división
en el MCD \rightarrow las raíces del MCD son las raíces

de f y g

- Para factorizar en $\mathbb{Z}/p\mathbb{Z}$ solo tener p
números con raíces reales. SIEMPRE \exists q si
negativas tienen MOD 5

Ej: Si -7 es raíz en $\mathbb{Z}/5\mathbb{Z}$ tiene la $\overline{4}$

- Para reducir la desigualdad optimizada
nula en la original

• Si tengo dos condiciones en congruencias

Ej: $7 \mid a \wedge 4 \mid b$ non son divisibles k
distintos

• Si me dicen tienen $a \in \mathbb{C}$ tal que ... sabiendo

que $2i$ es raiz. OJO, esq en \mathbb{C} . No solo
la conjugada $-2i$.

• $0 \equiv 0(s)$ no operas mal, la eliminas.

Rdo: Si un numero divide para todo n significa que al hacer congruencias (sin separar por casos, ✓) da 0. Este caso NO tiene que ir en un TCR pues, es inutil contemplarlo. Si se lo agrega está mal. Si un numero tenemos que separar en el caso de si divide o no, hay dos opciones: Si colocamos que por ejemplo $7 \mid a$ y llegamos a 0 entonces está bien a es congruente a 0 modulo 7 PERO si estemos en el caso de 7 NO divide a "a" y llego a 0 MODULO 7 entonces es absurdo porque en este caso 7 NO dividia a "a" y llegué igual a 0.

10:57 ✓

Importante SIEMPRE recordar eso, que si divide para todo n porque la congruencia se anula entonces NO lo contemplo a ese caso en el TCR

10:58 ✓

Y que si hago FERMAT separando en casos, y un NUMERO NO DIVIDE pero llego a que a es congruente a 0 MOD 7 justamente hay un absurdo porque estoy diciendo que 7 NO divide a a.

Si con el caso de 7 NO divide a "a" llego a 0 congruente 0 mod 7 entonces 7 divide para todo n (preguntar esto ultimo que dije, es una hipotesis)

10:59 ✓

Importante2: Si nosotros necesitamos que algo no divida, y llegamos a una congruencia y hacemos tabla de restos. Si se cumple esa condicion significa que divide pero si nosotros necesitamos que NO divida tomamos TODOS LOS CASOS menos el del 0 y esos.

11:10 ✓

Para s/a: Por el PTF, si s es primo \Rightarrow s/a

(necesito que s no divida)

$$a^4 \equiv 1(s)$$

$$19 = 4 \cdot 4 + 3$$

$$\text{Entonces } -a + 3a^3 + 3a \equiv 3a^3 + 2a \equiv a(3a^2 + 2)(s) \Rightarrow \text{No me interesa}$$

si $a \equiv 0(s)$ divide.

$$\text{Ver } 3a^2 + 2 \equiv ?(s) \Rightarrow 3a^2 \equiv 3(s) \Leftrightarrow a^2 \equiv 1(s) \Rightarrow \text{Luego cumplen}$$

que s divide

a	0	1	2	3	4
a^2	0	1	4	4	1

mod 5

luego s divide

•

$d | a \wedge d | b \Rightarrow d | a + b$ (vale con la resta tambien)

• $p | ab \Rightarrow p | a \vee p | b$ y no vale la vuelta en general.

• $d | a \wedge d | b \Rightarrow d | ab$

• $d | a \wedge b | a$ con d, b coprimos entonces $db | a$

• $d | a \Leftrightarrow d^n | a \Leftrightarrow d | a^n$ con d y a coprimos. Es decir si ambos no se dividen y tienen una potencia se las puedo quitar

$d = cb$

• $d | (f,f') \Leftrightarrow d | f \wedge d | f'$

• $d | f \wedge d | f' \Leftrightarrow c | f \wedge b | f \wedge c | f' \wedge b | f'$ (esta ultima es $d | a \wedge c | a \Leftrightarrow dc | a$)

• $d | a \Leftrightarrow d | ca$

• $d | ab \Leftrightarrow d | b$ (con d y a coprimos)

• $d | a \Leftrightarrow d^n | a^n$

22:29 ✓

• $w + \bar{w} = 2\operatorname{Re}(w)$

• $w * \bar{w} = |w|^2$

• $|w^2| = |w|^2$

• $w^{-1} = \bar{w}$ en \mathbb{G}_n

• $w - \bar{w} = 2\operatorname{Im}(w)$

• $w = \bar{w}$ si w pertenece a \mathbb{R}

• $w^{-1} = \bar{w}/|w|^2$

• $|wz| = |w| * |z|$

• \bar{w} elevado a la $n = w$ elevado a la n conjugado

• $n|m \Rightarrow \mathbb{G}_n \subset \mathbb{G}_m$ ej: $\mathbb{G}_3 \subset \mathbb{G}_6$

• $w^n \equiv w^{\text{ra}(n)}$ ej: Si estoy en \mathbb{G}_2 , w^{10} es w^0 .

• z, w pertenecen a \mathbb{G}_n entonces z^*w tambien. Ej: g_2 , si z, w estan en g_2 z^*w tambien.

Editado 22:29 ✓

• El Grado del MCD nos dice la Com de Raíces que tienen los 2 polinomios.

Ej: $(f: x^3 + 3x + 1) = 2$ las raíces que vienen de la $x^3 + 3x + 1$ no nos interesan las que vienen de x por.

• Si me piden polinomio de Grado Minimo No puedo ofrecer una raíz qd si PERO si tengo dos raíces qd digo qd tienen multiplicidad Al MENOS X, las pongo sobre la X al numero que necesite.

