Números Enteros

1 Introducción

Vamos a considerar ya conocido el conjunto de los números naturales $0, 1, 2, 3....$ (denotado por N), usados habitualmente para contar, enumerar, etc.

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.

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

2 Orden de los 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.

3 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.

1. La **suma** de números enteros es cerrada, es decir, la suma de dos números enteros da como resultado otro número entero.

   Además 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: $a + 0 = a$. para todo a entero.

- *Ley de Monotonía de la suma.* Dados tres números enteros a, b y c,vale que si $a \leq b$ entonces $a + c \leq b + c$.

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

3. La **multiplicación** de números enteros da como resultado un número entero, es decir, la multiplicación es una operación cerrada en Z. Además se cumplen 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, $a.1 = 1.a = a$ para cualquier a entero.
   - *Ley de Monotonía del producto.* Dados números enteros a, b,vale que si $a \leq b$ entonces $a.c \leq b.c$ cualquiera sea c.

   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.

   Es decir, $a(b + c) = ab + ac$

La **división** de enteros tiene características especiales y la estudiaremos con algo más de detalle en el próximo apartado.

4 Divisibilidad en Z

Definición 4.1 *Dados dos números enteros a y b, con b no nulo.*
Se dice que a ***divide*** *a b , y se escribe a|b si existe un entero c tal que $b = ac$.*
En este caso se dice que a es un divisor de b, b es divisible por a ó que b es múltiplo de a

4.1 Propiedades Básicas

Dados a, b, c enteros cualesquiera, valen las siguientes propiedades:

- $a|a$
- $1|a$
- $a|0$
- $a|b$ 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 $a|b+c$

Demostraremos algunas de estas propiedades a modo de ejemplo (el resto de las demostraciones quedan como ejercicio para el lector)

- $a|a$

  Queremos ver que cualquier entero a se divide a si mismo, es decir, por la definición, queremos ver que existe algún entero c tal que $a = a.c$, y como vemos ese entero c existe y es 1, $a = a.1$. Luego, a divide a a

- $a|0$

  Ahora probemos que cualquier entero divide a 0. De esta forma vemos que el 0 (el neutro para la suma de enteros) tiene infinitos divisores (pero él mismo no divide a ningún entero!! por qué? demuéstrelo!) Como antes, queremos ver si existe ese entero c tal que $0 = a.c$ para cualquier entero a, pero ese entero c es el mismo 0!! ya que $0 = a.0$ para todo a, y de esta forma $a|0$.

- $a|b$ y $b|c$ entonces $a|c$

  Sabiendo que $a|b$ y que $b|c$ tenemos que probar que $a|c$, o sea, que existe un entero k tal que $c = a.k$. Por hipótesis sabemos que existe un entero h tal que $b = a.h$ y un entero t tal que $c = b.t$, luego $c = b.t = (a.h).t$ y como el producto de enteros es cerrado y asociativo vale que $c = b.t = (a.h).t = a.(h.t) = a.k$ con $k = h.t$ en Z, y por lo tanto a divide a c (valiendo la propiedad transitiva de la división de enteros).

- $a|b$ y $a|c$ entonces $a|b + c$

  Vamos a suponer que $a|b$ y $a|c$ entonces existen enteros B y C tales que $b = a.B$ y $c = a.C$, luego $b+c = a.B+a.C = a.(B+C)$ y como vale la propiedad distributiva (aqui la usamos sacando factor común a) y la suma es cerrada en Z existe $k = B + C$ entero tal que $b + c = a.k$ y probamos que $a|b + c$.

4.2 Enteros Primos

Definición 4.2 *Un número entero $p \neq 1$ 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: $2, 3, 5, 7, ...$ son primos
$4, 6, 8, 9....$ son compuestos.

Algunas propiedades importantes relativas que no demostraremos:

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

Teorema 4.3 (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.*

4.3 Algoritmo de la División

Dados $a, b \in Z$ con $b \neq 0$, cuando no existe el entero c que haga valer la igualdad $a = bc$, 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 4.4 *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 $0 \leq r < |b|$*

Ejemplo 4.5 *Sea a y b dos números enteros que tienen restos 4 y 7 respectivamente en la división por 11. Hallar el resto de la división por 11 de $2a+b$*

Por el algoritmo de la división y los datos que nos dan podemos saber que $a = 11A+4$ y $b = 11B+7$, y queremos ver cual es el resto de la división de $2a+b$, o sea, queremos encontrar r de $2a+b = 11Q+r$.

$2a+b = 2(11A+4)+(11B+7) = 2.11A+8+11B+7 = 22A+11B+15 = 11(2A)+11B+11+4 = 11(2A+B+1)+4$
Luego, el resto es 4

4.4 Máximo Común Divisor

Se define el **Máximo Común Divisor (MCD)** de dos o más números enteros al mayor número entero que los divide sin dejar resto.

Teorema 4.6 (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 es el denominado ***máximo común divisor entre a y b*** *y se lo denota (a, b) ó $m.c.d(a, b)$*

Ejemplos 4.7 *Encontar el máximo común divisor entre 8 y 64, y entre 45 y 60.*

- *Como el 8 es un divisor de 64 (y obviamente de él mismo) el $m.c.d(8, 64)$ será 8.*
- *Claramente vemos que 45 y 60 no se dividen mutuamente, tenemos que buscar dividores comunes y entre ellos tomar el menor. Podríamos listar todos los divisores de cada número y de allí elegirlo, o podemos descomponer cada entero en producto de primos y buscar los factores en común.*

  $45 = 15.3 = 5.3.3 = 5.3^2$

  $60 = 20.3 = 4.5.3 = 2.2.5.3 = 2^2.5.3$

  Vemos que $5.3 = 15$ es el mayor factor en común, y por lo tanto será el m.c.d

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

Ejemplos 4.8

- $(60, 45) = (45, 15) = (15, 0) = 15$
- $(86, 22) = (22, 20) = (20, 2) = (2, 0) = 2$

Una propiedad muy útil es la llamada *Identidad de Bézout* que veremos sin su demostración

Proposición 4.9 *Dados $a, b \in Z$ y d su m.c.d, existen enteros m y n tales que $d = ma + nb$*

Ejemplo 4.10 *Usemos la Identidad de Bézout para probar el siguiente resultado: Si $(a, b) = d$; $a|c$ y $b|c$ entonces $ab|cd$*

Queremos probar que ab divide a cd siendo d el máximo común divisor entre a y b y sabiendo que a c lo dividen tanto a como b.

Como $a|c$ existe, por definición de división, un entero A tal que $c = aA$, y como $b|c$ existe un entero B tal que $c = bB$.

Por otro lado, por ser $d = (a, b)$ y la Identidad de Bézout, existen enteros m y n tales que $d = ma+nb$.

Luego, $cd = c(ma+nb) = cma+cnb = mac+nbc = mabB+nbaA = ab(mB+nA)$ ya que el producto de enteros es cerrado, conmutativo y asociativo.

De esta forma vemos que existe un entero $k = mB + nA$ tal que $cd = ab.k$ y por lo tanto $ab|cd$

Definición 4.11 *Si $(a, b) = 1$ se dice que a y b son* ***coprimos***

Ejemplo 4.12 *Sean a y b dos enteros coprimos, demostrar que $a + b$ y a son coprimos.*

Una forma de probar que dos enteros son coprimos es suponer que no lo son. Supongamos que existe d un entero tal que $d = (a + b, a)$, por definición de m.c.d este entero divide a $a + b$ y divide a a.

Fácilmente se puede probar que si $d|a + b$ y $d|a$ entonces d debe dividir a b. Luego, $d|a$ y $d|b$ y por lo tanto $d|(a, b)$ por definición de m.c.d. Pero entonces $d|1$ y no hay no le queda otra opción que ser $d = 1$.

Observación 4.13 *Si p es primo, entonces el (a, p) para cualquier $a \in Z$ será el propio p o son coprimos.*

Esto vale ya que al ser p primo el único factor en común que puede tener con otro entero es él mismo, en ese caso lo divide y el $m.c.d$ es el primo p. Caso contrario, no tienen factores en común y el $m.c.d$ es 1, es decir, son coprimos.

4.5 Mínimo Común Múltiplo

El Mínimo Común Múltiplo (abreviado $m.c.m$) de dos o más números naturales es el menor número natural distinto de cero que es múltiplo común de todos ellos (o el ínfimo del conjunto de los múltiplos comunes).

Teorema 4.14 (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 4.15 *Se puede demostrar que $|a.b| = (a, b)[a, b]$*