Múltiplos y divisores

$a, b \in \mathbb{Z}$; $a \neq 0$; $n \in \mathbb{Z}$

Si $b = n \cdot a \rightarrow \begin{cases} a \text{ es divisor de } b \quad \frac{b}{a} = n \\ b \text{ es múltiplo de } a \end{cases}$

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

Si a y b son múltiplos de $c \rightarrow a+b$ y $a-b$ también lo son, igual que lo es $a \cdot b$

MCD y MCM

MCD(a, b): el mayor entero que divide a ambos.

Producto de factores primos comunes con menor exponente

MCM(a, b): menor entero múltiplo de ambos

Producto de factores comunes y no comunes al mayor exponente.

$24 = 2^3 \cdot 3$; $126 = 2 \cdot 3^2 \cdot 7$

$$\begin{array}{r|l} 24 & 2 \\ 12 & 2 \\ 6 & 2 \\ 3 & 3 \\ 1 & \end{array} \qquad \begin{array}{r|l} 126 & 2 \\ 63 & 3 \\ 21 & 3 \\ 7 & 7 \\ 1 & \end{array}$$

$MCD = 2 \cdot 3 = 6$

$MCM = 2^3 \cdot 3^2 \cdot 7 = 126 \cdot 4 = 504$

Divisor: Número que divide a otro número dejando un resto de 0.

Múltiplo. Número que resulta de multiplicar el número del que es múltiplo y otro entero

Cociente y resto

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

$a > 0 \rightarrow \exists! c \in \mathbb{Z} \wedge \exists! r \in \mathbb{Z}$, $r < a$ de manera que

$b = a \cdot c + r$ $\quad$ $\begin{array}{r|l} b & a \\ \hline r & c \end{array}$

Además, si r es 0, $b = a \cdot c$, de modo que a es divisor de b, y b es múltiplo de a

Alg. de Euclides para el MCD

Dada fórmula de la división: $b = a \cdot c + r$.

Si hacemos la división $\frac{b}{a} \rightarrow MCD(b,a) = MCD(a,r)$,

pero el primer término ha de ser mayor.

$$\underline{b > a > 0}$$

$$\hookrightarrow 2x + 1y \overset{x,\, b<a}{=} c \longleftrightarrow +1x + 2y \overset{\checkmark,\, b>a}{=} c$$

$$MCD(b,a) \begin{cases} r = 0 \rightarrow a \text{ divide a } b \rightarrow MCD(b,a) = a \\ r \neq 0 \rightarrow MCD(a,b) = MCD(a, r_1) \end{cases}$$

$$MCD(a, r_1) \begin{cases} r_1 = 0 \rightarrow MCD(a, r_1) = r_1 \\ r_1 \neq 0 \rightarrow MCD(a, r_1) = MCD(r_1, r_2) \end{cases}$$

...

$MCD(845, 155) = MCD(155, 845 \pmod{155}) =$

$MCD(155, 70) = MCD(70, 155 \pmod{70}) =$

$MCD(70, 15) = MCD(15, 10) = MCD(10, 5) =$

$MCD(5, 0) = 5$

$$\begin{array}{r|l} 845 & 155 \\ \hline 70 & 5 \end{array}$$

$$\begin{array}{r|l} 155 & 70 \\ \hline 15 & 2 \end{array}$$

Tabla

i		0	1	2	3	4	5
	coc						
divid	divis						
resto							

MCD(126, 24) = 6

i		0	1	2	3	4	5
	coc		5	4			
divid	divis	126	24	6	0		
resto		6	0				

Números fraccionales y fracciones continuas

Cualquier racional se puede expresar como una fracción de enteros:

$$\forall q \in \mathbb{Q}, \exists a, b \in \mathbb{Z} ; q = \frac{b}{a}$$

También se pueden representar como fracciones:

$$q = p, a_1 a_2 a_3 a_4 \cdots$$

Donde p y a_i son dígitos entre el 0 y el 9.

Por último, se puede representar en forma de fracción continua:

$$q = [q_1 ; q_2, q_3, \dots, q_n, \dots], \text{ o}$$

$$q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{\ddots \, q_n + \cfrac{1}{\cdots}}}}$$

Eg.: $q = [4; 1, 5, 3, 2]$

$$4+\cfrac{1}{1+\cfrac{1}{5+\cfrac{1}{3+\cfrac{1}{2}}}} = 4+\cfrac{1}{1+\cfrac{1}{5+\cfrac{1}{\frac{7}{2}}}} = 4+\cfrac{1}{1+\cfrac{1}{5+\frac{2}{7}}} =$$

$$= 4+\cfrac{1}{1+\cfrac{1}{\frac{35+2}{7}}} = 4+\cfrac{1}{1+\frac{7}{37}} = 4+\cfrac{1}{\frac{37+7}{37}} = 4+\frac{37}{44} =$$

$$\frac{4\cdot 44+37}{44} = \frac{176+37}{44} = \frac{213}{44}$$

Eg.: $q = \frac{213}{44}$

$b = 213 \quad a = 44$

$b = ac + r$

$213 \,\underline{|\, 44}$
$37 \quad 4$

$44 \,\underline{|\, 37}$
$7 \quad 1$

$44 = 37 + 7$

$213 = 4\cdot 44 + 37$

$$\frac{213}{44} = \frac{4\cdot 44+37}{44} = 4+\frac{37}{44} = 4+\cfrac{1}{\frac{44}{37}} = 4+\cfrac{1}{\frac{37+7}{37}} = 4+\cfrac{1}{1+\frac{7}{37}}$$

...

Euclides con fracciones continuas.

$b = a \cdot c + r \rightsquigarrow b = a \cdot q_1 + r_1$; $\begin{matrix} c = q_1 \\ r = r_1 \end{matrix}$

$\begin{array}{l|l} b & a \\ \hline r_1 & q_1 \end{array}$ $\quad b = a \cdot q_1 + r_1$

$\begin{array}{l|l} a & r_1 \\ \hline r_2 & q_2 \end{array}$ $\quad a = r_1 \cdot q_2 + r_1$

$$\left.\begin{array}{l} \begin{array}{l|l} r_1 & r_2 \\ \hline r_3 & q_3 \end{array} \quad r_1 = r_2 \cdot q_3 + r_3 \\ \\ \begin{array}{l|l} r_2 & r_3 \\ \hline r_4 & q_4 \end{array} \quad r_2 = r_3 \cdot q_4 + r_4 \end{array}\right\} \; r_i = r_{i+1} \cdot q_{i+2} + r_{i+2}$$

Fracciones reducidas:

Al expresar un racional en forma de decimal, se puede aproximar a K cifras decimales y sacar a partir de ahí una fracción continua reducida.

$$\frac{b}{a} = [q_1] = (1^{ra} \text{ aprox.}) = \frac{P_1}{Q_1}$$

$$[q_1; q_2] = (2^{da} \text{ aprox.}) = \frac{P_2}{Q_2}$$

$$[q_1; q_2, q_3] = (3^{ra} \text{ aprox.}) = \frac{P_3}{Q_3}$$

$$\cdots$$

$$[q_1; q_2, q_3, \ldots, q_K] = (K^{ma} \text{ aprox.}) = \frac{P_K}{Q_K}$$

$$\frac{b}{a} = q = [q_1; q_2, q_3, \dots, q_k]$$

$$q = [q_1] = q_1 = \frac{P_1}{Q_1} = \begin{cases} P_1 = q_1 \\ Q_1 = 1 \end{cases}$$

$$q = [q_1; q_2] = q_1 + \frac{1}{q_2} = \frac{q_1 \cdot q_2 + 1}{q_2} = \frac{P_2}{Q_2} = \begin{cases} P_2 = q_1 \cdot q_2 + 1 \\ Q_2 = q_2 \end{cases}$$

$$P_2 = q_1 \cdot q_2 + 1 = P_1 \cdot q_2 + 1$$

$$Q_2 = q_2$$

$$q = [q_1; q_2, q_3] = q_1 + \frac{1}{q_2 + \frac{1}{q_3}} = q_1 + \frac{1}{\frac{q_2 \cdot q_3 + 1}{q_3}} = q_1 + \frac{q_3}{q_2 \cdot q_3 + 1} =$$

$$= \frac{q_1 \cdot q_2 \cdot q_3 + q_1 + q_3}{q_2 \cdot q_3 + 1} = \frac{q_3(q_1 \cdot q_2 + 1) + q_1}{q_3 \cdot q_2 + 1} = \frac{q_3 P_2 + P_1}{q_3 Q_2 + Q_1} = \frac{P_3}{Q_3}$$

$$\left.\begin{matrix} P_3 = q_3 P_2 + P_1 \\ Q_3 = q_3 Q_2 + Q_1 \end{matrix}\right\} \rightarrow \begin{matrix} P_k = q_k P_{k-1} + P_{k-2} \\ Q_k = q_k Q_{k-1} + Q_{k-2} \end{matrix}$$

$$\frac{P_k}{Q_k} = \frac{q_k P_{k-1} + P_{k-2}}{q_k Q_{k-1} + Q_{k-2}} = \frac{b}{a} = q$$

Talla

i	0	1	2	3	4	5
P_i	$\underline{1}$	$\underline{q_1}$	$q_2 P_1 + 1$	$q_3 P_2 + P_1$		
Q_i	0	$\underline{1}$	$q_2 \cdot 1 + 0$	$q_3 Q_2 + 1$		

$$P_k = q_k P_{k-1} + P_{k-2}$$

$$P_1 = q_1 \cdot 1 + 0$$

$$\begin{cases} q_k = q_1 \\ P_{k-1} = 1 \rightarrow P_0 = 1 \\ P_{k-2} = 0 \end{cases}$$

(Misma lógica para Q_0)

Euclides con fracciones reducidas

(euclides)

	i	0	1	2	3	4	5	
	coc		q_1	q_2	q_3	q_4	q_5	…
divid	divis	b	a	r_1	r_2	r_3	r_4	…
resto		r_1	r_2	r_3	r_4	r_5	r_6	…
	P_k	1	q_1	$q_2 p_1 + 1$	$q_3 p_2 + p_1$			
	Q_k	0	1	q_2	$q_3 Q_2 + 1$			

En la tabla del algoritmo de Euclides está todo lo necesario para aplicar la fórmula de las fracciones parciales.

Ecuaciones diofánticas

Son de la forma $ax + by = c$,
donde $a, b \in \mathbb{Z}$ y $x, y \in \mathbb{Z}$

Se cumple que $MCD(a, b) = MCD(a, m)$,
y que al hallar $MCD(a, b)$ se puede
comprobar si hay soluciones, cuantas hay
y que forma tienen.

Si tiene solución, se le denomina compatible, si
no, es incompatible. Al proceso de determinar
si es o no compatible se le llama discusión

$$4x + 5y = 8 \xrightarrow{\text{soluciones}} \begin{cases} (0,2) \\ (7,-4) \\ (-3,4) \end{cases}$$

$$6x + 9y = 2 \leftrightarrow 3(2x + 3y) = 2 \leftrightarrow 2x + 3y = \frac{2}{3} \quad X$$

No es diofántica, no tiene solución

Propiedades

1.- Si es compatible $\rightarrow$ MCD(a, b) divide a c.

2.- Si (x_0, y_0) es solución $\rightarrow$ (x, y) donde $\begin{matrix} x = x_0 + b \cdot K \\ y = y_0 - a \cdot K \end{matrix}$, $K \in \mathbb{Z}$, también son soluciones (es decir, todos los múltiplos de (x, y)).

$4x + 5y = 8 \rightarrow (2,0)$ es solución.

$K = 2$, $x = 2 + 5 \cdot 2 = 12$; $y = 0 - 4 \cdot 2 = -8$

$\hookrightarrow 4 \cdot 12 + 5(-8) = 8 \leftrightarrow 48 - 40 = 8 \leftrightarrow 8 = 8$ ✓

$K = -3$, $x = 2 + 5 \cdot (-3) = -13$; $y = 0 - 4 \cdot (-3) = 12$

$\hookrightarrow 4 \cdot (-13) + 5 \cdot 12 = 8 \leftrightarrow -52 + 60 = 8 \leftrightarrow 8 = 8$ ✓

Teorema de Bézout

$a, b \in \mathbb{Z}$; $a \neq 0$; $b \neq 0$

Si $m = MCD(a,b) \rightarrow \exists p, q \in \mathbb{Z}$ de modo que:

$$ap + bq = m$$

Ids. de Bézout

(ecuación diofántica)

$$\begin{array}{r|l} b & a \\ \hline r_1 & q_1 \end{array} \rightarrow b = a \cdot q_1 + r_1 \leftrightarrow r_1 = b - a \cdot q_1 = -a \cdot \overset{P_1}{q_1} + b \cdot \overset{Q_1}{1} =$$

$$= -aP_1 + bQ_1$$

$$\begin{array}{r|l} a & r_1 \\ \hline r_2 & q_2 \end{array} \rightarrow r_2 = a - r_1 \cdot q_2 = -r_1 \cdot q_2 + a \cdot 1 =$$

$$= -(-aP_1 + bQ_1) \cdot q_2 + a \cdot 1 = +aP_1 q_2 - bQ_1 q_2 + a =$$

$$= +a(P_1 q_2 + 1) - bQ q_2 = aP_2 - bQ_2$$

$$\begin{array}{r|l} r_1 & r_2 \\ \hline r_3 & q_3 \end{array} \rightarrow r_3 = r_1 - r_2 \cdot q_3 = -r_2 \cdot q_3 + r_1 =$$

$$= -(aP_2 - bQ_2)q_3 + (-aP_1 + bQ_1) =$$

$$= -aP_2 q_3 + bQ_2 q_3 - aP_1 + bQ_1 =$$

$$= -a(P_2 q_3 + P_1) + b(P_2 q_3 + Q_1) = -aP_3 + bQ_3$$

$$m = r_i = (-1)(aP_i - bQ_i) \quad i \in \mathbb{N}$$

el último elemento

iteraciones del MCD(a,b)

Ej.: $a = 162$
$b = 136$

1.: $MCD(162, 136)$ ↪ m (resultado)
↪ i (iteraciones)

	i	0	1	2	3	4	5	6	7	8
	co (q_i)		1	5	4	3				
Divid	divis	162	136	26	6	2	0			
resto		26	6	2	0					
	P_i	1	1	6	25					
	Q_i	0	1	5	21					

$$MCD(162, 136) \begin{cases} m = 2 \\ i = 4 - 1 = 3 \end{cases}$$

2.: Bézout

$$m = r_4 = (-1)^3 (aP_3 - bQ_3) = aP_3 - bQ_3 = a \cdot 25 + b \cdot 21$$

$p = -25$; $q = +21$

$$m = ap + bq = 162p + 136q$$

$$m = 162 \cdot (-25) + 162 \cdot 21 = -3400 + 3402 = 2$$

$m = 2$ ✓

$a = 81 \quad b = 24$

	i	0	1	2	3	4	5	6	7	8
	cc (q_i)		3	2	1	2				
Divid	divis	81	24	9	6	3,	0			
resto		9	6	3	0					
	P_i	$\underline{1}$	3	7	10	27				
	Q_i	$\underline{0}$	$\underline{1}$	2	3	8				

$$MCD(81, 24) \begin{cases} m = 3 \\ i = 3 \end{cases} \quad b > a > 0$$

$$m = a \cdot p + b \cdot q = 81p + 24q = 24p + 81q$$

$$m = r_4 = (-1)^3 (aP_3 - bQ_3) = -aP_3 + bQ_3 = -10a + 3b$$

$$p = -10 \; ; \; q = 3$$

$$m = 24 \cdot (-10) + 81 \cdot 3 = -240 + 243 = 3 \checkmark$$

!! Aplicado a la diofántica

$$ax+by=c \longleftrightarrow \frac{c}{m} \in \mathbb{Z} \longleftrightarrow \left(\frac{ax}{m}+\frac{by}{m}\right) \in \mathbb{Z}$$

$a,b,c = \mathbb{Z}$; $x,y \in \mathbb{Z}$; $m = MCD(a,b)$

Es decir, si el MCD de a y b divide a c, la ecuación tiene, por lo menos, una solución. Además, se podrá simplificar la ecuación dividiendo por el MCD.

Si consideramos que $p = x_0$ y $q = y_0$, tenemos además que las soluciones son de la forma:

$$(\underbrace{p+b\cdot k}_{x}, \underbrace{q-a\cdot k}_{y})$$

Congruencia en $\mathbb{Z}$

$a, b \in \mathbb{Z}$, $p > 1$.

$$a \equiv b \pmod{p} \longleftrightarrow a - b = p \cdot K, \; K \in \mathbb{Z}$$

$$\longleftrightarrow \begin{array}{l|l} a & p \\ \hline r_a & q_a \end{array} \; y \; \begin{array}{l|l} b & p \\ \hline r_b & q_b \end{array} \rightarrow r_a = r_b = r$$

$$\updownarrow$$

$$a = p q_a + r \wedge b = p q_b + r \leftrightarrow r = a - p q_a = b - p q_b$$

$$[a] = [a \cdot p \cdot K], \; K \in \mathbb{Z} \qquad [a]$$

$$[a] = \{ x \in \mathbb{Z} \mid x R a \} = \{ x \in \mathbb{Z} \mid x - a = p \cdot K \} =$$

$$= \{ x \in \mathbb{Z} \mid x = a + p \cdot K \}$$

$$\mathbb{Z}_p = \{ [0], [1], [2], \ldots, [p-1] \}$$

Aritmética Modular

Son operaciones con clases:

$[a]+[b]=[a+b]$; $[a]\cdot[b]=[a\cdot b]$

$[a]\cancel{-[b]}=[a]+[b]^{-1}$ ⇝ No se puede restar clases.

El inverso $[a]^{-1}$ existe si y sólo si:

1) $\exists [x]\in\mathbb{Z}_m$ $[a\cdot x]=[1]$

11) $\exists_x\in\mathbb{Z}$ $(a\cdot x)-1=m\cdot K,\ K\in\mathbb{Z}$

111) $\exists x,y\in\mathbb{Z}$ $1=a\cdot x+m\cdot y$

Aplicando Bézout sobre la 111, tenemos que...

$[a]$ tiene inverso si y sólo si $MCD(a,m)=1$

Además en este caso, $[a]^{-1}=[x]$, donde x forma parte de la ecuación $1=a\cdot x+m\cdot y$. Es decir, habrá que encontrar la identidad de Bézout correspondiente a x, (la P_i).

Ej.: ¿∃! $[11]^{-1}$ $\mathbb{Z}_{27}$? ⇝ $1 \equiv 11 \pmod{27}$

$11x + 27y = 1$

$$MCD(27, 11) \begin{cases} p = 1 \checkmark \text{ tiene inversa} \\ i = 3 - 1 = 2 \end{cases}$$

	i	0	1	2	3	4
	coc		2	2	5	
divid	divis	27	11	5	1	0
resto		5	1	0		
	P_i	1	2	5		
	Q_i	0	1	2		

Bézout: $11x + 27y = 1$

$$1 = (-1)^2 (aP_2 - bQ_2) = a \cdot 5 - b \cdot 2 \begin{cases} x_0 = 5 \\ y_0 = -2 \end{cases}$$

$11 \cdot 5 + 27 \cdot (-2) = 55 + 54 = 1 \checkmark$

$(5, -2)$ son solución

↳ $(5 + 27 \cdot K, -2 - 11 \cdot K)$, $K \in \mathbb{Z}$ son soluciones.

$[a]^{-1} = [x_0]^{-1} \leftrightarrow [11]^{-1} = [5]$, en $\mathbb{Z}_{127}$

Ecuaciones en congruencias

Son expresiones del tipo $a \cdot x \equiv b \pmod{m}$

$\exists x \in \mathbb{Z} \quad [a] \cdot [x] \equiv [b]$ en $\mathbb{Z}_m$

$\Updownarrow$

$\exists x \in \mathbb{Z} \quad a \cdot x \equiv b \pmod{m}$

$\Updownarrow$

$\exists x \in \mathbb{Z} \quad ax - b = m \cdot K \leftrightarrow b = ax - mK$

$\Updownarrow$

$y = -K$

$\exists x, y \in \mathbb{Z} \quad b = ax + my \leftarrow$ Diofántica

$\Updownarrow$

$MCD(a, m) = b \cdot K, \; K \in \mathbb{Z} \leftrightarrow MCD(a, m) \mid b$

$a \cdot x \equiv b \pmod{m}$ solo tiene solución si se cumple esto.

$a, b \in \mathbb{Z}$, $b \neq 0$, $a \neq 0$, $d = MCD(a, m)$

$[a] \cdot [x] = [b]$ en $\mathbb{Z}_m \leftrightarrow ax \equiv b \pmod m$

solución si $MCD(a, m) = b \cdot K$

- Si $MCD(a, m) = 1$, existe $[a]^{-1}$, que se puede multiplicar a ambos lados de la ecuación, despejando así $[x]$

$$[a] \cdot [x] = [b] \leftrightarrow [x] = [a]^{-1} \cdot [b]$$

- Si $MCD(a, m) \neq 1 \wedge MCD(a, m) \mid b$

$d = MCD$.
La ecuación tiene d soluciones, de la forma

$s, s + \frac{m}{d}, s + 2\frac{m}{d}, s + 3\frac{m}{d}, \dots$

donde s: $\left[\frac{a}{d}\right] \cdot [x] = \left[\frac{b}{d}\right]$, en $\mathbb{Z}_{m/d}$, que solo tiene una solución $\leadsto MCD\left(\frac{a}{d}, \frac{m}{d}\right) = 1$

- Si no se da ninguno de estos casos, no hay solución.

Ej.: $[5]\cdot[x]=[2]$ en $\mathbb{Z}_7 \leftrightarrow \underset{a}{5}x \equiv \underset{b}{2} \pmod{\underset{m}{7}}$

$MCD(a,m) = MCD(5,7) = 1 \rightsquigarrow$ 1 solución

¿$[5]^{-1}$ en $\mathbb{Z}_7$? — $b>a>0$ ✓ ← El orden importa en Bézout

$5x+7y=1 \rightsquigarrow$ Diofántica $\rightsquigarrow$ Bézout

$MCD(b,a) \begin{cases} r=1 ✓ \\ i=3-1=2 \end{cases}$

	i	0	1	2	3	4	5	6
	q		1	2				
do	d_i	7	5	2	1	0		
r		2	1	0				
	P_i	1	1	3				
	Q_i	0	1	2				

$1 = (-1)^2 (aP_2 - bQ_2) = a3 - b2 \begin{cases} x_0 = 3 \\ y_0 = -2 \end{cases}$

$1 = 5\cdot 3 + 7\cdot(-2) = 15 - 14 = 1$ ✓

$[5]^{-1}$ en $\mathbb{Z}_7 = 3$

$[x] = [3]\cdot[2] = [6]$

Ej.: $4x \equiv 4 \pmod 6$ $\quad MCD(4,6) = \underline{2}$,

$\uparrow$ a $\quad \uparrow$ b $\quad \uparrow$ m $\quad$ ↳ 2 soluciones

$2 \neq 1 \wedge 2 | b$ ← 4

¿s? → $2x \equiv 2 \pmod 3$ $\quad MCD(2,3) = 1$

Bezout: $2x + 3y = 1$ ← b>a>0 ✓ MCD (3,2)

i	0	1	2	3
q		1	2	
do dr	3	2	1,	0
r	1	0		
P_i	1	1	3	
Q_i	0	1	2	

mcd = 1

$i = 2 - 1 = 1$

$1 = -aP_1 + mQ_1 = -a + m \begin{cases} x_0 = -1 \\ y_0 = 1 \end{cases}$

(según el g. correcto es [1], no [2])

$x_0 < 0$, no vale

$(2, -1)$ también es solución

$[2]^{-1} = [2]$ en $\mathbb{Z}_3$ ⟶ $[x] = [2]$

$\overset{a}{2} \cdot \overset{x}{2} - 1 = 3 \cdot 1$ ✓

$[4] = [1] = $ ✓

Sol.: $[2], [2+3]$