Universidad Tecnológica Nacional
Facultad Regional Buenos Aires

Secretaría de Gestión Académica

NUMEROS NATURALES Y NUMEROS ENTEROS

Unidad 1

ELEMENTOS DE LOGICA

En esta primera unidad iniciamos el desarrollo de los contenidos de la asignatura haciendo una revisión de algunos conceptos que serán fundamentales para comprender luego otros temas propios de matemática discreta.
Algunos de esos conceptos provienen de la lógica y sirven de base para abordar los números enteros; otras nociones se refieren a los conjuntos, tema que resulta necesario para desarrollar muchos conceptos nuevos, propios de esta materia, por ejemplo, relaciones de orden, grupos y lenguajes.
Comenzamos, entonces, con el repaso de los conceptos de lógica.

La lógica estudia métodos de razonamiento que separan los razonamientos válidos de los no válidos. El interés por el análisis de los razonamientos se debe a que en las ciencias de la computación deben aplicarse para lograr que los programas realicen lo que se pretende.
Los razonamientos se basan en la enunciación de una secuencia proposiciones, que se conocen como premisas, para arribar a una conclusión.

Una *proposición* es todo enunciado al que se le puede asignar un valor de verdad.

Es decir que son afirmaciones que pueden resultar verdaderas o falsas. Para denotarlas se utilizan letras minúsculas como p, q, r.

e

Por ejemplo:

$p: 1 + 1 = 2$
$q: 1 + 1 = 3$

La proposición p es verdadera con lo que se escribirá de la forma: $V(p) = V$
La proposición q es falsa y se escribe: $V(q) = F$

Por el contrario, no son proposiciones enunciados tales como:

"Hola", "¿cómo estás?",
dado que no puede decirse nada acerca de su verdad o falsedad.

Las proposiciones pueden ser simples o compuestas.

Las *proposiciones simples* son las proposiciones p, q, r.

Las *proposiciones compuestas* se construyen con proposiciones simples y operadores que denominamos conectivos lógicos.

Representamos los conectivos en el cuadro que sigue, con su respectivo nombre y modo de leerlo

Conectivo	Se lee	Nombre
$\sim$	No	Negación
$\wedge$	Y	Producto lógico o conjunción
$\vee$	O (inclusivo)	Suma lógica o disyunción
$\Rightarrow$	Si ... entonces	Condicional
$\Leftrightarrow$	Si y sólo si	Bicondicional
$\veebar$	O (exclusivo)	Disyunción excluyente

Para obtener el valor de verdad de una proposición compuesta se utilizan tablas de verdad teniendo en cuenta como actúan los conectivos lógicos, según las siguientes definiciones:

Negación:

La negación $\sim p$ de p se define por medio de la siguiente tabla de verdad:

p	~p
V	F
F	V

e Por ejemplo:

Sea p: hay un premio Nobel de ciencias de la computación.
$\sim p$: no hay un premio Nobel de ciencias de la computación.

Conjunción:

Sean p y q proposiciones, se llama conjunción de p y q, y se denota $p \wedge q$, a la proposición p y q, y le corresponde la siguiente tabla de verdad:

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

e Por ejemplo:

Sean las proposiciones simples:
p: $1 + 1 = 3$ y q: una década tiene 10 años.

Entonces la conjunción es:
$p \wedge q$: $1 + 1 = \mathbf{3}$ y una década tiene 10 años.

Disyunción:

Sean p y q proposiciones. Se llama disyunción de p y q, y se denota $p \vee q$, a la proposición p o q, y le corresponde la siguiente tabla de verdad:

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

Por ejemplo:

Sean las proposiciones simples:
p: $1 + 1 = 3$ y **q:** una década tiene 10 años.
Entonces la disyunción es:
$p \vee q$: $1 + 1 = \mathbf{3}$ o una década tiene 10 años.

Condicional:

Sean p y q proposiciones, la proposición compuesta: si p, entonces q, se llama proposición condicional y se denota por $p \Rightarrow q$.
La proposición p se denomina hipótesis (o antecedente) y la proposición q, conclusión (o consecuente). La tabla de verdad que corresponde es la siguiente:

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

Por ejemplo:

Sean las proposiciones simples:
p: $1 + 1 = 3$ y **q:** una década tiene 10 años.
Entonces el condicional $p \Rightarrow q$ es:
$p \Rightarrow q$: Si $1 + 1 = \mathbf{3}$ entonces una década tiene 10 años.

¿Te convence el valor de verdad del condicional en los dos últimos renglones? Si no es así, considera el siguiente ejemplo:

María le dice a Juan: *"si mañana llueve, salgo a pasear con vos"*
Las cuatro situaciones que se pueden dar son las que corresponden a los cuatro renglones de la tabla de verdad. Analicemos uno por uno:

- en el primer caso, las dos proposiciones son verdaderas, lo cual en nuestro ejemplo significa que llueve y que María pasea con Juan. No hay duda de que la promesa de María era cierta.

- en el segundo caso, la primera proposición es verdadera, lo cual en nuestro ejemplo significa que llueve, pero como la segunda es falsa, significa que María no sale a pasear con Juan. No hay duda de que la promesa de María no se cumple.

- pero ¿qué ocurre en el tercer y cuarto caso? Ambos tienen el antecedente falso, o sea que en nuestro ejemplo significa que no llueve. En uno de los casos (el tercero), María sale a pasear con Juan, y en el otro caso (el cuarto) no pasean. ¿Qué podemos decir de la promesa efectuada? ¿Tenemos elementos para decir que no se cumplió? Por supuesto que no. Pues la promesa fue con la condición de que lloviera, María no prometió nada si no llovía. Así que como no tenemos evidencia suficiente para decir que María no cumple su promesa, la debemos considerar inocente (como en los juicios).

<u>Bicondicional:</u>

Sean p y q proposiciones, la proposición compuesta: $\mathbf{p}$ si y sólo si $\mathbf{q}$, se llama proposición bicondicional y se denota por $p \Leftrightarrow q$.
El valor de veracidad de la proposición $p \Leftrightarrow q$ está definido por la siguiente tabla de verdad:

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

e Por ejemplo:

Sean p: $1 + 1 = 3$ y q: una década tiene 10 años.
$p \Leftrightarrow q$: $1 + 1 = 3$ si y sólo si una década tiene 10 años.

<u>Disyunción excluyente:</u>

Sean p y q proposiciones, la proposición compuesta: p ó (excluyente) q, se llama proposición disyunción excluyente y se denota por $p \veebar q$.
El valor de veracidad de la proposición $p \veebar q$ está definido por la siguiente tabla de verdad:

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

Por ejemplo:

Sean p: $1 + 1 = 3$ y q: una década tiene 10 años.
$p \Leftrightarrow q$: $1 + 1 = 3$ ó (excluyente) si una década tiene 10 años.

Un ejemplo de la vida cotidiana donde se utiliza la disyunción excluyente es el caso de una mamá que le dice a su hijo: “elegí el autito o el trencito, pero no ambos. Te voy a comprar uno solo”.

O bien, otro ejemplo que viviste hace no mucho tiempo es en el recuperatorio del curso de ingreso. Los que pueden presentarse a dar recuperatorio de parcial son los que tienen aprobado uno solo. Entonces si consideramos las proposiciones simples:
p: “el alumno aprobó el primer parcial”
q: “el alumno aprobó el segundo parcial”
… debemos decir que para dar el recuperatorio se debe cumplir que: $p \veebar q$ ya que el que aprobó los dos parciales, no tiene nada que recuperar.

Algunas observaciones que vale la pena tener en cuenta.

Dada $p \Rightarrow q$:

** la proposición $q \Rightarrow p$ se dice *recíproca*
** la proposición $\sim q \Rightarrow \sim p$ se dice *contrarrecíproca*
** la proposición $\sim p \Rightarrow \sim q$ se dice *contraria*

Las tablas de verdad correspondientes a estas proposiciones son:

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

Si una proposición compuesta tiene n proposiciones simples entonces el número de filas en la tabla de verdad es 2^n.

Para continuar, veamos algunos *tipos especiales de proposiciones compuestas.* Ellas son: la *tautología*, la *antitautología* y la *contingencia.*

Tautología

Llamamos *tautología* (V) a aquella proposición compuesta cuyo valor de verdad es siempre verdadero en forma independiente del valor de verdad de las proposiciones simples que la componen.

Por ejemplo:

p	q	$(p \wedge q) \vee \sim (p \wedge q)$
V	V	V
V	F	V
F	V	V
F	F	V

Antitautología o Contradicción (F)

Llamamos *antitautología* o *contradicción* a aquella proposición compuesta cuyo valor de verdad es siempre falso en forma independiente del valor de verdad de las proposiciones simples que la componen.

Por ejemplo:

p	q	$(p \vee q) \wedge \sim (p \vee q)$
V	V	F
V	F	F
F	V	F
F	F	F

Contingencia

Se denomina *contingencia* a aquella proposición compuesta cuyo valor de verdad depende del valor de verdad de las proposiciones simples que la componen.

Por ejemplo:

p	q	$p \vee (p \wedge q)$
V	V	V
V	F	V
F	V	F
F	F	V

Hasta aquí, entonces, tenemos que:

- *Una* proposición *es todo enunciado al que se le puede asignar un valor de verdad.*
- *Las proposiciones pueden ser* simples o compuestas: *las proposiciones simples son las proposiciones* p, q, r. *Las proposiciones compuestas se construyen con proposiciones simples y* conectivos lógicos *(negación; producto lógico o conjunción; suma lógica o disyunción; condicional; bicondicional; o excluyente)*
- *Para obtener el valor de verdad de una proposición compuesta se utilizan* tablas de verdad *teniendo en cuenta como actúan los conectivos lógicos.*

Proposiciones Lógicamente Equivalentes

Estamos transitando un nuevo camino, el de la lógica; para ello, es necesario que conozcamos algunas reglas que nos permitirán saber si estamos avanzando correctamente. Estas reglas son las *equivalencias lógicas entre proposiciones.*

¿Cuándo decimos que son equivalentes las proposiciones o, lo que es lo mismo, que las proposiciones son lógicamente equivalentes?

Las proposiciones compuestas $P = P(p_1,\dots, p_n)$ y $Q = Q(p_1,\dots, p_n)$ son lógicamente equivalentes siempre que, dados cualesquiera valores de verdad de $p_1, \dots, p_n$, P y Q son ambas verdaderas o ambas falsas. Se cumple cuando: $P(p_1, \dots, p_n) \Leftrightarrow Q(p_1, \dots, p_n)$ es una tautología.

Lo denotamos $P \equiv Q$

e Por ejemplo: $\sim p \vee q \equiv p \Rightarrow q$

Tengamos en cuenta, además, que si las equivalencias no nos convencen a priori podemos demostrarlas; para eso debemos usar las tablas de verdad.
A continuación presentamos los distintos tipos de equivalencias.

1. Involutiva: $\sim\sim p \equiv p$
2. Idempotencia: $(p \vee p) \Leftrightarrow p \Leftrightarrow (p \wedge p)$
3. Conmutatividad:
   $(p \vee q) \Leftrightarrow (q \vee p)$
   $(p \wedge q) \Leftrightarrow (q \wedge p)$
   $(p \Leftrightarrow q) \Leftrightarrow (q \Leftrightarrow p)$

4. Absorción:
   $p \vee (p \wedge q) \Leftrightarrow p \Leftrightarrow p \wedge (p \vee q)$

5. Identidad:
   $p \wedge V \Leftrightarrow p$
   $p \wedge F \Leftrightarrow F$
   $p \vee V \Leftrightarrow V$
   $p \vee F \Leftrightarrow p$

6. Leyes de De Morgan:
   $\sim (p \wedge q) \Leftrightarrow \sim p \vee \sim q$
   $\sim (p \vee q) \Leftrightarrow \sim p \wedge \sim q$

7. Asociatividad:
   $p \vee (q \vee r) \Leftrightarrow (p \vee q) \vee r$
   $p \wedge (q \wedge r) \Leftrightarrow (p \wedge q) \wedge r$

8. Distributividad:
   $p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r)$
   $p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$

Ahora bien, *¿para qué utilizaremos las equivalencias lógicas?* Entre otras cosas para poder simplificar proposiciones compuestas y otorgarles un aspecto más amigable.

Veamos el siguiente caso:

$(p \wedge \sim q) \Rightarrow (r \wedge \sim r) \Leftrightarrow$ utilizando equivalencia de proposiciones
$\sim (p \wedge \sim q) \vee (r \wedge \sim r) \Leftrightarrow$ utilizando De Morgan
$(\sim p \vee \sim\sim q) \vee (r \wedge \sim r) \Leftrightarrow$ utilizando involución
$(\sim p \vee q) \vee (r \wedge \sim r) \Leftrightarrow$ utilizando contradicción
$(\sim p \vee q) \vee f \Leftrightarrow$ utilizando identidad
$\sim p \vee q \Leftrightarrow$ utilizando equivalencia de proposiciones
$p \Rightarrow q$

Con lo cual $(p \wedge \sim q) \Rightarrow (r \wedge \sim r)$ y $p \Rightarrow q$ son equivalentes. Esto podemos probarlo haciendo ambas tablas de verdad.

Les proponemos que las realicen antes de continuar. Si no lo logran, pueden consultar a los tutores.

Veamos otro ejemplo:

Dada la siguiente proposición:

$$p \Rightarrow \sim [(\sim p \Rightarrow q) \wedge \sim (\sim p \wedge r)]$$

Apliquemos equivalencia del condicional en $(\sim p \Rightarrow q)$ y al mismo tiempo apliquemos De Morgan en $\sim(\sim p \wedge r)$. Obtenemos:

$$p \Rightarrow \sim [\, (\sim(\sim p) \vee q\,) \wedge [\sim(\sim p) \vee (\sim r)]\,]$$

Ahora apliquemos la ley involutiva en $\sim(\sim p)$:

$$p \Rightarrow \sim [\, (\, p \vee q\,) \wedge [\, p \vee (\sim r)]\,]$$

Distributiva de $\vee$ respecto de $\wedge$:

$$p \Rightarrow \sim [\, p \vee (\, q \wedge \sim r)\,]$$

Equivalencia del condicional:

$$\sim p \vee \sim [\, p \vee (\, q \wedge \sim r)\,]$$

Apliquemos nuevamente De Morgan:

$$\sim p \vee [\, \sim p \wedge \sim(\, q \wedge \sim r)\,]$$

Finalmente, por absorción: $\sim p$

Predicado o Función proposicional

Comencemos analizando el siguiente enunciado:

x es un número impar

No podemos decir que es una proposición porque para que sea verdadera o falsa depende del valor que le asignemos a x.
Tenemos una expresión de la forma $p(x)$, en nuestro caso, $p(x)$: **x es un número impar.** Esta expresión será cierta para todos los números enteros impares y falsa para todos los pares.
Tengamos en cuenta que para asignarle un valor de verdad necesitamos recurrir a los elementos de un conjunto, en particular, en este caso, al de los números enteros.
Podemos, entonces, concluir en la siguiente definición

Sea A un conjunto no vacío, llamamos predicado o función proposicional con dominio en A a toda expresión $p(x)$ tal que para cualquier elemento a del conjunto A se verifica que $p(a)$ es proposición.

Por ejemplo:

Sea $\mathbf{A} = \mathbb{N}$ (números naturales)

$p(x)$: "$x > 3$"

Si $x = 1$ entonces $p(1)$: "$1 > 3$" entonces el valor de verdad de la proposición $p(1)$ es falso.
Si $x = 9$ entonces $p(9)$: "$9 > 3$" entonces el valor de verdad de la proposición $p(9)$ es verdadero.

Digamos ahora:

Todos los números naturales son impares.

Podemos dar un valor de verdad: el enunciado es falso y por lo tanto es una proposición. Ahora bien, ¿cómo convencemos a alguien de que esa afirmación es falsa?; debemos mostrar un caso, por lo menos uno, que asevere que realmente el enunciado es falso. Elegimos, por ejemplo,

el número **4** es par

y solucionamos nuestro problema.

La situación que planteamos podemos escribirla utilizando los siguientes símbolos: $\forall$ y $\exists$, que se llaman *cuantificadores*. Debemos tener en cuenta que algunas veces para dar una proposición podemos usar cuantificadores.

- El *cuantificador universal (* $\forall$*)*, significa para todo (es decir cualquiera).

  Si $p(x)$ es verdadera para todo x en $\mathbf{A}$ entonces decimos que $\forall\, x$: $p(x)$ es verdadera.

- *El cuantificador existencial (* $\exists$*)*, significa que existe al menos un ...

  Así $\exists\, x \in \mathbf{A}$ se lee "existe al menos un x en $\mathbf{A}$".

Entonces, para el enunciado *"Todos los números naturales son impares: " Que se denota* $\forall x \in \mathbb{N}$: x *es impar "*, su negación es la siguiente:

$\sim[\forall x \in \mathbb{N}$: x es impar$] \Leftrightarrow \exists\, x \in \mathbb{N}$: x no es impar$]$

Veamos otro ejemplo que resolveremos juntos. Para ello te pedimos que completes los puntos suspensivos.

Supongamos que María dice: “Todos los alumnos de este curso aprobaron el parcial”
Y Hernán le responde: “Eso no es verdad. Aquí hay un alumno que no aprobó”

¿Es suficiente la justificación que da Hernán? …………………………………………………………………....
………

En otra ocasión, María dice: “Algún alumno de este curso aprobó el parcial” y nuevamente Hernán está en desacuerdo.

¿Qué debería hacer ahora para justificar su posición?...
………

¿Podemos dar al siguiente resultado?

$$\sim [\forall\ x : p(x)] \equiv \exists\ x : \sim p(x) \qquad \sim [\exists\ x : p(x)] \equiv \forall\ x : \sim p(x)$$

e

Otro caso:
Supongamos que queremos expresar simbólicamente el siguiente enunciado:
“Para todo número entero existe otro número entero que lo divide”. Vemos que hay dos variables: el número entero que es dividido y el que divide; podríamos escribirlo así:

$$\forall x: \exists y: x|y$$

Podemos preguntarnos, ¿será lo mismo escribir $\exists y: \forall x: x|y$?; en realidad, nos estamos haciendo la siguiente pregunta: ¿es lo mismo $\forall x : \exists y : p(x;y)$ que $\exists y : \forall x : p(x;y)$?

Analicemos algunos otros casos: en el conjunto de los números enteros sabemos que el número 0 es neutro para la suma. ¿Cómo puede escribirse que el neutro para la suma es el 0 usando los cuantificadores? Veamos las siguientes formas

1. $\exists\ 0 \in Z, \forall z \in Z: 0+z = z+0 = z$
2. $\forall z \in Z, \exists\ 0 \in Z: 0+z = z+0 = z$

La correcta es la 1, donde decimos que existe el 0 y que es el elemento neutro para la suma.
En la 2 estamos diciendo que cada entero tiene su neutro y nosotros sabemos que el neutro es único y es el 0.

Veamos otro ejemplo[9] a partir de las mismas expresiones:

[9] Este ejemplo es un aporte de la Profesora Ana María Gómez

Supongamos que x son las mujeres solteras, y son los varones solteros y la propiedad $p(x;y)$ significa que x e y son novios. La primera proposición dice que para todas las mujeres solteras x existe un varón y, que es el novio. La segunda proposición, en cambio, dice que existe un varón y, tal que todas las mujeres x del mundo son sus novias. Son afirmaciones muy diferentes, ¿no?

Por lo tanto ***los cuantificadores no conmutan***

Algunos ejemplos para repasar:

Consideremos el siguiente enunciado

$p\ (x)$: x es un número par

¿Es una proposición lógica? ☐ SI ☐ NO ¿Por qué?
....

A este tipo de enunciados se los llama ....

Son enunciados con variables que pueden convertirse en proposiciones lógicas de las siguientes formas:

1) Asignando valores a las variables (ejemplo: 3 es un número par)

2) Cuantificándolas (ejemplo: todos los números son pares)

Ejemplos:

Sean: $P(x)$: "x es múltiplo de 5" $Q(x)$: "x es par" $R(x)$: "x es impar"

$A = \{10, 15, 20\}$ $B = \{3, 6, 9, 12\}$

- Para decir que todos los elementos del conjunto A son múltiplos de 5 escribimos:
  $\forall\ x \in A : P(x)$
- Para decir que algunos elementos del conjunto B son pares escribimos: $\exists\ x \in B : Q(x)$
- Para decir que algunos elementos del conjunto A son pares y múltiplos de 5 escribimos:
  $x \in A : [\ P(x) \wedge Q(x)\ ]$

¿Existen elementos de B que sean impares y múltiplos de 5? .... ¿Cómo se escriben?

....

¿Es cierto que todos los múltiplos de 5 son impares? .... ¿Cómo se escriben?

....

Analiza el valor de verdad de las siguientes proposiciones con cuantificadores:

1. $\exists\, x \in \mathbb{Z}: x \cdot 2 = 7$
2. $\forall\, x \in \mathbb{R}: x^2 > -1$
3. $\forall\, x \in \mathbb{Z}: \exists\, y \in \mathbb{Z}: \; x + y = 5$
4. $\exists\, x \in \mathbb{R}: \forall\, y \in \mathbb{R}: \; x \cdot y = y$

Recordemos cómo negar los cuantificadores:

$\sim[\, \forall\, x: p(x) \,] \Leftrightarrow [\, \exists\, x: \sim p(x) \,]$
$\sim[\, \exists\, x: p(x) \,] \Leftrightarrow [\, \forall\, x: \sim p(x) \,]$

Nega cada una de las siguientes proposiciones:

p: $\forall\, x \in \mathbb{R}: \; x^2 > 0$ **~ p:** ……………………………..………...

q: $\exists\; x \in \mathbb{Z}: (\, x + 3 = 8 \;\wedge\; x > 4 \,)$ **~ q:** ……………………………..………...

r: $\exists\, x \in \mathbb{R}: \forall\, y \in R: x \bullet y = y$ **~ r:** ……………………………..………....

s: $\forall\, x \in \mathbb{R}: (\, x > 0 \Rightarrow \; x + 2 > 3 \,)$ **~ s:** ……………………………..………....

Consideremos ahora los siguientes predicados definidos en el conjunto de los números naturales.

$p(x;y) : \forall x\; \forall y: x \geq y$

$q(x;y) : \forall x\; \exists y: x \geq y$

$r(x;y) : \exists x\; \forall y: x \geq y$

$t(x;y) : \exists x\; \exists y: x \geq y$

En cada caso la variable x y la variable y están afectadas por un cuantificador, universal o existencial; diremos entonces que son variables acotadas.
Si tuviéramos $p(x) : x\text{-}2 < 3$, la variable x no está afectada por un cuantificador; decimos que la variable no cuantificada es una variable libre.
Es decir que en el predicado $p(x)$ a la variable x la llamamos variable libre y en $\forall\, x: p(x)$, x es variable acotada.

¿Cómo analizamos el valor de verdad de una proposición dada por cuantificación con más de una variable?
Veamos el valor de verdad de $p(x;y) : \forall x: \forall y: x \geq y$ en el conjunto de los números reales. Consideremos primero $\forall y: x \geq y$, como la x no está cuantificada es una variable libre y la y es la variable acotada, sea $x = 5$ y en el enunciado original queda $\forall y: 5 \geq y$ que es falso para, por ejemplo $y = 8$. Por lo tanto $V(p(x;y))$ es falso.

Veamos ahora qué pasa con el valor de verdad de $t(x;y) : \exists x: \exists y: x \geq y$.

Si actuamos de la misma manera queda $\exists y: x \geq y$, donde x es libre e y está acotada, que es verdadera ya que podemos elegir siempre un x que sea mayor o igual que el y propuesto.

Antes de finalizar este punto, recordemos que:

- *Decimos que dos proposiciones son lógicamente equivalentes siempre que dados cualesquiera valores de verdad, ambos son* V *o* F*. Se pueden demostrar usando las tablas de verdad.*

- *Sea* A *un conjunto no vacío, llamamos predicado o función proposicional con dominio en* A *a toda expresión* $p(x)$ *tal que para cualquier elemento* a *del conjunto* A *se verifica que* $p(a)$ *es proposición.*

- *En algunos casos, para dar una proposición podemos usar cuantificadores (universal o existencial); pero es importante recordar que los cuantificadores* no *conmutan.*

- *Cuando las variables* x e y *están afectadas por un cuantificador, se trata de variables acotadas; cuando una de las variables* no *está afectada por un cuantificador se denomina variable libre.*

Hasta aquí nuestro repaso de las nociones de lógica que aplicaremos en las próximas unidades. Avancemos ahora con los temas que siguen: conjuntos, inducción matemática y números enteros.

CONJUNTOS

Tal como anticipamos al inicio de la unidad, los conceptos vinculados al tema conjuntos son necesarios para abordar luego otros tales como las relaciones de orden, grupos y lenguajes que estudiaremos en las próximas unidades.

Empezando por caracterizar un conjunto, podemos decir que simplemente es cualquier colección de objetos o sea toda agrupación de elementos.

Los conjuntos se indican con letras mayúsculas y los elementos con letras minúsculas. Si un conjunto es finito y no demasiado extenso se puede describir nombrando cada uno de sus elementos, es decir, por extensión o enumeración. Asimismo, darlo por comprensión es dar una propiedad que caracteriza a todos los elementos de ese conjunto.

e

Por ejemplo:
$A = \{2, 4, 6, 8\}$
El conjunto A está definido por extensión.
$B = \{$ x tal que x es un número par y $2 \leq x \leq 8$ $\}$
El conjunto B está definido por comprensión.

Las que siguen son definiciones y relaciones entre conjuntos, que aplicaremos luego en temas posteriores, tales como en las operaciones entre conjuntos.

Cardinalidad de un conjunto

Un conjunto A se dice finito si tiene n elementos distintos con $n \in \mathbb{N}$, en ese caso el cardinal de A es n y lo indicamos $|A| = n$.

Conjunto vacío

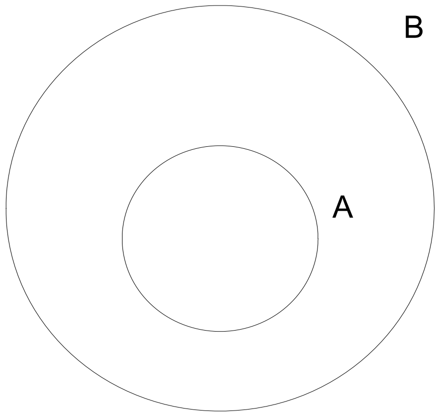
Si el conjunto A no tiene elementos, su cardinal es 0.
El conjunto que no tiene elemento alguno se llama conjunto vacío o nulo y se denota $\emptyset$,
$\emptyset = \{\ \}$.

e

Por ejemplo:
$A = \{x \in \mathbb{R}$ tal que $x^2 + 2 = 0$ $\}$

Inclusión de conjuntos

Dados dos conjuntos A y B, decimos que A está incluido (o contenido) en B si todos los elementos de A están en B. Lo indicamos como $\mathrm{A} \subseteq \mathrm{B}$ sí y sólo sí $x \in \mathrm{A} \Rightarrow x \in \mathrm{B}$.
La relación que liga a los conjuntos entre sí es la inclusión.



$\boxed{\mathrm{A} \subseteq \mathrm{B}}$

Igualdad de conjuntos

Dos conjuntos X e Y son iguales si tienen los mismos elementos. En este caso se escribirá $\mathrm{X} = \mathrm{Y}$. Dicho en otras palabras, siempre que $x \in \mathrm{X}$ se cumple que $x \in \mathrm{Y}$, y siempre que $x \in \mathrm{X}$ se cumple que $x \in \mathrm{Y}$, y así $\mathrm{X} = \mathrm{Y}$.

Por ejemplo:
$\mathrm{A} = \{ x \text{ tal que } x^2 + x - 6 = 0 \}$ y $\mathrm{B} = \{2, -3\}$, entonces $\mathrm{A} = \mathrm{B}$.

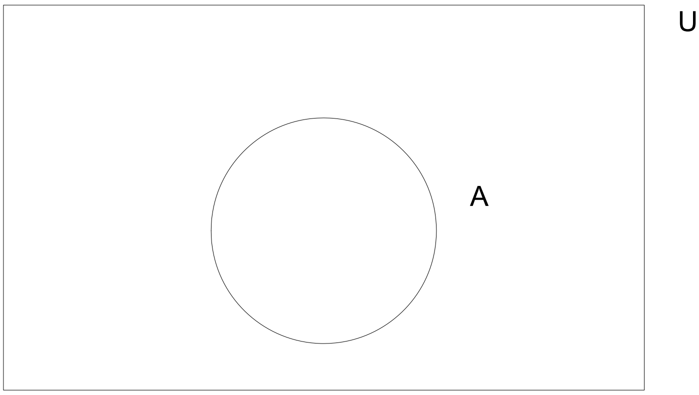
Supóngase que X e Y son conjuntos. Si todo elemento de X es un elemento de Y se dice que X es un subconjunto de Y y se expresa $\mathrm{X} \subseteq \mathrm{Y}$.

Si vinculamos la noción de igualdad con el concepto de inclusión podemos decir que A y B son iguales si $\mathrm{A} \subseteq \mathrm{B} \wedge \mathrm{B} \subseteq \mathrm{A}$.

Conjunto Universal

Se llama conjunto referencial o universal al conjunto U que hace verdadera la siguiente proposición:
$x \in \mathrm{A} \Rightarrow x \in \mathrm{U}$.

En un diagrama de Venn se representa con un rectángulo



Operaciones con conjuntos

Las que siguen son operaciones que pueden realizarse con conjuntos, tales como: intersección, unión, diferencia, complemento y diferencia simétrica.

➔ Dados dos conjuntos A y B llamamos *intersección* entre A y B e indicamos $A \cap B$ al siguiente conjunto:

$A \cap B = \{$ x tal que $x \in A \wedge x \in B \}$

Por ejemplo:

Sea $A = \{ 1, 3 \}$ y $B = \{ 1, 2, 3, 4 \}$
$A \cap B = \{ 1, 3 \}$

➔ Dados dos conjuntos A y B llamamos *unión* entre A y B e indicamos $A \cup B$ al siguiente conjunto:

$A \cup B = \{$ x tal que $x \in A \vee x \in B \}$

Por ejemplo:

Sea $A = \{ 1, 3 \}$ y $B = \{ 1, 2, 3, 4 \}$
$A \cup B = \{ 1, 2, 3, 4 \}$

➔ Dados dos conjuntos A y B llamamos *diferencia* entre A y B e indicamos $A - B$ al siguiente conjunto:

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

e Por ejemplo:

Sea $A = \{ 1, 3 \}$ y $B = \{ 1, 2, 3, 4 \}$
$A - B = \varnothing$
$B - A = \{ 2, 4 \}$

➔ Dado el conjunto A llamamos *complemento* de A e indicamos $\overline{A}$ al siguiente conjunto:

$\overline{A} = \{ x$ tal que $x \in U \wedge x \notin A \} = U - A$

e Por ejemplo:

Sea $A = \{ x$ tal que $x \in \mathbb{N}$ y x es impar $\}$ y $U = \mathbb{N}$

$\overline{A} = \{ x$ tal **que** $x \in \mathbb{N}$ y x es par $\}$

➔ Dados los conjuntos A y B llamamos *diferencia simétrica* entre A y B e indicamos $A \triangle B$ al siguiente conjunto:

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

e Por ejemplo:

Sea $A = \{ 1, 3 \}$ y $B = \{ 1, 2, 3, 4 \}$
$A \triangle B = \{ 2, 4 \}$

Propiedades de las operaciones

Las operaciones anteriores cumplen las siguientes propiedades:

1. Involución:

   $\overline{\overline{A}} = A$

2. Idempotencia:

   $A \cup A = A$
   $A \cap A = A$

3. Conmutatividad:

$$A \cup B = B \cup A$$
$$A \cap B = B \cap A$$

4. Neutro y absorbente:

$$A \cap U = A, \ A \cup U = U$$
$$A \cap \varnothing = \varnothing, \ A \cup \varnothing = A$$

5. Absorción:

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

6. Leyes de De Morgan:

$$\overline{A \cup B} = \bar{A} \cap \bar{B}$$

$$\overline{A \cap B} = \bar{A} \cup \bar{B}$$

7. Asociatividad:

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

8. Distributividad:

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

9. Propiedades del complemento:

$$A \cap \bar{A} = \varnothing$$

$$A \cup \bar{A} = U$$

e Por ejemplo:

$\overline{A} \cap (A \cup B) = \overline{A} \cap B$

$\overline{A} \cap (A \cup B) = (\overline{A} \cap A) \cup (\overline{A} \cap B)$ por propiedad distributiva.

$= \varnothing \cup (\overline{A} \cap B)$

$= \overline{A} \cap B$

A continuación definiremos un conjunto de partes de un conjunto dado. Este es un concepto con el que vamos a trabajar mucho en unidades posteriores, al tratar temas como relaciones de orden y Álgebras de Boole.

Conjunto de partes

Se llama conjunto de partes o conjunto potencia de A al conjunto:

$P(A) = \{ X$ tal que $X \subseteq A \}$

Tengamos en cuenta:

- ✓ El conjunto potencia de A es un conjunto cuyos elementos son todos los subconjuntos de A.
- ✓ Si $|A| = n \Rightarrow |P(A)| = 2^n$
- ✓ $\forall A: P(A) \neq \varnothing$
- ✓ Si $A = \varnothing \Rightarrow |P(A)| = 1$

e Por ejemplo:

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

$|A| = 3 \Rightarrow |P(A)| = 2^3 = 8$

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

Demostraciones de propiedades con conjuntos

Hay diferentes formas de demostrar propiedades de los conjuntos. Algunas de esas formas son las siguientes:

<table>
<tr><td rowspan="4">Demostraciones a nivel de elementos</td><td rowspan="2">Sin antecedente</td><td>Con una inclusión en el consecuente
Ejemplo: $A \subseteq A \cup B$</td></tr>
<tr><td>Con una igualdad en el consecuente
Ejemplo:
$A \cap (B \cap C) = (A \cap B) \cap C$</td></tr>
<tr><td rowspan="2">Con antecedente y consecuente</td><td>Demostrar a partir del 1er miembro de la tesis
$[C \subseteq A \cup B \Rightarrow (C - B) \subseteq A]$</td></tr>
<tr><td>Desarrollar la hipótesis completa hasta llegar a la tesis
$(A - B = \varnothing \Leftrightarrow A \subseteq B)$</td></tr>
<tr><td>Demostraciones conjuntistas</td><td colspan="2">Utilizando propiedades básicas de conjuntos demostradas previamente</td></tr>
</table>

Comencemos a demostrar cada uno de estos ejemplos…

- Empecemos por las *demostraciones de elementos:*

Sin antecedente y con una inclusión en el consecuente.

Es decir, debemos probar que $A \subseteq A \cup B$

Sabemos que por definición de inclusión, es lo mismo probar que $\forall x: x \in A \Rightarrow x \in A \cup B$

Debemos partir del primer miembro y luego de una cadena de implicaciones llegar al segundo miembro.

$\forall x: x \in A \Rightarrow x \in A \vee x \in B \Rightarrow x \in A \cup B$

propiedad $p \Rightarrow p \vee q$ definición de unión

Sin antecedente y con una igualdad en el consecuente

Ahora tenemos que probar una igualdad $A \cap (B \cap C) = (A \cap B) \cap C$

Recordemos que dos conjuntos son iguales cuando se incluyen mutuamente. O sea, que en principio este ejercicio comprende dos partes:

Primera inclusión: $\forall x: x \in A \cap (B \cap C) \Rightarrow x \in (A \cap B) \cap C$

Segunda inclusión: $\forall x: x \in (A \cap B) \cap C \Rightarrow x \in A \cap (B \cap C)$

Demostremos la primera:

$\forall\, x: x \in A \cap (B \cap C) \Rightarrow$	aplicamos definición de intersección
$\Rightarrow x \in A \wedge x \in (B \cap C) \Rightarrow$	aplicamos definición de intersección
$\Rightarrow\ x \in A \wedge (x \in B \wedge x \in C) \Rightarrow$	por la asociatividad de la $\wedge$
$\Rightarrow\ (x \in A \wedge\ x \in B) \wedge x \in C \Rightarrow$	por definición de intersección
$\Rightarrow\ x \in (A \cap B) \wedge x \in C \Rightarrow$	por definición de intersección
$\Rightarrow\ x \in (A \cap B) \cap C$	con lo cual llegamos al segundo miembro

Es importante tener en cuenta que a esta altura no terminamos el ejercicio, pues nos falta la segunda inclusión. Si nos fijamos bien, en la mayoría de los casos se trata de hacer el camino inverso –aunque recordemos que no en todos ocurre esto-. Nos queda:

$\forall\, x: x \in A \cap (B \cap C) \Leftrightarrow$	por definición de intersección
$\Leftrightarrow\ x \in A \wedge x \in (B \cap C) \Leftrightarrow$	por definición de intersección
$\Leftrightarrow\ x \in A \wedge (x \in B \wedge x \in C) \Leftrightarrow$	por la asociatividad de la $\wedge$
$\Leftrightarrow\ (x \in A \wedge\ x \in B) \wedge x \in C \Leftrightarrow$	por definición de intersección
$\Leftrightarrow\ x \in (A \cap B) \wedge x \in C \Leftrightarrow$	por definición de intersección
$\Leftrightarrow\ x \in (A \cap B) \cap C$	

Con antecedente y consecuente realizando la demostración a partir del primer miembro de la tesis

Debemos probar que $C \subseteq A \cup B \Rightarrow (C - B) \subseteq A$

A diferencia de los ejercicios anteriores, en este caso tenemos un antecedente o hipótesis $(C \subseteq A \cup B)$ y un consecuente o tesis $((C - B) \subseteq A)$, que es lo que hay que demostrar. Si nos fijamos en la tesis, se trata de una inclusión y la vamos a demostrar como toda inclusión, es decir: $\forall\, x: x \in (C - B) \Rightarrow x \in A$

En el camino de implicaciones para llegar al segundo miembro, además de definiciones y propiedades, podemos utilizar la hipótesis.

Apliquemos estas demostraciones en el ejercicio que sigue:

Completá señalando en cada paso cuál es la propiedad utilizada:

$\forall\, x: x \in (C - B) \Rightarrow\ x \in C \wedge x \notin B$

$\Rightarrow x \in (A \cup B) \wedge x \notin B$

$\Rightarrow (x \in A \vee x \in B) \wedge x \notin B\ \Rightarrow$

$\Rightarrow (x \in A \wedge x \notin B) \vee (x \in B \wedge\ x \notin B)$

$\Rightarrow (x \in A \wedge x \notin B) \vee F\ \ \Rightarrow\ \ x \in A\ \wedge x \notin B\ \Rightarrow$

$\Rightarrow x \in A$

Con antecedente y consecuente desarrollando la hipótesis completa hasta llegar a la tesis

En este caso es una equivalencia o doble implicación: $A - B = \varnothing \Leftrightarrow A \subseteq B$
Si lo hacemos como en caso anterior es necesario realizar dos ejercicios. En cambio, lo vamos a demostrar desarrollando el antecedente completo hasta llegar al consecuente.

Como en el caso anterior, señalá en cada paso cuál es la propiedad utilizada:

$$A - B = \varnothing \Leftrightarrow \sim \exists\, x: x \in (A - B) \Leftrightarrow \forall\, x: \sim [\, x \in (A - B)] \Leftrightarrow \forall\, x: \sim [x \in A \wedge x \notin B] \Leftrightarrow$$

$$\Leftrightarrow \forall\, x: x \notin A \vee x \in B \Leftrightarrow [\forall\, x: x \in A \Rightarrow x \in B\,] \Leftrightarrow A \subseteq B$$

- Sigamos con las *demostraciones conjuntistas:*

  Por ejemplo, demostremos $(A \cup B) \cap (\overline{A} \cup \overline{B}) = (B - A) \cup (A - B)$ en forma conjuntista, utilizando las propiedades de conjuntos básicas, sin bajar al nivel de la lógica:

  $$(A \cup B) \cap (\overline{A} \cup \overline{B}) = (A \cap \overline{A}) \cup (A \cap \overline{B}) \cup (B \cap \overline{A}) \cup (B \cap \overline{B}) =$$

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

Realizá las siguientes demostraciones:

1. $A \subseteq B \wedge B \cap C = \varnothing \Rightarrow A \cap C = \varnothing$
2. $A - (B - C) = (A - B) \cup (A \cap C)$
3. $(A \cup \overline{B}) \cap (B \cup \overline{A}) = (A \cap B) \cup (\overline{A} \cap \overline{B})$
4. $P(A) \cup P(B) \subseteq P(A \cup B)$

Partición de un conjunto

Sea un conjunto $A \neq \varnothing$. Sea $P = \{A_1, A_2, \ldots\ldots, A_n\}$
P es una partición de $A \Leftrightarrow$ 1) $A_i \neq \varnothing \quad \forall i$
2) $A_i \cap A_j = \varnothing \quad \forall i \neq j$
3) $\bigcup A_i = A$

Algunas observaciones para tener en cuenta:

Las particiones están incluidas en el conjunto de partes.
Los subconjuntos A_i reciben el nombre de celdas de la partición.
La condición 3 también se puede expresar: $\forall\, x \in A : \exists\, A_i \in P : x \in A_i$

Para finalizar, te proponemos realizar algunos ejercicios sobre particiones.

1- ¿Cuáles de los siguientes conjuntos son particiones de $A = \{ a, b, c, d, e \}$?
En caso negativo, indicá cual de las tres condiciones no se cumple.
$P_1 = \{ \{a,b,c\}, \{d,e\} \}$
$P_2 = \{ \{a,b\}, \{c,d\}, \{b,e\} \}$
$P_3 = \{ \{a,b\}, \{c\}, \{e\} \}$
$P_4 = \{ \{a\}, \{b\}, \{c\}, \{d,e\} \}$
$P_5 = \{ \{a\}, \{b,c,d\}, \{ \}, \{e\} \}$

2- ¿Cuáles de los siguientes conjuntos $P = \{A_1, A_2, A_3\}$ son particiones de $\mathbb{R}$?

a) $A_1 = (-\infty ; -2]$
$A_2 = (-2 ; 0]$
$A_3 = (1; +\infty)$

b) $A_1 = (-\infty ; -1)$
$A_2 = \{ -1 , 2 \}$
$A_3 = (-1; +\infty) - \{ 2 \}$

c) $A_1 = (-\infty ; -3]$
$A_2 = (-3 ; 0)$
$A_3 = \mathbb{R}^+$

d) $A_1 = (-\infty ; 4)$
$A_2 = \{ 0 , 5 \}$
$A_3 = [4; +\infty) - \{ 5 \}$

Sintetizando:

- *Un conjunto puede describirse por extensión o por comprensión.*
- *Las operaciones entre conjuntos son: intersección, unión, diferencia, complemento, diferencia simétrica.*
- *Estas operaciones presentan las propiedades: involución, idempotencia, conmutatividad, neutro y absorbente, absorción, leyes de De Morgan, asociatividad, distributividad, propiedades del complemento.*
- *Entre las diferentes formas de demostrar las propiedades de conjuntos encontramos:*

  Demostraciones a nivel de elementos
  - *Sin antecedente*
    - *Con una inclusión en el consecuente*
    - *Con una igualdad en el consecuente*
  - *Con antecedente y consecuente*
    - *Demostrar a partir del 1er miembro de la tesis*
    - *Desarrollar la hipótesis completa hasta llegar a la tesis*

  Demostraciones conjuntistas
  - *Utilizando propiedades básicas de conjuntos demostradas previamente*

- *Llamamos Partición a todo subconjunto P del conjunto de partes de A, $P(A)$ que cumple las siguientes condiciones: ningún componente de P es el conjunto vacío, dos componentes distinto no tienen elementos en común y todos los elementos de A están en alguno de los componentes de P.*

INDUCCION MATEMATICA

En muchos casos queremos demostrar que alguna propiedad relativa a los números naturales es cierta. Para demostrarlo podemos analizar algunos casos particulares -para algunos valores naturales- pero no podemos hacerlo con todos, pues son infinitos.
Por ejemplo, si observamos la suma de los primeros números impares:

$1 = 1$
$1 + 3 = 4$
$1 + 3 + 5 = 9$
$1 + 3 + 5 + 7 = 16$

¿Notás algo en particular? Observá bien los resultados...

Vemos que todos son cuadrados perfectos:

$1 = 1 = 1^2$
$1 + 3 = 4 = 2^2$
$1 + 3 + 5 = 9 = 3^2$
$1 + 3 + 5 + 7 = 16 = 4^2$

Por lo tanto, si agregamos otro número impar seguramente obtendremos $5^2 = 25$ y así sucesivamente.
Pero, ¿podemos estar seguros de ello? ¿Se cumplirá realmente con cualquier cantidad de impares sumados? Para poder responder con certeza a este interrogante y muchos similares vamos a utilizar la *Inducción Matemática*, que estudiaremos en esta sección.
Para comenzar definiremos conjunto inductivo y conjunto de números naturales, así como la relación entre ambos.

¿Qué es un conjunto inductivo?

Sea $\mathbf{R}$ el conjunto de los números reales, dado $\varnothing \neq A \subseteq \mathbb{R}$, decimos que A es inductivo si:

1) $1 \in A$
2) $\forall\, x \in A \Rightarrow x+1 \in A$

¿Qué es el conjunto de números naturales?

$\mathbb{N} = \bigcap_{A \subseteq R} A$ tal que A es inductivo

O sea que…

el *conjunto de los números naturales* es la intersección de todos los conjuntos inductivos. Es el más pequeño de los conjuntos inductivos en el sentido de la inclusión.

Una herramienta que podemos utilizar para demostrar propiedades relativas al conjunto de los naturales es la *inducción completa*.

Principio de Inducción Completa (PIC)

Sea $p(n)$ un predicado o función proposicional con dominio en el conjunto $\mathbb{N}$ de los números naturales.

Si:
$$1)\ v[\,p(1)\,] = V$$
$$2)\ v[\,p(h)\,] = V \Rightarrow v[\,p(h+1)\,] = V$$

Entonces: todas las $p(n)$ son verdaderas.

Tengamos presente que:

a) el paso $1)$ se llama PASO BASE de la inducción y consiste en evaluar la proposición con $n = 1$

b) el paso $2)$ se llama PASO INDUCTIVO

El antecedente de $2)$ se llama HIPOTESIS INDUCTIVA y el consecuente es la TESIS INDUCTIVA
La hipótesis inductiva consiste en tomar como válida la propiedad en un determinado valor de n que llamamos h. A partir de esto, se debe probar la tesis inductiva, o sea que la propiedad es válida para el valor siguiente de h, es decir para $h+1$.

Tengamos en cuenta que este método se puede usar aunque no se comience con n=1

Dado $m \neq 1$:

Si :
$$1)\ v[\,p(m)\,] = V$$
$$2)\ v[\,p(h)\,] = V \Rightarrow v[\,p(h+1)\,] = V$$

Entonces: $p(n)$ es verdadera para todo $n \geq m$.

e Veamos algunos ejemplos del proceso de inducción

Ejemplo 1

Demostrar que: $$\sum_{k=1}^{n} k\ k! = (n+1)! - 1 \qquad \forall n \in \mathbb{N}$$

¿Qué significa el símbolo $\sum$ y el signo de admiración?
Vayamos de a poco.

El símbolo $\sum$ indica sumatoria, es decir, una suma de varios términos.
Debajo del signo hay una letra que es el contador igualado a su valor inicial. Arriba del signo se escribe el valor final del contador; luego, se reemplaza en la expresión por los sucesivos valores del contador y se suman.

Por ejemplo:

$$\sum_{n=1}^{5} n^2 = 1^2 + 2^2 + 3^2 + 4^2 + 5^2 = 1 + 4 + 9 + 16 + 25 = 55$$

$$\sum_{n=1}^{3} n \bullet 2^n = 1 \bullet 2^1 + 2 \bullet 2^2 + 3 \bullet 2^3$$

Ahora veamos el signo de admiración; este signo es el símbolo de factorial.

¿Qué es el factorial de un número?
Se llama factorial de un número natural a otro número natural que se obtiene multiplicando todos los naturales anteriores al dado.

En forma recursiva se define: $0! = 1 \wedge n! = (n-1)!\, n$

Ejemplos:
$4! = 4 \bullet 3! = 4 \bullet 3 \bullet 2! = 4 \bullet 3 \bullet 2 \bullet 1! = 4 \bullet 3 \bullet 2 \bullet 1 \bullet 0! = 24$
$5! = 5 \bullet 4! = 5 \bullet 24 = 120$

Solución:

Paso base: $n = 1$:

$$p(1): \quad \sum_{k=1}^{1} k\ k! = (\ 1+1\ )! - 1$$

Vamos a analizar el valor de verdad de $p(1)$. Para ello calculamos ambos miembros por separado y luego comparamos:

Primer miembro de $p(1)$: $1\ 1! = 1$
Segundo miembro de $p(1)$: $(1+1)! - 1 = 2! - 1 = 2 - 1 = 1$

Como los dos miembros son iguales, entonces $v\ [p(1)] = V$

Paso inductivo:

Hipótesis Inductiva: $n = h$ $\quad \sum_{k=1}^{h} k\ k! = (\ h+1\ )! - 1$

Tesis Inductiva: $n = h+1$ $\quad \sum_{k=1}^{h+1} k\ k! = (\ h+1+1\ )! - 1$

Demostración: para demostrar la igualdad de la tesis partimos del primer miembro y trataremos de llegar al segundo.

$$\sum_{k=1}^{h+1} k\ k! =^{(1)} \sum_{k=1}^{h} k\ k! + (h+1)\,(h+1)! \ =^{(2)}\ (h+1)! - 1 + (h+1)\,(h+1)! \ =^{(3)}$$
$$=^{(4)} (h+1)!\,(1+h+1) -1 =^{4} (h+1+1)! -1$$

Así, llegamos al segundo miembro. Justificaciones:

(1) De los $h+1$ términos dejamos aparte el último de ellos
(2) Utilizamos la hipótesis inductiva
(3) Sacamos factor común $(h+1)!$ entre primer y tercer términos
(4) Usamos definición recursiva de factorial

Ejemplo 2:

Demostrar $\forall\ n \geq 3 :\ \ (2n)! > 8^{n-1}\, n^2$

Solución:

Paso base: $n = 3$:
(En este caso comenzamos de $n=3$ en vez de $n=1$ ya que lo dice el enunciado)

$$p(1):\quad (2 \bullet 3)! > 8^{3-1} \bullet 3^2$$

Veamos si $p(1)$ es verdadera:

Primer miembro de $p(1)$: $(2 \bullet 3)! = 6! = 720$
Segundo miembro de $p(1)$: $8^{3-1} \bullet 3^2 = 64 \bullet 9 = 576$
Como $720 > 576$, entonces $v\ [p(1)] = V$

Paso inductivo:

Hip. Ind.: $n = h$ $\quad (2h)! > 8^{h-1}\, h^2$

Tesis Ind: $n = h+1$ $\quad (2(h+1))! > 8^{h}\, (h+1)^2$

Demostración: para demostrar la tesis, partimos del primer miembro de la misma y trataremos de probar que es mayor que el segundo.

$$(2(h+1))! = (2h+2)! =^{(1)} (2h+2)\,(2h+1)\,(2h)! >^{(2)} (4h^2+6h+2) \bullet 8^{h-1}\, h^2 >^{(3)}$$
$$>^{(3)} (h^2+2h+1)\, 8^h \bullet 8^{-1} \bullet h^2 >^{(4)} 8^h (h+1)^2 \bullet 8^{-1} \bullet h^2 >^{(5)} 8^h (h+1)^2$$

Con lo cual quedó demostrado que: $2(h+1))! > 8^h (h+1)^2$

Justificaciones de cada paso:

(1) Usamos la definición recursiva de factorial
(2) Distribuimos el producto de $(2h+2)(2h+1)$ y utilizamos la hipótesis inductiva
(3) Acotamos la expresión $(4h^2 + 6h + 2)$ por una expresión menor $(h^2+ 2h + 1)$ ya que resulta conveniente para lo que debemos probar
(4) Escribimos el cuadrado de una suma que teníamos desarrollado
(5) Dado que como $h \geq 3$ entonces $h^2 \geq 9$ por lo tanto $h^2 > 8$

En este momento, te proponemos resolver los ejercicios de inducción de la guía (3.1.1 y 3.1.2)

SUCESIONES

Una sucesión es una lista de objetos, uno después del otro, numerada en el orden creciente de los números naturales.

Formalmente, una sucesión es una función $f: \mathbb{N} \to \mathbb{R}$

Hay que tener en cuenta que en una sucesión:

1. Los elementos pueden o no repetirse.
2. A veces en vez de $\mathbb{N}$ se puede tomar $\mathbb{N}_0$

Por ejemplo:

S_1 : $1,4,9,16,25,\ldots,n^2,\ldots.$
S_2 : $1,-1,1,-1,1,-1,1,-1,\ldots\ldots,(-1)^n,\ldots$

Notaciones: $S: a_1,a_2,\ldots\ldots,a_n,\ldots\ldots$ $\qquad S : (a_i)_{i \in N}$

RECURSION

Una definición es recursiva si hace referencia a ella misma.

e Por ejemplo: la definición de factorial es recursiva $n! = n \bullet (n-1)!$ con $0! = 1$

Lo mismo ocurre al dar una sucesión, es decir que también puede definirse en forma recursiva. Al definir el término general, se puede hacer referencia a términos anteriores.

Ejemplo:

Sea la sucesión definida por: $a_n = 2 \bullet a_{n-1}$ con $a_1 = 4$

Veamos algunos elementos de la sucesión:
Ya sabemos que $a_1 = 4$. calculemos el siguiente: $a_2 = 2 \bullet a_1$ entonces: $a_2 = 2 \bullet 4 = 8$
Y el próximo es: $a_3 = 2 \bullet a_2$ entonces: $a_3 = 2 \bullet 8 = 16$
Y así sucesivamente.
En este caso es fácil darse cuenta que los elementos de la sucesión son todos potencias de 2, pero hay muchos casos donde no es tan sencillo descubrir la regla general a simple vista.

A las sucesiones dadas en forma recursiva, se las llama relaciones o ecuaciones de recurrencia.

¿Qué significa resolver una relación de recurrencia? Significa encontrar una expresión del a_n que satisfaga la relación y que no sea recursiva.

Clasificación de relaciones de recurrencia:

Orden: es la mayor diferencia entre los subíndices de los elementos de la sucesión que figuran en la relación de recurrencia. Es decir, el orden indica cuántos términos anteriores hay que conocer para obtener uno en particular.

Grado: es el mayor exponente al que están elevados los elementos de la sucesión que figuran en la relación de recurrencia.

Ecuación Homogénea: al igual que las ecuaciones algebraicas, las homogéneas son las que no tienen términos independientes; pero en este caso no necesariamente los términos independientes son constantes sino que todos aquellos en los que no figuran elementos de la sucesión. Por ejemplo los siguientes términos son independientes:
$3 \bullet n$, 4, n^2, etc.

Ecuación de coeficientes constantes: en estas ecuaciones ninguno de los coeficientes de los elementos de la sucesión dependen de n. Por el contrario, si alguno depende de n, se dice que la ecuación tiene coeficientes variables.

e

Algunos ejemplos:

a) $a_n = 3\ a_{n-1} + 2n^2$ es de orden 1 (diferencia entre n y $n-1$), grado 1 o lineal (exponentes 1), no homogénea (pues figura el término $2n^2$) y de coeficientes constantes (1 y 3).

b) $a_n = a_{n-1} + a_{n-2}$ es de orden 2, lineal, homogénea y de coeficientes constantes.

c) $a_n^3 = 2\ a_{n-1} - 1$ es de orden 1, grado 3, no homogénea y coeficientes constantes.

d) $2\ a_n = n\ a_{n-2}$ es de orden 2, lineal, homogénea y de coeficientes variables (n)

Vamos a analizar ahora las relaciones de recurrencia de orden 1 y de orden 2, homogéneas con coeficientes constantes y sus respectivas resoluciones

Relaciones de recurrencia lineales de orden 1, homogéneas

Son de la forma: $an = k \bullet a_{n-1}$ siendo k una constante real no nula.

e

Resolución:

Supongamos que conocemos el valor de a_0. Cuánto vale el a_1? $a_1 = k \bullet a_0$

Y a_2? $a_2 = k \bullet a_1$ que a su vez es $a_2 = k\ k\ a_0 = k^2\ a_0$

Y a_3? $a_3 = k \bullet a_2$ que a su vez es $a_3 = k\ k\ k\ a_0 = k^3\ a_0$

O sea que pareciera que: $a_n = k^n \bullet a_0$

Pero para estar seguros de la fórmula encontrada, debemos demostrarla. Vamos a hacerlo por medio de Inducción Completa.

¿Qué es lo que hay que demostrar?

Dato del ejercicio: la fórmula recursiva $a_n = k\ a_{n-1}$ y el valor de a_0
Fórmula encontrada no recursiva: $a_n = k^n\ a_0$
Lo que debemos probar es que la nueva fórmula define la misma sucesión que la otra.

Paso base:

$n = 0$ (ya que el primer término es a_0)
Lo calculamos con la nueva fórmula: $a_0 = k^0\ a_0 = a_0$ entonces se cumple $p(0)$ es V

Paso inductivo:

Hip. Ind: $n = h$ $\qquad a_h = k^h\ a_0$
Tesis Ind: $n = h+1$ $\qquad a_{h+1} = k^{h+1}\ a_0$
Dem./ $\qquad a_{h+1} = k\ a_h = k\ k^h\ a_0 = k^{h+1}\ a_0$

Por dato del ejercicio $\qquad$ Hip. Ind. $\qquad$ Producto de potencias de igual base

Por lo tanto, queda demostrado que $\forall\ n \in N_0$: $p(n)$ es verdadera

Ejemplo:

La siguiente relación de recurrencia: $3\ a_n - 5\ a_{n-1} = 0$ con $a_0 = 4$

Es equivalente a: $\qquad a_n = \frac{5}{3}\ a_{n-1}$

Tiene por solución: $\qquad a_n = \left(\frac{5}{3}\right)^n \bullet 4$

Relaciones de recurrencia lineales de orden 2, homogéneas

Son de la forma: $\qquad c_n\ a_n + c_{\ n-1}\ a_{\ n-1} + c_{\ n-2}\ a_{\ n-2} = 0$

Resolución:

Supongamos que $a_n = x^n$ es una solución de la ecuación. Por lo tanto debe satisfacerla:

$$c_n\ x^n + c_{n-1}\ x^{n-1} + c_{n-2}\ x^{n-2} = 0$$

Sacamos factor común .... y obtenemos:

$$x^{n-2}\ \ (\ c_n\ x^2 + c_{n-1}\ x + c_{n-2}\ ) = 0$$

Como x no puede ser cero, entonces debe ser $c_n\ x^2 + c_{n-1}\ x + c_{n-2}\ = 0$
Lo cual es una ecuación algebraica de segundo grado que se llama ecuación característica.

Sus raíces pueden ser → reales y distintas
→ reales e iguales (una raíz doble)
→ complejas conjugadas

Según sean las raíces de la ecuación característica, la solución general será:

- Reales distintas: $a_n = k_1\, r_1^{\,n} + k_2\, r_2^{\,n}$
- Reales iguales: $a_n = k_1\, r_1^{\,n} + k_2\, n\, r_1^{\,n}$
- Complejas: ídem primer caso pero se opera con De Moivre (no se consideran en esta materia)

Las constantes k_1 y k_2 se calculan con los datos iniciales

Importante: Para poder resolver una relación de recurrencia de orden n se necesitan conocer n condiciones iniciales.

Veamos dos ejemplos:

e

Ejemplo 1

$a_n - 5\, a_{n-1} + 6\, a_{n-2} = 0$ con $a_0 = 3$ y $a_1 = 5$

Directamente planteamos la ecuación característica: $x^2 - 5\,x + 6 = 0$
Calculamos sus raíces, que son: $r_1 = 2$ y $r_2 = 3$
Resultaron ser raíces REALES y DISTINTAS
Planteamos la forma de la solución general: $a_n = k_1\, r_1^{\,n} + k_2\, r_2^{\,n}$
Y ahora, teniendo en cuenta las condiciones iniciales:
$a_0 = 3$ entonces $3 = k_1\, r_1^{\,0} + k_2\, r_2^{\,0}$ o sea $k_1 + k_2 = 3$
$a_1 = 5$ entonces $5 = k_1\, r_1^{\,1} + k_2\, r_2^{\,1}$ o sea $2\,k_1 + 3\,k_2 = 5$

Nos ha quedado un sencillo sistema de ecuaciones lineales. Al resolverlo obtenemos: $k_1 = 4$ y $k_2 = -1$
Por lo tanto, nuestra solución es: $a_n = 4 \bullet 2^n - 3^n$

Ejemplo 2:

$a_{n+2} = 4\, a_{n+1} - 4\, a_n$ con $a_0 = 1$ y $a_1 = 5$

La ecuación característica es: $x^2 - 4\,x + 4 = 0$ que tiene como raíces: $r_1 = 2$ y $r_2 = 2$
O sea que son raíces REALES e IGUALES
Planteamos la forma de la solución general: $a_n = k_1 \bullet 2^n + k_2 \bullet n \bullet 2^n$
Y ahora, teniendo en cuenta las condiciones iniciales:
$a_0 = 1$ entonces $k_1 = 1$
$a_1 = 5$ entonces $2 \bullet k_1 + 2 \bullet 1 \bullet k_2 = 5$ entonces: $k_2 = 1.5$

Por lo tanto, nuestra solución es: $a_n = 2^n + 1.5 \bullet n \bullet 2^n$

Demostración por Inducción:

Paso base:
Por ser de segundo orden hay que probar los dos datos iniciales:
$n = 0$: $a_0 = 2^0 + 1.5 \bullet 0 \bullet 2^0 = 1$
$n = 1$: $a_1 = 2^1 + 1.5 \bullet 1 \bullet 2^1 = 2 + 3 = 5$ se verifica

Paso inductivo:

Hip. Ind: $n = h$ $\quad a_h = 2^h + 1.5 \bullet h \bullet 2^h$
$a_{h-1} = 2^{h-1} + 1.5 \bullet (h-1) \bullet 2^{h-1}$
Tesis Ind: $n = h+1$ $\quad a_{h+1} = 2^{h+1} + 1.5 \bullet (h+1) \bullet 2^{h+1}$

Dem./
Comenzamos desarrollando el primer miembro de la tesis:
$a_{h+1} = 4\, a_h - 4\, a_{h-1} = 4 \bullet (\, 2^h + 1.5 \bullet h \bullet 2^h\,) - 4 \bullet (\, 2^{h-1} + 1.5 \bullet (h-1) \bullet 2^{h-1}) =$
$= 4 \bullet 2^h + 6 \bullet h \bullet 2^h - 4 \bullet 2^{h-1} - 6\,(h-1) \bullet 2^{h-1} = 4 \bullet 2^h + 6 \bullet h \bullet 2^h - 2 \bullet 2^h - 3\,h \bullet 2^h + 3 \bullet 2^h =$
$= 4 \bullet 2^h + 6 \bullet h \bullet 2^h - 2 \bullet 2^h - 3\,h \bullet 2^h + 3 \bullet 2^h = 5 \bullet 2^h + 3 \bullet h \bullet 2^h$ (expresión 1)

Ahora desarrollamos el segundo miembro de la tesis:

$2^{h+1} + 1.5 \bullet (h+1) \bullet 2^{h+1} = 2^h \bullet 2 + 1.5 \bullet h \bullet 2^h \bullet 2 + 1.5 \bullet 2^h \bullet 2 = 2 \bullet 2^h + 3 \bullet h \bullet 2^h + 3 \bullet 2^h =$
$=5 \bullet 2^h + 3 \bullet h \bullet 2^h$ (expresión 2)

Como ambas expresiones son iguales, ha quedado probada la tesis. Y por principio de inducción: $\forall\, n \in N_0$: $p(n)$ es verdadera

Sintetizando:

- *El Principio de Inducción Completa se utiliza para demostrar propiedades relativas al conjunto de los números naturales.*
- *El PASO BASE de la inducción consiste en evaluar la proposición con $n = 1$ (o el primer elmento indicado). En el PASO INDUCTIVO el antecedente se llama HIPOTESIS INDUCTIVA y el consecuente es la TESIS INDUCTIVA. Si se verifica la igualdad en el paso base y de la hipótesis inductiva se obtiene la tesis inductiva , la propiedad es válida para todos los números naturales*
- *Una sucesión es una lista de objetos, uno después del otro, numerada en el orden creciente de los números naturales. Formalmente, una sucesión es una función f: $\mathbb{N} \to \mathbb{R}$*
- *Hay que tener en cuenta que en una sucesión: los elementos pueden o no repetirse; a veces en vez de $\mathbb{N}$ se puede tomar $\mathbb{N}_0$.*
- *Una definición es recursiva si hace referencia a ella misma.*

- *A las sucesiones dadas en forma recursiva se las llama* ***relaciones o ecuaciones de recurrencia.*** *Resolver una relación de recurrencia significa encontrar una expresión del* a_n *que satisfaga la relación y que no sea recursiva.*

- *En una relación de recurrencia se caracteriza el orden, el grado, la homogeneidad y los coeficientes*

- *Las relaciones de recurrencia lineales de orden 2, homogéneas son de la forma:* $c_n\, a_n + c_{n-1}\, a_{n-1} + c_{n-2}\, a_{n-2} = 0$

Ahora podés intentar resolver los ejercicios de recursión de la guía (3.2.1 al 3.2.6)

Una vez resueltos pasamos al último de los temas de la Unidad: los Números Enteros.

NUMEROS ENTEROS

Si bien en la sección anterior estudiamos los números naturales, cómo demostrar propiedades relativas a ellos y, en particular, las sucesiones y la recursividad, no todos los modelos matemáticos son con números naturales. Para muchas aplicaciones es necesario trabajar con números enteros.

Recordemos que el conjunto de los números enteros es: $\mathbb{Z} = \mathbb{N} \cup \{0\} \cup \{-x \,/\, x \in \mathbb{N}\}$

En el conjunto $\mathbb{Z}$, la adición y la multiplicación son operaciones cerradas, es decir, siempre se pueden efectuar y devuelven un resultado entero. Pero con la división no pasa lo mismo, pues por ejemplo, si queremos dividir 8 por 3 ningún número entero coincide.

Por ello es que definimos la "división entera", tal cual la habías aprendido en la escuela primaria. Seguramente lo recordás.

División entera:

$$\begin{array}{r|l} D & d \\ \cline{2-2} r \,/ & c \end{array}$$

Dados dos números enteros D y d, existen y son únicos otros dos enteros c y r tales que:

$$\mathbf{D = d\,c + r} \quad \text{con} \quad \mathbf{0 \leq r < |d|}$$

D se llama DIVIDENDO, d es el DIVISOR, c es el COCIENTE y r el RESTO de la división entera.

Esto se llama *Algoritmo de la División* y se puede demostrar.

e

Ejemplos:

a) El cociente y el resto de la división entera de 17 por 3 son respectivamente:
$c = 5$ y $r = 2$ ya que $17 = 3 \bullet 5 + 2$ y $0 \leq 2 < 3$

b) El cociente y el resto de la división entera de -8 por 5 son respectivamente:
$c = -2$ y $r = 2$ ya que $-8 = 5 \bullet (-2) + 2$ y $0 \leq 2 < 5$

c) El cociente y el resto de la división entera de -13 por -4 son respectivamente:
$c = 4$ y $r = 3$ ya que $-13 = (-4) \bullet 4 + 3$ y $0 \leq 3 < 4$

d) El cociente y el resto de la división entera de 15 por -6 son respectivamente:
$c = -2$ y $r = 3$ ya que $15 = (-6) \bullet (-2) + 3$ y $0 \leq 2 < 3$

Tratemos de generalizar un poco lo que hemos observado en los cuatro casos anteriores:

Si $d > 0$: $c = \text{ent}(D/d) \wedge r = \text{mant}(D/d) \bullet d$

Por ejemplo, en los casos a) y b) anteriores:

a) En reales: $\frac{17}{3} = 5.66666666666666\ldots$

entonces: $c = \text{ent}\,(\frac{17}{3}) = 5 \quad \wedge \quad r = \text{mant}\,(\frac{17}{3}) \bullet 3 = 0.66666666\ldots \bullet 3 = 2$

b) En reales: $\frac{-8}{5} = -1.6$

entonces: $c = \text{ent}\,(\frac{-8}{5}) = -2 \quad \wedge \quad r = \text{mant}\,(\frac{-8}{5}) \bullet 5 = 0.4 \bullet 5 = 2$

Si $d < 0$: $d' = -d \Rightarrow$ se resuelve esta división como en los casos anteriores obteniendo:
$c' = \text{ent}\,(D/d') \wedge r' = \text{mant}\,(D/d') \bullet d'$ Luego: $c = -c' \wedge r = r'$

Por ejemplo, en los casos **c)** y **d)** anteriores:

c) Resolvemos: $\frac{-13}{4}$ en reales: $\frac{-13}{4} = -3.25$

entonces: $c' = \text{ent}\,(\frac{-13}{4}) = -4 \quad \wedge \quad r' = \text{mant}\,(\frac{-13}{4}) \bullet 4 = 0.75 \bullet 4 = 3$

Por lo tanto el cociente y resto de la división de -13 por -4 son: $c = -c' = 4 \wedge r = r' = 3$

d) Resolvemos: $\frac{15}{6}$ en reales: $\frac{15}{6} = 2.5$

entonces: $c' = \text{ent}\,(\frac{15}{6}) = 2 \quad \wedge \quad r' = \text{mant}\,(\frac{15}{6}) \bullet 6 = 0.5 \bullet 6 = 3$

Por lo tanto el cociente y resto de la división de 15 por -6 son: $c = -c' = -2 \wedge r = r' = 3$

Divisibilidad

Sean $a, b \in \mathbb{Z}$, con $a \neq 0$: $a \mid b \Leftrightarrow \exists\, k \in \mathbb{Z} \,/\, b = k\,a$

Se lee:

a "divide a" b
a "es divisor de" b
b "es múltiplo de" a
b "es divisible por" a

Propiedades:

1) $\forall\, a \in \mathbb{Z}, a \neq 0:\; a \mid a$

2) $\forall\, a, b, c \in \mathbb{Z}, a \neq 0 \wedge b \neq 0:\; a \mid b \;\wedge\; b \mid c$ entonces $a \mid c$

3) $\forall\, a, b, c \in \mathbb{Z}, a \neq 0:\; a \mid b \;\wedge\; a \mid c$ entonces $a \mid b + c$

4) $\forall\, a, b \in \mathbb{Z}, a \neq 0:\; a \mid b \;\wedge\; k \in \mathbb{Z}$ entonces $a \mid k\,b$

Los números enteros n que sólo son divisibles por $1, -1, n, -n$ se llaman PRIMOS.

Los primeros números primos son: $2, 3, 5, 7, 11, 13, 17, 19, 23$, ...y sus opuestos!!!!!
Los matemáticos han demostrado que existen infinitos números primos, pero aún no encontraron una fórmula general para obtenerlos.

¿Por qué son importantes los números primos?
Pues cumplen muchas propiedades que no cumplen los números compuestos (los que no son primos).
Los números $1, -1, 0$ no son primos pero tampoco compuestos, son casos particulares.

Por ejemplo, pensemos si el siguiente condicional es verdadero o falso:

Sean, $n, a, b \in \mathbb{Z}$: Si $n \mid a \bullet b$ entonces $n \mid a \vee n \mid b$

Este condicional es FALSO, pues por ejemplo: $6 \mid 4 \bullet 9$ pero no es cierto que $(6 \mid 4 \vee 6 \mid 9)$

En cambio si nos dijeran que el número n es primo, entonces sí la propiedad es cierta y se puede demostrar fácilmente. Es la que enunciamos a continuación:

Propiedad: Si $p \mid a \bullet b \wedge p$: primo $\Rightarrow p \mid a \vee p \mid b$

Teorema fundamental de la aritmética

Todo número entero distinto de 0, 1 y -1, es o bien primo o se puede escribir como producto de factores primos de manera única salvo el orden.

Ejemplo:

$84 = 2^2 \bullet 3 \bullet 7 \qquad 165 = 3 \bullet 5 \bullet 11$

A continuación demostraremos un ejercicio de divisibilidad:

$5 \mid 23^n - 18^n, \forall\, n \in \mathbb{N}$

Para demostrar esta propiedad vamos a utilizar inducción completa.

Nos conviene escribir la proposición en forma de igualdad, de esta forma:

P(n): $23^n - 18^n = 5\,k \wedge k \in \mathbb{Z}$

Paso base:

n =1: $23^1 - 18^1 = 5 = 5 \bullet 1 \wedge 1 \in \mathbb{Z}$

Paso inductivo:

Hip. Ind: $23^h - 18^h = 5\,k \wedge k \in \mathbb{Z}$

Tesis Ind: $23^{h+1} - 18^{h+1} = 5\,t \wedge t \in \mathbb{Z}$

Dem./ $23^{h+1} - 18^{h+1} = 23^h \bullet 23 - 18^h \bullet 18 = 23^h \bullet (5 + 18) - 18^h \bullet 18 =$

$= 5 \bullet 23^h + 18 \bullet (23^h - 18^h) = 5 \bullet 23^h + 18 \bullet 5\,k = 5 \bullet (23^h + 18\,k) = 5\,t$

Pues $23^h + 18\,k \in \mathbb{Z}$ por ser productos y suma de enteros.

Por lo tanto, por principio de inducción, $\forall n \in \mathbb{N}$ se cumple $p(n)$ es verdadera

MCM (mínimo común múltiplo) y MCD (máximo común divisor)

Sean $a, b \in \mathbb{Z}$, no simultáneamente nulos, y sea $m \in \mathbb{Z}^+$, entonces $m = m.c.m.\ (a,b)$ si y sólo si se cumplen las siguientes condiciones:

1) $a \mid m$
2) $b \mid m$
3) Si $m' > 0$: $a \mid m' \wedge b \mid m' \Rightarrow m \mid m'$

Sean $a, b \in \mathbb{Z}$, no simultáneamente nulos, y sea $d \in \mathbb{Z}^+$, entonces $d = m.c.d.\ (a,b)$ si y sólo si se cumplen las siguientes condiciones:

1) $d \mid a$
2) $d \mid b$
3) Si $d' > 0$: $d' \mid a \wedge d' \mid b \Rightarrow d' \mid d$

Notaciones:

$$\text{m.c.m.}(a,b) = [\ a, b\ ] \qquad\qquad \text{m.c.d.}(a,b) = (\ a, b\ )$$

Tengamos en cuenta que:

Si $a = 0 \vee b = 0$ entonces $\text{m.c.m.}(a,b) = 0 = \text{mcm}(a,b)$

Propiedad del MCD entre dos enteros: puede ser escrito como combinación lineal entera de dichos enteros
Si $d = \text{m.c.d.}(a,b)$ entonces $\exists\ k_1, k_2 \in \mathbb{Z}$ tales que $d = k_1\ a + k_2\ b$

Propiedad del MCM y MCD: el producto de ambos es igual al módulo de $a \bullet b$

$$(\ a,b\ ) \bullet [\ a,b] = |\ a \bullet b\ |$$

e

Por ejemplo:

Dados los enteros: $a = 64$ y $b = 48$, vamos a calcular el $\text{m.c.d.}(64,48)$ y el $\text{m.c.m.}(64,48)$
Primero factoreamos ambos números: $64 = 2^6 \qquad 48 = 2^4 \bullet 3$
Entonces: $\text{m.c.d.}(64,48) = 2^4 = 16$ y $\text{m.c.m.}(64,48) = 2^6 \bullet 3 = 192$
El producto: $16 \bullet 192$ es 3072 que es igual al producto $64 \bullet 48 = 3072$
Podemos escribir al 16 como combinación lineal entera de 64 y 48: $16 = 1 \bullet 64 + (-1) \bullet 48$

e

¿Cómo encontramos los dos enteros s y t para escribir al $\text{m.c.d.}(a,b)$ como combinación lineal entera de ambos cuando "no se ven a simple vista"?

Una forma es utilizando el Algoritmo de Euclides para calcular el máximo común divisor por sucesivas divisiones. Veamos…

Algoritmo de Euclides para calcular el máximo común divisor

Dados dos enteros a y b, el $\text{m.c.d.}(a,b) = \text{m.c.d.}(b,r)$ siendo r el resto de la división de a por b. Esta propiedad puede demostrarse.
Volvemos a aplicar esta propiedad, es decir $\text{m.c.d.}(b,r) = \text{m.c.d.}(r, r_1)$ siendo r_1 el resto de la división de b por r. Luego $\text{m.c.d.}(r, r_1) = \text{m.c.d.}(r_1,r_2)$ siendo r_2 el resto de la división de r por r_1. Y así sucesivamente hasta llegar a un resto igual a cero. De esta manera se puede encontrar el m.c.d. entre dos enteros dados, ya que es el último resto no nulo.

e

Por ejemplo:
Vamos a calcular el $\text{m.c.d.}(720, 224)$. Para ello realizamos las siguientes divisiones enteras sucesivas:

1) $720 / 224 \Rightarrow c = 3 \wedge r = 48$

2) $224 / 48 \Rightarrow c_1 = 4 \wedge r_1 = 32$

3) $48 / 32 \Rightarrow c_2 = 1 \wedge r_2 = 16$

4) $32 / 16 \Rightarrow c_3 = 2 \wedge r_3 = 0$

Entonces m.c.d.(720,224) = 16

También se puede hacer en forma matricial:

Primero se coloca la matriz identidad de orden 2, y en una tercer columna los dos números enteros, siendo el mayor el de la primera fila.

1	0	720	F_1
0	1	224	F_2

La idea es ir obteniendo nuevas filas, siempre operando con las últimas dos anteriores, de modo de restar de la anteúltima la mayor cantidad de veces que entra el término independiente de la última. En realidad es hacer la división entera y restar el cociente por el elemento de la última fila.
Por ejemplo, en este caso, al dividir 720 por 224, se obtiene cociente 3, entonces vamos a restar 3 veces la fila 2 de la fila 1, la resta se hace en toda la fila:

1	0	720	F_1
0	1	224	F_2
1	-3	48	$F_3 = F_1 - 3\,F_2$

Y luego seguimos este procedimiento hasta llegar a un valor nulo. El anterior al nulo es el máximo común divisor.

1	0	720	F_1
0	1	224	F_2
1	-3	48	$F_3 = F_1 - 3\,F_2$
-4	13	32	$F_4 = F_2 - 4\,F_3$
5	-16	16	$F_5 = F_3 - F_4$
		0	$F_6 = F_4 - 2\,F_5$

Obtenemos que m.c.d.(720,224) = 16 y además: $16 = 5 \bullet 720 + (-16) \bullet 16$

TEOREMA DE BEZAUT

Este Teorema enuncia que:
Dados dos enteros a y b, entonces m.c.d.(a,b) = 1 $\Leftrightarrow$ $1 = s \bullet a + t \bullet b$ con $s,t \in \mathbb{Z}$

Este teorema nos sirve para demostrar que dos enteros son coprimos, o sea que su m.c.d. es 1 solamente demostrando que 1 es combinación lineal entera de ambos.

e Ejemplo 1:

Como $1 = 3 \bullet 8541 + (-2) \bullet 12811$ entonces podemos asegurar que m.c.d.(8541, 12811) = 1

Ejemplo 2:

Dos enteros consecutivos siempre son coprimos. (m.c.d.(x, x+1) = 1)
Ya que $1 \bullet (x+1) + (-1) \bullet x = 1$

Ejemplo 3:

Sabiendo que **a** y **b** son coprimos, podemos demostrar que **a** y **a+b** también lo son.
Podemos demostrarlo:

$1 = s \bullet a + t \bullet b$ con $s, t \in Z \Rightarrow 1 = s \bullet a + t \bullet (b+a-a) \Rightarrow 1 = s \bullet a + t \bullet (b+a) - t \bullet a \Rightarrow$

$1 = (s-t) \bullet a + t \bullet (b+a) \Rightarrow 1 = k \bullet a + t \bullet (b+a)$ con $k \in Z$ pues es resta de dos enteros.

$\Rightarrow$ m.c.d.(a, a+b) = 1

En la Guía de TP podés resolver los ejercicios de enteros (4.1 al 4.7). Cualquier duda, no dudes en consultar a tus tutores.

A continuación veremos el último tema de esta primera unidad, que es la base para poder entender luego la representación numérica en las computadoras, así como también para comprender lo que vas a estudiar en otra asignatura llamada “Arquitectura de computadoras”.

SISTEMAS DE NUMERACION

Desde hace mucho tiempo, el hombre ha utilizado símbolos para representar los números. Un sistema de numeración conocido es el romano, el cual consta de los símbolos I, V, X, L, C, D, M, donde cada uno representa una cantidad fija y hay ciertas reglas para formar los otros números.
El sistema de numeración utilizado por nosotros es posicional ya que cada símbolo tiene distinto valor según la posición en la que se encuentra (unidades, decenas, centenas, etc.) Se usan 10 símbolos, por eso nuestro sistema se llama decimal. Pero las computadoras representan los números en otro sistema, que es el binario (utilizando únicamente dos símbolos 0 y 1), o bien el hexadecimal, que utiliza 16 símbolos. Para poder comprender bien estos otros sistemas, repasemos un poco nuestro sistema decimal.

Expresión polinómica de un número entero:

Pensemos en un número entero, por ejemplo: $x = 5684379$

Recordemos que podemos escribirlo de la siguiente manera:

$$x = 5 \bullet 10^6 + 6 \bullet 10^5 + 8 \bullet 10^4 + 4 \bullet 10^3 + 3 \bullet 10^2 + 7 \bullet 10 + 9$$

Esta forma se denomina expresión o descomposición polinómica en función de la base, que es 10 en este caso.

Generalizando:

Sea x un número decimal entero, formado por los dígitos:
$x_n\ x_{n-1}\ ...\ x_1\ x_0$ con $x_i \in \{0,1,2,3,4,5,6,7,8,9\}$

Entonces dicho número significa: $x = x_n\, 10^n + x_{n-1}\, 10^{n-1} + ... + x_1\, 10 + x_0$

Lo mismo ocurre con otros sistemas de numeración posicionales, que en vez de utilizar como base al 10, utilizan otras.

Sistema	Cantidad de Símbolos	Símbolos
binario	2	0, 1
base 3	3	0, 1, 2
base 4	4	0, 1, 2, 3
....		
base 11	11	0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A
....		
base 16	16	0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F

En cada uno de ellos, la notación posicional es equivalente a la polinómica. O sea:

$x_n\ x_{n-1}\ ...\ x_1\ x_0 = x_n\, b^n + x_{n-1}\, b^{n-1} + ... + x_1\, b + x_0$ donde b es la base.
Tené en cuenta que el número b, la base, es un número distinto de 1, ¿podés explicarlo?, pensalo en función de la descomposición factorial, donde la base, b, está elevada a distintas potencias, ¿ tiene sentido 1^m?

e Ejemplo:

Si queremos representar 5 unidades en el sistema de base 3, pensemos que $5 = 1 \bullet 3^1 + 2 \bullet 3^0$, entonces, el 5 en base 3 se escribe: 12_3

Si queremos representar 59 unidades en el sistema hexadecimal, pensemos que $59 = 3 \bullet 16 + 11$, entonces se escribe: 3 B

Pasaje de números de otras bases a base 10

Para realizar este pasaje se desarrolla la expresión polinómica y se hace la cuenta en decimal.

e Ejemplo: $20121_3 = 2 \bullet 3^4 + 0 \bullet 3^3 + 1 \bullet 3^2 + 2 \bullet 3 + 1 = 178_{10}$

Consideremos que puede utilizarse la regla de Ruffini tomando como coeficientes del dividendo a los dígitos del número dado ordenados de mayor a menor y el divisor es $x - b$ (siendo b la base). El valor equivalente en decimal es el resto de la división.

Tomando el mismo ejemplo anterior: 20121_3

$$\begin{array}{c|ccccc} & 2 & 0 & 1 & 2 & 1 \\ 3 & & 6 & 18 & 57 & 177 \\ \hline & 2 & 6 & 19 & 59 & 178 \end{array} \longleftarrow$$

este es el valor en decimal

Pasaje de números decimales a otras bases

Si consideramos el número $x = 3269$ expresado en base 10, y queremos por ejemplo expresarlo en base 4, podemos tratar de descomponerlo de la siguiente forma:

$$x = x_5 \bullet 4^5 + x_4 \bullet 4^4 + x_3 \bullet 4^3 + x_2 \bullet 4^2 + x_1 \bullet 4 + x_0$$

Aclaramos que no consideramos potencias mayores ya que en este caso $4^6 = 4096$ es mayor que nuestro número,

Si sacamos factor común 4 nos queda entre todos los términos excepto el último:

$$x = 4 \bullet (x_5 \bullet 4^4 + x_4 \bullet 4^3 + x_3 \bullet 4^2 + x_2 \bullet 4 + x_1) + x_0$$

podemos observar que esta expresión se puede interpretar como una división entera de x por 4, cuyo resto es x_0 y el cociente es $c = x_5 \bullet 4^4 + x_4 \bullet 4^3 + x_3 \bullet 4^2 + x_2 \bullet 4 + x_1$.

Es decir que el valor de x_0 es el resto de la división del número dado por 4.

Si repetimos esto con el cociente: $c = x_5 \bullet 4^4 + x_4 \bullet 4^3 + x_3 \bullet 4^2 + x_2 \bullet 4 + x_1$

Sacando factor común nuevamente 4: $c = 4 \bullet (x_5 \bullet 4^3 + x_4 \bullet 4^2 + x_3 \bullet 4 + x_2) + x_1$
Vemos que el valor de x_1 es el resto de la división del primer cociente por 4.

Nuevamente aplicamos lo mismo con el nuevo cociente obtenido:

$$c' = x_5 \bullet 4^3 + x_4 \bullet 4^2 + x_3 \bullet 4 + x_2 = 4 \bullet (x_5 \bullet 4^2 + x_4 \bullet 4 + x_3) + x_2$$

con lo cual el valor de x_2 es el resto de la división del segundo cociente por 4.

Nuevamente aplicamos lo mismo con el nuevo cociente obtenido:

$$c'' = x_5 \bullet 4^2 + x_4 \bullet 4 + x_3 = 4 \bullet (x_5 \bullet 4 + x_4) + x_3$$

con lo cual el valor de x_3 es el resto de la división del tercer cociente por 4.

Finalmente (en este caso) consideramos el nuevo cociente obtenido:

$$c''' = x_5 \bullet 4 + x_4$$

con lo cual el valor de x_4 es el resto de la división del cuarto cociente por 4 y el valor de x_5 es el cociente de esta última división entera.

Haciendo las cuentas:

Primera división: $3269 = 4 \bullet 817 + 1$ entonces $x_0 = 1$
Segunda división: $817 = 4 \bullet 204 + 1$ entonces $x_1 = 1$
Tercera división: $204 = 4 \bullet 51 + 0$ entonces $x_2 = 0$
Cuarta división: $51 = 4 \bullet 12 + 3$ entonces $x_3 = 3$
Primera división: $12 = 4 \bullet 3 + 0$ entonces $x_4 = 0$ y $x_5 = 3$

Escribiendo el número: $3269 = 303011_4$

Generalicemos:

Sea x un número decimal que deseamos escribir en base b.

$$x = x_n b^n + x_{n-1} b^{n-1} + ... + x_2 b^2 + x_1 b + x_0$$

Sacamos factor común b:

$$x = b (x_n b^{n-1} + x_{n-1} b^{n-2} + ... + x_2 b + x_1) + x_0$$

Se puede interpretar como la división de x por b, donde el cociente es c y el resto es x_0.

Análogamente, consideramos el cociente c:

$$c = b (x_n b^{n-2} + x_{n-1} b^{n-3} + ... + x_3 b + x_2) + x_1$$

con lo cual x_1 es el resto de la división.

Se continúa así hasta que el cociente sea cero.

e

Ejemplo:

Expresar 4798_{10} en base 4

Podemos efectuar las divisiones con la disposición práctica:

```
4798 | 4
07     1199 | 4
 39     39    299 | 4
  38    39     19    74 | 4
   2     3      3    34   18 | 4
                      2    2    4 | 4
                                0    1 | 4
                                     1   0
```

Por lo tanto leyendo de atrás hacia delante los restos: $4798_{10} = 1022332_4$

Un ejercicio para que practiques:

Escribí 10423_5 en base 10 y luego expresalo en base 2.

Al final de la unidad vas a encontrar la Tabla de Equivalencias entre diferentes bases, de los primeros 40 números naturales.

Pasaje de una base a otra que sea potencia

Existen algunos casos en que se puede pasar de una base a otra sin necesidad de utilizar como intermedia la decimal. Esos casos son aquellos en los que una de las bases es potencia de otra.

Pasaje de Base 2 a Base 4 : como $4 = 2^2$, entonces se toman los dígitos de dos en dos.

Ejemplo:

$$\text{Base 2}: \quad \underbrace{1\ 0}_{2}\ \underbrace{1\ 1}_{3}\ \underbrace{0\ 1}_{1}\ \underbrace{1\ 1}_{3}\ \underbrace{0\ 0}_{0}\ \underbrace{1\ 0}_{2}\ \underbrace{1\ 1}_{3}$$

Base 4 : 2 3 1 3 0 2 3

Pasaje de Base 2 a Base 8: como $8 = \mathbf{2^3}$, entonces se toman los dígitos de tres en tres.

Ejemplo:

$$\text{Base 2}: \quad \underbrace{1\ 0}_{2}\ \underbrace{1\ 1\ 0}_{6}\ \underbrace{1\ 1\ 1}_{7}\ \underbrace{0\ 0\ 1}_{1}\ \underbrace{0\ 1\ 1}_{3}$$

Base 8 : 2 6 7 1 3

Pasaje de Base 2 a Base 16 : como $16 = 2^4$, entonces se toman los dígitos de .... en ....

e Ejemplo:

Base 2 : 10 1101 1100 1011

Base 16 : 2 D C B

Pasaje de Base 4 a Base 16 : como $16 = 4^2$, entonces se toman los dígitos de .... en ....

e Ejemplo:

Base 4 : : 2 3 1 3 0 2 3

Base 16 : 2 D C B

No sólo esto se puede usar para pasar de bases potencias de 2, sino para potencias de cualquier base, por ejemplo de 3:

Pasaje de Base 3 a Base 9 : como $9 = 3^2$, entonces se toman los dígitos de tres en tres

Base 3 : 1 0 1 2 0 1 1 2 2 0

Base 9 : 3 5 1 5 6

Operaciones en las distintas bases

Si bien este tema vas a estudiarlo con más detalle en otra asignatura (Arquitectura de computadores), te comentamos brevemente como se realizan las operaciones en las diferentes bases. En realidad, se resuelven de la misma manera que en el sistema decimal pero teniendo en cuenta la tabla en la base correspondiente.

<u>Suma:</u>
Se van sumando los dígitos desde la derecha y si nos pasamos se le pasa al de la izquierda, igual que en decimal, pero con la correspondiente tabla.

Ejemplo de suma en binario:

$$
\begin{array}{rl}
1\,1\,0\,1\,0\,1\,0\,1\,0\,1 & \text{(853 decimal)} \\
+\quad 0\,1\,0\,1\,1\,0\,0\,1\,1\,1 & \text{(359 decimal)} \\
\hline
1\,0\,0\,1\,0\,1\,1\,1\,1\,0\,0 & \text{(1212 decimal)}
\end{array}
$$

Resolvé: $B0C0EF_{16} + 123A0_{16} + 1453CF_{16} =$

$1000111_2 + 1213072_8 =$

Resta:

¿Cómo restás en decimal?

Por ejemplo, para hacer 834 - 567, debemos pedir prestado ya que no podemos restar 7 de 4.
Lo mismo puede utilizarse para las restas en otras bases. Pero hay un procedimiento mejor para ello, que emplea suma en vez de resta:

Resta por Suma de Complemento a la Base menos 1

Observá esto:

Método tradicional	Complemento a la (base -1)	
8 3 4	Minuendo	8 3 4
- 5 6 7	Complemento a 9 (10-1) del sustraendo	+ 4 3 2
2 6 7	Agrego un 1	1
	Sumo todo	1 2 6 7

¿Qué obtenemos? El primer uno se descarta y nos queda el resultado.

¿Por qué este método es muy práctico en binario?

Porque en binario, el complemento a 1 es simplemente cuestión de cambiar ceros por unos y unos por ceros.

Ejemplo:

Resolvamos por medio de complemento a la base menos 1:

$10010111100_2 - 101100111_2 =$

No lo olvides: debemos completar el sustraendo para que tenga la misma cantidad de dígitos que el minuendo.

$1\,0\,0\,1\,0\,1\,1\,1\,1\,0\,0_2$	se copia igual:	$1\,0\,0\,1\,0\,1\,1\,1\,1\,0\,0_2$
$-\ 0\,0\,1\,0\,1\,1\,0\,0\,1\,1\,1_2$	lo complemento:	$1\,1\,0\,1\,0\,0\,1\,1\,0\,0\,0_2$
	Agrego un 1:	1_2
	Sumamos todo:	$1\,0\,1\,1\,0\,1\,0\,1\,0\,1\,0\,1_2$
	Descartamos el primer 1:	$0\,1\,1\,0\,1\,0\,1\,0\,1\,0\,1_2$

Este número es: $1\,1\,1\,0\,1\,0\,1\,0\,1\,0\,1_2 = 1 + 4 + 16 + 64 + 256 + 512 = 853$

Multiplicaciones y divisiones:

Se hacen teniendo en cuenta las tablas en cada base. En esta asignatura no vamos a profundizarlas.

Para finalizar resolvé los siguientes ejercicios:

1) Calcula x: $1645_x - 571_x = 1064_x$

2) Calcula x: $203_x\ 1010_x = 205030_x$

3) Halla b: $11_b\ 35_b = 385_b$

4) Halla b: $111_b \mid 10101_b$

5) Halla h: $4h3_5 = h30_9$

6) Un número de tres cifras $x_2x_1x_0$ en base 3 representa $5/8$ de lo que representa en base 4. Halla dichos dígitos y escribe el número en base 2.

Con esto damos por finalizada la Unidad 1. Una vez que hayas completado todos los ejercicios de la guía, te propondremos una autoevaluación antes de pasar a la segunda unidad. Buena suerte!!!!

Tabla de equivalencias entre distintas bases:

Para que tengas a mano, a continuación hay una tabla de los primeros 40 números naturales, expresados en distintas bases.

Decimal	Binario	Base 3	Base 4	Base 5	base 8	Base 16
1	1	1	1	1	1	1
2	10	2	2	2	2	2
3	11	10	3	3	3	3
4	100	11	10	4	4	4
5	101	12	11	10	5	5
6	110	20	12	11	6	6
7	111	21	13	12	7	7
8	1000	22	20	13	10	8
9	1001	100	21	14	11	9
10	1010	101	22	20	12	A
11	1011	102	23	21	13	B
12	1100	110	30	22	14	C
13	1101	111	31	23	15	D
14	1110	112	32	24	16	E
15	1111	120	33	30	17	F
16	10000	121	100	31	20	10
17	10001	122	101	32	21	11
18	10010	200	102	33	22	12
19	10011	201	103	34	23	13
20	10100	202	110	40	24	14
21	10101	210	111	41	25	15
22	10110	211	112	42	26	16
23	10111	212	113	43	27	17
24	11000	220	120	44	30	18
25	11001	221	121	100	31	19
26	11010	222	122	101	32	1A
27	11011	1000	123	102	33	1B
28	11100	1001	130	103	34	1C
29	11101	1002	131	104	35	1D
30	11110	1010	132	110	36	1E
31	11111	1011	133	111	37	1F
32	100000	1012	200	112	40	20
33	100001	1020	201	113	41	21
34	100010	1021	202	114	42	22
35	100011	1022	203	120	43	23
36	100100	1100	210	121	44	24
37	100101	1101	211	122	45	25
38	100110	1102	212	123	46	26
39	100111	1110	213	124	47	27
40	101000	1111	220	130	50	28