# DIVISIBILIDAD: Resultados

F. Bellot Rosado

Se enumeran a continuación, como referencia, ciertos resultados sobre divisibilidad.

**1.1 Definición.** Dados los enteros $a$ y $b$, se dice que $a$ ***divide a*** $b$ (Notación: $a \mid b$) si existe un entero $q$ tal que $aq = b$.

Si $a$ no divide a $b$, entonces existen enteros $q, r$ tales que

$$b = aq + r, \quad \text{con } 0 \leq r < a, \qquad \text{q y r únicos.}$$

1.2 Todo número es divisor de sí mismo ; 1 es divisor de cualquier número ; 0 es divisible por cualquier número.

1.3 Todo número compuesto tiene al menos un divisor primo ( en efecto, si N es compuesto, tiene un divisor n, distinto de N y de 1, *que no es mayor que cualquier otro divisor.* Este divisor debe ser primo, porque de lo contrario, tendría un divisor menor que él mismo y mayor que 1 que también sería divisor de N, y esto es imposible por la manera como se ha elegido n ).

1.4 La sucesión de números primos es ilimitada (Primer teorema de Euclides)

En efecto, dado cualquier número primo $p$, construímos el número siguiente, multiplicando todos los números primos hasta $p$, inclusive, y sumando 1 al producto:

$$N = 2 \cdot 3 \cdot 5 \cdot 7 \cdot \cdots \cdot p + 1$$

Este número, o bien es primo, en cuyo caso hemos terminado, o en caso contrario admite un divisor primo, que es mayor que $p$ porque $N$ da resto 1 al ser dividido por todos los números primos 2,3,$\cdots$ , $p$.

1.5 La descomposición de un número en producto de potencias de factores primos es única.

1.6 (Segundo teorema de Euclides) Si un número divide a un producto de dos factores y es primo con uno de ellos, entonces divide al otro factor.

## 1.7 Propiedades del máximo común divisor y del mínimo común múltiplo :

Notación : m.c.d., (a,b) ; m.c.m., $[a, b]$.

$$
\begin{array}{cc}
(a,a) = a & [a,a] = a \\
(a,b) = (b,a) & [a,b] = [b,a] \\
(a,(b,c)) = ((a,b),c) & [a,[b,c]] = [[a,b],c] \\
[(a,b),a] = a & ([a,b],a) = a \\
k \cdot (a,b) = (ka,kb) & k \cdot [a,b] = [ka,kb] \\
[(a,b),c] = ([a,c],[a,c]) & ([a,b],c) = [(a,b),(a,c)]
\end{array}
$$

El producto de dos números es igual al de su m.c.d. por su m.c.m.

$$ab = (a,b) \cdot [a,b]$$

Si se dividen dos números por su m.c.d., los cocientes obtenidos son primos entre sí.

Todo divisor de 2 ó varios números es divisor de su m.c.d.

Todo múltiplo de 2 ó varios números lo es de su m.c.m.

Para todo entero $x$, $(a,b) = (a, b + ax)$

Si $(a,m) = (b,m) = 1$, entonces $(ab,m) = 1$.

Para todos $a, k$ enteros no simultáneamente nulos, $(a, a+k) \mid k$.

## Algoritmo de Euclides para calcular el m.c.d. de dos números.

Sean $a > b$ los enteros cuyo m.c.d. se desea determinar. Entonces

$$\begin{aligned} a &= bq_1 + r_1\ ; b > r_1 \\ b &= r_1 q_2 + r_2;\ \ r_1 > r_2 \\ r_1 &= r_2 q_3 + r_3;\ \ r_2 > r_3 \\ &\ldots \end{aligned}$$

La sucesión decreciente de enteros positivos

$$b > r_1 > r_2 > r_3 > \cdots \geq 0$$

tiene que ser finita; aparecerá un resto igual a 0; entonces si $r_{n+1} = 0$ el proceso termina con

$$r_{n-2} = r_{n-1} q_n + r_n\ \ ;\ \ r_{n-1} = r_n q_{n+1}.$$

y el máximo común divisor de a y b es $r_n$(el último resto distinto de cero); cuando $r_n = 1$, a y b son primos entre sí.

## 1.8 Teorema de Bézout

Si $a$ y $b$ son primos entre sí, existen enteros $x, y$ tales que

$$ax + by = 1$$

(Basta sustituir hacia atrás en las igualdades que dan el algoritmo de Euclides)

**Una observación menos obvia de lo que parece:** Dos números enteros consecutivos son primos entre sí.

## 1.9. **La función** *parte entera*

Si $x \in \mathbb{R}$ , la *parte entera de x* $(Notaciones : [x], \lfloor x \rfloor, E(x))$ es el mayor entero que es menor o igual que $x$.

Si $x, y$ son enteros, con $x = qy + r, 0 \leq r < y$, entonces $[x/y] = q$.

**Propiedades de la parte entera :**

i) Para $x \in \mathbb{R}$ , son equivalentes :

$$\begin{aligned} [x] &\leq x \leq [x] + 1 \\ x - 1 &< [x] \leq x \\ 0 &\leq x - [x] < 1 \\ -x - 1 &< [-x] \leq -x \end{aligned}$$

ii) Si $m$ es entero, $[x + m] = [x] + m$

iii) Se verifican las relaciones

$$\begin{aligned} [x]+[y] &\leq [x+y] \leq [x]+[y]+1 \\ [x-y] &\leq [x]-[y] \leq [x-y]+1 \end{aligned}$$

iv) Si $m$ es natural y $x \in \mathbb{R}$ , entonces

$$\left[\frac{[x]}{m}\right] = \left[\frac{x}{m}\right].$$

En efecto, sean $x = n + a, 0 \leq a < 1; n = qm + r, 0 \leq r \leq m - 1$

Entonces se tiene : por un lado, $[x/m] = [(qm + r + a)/m] = q + [(r + a)/m] = q$ porque $0 \leq r + a < m$.

Por otra parte,

$$\left[\frac{[x]}{m}\right] = \left[\frac{n}{m}\right] = \left[q + \frac{r}{m}\right] = q \text{ pues } r < m.$$

v) $[x] \cdot [y] \leq [xy]$

vi) $\left[x + \frac{1}{2}\right]$ es el entero más próximo a $x$. Si dos enteros son igualmente próximos a $x$, se conviene en que es el mayor de los dos.

vii) $x - [x]$ es la *parte decimal o mantisa de x. Notación :* $\{x\}$

viii) Si $n_1, n_2, n_3, \cdots$ (en número finito) son enteros cualesquiera cuya suma es $s$ y $a$ es cualquier número entero, entonces

$$\left[\frac{s}{a}\right] \geq \left[\frac{n_1}{a}\right] + \left[\frac{n_2}{a}\right] + \cdots \text{ (la suma es finita)}$$

ix) **Máxima potencia de un primo que divide a un factorial**

Si $p$ es un número primo, y $p^k$ es la mayor potencia de $p$ que divide a $n!$, entonces el valor del exponente $k$ se puede calcular mediante

$$k = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \cdots$$

En efecto : la suma es finita porque alguna potencia de $p$ es mayor que $n$ y a partir de ese momento los términos de la suma son 0; y además, de los números $1, 2, \cdots, n$, hay $[n/p]$ que son divisibles por $p$, hay $[n/p^2]$ que son divisibles por $p^2$, y así sucesivamente.

La propiedad iv) acorta el trabajo para calcular el mayor exponente de un primo $p$ en $n!$ :

$[400/5] = 80, [80/5] = 16, [16/5] = 3$ ; $80 + 16 + 3 = 99$ ceros en que termina $400!$

x) Si $n, k, r$ son enteros positivos, con $r \leq k-1$, entonces

$\left[\frac{n}{k}\right]$ es el número de múltiplos positivos de k que son menores o iguales que n

$\left[\frac{n+r}{k}\right]$ es el número de enteros positivos, menores o iguales que n, que dan resto $k-r$ al ser divididos por $k$

Ejemplo, $[41/10]=4$, número de enteros menores o iguales que 37 que dan resto 6 al ser divididos por 10.

Ir a la sección de Problemas

Ir a la sección de Soluciones