Tema 2 (Segunda parte): Teoría de números

David de Frutos Escrig
versión original elaborada por
María Inés Fernández Camacho

MATEMÁTICA DISCRETA Y LÓGICA MATEMÁTICA
(Ingeniería Informática - Ciencias Matemáticas)
UCM Curso 18/19

DEF:

Dados dos números enteros $a, b \in \mathbb{Z}$ *se dice que* a *es* **divisible** *por* b *(o también que* b *es* **divisor** *o* **factor** *de* a*, o que* a *es* **múltiplo** *de* b*) cuando existe algún entero* $c \in \mathbb{Z}$ *tal que* $a = cb$.

Notación:

- $b \mid a$ denota que b es divisor de a.
- $b \nmid a$ denota que b no es divisor de a.
- $a = \dot{b}$ denota que a es múltiplo de b.

Ejs:

$$9|18,\ \ 6|18,\ \ 2|18,\ \ 2\nmid 9,\ \ 18\nmid 6$$
$$18 = \dot{3},\ 6 = \dot{2}$$

Si $b|a$ y además el entero c tal que $a = c \cdot b$ es único, entonces decimos que c es el cociente exacto de la división de a entre b y escribimos $c = \frac{a}{b}$

Hecho 1: $0 \mid 0$, pero $\frac{0}{0}$ está indefinido.

(El 0 es divisor del 0)

Dem: $0 \mid 0$ **ya que** $\forall c \in \mathbb{Z},\ 0 = c \cdot 0$, **pero** $\frac{0}{0}$ **está indefinido ya que no existe un único** $c \in \mathbb{Z}$ **tal que** $0 = c \cdot 0$.

Hecho 2: $\forall b \in \mathbb{Z},\ b \neq 0,$ ($0 \nmid b$ y, por tanto, $\frac{b}{0}$ está indefinido).

(Ningún entero distinto de 0 tiene como divisor al 0)

Dem: $\forall b \in \mathbb{Z},\ b \neq 0$, **se tiene que** $\forall c \in \mathbb{Z},\ c \cdot 0 = 0 \neq b$.

DEF:

Dados $D, d \in \mathbb{Z}$, *si existe un* **único** $c \in \mathbb{Z}$ *tal que* $D = c \cdot d$, *entonces decimos que* c *es el* **cociente exacto** *de la división de* D (**dividendo**) *entre* d (**divisor**), *se escribe* $c = \frac{D}{d}$ *y a la operación realizada para calcular el cociente exacto se la llama* **división exacta**.

ALGUNAS PROPIEDADES MÁS DE LA DIVISIBILIDAD DE NÚMEROS ENTEROS

Si $a, b, c, d \in \mathbb{Z}$, entonces

(1) $a \mid 0$, $(0 = \dot{a})$ (El 0 es múltiplo de cualquier entero)

(2) $1 \mid a$ (El 1 es divisor de cualquier entero)

(3) $a \mid 1$ si y sólo si $a = \pm 1$

(4) Si $a \mid b$ y $c \mid d$, entonces $ac \mid bd$

(5) $a \mid a$

(6) Si $a \mid b$ y $b \mid a$, entonces $a = \pm b$

(7) Si $a \mid b$ y $b \mid c$, entonces $a \mid c$

(8) Si $a \mid b$ y $a > 0$ y $b > 0$, entonces $a \leq b$

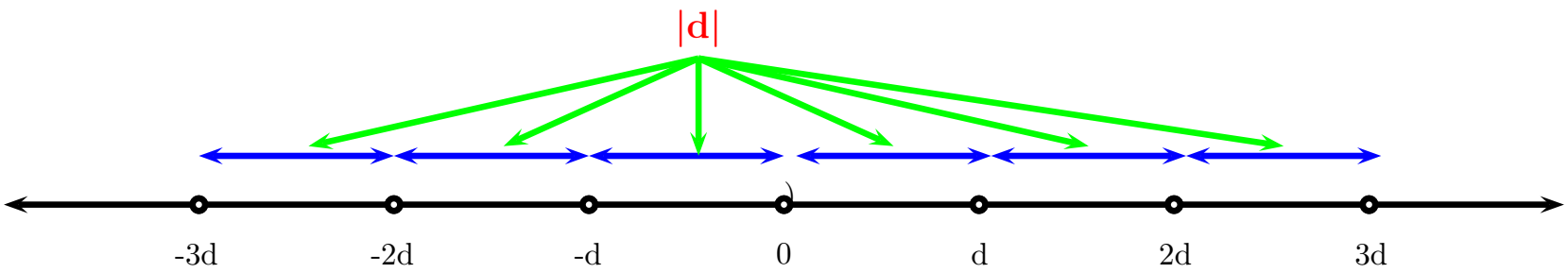
(9) Si $a \mid b$ y $a \mid c$, entonces $a \mid (bx + cy)$ para cualquier par de números $x, y \in \mathbb{Z}$
(Si a es divisor de b y de c, entonces a es divisor de cualquier combinación lineal entera de b y c)

(10) $a \mid b$ si y sólo si $|a| \Big| |b|$

Dem: Mera aplicación de la definición de divisor. Se deja como ejercicio.

DIVISIÓN ENTERA O EUCLÍDEA

Si $D, d \in \mathbb{Z}$, $d \neq 0$, en general D no será múltiplo de d, pero siempre existirán dos múltiplos consecutivos de d entre los que se encuentre D, ya que la distancia entre dos múltiplos consecutivos de d es $|d|$.



DIVISIÓN ENTERA O EUCLÍDEA

DEF:

1) *Dados* $D, d \in \mathbb{Z}, \ d > 0,$ *siendo* c *el mayor número entero tal que* $c \cdot d \leq D \leq (c+1) \cdot d$, *entonces*

- c *y* $c+1$ *reciben los nombres respectivos de* **cocientes enteros por defecto y por exceso** *de la división de* D (**dividendo**) *por* d (**divisor**)
- *los números* $r, r' \in \mathbb{N}$ *definidos por las igualdades* $r = D - c \cdot d, \ r' = (c+1) \cdot d - D = d - r$ *reciben los nombres respectivos de* **restos enteros por defecto y por exceso**.

2) *Dados* $D, d \in \mathbb{Z}, \ d < 0,$ *el cociente y el resto enteros por defecto/exceso de la división de* D *entre* d, *se definen como el cociente y el resto enteros por defecto/exceso de* $(-D)$ *entre* $(-d)$.

DIVISIÓN ENTERA O EUCLÍDEA

DEF:

Se llama **división entera** *entre enteros a la operación aritmética cuyo objetivo es el cálculo de los cocientes y restos enteros.*

Obs:

- La división entera de D entre 0 no está definida.
- Si no se dice lo contrario, al hablar de cocientes y restos enteros nos referiremos a cocientes y restos por defecto.

DIVISIÓN ENTERA O EUCLÍDEA

- Si $c \cdot d = D$, entonces $r = 0$, y $c = \frac{D}{d}$ es el cociente exacto de D entre d .
- Si $D > 0$ y $D < d$ entonces $c = 0$ y $r = D$ (de lo contrario $r \notin \mathbb{N}$)
- En cualquier caso, r es la distancia (siempre positiva) entre $c \cdot d$ y D.

Ej:

D	d	c	r	c + 1	r '
18	5	3	3	4	2
-18	5	-4	2	-3	3
18	-5	-4	2	-3	3
-18	-5	3	3	4	2
18	6	3	0	4	6
-18	6	-3	0	-2	6
18	-6	-3	0	-2	6
-18	-6	3	0	4	6

"ALGORITMO" DE LA DIVISIÓN

Teorema de la división

Dados $D, d \in \mathbb{Z}$, $d \neq 0$, existen dos enteros c y r **unívocamente determinados**, tales que $D = c \cdot d + r$ y $0 \leq r < |d|$.
Los números c y r se llaman **cociente** y **resto** de la división entera (euclídea) con **dividendo** D y **divisor** d.

Notación: $c \equiv_{not} D \text{ div } d$ $\quad$ $r \equiv_{not} D \text{ mod } d$

Dem: ...

"ALGORITMO" DE LA DIVISIÓN

Obs:

- La condición $\mathbf{0 \leq r < |d|}$ es la que "caracteriza" al "algoritmo" de la división entera:
  - Aunque 18 = (-4)(-5) - 2, -2 **no** puede ser el resto de la división entera de 18 entre -5, por ser un número negativo.
  - Aunque 18 = 3(-5) + 33, 33 **no** puede ser el resto de la división entera de 18 entre -5, pues 33 no es menor que |-5|.
  - 18 = (-3)·(-5)+ 3, c= -3, r = 3 .

"ALGORITMO" DE LA DIVISIÓN

Obs:

- Fijado el divisor b sólo hay $|b|$ posibles restos: 0,1,2, $\cdots$, $|b|-1$, lo que nos permite clasificar los infinitos números enteros en una cantidad finita de clases, según los restos que producen al dividirlos por b.
- Puede ser útil "leer el teorema de atrás hacia delante": para cada $d \neq 0$ y $0 \leq r < |d|$ los valores $D = c \cdot d + r$ son aquellos que divididos por $\boldsymbol{d}$ dan resto $\boldsymbol{r}$, y cada $D \in \mathbb{Z}$ podrá ser obtenido para algún tal r (de manera única).

"ALGORITMO" DE LA DIVISIÓN

Ejemplo: **Demúestrese que el cuadrado de cualquier número entero es de la forma $3 \cdot k$ o $3 \cdot k + 1$ para algún $k \in \mathbb{Z}$**

"Leyendo de atrás hacia adelante el teorema", demostrar que "dado $n \in \mathbb{Z}$ entonces $n^2 = 3 \cdot k$ o $n^2 = 3 \cdot k + 1$ para algún $k \in \mathbb{Z}$ " es equivalente a demostrar que "al dividir n^2 entre 3 queda siempre resto 0 o 1".

El teorema de la división, de nuevo leído hacia atrás, garantiza que tendremos $n = 3 \cdot c, \quad n = 3 \cdot c + 1 \quad \text{o} \quad n = 3 \cdot c + 2$

Con lo que:

- Si $n = 3 \cdot c$ entonces $n^2 = 3 \cdot (3 \cdot c^2) = 3 \cdot k$ para $k = 3 \cdot c^2 \in \mathbb{Z}$.
- Si $n = 3 \cdot c + 1$ entonces $n^2 = 3 \cdot (3 \cdot c^2 + 2 \cdot c) + 1 = 3 \cdot k + 1$ para $k = (3 \cdot c^2 + 2 \cdot c) \in \mathbb{Z}$.
- Si $n = 3 \cdot c + 2$ entonces $n^2 = 3 \cdot (3 \cdot c^2 + 4 \cdot c + 1) + 1 = 3 \cdot k + 1$ para $k = (3 \cdot c^2 + 4 \cdot c + 1) \in \mathbb{Z}$.

Máximo común divisor

Def:

El máximo común divisor de dos números enteros a *y* b *es el mayor número natural* d *que es divisor común de* a *y* b*; es decir* d *es el máximo común divisor de* a *y* b *si y sólo si*

i) $d \mid a$

ii) $d \mid b$

iii) $\forall c \in \mathbb{Z}$ *tal que* $c \mid a$ *y* $c \mid b$, *entonces* $c \leq d$

Notación: $d = \text{m.c.d.}(a, b)$ indica que **existe** el máximo común divisor de a y b y que vale d.

Máximo común divisor

Propiedades:

(1) **No existe m.c.d.$(0,0)$**

(2) **$\forall a, b \in \mathbb{Z}$, $a \neq 0$ o $b \neq 0$, se cumple m.c.d.(a,b) = m.c.d.(b,a)**

(3) **$\forall a \in \mathbb{Z}$, $a \neq 0$ se cumple m.c.d.$(a,0)$ = m.c.d.$(0,a) = |a|$**

(4) **$\forall a, b \in \mathbb{Z}$, $a \neq 0$ o $b \neq 0$, se cumple m.c.d.(a,b) = m.c.d.$(|a|,|b|)$**

Teorema:

$\forall a, b \in \mathbb{Z}$, $a \neq 0$ o $b \neq 0$, existe el máximo común divisor de a y b y es único.

Dem: Como $\forall n \in \mathbb{Z},\ 1 \mid n$ y $\forall n \in \mathbb{Z},\ n \neq 0,\ |n|$ es el mayor divisor de n; el conjunto de los divisores positivos comunes de a y b es un subconjunto finito, no vacío, de $\mathbb{N}$, que tendrá un máximo único.

Lema de reducción de Euclides

Lema de reducción de Euclides

Dados $a, b \in \mathbb{Z}_1$, $a \geq b$, y $c, r \in \mathbb{Z}_0$ tales que $a = c \cdot b + r$ y $0 \leq r < b$, se tiene que $\text{m.c.d.}(a, b) = \text{m.c.d.}(b, r)$.

Basta demostrar que los divisores comunes de a y b coinciden con los de b y r :

$\Longrightarrow)$ $(m|a \text{ y } m|b) \to (m|b \text{ y } m|r)$

$(m|a \text{ y } m|b) \sim (\exists k, l \in \mathbb{Z},\ a = k \cdot m \text{ y } b = l \cdot m)$

$(m|a \text{ y } m|b) \to (\exists k, l \in \mathbb{Z},\ b = l \cdot m$

$r = a - c \cdot b = k \cdot m - c \cdot l \cdot m = (\underbrace{k - c \cdot l}_{\in \mathbb{Z}}) \cdot m)$

$\to (m|b \text{ y } m|r)$

$\Longleftarrow)$ $(m|b \text{ y } m|r) \to (m|a \text{ y } m|b)$

Inmediato

En realidad, lo hemos demostrado utilizando $a \neq 0$ o $b \neq 0$ como única restricción.

Algoritmo de Euclides

$\{a, b \in \mathbb{Z} \quad a \geq b \geq 0,\ (a \neq 0) \vee (b \neq 0)\}$

Si $b = 0$

entonces $\{a \neq 0\}$ $d \leftarrow |a|$ $\{d = \text{m.c.d.}(a, 0) = |a|\}$

si no $\{a \geq b > 0\}$ $d \leftarrow \text{m.c.d.}(b, a \bmod b)$

$\{d = \text{m.c.d.}(a, b)\}$

i		
0	$a = c_0 \cdot b + r_0$	$0 < r_0 < b$
1	$b = c_1 \cdot r_0 + r_1$	$0 < r_1 < r_0$
2	$r_0 = c_2 \cdot r_1 + r_2$	$0 < r_2 < r_1$
$\cdots$	$\cdots\cdots$	$\cdots$
k	$r_{k-2} = c_k \cdot r_{k-1} + r_k$	$0 < r_k < r_{k-1}$
k+1	$r_{k-1} = c_{k+1} \cdot r_k + 0$	$r_{k+1} = 0$
k+2	$d \leftarrow r_k$	$r_0 > r_1 \cdots \geq 0$

a_i:Dividendo tras i-ésima reducción de Euclides
b_i:Divisor tras la i-ésima reducción de Euclides
c_i:Cociente tras i-ésima reducción de Euclides
r_i:Resto tras la i-ésima reducción de Euclides

$a_0 = a, \quad b_0 = b$

$a_i = b_{i-1} \qquad i \geq 1$

$b_i = a_{i-1} \bmod b_{i-1} \qquad i \geq 1$

$a_{k+2} = r_k = d$

$b_{k+2} = r_{k+1} = 0$

Algoritmo de Euclides

Ej: m.c.d.(51,21) = 3

i	a_i	b_i	r_i	c_i
0	51	21	9	2
1	21	9	3	2
2	9	3	0	3
3	3	0		

$k = 1 \quad ; \quad i = k+2 = 3$

Teorema de Bézout

Siendo $a, b \in \mathbb{Z}$, $(a \neq 0)$ o $(b \neq 0)$ y $d = \text{m.c.d.}(a, b)$, tenemos que $\exists\, m, n \in \mathbb{Z}$, tales que $d = m \cdot a + n \cdot b$.

Dem: Sea $C = \{a \cdot x + b \cdot y / a \cdot x + b \cdot y > 0, \quad x, y \in \mathbb{Z}\}$

C es un subconjunto no vacío de $\mathbb{N}$, ya que $(a \cdot a + b \cdot b) \in C$, y por el principio de buena ordenación tiene un mínimo $d = m \cdot a + n \cdot b$, con $m, n \in \mathbb{Z}$.

Veamos que $d = \text{m.c.d.}(a, b)$:

- $d|a$ En efecto: por el teorema de la división $\exists\, c, r \in \mathbb{Z}$ únicos tales que $r = a - c \cdot d$ y $0 \leq r < d$. $(|d| = d$ pues $d \in C)$

  Luego r puede ponerse como combinación lineal entera de a y b, ya que $r = a - c \cdot (m \cdot a + n \cdot b) = a \cdot \underbrace{(1 - c \cdot m)}_{\in \mathbb{Z}} + b \cdot \underbrace{(-c \cdot n)}_{\in \mathbb{Z}}$, para ciertos $m, n \in \mathbb{Z}$. Por tanto, como $0 \leq r < d$, necesariamente tendremos $r = 0$, ya que d es el mínimo de C, concluyéndose que $a = c \cdot d$.

- $d|b$ Arriba podemos tomar b en lugar de a, pues m.c.d.(b, a) = m.c.d.(a, b).
- $\forall c \in \mathbb{Z}$ tal que $c \mid a$ y $c \mid b$, se tiene $c \leq d$

$$(c|a \wedge c \mid b) \rightarrow c \mid (\underbrace{a \cdot m + b \cdot n}_{d})$$

Luego $c \mid d$ y por tanto $c \leq |c| \leq d$, ya que $c \mid d \rightarrow |c| \Big| d$ y

$$\forall m, n \in \mathbb{N} \ \ (m \mid n \rightarrow m \leq n)$$

Obs:

- El m.c.d.(a, b) es la combinación lineal entera positiva "más pequeña" de a y b.
- La expresión de m.c.d.(a, b) como combinación lineal entera positiva de a y b, no es única.

Ej.:

$$\begin{aligned} \text{m.c.d.}(-18, 24) &= 6 \\ -18 \cdot 1 + 24 \cdot 1 &= 6 \\ -18 \cdot 5 + 24 \cdot 4 &= 6 \\ -18 \cdot (-3) + 24 \cdot (-2) &= 6 \end{aligned}$$

Algoritmo de Euclides extendido para obtener una identidad de Bézout

Se parte de la iteración $i = k + 2$ con la que termina el algoritmo de Euclides al calcular $d = \text{m.c.d.}(a, b)$, y se procede del siguiente modo:

$i \leftarrow k + 2$
$m_i \leftarrow 1$
$n_i \leftarrow 0$
Mientras que $i \neq 0$ **hacer**
  $i \leftarrow i - 1$
  $m_i \leftarrow n_{i+1}$
  $n_i \leftarrow m_{i+1} - n_{i+1} \cdot c_i$
fmientras
$m \leftarrow m_0$
$n \leftarrow n_0$

Algoritmo de Euclides extendido para obtener una identidad de Bézout

$$
\begin{array}{lll}
m_{k+2} = 1, \quad n_{k+2} = 0 & & a_0 = a, \quad b_0 = b \\
m_i = n_{i+1} & 0 \leq i \leq k+1 & a_i = b_{i-1} \qquad\qquad k+2 \geq i \geq 1 \\
n_i = m_{i+1} - n_{i+1} \cdot c_i & 0 \leq i \leq k+1 & b_i = a_{i-1} \bmod b_{i-1} \quad k+2 \geq i \geq 1 \\
m = m_0, \quad n = n_0 & & c_i = a_i \operatorname{div} b_i \qquad\quad k+2 \geq i \geq 0
\end{array}
$$

La corrección de este algoritmo puede demostrarse probando que

$$\forall\, i \in \{0, \cdots, k+2\} \quad \text{m.c.d.}(a_i, b_i) = m_i \cdot a_i + n_i \cdot b_i$$

por inducción simple por predecesores.

Algoritmo de Euclides extendido para obtener una identidad de Bézout

Ej: m.c.d.$(272,18) = 2 = 1 \cdot 272 + (-15) \cdot 18$, $m = 1$, $n = -15$

i	a_i	b_i	r_i	c_i	m_i	n_i
0	272	18	2	15	1	-15
1	18	2	0	9	0	1
2	2	0			1	0

m.c.d.$(51,21) = 3 = ? \cdot 51 + ?' \cdot 21$, $m = ?$, $n = ?'$

Lema de múltiplos:

$$\forall\, a, b \in \mathbb{Z},\ \ \forall k \in \mathbb{N}_1 \ \ \text{m.c.d.}(k \cdot a, k \cdot b) = k \cdot \text{m.c.d.}(a, b)$$

Dem.:

Sea $d = \text{m.c.d.}(a, b)$

$$(d \mid a \ \text{ y } d \mid b\,) \to (k \cdot d \mid k \cdot a \quad \text{y} \quad k \cdot d \mid k \cdot b\,)$$

$$\forall d' \in \mathbb{Z},\ \ d' \mid k \cdot a \quad \text{y} \quad d' \mid k \cdot b, \ \text{entonces} \quad d' \leq k \cdot d$$

En efecto:

$$\exists\, m, n \in \mathbb{Z},\ \ d = m \cdot a + n \cdot b \ \ \text{(Bézout)}$$
$$\to \ \exists\, m, n \in \mathbb{Z},\ \ k \cdot d = m \cdot k \cdot a + n \cdot k \cdot b$$

$$(d' \mid k \cdot a \ \text{ y } d' \mid k \cdot b\,) \to (d' \mid \underbrace{m \cdot k \cdot a + n \cdot k \cdot b}_{k \cdot d})$$

$$\to d' \mid k \cdot d$$
$$\to |d'| \,\Big|\, k \cdot d \qquad [\ |k \cdot d| = k \cdot d\ ]$$
$$\to d' \leq k \cdot d \qquad [\ d' \leq |d'| \leq k \cdot d\ ] \square$$

Lema de reducción: $\forall\, a, b \in \mathbb{Z}$, si $d = \text{m.c.d.}(a, b)$ entonces

$$\exists\, a_1, b_1 \in \mathbb{Z},\ a = d \cdot a_1,\ \ b = d \cdot b_1 \ \text{ con } \ \text{m.c.d.}(a_1, b_1) = 1$$

Dem.:

$d = \text{m.c.d.}(a, b) \ \rightarrow\ (\exists\, a_1, b_1 \in \mathbb{Z},\ a = d \cdot a_1,\ \text{y}\ \ b = d \cdot b_1)$

ya que $d \mid a$ y $d \mid b$.

$d = \text{m.c.d.}(a, b) = \ \text{m.c.d.}(d \cdot a_1, d \cdot b_1) = d \cdot \text{m.c.d.}(a_1, b_1)$

justificándose la última igualdad por el lema anterior.

Luego $\text{m.c.d.}(a_1, b_1) = 1$, ya que $d \in \mathbb{N}_1$.

Def:

Decimos que dos enteros a y b no nulos son primos entre sí (coprimos o primos relativos), si $m.c.d.(a,b) = 1$

Teorema: a y b no nulos son primos entre sí, si y sólo si, existen $m, n \in \mathbb{Z}$ tales que $m \cdot a + n \cdot b = 1$.

Dem.: $\Longrightarrow$) a y b primos entre sí $\sim$ m.c.d.$(a, b) = 1$
$\rightarrow (\exists m, n \in \mathbb{Z},\ 1 =$ m.c.d.$(a, b) = m \cdot a + n \cdot b)$
(Th. Bézout)

$\Longleftarrow$) Sea $c \in \mathbb{Z}, (c \mid a$ y $c \mid b)$. Entonces $\exists\, k, l \in \mathbb{Z}, (a = k \cdot c$ y $b = l \cdot c)$, y por tanto $\exists\, k, l, m, n \in \mathbb{Z}, (1 = m \cdot a + n \cdot b = m \cdot k \cdot c + n \cdot l \cdot c = (\underbrace{m \cdot k + n \cdot l}_{\in \mathbb{Z}}) \cdot c)$, luego $c \mid 1$. Lo que nos permite concluir que m.c.d.$(a, b) = 1$, pues 1 es divisor de cualquier número y es el único divisor positivo del propio 1.

Lema de Euclides

Dados $a, b, c \in \mathbb{Z}$, $(a \neq 0)$ o $(b \neq 0)$, si $a \mid b \cdot c$ y $\text{m.c.d.}(a, b) = 1$, entonces $a \mid c$.

Dem.:

$$\text{m.c.d.}(a, b) = 1 \rightarrow (\exists\, m, n \in \mathbb{Z},\ 1 = m \cdot a + n \cdot b) \quad \text{(Th. Bézout)}$$
$$\rightarrow (\exists\, m, n \in \mathbb{Z},\ c = m \cdot a \cdot c + n \cdot b \cdot c)$$

$$a \mid b \cdot c \rightarrow (\exists\, k \in \mathbb{Z},\ b \cdot c = k \cdot a)$$

Luego $\exists m, n, k \in \mathbb{Z},\ c = m \cdot a \cdot c + n \cdot k \cdot a = (\underbrace{m \cdot c + n \cdot k}_{\in \mathbb{Z}}) \cdot a$,

concluyendose que $a \mid c$.

Ejercicio: Dados $a, b, c \in \mathbb{Z}$, $(a \neq 0)$ o $(b \neq 0)$, refuta la siguiente afirmación: si $a \mid b \cdot c$, entonces $a \mid b$ o $a \mid c$.

Mínimo común múltiplo

El mínimo común múltiplo de dos números enteros a y b es el menor número natural **positivo** m que es múltiplo común de a y b, en caso de que alguno tal exista. Sería entonces el menor $m \in \mathbb{N}_1$ que cumpla las tres condiciones siguientes:

I) $a \mid m \quad (m = \dot{a})$

II) $b \mid m \quad (m = \dot{b})$

III) $\forall c \in \mathbb{N}_1$ **si** $(c = \dot{a})$ **y** $(c = \dot{b})$, **entonces** $m \leq c$

Notación: $m = \text{m.c.m.}(a, b)$ indica que **existe** el mínimo común múltiplo de a y b y que vale m.

Mínimo común múltiplo

Teorema:

$\forall a, b \in \mathbb{Z}$, $a \neq 0$ y $b \neq 0$, existe el mínimo común múltiplo de a y b y es único

Dem: Sea $M_{ab} = \{n \in \mathbb{N}_1 / n = \dot{a} \text{ y } n = \dot{b}\}$

Como $|a \cdot b|$ es múltiplo positivo común de ambos, M_{ab} es un subconjunto no vacío de $\mathbb{N}$ que tiene un mínimo único.

Propiedades:

(1) Para ningún $a \in \mathbb{Z}$, existe nunca **m.c.m.$(a, 0)$**, ni existe **m.c.m.$(0, a)$**

Dem: Aunque $0 = \dot{a}$ para cualquier a, el único múltiplo de 0 es 0, y por tanto no existe ningún número natural **positivo** que sea múltiplo común de 0 y a.

(2) $\forall a, b \in \mathbb{Z}$, $a \neq 0$ y $b \neq 0$, se cumple **m.c.m.(a, b) = m.c.m.(b, a)**

(3) $\forall a, b \in \mathbb{Z}$, $a \neq 0$ y $b \neq 0$, se cumple **m.c.m.(a, b) = m.c.m.$(|a|, |b|)$**

Mínimo común múltiplo

(4) $\forall a, b \in \mathbb{N}_1$, se cumple $\mathbf{m.c.d.}(a,b) \cdot \mathbf{m.c.m.}(a,b) = a \cdot b$

Dem: Sean
$d = \text{m.c.d.}(a,b)$, $m = \frac{a \cdot b}{d}$ y a_1, b_1 los enteros del lema de reducción,
con lo que $m = b_1 \cdot a$, $(m = \dot{a})$, $m = a_1 \cdot b$, $(m = \dot{b})$ y $m \in \mathbb{N}_1$.
Entonces para concluir $m = \text{m.c.m.}(a,b)$ basta con demostrar

$$\forall c \in \mathbb{N}_1 \ \ ((c = \dot{a}) \ \text{y} \ (c = \dot{b})) \ \rightarrow \ m \leq c$$

En efecto:

$$((c = \dot{a}) \ \text{y} \ (c = \dot{b})) \ \rightarrow \ (\exists\, r, s \in \mathbb{N}_1, \ c = r \cdot a \ \text{y} \ c = s \cdot b)$$

Por Th. Bézout: $\exists\, m_1, n_1 \in \mathbb{Z}, \ d = m_1 \cdot a + n_1 \cdot b$.

Dividiendo c entre m (puede dividirse por ser $m > 0$) :

$$\exists\, m_1, n_1 \in \mathbb{Z} \ \ \exists\, r, s \in \mathbb{N}_1, \ \ \frac{c}{m} = \frac{c \cdot d}{a \cdot b} = \frac{c \cdot (m_1 \cdot a + n_1 \cdot b)}{a \cdot b} = \frac{c}{b} \cdot m_1 + \frac{c}{a} \cdot n_1$$
$$= \frac{s \cdot b}{b} \cdot m_1 + \frac{r \cdot a}{a} \cdot n_1 = s \cdot m_1 + r \cdot n_1 \in \mathbb{N}_1$$

Luego $c = (s \cdot m_1 + r \cdot n_1) \cdot m$ con $s \cdot m_1 + r \cdot n_1 \in \mathbb{N}_1$,
de modo que $m \,|\, c$ y por tanto $m \leq c$ (por ser $m, c > 0$)

.

Números primos

Def:

Un número entero p es primo si $p \geq 2$ y los únicos divisores **positivos** *de p son el 1 y el propio p*

Def:

Un número entero $x \geq 2$ es **compuesto** *cuando no es primo; es decir si existe una "factorización" $x = k \cdot l$ que expresa x como producto de dos enteros k y l, tales que $1 < k < x$ y $1 < l < x$*

Obs:

- Todo entero n tiene a $1, n, -1$ y $-n$ como divisores, a los que se llama divisores triviales, mientras que los demás divisores (si los tiene) son divisores propios. Entonces un número entero $p \geq 2$ es primo si no tiene divisores propios o, equivalentemente, si sus únicos divisores son los triviales.
- 2 es el menor número primo y todos los demás números positivos pares son compuestos (pues tienen a 2 como divisor propio).
- El 1 ni es primo, ni es compuesto: ($1 \ncong 2$) y sólo tiene divisores triviales (1 y -1).
- El 0 ni es primo, ni es compuesto: ($0 \ncong 2$) y aunque tiene infinitos divisores propios, no puede factorizarse como producto de enteros positivos.
- Los números enteros negativos se dividen en tres clases: -1, los opuestos de los números primos y los opuestos de los números compuestos.

Proposición

$\forall\, a \in \mathbb{Z}\ \ \forall\, p \in \mathbb{Z},\ p$ primo, se tiene que

$$\text{m.c.d.}(p, a) = \begin{cases} p & \text{si} \quad p \mid a \\ 1 & \text{si} \quad p \nmid a \end{cases}$$

Dem: Los únicos posibles divisores positivos comunes de p y a son 1 y p.

Proposición

Si p es primo y $x_1, x_2, \cdots, x_n$ son enteros tales que $p \mid x_1 \cdot x_2 \cdot \ldots \cdot x_n$, entonces $p \mid x_i$ para algún i con $1 \leq i \leq n$.

Dem: Por inducción simple sobre n, con $n \geq 1$.

$$\text{P(n):} \quad p \left| \prod_{i=1}^{n} x_i \right. \rightarrow \exists\, j \in \{1, \cdots, n\},\ p \mid x_j$$

Caso base: n $= 1$ $p \mid x_1$ Trivial

Paso inductivo: Sea k $\in \mathbb{Z}$, $k \geq 1$

HI: P(k): $p \left| \prod_{i=1}^{k} x_i \right. \rightarrow \exists\, j \in \{1, \cdots, k\},\ p \mid x_j$

¿P(k) $\rightarrow$ P(k+1) ?

¿P(k) $\to$ P(k+1) ?

Sea $x = \prod_{i=1}^{k} x_i$

Subcaso i) $p \mid x \to \exists\, j \in \{1, \cdots, k\} \subseteq \{1, \cdots, k+1\},\ p \mid x_j$ [HI]

Subcaso ii) $p \nmid x \to$ m.c.d.$(p, x) = 1$ [p primo]

$\to \exists\, m, n \in \mathbb{Z},\ 1 = m \cdot p + n \cdot x$ [Th. Bézout]

$\to \exists\, m, n \in \mathbb{Z},\ x_{k+1} = (m \cdot p + n \cdot x) \cdot x_{k+1}$

$\to \exists\, m, n, l \in \mathbb{Z},\ x_{k+1} = (\underbrace{m \cdot x_{k+1} + n \cdot l}_{\in \mathbb{Z}}) \cdot p$ [$p \mid x \cdot x_{k+1}$]

$\to p \mid x_{k+1}$

Luego $\exists\, j \in \{1, \cdots, k+1\},\ p \mid x_j$

Ejercicio: Escribe una demostración alternativa del Subcaso ii) usando el Lema de Euclides.

Teorema fundamental de la aritmética

$\forall\, n \in \mathbb{N},\ \ n \geq 2$ puede expresarse de forma única (salvo el orden de los factores) como

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_m^{e_m}$$

dónde $p_1, p_2, \cdots, p_m$ son primos distintos y $m, e_1, e_2, \cdots, e_m \in \mathbb{N}_1$
(es decir $\forall\, n \in \mathbb{N}\ \ n \geq 2$, su descomposición en factores primos es única)

Dem:

Parte 1 : Todo $n \in \mathbb{N}_2$ puede descomponerse en factores primos

Lo demostraremos por inducción completa sobre n.

Caso base:

n = 2 Obvio: m = 1, $e_1 = 1$, $p_1 = 2$

Paso inductivo completo: Dado $k > 2$

HIC: $\forall$ l , $2 \leq$ l $<$ k, l puede descomponerse en factores primos

CIC: k puede descomponerse en factores primos

Caso i) k es primo, Obvio: m = 1, $p_1 = k$, $e_1 = 1$

Caso ii) k es compuesto, es decir $\exists\, a, b \in \{2, 3, \cdots, k-1\}$ tales que k=$a \cdot b$

Por HIC a y b pueden descomponerse en factores primos
y por tanto también k = $a \cdot b$

Luego $\forall\, n \in \mathbb{N}_2$, n puede descomponerse en factores primos

Parte 2 : $\forall n \in \mathbb{N}_2$ su descomposición en factores primos es única

Lo demostraremos por inducción completa sobre n.

Caso base:

n = 2 Obvio: m = 1, $e_1 = 1$, $p_1 = 2$

Paso inductivo completo: Dado $k > 2$

HIC: $\forall$ l , $2 \leq$ l $<$ k, la descomposición en factores primos de l es única

CIC: la descomposición de k en factores primos es única

Caso i) k es primo, Obvio: m = 1, $p_1 = k$, $e_1 = 1$

Caso ii) k es compuesto.

Supongamos que k puede descomponerse en factores primos de dos formas distintas $k = \prod_{i=1}^{s} p_i$, con p_i primos no necesariamente distintos para $1 \leq i \leq s$ y $k = \prod_{j=1}^{r} q_j$, con q_j primos no necesariamente distintos para $1 \leq j \leq r$. Obviamente $s, r > 1$, por ser k compuesto.

$$\begin{aligned} k = \prod_{i=1}^{s} p_i &\to p_1 \mid k \\ &\to p_1 \mid q_1 \cdot q_2 \cdots q_r \\ &\to p_1 \mid q_j \text{ para algún } j \in \{1, \cdots, r\} \\ &\to p_1 = q_j \text{ para algún } j \in \{1, \cdots, r\} \quad \text{[por ser } p_1 \text{ y } q_j \text{ primos]} \end{aligned}$$

Sea $a = p_2 \cdot p_3 \cdots p_s$. Entonces $k = p_1 \cdot a = q_j \cdot a = q_j \cdot \prod_{u=1, u \neq j}^{r} q_u$.

Luego $a = p_2 \cdot p_3 \cdots p_s = \prod_{u=1, u \neq j}^{r} q_u$, lo que es absurdo, pues al ser $2 \leq a < k$ por la HIC, su descomposición en factores primos ha de ser única.

Para cualquier primo existe otro primo mayor.

Infinitud del conjunto de los números primos

Teorema: Si p es primo, cualquier factor primo de $1+p!$ es mayor que p.

Dem: Sean p y q primos tales que $q \,|\, (1+p!)$.

Supongamos que $q \leq p$

$$q \,|\, (1+p!) \quad \to \exists\, n \in \mathbb{Z}_1 \;\; 1+p! = n \cdot q \qquad [q, p \geq 2]$$

$$\begin{aligned} (2 \leq q \leq p) \quad & \to q \,|\, p! \to \exists\, m \in \mathbb{Z}_1 \;\; p! = m \cdot q \\ & \to \exists\, n, m \in \mathbb{Z}_1 \;\; n \cdot q = 1 + p! = 1 + m \cdot q \\ & \leftrightarrow \exists\, n, m \in \mathbb{Z}_1, \;\; (n-m) \cdot q = 1 \\ & \to q \,|\, 1 \qquad \text{lo que es absurdo pues } \; q \geq 2 \end{aligned}$$

Cálculo del máximo común divisor y del mínimo común múltiplo usando descomposiciones en factores primos

Dadas las descomposiciones de a y b en factores primos:

- Los factores primos del máximo común divisor tienen que ser divisores comunes de a y b, luego para calcular m.c.d.(a,b) hay que quedarse con esos divisores primos comunes elevados al menor exponente con que aparezcan en ambas factorizaciones.
- Cada uno de los factores primos de a o de b debe serlo del mínimo común múltiplo, luego para calcular m.c.m.(a,b) hay que quedarse con todos los divisores primos de a o de b, elevados al mayor exponente con que aparezcan en sus factorizaciones.

Ej:

$$a = 360 = 2^3 \cdot 3^2 \cdot 5 \qquad \text{m.c.d.}(360, 336) = 2^3 \cdot 3 = 24$$

$$b = 336 = 2^4 \cdot 3 \cdot 7 \qquad \text{m.c.m.}(360, 336) = 2^4 \cdot 3^2 \cdot 5 \cdot 7 = 5040$$