

# Teoría de Números

---

## Temas:

---

1. Algoritmo de la División
2. Algoritmo de Euclides
3. Ecuaciones Diofánticas
4. Mínimo Común Múltiplo
5. Ejercicios

## Algoritmo de la División

---

Dados  $a, b \in \mathbb{Z}$  con  $b \geq 1$ , existen  $q, r \in \mathbb{Z}$  con  $0 \leq r < b$  tales que:

$$a = bq + r$$

### Demostración

Tomemos el conjunto  $R = \{r \geq 0 : r = a - bq\}$  con  $q \in \mathbb{Z}$  y sea  $r_0$  el elemento mínimo del conjunto, luego sabemos que  $r_0 \geq 0$  porque así construimos el conjunto, probemos ahora que  $r_0 < b$ . Supongamos lo contrario, entonces  $a = bq + r_0$ , y como  $r_0 \geq b \Rightarrow r_0 = b + t \Rightarrow a = b(q + 1) + t$  contradicción porque encontramos un elemento menor que  $r_0$  que pertenece al conjunto  $R \Rightarrow 0 \leq r_0 < b$

## Algoritmo de Euclides

---

Se basa en el hecho evidente de que, si  $a = bq + r$ , cualquier número que divida a  $a$  y  $b$  también divide a  $b$  y  $r$  (y viceversa); en consecuencia:

$$\text{mcd}(a, b) = \text{mcd}(b, r)$$

### Demostración

Supongamos que  $\text{mcd}(a, b) = d_1 \geq \text{mcd}(b, r) = d_2$ , como  $d_1 \div a$  y  $d_1 \div b \Rightarrow d_1 \div r \Rightarrow d_1 \div \text{mcd}(b, r)$  y como  $d_1 \geq d_2 \Rightarrow d_1 = d_2$ . Análogamente suponiendo que  $d_2 \geq d_1$

## Ecuaciones Diofánticas

---

Sean  $a, b$  dos enteros no ambos nulos,  $d = \text{mcd}(a, b)$  y  $c$  otro entero. La ecuación diofántica es de la forma:

$$ax + by = c$$

Existen infinitos valores para  $x, y$  que la satisfacen  $\Leftrightarrow d \div c$  y siendo  $x_0, y_0$  solución, todas las soluciones tienen la forma:

$$x = x_0 + \frac{b}{d}k$$

$$y = y_0 - \frac{a}{d}k$$

### Demostración (mía)

La primera parte es más sencilla, supongamos que  $d$  no divide a  $c$ , luego, si  $a = da_0$  y  $b = db_0 \Rightarrow ax + by = d(a_0x + b_0y) = c$  contradicción porque no existen valores de  $x, y$  que lo cumplan  $\Rightarrow d \nmid c$

### Demostración (Recorrido por la Teoría de Números)

Demostraremos por el libro por qué todas las soluciones tienen esa forma, sean  $x_1, y_1$  otra solución de la ecuación, entonces se cumple que:

$$ax_0 + by_0 = ax_1 + by_1$$

Dividiendo por  $d$  y agrupando términos semejantes resulta en:

$$a_1(x_1 - x_0) = b_1(y_0 - y_1)$$

Como  $\text{mcd}(a_1, b_1) = 1 \Rightarrow a_1 \div (y_0 - y_1)$  y  $b_1 \div (x_1 - x_0)$  de donde resulta que:

$$x_0 + \frac{b}{d}k = x_1$$

$$y_0 - \frac{a}{d}k = y_1$$

# Mínimo Común Múltiplo

Se define el mínimo común múltiplo (*mcm*) de dos enteros  $a$  y  $b$  no nulos como:

$$mcm(a, b) = \min\{m \in \mathbb{N} : a \div m, b \div m\}$$

## MCM de dos números

Sean  $a, b$  enteros no nulos, y  $d = mcd(a, b)$  entonces se cumple que:

$$mcm(a, b) = \frac{ab}{d}$$

## Demostración

Sea  $m$  múltiplo común de  $a, b$ , entonces  $m = ak_1 = bk_2 \implies a_1k_1 = b_1k_2$  siendo  $a_1 = \frac{a}{d}$  y  $b_1 = \frac{b}{d}$ , pero como  $mcd(a_1, b_1) = 1 \implies b_1 \div k_1$  de donde  $k_1 = b_1k_3$  y sustituyendo  $k_1$  en  $m = ak_1$  resulta en:

$$m = \frac{ab}{d}k_3$$

Luego, como todo múltiplo común de  $a, b$  podemos expresarlo como múltiplo común de  $\frac{ab}{d} \implies$  ese es el  $mcm(a, b)$

## Ejercicios

### Problema 1

Sean  $a_1, a_2, \dots, a_n \in \mathbb{Z}$ . Prueba que son coprimos dos a dos  $\iff$   
 $mcm(a_1, a_2, \dots, a_n) = a_1 a_2 \cdots a_n$

# Solución

Lema 1: Sea  $m$  múltiplo de los  $a_1, a_2, \dots, a_n$ , entonces  $m$  es múltiplo del  $mcm(a_1, a_2, \dots, a_n)$ . Demostremoslo:

- $m$  es múltiplo de los  $a_i \Rightarrow \forall i = \{1, \dots, n\} : a_i \div m$ . Sea  $t = mcm(a_1, a_2, \dots, a_n)$ , probemos que  $t \div m$ . Sea  $m = tq + r$  con  $0 \leq r < t$ , entonces:

$$r = m - tq$$

Pero como tanto  $m$  como  $t$  son divisibles entre los  $a_i$ :

$$r = (a_i * h) - q(a_i * p)$$

$$r = a_i(h - qp)$$

En conclusión, hemos encontrado un  $r < t$  tal que es múltiplo común de todos los  $a_i$  menor que el  $mcm$ , lo cual solo es posible si  $r = 0$ , de donde  $t \div m$

Lema 2:  $mcm(a_1, a_2, \dots, a_k) = mcm(a_1, mcm(a_2, \dots, a_k))$

- Para demostrar esto debemos analizar los múltiplos que genera cada miembro por separado, si demostramos que todo múltiplo del miembro izquierdo es múltiplo del miembro derecho y análogamente hacemos el análisis con el miembro derecho, habremos probado la igualdad.

Notemos que todo múltiplo de  $mcm(a_1, a_2, \dots, a_k)$  es múltiplo de todos los  $a_i$  y en particular de  $a_2, \dots, a_k \Rightarrow$  es múltiplo del  $mcm(a_2, \dots, a_k)$  por Lema 1 y como es múltiplo de  $a_1 \Rightarrow$  es múltiplo del  $mcm(a_1, mcm(a_2, \dots, a_k))$

Similar se hace el análisis con el miembro derecho, todo múltiplo de  $mcm(a_1, mcm(a_2, \dots, a_k))$  es múltiplo de  $a_1$  y del  $mcm(a_2, \dots, a_k) \Rightarrow$  es múltiplo de  $a_2, \dots, a_k$ , y por tanto múltiplo del  $mcm(a_1, a_2, \dots, a_k)$

Probemos por inducción que si  $a_1, a_2, \dots, a_n$  son coprimos dos a dos  $\Rightarrow$   
 $mcm(a_1, a_2, \dots, a_n) = a_1 a_2 \cdots a_n$

- Caso base  $n = 2$ : Si  $a$  y  $b$  son coprimos  $\Rightarrow mcm(a, b) = ab$  porque  $mcm(a, b) = \frac{ab}{mcd(a, b)}$  y como  $a, b$  son coprimos entonces  $mcd(a, b) = 1 \Rightarrow mcm(a, b) = ab$

Hipótesis de inducción: Supongamos que para  $n = k$  lo cumple, entonces  $mcm(a_1, a_2, \dots, a_k) = a_1 a_2 \cdots a_k$  siendo  $a_1, a_2, \dots, a_k$  coprimos

Probemos que para  $n = k + 1$  se cumple: Para eso necesitamos una forma de descomponer el  $mcm(a_1, a_2, \dots, a_{k+1})$  en un  $mcm$  más pequeño, para lo cual utilizaremos el ya demostrado *Lema 2*, con lo cual  $mcm(a_1, a_2, \dots, a_{k+1}) = mcm(a_1, mcm(a_2, \dots, a_{k+1}))$

Luego, por hipótesis de inducción  $mcm(a_2, \dots, a_{k+1}) = a_2 \cdots a_{k+1}$  por lo que  $mcm(a_1, a_2, \dots, a_{k+1}) = mcm(a_1, a_2 \cdots a_{k+1})$  y como todos los  $a_i$  son primos relativos dos a dos, ambos términos dentro del  $mcm$  son coprimos y por tanto, por el caso base  $mcm(a_1, a_2, \dots, a_{k+1}) = a_1 a_2 \cdots a_{k+1}$

Demostremos ahora la otra dirección del ( $\Leftrightarrow$ ), si se cumple que  $mcm(a_1, a_2, \dots, a_n) = a_1 a_2 \cdots a_n$  entonces todos son coprimos dos a dos.

- Como  $mcm(a_1, a_2, \dots, a_n) = mcm(a_1, mcm(a_2, \dots, a_n))$  por el *Lema 2*, entonces se cumple que  $mcm(a_1, a_2, \dots, a_n) = mcm(a_1, a_2 \cdots a_n) = a_1 a_2 \cdots a_n$  y está demostrado en conferencia que  $mcm(a, b) = \frac{ab}{mcd(a,b)}$ , luego  $mcd(a_1, a_2 \cdots a_n) = 1$  por lo que  $a_1$  es primo relativo con  $a_2 \cdots a_n$  de donde  $a_1$  es primo relativo con cada  $a_i$  con  $2 \leq i \leq n$ .

Haciendo el análisis con cada  $a_i$  llegamos a la conclusión de que si se cumple la premisa entonces los  $a_i$  son coprimos dos a dos.

## Problema 2

Prueba que  $\sqrt[m]{n}$  es entera o irracional para  $m, n$  enteros positivos.

## Solución

Supongamos que no se cumple que  $\sqrt[m]{n}$  sea entera o irracional, entonces es de la forma  $\frac{p}{q}$  con  $q \neq 1$  y  $mcd(p, q) = 1 \Rightarrow q \sqrt[m]{n} = p \Rightarrow q^m n = p^m$ , pero como  $p$  y  $q$  son coprimos  $\Rightarrow q^m$  y  $p^m$  también son coprimos, sin embargo  $q^m \div p^m \Rightarrow q = 1$

Probemos que si  $a, b$  enteros tal que  $mcd(a, b) = 1$  y  $a^m \div b^m \Rightarrow a = 1$ . Como  $mcd(a, b) = 1$  entonces  $a$  es coprimo con cualquier potencia de  $b$ , y como  $b^m$  es coprimo con  $a$ , al elevar  $a$   $m$ -veces también serán coprimos, y como  $a^m \div b^m$  el único  $a$  que cumple es 1.

Acabamos de probar que si  $\sqrt[m]{n}$  es racional entonces es entera, luego, se deduce que si no es entera no es racional y por tanto es irracional.

## Problema 3

Resuelve:  $188x + 508y = 1580$

## Problema 4

Sean  $a, b$  enteros positivos. Determine cuántos números entre  $a, 2a, 3a, \dots, ba$  son divisibles por  $b$ .

## Solución

Sea  $d = \text{mcd}(a, b)$  y las descomposiciones:

$$a = a_1 d$$

$$b = b_1 d$$

De donde  $\text{mcd}(a_1, b_1) = 1$ . Entonces debemos hallar cuantos  $k$  menores o iguales que  $b$  cumplen que  $\frac{ak}{b} = n$  siendo  $n$  natural. Pero sustituyendo  $a$  y  $b$  por sus descomposiciones tenemos que  $\frac{a_1 dk}{b_1 d}$  simplificando  $d$  resulta en  $\frac{a_1 k}{b_1}$ , como  $\text{mcd}(a_1, b_1) = 1$  basta encontrar cuántos números de 1 a  $b$  son divisibles por  $b_1$ , y esa cantidad es  $\frac{b}{b_1} = \text{mcd}(a, b) = d$

## Problema 5

Prueba que si  $a, b, c$  son enteros positivos  $\Rightarrow \text{mcm}(a, b, c) = \frac{abc}{\text{mcd}(ab, bc, ca)}$

## Solución (Abel)

Para hacer este ejercicio por esta vía solo es necesario saber tres cosas:

1. 
$$\text{mcm}(a, b) = \frac{ab}{\text{mcd}(a, b)}$$

$$2. \quad mcm(a, b, c) = mcm(a, mcm(b, c))$$

$$3. \quad mcd(a, b, c) = mcd(a, mcd(b, c))$$

Procedamos con la demostración, partiendo del miembro izquierdo y utilizando (2) se cumple que  $mcm(a, b, c) = mcm(a, mcm(b, c))$ , luego, aplicando la propiedad (1) dos veces resulta en:

$$mcm(a, b, c) = \frac{abc}{mcd(b, c) * mcd(a, \frac{bc}{mcd(b, c)})}$$

Teniendo en cuenta lo demostrado en (Problema 5 clase 2) llegamos a que:

$$mcd(b, c) * mcd(a, \frac{bc}{mcd(b, c)}) = mcd(a * mcd(b, c), bc)$$

Y volviendo a aplicar la propiedad anterior en el último resultado resulta:

$$mcd(a * mcd(b, c), bc) = mcd(mcd(ab, ac), bc)$$

Y por la propiedad (3) concluimos que:

$$mcd(mcd(ab, ac), bc) = mcd(ab, ac, bc)$$