

# Divisibilidad

Prof. Jhon Fredy Tavera Bucurú

Universidad del Tolima

Divisibilidad

Máximo común divisor

Lema de Euclides

Teorema de Bachet-Bezout

Teorema Fundamental de la Aritmetica

Mínimo Común Múltiplo

Algunas propiedades de los números primos

# Divisibilidad

# Definición: Divisibilidad

## Definición

*Dado dos enteros  $d$  y  $a$ , decimos que  $d$  divide a  $a$  (o que  $d$  es un divisor de  $a$ ) si existe un entero  $q$  tal que:*

$$a = qd.$$

*Escribimos  $d \mid a$  para indicar que  $d$  divide a  $a$ .*

# Definición: Divisibilidad

## Definición

*Dado dos enteros  $d$  y  $a$ , decimos que  $d$  divide a  $a$  (o que  $d$  es un divisor de  $a$ ) si existe un entero  $q$  tal que:*

$$a = qd.$$

*Escribimos  $d \mid a$  para indicar que  $d$  divide a  $a$ .*

## Ejemplos:

- ▶  $-5 \mid 10$ , ya que existe  $q = -2$  tal que  $10 = (-2)(-5)$ .
- ▶  $10 \nmid -5$ , porque no existe un entero  $q$  tal que  $-5 = 10q$ .

## Lema

Sea  $a, b, c, d \in \mathbb{Z}$ . Tenemos:

- (i) ("**d divide**") Si  $d \mid a$  y  $d \mid b$ , entonces  $d \mid (ax + by)$  para cualquier combinación lineal  $ax + by$  de  $a$  y  $b$  con coeficientes  $x, y \in \mathbb{Z}$ .
- (ii) (**Limitación**) Si  $d \mid a$ , entonces  $a = 0$  o  $|d| \leq |a|$ .
- (iii) (**Transitividad**) Si  $a \mid b$  y  $b \mid c$ , entonces  $a \mid c$ .

## Demostración:

### (i) "d divide"

Si  $d \mid a$  y  $d \mid b$ , entonces podemos escribir  $a = dq_1$  y  $b = dq_2$  con  $q_1, q_2 \in \mathbb{Z}$ . Luego,  $ax + by = d(q_1x + q_2y)$ . Como  $q_1x + q_2y \in \mathbb{Z}$ , tenemos  $d \mid (ax + by)$ .

## **Demostración:**

### **(i) "d divide"**

Si  $d \mid a$  y  $d \mid b$ , entonces podemos escribir  $a = dq_1$  y  $b = dq_2$  con  $q_1, q_2 \in \mathbb{Z}$ . Luego,  $ax + by = d(q_1x + q_2y)$ . Como  $q_1x + q_2y \in \mathbb{Z}$ , tenemos  $d \mid (ax + by)$ .

### **(ii) Limitación**

Para mostrar  $|d| \leq |a|$ , supongamos que  $d \mid a$  y  $a \neq 0$ . En este caso,  $a = dq$  con  $q \neq 0$ . Así,  $|q| \geq 1$  y  $|a| = |d||q|$ , lo que implica  $|d| \leq |a|$ .



## **Demostración:**

### **(i) "d divide"**

Si  $d \mid a$  y  $d \mid b$ , entonces podemos escribir  $a = dq_1$  y  $b = dq_2$  con  $q_1, q_2 \in \mathbb{Z}$ . Luego,  $ax + by = d(q_1x + q_2y)$ . Como  $q_1x + q_2y \in \mathbb{Z}$ , tenemos  $d \mid (ax + by)$ .

### **(ii) Limitación**

Para mostrar  $|d| \leq |a|$ , supongamos que  $d \mid a$  y  $a \neq 0$ . En este caso,  $a = dq$  con  $q \neq 0$ . Así,  $|q| \geq 1$  y  $|a| = |d||q|$ , lo que implica  $|d| \leq |a|$ .

### **(iii) Transitividad**

Si  $a \mid b$  y  $b \mid c$ , entonces existen  $q_1, q_2 \in \mathbb{Z}$  tales que  $b = aq_1$  y  $c = bq_2$ . Por lo tanto,  $c = a(q_1q_2)$  y  $a \mid c$ .



# Ejemplo

## Enunciado:

Encuentre todos los enteros positivos  $n$  tales que

$$2n^2 + 1 \mid n^3 + 9n - 17.$$

# Ejemplo

## Enunciado:

Encuentre todos los enteros positivos  $n$  tales que

$$2n^2 + 1 \mid n^3 + 9n - 17.$$

## Solución:

Utilizando que  $2n^2 + 1$  divide para reducir el grado de  $n^3 + 9n - 17$ , tenemos que:

$$2n^2 + 1 \mid n^3 + 9n - 17,$$

$$2n^2 + 1 \mid 2n^2 + 1.$$

# Ejemplo

## Enunciado:

Encuentre todos los enteros positivos  $n$  tales que

$$2n^2 + 1 \mid n^3 + 9n - 17.$$

## Solución:

Utilizando que  $2n^2 + 1$  divide para reducir el grado de  $n^3 + 9n - 17$ , tenemos que:

$$2n^2 + 1 \mid n^3 + 9n - 17,$$

$$2n^2 + 1 \mid 2n^2 + 1.$$

Luego,

$$2n^2 + 1 \mid (n^3 + 9n - 17) \cdot 2 + (2n^2 + 1) \cdot (-n),$$

lo cual implica:

$$2n^2 + 1 \mid 17n - 34.$$

Como el grado de  $17n - 34$  es menor que el de  $2n^2 + 1$ , podemos utilizar la "limitación" para obtener una lista finita de candidatos para  $n$ . Tenemos:

$$17n - 34 = 0 \Leftrightarrow n = 2 \quad \text{o} \quad 2n^2 + 1 \leq |17n - 34| \Leftrightarrow n = 1, 4, 5.$$

De estos candidatos, solo  $n = 2$  y  $n = 5$  son soluciones.

# Definición: Máximo Común Divisor (MCD)

Dado dos números enteros  $a$  y  $b$  con  $a \neq 0$  o  $b \neq 0$ , podemos asociar a cada uno de ellos su conjunto de divisores positivos,  $D_a$  y  $D_b$  respectivamente.

# Definición: Máximo Común Divisor (MCD)

Dado dos números enteros  $a$  y  $b$  con  $a \neq 0$  o  $b \neq 0$ , podemos asociar a cada uno de ellos su conjunto de divisores positivos,  $D_a$  y  $D_b$  respectivamente.

La intersección de estos conjuntos  $D_a \cap D_b$  es finita (por la "limitación") y no vacía (ya que 1 pertenece a la intersección).

Por ser finito,  $D_a \cap D_b$  posee un elemento máximo, que es llamado el **máximo divisor común** (MCD) de los números  $a$  y  $b$ .

Denotamos este número por  $\text{MCD}(a, b)$  también lo podemos notar como  $(a, b)$ .

# Definición: Máximo Común Divisor (MCD)

Dado dos números enteros  $a$  y  $b$  con  $a \neq 0$  o  $b \neq 0$ , podemos asociar a cada uno de ellos su conjunto de divisores positivos,  $D_a$  y  $D_b$  respectivamente.

La intersección de estos conjuntos  $D_a \cap D_b$  es finita (por la "limitación") y no vacía (ya que 1 pertenece a la intersección).

Por ser finito,  $D_a \cap D_b$  posee un elemento máximo, que es llamado el **máximo divisor común** (MCD) de los números  $a$  y  $b$ .

Denotamos este número por  $\text{MCD}(a, b)$  también lo podemos notar como  $(a, b)$ .

Para  $a = b = 0$ , convencionamos que  $\text{MCD}(0, 0) = 0$ .



# Definición: Máximo Común Divisor (MCD)

Dado dos números enteros  $a$  y  $b$  con  $a \neq 0$  o  $b \neq 0$ , podemos asociar a cada uno de ellos su conjunto de divisores positivos,  $D_a$  y  $D_b$  respectivamente.

La intersección de estos conjuntos  $D_a \cap D_b$  es finita (por la "limitación") y no vacía (ya que 1 pertenece a la intersección).

Por ser finito,  $D_a \cap D_b$  posee un elemento máximo, que es llamado el **máximo divisor común** (MCD) de los números  $a$  y  $b$ .

Denotamos este número por  $\text{MCD}(a, b)$  también lo podemos notar como  $(a, b)$ .

Para  $a = b = 0$ , convencionamos que  $\text{MCD}(0, 0) = 0$ .

Cuando  $\text{MCD}(a, b) = 1$ , decimos que  $a$  y  $b$  son **primos relativos**.

# Ejemplos: Máximo Común Divisor (MCD)

## Ejemplo:

Calculemos el MCD de  $-24$  y  $36$ :

Divisores de positivos de  $-24$  son los mismos que los de  $24$

$$D_{-24} = D_{24} = \{1, 2, 3, 4, 6, 8, 12, 24\}$$

$$\text{Divisores de } 36 : D_{36} = \{1, 2, 3, 4, 6, 9, 12, 18, 36\}$$

$$\text{Intersección: } D_{24} \cap D_{36} = \{1, 2, 3, 4, 6, 12\}$$

$$\text{Por lo tanto, } \text{MCD}(-24, 36) = 12.$$

**Observación:** Los divisores de un número  $a$  y de su inverso aditivo  $-a$  son los mismos, en particular,  $D_a = D_{-a}$ .

# Lema de Euclides

## Lema (Euclides)

*Si  $a = bq + r$ , entonces  $MCD(a, b) = MCD(b, r)$ .*

# Lema de Euclides

## Lema (Euclides)

*Si  $a = bq + r$ , entonces  $MCD(a, b) = MCD(b, r)$ .*

**Demostración:** Basta mostrar que  $D_a \cap D_b = D_b \cap D_r$ , ya que si estos conjuntos son iguales, en particular sus máximos también serán iguales.

# Lema de Euclides

## Lema (Euclides)

*Si  $a = bq + r$ , entonces  $MCD(a, b) = MCD(b, r)$ .*

**Demostración:** Basta mostrar que  $D_a \cap D_b = D_b \cap D_r$ , ya que si estos conjuntos son iguales, en particular sus máximos también serán iguales.

Si  $d \in D_a \cap D_b$ , tenemos  $d \mid a$  y  $d \mid b$ , luego  $d \mid a - bq$  implica  $d \mid r$  y, por lo tanto,  $d \in D_b \cap D_r$ .

# Lema de Euclides

## Lema (Euclides)

*Si  $a = bq + r$ , entonces  $MCD(a, b) = MCD(b, r)$ .*

**Demostración:** Basta mostrar que  $D_a \cap D_b = D_b \cap D_r$ , ya que si estos conjuntos son iguales, en particular sus máximos también serán iguales.

Si  $d \in D_a \cap D_b$ , tenemos  $d \mid a$  y  $d \mid b$ , luego  $d \mid a - bq$  implica  $d \mid r$  y, por lo tanto,  $d \in D_b \cap D_r$ .

De la misma forma, si  $d \in D_b \cap D_r$ , tenemos  $d \mid b$  y  $d \mid r$ , luego  $d \mid bq + r$  implica  $d \mid a$  y, así,  $d \in D_a \cap D_b$ .

# Lema de Euclides

## Lema (Euclides)

*Si  $a = bq + r$ , entonces  $\text{MCD}(a, b) = \text{MCD}(b, r)$ .*

**Demostración:** Basta mostrar que  $D_a \cap D_b = D_b \cap D_r$ , ya que si estos conjuntos son iguales, en particular sus máximos también serán iguales.

Si  $d \in D_a \cap D_b$ , tenemos  $d \mid a$  y  $d \mid b$ , luego  $d \mid a - bq$  implica  $d \mid r$  y, por lo tanto,  $d \in D_b \cap D_r$ .

De la misma forma, si  $d \in D_b \cap D_r$ , tenemos  $d \mid b$  y  $d \mid r$ , luego  $d \mid bq + r$  implica  $d \mid a$  y, así,  $d \in D_a \cap D_b$ .

Por lo tanto,  $\text{MCD}(a, b) = \text{MCD}(b, r)$ .



# Ejemplo

Cual es el  $MCD(26^{64} + 1, 26^{16} + 1)$ ? este ejercicio es un caso particular de...



# Ejemplo

Cual es el  $MCD(26^{64} + 1, 26^{16} + 1)$ ? este ejercicio es un caso particular de...

## **Enunciado:**

Sean  $m \neq n$  dos números naturales. Demostrar que

$$MCD(a^{2^m} + 1, a^{2^n} + 1) = \begin{cases} 1 & \text{si } a \text{ es par,} \\ 2 & \text{si } a \text{ es impar.} \end{cases}$$

## Ejemplo

Cual es el  $MCD(26^{64} + 1, 26^{16} + 1)$ ? este ejercicio es un caso particular de...

### Enunciado:

Sean  $m \neq n$  dos números naturales. Demostrar que

$$MCD(a^{2^m} + 1, a^{2^n} + 1) = \begin{cases} 1 & \text{si } a \text{ es par,} \\ 2 & \text{si } a \text{ es impar.} \end{cases}$$

### Solución:

Supongamos sin pérdida de generalidad que  $m > n$  y observemos la factorización

$$a^{2^m} - 1 = (a^{2^{m-1}} + 1)(a^{2^{m-2}} + 1) \cdots (a^{2^n} + 1)(a^{2^n} - 1).$$

Note que cada producto adiciona 1 al exponente

Por lo tanto,

$$a^{2^m} + 1 = (a^{2^n} + 1) \cdot q + 2,$$

con  $q \in \mathbb{Z}$ , y así

$$\text{MCD}(a^{2^m} + 1, a^{2^n} + 1) = \text{MCD}(a^{2^n} + 1, 2).$$

Finalmente,  $\text{MCD}(a^{2^n} + 1, 2)$  es igual a 2 si  $a^{2^n} + 1$  es par, es decir, si  $a$  es impar; y es igual a 1 en caso contrario.

# Algoritmo de Euclides

Si  $0 < b < a$ , aplicamos el algoritmo de división y escribimos:

$$a = bq_1 + r_1, \quad 0 \leq r_1 < b.$$

# Algoritmo de Euclides

Si  $0 < b < a$ , aplicamos el algoritmo de división y escribimos:

$$a = bq_1 + r_1, \quad 0 \leq r_1 < b.$$

Si  $r_1 = 0$ , entonces  $b \mid a$  y  $\text{MCD}(a, b) = b$ . Si no, aplicamos nuevamente el algoritmo para obtener:

$$b = r_1q_2 + r_2, \quad 0 \leq r_2 < r_1.$$

# Algoritmo de Euclides

Si  $0 < b < a$ , aplicamos el algoritmo de división y escribimos:

$$a = bq_1 + r_1, \quad 0 \leq r_1 < b.$$

Si  $r_1 = 0$ , entonces  $b \mid a$  y  $\text{MCD}(a, b) = b$ . Si no, aplicamos nuevamente el algoritmo para obtener:

$$b = r_1q_2 + r_2, \quad 0 \leq r_2 < r_1.$$

Si  $r_2 \neq 0$  repetimos el proceso, hasta llegar, a lo sumo en  $b$  pasos, a un residuo cero, obteniendo las siguientes ecuaciones:

$$a = bq_1 + r_1, \quad 0 < r_1 < b,$$

$$b = r_1q_2 + r_2, \quad 0 < r_2 < r_1,$$

$$r_1 = r_2q_3 + r_3, \quad 0 < r_3 < r_2,$$

$$\vdots$$

$$r_{k-2} = r_{k-1}q_k + r_k, \quad 0 < r_k < r_{k-1},$$

$$r_{k-1} = r_kq_{k+1} + 0.$$

$$\begin{aligned}
 a &= bq_1 + r_1, & 0 < r_1 < b, \\
 b &= r_1q_2 + r_2, & 0 < r_2 < r_1, \\
 r_1 &= r_2q_3 + r_3, & 0 < r_3 < r_2, \\
 &\vdots \\
 r_{k-2} &= r_{k-1}q_k + r_k, & 0 < r_k < r_{k-1}, \\
 r_{k-1} &= r_kq_{k+1} + 0.
 \end{aligned}$$

La aplicación repetida del Lema de Euclides nos permite afirmar que:

$$\text{MCD}(a, b) = \text{MCD}(b, r_1) = \text{MCD}(r_1, r_2) = \cdots = \text{MCD}(r_{k-1}, r_k) = r_k.$$



## Teorema (Teorema de Bachet-Bézout)

*Sean  $a, b \in \mathbb{Z}$ . Entonces existen  $x, y \in \mathbb{Z}$  tales que:*

$$ax + by = \text{MCD}(a, b).$$

*Por lo tanto, si  $c \in \mathbb{Z}$  es tal que  $c \mid a$  y  $c \mid b$ , entonces  $c \mid \text{MCD}(a, b)$ . Es decir podemos escribir el máximo común divisor de dos números enteros como combinación lineal de ellos.*

# Demostración Teorema Bache-Bézout

**demostracion** El caso  $a = b = 0$  es trivial (tenemos  $x = y = 0$ ). En otros casos, consideremos el conjunto de todas las combinaciones lineales positivas de  $a$  y  $b$ :

$$I(a, b) = \{ax + by : x, y \in \mathbb{Z}\}.$$

Ya que  $I(a, b) \neq \emptyset$ , por el PBO existe  $\text{Min}(I(a, b)) = d$ , es decir  $d = ax_0 + by_0$ . Probaremos que  $d$  divide a todos los elementos de  $I(a, b)$ .

# Demostración Teorema Bache-Bézout

**demostracion** El caso  $a = b = 0$  es trivial (tenemos  $x = y = 0$ ). En otros casos, consideremos el conjunto de todas las combinaciones lineales positivas de  $a$  y  $b$ :

$$I(a, b) = \{ax + by : x, y \in \mathbb{Z}\}.$$

Ya que  $I(a, b) \neq \emptyset$ , por el PBO existe  $\text{Min}(I(a, b)) = d$ , es decir  $d = ax_0 + by_0$ . Probaremos que  $d$  divide a todos los elementos de  $I(a, b)$ .

De hecho, dado  $m = ax + by \in I(a, b)$ , sean  $q, r \in \mathbb{Z}$  el cociente y el resto en el algoritmo de la division de  $m$  por  $d$ , de modo que  $m = dq + r$  y  $0 \leq r < d$ .

Ahora note que:

$$r = m - dq = a(x - qx_0) + b(y - qy_0) \in I(a, b).$$

Pero como  $r < d$  y  $d$  es el menor elemento positivo de  $I(a, b)$ , se sigue que  $r$  no puede ser positivo, es decir  $r = 0$  y, por lo tanto,  $d \mid m$ .

En particular, como  $|a|, |b| \in I(a, b)$  tenemos que  $d \mid a$  y  $d \mid b$  ( $d$  es un divisor común), por lo que  $d \leq \text{MCD}(a, b)$ .

Además, por la propiedad "divide combinación lineal"

$$\text{MCD}(a, b) \mid ax_0 + by_0$$

es decir  $\text{MCD}(a, b) \leq d$ . Entonces  $\text{MCD}(a, b) = d$

## Teorema

*Sean  $a$  y  $b$  enteros no ambos nulos. Entonces,*

*$\text{MCD}(a, b) = 1$  si y solo si existen enteros  $x, y$  tales que  $1 = ax + by$ .*

## Teorema

*Sean  $a$  y  $b$  enteros no ambos nulos. Entonces,*

*$\text{MCD}(a, b) = 1$  si y solo si existen enteros  $x, y$  tales que  $1 = ax + by$ .*

**Demostración:** Si  $\text{MCD}(a, b) = 1$ , el Teorema de Bache-Bézout garantiza la existencia de tales  $x$  y  $y$ . Recíprocamente, si existen  $x$  y  $y$  tales que  $1 = ax + by$ , entonces  $\text{MCD}(a, b) \mid 1$  y, por lo tanto,  $\text{MCD}(a, b) = 1$ . □

## Teorema

Si  $k \neq 0$  entonces  $(ka, kb) = |k|(a, b)$

### Demostración.

Basta probar el resultado para  $k > 0$ . Supongamos que  $d = (a, b)$ ; entonces  $kd \mid ka$  y  $kd \mid kb$ , y por lo tanto  $kd \mid (ka, kb)$ .

Por otra parte,  $d = ax + by$  para algún par de enteros  $x, y$ . Luego

$$kd = kax + kby,$$

y por lo tanto  $(ka, kb) \mid kd$ . De aquí se sigue que

$$kd = k(a, b) = (ka, kb).$$



## Teorema

Si  $a \mid bc$  y  $\text{MCD}(a, b) = 1$ , entonces  $a \mid c$ .

**Demostración:** Como  $a \mid bc$ , existe  $k$  tal que  $bc = ak$ .

Como  $\text{MCD}(a, b) = 1$ , existen enteros  $x$  y  $y$  tales que  $ax + by = 1$ .

Por lo tanto:

$$c = c(ax + by) = acx + bcy = acx + ak y = a(cx + ky),$$

es decir,  $a \mid c$ .





# Definición: Número Primo

Recordemos que un número natural  $p > 1$  se llama **primo** si sus únicos divisores positivos son 1 y  $p$ . Un número natural  $n > 1$  se llama **compuesto** si admite otros divisores además de 1 y  $n$ .

# Definición: Número Primo

Recordemos que un número natural  $p > 1$  se llama **primo** si sus únicos divisores positivos son 1 y  $p$ . Un número natural  $n > 1$  se llama **compuesto** si admite otros divisores además de 1 y  $n$ .  
Es decir

$p$  es primo sii  $p = nm$   $n, m \in \mathbb{N}$ , entonces  $n = 1$  o  $m = 1$ .

**Observación:** El número 1 no es ni primo ni compuesto.

# Corolarios

## Corolario

*Si  $p$  es primo y  $p \mid ab$ , entonces  $p \mid a$  o  $p \mid b$ .*

**Demostración:** Si  $p \nmid a$ , entonces  $\text{MCD}(a, p) = 1$ , y por el teorema anterior  $p \mid b$ . □

# Corolarios

## Corolario

*Si  $p$  es primo y  $p \mid ab$ , entonces  $p \mid a$  o  $p \mid b$ .*

**Demostración:** Si  $p \nmid a$ , entonces  $\text{MCD}(a, p) = 1$ , y por el teorema anterior  $p \mid b$ . □

## Corolario

*Si  $p$  es primo y  $p \mid a_1 a_2 \dots a_n$ , entonces  $p \mid a_i$  para algún  $i$ ,  $1 \leq i \leq n$ .*

**Demostración:** La demostración es por inducción. El caso base es  $n = 2$ , que se demuestra con el corolario anterior. Supongamos que el resultado es cierto para  $n = k$ , es decir, si  $p \mid a_1 a_2 \dots a_k$ , entonces  $p \mid a_i$  para algún  $i$ ,  $1 \leq i \leq k$ . Ahora, consideremos el caso  $n = k + 1$ . Si  $p \mid a_1 a_2 \dots a_k a_{k+1}$ , entonces por el corolario anterior,  $p \mid a_1 a_2 \dots a_k$  o  $p \mid a_{k+1}$ . Por la hipótesis de inducción,  $p$  divide a alguno de los  $a_i$ ,  $1 \leq i \leq k + 1$ . Esto completa la inducción. □

## Teorema ( fundamental de la aritmetica)

*Sea  $n \geq 2$  un número natural. Podemos escribir  $n$  de una única forma como un producto*

$$n = p_1 \cdots p_m$$

*donde  $m \geq 1$  es un natural y  $p_1 \leq \cdots \leq p_m$  son primos.*

**Demostración:** Mostramos la existencia de la factorización de  $n$  en primos por inducción. Si  $n$  es primo no hay nada que probar (escribimos  $m = 1$ ,  $p_1 = n$ ). Si  $n$  es compuesto podemos escribir  $n = ab$ ,  $a, b \in \mathbb{N}$ ,  $1 < a < n$ ,  $1 < b < n$ . Por hipótesis de inducción,  $a$  y  $b$  se descomponen como producto de primos. Juntando las factorizaciones de  $a$  y  $b$  (y reordenando los factores) obtenemos una factorización de  $n$ .

Vamos ahora a mostrar la unicidad. Sea  $S$  el conjunto de todos los números que admiten más de una factorización, Supongamos por absurdo que  $S \neq \emptyset$ , por el PBO, existe  $n = \min S$  el cual posee al menos dos factorizaciones diferentes

$$n = p_1 \cdots p_m = q_1 \cdots q_{m'},$$

con  $p_1 \leq \cdots \leq p_m$ ,  $q_1 \leq \cdots \leq q_{m'}$  y que  $n$  es mínimo con tal propiedad. Como  $p_1 \mid q_1 \cdots q_{m'}$  tenemos  $p_1 \mid q_i$  para algún valor de  $i$  por el corolario. Luego, como  $q_i$  es primo,  $p_1 = q_i$  y  $p_1 \geq q_1$ . Análogamente  $p_1 \leq q_1$ , por tanto  $p_1 = q_1$ . Pero

$$\frac{n}{p_1} = p_2 \cdots p_m = q_2 \cdots q_{m'}.$$

admite una única factorización, por la minimalidad de  $n$ , donde  $m = m'$  y  $p_i = q_i$  para todo  $i$ , lo que contradice el hecho de que  $n$  tenga dos factorizaciones. □

## Definición: Mínimo Común Múltiplo

El **mínimo común múltiplo** (MCM) de dos enteros no nulos  $a$  y  $b$  es el menor entero positivo que es múltiplo de ambos. Se denota como

$$\text{MCM}(a, b) \quad \text{o simplemente} \quad [a, b].$$

Para que un número  $m$  sea el MCM de  $a$  y  $b$ , deben cumplirse las siguientes condiciones:

- (i)  $m > 0$ .
- (ii)  $a \mid m$  y  $b \mid m$  (es decir,  $m$  es múltiplo de  $a$  y de  $b$ ).
- (iii) Si  $n$  es un entero tal que  $a \mid n$  y  $b \mid n$ , entonces  $m \mid n$  (es decir,  $m$  es el menor de todos los múltiplos comunes).



## Teorema: Fórmula del Mínimo Común Múltiplo

Sean  $a$  y  $b$  enteros no nulos. Entonces,

$$[a, b] = \frac{|ab|}{(a, b)},$$

donde  $(a, b)$  representa el máximo común divisor de  $a$  y  $b$ .

## Demostración

Sea  $m = \frac{|ab|}{(a,b)}$ . Veamos que  $m$  satisface las condiciones (i), (ii) y (iii).

Evidentemente  $m > 0$ . Sea  $d = (a, b)$ , entonces  $a = Ad$  y  $b = Bd$  donde  $(A, B) = 1$ . Así,

$$m = \frac{|ab|}{d} = \frac{|a| |b|}{d} = |a| |B| = a(\pm B),$$

luego  $a \mid m$  y de forma similar  $b \mid m$ .

Sea ahora  $n$  un entero tal que  $a \mid n$  y  $b \mid n$ . Entonces existen enteros  $r$  y  $s$  tales que  $n = ar = bs$ . En consecuencia  $Adr = Bds$  y por lo tanto  $Ar = Bs$ . Así,  $B \mid Ar$  y como  $(A, B) = 1$  se deduce que  $B \mid r$ , es decir,  $r = Bt$  para algún  $t \in \mathbb{Z}$ .

Reemplazando tenemos:

$$n = ar = a(Bt) = (aB)t = (ab/d)t = \pm mt,$$

es decir,  $m \mid n$  y se completa la demostración.

## Teorema

Sea  $n = \prod_{i=1}^k p_i^{n_i}$  la representación canónica de un entero  $n$ , y sea  $d$  un entero positivo. Entonces,  $d \mid n$  si y sólo si

$$d = \prod_{i=1}^k p_i^{d_i}$$

donde  $0 \leq d_i \leq n_i$  para cada  $i$ ,  $1 \leq i \leq k$ .

## Demostración

Supongamos que  $d = \prod_{i=1}^k p_i^{d_i}$  donde  $0 \leq d_i \leq n_i$ . Entonces,

$$\begin{aligned} n &= \prod_{i=1}^k p_i^{n_i} = \prod_{i=1}^k p_i^{n_i - d_i + d_i} \\ &= \left( \prod_{i=1}^k p_i^{n_i - d_i} \right) \left( \prod_{i=1}^k p_i^{d_i} \right) = (c)(d) \end{aligned}$$

donde  $c = \prod_{i=1}^k p_i^{n_i - d_i}$  es un entero. Luego  $d \mid n$ .

Recíprocamente, supongamos que  $d \mid n$ . Por definición, existe un entero positivo  $c$  tal que  $n = cd$ .

La unicidad de la representación canónica de  $n$  garantiza que los primos que aparecen en la factorización de  $c$  y  $d$  son los mismos que en la de  $n$ . Así:

$$d = \prod_{i=1}^k p_i^{d_i}, \quad c = \prod_{i=1}^k p_i^{c_i}, \quad n = \prod_{i=1}^k p_i^{n_i},$$

donde  $d_i \geq 0$ ,  $c_i \geq 0$  y  $n_i = d_i + c_i$ . Por tanto,  $d$  tiene la forma mencionada. □

## Teorema

Sean

$$a = \prod_{i=1}^k p_i^{a_i}, \quad b = \prod_{i=1}^k p_i^{b_i},$$

donde  $p_i$  es primo para todo  $i$ , y  $a_i \geq 0$ ,  $b_i \geq 0$  para todo  $i$ .

Entonces:

$$(a, b) = \prod_{i=1}^k p_i^{s_i} \quad \text{y} \quad [a, b] = \prod_{i=1}^k p_i^{t_i},$$

donde

$$s_i = \min\{a_i, b_i\}, \quad t_i = \max\{a_i, b_i\}.$$

## Demostración

Sea  $d = \prod_{i=1}^k p_i^{s_i}$ . Veamos que  $d$  satisface las condiciones (i), (ii), (iii).

Es un producto de positivos (i).

Además, como  $0 \leq s_i \leq a_i$  y  $0 \leq s_i \leq b_i$  para cada  $i$ , por el teorema anterior  $d \mid a$  y  $d \mid b$ , así que  $d$  satisface (ii).

Finalmente, si  $f \mid a$  y  $f \mid b$ , entonces

$$|f| = \prod_{i=1}^k p_i^{f_i}$$

donde  $0 \leq f_i \leq a_i$  y  $0 \leq f_i \leq b_i$  para cada  $i$ , y entonces  $|f| \mid d$ . Luego  $f \mid d$  y así  $d$  satisface (iii).

Como  $[a, b] = \frac{|ab|}{(a, b)}$  se demuestra el correspondiente resultado para el MCM. □

# Primos

## Observación

Un método simple y eficiente para enteros positivos relativamente pequeños es verificar si el entero dado tiene o no divisores primos menores que él.

Puesto que si  $n = ab$  entonces  $a \leq \sqrt{n}$  o  $b \leq \sqrt{n}$ , es suficiente determinar si algún primo menor o igual a  $\sqrt{n}$  es divisor de  $n$ .

## Teorema

**El número de primos es infinito.**



## Demostración

—Dada por Euclides—. Supongamos que solo hay un número finito de primos,

$$p_1, p_2, \dots, p_n,$$

y sea

$$N = p_1 p_2 \cdots p_n + 1.$$

Como  $N > 1$ , entonces  $N$  es primo o se expresa como producto de primos. Ya que  $N$  es mayor que cada uno de los primos  $p_i$ , entonces  $N$  no es primo.

Además, ningún primo  $p_i$  divide a  $N$  pues si  $p_i \mid N$ , entonces

$$p_i \mid (N - p_1 p_2 \cdots p_n) = 1,$$

lo que es imposible.

Esto contradice el TFA (Teorema Fundamental de la Aritmética) y por tanto el número de primos es infinito.  $\square$