Los enteros

Denotaremos por $\mathbf{Z}$ el conjunto de números enteros y por

$$\mathbf{N} = \{0, 1, 2, ...\}$$

el conjunto de los números naturales.

Tenemos operaciones elementales de suma y multiplicación de números enteros con los propiedades siguientes para todos los $a, b, c \in \mathbf{Z}$:

1. Propiedades asociativas, $a + (b + c) = (a + b) + c$, $a(bc) = (ab)c$;
2. Propiedades conmutativas $a + b = b + a$, $ab = ba$;
3. Propiedad distributiva $a(b + c) = ab + ac$;
4. Elementos neutros $a + 0 = a$, $a1 = a$;
5. Elemento simétrico para la suma, existe $-a \in \mathbf{Z}$ tal que $a + (-a) = 0$.

Escribiremos $a - b = a + (-b)$.

Dominio de integridad: $ab = 0$ si y sólo si $a = 0$ ó $b = 0$.

Tenemos definido un orden en los números enteros que verifica

$a < b$ implica $a + c < b + c$

$a < b$ implica $ac < bc$ cuando c es un entero positivo.

Finalmente tenemos definido el **valor absoluto** en los números enteros mediante $|a|$ es a si a es un número natural y $-a$ en caso contrario.

Supondremos como axioma básico el de **conjunto bien ordenado**

Principio de buena ordenación

Toda subconjunto S de números naturales no vacío contiene un elemento mínimo (i.e. un elemento $a \in S$ verificando $a \leq x$ para todo $x \in S$).

Este es equivalente a los dos principios de inducción siguientes

Principio de inducción matemática I

Si S es un subconjunto del conjunto de los números naturales tal que $0 \in S$ y que verifica que

si $n \in S$, entonces $n + 1 \in S$ para cada número natural n

necesariamente se tiene que $S = \mathbf{N}$.

Principio de inducción matemática II

Si S es un subconjunto del conjunto de los números naturales tal que $0 \in S$ y que verifica que

2. si $m \in S$ para cada $0 \leq m < n$ entonces $n \in S$ para cada número natural n

necesariamente se tiene que $S = \mathbf{N}$.

Demostración por inducción

Sea $P(n)$ una afirmación relativa a los números naturales y supongamos que queremos demostrala para todo número natural. Entonceds por el principio de inducción podemos

1) Probar $P(0)$

y

2) Probar que para todo n, si suponemos $P(n)$ entonces deducimos $P(n + 1)$.

Divisibilidad

Definición Sean a, b enteros. Entonces a divide a b (equivalentemente a es un divisor de b) si existe un entero c tal que $b = ac$. Si a divide a b, entonces escribiremos $a|b$.

Propiedades de la divisibilidad

Sean a, b, c enteros, entonces se tiene

i) a—a

ii) Si $a|b$ y $b|c$, entonces $a|c$

iii) Si $a|b$ y $a|c$, entonces $a|(bx + cy)$ para todos los enteros x, y

iv) Si $a|b$ y $b|a$, entonces $a = +b$ o $a = -b$.

Algoritmo de división de enteros

Si a, b son enteros con $b \geq 1$, la división ordinaria de a entre b da dos enteros, un cociente q y un resto r tales que

$$a = bq + r$$

donde $0 \leq r < b$. Además el cociente y resto son únicos.

Escribimos $r = a \, mod \, b$.

Definición. Un entero c es un divisor común de a y b si $c|a$ y $c|b$.

Definición. Un entero no negativo d es el máximo común divisor de los enteros a y b, escribimos $d = mcd(a, b)$ o simplemente $d = (a, b)$, si

i) d es un divisor común de a y b; y

ii) si c es otro divisor común entonces $c|d$.

Algoritmo de Euclides para calcular el mcd

ENTRADA: dos números enteros a y b con $a \geq b$.

SALIDA: el mcd de a y b.

1. Mientras $b \neq 0$ hacer lo siguiente
   1.1. Poner $r \leftarrow a \, mod \, b$, $a \leftarrow b$, $b \leftarrow r$.
2. Devolver a.

Algoritmo de Euclides extendido

ENTRADA: dos números enteros a y b con $a \geq b$.

SALIDA: el mcd de a y b y enteros x, y satisfaciendo $ax+by = d$.

1. Si $b = 0$ entonces poner $d \leftarrow a$, $x \leftarrow 1$, $y \leftarrow 0$ y devolver (d, x, y).
2. Poner $x_2 \leftarrow 1$, $x_1 \leftarrow 0$ $y_2 \leftarrow 0$, $x_2 \leftarrow 1$
3. Mientras $b > 0$ hacer lo siguiente
   3.1. $q \leftarrow [a/b]$, $r \leftarrow a - qb$, $x \leftarrow x_2 - qx_1$, $y \leftarrow y_2 - qy_1$.
   3.2. $a \leftarrow b$, $b \leftarrow r$, $x_2 \leftarrow x_1$, $x_1 \leftarrow x$, $y_2 \leftarrow y_1$, $y_1 \leftarrow y$.
4. Poner $d \leftarrow a$, $x \leftarrow x_2$, $y \leftarrow y_2$, y devolver (d, x, y).