Teoría de Números

Matemática IV, Facultad de Informática, UNLP.
2019

Números Naturales

Los números naturales son aquellos que permiten contar los elementos de un conjunto. Se trata del primer conjunto de números que fue utilizado por los seres humanos para contar objetos. Tienen dos

grandes usos: se utilizan para especificar el tamaño de un conjunto finito y para describir qué posición ocupa un elemento dentro de una secuencia ordenada.

Históricamente, se han realizado propuestas para axiomatizar la noción habitual de números naturales, de entre las que destacan las de Peano y la construcción a partir de la teoría de conjuntos.

Números Enteros

Un número entero es cualquier elemento del conjunto formado por los números naturales, sus opuestos (versiones negativas de los naturales) y el cero.
Estos son:

- Los naturales (o enteros positivos): $+1, +2, +3, +4, +5...$
- El cero, que no es ni positivo ni negativo.
- Los enteros negativos: $-1, -2, -3, -4, -5...$

El conjunto de los enteros se designa por Z.

$Z = \{.... - 3, -2, -1, 0, 1, 2, 3, ...\}$

Orden de lo números enteros

El orden de los números enteros se define como:
Dados dos enteros de signos distintos, a y $-b$, el negativo es menor que el positivo: $-b < a$
Dados dos enteros con el mismo signo, el menor de los dos números es:

- El de menor valor absoluto, si el signo común es $+$
- El de mayor valor absoluto, si el signo común es $-$.
- El cero, 0, es menor que todos los positivos y mayor que todos los negativos.

Operaciones con números enteros

Los números enteros pueden sumarse, restarse, multiplicarse y dividirse, siguiendo el modelo de los naturales añadiendo unas normas para el uso del signo.

La **suma** de números enteros cumple las siguientes propiedades:

- *Propiedad asociativa.* Dados tres números enteros a, b y c, las sumas $(a+b)+c$ y $a+(b+c)$son iguales.
- *Propiedad conmutativa.* Dados dos números enteros a y b, las sumas $a+b$ y $b+a$ son iguales.
- *Elemento neutro.* Todos los números enteros a quedan inalterados al sumarles 0: $a+0=a$.

La **resta** de dos enteros (*minuendo menos sustraendo*) se realiza sumando el *minuendo* más el *sustraendo* cambiado de signo.

La **multiplicación** de números enteros cumple las siguientes propiedades:

- *Propiedad asociativa.* Dados tres enteros a, b y c, los productos $(a.b).c$ y $a.(b.c)$ son iguales.
- *Propiedad conmutativa.* Dados dos números enteros a y b, los productos $a.b$ y $b.a$ son iguales.
- *Elemento neutro.* Existe un número entero especial 1 tal que todos los números enteros a quedan inalterados al multiplicarlos por él.

Propiedad distributiva:
Dados tres números enteros a, b y c, el producto $a.(b+c)$ y la suma de productos $(a.b)+(a.c)$ son idénticos.

Divisibilidad en Z

Definición

Dados dos números enteros a y b, con b no nulo.
Se dice que b ***divide*** *a a , y se escribe $b|a$ si existe un entero c tal que $a = bc$.*
En este caso se dice que b es un divisor de a, a es divisible por b ó que a es múltiplo de b

Propiedades básicas : para a, b y c enteros,

- $a|a$
- $1|a$
- $a|0$
- $a|b$ entonces $a|-b$, $-a|b$ y $-a|-b$
- $a|b$ entonces $a|bc$
- $a|b$ y $b|c$ entonces $a|c$
- $a|b$ y $a|c$ entonces $a|b+c$

Divisibilidad en Z

Definición

Un número entero $p \neq 1, -1$, se dice ***primo*** *si sus únicos divisores son los triviales (ésto es el propio número, su opuesto, 1 y -1). Caso contrario se dice que el número es* ***compuesto***

Ej: $2, 3, 5, 7, \ldots.$ son primos
$4, 6, 8, 9 \ldots.$ son compuestos.

Algunas propiedades importantes relativas:

- Hay infinitos números primos
- Si m es un entero compuesto, entonces existe un primo p tal que p divide a m

Divisibilidad en Z

Dados $a, b \in Z$ con $b \neq 0$, se trata de realizar la división entera (o inexacta) entre a y b. Es decir que se trata de aproximar *de la mejor manera posible* a a por un múltiplo de b. La diferencia entre a y dicho número es lo que llamamos *resto* de la división; que será nulo en el caso que a sea múltiplo de b.

Teorema (Algoritmo de la división)

Dados $a, b \in Z$ con $b \neq 0$, existen y son únicos c (cociente) y r (resto) enteros tales que $a = bc + r$ con $0 \leq r < |b|$

Divisibilidad en Z

Teorema (Máximo Común Divisor)

Dados $a, b \in Z$ no simultáneamente nulos, existe un único entero d que satisface:

- $d|a$ *y* $d|b$
- *Si existe* D *tal que* $D|a$ *y* $D|b$ *entonces* $D|d$

Este entero d se denomina ***máximo común divisor entre a y b*** *y se lo denota (a, b) ó $m.c.d(a, b)$*

Observación

Dados $a, b \in Z$ y d su m.c.d, existen enteros m y n tales que $d = ma + nb$

Definición

Si $(a, b) = 1$ se dice que a y b son ***coprimos***

Algoritmo de Euclides

El algoritmo de Euclides es un método antiguo y eficiente para calcular el *mcd*. Fue originalmente descrito por Euclides en su obra Elementos. El algoritmo extendido es una ligera modificación que permite expresar al *mcd* como una combinación lineal.

Dados $a, b \in Z$, supongamos $a \geq b$ con $b \neq 0$.
Por el algoritmo de la división existen c_1 y r_1 tales que $a = c_1 b + r_1$ con $0 \leq r_1 < b$.
Si $r_1 = 0$, $(a, b) = (b, r_1) = (b, 0) = b$
Si $r_1 \neq 0$, podemos decir que existen c_2 y r_2 tales que $b = c_2 r_1 + r_2$ con $0 \leq r_2 < r_1$. Si r_2 es cero, ya está, el mcd es r_1, si no es cero repetimos el proceso. Y así sucesivamente.

Concluímos:
$(a, b) = (b, r_1) = (r_1, r_2) = (r_2, r_3) = ... = (r_{n-1}, r_n) = (r_n, 0) = r_n$
siendo r_n el último resto no nulo

Divisibilidad en Z

Teorema (Mínimo Común Múltiplo)

Dados $a, b \in Z$, existe un único entero m que satisface:

- $a|m$ *y* $b|m$
- *Si existe* M *tal que* $a|M$ *y* $b|M$ *entonces* $m|M$

Este entero m se denomina ***mínimo común múltiplo entre a y b*** *y se lo denota* $[a, b]$ *ó* $mcm[a, b]$

Observación

Se puede demostrar que $|a.b| = (a, b)[a, b]$

Teorema (Teorema Fundamental de la Aritmética)

Todo número entero distinto de $0, 1, -1$ *es producto finito de números primos y esa factorización es única salvo el orden.*