Números Enteros. Divisibilidad

Definición 1 *Sean $a, b \in \mathbb{Z}$. Se dice que a divide a b, y escribiremos $a|b$ si existe $k \in \mathbb{Z}$ tal que $b = a \cdot k$. En símbolos:*

$$a|b \Leftrightarrow \exists\, k \in \mathbb{Z}/b = a \cdot k$$

También diremos que a es un factor de b, que b es divisible por a o que b es múltiplo de a.

Observaciones:

1. Si a **no** divide a b escribiremos $a \nmid b$. Esto es,

$$a \nmid b \Leftrightarrow \forall k \in \mathbb{Z} : b \neq a \cdot k.$$

2. Si $a \in \mathbb{Z}, a \neq 0$, entonces a posee al menos los siguientes divisores:

$$1,\ -1,\ a,\ -a$$

   Estos divisores se llaman **divisores triviales** de a. A todo divisor distinto de los triviales, se lo llama **divisor propio** de a.

3. Los únicos enteros que admiten inverso multiplicativo son 1 y -1. Es decir, si $a \in \mathbb{Z}$, $a \neq 0$ y $a \cdot a^{-1} = 1$ entonces $a = 1$ o $a = -1$.

   Por lo tanto, si $k \cdot q = 1$ con $k, q \in \mathbb{Z}$ entonces $k = q = 1$ o $k = q = -1$, esto es, los únicos divisores de 1 son 1 y -1.

La relación divide verifica las siguientes propiedades.

Propiedad 1 *Para todo $a, b, c \in \mathbb{Z}$ se tiene que:*

1. *Reflexiva: $a|a$.*
2. *$a|0$.*
3. *$1|a$.*
4. *Transitiva: Si $a|b$ y $b|c$ entonces $a|c$.*
5. *Si $a|b$ y $a|c$ entonces $a|(bx + cy)$, cualesquiera sean $x, y \in \mathbb{Z}$.*
6. *Si $a|b$ entonces $a|-b$, $-a|b$ y $-a|-b$.*
7. *Si $a|b$ entonces $ac|bc$.*
8. *Si $a|b$ y $b|a$ entonces $|a| = |b|$.*

Probaremos las propiedades 1, 4, 5 y 8. El resto de las demostraciones se proponen como ejercicio.

Demostración 1: Como existe $1 \in \mathbb{Z}/a = a \cdot 1$ entonces $a|a$.

Demostración 4: Por hipótesis $a|b$ y $b|c$ entonces existen $k, t \in \mathbb{Z}$ tales que $b = ak$ y $c = bt$. Reemplazando tenemos:

$$c = bt = (ak)t = a(kt).$$

Luego existe $s = kt,\ s \in \mathbb{Z}$ tal que $c = as$, es decir, $a|c$.

Demostración 5: Por hipótesis $a|b$ y $a|c$ entonces existen enteros k y t tales que $b = ak$ y $c = at$.
Considerando que $x, y \in \mathbb{Z}$ tenemos que:

$$bx + cy = (ak)x + (at)y = a(kx) + a(ty) = a(kx + ty),$$

luego existe $s = kx + ty,\ s \in \mathbb{Z}$ tal que $bx + cy = a \cdot s$, es decir, $a|bx + cy$.

Demostración 8: Como $a|b$ y $b|a$ entonces existen $k, t \in \mathbb{Z}$ tales que $b = ak$ y $a = bt$.
Luego

$$b = ak = (bt)k = b(tk),$$

de lo que deducimos que $t \cdot k = 1$. Como k y t son números enteros, $k = t = 1$ o $k = t = -1$.
Si $k = t = 1$, tenemos que $a = b$ y en caso que $k = t = -1$, podemos asegurar que $a = -b$.
En consecuencia $a = b$ o $a = -b$, es decir, $|a| = |b|$.

Algoritmo de la División Entera.

Teorema 1 *Dados dos enteros a y b, con $b \neq 0$, existen enteros q y r, llamados respectivamente el cociente y el resto de dividir a a por b, unívocamente determinados tales que:*

$$a = b \cdot q + r \quad \text{con } 0 \leq r < |b|$$

Observaciones:

1. Si $b|a$ entonces existen $q, r \in \mathbb{Z}/a = b \cdot q + r$, con $r = 0$.
2. Si $b \nmid a$ entonces existen $q, r \in \mathbb{Z}/a = b \cdot q + r$, con $0 < r < |b|$.

Números Primos

Definición 2 *Un número entero "a" distinto de 0, 1 y -1, se dice* **primo** *si sus únicos divisores son los triviales, es decir, si los únicos divisores de "a" son:*

$$1,\ -1,\ a \text{ y } -a.$$

La defínción anterior es equivalente a decir que un entero diferente de 0, 1 y -1 es primo si tiene exactamente cuatro divisores.

A todo número entero distinto de 0, 1 y -1, que no sea primo, se le dice **compuesto**.

Teorema 2 *(Euclides) Existen infinitos números primos.*

El siguiente teorema nos proporciona un mecanismo simple para saber si un número es primo o no.

Teorema 3 *Sea $n \in \mathbb{Z},\ n > 1$. Si n no es primo entonces existe un primo p tal que $p|n$ y $p \leq \sqrt{n}$.*

Podemos ejemplificar este teorema tomando $n = 91$. Como la parte entera de $\sqrt{91}$ es 9, debemos considerar los enteros primos positivos menores o iguales a 9, es decir,

$$p \in \{2, 3, 5, 7\}$$

y controlar si $p|91$ para algún $p \in \{2, 3, 5, 7\}$. Sabemos que 7 divide a 91, de lo que deducimos que 91 no es primo.

Si consideramos $n = 97$, como a parte entera de $\sqrt{97}$ es 9 y

$$2 \nmid 97, \quad 3 \nmid 97, \quad 5 \nmid 97, \quad 7 \nmid 97$$

entonces podemos concluír que 97 es primo.

Propiedad 2 *Sea p un número primo. Si $p|ab$ entonces $p|a$ o $p|b$.*

Haremos la demostración de esta propiedad luego de la definición de máximo común divisor.

Esta propiedad **no** es cierta si p no es un número primo. Se propone como ejercicio buscar un contraejemplo que justifique la falsedad, en caso que p no sea un número primo.

Teorema Fundamental de la Aritmética.

Teorema 4 *Todo número entero a distinto de $0,\ 1$ y -1, es un número primo o bien se puede escribir como ± 1 por un producto de números primos positivos distintos dos a dos. Esta representación de un número entero como producto de primos es única, salvo el orden de los factores.*

Es decir, todo entero a distinto de $0,\ 1$ y -1 puede factorizarse del siguiente modo:

$$a = \pm p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s},$$

donde los primos positivos $p_1,\ p_2,\ p_3, \ldots,\ p_s$, son distintos dos a dos y las potencias $\alpha_i \in \mathbb{N}$ para $1 \leq i \leq s$.

El siguiente teorema nos proporciona una herramienta para hallar los divisores positivos de un número entero a dado. Sin pérdida de generalidad, podemos considerar $a > 1$ ya que los divisores de a y de $-a$ coinciden.

Teorema 5 *Sea $a > 1$ y sea $a = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_s^{e_s}$, donde los p_i son primos distintos dos a dos, y $e_i \in \mathbb{N}$, con $1 \leq i \leq s$. Sea $b \in \mathbb{Z}$, $b > 0$, entonces*

$$b|a \;\Leftrightarrow\; b = p_1^{t_1} \cdot p_2^{t_2} \cdot \ldots \cdot p_s^{t_s}, \quad 0 \leq t_i \leq e_i, \text{ para } 1 \leq i \leq s.$$

Hallados los divisores positivos de a, todos sus divisores se obtienen calculando los opuestos de los divisores positivos encontrados.

De forma inmediata al teorema anterior, podemos hallar la cantidad de divisores de un número entero dado.

Sea $a \in \mathbb{Z},\ a > 1,\ a = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_n^{e_n}$, llamaremos con $d(a)$ al **número de divisores positivos de** a. Luego

$$d(a) = (e_1 + 1) \cdot (e_2 + 1) \cdot \ldots \cdot (e_n + 1).$$

Máximo Común Divisor.

Sean $a, b \in \mathbb{Z}$ y supongamos que al menos uno de ellos es distinto de cero.

Sean $D(a) = \{c \in \mathbb{Z} :\ c|a\}$ y $D(a,b) = D(a) \cap D(b) = \{c \in \mathbb{Z} :\ c|a \ \wedge\ c|b\}$.

Observemos que $D(a) = D(-a)$, si $a \neq 0$ entonces $D(a)$ es un conjunto finito y si a y b no son simultáneamente nulos $D(a,b)$ es no vacío y finito.

El mayor de todos los elementos de $D(a,b)$ se denomina **máximo común divisor** de a y b y se nota (a,b).

Por ejemplo, si consideramos $a = 75$ y $b = -12$ entonces

$$D(a) = \{\pm 1,\ \pm 3,\ \pm 5,\ \pm 15,\ \pm 25,\ \pm 75\} \text{ y } D(b) = \{\pm 1,\ \pm 2,\ \pm 3,\ \pm 4,\ \pm 6,\ \pm 12\},$$

luego $D(a,b) = D(a) \cap D(b) = \{\pm 1,\ \pm 3\}$, de lo que deducimos que

$$(75, -12) = 3$$

Como consecuencia inmediata de la definición anterior resulta que (a,b) tiene las siguientes propiedades, cuyas demostraciones se dejan como ejercicio para el lector.

Propiedad 3 *Sean a y b enteros no simultáneamente nulos.*

1. $(a,b) > 0$.
2. $(a,b) = (b,a)$.
3. $(a,b) = (-a,b) = (a,-b) = (-a,-b)$.
4. *Si p es un entero primo entonces $p|a$ o $(a,p) = 1$.*

La definición de máximo común divisor puede no ser simple desde el punto de vista práctico. A continuación veremos un método que permite determinar el máximo común divisor a través de un algoritmo, llamado Algoritmo de Euclides.

La siguiente propiedad nos asegura que el desarrollo del algoritmo de Euclidez nos proporsiona el máximo común divisor entre dos enteros no simultáneamente nulos.

Propiedad 4 *Si a y b son enteros, $b \neq 0$ y r es el resto de dividir a "a" por "b", entonces $(a, b) = (b, r)$.*

Algoritmo de Euclides

Sean a y b dos enteros no simultáneamente nulos. Como $(a, b) = (a, -b)$ podemos suponer sin pérdida de generalidad, que a, b son enteros positivos. Consideremos las siguientes divisiones sucesivas:

$$\begin{array}{rcll} a & = & b \cdot q_1 + r_1, & \text{con } 0 < r_1 < b \\ b & = & r_1 \cdot q_2 + r_2, & \text{con } 0 < r_2 < r_1 \\ r_1 & = & r_2 \cdot q_3 + r_3, & \text{con } 0 < r_3 < r_2 \\ & \vdots & & \\ r_i & = & r_{i+1} \cdot q_{i+2} + r_{i+2}, & \text{con } 0 < r_i < r_{i-1}, \text{ donde } 2 \leq i \leq n-3 \\ & \vdots & & \\ r_{n-2} & = & r_{n-1} \cdot q_n + r_n, & \text{con } 0 < r_n < r_{n-1} \\ r_{n-1} & = & r_n \cdot q_{n+1}. & \end{array}$$

Como al cabo de un número finito de pasos obtenemos un resto nulo, aplicando la propiedad anterior podemos asegurar que

$$(a, b) = (b, r_1) = (r_1, r_2) = (r_2, r_3) = \ldots = (r_{n-2}, r_{n-1}) = (r_{n-1}, r_n) = r_n.$$

El algoritmo se puede esquematizar de la siguiente manera:

	q_1	q_2	q_3	$\cdots$	q_{n-1}	q_n	q_{n+1}
a	b	r_1	r_2	$\cdots$	r_{n-2}	r_{n-1}	r_n
r_1	r_2	r_3	r_4	$\cdots$	r_n	0	

Luego $(a, b) = r_n$, pues r_n es el último resto no nulo. Si el resto es cero en la primera división entonces a es múltiplo de b y $(a, b) = b$.

El siguiente teorema es una consecuencia importante del Algoritmo de Euclides:

Teorema 6 *Dados $a, b \in \mathbb{Z}, b \neq 0$, existen enteros x e y tales que $(a, b) = ax + by$.*

Observaciones

1. Si $t = ax + by$, con $x, y \in \mathbb{Z}$, **no necesariamente** t es el máximo común divisor entre a y b, es decir, t puede ser distinto a (a, b).

   Por ejemplo: sea $a = 6$ y $b = 4$, $8 = 0 \cdot 6 + 2 \cdot 4$ y sin embargo $8 \neq (6, 4)$, pues $(6, 4) = 2$.

2. Los enteros de la combinación lineal, x e y no son únicos.

   Por ejemplo: $(6,4) = 2 = 6 \cdot 1 + 4 \cdot (-1) = 6 \cdot (-1) + 4 \cdot 2 = 6 \cdot (-3) + 4 \cdot 5$.

3. Como $(a,b) = (a,-b) = (-a,b) = (-a,-b)$, para calcular el máximo común divisor entre dos enteros, podemos aplicar el algoritmo de Euclides, directamente a los números enteros positivos.

4. Si un número entero t es común divisor de a y de b, es decir $t|a$ y $t|b$, entonces t **no necesariamente** es (a,b). Podemos asegurar que t divide a (a,b). Es decir:

$$si\ t|a\ y\ t|b\ \ entonces\ \ t|(a,b)$$

Propiedad 5 *Sean $a,b,c \in \mathbb{Z}$, a y b no simultáneamente nulos. Entonces existen enteros x,y tales que $ax+by=c \Leftrightarrow (a,b)|c$.*

Corolario 1 *Existen $x,y \in \mathbb{Z}$ tales que $ax+by=1$ equivale a $(a,b)=1$.*

Definición 3 *Dados dos enteros a y b, no simultáneamente nulos, se dicen* **relativamente primos o coprimos**, *si $(a,b)=1$.*

Propiedad 6 *Sean $a,b,p \in \mathbb{Z}$. Si p es primo y $p|ab$ entonces $p|a$ o $p|b$.*

Demostración: Supongamos que p es un número primo tal que $p|ab$ y $p \nmid a$.
Como $p \nmid a$ por la propiedad anterior aseguramos que $(a,p)=1$, entonces

$$\exists\ x,y \in \mathbb{Z}/\ 1 = ax+py.$$

Como $p|ab$, existe $k \in \mathbb{Z}$ tal que $ab=pk$.
Luego $b=(ax+py)b = abx+pby = pkx+pby = p(kx+by)$, entonces existe $s=kx+by,\ s \in \mathbb{Z}$ tal que $b=ps$, es decir, $p|b$.

Propiedad 7 *(Euclides) Sean $a,b,c \in \mathbb{Z}$. Si $a|bc$ y $(a,b)=1$ entonces $a|c$.*

Demostración: Por hipótesis $a|bc$ y $(a,b)=1$ entonces existen $k,t,r \in \mathbb{Z}$ tal que $bc=ka$ y $1=ta+rb$, de lo que deducimos $bc=ka$ y $c=(ta+rb)c=tac+rbc$. Reemplazando tenemos

$$c = tac+rka = (tc+rk)a.$$

Luego existe $s=tc+rk,\ s\mathbb{Z}$ tal que $c=sa$, es decir, $a|c$.

Propiedad 8 *Sean $a, b, n \in \mathbb{Z}$. Si $a|n$, $b|n$ y $(a, b) = 1$ entonces $ab|n$.*

Demostración: Por hipótesis $(a, b) = 1$ lo que equivale a que existen $k, t \in \mathbb{Z}$ tal que $1 = ka+tb$, luego $n = (ka + tb)n = kan + tbn \quad (1)$.
Como $a|n$ y $b|n$ entonces existen $r, s\mathbb{Z}$ tales que $n = ra$ y $n = sb$, reemplazando en (1) tenemos:

$$n = kan + tbn = ka(sb) + tb(ra) = ks(ab) + tr(ab) = (ks + tr)ab.$$

De lo que deducimos que existe $u = ks + tr,\ u \in \mathbb{Z}$ tal que $n = u(ab)$, es decir, $ab|n$.

Observación Esta proposición **no es cierta** si a y b **no son coprimos**, es decir, si $(a, b) \neq 1$.

Por ejemplo: si $a = 2$, $b = 6$ y $n = 6$, a y b no son coprimos pues $(2, 6) = 2$.

$$2|6 \text{ y } 6|6 \quad \textit{pero} \quad 2.6 \nmid 6$$

Mínimo Común Múltiplo.

Dado un número entero a, sea $M(a) = \{c \in \mathbb{N} \cup \{0\} :\ a|c\}$, es decir, $M(a)$ es el conjunto de los múltiplos no negativos de a.

Observemos que $M(0) = \{0\},\ M(1) = \mathbb{N} \cup \{0\}$ y $M(a) \neq \emptyset$, cualquiera sea $a \in \mathbb{Z}$.

Si a y b son dos enteros cualesquiera, $M(a, b) = M(a) \cap M(b)$ es el conjunto de los múltipos no negativos de a y b. Como $M(a, b) \neq \emptyset$ y $M(a, b) \subseteq \mathbb{N} \cup \{0\}$, al menor elemento del conjunto $M(a, b)$ se lo denomina **mínimo común múltiplo** entre a y b y se nota $[a, b]$.

La siguiente propiedad nos proporsiona una forma de calcular el mínimo común múltiplo de dos enteros no simultáneamente nulos, utilizando el máximo común divisor entre ellos.

Propiedad 9 *Sean a y b dos enteros no simultáneamente nulos, entonces*

$$[a, b] = \frac{|a \cdot b|}{(a, b)}.$$

La siguiente proposición establece un método para calcular el máximo común divisor y el mínimo común múltiplo entre dos números enteros a partir de sus descomposiciones en factores primos.

Propiedad 10 *Si $a = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_s^{e_s}$ y $b = p_1^{t_1} \cdot p_2^{t_2} \cdot \ldots \cdot p_s^{t_s}$, con $e_i \geq 0,\ t_i \geq 0$ para $1 \leq i \leq s$, entonces*

$$(a, b) = p_1^{m_1} \cdot p_2^{m_2} \cdot \ldots \cdot p_s^{m_s} \quad \text{y} \quad [a, b] = p_1^{M_1} \cdot p_2^{M_2} \cdot \ldots \cdot p_s^{M_s}.$$

donde m_i es el menor de los números e_i y t_i, y M_i es el mayor de los números e_i y t_i, para $1 \leq i \leq s$.