CAPITULO III: TEORÍA DE NÚMEROS

En este capítulo, se hace de los conjuntos numéricos una presentación intuitiva en unos casos y formal en otros. A partir de los Naturales, iremos ampliando los otros conjuntos numéricos.

3.1 Números Naturales

Consideraremos como **número natural o aritmético** cero, uno, dos, . . . y denotaremos 0, 1, 2, . . . a la **idea natural** que expresa cuantos elementos tiene un conjunto finito. Al conjunto de todos los números naturales se denota con **N**.

Además, acordemos que si dos conjuntos finitos son equipotentes, o sea sus elementos pueden ser puestos en correspondencia biunívoca, a éstos se les asocia el mismo natural.

Al conjunto vacío $\varnothing$ le asociamos el natural 0.
A cualquier conjunto unitario {a} le asociamos el natural 1.

NOTA. A partir de este conjunto unitario, para abstraer los demás números naturales, es suficiente ir añadiendo cada vez un elemento más al conjunto anterior; así:

Al conjunto {a, b} le asociamos el natural 2.
Al conjunto { a, b, c} le asociamos el natural 3; etc.

De esta manera es evidente que a cada número natural sigue otro, luego, este conjunto **N** es infinito. Tabulemos una parte de **N**

$$\mathbf{N} = \{ 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, \ldots \}$$

Consideremos el subconjunto **N*** de **N**

$$\mathbf{N^*} := \mathbf{N}-\{0\} = \{ 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, \ldots \}$$

NOTA. El lector está familiarizado con la suma y multiplicación de números que son **operaciones internas binarias**. Por ahora diremos **estructura** a un conjunto con una o dos operaciones internas. En el próximo capítulo hablaremos de estructuras algebraicas.

3.1.1 Operaciones y propiedades en N

El conjunto **N** está dotado de la operación interna binaria ADICIÓN.

La estructura aditiva (**N**,+), tiene las siguientes propiedades:

1) **N** es cerrado respecto a +; esto es: $\forall a,b\in\mathbf{N} \quad a+b\in\mathbf{N}$
2) El + es conmutativo en **N** ; esto es: $\forall a,b\in\mathbf{N} \quad a+b = b+a$
3) El + es asociativo en **N**; esto es: $\forall a,b,c\in\mathbf{N} \quad (a+b)+c = a+(b+c)$
4) Existe el 0 en **N** como elemento neutro respecto al + (existencia del elemento neutro); esto es: $\exists 0\in\mathbf{N} \ / \ \forall a\in\mathbf{N} \quad a+0 = a$

El conjunto **N** está dotado de la operación interna MULTIPLICACIÓN ($\bullet$).

La estructura multiplicativa (**N**, $\bullet$) tiene las siguientes propiedades:

1) **N** es cerrado respecto a $\bullet$; esto es: $\forall a,b\in\mathbf{N}\quad a.b\in\mathbf{N}$

2) El **.** es conmutativo en **N**; esto es: $\forall a,b\in\mathbf{N}\quad a.b = b.a$

3) El **.** es asociativo en **N**; esto es: $\forall a,b,c\in\mathbf{N}\quad (a.b).c = a.(b.c)$

4) Existe el $1\in\mathbf{N}$ como elemento neutro en **N** respecto al **.** (existencia del elemento neutro);

esto es: $\exists 1\in\mathbf{N} / \forall a\in\mathbf{N}\quad a.1 = a$

La multiplicación es distributiva con la adición, esto es:

$$\forall a,b,c\in\mathbf{N}\quad a.(b+c) = a.b+a.c \text{ y además } (b+c).a = b.a+c.a$$

DEF. Definimos en **N la relación** de orden **<** de la siguiente manera:

$$\forall a,b\in\mathbf{N}\quad a < b \overset{\text{def}}{\iff} \exists\, c\in\mathbf{N}\quad c\neq 0\quad \text{t.q}\quad a+c = b$$

NOTA. El conjunto de los naturales es totalmente ordenado con la relación <, ya que dados dos elementos cualesquiera $a,b\in\mathbf{N}$ para ellos se verifica la propiedad de **tricotomía;** esto es: $a = b$ o $a < b$ o $b < a$

Por esta razón, podemos escribir $0 < 1 < 2 < 3 < 4 < 5 < \ldots$ y por eso se dice que **<** es una relación de orden total en **N** y **N** se dice totalmente ordenado con esta relación.

NOTA. Algunos autores manifiestan lo siguiente:

a) Si queremos referirnos a que un conjunto cualquiera tiene por ejemplo cinco elementos, a este **5** se lo considera **natural cardinal**.

b) Si nos referimos al orden que ocupa un elemento en un conjunto, por ejemplo " primer elemento ", " segundo elemento ", a estos se los considera **naturales ordinales.**

3.1.2 Algo más en los Naturales

NOTA. Sean a,b dos números naturales; si la división de a por b es un natural (entero) por ejemplo p , se dice que :

a es divisible por b, o
a es múltiplo de b, o
b es divisor de a, o
b divide a,
y se denota $b \mid a$, lo que significa que $\exists p\in\mathbf{N} / a = pb$.

TEOREMA 1 (**de la división**). Por todo $a,b\in\mathbf{N}^*$ existen y son únicos $p,r\in\mathbf{N}$ tal que:

$$a = pb+r\ ,\ 0 \leq r < b.$$

a se dice dividendo; **b** se dice divisor; **p** se dice cociente, **r** se dice resto.

EJEMPLO 1

$$a = 8,\ b = 5, \text{ existen } p = 1,\ r = 3\quad \text{tq}\quad 8 = 1.5 + 3$$

3.1.2.1 Número par e impar

DEF. Se dice que $a\in\mathbf{N}$ es par si $\exists b\in\mathbf{N}$ tq $a = 2b$.

DEF. Se dice que $a \in \mathbf{N}$ es impar si no es par.

NOTA. Si $a \in \mathbf{N}$ es impar entonces existe $n \in \mathbf{N}$ tq $a = 2n+1$

LEMA 1. Se cumplen además en **N** las siguientes propiedades:

1) $\forall a \in \mathbf{N}^*$ $a \mid a$ ya que $\exists p = 1 / a = 1.a$

2) $\forall a \in \mathbf{N}$ $1 \mid a$ ya que $\exists p = a / a = a.1$

EJEMPLO 2

$\forall n \in \mathbf{N}^*$ $n(n+1)$ es divisible por 2.

3.1.2.2 Número primo

DEF. Sea $a \in \mathbf{N}$ $a \geq 2$, a es **primo** si es divisible "**únicamente**" para sí mismo y para la unidad.

Indiquemos con **P** el conjunto de los números primos, tabulemos una parte suya:

$$\mathbf{P} = \{ 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, \ldots \}$$

LEMA 2. El conjunto **P** de los números primos es infinito.

LEMA 3. $p \mid a$ y $p \mid b \Rightarrow p \mid a+b$

Descomposición en **factores primos** de $a \in \mathbf{N}$, $a \geq 2$

Sea a = 24, se tiene.

$$a = 24 = 2.12 = 2.2.6 = 2.2.2.3 = 2^3.3$$

En general se dirá que un número natural a está expresado en factores primos si:

$$a = p_1^{n_1}.p_2^{n_2}.\ \ldots\ .p_r^{n_r}$$

donde $p_1, p_2, \ldots, p_r$ son números primos y $n_1, n_2, \ldots, n_r \in \mathbf{N}^*$.

3.1.2.3 Divisores y múltiplos (de un número natural $a \neq 0$)

1) El conjunto de los divisores de $a \in \mathbf{N}^*$ es:

$$\mathcal{D}_a = \{ x \in \mathbf{N} / x \mid a \}, \text{ o lo que es lo mismo } \mathcal{D}_a = \{ x \in \mathbf{N} / \exists q \in \mathbf{N} : a = xq \}.$$

Por ejemplo si a = 30, se tiene

$$\mathcal{D}_{30} = \{1, 2, 3, 5, 6, 10, 15, 30\}$$

2) El conjunto de los múltiplos de $a \in \mathbf{N}^*$ es:

$$\mathcal{M}_a = \{ y \in \mathbf{N} / a \mid y \}, \text{ o lo que es lo mismo } \mathcal{M}_a = \{ y \in \mathbf{N} / \exists p \in \mathbf{N}: y = ap \}$$

Por ejemplo si a = 3 se tiene

$$\mathcal{M}_3 = \{ 3, 6, 9, 12, 15, 18, 21, 24, 27, \ldots \}$$

DEF. Dados dos números naturales a,b∈ **N***, el conjunto de los divisores de a y b es el siguiente:

$$\mathcal{D}_{a,\,b} := \mathcal{D}_a \cap \mathcal{D}_b$$

EJEMPLO 3

Si a = 4, b = 6 se tiene $\mathcal{D}_4 = \{1, 2, 4\}$, $\mathcal{D}_6 = \{1, 2, 3, 6\}$, $\mathcal{D}_{4,\,6} = \mathcal{D}_4 \cap \mathcal{D}_6 = \{1,2\}$

3.1.2.4 Máximo común divisor

DEF. Dados dos números naturales a,b∈ **N***, se llama máximo común divisor de a y b y se denota mcd (a,b) al max $\{\mathcal{D}_a \cap \mathcal{D}_b\}$; es decir:

$$\text{mcd}\,(a,b) = \max\{\mathcal{D}_a \cap \mathcal{D}_b\}$$

EJEMPLO 4

Sean a = 6 y b = 9, se tiene

mcd(6,9) = max $\{\mathcal{D}_6 \cap \mathcal{D}_9\}$ = max **{** {1, 2, 3, 6} ∩ {1, 3, 9} **}** = max {1,3} = 3

DEF. a,b∈**N*** se dicen *PRIMOS ENTRE SI* cuando mcd (a,b) = 1.

EJEMPLO 5. Son primos entre sí por ejemplo los siguientes pares de números:

3 y 4, 9 y 16, 5 y 6; etc

3.1.2.5 Mínimo común múltiplo

DEF. Dados dos números naturales a,b∈**N*** se llama **mínimo común múltiplo** de a y b y denotaremos MCM(a,b) al mínimo de los múltiplos comunes de a y b, o sea

$$\text{MCM}\,(a,b) = \min\{\mathcal{M}_a \cap \mathcal{M}_b\}$$

EJEMPLO 8

a = 3 $\mathcal{M}_3$= { 3, 6, 9, 12, 15, 18, 21, 24, 27, . . . }

b = 4 $\mathcal{M}_4$ = { 4, 8, 12, 16, 20, 24, 28, . . . }

$$\text{MCM}(3,4) = \min\{\mathcal{M}_3 \cap \mathcal{M}_4\} = \min\{\,12, 24, 36, \ldots\} = 12$$

Actividad de AUTÓNOMA SEMANA : Consultar el Algoritmo de EUCLIDES (para hallar el máximo común divisor) y aplicar en un ejemplo

ACTIVIDAD DE EXPRIMENTACIÓN SEMANA :

1) Hallar : a) mcd (10672, 4147); b) mcd (731, 443); c) MCM(18,45).