

➤ [Para volver a Menú](#)

DIVISIBILIDAD

DIVISIBILIDAD EN $(\mathbb{N}, +, \cdot, <)$

Frente a la imposibilidad de realizar la división exacta en todos los casos dentro de la estructura de los naturales definiremos la división entera que seguramente como todos sospechamos una buena definición puede ser:

$$\left. \begin{array}{l} a \\ r \end{array} \right\} \begin{array}{l} b \\ q \end{array} \left\} \Leftrightarrow \begin{cases} a = bq + r \\ r < b \end{cases}$$

Si somos rigurosos previamente a esta definición debemos discutir en que condiciones existen q y r , y cuando ello ocurre cuantos “ q ” y cuantos “ r ” hay.

Teorema

$$\mathbf{H)} \left\{ \begin{array}{l} a \in \mathbb{N}, b \in \mathbb{N} \\ b \neq 0 \end{array} \right. \quad \mathbf{T)} \left\{ \begin{array}{l} 1) \exists q, r \in \mathbb{N} / a = bq + r \quad y \quad r < b \\ 2) q \text{ y } r \text{ son uni cos} \end{array} \right.$$

Dem:

Consideramos $H = \{x \in \mathbb{N} / bx \leq a\}$. Intentaremos demostrar que H tiene máximo y que este es el “ q ” de la tesis. Para ello utilizaremos el principio de buena ordenación.

i) $H \subseteq \mathbb{N}$ por la propia definición de H .

ii) $H \neq \emptyset$ pues: $0 \cdot b = 0 \leq a \Rightarrow 0 \in H$

iii) H acotado superiormente. Efectivamente cualquier natural mayor o igual que $\frac{a}{b}$ es cota superior de H .

De i) ii) y iii) utilizando buena ordenación o más precisamente su consecuencia inmediata podemos afirmar que existe el máximo de H al que denominamos “alevosamente” q .

$$\left. \begin{array}{l} q \in H \Rightarrow bq \leq a \\ \text{como } a, bq \in \mathbb{N} \end{array} \right\} \Rightarrow a - bq \in \mathbb{N} \quad \text{Llamando } r = a - bq \text{ tenemos que } a = bq + r.$$

Nos falta demostrar que $r < b$. Hagámoslo.

$$\left. \begin{array}{l} q = \max H \Rightarrow q + 1 \notin H \\ \text{como } q + 1 \in \mathbb{N} \end{array} \right\} \Rightarrow b(q + 1) > a \Rightarrow bq + b > a = bq + r \Rightarrow b > r$$

Probemos ahora la unicidad.

Suponemos que existen $q' \text{ y } r' \in \mathbb{N} / a = bq' + r' \quad y \quad r' < b$

Si $q \neq q'$; por ejemplo $q > q' \Rightarrow q - q' > 0 \Rightarrow q - q' \geq 1$ (pues estamos con naturales) $\Rightarrow b(q - q') \geq b$ (recordemos que $b > 0$ por ser un natural no nulo).

Por otra parte $\left. \begin{array}{l} a = bq + r \\ a = bq' + r' \end{array} \right\} \Rightarrow b(q - q') + r - r' = 0 \Rightarrow r' = b(q - q') + r \geq b(q - q') \geq b \Rightarrow r' \geq b$

Lo cual contradice la suposición, Por lo tanto $q = q'$.

Si $q = q' \Rightarrow \left\{ \begin{array}{l} a = bq + r \\ a = bq + r' \end{array} \right\} \Rightarrow bq + r = bq + r' \Rightarrow r = r'$

Por lo tanto q y r son únicos.

Definición

Dados a y b naturales, $b \neq 0$ realizar la **división entera** de a entre b es encontrar q y r naturales tales que:

- i) $a = bq + r$
- ii) $r < b$

Lo cual representamos esquemáticamente $\begin{array}{r} a \\ b \end{array} \begin{array}{r} b \\ r \end{array} \begin{array}{r} q \\ q \end{array}$

En caso de que $r=0$ decimos que b **divide** a a o que a es **múltiplo** de b

Anotamos b/a ó $a = b \cdot$

Podemos independizar la definición de divisor o de múltiplo de la definición de división entera.

$$b/a \Leftrightarrow \exists q \in \mathbb{N} \text{ tal que } a = bq$$

Ejercicios:

1) Consideramos $R: \mathbb{N}^* \rightarrow \mathbb{N}^*$; $xRy \Leftrightarrow x / y$.

Probar que R es una relación de orden amplio (una relación que cumple idéntica, antisimétrica y transitiva)

2) Probar: $\left. \begin{array}{l} x / a \\ x / b \end{array} \right\} \Rightarrow x / a \pm b$ (Si un número divide a otros dos divide a su suma y a su resta)

3) Idem. $\left. \begin{array}{l} x / a \\ c \in \mathbb{N} \end{array} \right\} \Rightarrow x / ac$ (Si un número divide a a divide a todos sus múltiplos)

4) Idem. $\left. \begin{array}{l} x / a \wedge x / b \\ \lambda, \mu \in \mathbb{N} \end{array} \right\} \Rightarrow x / \lambda a + \mu b$ (Si un número divide a otros dos divide a cualquier combinación lineal)

5) Probar: $\left. \begin{array}{l} x / a \wedge x / b \\ a \quad b \\ r \quad q \end{array} \right\} \Rightarrow x / r$

6) Probar: $\left. \begin{array}{l} x / y \\ y \neq 0 \end{array} \right\} \Rightarrow x \leq y$ (Los divisores de un natural no nulo son menores o iguales que el natural dado)

Ejercicios:

1) Completar de todas las formas posibles:

$$\begin{array}{llll} \text{i) } \begin{array}{l} 9 \\ 13 \end{array} & \text{ii) } \begin{array}{l} a \\ 35 \end{array} & \begin{array}{l} a < 200 \\ 4 \end{array} & \text{iii) } \begin{array}{l} 60 \\ 12 \end{array} & \text{iv) } \begin{array}{l} a \\ q \end{array} & \begin{array}{l} 17 \\ q \end{array} & \begin{array}{l} a > 200 \\ \end{array} \end{array}$$

2) Hallar a natural sabiendo que: $\begin{array}{l} a \\ q^2 \end{array} \begin{array}{l} 37 \\ q \end{array}$

3) Hallar todas las posibles ternas de naturales (a,b,c) tales que:

$$\begin{array}{ll} a & b \\ 12 & c \end{array} \quad \begin{array}{ll} a+7 & 15 \\ b & c \end{array}$$

Nota

Siendo a un número natural anotamos $d(a)$ al conjunto de todos sus divisores

$$d(a) = \{x \in \mathbb{N}; x / a\}$$

Así por ejemplo: $d(6) = \{1,2,3,6\}$ $d(0) = \mathbb{N}^*$

Definiremos al máximo común divisor de dos naturales a y b como el máximo de los divisores comunes; o sea como el máximo del conjunto $d(a) \cap d(b)$. Para dar esta definición probemos previamente que dicho máximo existe.

Teorema

$$\left. \begin{array}{l} a \in \mathbb{N}, b \in \mathbb{N} \\ a^2 + b^2 \neq 0 \end{array} \right\} \Rightarrow \exists \max d(a) \cap d(b)$$

Dem: Observemos que $d(a) \cap d(b)$ es un conjunto de naturales; es pues razonable pensar en utilizar el principio buena ordenación. Para ello debemos probar:

i) $d(a) \cap d(b) \subseteq \mathbb{N}$ Lo cual es inmediato pues por definición $d(a) \subseteq \mathbb{N}$ y $d(b) \subseteq \mathbb{N}$

ii) $d(a) \cap d(b) \neq \emptyset$ $1 \in d(a) \wedge 1 \in d(b) \Rightarrow 1 \in d(a) \cap d(b)$

iii) $d(a) \cap d(b)$ acotado superiormente. Como por hipótesis a y b no son simultaneamente nulos, supongamos por ej que $a \neq 0$
 $\forall x \in d(a) \cap d(b) \Rightarrow x \in d(a) \Rightarrow x / a$, como $a \neq 0 \Rightarrow$
 $\Rightarrow x \leq a \Rightarrow a$ es cota superior de $d(a) \cap d(b)$

De i) ii) y iii) aplicando el principio de buena ordenación estamos en condiciones de afirmar que $\exists \max d(a) \cap d(b)$.

Definición

Dados dos naturales a y b no simultáneamente nulos. Llamamos **máximo común divisor** de a y b al $\text{máx } d(a) \cap d(b)$.

Anotamos $D(a,b)$; así por ejemplo $D(10,25)=5$ $D(0,b)=b$ si $b \neq 0$

Teorema

$$\left. \begin{array}{l} a \quad b \\ r \quad q \end{array} \right\} \Rightarrow d(a) \cap d(b) = d(b) \cap d(r)$$

Dem. Debemos probar que: i) $\forall x \in d(a) \cap d(b) \Rightarrow x \in d(b) \cap d(r)$

ii) $\forall x \in d(b) \cap d(r) \Rightarrow x \in d(a) \cap d(b)$

$$i) \forall x \in d(a) \cap d(b) \Rightarrow \left\{ \begin{array}{l} x \in d(a) \Rightarrow x / a \\ \wedge \\ x \in d(b) \Rightarrow x / b \Rightarrow x / bq \end{array} \right\} \Rightarrow x / a - bq = r \Rightarrow x \in d(r) \quad \text{como } x \in d(b) \Rightarrow$$

$$\Rightarrow x \in d(b) \cap d(r)$$

$$ii) \forall x \in d(b) \cap d(r) \Rightarrow \left\{ \begin{array}{l} x \in d(b) \Rightarrow x / b \Rightarrow x / bq \\ x \in d(r) \Rightarrow x / r \end{array} \right\} \Rightarrow x / bq + r = a \Rightarrow x \in d(a) \Rightarrow x \in d(a) \cap d(b)$$

COROLARIO

$$\left. \begin{array}{l} a \quad b \\ r \quad q \end{array} \right\} \Rightarrow D(a, b) = D(b, r)$$

La demostración es una consecuencia inmediata del teorema anterior.

Obs. $\begin{array}{l} 144 \quad 50 \\ 44 \quad 2 \end{array}$ entonces $D(144,50)=D(50,44)$

$\begin{array}{l} 50 \quad 44 \\ 6 \quad 1 \end{array}$ entonces $D(50,44)=D(44,6)$

$\begin{array}{l} 44 \quad 6 \\ 2 \quad 7 \end{array}$ entonces $D(44,6)=D(6,2)$

$\begin{array}{l} 6 \quad 2 \\ 0 \quad 3 \end{array}$ entonces $D(6,2)=D(2,0)=2$

Por lo tanto $D(144,50)=2$. La aplicación sucesiva del último corolario nos permitió calcular el máximo común divisor de 144 y 50; intentemos generalizar este procedimiento.

Algoritmo de Euclides

Consideramos $a, b \in \mathbb{N}$ $a > b > 0$. Para hallar $D(a,b)$ realizamos la división

$$\left. \begin{array}{l} a \quad b \\ r_1 \quad q_1 \end{array} \right\} \Rightarrow D(a, b) = D(b, r_1)$$

Si $r_1 = 0 \Rightarrow D(a, b) = D(b, 0) = b$

Si $r_1 \neq 0$ realizamos la division $\begin{array}{l} b \quad r_1 \\ r_2 \quad q_2 \end{array} \Rightarrow D(b, r_1) = D(r_1, r_2)$

Si $r_2 = 0 \Rightarrow D(a, b) = D(b, r_1) = D(r_1, 0) = r_1$

Si $r_2 \neq 0$ realizamos la division $\begin{array}{l} r_1 \quad r_2 \\ r_3 \quad q_3 \end{array} \Rightarrow D(r_1, r_2) = D(r_2, r_3)$

Si $r_3 = 0 \Rightarrow D(a, b) = D(b, r_1) = D(r_1, r_2) = D(r_2, 0) = r_2$

Si $r_3 \neq 0$

El proceso continua hasta encontrar un resto nulo. ¿No existirá algún caso en donde esto no ocurre? (o sea que el proceso sea infinito).

Aparentemente no pues: $b > r_1 > r_2 > r_3 > \dots$ Probémoslo mas rigurosamente. Consideramos

H el conjunto de los restos obtenidos mediante este proceso de divisiones sucesivas; demostremos que H tiene mínimo y que este es 0.

$$\left. \begin{array}{l} H \subseteq \mathbb{N} \\ H \neq \emptyset \quad (r_i \in H) \end{array} \right\} \Rightarrow \exists r_n = \text{mín } H$$

SI $r_n \neq 0$ realizamos la division $\begin{array}{l} r_{n-1} \quad r_n \\ r_{n+1} \quad q_{n+1} \end{array} \Rightarrow r_{n+1} \in H$ y $r_{n+1} < r_n = \text{min}H$ Absurdo

Por lo tanto $r_n = 0$ y en consecuencia este mecanismo de divisiones sucesivas nos conduce en todos los casos a un resto nulo siendo el último resto no nulo (r_{n-1}) el máximo común divisor buscado.

Suele utilizarse el siguiente esquema:

$$\begin{array}{cccccccc} & q_1 & q_2 & q_3 & \dots & q_n & & \\ a & b & r_1 & r_2 & \dots & r_{n-2} & r_{n-1} & D(a,b)=r_{n-1} \\ r_1 & r_2 & r_3 & \dots & & & & 0 \end{array}$$

Así por ejemplo para calcular $D(144,100)$

	1	2	3	1	2
144	100	44	12	8	4
44	12	8	4	0	

Entonces $D(144,100)=4$

Nota

Si en el algoritmo anterior utilizamos sucesivamente el teorema en lugar del corolario tenemos: $d(a) \cap d(b) = d(b) \cap d(r_1) = d(r_1) \cap d(r_2) = \dots = d(r_{n-1}) \cap d(0) = d(r_{n-1})$ como $r_{n-1} = D(a, b) \Rightarrow d(a) \cap d(b) = d(D(a, b))$ El conjunto de los divisores comunes a a y b es el conjunto de los divisores de su máximo común divisor.

En otras palabras:
$$\left. \begin{matrix} x / a \\ x / b \end{matrix} \right\} \Leftrightarrow x / D(a, b)$$

Teorema

$$D(a, b) = D \Leftrightarrow \begin{cases} \text{i) } D / a \wedge D / b \\ \text{ii) Si } x / a \wedge x / b \Rightarrow x / D \end{cases}$$

Dem (\Rightarrow) Partimos de la hipótesis que $D = D(a, b) = \text{máx } d(a) \cap d(b) \Rightarrow D \in d(a) \cap d(b) \Rightarrow$

$$\Rightarrow \begin{cases} D \in d(a) \Rightarrow D / a \\ D \in d(b) \Rightarrow D / b \end{cases} \quad \text{Quedaría por demostrar la condición ii); pero ello ya fué probado}$$

en la nota inmediata anterior.

(\Leftarrow) Ahora debemos demostrar que $D = \text{máx } d(a) \cap d(b) \Leftrightarrow \begin{cases} \text{i) } D \in d(a) \cap d(b) \\ \text{ii) } D \geq x \quad \forall x \in d(a) \cap d(b) \end{cases}$

i) Por hipótesis $\left. \begin{matrix} D / a \Rightarrow D \in d(a) \\ D / b \Rightarrow D \in d(b) \end{matrix} \right\} \Rightarrow D \in d(a) \cap d(b)$

ii) $\left. \begin{matrix} \forall x \in d(a) \cap d(b) \Rightarrow x / a \wedge x / b \quad \text{entonces por hipótesis } x / D \\ \text{como } D \neq 0 \end{matrix} \right\} \Rightarrow x \leq D$

De i) y ii) deducimos que $D = \text{máx } d(a) \cap d(b) = D(a, b)$

Nota: El teorema recién demostrado nos brinda una condición necesaria y suficiente para que D sea máximo común divisor de a y b . D como tal podría sustituir a la definición dada de máximo común divisor. Es mas algunos autores toman la proposición del teorema inmediato anterior como definición; no necesitando de esta manera el “ \Leftarrow ”

.Por este motivo entre otros es la opción que se toma en Z y en polinomios.

Veamos ahora algunas otras propiedades del máximo común divisor.

Lema
$$\left. \begin{matrix} a & b \\ r & q \\ x \in N^* \end{matrix} \right\} \Rightarrow \begin{cases} ax & bx \\ rx & q \end{cases}$$

Dem:

$$\left. \begin{matrix} a & b \\ r & q \end{matrix} \right\} \Rightarrow \begin{cases} a = bq + r \Rightarrow ax = bxq + rx \\ r < b; \text{ como } x > 0 \Rightarrow rx < bx \end{cases} \quad \text{Entonces } ax \text{ dividido } bx \text{ da cociente } q \text{ y resto } rx.$$

Teorema

$$\left. \begin{matrix} D(a, b) = D \\ x \in \mathbb{N}^* \end{matrix} \right\} \Rightarrow D(ax, bx) = Dx$$

Dem

$$\begin{array}{ccc} q_1 & q_2 & \dots\dots\dots q_{n+1} \\ a & b & r_1 \dots\dots\dots r_{n-1} \quad r_n \end{array} \quad \text{Entonces} \quad \begin{array}{ccc} q_1 & q_2 & \dots\dots\dots q_{n+1} \\ ax & bx & r_1x \dots\dots\dots r_{n-1}x \quad r_nx \\ r_1 & r_2 & \dots\dots\dots 0 \\ r_1x & r_2x & \dots\dots\dots 0 \end{array}$$

Por lo tanto $D(ax, bx) = r_n x = D(a, b)x$

Corolario

$$\left. \begin{matrix} x/a \wedge x/b \\ D(a, b) = D \end{matrix} \right\} \Rightarrow D\left(\frac{a}{x}, \frac{b}{x}\right) = \frac{D}{x}$$

Dem: $D\left(\frac{a}{x}, \frac{b}{x}\right) = D' \Rightarrow D\left(\frac{a}{x}x, \frac{b}{x}x\right) = D'x \Rightarrow D(a, b) = D'x \Rightarrow D = D'x \Rightarrow D' = \frac{D}{x}$

Definición

Consideramos a y b dos números naturales.
Decimos que a y b son **primos entre sí** $\Leftrightarrow D(a, b) = 1$

Obs: a y b son primos entre sí \Leftrightarrow el 1 es su único divisor común

Teorema

$$D(a, b) = D \Leftrightarrow \begin{cases} a = Da' \\ b = Db' \\ D(a', b') = 1 \end{cases}$$

Dem: $(\Rightarrow) \quad D(a, b) = D \Rightarrow D/a \wedge D/b \Rightarrow \begin{cases} a = Da' \\ b = Db' \end{cases} \Rightarrow \text{MCD}(Da', Db') = D \Rightarrow \text{MCD}(a', b') = 1$

$(\Leftarrow) \quad D(a', b') = 1 \Rightarrow D(Da', Db') = 1D \Rightarrow D(a, b) = D$

Nota: Este último teorema nos permite muchas veces acortar sensiblemente los “tanteos”; veamos un ejemplo.

Hallar dos naturales a y b sabiendo que $ab=9900$ y $D(a,b)=30$

$D(a, b) = 30 \Rightarrow \begin{cases} a = 30a' \\ b = 30b' \end{cases}$ Sustituyendo tenemos : $30a'30b' = 9900 \Rightarrow a'b' = 11$

obsérvese que es mucho más cómodo tantear dos números cuyo producto sea 11 y sean primos entre sí ; que dos números cuyo producto sea 9900 y su máximo común divisor 30.

a'	b'	a=30a	b=30b
1	11	30	330
11	1	330	30

Nota: Yendo a otra situación. Sabemos que si un número divide a otro divide a cualquiera de sus múltiplos; si c/b entonces c/ab . ¿Es cierto el recíproco? ¿Si un número divide a un producto divide necesariamente a uno de los factores?

Teorema de Euclides

$$\left. \begin{array}{l} c / ab \\ D(a, c) = 1 \end{array} \right\} \Rightarrow c / b$$

Dem: $D(a, c) = 1 \Rightarrow D(ab, cb) = b$

$$\left. \begin{array}{l} c / ab \text{ por hipótesis} \\ c / cb \text{ por definición} \end{array} \right\} \Rightarrow c / D(ab, cb) \Rightarrow c / b$$

Teorema

$$\left. \begin{array}{l} c / a_1 a_2 \dots a_{n-1} a_n \\ D(c, a_1) = D(c, a_2) = \dots = D(c, a_{n-1}) = 1 \end{array} \right\} \Rightarrow c / a_n$$

Puede demostrarse por inducción completa; a cargo del lector.

Mínimo común múltiplo

Siendo $a \in \mathbb{N}^*$ anotamos $m(a)$ al conjunto de sus múltiplos no nulos; más precisamente:

$$m(a) = \{na ; n \in \mathbb{N}^*\}$$

Parecería razonable definir mínimo común múltiplo de a y b como el $\min m(a) \cap m(b)$. Para ello tenemos que demostrar previamente que dicho mínimo existe.

Teorema

$$a, b \in \mathbb{N}^* \Rightarrow \exists \min m(a) \cap m(b)$$

Dem

- i) $m(a) \cap m(b) \subseteq \mathbb{N}$ por definición
 ii) $m(a) \cap m(b) \neq \emptyset$ pues $ab \in m(a) \cap m(b)$ Entonces por P.B.O. $\exists \min m(a) \cap m(b)$

Definición

$a, b \in \mathbb{N}^*$. Llamamos **mínimo común múltiplo de a y b** (anotamos $m(a, b)$)

$$m(a, b) = \min m(a) \cap m(b)$$

Veremos a continuación un teorema que nos vincula el mínimo común múltiplo con el máximo comun divisor.

Teorema

$$m(a,b).D(a,b)=ab \quad \text{con } a, b \in \mathbb{N}^*$$

Dem: Intentaremos escribir $m(a) \cap m(b)$ de forma que pueda hallarse su mínimo; para ello buscamos una condición necesaria y suficiente para que $x \in m(a) \cap m(b)$.

$$\text{Si } x \in m(a) \cap m(b) \Rightarrow \left\{ \begin{array}{l} x \in m(a) \Rightarrow \exists k \in \mathbb{N}^*; x = ka \\ x \in m(b) \Rightarrow \exists h \in \mathbb{N}^*; x = hb \end{array} \right\} \Rightarrow ka = hb$$

$$\text{Por otra parte si } D(a,b)=D \Rightarrow \left\{ \begin{array}{l} a = Da' \\ b = Db' \\ \text{con } D(a', b') = 1 \end{array} \right. \quad \text{Sustituyendo tenemos}$$

$$kDa' = hDb' \Rightarrow ka' = hb' \quad \text{entonces } a' / hb' \quad \text{como } D(a', b') = 1 \quad \text{por Euclides } a' / h \Rightarrow \exists t \in \mathbb{N}^*; h = ta'$$

$$\text{Además } x=hb \Rightarrow x = ta'b \quad \text{como } b = Db' \Rightarrow x = ta'b'D$$

Probamos entonces que: $\forall x \in m(a) \cap m(b) \Rightarrow x = ta'b'D$. Demostremos ahora que también es cierto el recíproco.

$$\forall x \in \mathbb{N}; x = ta'b'D \Rightarrow \left\{ \begin{array}{l} x = ta'b \Rightarrow x \in m(b) \\ x = tab' \Rightarrow x \in m(a) \end{array} \right\} \Rightarrow x \in m(a) \cap m(b)$$

Por lo tanto: $\forall x \in \mathbb{N}^*$ tal que $x = ta'b'D \Rightarrow x \in m(a) \cap m(b)$

De ambas proposiciones subrayadas podemos afirmar que:

$$m(a) \cap m(b) = \{x \in \mathbb{N}; x = ta'b'D; t \in \mathbb{N}^*\}$$

El mínimo del conjunto se da para $t=1$ Entonces: $m(a, b) = a'b'D$ con $D=D(a, b)$ multiplicando ambos miembros por D tenemos

$$m(a,b)D(a,b)=ab$$

Ejercicios Probar: 1) $D(a, b) = 1 \Rightarrow D(a, b^n) = 1$

$$2) D(a, b) = 1 \Rightarrow D(a^p, b^n) = 1$$

$$3) D(a, b) = 1 \Rightarrow D(a + b, b) = 1$$

$$4) D(a, b) = 1 \Rightarrow D(a - b, b) = 1$$

$$5) D(a, b) = D \Rightarrow D(a^n, b^n) = D^n$$

$$6) m(a, b) = m \Rightarrow m(ax, bx) = mx \quad (x \in \mathbb{N}^*)$$

$$7) \left. \begin{array}{l} \text{Si } x / a \wedge x / b \\ m(a, b) = m \end{array} \right\} \Rightarrow m\left(\frac{a}{x}, \frac{b}{x}\right) = \frac{m}{x}$$

$$8) m(a, b) = m \Rightarrow m(a^n, b^n) = m^n$$

Números primos y compuestos

Definición

$a \in \mathbb{N}; a \neq 0, a \neq 1$ Decimos que a es **primo** $\Leftrightarrow d(a) = \{1, a\}$. Si a no es primo lo denominamos **compuesto**

Obs:

Como todos los naturales no nulos aceptan a 1 y si mismos como divisores podemos decir que un número es primo si y solo si acepta dos divisores.

Mediante esta definición los números naturales quedan clasificados en primos, compuestos, 0 y 1.

¿Porqué 0 y 1 no son ni primos ni compuestos? ¿Porqué los naturales distintos de 0 y de 1 que no son primos se llaman compuestos y no simplemente no primos?

Teorema

El menor de los divisores de un número compuesto distinto de 1 es primo.

Dem:

Consideramos $a \in \mathbb{N}^*; a \neq 1$ $d = \min(d(a) - \{1\})$ Debemos probar que d es primo.

Obsérvese que d existe pues $d(a) - \{1\}$ es un conjunto de naturales no vacío.

Intentaremos una demostración por absurdo; suponemos que d no es primo, como no es ni 0 ni 1 entonces es compuesto aceptando entonces un divisor distinto de 1 y de d .

$\exists d' \in \mathbb{N}^*, d' \neq 1, d' \neq d$ tal que $d' \mid d$ como $d \mid a \Rightarrow d' \mid a \Rightarrow d' \in d(a) - \{1\}$. Pero $d' \mid d$ y $d' \neq d \Rightarrow d' < d$

Encontramos pues un elemento del conjunto menor que el mínimo lo que genera el abs.

Teorema

El conjunto de los números primos no tiene máximo

Dem:

Sea H el conjunto de todos los números primos; queremos probar que H no tiene máximo. Lo cual haremos por absurdo.

Suponemos en consecuencia que existe $M = \max H$. Consideramos ahora $P = 2 \cdot 3 \cdot 5 \cdot \dots \cdot M + 1$ (el producto de todos los números primos más 1)

$P > M = \max H \Rightarrow P \notin H$ como además $P \neq 0$ y $P \neq 1 \Rightarrow P$ es compuesto Aplicando ahora el teorema inmediato anterior $d = \min[d(P) - \{1\}]$ es primo; pero por la definición dada de P , este dividido cualquier número primo da resto 1. Generándose así la contradicción buscada.

Teorema Euclides para primos

$$\left. \begin{array}{l} p \mid ab \\ p \text{ primo} \end{array} \right\} \Rightarrow \left\{ \begin{array}{l} p \mid a \\ \vee \\ p \mid b \end{array} \right.$$

Dem:

Si p/a el teorema está demostrado.

Si $p \nmid a$ $D(a,p)=1$ pues p es primo; como por hipótesis p/ab aplicando Euclides tenemos que p/b .

Teorema

$$\left. \begin{array}{l} p/a_1 a_2 \dots a_n \\ p \text{ primo} \end{array} \right\} \Rightarrow p/a_i \text{ para algún } i \text{ de } 1 \text{ a } n$$

Demostración por I.C. a cargo del lector.

Definición

Consideramos a un número compuesto. Si $a = p_1 p_2 \dots p_n$ con p_i primo decimos que a admite una **descomposición en producto de factores primos** (D.P.F.P.)

Teorema

$$a \in \mathbb{N}; a \text{ compuesto} \Rightarrow \begin{cases} 1) a \text{ admite una D.P.F.P.} \\ 2) \text{ Dicha D.P.F.P. es única} \end{cases}$$

Dem 1):

$$a \text{ es compuesto} \Rightarrow \exists p_1 = \min(d(a) - \{1\}) \text{ siendo } p_1 \text{ primo} \Rightarrow a = p_1 d_1$$

Si d_1 es primo entonces $p_1 d_1$ es D.P.F.P. de a

$$\begin{aligned} \text{Si } d_1 \text{ es compuesto} &\Rightarrow \exists p_2 = \min(d(d_1) - \{1\}) \text{ siendo } p_2 \text{ primo} \Rightarrow d_1 = p_2 d_2 \Rightarrow \\ &\Rightarrow a = p_1 p_2 d_2 \end{aligned}$$

Si d_2 es primo entonces $p_1 p_2 d_2$ es la D.P.F.P. de a

Si d_2 es compuesto

.....
.....

El proceso continua hasta que llegamos a un cociente d_n primo; si este mecanismo de divisiones sucesivas es siempre finito nos asegurariamos de la existencia de la D.F.

Probemos entonces que siempre llegamos a un d_n primo.

Sea H el conjunto de los d_i , $H \subseteq \mathbb{N}, H \neq \emptyset$ ($d_1 \in H$) $\Rightarrow \exists d_n = \min H$ d_n primo pues si

si d_n fuese compuesto $\exists p_{n+1} = \min(d(d_n) - \{1\})$ con p_{n+1} primo $\Rightarrow d_n = p_{n+1} d_{n+1} \Rightarrow d_{n+1} \in H$ y además

$d_{n+1} < d_n = \min H$ lo cual es contradictorio; en consecuencia es proceso descrito

es finito y nos conduce en todos los casos a la D.F. de a .

Dem 2) Unicidad

$$\begin{array}{l} a = p_1 p_2 \dots p_n \text{ con } p_i \text{ primo } \forall i \text{ de } 1 \text{ a } n \quad p_1 \leq p_2 \leq \dots \leq p_n \\ a = q_1 q_2 \dots q_m \text{ con } q_i \text{ primo } \forall i \text{ de } 1 \text{ a } m \quad q_1 \leq q_2 \leq \dots \leq q_m \end{array}$$

Queremos demostrar que $n = m$ y $p_i = q_i \forall i$ de 1 a n . Igualando nos queda

$$p_1 p_2 \dots p_n = q_1 q_2 \dots q_m \Rightarrow \begin{cases} p_1 / q_1 q_2 \dots q_m \text{ como } p_1 \text{ primo} \Rightarrow p_1 / q_j \text{ para algún } j \text{ de } 1 \text{ a } m \Rightarrow \\ q_1 / p_1 p_2 \dots p_n \text{ como } q_1 \text{ primo} \Rightarrow q_1 / p_k \text{ para algún } k \text{ de } 1 \text{ a } n \Rightarrow \end{cases}$$

$\Rightarrow p_1 = q_j \geq q_1$
 $\Rightarrow q_1 = p_k \geq p_1$ Entonces $p_1 = q_1$ simplificando tenemos $p_2 \dots p_n = q_2 \dots q_m$

Reiterando el razonamiento $p_2 = q_2, p_3 = q_3, \dots, p_n = q_n$ (si $n \geq m$)

Si $n > m$ después de simplificar nos queda $q_{n+1} q_{n+2} \dots q_m = 1 \Rightarrow q_{n+1} = q_{n+2} = \dots = q_m = 1$
 lo que contradecía que q_i es primo; por lo tanto $n=m$.

Ejercicios:

1) Si $a = p_1^\alpha p_2^\alpha \dots p_n^\alpha$ con p_i primo

Probar: $x/a \Leftrightarrow x = p_1^\beta p_2^\beta \dots p_n^\beta$ con $0 \leq \beta_i \leq \alpha_i \forall i$ de 1 a n

2) Si $a = p_1^\alpha p_2^\alpha \dots p_n^\alpha$ y $b = p_1^\beta p_2^\beta \dots p_n^\beta$ con p_i primo

Probar: $D(a, b) = p_1^\gamma p_2^\gamma \dots p_n^\gamma$ siendo $\gamma_i = \min\{\alpha_i, \beta_i\}$

$m(a, b) = p_1^\delta p_2^\delta \dots p_n^\delta$ siendo $\delta_i = \max\{\alpha_i, \beta_i\}$

3) Utilizando la D.P.F.P de un número escribir todos sus divisores; describir un método práctico para obtener todos sus divisores.

4) Deducir una fórmula que permita calcular la cantidad de divisores de un número dado.

5) Probar que si $a = p_1^\alpha p_2^\alpha \dots p_n^\alpha$ con p_i primo los divisores de a son los sumandos que se obtienen al desarrollar el producto:

$$P = (p_1^0 + p_1^1 + \dots + p_1^\alpha)(p_2^0 + p_2^1 + \dots + p_2^\alpha) \dots (p_n^0 + p_n^1 + \dots + p_n^\alpha)$$

6) Utilizando 5) probar que el número de divisores de a ($v(a)$) es:

$$v(a) = (\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_n + 1)$$

y que la suma de todas ellas (S_a) es:

$$S_a = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \dots \frac{p_n^{\alpha_n+1} - 1}{p_n - 1}$$

Ejercicios (Repartido 11 del curso presencial)

I) Completar de todas las formas posibles los siguientes esquemas de divisiones enteras

i) $\frac{9}{13}$ ii) $\frac{a}{35} \frac{1}{4}$ $a < 200$ iii) $\frac{60}{12}$ iv) $\frac{a}{q} \frac{17}{q}$ $a > 200$

II) En la división $\frac{a}{r} \frac{b}{16}$, r es el mayor posible y $a+b=341$ Hallar a, b y r.

III) Hallar a sabiendo que $\frac{a}{q^2} \mid \frac{37}{q}$

IV) Hallar a y b sabiendo que: $\frac{a}{q} \mid 15$, $\frac{b}{q-8} \mid 12$, $a+b=420$

V) Hallar todas las ternas posibles de naturales (a,b,c) tales que: $\frac{a}{12} \mid \frac{b}{c}$ y $\frac{a+7}{b} \mid \frac{15}{c}$

VI) Completar los siguientes esquemas de algoritmo de Euclides

	3		
	3		1
		0	

	1	2	3
			75
		0	

VII) Hallar dos naturales a y b sabiendo que $a+b=360$ y $D(a,b)=30$

VIII) Hallar dos naturales a y b sabiendo que $a,b=9900$ y $D(a,b)=30$

IX) Hallar a y b naturales sabiendo que: $a-b=48$, $\frac{a+b}{D(a,b)} = 88$

X) Hallar los naturales a y b sabiendo que: $m(a,b).D(a,b) = 9000$, $\frac{m(a,b)}{D(a,b)} = 90$ y además $a+b < 200$

XI) Ídem: sabiendo que $ab = 192$, $\frac{(m+D)^2}{4mD} = \frac{169}{48}$ siendo $m = m(a,b)$ y $D = D(a,b)$.

XII) Ídem. sabiendo que: $D(a^2 + ab + b^2, a^2) = 36$, $\frac{a^2 - b^2}{D^2} = 29$ siendo $D = D(a,b)$

XIII) Ídem. sabiendo que: $a^2 - b^2 = 6399$ $m(a,b) = 4620$

XIV) Ídem sabiendo que: $m(a,b) = 504$, $a > b$ y $\frac{a}{20} \mid \frac{b}{q}$

XV) Se sabe que: $11a + 8b = \dot{9}$, $3a + 4b = \dot{9}$

i) Probar que: $a = \dot{9}$ y $b = \dot{9}$

ii) Si además $D(a,b) = 9$, $\frac{a}{27} \mid \frac{b}{q}$, $a = 2b + 135$. Calcular a y b.

XVI) Sabiendo que: $D(b, c) = 3D(a, c)$ y $m(a, c) = 2m(b, c)$

i) Probar que: $a = \dot{2}$ y $b = \dot{3}$

ii) Demostrar que: $(a^3 - a)(b^3 - 9b) = \overline{162}$

iii) Si $D(a, b) = 1$ calcular: $D(b, c)$ y $D(a, c)$.

XVII) Determinar un número natural n compuesto de los factores primos 2, 5 y 7 sabiendo que $5n$ tiene 8 divisores mas que n , $7n$ tiene 12 divisores mas que n y $8n$ tiene 18 divisores mas que n .

XVIII) Hallar $x = 2^a 3^b 5^c$ sabiendo que $\frac{x}{2}$ tiene 30 divisores menos que x , $\frac{x}{3}$ tiene 35 divisores menos que x y $\frac{x}{5}$ tiene 42 divisores menos que x .

XIX) Determinar el número mas pequeño que admite 15 divisores.

XX) i) Probar que si m tiene un número impar de divisores entonces $\exists n \in \mathbb{N}; n^2 = m$ (o sea que m es un cuadrado perfecto.

ii) Hallar $m \in \mathbb{N}$ sabiendo que tiene 9 divisores y que $m - 1 = 39p$; p es primo.

XXI) Determinar todas las ternas de números naturales (a, b, c) que verifican: $D(a, b) = 3^3 \cdot 5$,
 $m(b, c) = 2 \cdot 3^4 \cdot 5 \cdot 7$ y $a \cdot c = 2 \cdot 3^5 \cdot 5 \cdot 7 \cdot 13$

XXII) Hallar $n \in \mathbb{N}$; $n = p^q \cdot q^p$ con p y q primos $p \neq q$ sabiendo que en número de divisores de n es $2p \cdot q$.

XXIII) i) Hallar a, b y $n \in \mathbb{N}$ sabiendo que: $n \neq 1$, $D(an, bn) = 21$, $a^2 - b^2 = \frac{21^3}{n^2}$ y $a - b = 21$

ii) Sea $N = 2^\alpha \cdot a^\beta$ y $N' = b^{\alpha+1} \cdot 5^\beta$ Hallar N y N' sabiendo que $5N$ tiene 20 divisores mas que $\frac{N'}{2}$ y que $\frac{N}{N'}$ tiene dos divisores.

iii) Hallar todos los naturales h sabiendo que: $h^2 + 4h = \dot{7}$ $D(h+4, 7) = 1$ y $m(h, 70) = \sqrt[4]{N'}$

XXIV) i) ¿Qué condición deben cumplir los números naturales a para que tengan 12 divisores y $D(a, 225) = 15$?

ii) Hallar a para que cumpla además que la suma de sus divisores es 168.

iii) Para el valor de a hallado en ii) probar que: $n^5 + 5n^2 - 6n = \dot{a}$

XXV) Probar: $D(a + nb, a + (n+2)b) = 1 \quad \forall n \in \mathbb{N} \Leftrightarrow b = \dot{2}$ y $D(a, b) = 1$

XXVI) i) Hallar a sabiendo que: $D(a, 75) = 5$ y $m(a, 75) = 150$

ii) Para a hallado probar que: $a^{n+1} + a^n - a - 1 = \overline{99}$

XXVII) Se realizan las divisiones enteras de un natural n entre dos naturales consecutivos p y $p+1$. Demostrar que la condición necesaria y suficiente para que los cocientes sean iguales es que el cociente de la primera división sea menor o igual que el resto de la primera división.

XXVIII) Sean a, b y c números naturales tales que: $D(a, b) = 2^3 \cdot 3^2$, $m(b, c) = 2^5 \cdot 3^3 \cdot 7^2$ y $m(a, c) = 2^5 \cdot 3^2 \cdot 5 \cdot 7$

i) Probar: $2^5 \cdot 7 / c$, $7^2 / b$, $7^2 \nmid c$, $5 / a$ y $3^2 / b$.

ii) Si además se sabe que: $v(a) = 30$, $v(b) = 48$ y $v(c) = 36$. Hallar a, b y c .

XXIX) a, b y c son tres números naturales que cumplen: $D(a, b) = 2^2 \cdot 3^3$, $D(a, b, c) = 3^2$

$m(a, b, c) = 2^3 \cdot 3^4 \cdot 5 \cdot 7$, $5 / b$, $v(b) = 32$ y $v(c) = 9$.

Determinar a, b y c justificando el procedimiento.

XXX) i) Probar: $D(a+b, m(a, b)) = D(a, b)$

ii) Hallar dos naturales a y b para que: $m(a, b) = 630$ y $a + b = 231$

XXXI) i) Se sabe que $D(a, b) = D(c, d)$, $m(a, b) = m(c, d)$, $c \cdot d = 2^7 \cdot 3^4 \cdot 5^2$ y $v(a) = 7$

Hallar a y b .

ii) Hallar todas las parejas (c, d) sabiendo además que $c = \overline{25}$

DIVISIBILIDAD EN $(\mathbb{Z}, +, \cdot, \leq)$

Introducción

Pretendemos en esta sección extender varios de los conceptos vistos bajo este mismo título en la estructura de los naturales ahora a los enteros. Así como también introducir otros nuevos estrechamente vinculados (Congruencias, clases residuales, ecuaciones diofánticas, etc.)

Por lo dicho parece razonable comenzar por definir división entera entre números enteros. Una posibilidad puede ser tomar textualmente la definición vista para los naturales. O sea:

$$a \text{ b } \Leftrightarrow \begin{cases} a = bq + r \\ r < b \end{cases}$$
 Pero tal opción nos haría perder la unicidad del cociente y del resto, ya que:

con esta definición $\begin{matrix} 14 & 3 \\ 2 & 4 \end{matrix}$ pero también $\begin{matrix} 14 & 3 \\ -1 & 5 \end{matrix}$ Como otras infinitas posibilidades .

Este inconveniente lo podemos subsanar exigiendo que el resto no sea negativo. En otras palabras nuestro proyecto de definición es:

$$a \text{ b } \Leftrightarrow \begin{cases} a = bq + r \\ 0 \leq r < b \end{cases} \quad (\text{Estamos suponiendo que } b \in \mathbb{Z}^+)$$

Antes de asumir tal proyecto como definición debemos demostrar el siguiente:

Teorema

$$H) \begin{cases} a, b \in \mathbb{Z} \\ b > 0 \end{cases} \quad T) \begin{cases} 1) \exists q, r \in \mathbb{Z}; a = bq + r \wedge 0 \leq r < b \\ 2) q \text{ y } r \text{ son únicos} \end{cases}$$

Dem1):

Consideramos $M = \{m \in \mathbb{N}; m = a - bx \text{ con } x \in \mathbb{Z}\}$ Intentaremos probar que M tiene mínimo y que dicho mínimo es el resto que andamos buscando. Como M es un conjunto de naturales, para demostrar que tiene mínimo es mas que razonable pensar en buena ordenación. Con tal objetivo debemos verificar que:

- i) $M \subseteq \mathbb{N}$ Lo cual es cierto por la definición dada del conjunto M.
- ii) $M \neq \emptyset$ Para demostrar esta proposición discutiremos dos casos.
 - Si $a \geq 0$ Tomando $x=0$ tenemos que $m = a - bx = a - b \cdot 0 = a \in M$
 - Si $a < 0$ $\Rightarrow -a > 0$ como $b > 0$ aplicando Arquímedes tenemos que $\exists n \in \mathbb{N}; nb > -a \Rightarrow -nb < a$ Llamando $x = -n$ entonces $xb < a \Rightarrow a - bx \in \mathbb{N} \Rightarrow a - bx \in M$

Aplicando buena ordenación de $\left. \begin{matrix} i) \\ ii) \end{matrix} \right\} \Rightarrow \exists \text{mín } M$ al que denominamos “alevosamente” r.

Probemos que es el “r” de la tesis. $r = \min M \Rightarrow r \in M \Rightarrow r \in \mathbb{N} \wedge \exists q \in \mathbb{Z}; r = a - bq \Rightarrow a = bq + r$

Falta demostrar $0 \leq r < b$. Como $r \in \mathbb{N} \Rightarrow r \geq 0$; por lo tanto lo que nos falta probar es que $r < b$ lo que haremos por absurdo.

Supongamos que $r \geq b \Rightarrow a - bq \geq b \Rightarrow a \geq b + bq = (b+1)q \Rightarrow a - (b+1)q \in \mathbb{N} \Rightarrow k = a - (b+1)q \in M$

Pero $k < r = a - bq = \min M$ Lo cual es contradictorio. Por lo tanto $r < b$.

La demostración de la unicidad queda a cargo del lector. También puede demostrarse la existencia utilizando la división entera entre naturales, discutiendo si $a \leq 0$ ó si $a < 0$.

Definición

Sean $a, b \in \mathbb{Z}; b > 0$ Realizar la **división entera** de a entre b es encontrar $q, r \in \mathbb{Z}$ tal que:
 $a = bq + r \wedge 0 \leq r < b$

Nota:

Puede definirse la división entera para cualquier entero b no nulo (no solamente para los positivos) sustituyendo la segunda condición por: $0 \leq r < |b|$

En caso de que $r=0$ la división se dice exacta, ó también que a es divisible entre b, ó que **b divide a**, ó que **a es múltiplo de b**. (Anotamos b/a ó $a = \dot{b}$)

Independizando la definición de divisores (múltiplos) de la división entera tenemos:

$$b/a \quad (a = \dot{b}) \Leftrightarrow \exists q \in \mathbb{Z}; a = bq$$

El lector habrá observado que no solamente utilizamos la misma notación sino también la misma definición que en naturales. De manera análoga se demuestra que:

$$x/a \wedge x/b \Rightarrow x/\alpha a + \beta b \quad \forall \alpha, \beta \in \mathbb{Z}$$

En $(\mathbb{N}, +, \leq)$ vimos que: $a/b \wedge b/a \Leftrightarrow a = b$ ¿Ocurrirá lo mismo en $(\mathbb{Z}, +, \leq)$?

Teorema

$a, b \in \mathbb{Z}$

$$a/b \wedge b/a \Leftrightarrow |a| = |b|$$

Dem. (\Rightarrow)

$$\left. \begin{array}{l} a/b \Rightarrow \exists h \in \mathbb{Z}; b = ah \Rightarrow |b| = |a| |h| \Rightarrow |a| / |b| \\ b/a \Rightarrow \exists k \in \mathbb{Z}; a = bk \Rightarrow |a| = |b| |k| \Rightarrow |b| / |a| \end{array} \right\} \Rightarrow |a| = |b|$$

como $a, b \in \mathbb{Z} \Rightarrow |a|, |b| \in \mathbb{N}$

(\Leftarrow)

$$|a| = |b| \Rightarrow a = \pm b \Rightarrow \begin{cases} a = (\pm 1).b \Rightarrow b/a \\ b = (\pm 1).a \Rightarrow a/b \end{cases}$$

Definición

$a, b \in \mathbb{Z}^*$ Decimos que a y b son **asociados** $\Leftrightarrow a/b \wedge b/a$

Como consecuencia del teorema anterior los asociados de a son únicamente el propio a y su opuesto $-a$. En los naturales el único asociado de a es el propio a.

Máximo común divisor – mínimo común múltiplo

Antes de comenzar con el tratamiento de los temas del título necesitamos por razones técnicas recordar algunos conceptos de estructuras algebraicas, mas precisamente referidos a los anillos.

Definición

Consideramos: $(A, +, \cdot)$ un anillo conmutativo y con elemento unidad $e \in A; I \subseteq A; I \neq \emptyset$

Decimos que I es un **ideal** en $(A, +, \cdot)$ $\Leftrightarrow \begin{cases} 1) x_1 + x_2 \in I \quad \forall x_1, x_2 \in I \\ 2) a \cdot x \in I \quad \forall x \in I, \forall a \in A \end{cases}$

Ej: El conjunto de los enteros pares es un ideal de \mathbb{Z} . ¿El conjunto de los impares, es un ideal de \mathbb{Z} ?

Brindar otro ejemplo de ideal en \mathbb{Z} .

Nota:

Fácilmente el lector comprobará que siendo $(A, +, \cdot)$ un anillo conmutativo y con unidad, se cumple

1) $\{0\}$ y A son ideales en $(A, +, \cdot)$ cualesquiera que sea el anillo de referencia. Por ese motivo podemos denominarlos ideales triviales en A .

2) Si $x \in I \Rightarrow -x \in I$ Siendo I un ideal en $(A, +, \cdot)$

3) Todo ideal contiene al 0.

4) Si $1 \in I \Rightarrow I = A$

5) Sea: $\{I_j\}$ una familia de ideales en $A \Rightarrow \bigcap I_j$ es un ideal en A

6) Consideramos $S = \{a_1, a_2, \dots, a_p\}$ un subconjunto finito de A . Denominamos $I(S)$ al conjunto formado por todas las combinaciones lineales que pueden realizarse con los elementos de S .

$$\text{O sea: } I(S) = \left\{ x \in A ; x = \sum_{i=1}^p \alpha_i a_i \quad \text{con } \alpha_i \in A \right\}$$

Probar que $I(S)$ es un ideal en A al que llamaremos **ideal generado por S**.

Si un ideal está generado por un conjunto unitario decimos que es **principal**. Así por ejemplo el ideal de los pares es principal pues está generado por $\{2\}$. Si un ideal está generado por $\{a\}$ anotamos $I(a)$ en lugar de $I(\{a\})$ con el fin de simplificar la notación.

Teorema

En $(\mathbb{Z}, +, \cdot, \leq)$ todo ideal es principal.

Más precisamente: I un ideal en $\mathbb{Z} \Rightarrow I = \{0\}$ ó $I = I(c)$ siendo $c = \min I \cap \mathbb{Z}^+$

Dem.

Si $I = \{0\}$ Se cumple la tesis.

Si $I \neq \{0\}$ Comencemos por demostrar que existe el mínimo de $I \cap \mathbb{Z}^+$ para lo cual es más que previsible que utilizaremos el principio de buena ordenación.

$$1) I \cap \mathbb{Z}^+ \subseteq \mathbb{N} \quad I \cap \mathbb{Z}^+ \subseteq \mathbb{Z}^+ \subseteq \mathbb{N} \Rightarrow I \cap \mathbb{Z}^+ \subseteq \mathbb{N}$$

$$2) I \cap \mathbb{Z}^+ \neq \emptyset \quad \text{Como } I \neq \{0\} \Rightarrow \exists a \in I; a \neq 0 \text{ Además } I \text{ es un ideal} \Rightarrow \\ \Rightarrow -a \in I$$

Por otra parte al ser $a \neq 0$ a ó $-a$ es positivo.

En consecuencia a ó $-a \in I \cap \mathbb{Z}^+$

De 1) y 2) por el P.B.O. podemos afirmar que $\exists \min I \cap \mathbb{Z}^+$ al que denominamos c .

Probemos ahora que $M = I(c)$, para lo cual demostraremos:

$$i) \forall x \in I(c) \Rightarrow x \in I$$

$$ii) \forall x \in I \Rightarrow x \in I(c)$$

$$i) \forall x \in I(c) \Rightarrow x = a \cdot c \quad \text{con } a \in \mathbb{Z}. \text{ Como } c = \min I \cap \mathbb{Z}^+ \Rightarrow c \in I \text{ que es un ideal} \Rightarrow ac \in I \quad \forall a \in \mathbb{Z}$$

ii) $\forall x \in I$ debemos probar que $x \in I(c)$ o sea que $x = \dot{c}$. Para ello realizamos la división de x entre c demostrando que el resto es nulo.

$$\begin{array}{l} x \\ r \end{array} : \begin{array}{l} c \\ q \end{array} \Rightarrow \begin{cases} x = cq + r \\ 0 \leq r < c \end{cases}$$

Si $r \neq 0 \Rightarrow r = x - cq \in \mathbb{Z}^+$ Por otra parte como $x \in I, cq \in I$ (por i)) e I es un ideal $\Rightarrow r \in I$

Por lo tanto $r \in I \cap \mathbb{Z}^+$ pero $r < c = \min I \cap \mathbb{Z}^+$ Lo cual es contradictorio.

Entonces $r = 0 \Rightarrow x = cq \Rightarrow x \in I(c)$

Nota

En $(\mathbb{N}, +, \cdot, \leq)$ definimos $D(a, b) = \max d(a) \cap d(b)$

Y luego demostramos $D(a, b) = D \Leftrightarrow \begin{cases} \text{i) } D/a \wedge D/b \\ \text{ii) } \forall x \in \mathbb{N}; x/a \wedge x/b \Rightarrow x/D \end{cases}$

En otras palabras definimos el máximo común divisor como el máximo de los divisores comunes y luego demostramos que dicha proposición es equivalente a decir que el máximo común divisor es un divisor común que es dividido por cualquier otro divisor común.

Obsérvese que la proposición tomada como definición nos obliga a trabajar en una estructura ordenada (para poder hablar de máximo de un conjunto). En cambio la segunda proposición solamente hace referencia a divisibilidad.

En $(\mathbb{Z}, +, \cdot, \leq)$ nos es posible en principio considerar cualquiera de las dos proposiciones como posibles definiciones de máximo común divisor. Optaremos por la segunda para allanar el camino cuando el tema sea tratado en polinomios; ya que ahí no dispondremos de una relación de orden que nos permita hablar de máximo de un conjunto.

Por lo dicho pasamos al siguiente teorema.

Teorema

$$\left. \begin{matrix} a, b \in \mathbb{Z} \\ a^2 + b^2 \neq 0 \end{matrix} \right\} \Rightarrow \exists D \in \mathbb{Z}; \begin{cases} \text{i) } D/a \wedge D/b \\ \text{ii) } \forall x \in \mathbb{Z}; x/a \wedge x/b \Rightarrow x/D \end{cases}$$

Dem.

Consideramos $I(a, b)$ (el ideal generado por $\{a, b\}$) $I(a, b) = \{x \in \mathbb{Z}; x = pa + sb \text{ con } p, s \in \mathbb{Z}\}$

Como en \mathbb{Z} todo ideal es principal $I(a, b) = I(d)$ con $d = \min I(a, b) \cap \mathbb{Z}^+$ Intentemos demostrar que d es el D de la tesis. Para lo cual debemos probar:

$$\begin{aligned} \text{i) } & d/a \wedge d/b \\ \text{ii) } & \forall x \in \mathbb{Z}; x/a \wedge x/b \Rightarrow x/d \end{aligned}$$

i) $a \in I(a, b) = I(d)$ (basta tomar $p=1$ y $s=0$) $\Rightarrow a = d \Rightarrow d/a$ Análogamente se demuestra que d/b

ii) $d \in I(d) = I(a, b) \Rightarrow \exists p, s \in \mathbb{Z}$ tal que $d = pa + sb$

Por otra parte $\forall x \in \mathbb{Z}; x/a \wedge x/b \Rightarrow x/pa + sb \Rightarrow x/d$

Definición

Consideramos $a, b \in \mathbb{Z}; a^2 + b^2 \neq 0$ Decimos que D es **máximo común** divisor de a y b si y solo si:

$$\begin{aligned} \text{i) } & D/a \wedge D/b \\ \text{ii) } & \forall x \in \mathbb{Z}; x/a \wedge x/b \Rightarrow x/D \end{aligned}$$

El teorema inmediato anterior nos asegura la existencia de un máximo común divisor entre dos enteros no simultáneamente nulos. Pero nada nos dice acerca de cuantos máximos aceptan.

$$\text{Si } D \in \mathbb{Z} \text{ es máximo común divisor de } a \text{ y } b \Rightarrow \begin{cases} D/a \wedge D/b & (1) \\ \forall x \in \mathbb{Z}; x/a \wedge x/b \Rightarrow x/D & (2) \end{cases}$$

$$\text{Si } D' \in \mathbb{Z} \text{ es máximo común divisor de } a \text{ y } b \Rightarrow \begin{cases} D'/a \wedge D'/b & (3) \\ \forall x \in \mathbb{Z}; x/a \wedge x/b \Rightarrow x/D' & (4) \end{cases}$$

De (1) y (4) se deduce que $D/D' \mid a$ Y a partir de (2) y (3) $\Rightarrow D'/D \mid b$

Por lo tanto si a y b admiten dos máximos común divisor D y D' estos son asociados.

Es muy sencillo de probar que :

$$\left. \begin{array}{l} D \text{ es M.C.D de } a \text{ y } b \\ D' \text{ asociado a } D \end{array} \right\} \Rightarrow D' \text{ es M.C.D. de } a \text{ y } b$$

En consecuencia dos enteros no simultáneamente nulos aceptan dos máximos común divisor asociados entre sí. Así por ejemplo los M.C.D. de 6 y -9 son 3 y -3.

Nota:

Si $a, b \in \mathbb{Z}; a^2 + b^2 \neq 0$ probamos que tienen dos y solo dos M.C.D. D y D' asociados entre sí. Además por el teorema visto inmediatamente antes de la definición de M.C.D. $I(a, b) = I(D) \Rightarrow D \in I(a, b) \Rightarrow \exists p, s \in \mathbb{Z}; D = pa + sb$. Como $D' = -D$, D' también es C.L. de a y de b .

En definitiva podemos afirmar que los máximos común divisor de dos enteros a y b siempre pueden escribirse como combinación lineal de a y b .

Así como dimos una definición de M.C.D. independiente de la relación “<” intentaremos hacer lo propio respecto al m.c.m.

$$\text{Nuestro proyecto es: } m \text{ es m.c.m. de } a \text{ y } b \Leftrightarrow \begin{cases} 1) m = a \wedge m = b \\ 2) \forall x \in \mathbb{Z}; x = a \wedge x = b \Rightarrow x = m \end{cases}$$

Por lo dicho vamos al siguiente teorema.

Teorema

$$\text{H) } a, b \in \mathbb{Z}^* \quad \text{T) } \exists m \in \mathbb{Z} \text{ tal que } \begin{cases} \text{i) } m = a \wedge m = b \\ \text{ii) } \forall x \in \mathbb{Z}; x = a \wedge x = b \Rightarrow x = m \end{cases}$$

Dem.

Consideramos $H = \left\{ x \in Z; x = \dot{a} \wedge x = \dot{b} \right\}$ Es inmediato verificar que H es un ideal en Z.

Por lo tanto H es principal; en otras palabras $\exists m \in Z; H = I(m)$ Probemos ahora que m cumple las proposiciones i) y ii) de la tesis.

- i) $m \in I(m) = H \Rightarrow m = \dot{a} \wedge m = \dot{b}$
- ii) $\forall x \in Z; x = \dot{a} \wedge x = \dot{b} \Rightarrow x \in H = I(m) \Rightarrow x = \dot{m}$

Definición

Sean a y b dos enteros no nulos. Decimos que m ($m \in Z$) es **mínimo común múltiplo** de a y b si y solo si cumple:

- i) $m = \dot{a} \wedge m = \dot{b}$
- ii) $\forall x \in Z; x = \dot{a} \wedge x = \dot{b} \Rightarrow x = \dot{m}$

Dados dos enteros a y b no nulos el teorema inmediato anterior nos asegura la existencia de al menos un mínimo común múltiplo. Nada nos dice acerca de cuantos hay.

Probar que si a y b son dos enteros no nulos aceptan dos y solo dos m.c.m. y que además son asociados entre si.

Definición

- 1) $a, b \in Z$ decimos que a y b son **primos entre si** $\Leftrightarrow 1$ es M.C.D. de a y b.
- 2) $p \in Z$ $p \neq 0, p \neq 1$ decimos que p es **primo** $\Leftrightarrow d(p) = \{1, -1, p, -p\}$

Teorema de Euclides

$$\left. \begin{array}{l} c/a.b \\ a \text{ y } c \text{ primos entre si} \end{array} \right\} \Rightarrow c/b$$

Dem.

Como a y c son primos entre si 1 es M.C.D. de a y c $\Rightarrow \exists p, s \in Z; 1 = pa + sc$ multiplicando ambos miembros por b tenemos que: $b = pba + sbc$ Por hipótesis c/ab y por definición c/c ; entonces $c/pba + scb$ y como $pba + sbc = b \Rightarrow c/b$

Corolario

- 1) $\left. \begin{array}{l} a \text{ y } b \text{ primos entre si} \\ a/c \wedge b/c \end{array} \right\} \Rightarrow a.b/c$
- 2) $\left. \begin{array}{l} p \in Z \text{ } p \text{ primo} \\ p/ab \end{array} \right\} \Rightarrow p/a \vee p/b$

Demostración a cargo del lector.

Ejercicios

Demostrar:

$$1- \left. \begin{array}{l} a \mid b \\ r \mid q \\ D \text{ es M.C.D. de } a \text{ y } b \end{array} \right\} \Rightarrow D \text{ es M.C.D. de } b \text{ y } r$$

2- Que el procedimiento identificado en “divisibilidad en $(\mathbb{N}, +, \cdot, \leq)$ ” como algoritmo de Euclides también es válido en $(\mathbb{Z}, +, \cdot, \leq)$

3- $D = \max d(a) \cap d(b) \Rightarrow D$ es M.C.D. de a y b .

¿Es cierto el recíproco? ¿Ocurre algo similar con el m.c.m.?

4- D es M.C.D. de a y $b \Rightarrow Dx$ es M.C.D. de ax y bx

$$5- \left. \begin{array}{l} D \text{ es M.C.D. de } a \text{ y } b \\ x/a \\ x/b \end{array} \right\} \Rightarrow \frac{D}{x} \text{ es M.C.D. de } \frac{a}{x} \text{ y } \frac{b}{x}$$

$$6- D \text{ es M.C.D. de } a \text{ y } b \Rightarrow \begin{cases} a = Da' \\ b = Db' \\ a' \text{ y } b' \text{ primos entre si} \end{cases}$$

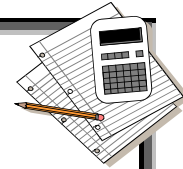
$$7- D \text{ es M.C.D. de } a \text{ y } b \Rightarrow \begin{cases} D \text{ es M.C.D. de } a \text{ y } -b \\ D \text{ es M.C.D. de } -a \text{ y } -b \end{cases}$$

$$8- m \text{ es m.c.m. de } a \text{ y } b \Rightarrow \begin{cases} m \text{ es m.c.m. de } a \text{ y } -b \\ m \text{ es m.c.m. de } -a \text{ y } -b \end{cases}$$

$$9- \text{ Si } D \text{ es M.C.D. de } a, b \text{ y } m \text{ es m.c.m. de } a, b \Rightarrow |m \cdot D| = |a \cdot b|$$

10- *“Todo entero compuesto puede expresarse como el producto de (± 1) por factores primos positivos. Esta expresión es única, salvo el orden en que los factores se consideren.”*
(sic. Álgebra moderna- Birkhoff – Mc. Lane)

ANOTACIONES



▲ [Inicio](#)