

MATEMATICA DISCRETA

UNIDAD 3

# DIVISIBILIDAD EN $\mathbb{Z}$



**-435**

**5**

**-7**

**1**

**44**

**0**

**-24**

Autor: Ing. María Alicia Piñeiro

# CONJUNTO DE LOS NUMEROS ENTEROS

En esta unidad vamos a trabajar en el conjunto  $\mathbb{Z}$  de los números enteros.

Recordemos que el conjunto de los números enteros es:

$$\mathbb{Z} = \mathbb{N} \cup \{0\} \cup \{-x / x \in \mathbb{N}\}$$

O bien:  $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$

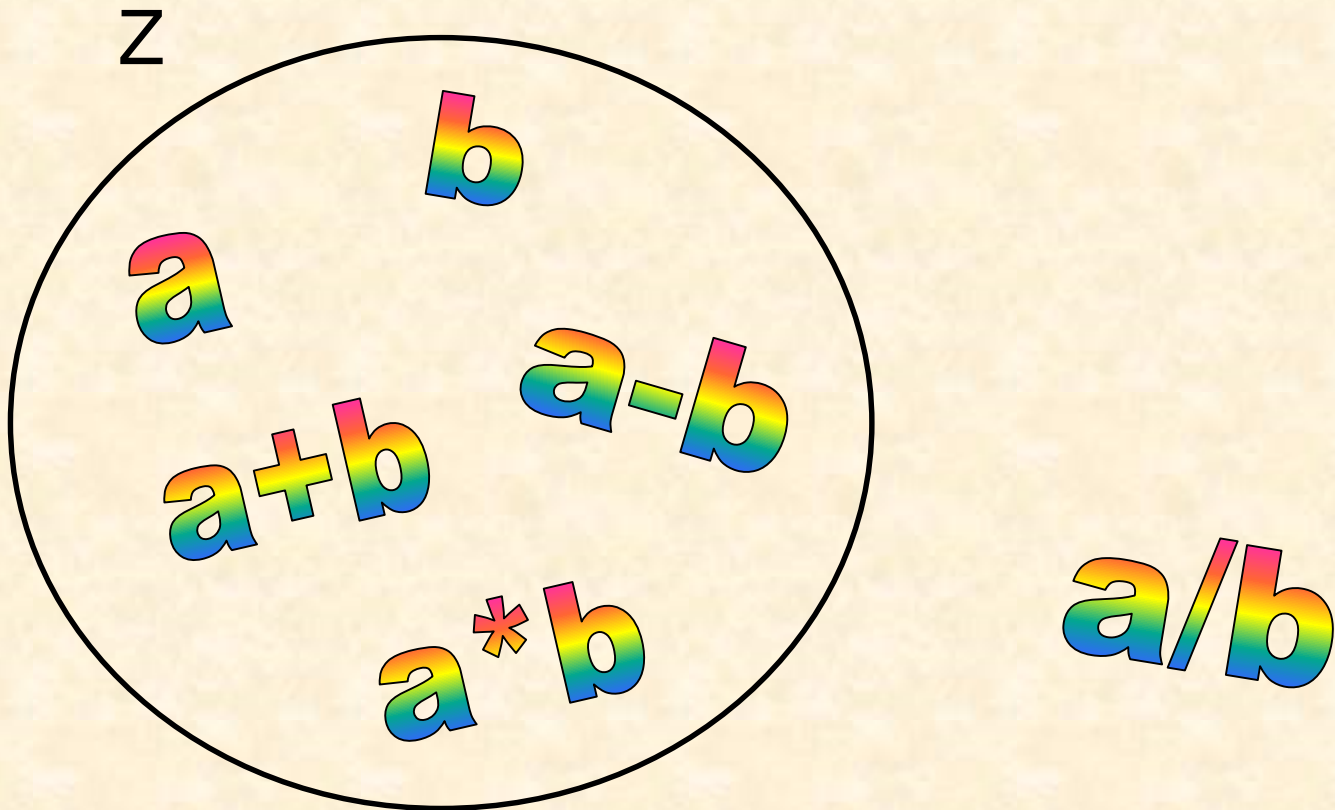
Y lo representamos:



# OPERACIONES CON NUMEROS ENTEROS

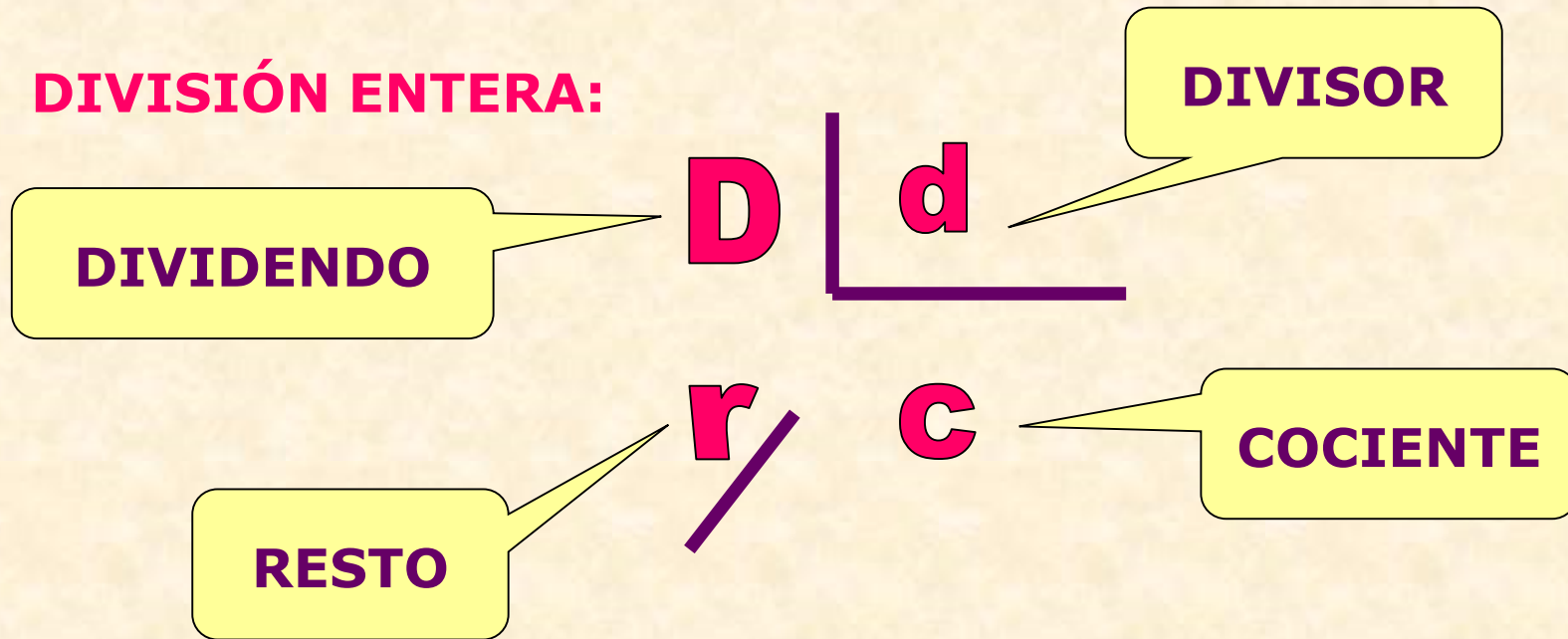
En el conjunto  $\mathbb{Z}$ , la adición, la sustracción y la multiplicación son operaciones cerradas, es decir, siempre se pueden efectuar y devuelven un resultado entero.

Pero con la división no pasa lo mismo, pues por ejemplo, si queremos dividir 8 por 3 ningún número entero coincide.



Por ello es que definimos la “división entera”, tal cual la habías aprendido en la escuela primaria.

## **DIVISIÓN ENTERA:**



**Dados dos números enteros  $D$  y  $d$ , con  $d \neq 0$ ,  
existen y son únicos otros dos enteros  $c$  y  $r$  tales que:**

$$D = c d + r \quad \text{y} \quad 0 \leq r < |d|$$

Esto se llama **Algoritmo de la División** y se puede demostrar.



## Ejercicio:

Indica el cociente y el resto de las siguientes divisiones:

Dividendo	Divisor	Cociente	Resto
17	3		
-8	5		
-13	-4		
15	-6		

Las respuestas correctas son:

Dividendo	Divisor	Cociente	Resto
17	3	<b>5</b>	<b>2</b>
-8	5	<b>-2</b>	<b>2</b>
-13	-4	<b>4</b>	<b>3</b>
15	-6	<b>-2</b>	<b>3</b>

Podemos generalizar de la siguiente forma:

$$\text{Si } d > 0 : \quad c = \text{ent}(D/d) \quad \wedge \quad r = \text{mant}(D/d) \cdot d$$

Por ejemplo, en los dos primeros casos anteriores:

1) En reales:  $\frac{17}{3} = 5.666666666666666...$

entonces:  $c = \text{ent}\left(\frac{17}{3}\right) = 5 \quad \wedge \quad r = \text{mant}\left(\frac{17}{3}\right) \cdot 3 = 0.66666666... \cdot 3 = 2$

2) En reales:  $\frac{-8}{5} = -1.6$

entonces:  $c = \text{ent}\left(\frac{-8}{5}\right) = -2 \quad \wedge \quad r = \text{mant}\left(\frac{-8}{5}\right) \cdot 5 = 0.4 \cdot 5 = 2$

Si  $d < 0$ :

$$d' = -d \Rightarrow c' = \text{ent}(D/d') \wedge r' = \text{mant}(D/d') \cdot d'$$

$$\text{Luego: } c = -c' \wedge r = r'$$

Por ejemplo, en dos últimos casos anteriores:

$$3) \text{ Resolvemos: } \frac{-13}{4} \quad \text{en reales: } \frac{-13}{4} = -3.25$$

$$\text{entonces: } c' = \text{ent}\left(\frac{-13}{4}\right) = -4 \quad \wedge \quad r' = \text{mant}\left(\frac{-13}{4}\right) \cdot 4 = 0.75 \cdot 4 = 3$$

Por lo tanto el cociente y resto de la división de -13 por -4 son:  $c = -c' = 4 \quad \wedge \quad r = r' = 3$

$$4) \text{ Resolvemos: } \frac{15}{6} \quad \text{en reales: } \frac{15}{6} = 2.5$$

$$\text{entonces: } c' = \text{ent}\left(\frac{15}{6}\right) = 2 \quad \wedge \quad r' = \text{mant}\left(\frac{15}{6}\right) \cdot 6 = 0.5 \cdot 6 = 3$$

Por lo tanto el cociente y resto de la división de 15 por -6 son:  $c = -c' = -2 \quad \wedge \quad r = r' = 3$


## RELACION DE DIVISIBILIDAD:

Definimos en  $\mathbb{Z}$  una relación entre dos enteros de la siguiente forma:

$$\text{Sean } a, b \in \mathbb{Z} : a \mid b \Leftrightarrow \exists k \in \mathbb{Z} / b = k \cdot a$$

**DIVIDE A "b"**  
**ES DIVISOR DE "b"**

**DIVISIBLE POR "a"**  
**MULTIPLO DE "a"**

 **Ejemplo:**  $8 \mid 72$  ya que  $\exists 9 \in \mathbb{Z} \wedge 72 = 9 \cdot 8$



## Propiedades básicas de la relación de divisibilidad:

1)  $\forall a \in \mathbb{Z} : a \mid a$

2)  $\forall a, b, c \in \mathbb{Z} : a \mid b \text{ y } b \mid c \text{ entonces } a \mid c$

3)  $\forall a, b, c \in \mathbb{Z} : a \mid b \text{ y } a \mid c \text{ entonces } a \mid b + c$

4)  $\forall a, b, c \in \mathbb{Z} : a \mid b \text{ entonces } a \mid b \cdot c$



¿Te animas a demostrar estas cuatro propiedades? Si tienes dudas, puedes consultar a tus tutores.

## NUMEROS PRIMOS:

**Los números enteros positivos mayores que 1, que sólo son divisibles por 1, -1, n, -n**

Los primeros números primos son:

**2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, ...**

 **¿Cuántos crees que existen?** ..... Sí, son infinitos!!!

Los matemáticos han demostrado que existen infinitos números primos, pero aún no encontraron una fórmula general para obtenerlos.

 **¿Por qué son importantes los números primos?**

Las aplicaciones de los números primos son muchas y se los suele relacionar con técnicas de cifrado. Por ejemplo, en el caso del algoritmo denominado RSA, se obtiene una clave a través de la multiplicación de dos números primos mayores a 10100; dado que no existen formas de factorizar rápidamente una cifra tan alta con ordenadores convencionales, éste resulta muy confiable.

Los números primos también cumplen muchas propiedades que no cumplen los números compuestos (los que no son primos y son mayores que 1).

Por ejemplo, pensemos si el siguiente condicional es verdadero o falso:



Sean,  $n, a, b \in \mathbb{Z}$ : Si  $n \mid a \bullet b$  entonces  $n \mid a \vee n \mid b$

Este condicional es FALSO, pues por ejemplo:  $6 \mid 4 \bullet 9$  pero no es cierto que  $(6 \mid 4 \vee 6 \mid 9)$

En cambio si nos dijeran que el número  $n$  es primo, entonces sí la propiedad es cierta y se puede demostrar fácilmente. Es la que enunciamos a continuación:

**Propiedad:** Si  $p \mid a \bullet b \wedge p: \text{primo} \Rightarrow p \mid a \vee p \mid b$

Pero para poder demostrarla debemos repasar un poco mas de conceptos teóricos.

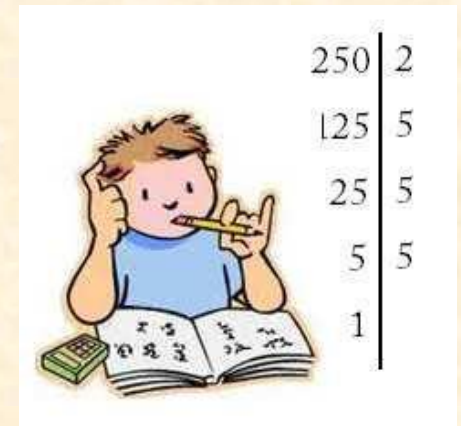
# TEOREMA FUNDAMENTAL DE LA ARITMÉTICA:

Este importante teorema establece lo siguiente:

Todo número entero es o bien primo o se puede escribir como producto de factores primos de manera única salvo el orden.

En forma simbólica:

$$n = p_1^{k_1} \cdot p_2^{k_2} \cdot \dots \cdot p_r^{k_r}$$



**Ejemplos:**

$$84 = 2^2 \cdot 3 \cdot 7$$

$$105 = 3 \cdot 5 \cdot 7$$

## M.C.M. (mínimo común múltiplo)

Sean  $a, b \in \mathbb{Z}$ , no simultáneamente nulos, y sea  $m \in \mathbb{Z}^+$ ,

$$m = \text{m.c.m.}(a,b) \begin{cases} 1) a \mid m \\ 2) b \mid m \\ 3) \text{ Si } m' > 0: a \mid m' \wedge b \mid m' \Rightarrow m \mid m' \end{cases}$$

Nota: Si  $a = 0 \vee b = 0$  entonces  $\text{m.c.m.}(a,b) = 0$

**Notación:**  $\text{m.c.m.}(a,b) = [a, b]$

## M.C.D (máximo común divisor)

Sean  $a, b \in \mathbb{Z}$ , no simultáneamente nulos, y sea  $d \in \mathbb{Z}^+$ ,

$$d = \text{m.c.d.}(a, b) \begin{cases} 1) d \mid a \\ 2) d \mid b \\ 3) \text{ Si } d' > 0: d' \mid a \wedge d' \mid b \Rightarrow d' \mid d \end{cases}$$

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

### Propiedad del MCD entre dos enteros:

Si  $d = \text{m.c.d.}(a, b)$  entonces  $\exists k_1, k_2 \in \mathbb{Z}$  tal que  $d = k_1 a + k_2 b$

Lo que dice esta propiedad, es que siempre el m.c.d. entre dos enteros se puede escribir como **combinación lineal entera** de ellos.

## Ejemplo:

Hallar el máximo común divisor entre 64 y 48  
y expresarlo como combinación lineal entera de ambos.

### **Solución:**

Primero factoreamos ambos números:  $64 = 2^6$        $48 = 2^4 \cdot 3$

Entonces:

$$\text{m.c.d.}(64,48) = 2^4 = 16$$

$$\text{m.c.m.}(64,48) = 2^6 \cdot 3 = 192$$

Y podemos escribir al 16 como combinación lineal entera de 64 y 48 de la siguiente forma:  $16 = 1 \cdot 64 + (-1) \cdot 48$





¿Cómo encuentro los dos enteros  $k_1$  y  $k_2$  para escribir al m.c.d.(a,b) como combinación lineal entera de ambos cuando “no se ven a simple vista”?

Una forma es utilizando el Algoritmo de Euclides para calcular el máximo común divisor por sucesivas divisiones.

Pero antes de eso, veamos dos propiedades:

$$\textbf{Propiedad del MCM y MCD:} \quad (a,b) [a,b] = |a b|$$

Con esta propiedad, conociendo uno de ellos (ya sea el m.c.m. o el m.c.d.) enseguida podemos encontrar el valor del otro.

En el ejemplo anterior se verifica:

El producto:  $16 \bullet 192$  es 3072 que es igual al producto  $64 \bullet 48 = 3072$



## Propiedad previa al Algoritmo de Euclides:

Dados dos enteros  $a$  y  $b$ , el  $\text{m.c.d.}(a,b) = \text{m.c.d.}(b,r)$   
siendo  $r$  el resto de la división de  $a$  por  $b$ .

### Demostración:

Para demostrar esta propiedad consideramos la siguiente definición:

$$D_{a,b} = \{ x \in \mathbb{Z} / x \mid a \wedge x \mid b \}$$

Es decir es el conjunto de todos los divisores comunes.

Si podemos demostrar que los conjuntos  $D_{a,b}$  y  $D_{b,r}$  son iguales, entonces quedará garantizado que el elemento mayor del primero conjunto es el mismo que del segundo.

## Solución:

Primero demostraremos que  $D_{a,b} \subseteq D_{b,r}$

$$\begin{aligned} \forall x \in D_{a,b} &\Rightarrow^{(0)} x \mid a \wedge x \mid b \Rightarrow^{(1)} x \mid b \cdot q + r \wedge x \mid b \wedge x \mid b \\ &\Rightarrow^{(2)} x \mid b \cdot q + r \wedge x \mid b \cdot (-q) \wedge x \mid b \\ &\Rightarrow^{(3)} x \mid b \cdot q + r + b \cdot (-q) \wedge x \mid b \Rightarrow \\ &\Rightarrow^{(4)} x \mid r \wedge x \mid b \Rightarrow x \in D_{b,r} \end{aligned}$$

*Justificaciones:*

- *Definición de  $D_{a,b}$*
- *Hipótesis  $a = b \cdot q + r$  e idempotencia de  $\wedge$*
- *Propiedad de divisibilidad (la n° 4 de la pag. 4)*
- *Propiedad de divisibilidad (la n° 3 de la pag. 4)*
- *Cancelamos números opuestos*
- *Definición de  $D_{b,r}$*

Falta probar la otra inclusión:  $D_{b,r} \subseteq D_{a,b}$  de manera análoga. Te la dejamos para que la practiques.

## Algoritmo de Euclides para calcular el máximo común divisor:

Dados dos enteros  $a$  y  $b$ , sabemos por la propiedad anterior, que  $\text{m.c.d.}(a,b) = \text{m.c.d.}(b,r)$  siendo  $r$  el resto de la división de  $a$  por  $b$ .

Volvemos a aplicar esta propiedad, es decir  $\text{m.c.d.}(b,r) = \text{m.c.d.}(r, r_1)$  siendo  $r_1$  el resto de la división de  $b$  por  $r$ . Luego  $\text{m.c.d.}(r, r_1) = \text{m.c.d.}(r_1, r_2)$  siendo  $r_2$  el resto de la división de  $r$  por  $r_1$ . Y así sucesivamente hasta llegar a un resto igual a cero. De esta manera se puede encontrar el m.c.d. entre dos enteros dados, ya que es el último resto no nulo.

Es decir, el algoritmo de Euclides consiste en calcular:

$$\text{m.c.d.}(a,b) = \text{m.c.d.}(b,r) \quad \text{siendo } a = b q + r$$

$$\text{m.c.d.}(b,r) = \text{m.c.d.}(r,r_1) \quad \text{siendo } b = r q_1 + r_1$$

$$\text{m.c.d.}(r, r_1) = \text{m.c.d.}(r_1, r_2) \quad \text{siendo } r = r_1 q_2 + r_2$$

■ ■ ■

$$\text{m.c.d.}(r_{n-1}, r_n) = \text{m.c.d.}(r_n, 0) \quad \text{siendo } r_{n-1} = r_n q_{n+1} + 0$$


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

## Ejemplo:

Vamos a calcular el m.c.d.(720, 224). Para ello realizamos las siguientes divisiones enteras sucesivas:

1)  $720 / 224 \Rightarrow c = 3 \wedge r = 48$

2)  $224 / 48 \Rightarrow c_1 = 4 \wedge r_1 = 32$

3)  $48 / 32 \Rightarrow c_2 = 1 \wedge r_2 = 16$

4)  $32 / 16 \Rightarrow c_3 = 2 \wedge r_3 = 0$

**m.c.d.(720,224) = 16**



Pero si ahora queremos escribir a dicho m.c.d. como combinación lineal entera de 720 y 224, ¿Cómo hacemos?

$$16 = \dots\dots\dots \cdot 720 + \dots\dots\dots \cdot 224$$

Para ello, es más práctica la forma matricial del Algoritmo de Euclides:

## Algoritmo de Euclides en FORMA MATRICIAL:

<b>1</b>	<b>0</b>	<b>720</b>	<b><math>F_1</math></b>
<b>0</b>	<b>1</b>	<b>224</b>	<b><math>F_2</math></b>
<b>1</b>	<b>-3</b>	<b>48</b>	<b><math>F_3 = F_1 - 3 F_2</math></b>
<b>-4</b>	<b>13</b>	<b>32</b>	<b><math>F_4 = F_2 - 4 F_3</math></b>
<b>5</b>	<b>-16</b>	<b>16</b>	<b><math>F_5 = F_3 - F_4</math></b>
		<b>0</b>	<b><math>F_6 = F_4 - 2 F_5</math></b>

**m.c.d.(720,224) = 16**

$$16 = \dots\dots\dots \mathbf{5} \cdot 720 + \dots\dots\dots \mathbf{-16} \cdot 224$$

## Explicación del algoritmo en forma matricial:

Primero se coloca la matriz identidad de orden 2, y en una tercer columna los dos números enteros, siendo el mayor el de la primera fila.

1	0	720	$F_1$
0	1	224	$F_2$

La idea es ir obteniendo nuevas filas, siempre operando con las últimas dos anteriores, de modo de restar de la anteúltima la mayor cantidad de veces que entra el término independiente de la última. En realidad es hacer la división entera y restar el cociente por el elemento de la última fila.

Por ejemplo, en este caso, al dividir 720 por 224, se obtiene cociente 3, entonces vamos a restar 3 veces la fila 2 de la fila 1, la resta se hace en toda la fila:

1	0	720	$F_1$
0	1	224	$F_2$
1	-3	48	$F_3 = F_1 - 3 F_2$

Y luego seguimos este procedimiento hasta llegar a un valor nulo. El anterior al nulo es el máximo común divisor.

1	0	720	$F_1$
0	1	224	$F_2$
1	-3	48	$F_3 = F_1 - 3 F_2$
-4	13	32	$F_4 = F_2 - 4 F_3$
5	-16	16	$F_5 = F_3 - F_4$
		0	$F_6 = F_4 - 2 F_5$

Obtenemos que  $\text{m.c.d.}(720, 224) = 16$

y además:  $16 = 5 \cdot 720 + (-16) \cdot 224$



## Ejercicio:

Calcular  $\text{m.c.d.}(435, 340)$  y escribirlo como combinación lineal entera de ellos



## Solución:

1	0	435	$F_1$
0	1	340	$F_2$
1	-1	95	$F_3 = F_1 - F_2$
-3	4	55	$F_4 = F_2 - 3 F_3$
4	-5	40	$F_5 = F_3 - F_4$
-7	9	15	$F_6 = F_4 - F_5$
18	-23	10	$F_7 = F_5 - 2 F_6$
-25	32	5	$F_8 = F_6 - F_7$
		0	$F_9 = F_7 - 2 F_8$

Obtenemos que  $\text{m.c.d.}(435,340) = 5$

y además:  $5 = (-25) \cdot 435 + 32 \cdot 340$



Veremos un teorema que nos será de gran utilidad:

## TEOREMA DE BEZAUT

$$\begin{array}{c} \text{Dados dos enteros } a \text{ y } b: \\ \text{m.c.d.}(a,b) = 1 \Leftrightarrow 1 = s \cdot a + t \cdot b \text{ con } s, t \in \mathbb{Z} \end{array}$$

Dem.

$\Rightarrow$  es verdadero por la propiedad del máximo común divisor

Nos queda por demostrar la recíproca  $\Leftarrow$

Sea  $d = \text{m.c.d.}(a,b)$  ( lo llamamos  $d$  pues aún no sabemos cuánto vale, pero intentaremos probar que es 1 )

Por definición del máximo común divisor, se cumple que:  $d \mid a \wedge d \mid b$

Por propiedad 4 vista antes:  $d \mid s \cdot a \wedge d \mid t \cdot b$

Y por propiedad 3 vista antes:  $d \mid s \cdot a + t \cdot b$

Por hipótesis,  $d \mid 1$ , pero como  $d \in \mathbb{Z}^+$  resulta  $d = 1$

Con lo cual queda demostrado el teorema.



## ¿Qué utilidad tiene este teorema?

Este teorema nos sirve para demostrar que dos enteros son coprimos, o sea que su m.c.d. es 1 solamente demostrando que 1 es combinación lineal entera de ambos.

Lo veremos aplicado en los siguientes ejemplos:



### Ejemplo 1:

Como  $1 = 3 \cdot 8541 + (-2) \cdot 12811$  entonces  $\text{m.c.d.}(8541, 12811) = 1$



### Ejemplo 2: Dos enteros consecutivos siempre son coprimos

Ya que:  $1 \cdot (x+1) + (-1) \cdot x = 1$



### Ejemplo 3:

Sabiendo que  $a$  y  $b$  son coprimos, podemos demostrar que  $a$  y  $a+b$  también lo son.

$$\text{Dem.) } 1 = s \cdot a + t \cdot b \text{ con } s, t \in \mathbb{Z} \Rightarrow 1 = s \cdot a + t \cdot (b+a-a)$$

$$\Rightarrow 1 = s \cdot a + t \cdot (b+a) - t \cdot a \Rightarrow 1 = (s-t) \cdot a + t \cdot (b+a)$$

$$\Rightarrow 1 = k \cdot a + t \cdot (b+a) \text{ con } k \in \mathbb{Z} \text{ pues es resta de dos enteros.}$$

$$\Rightarrow \text{m.c.d.}(a, a+b) = 1$$

### A tener en cuenta:

Ya sabemos por el Teorema de Bezaut, que es cierto:

$$1 = s \cdot a + t \cdot b \text{ con } s, t \in \mathbb{Z} \Rightarrow \text{m.c.d.}(a, b) = 1$$

Pero no es cierto para otro número mayor que 1

Por ejemplo, si  $3 = s \cdot a + t \cdot b$  con  $s, t \in \mathbb{Z} \Rightarrow \text{m.c.d.}(a, b) = 3$  es

FALSO. Para demostrar que es FALSO, daremos un contraejemplo:

$$3 = 9 \cdot 2 + (-3) \cdot 5 \text{ pero } \text{m.c.d.}(2, 5) \neq 3$$



**Demostrar:** Si  $p \mid a \bullet b \wedge p: \text{primo} \Rightarrow p \mid a \vee p \mid b$

HIPOTESIS)  $p \mid a \bullet b \wedge p: \text{primo} \Leftrightarrow a \bullet b = p \bullet k$  con  $k \in \mathbb{Z} \wedge p: \text{primo}$

TESIS)  $p \mid a \vee p \mid b$

DEM) Sabemos por propiedad de tercero excluido que una de estas dos proposiciones es verdadera:

$$p \mid a \vee \sim [p \mid a]$$

Si fuera verdadera la primera:  $p \mid a$ , entonces la Tesis es verdadera por ser una disyunción, y no hay nada que probar.

Por eso vamos a analizar el caso que  $\sim [p \mid a]$  se verdadera

Como  $p$  es primo  $\wedge$  no divide a "a", entonces  $\text{m.c.d.}(p, a) = 1$

Lo escribimos como combinación lineal entera de ambos:  $1 = s \bullet p + t \bullet a$

Multiplicamos ambos miembros por  $b$ :  $b = s \bullet p \bullet b + t \bullet a \bullet b$

Ahora por hipótesis reemplazamos:  $b = s \bullet p \bullet b + t \bullet p \bullet k$

Sacamos factor común  $p$ :  $b = p \bullet (s \bullet b + t \bullet k)$

Todo lo del paréntesis es entero por ser producto y suma de enteros, que son ambas operaciones cerradas:  $b = p \bullet q$  con  $q \in \mathbb{Z}$

Con lo cual obtuvimos que:  $p \mid b$  y esto hace verdadera la tesis.