

## **ALGORITMO DE EUCLIDES**

ALAN REYES-FIGUEROA  
TEORÍA DE NÚMEROS

(AULA 04) 15.JULIO.2024

# Lema de Bézout

## Teorema (Lema de BÉZOUT)

Para todo  $a, b \in \mathbb{Z}$ , existen  $M, N \in \mathbb{Z}$  tales que  $(a, b) = Ma + Nb$ .

Prueba: Sea  $S = \{xa + yb; x, y \in \mathbb{Z}, xa + yb > 0\}$ . Observe que  $a = 1 \cdot a + 0 \cdot b, b = 0 \cdot a + 1 \cdot b \in S$ , de forma que  $S$  es no vacío. Por el principio del buen orden,  $S$  posee un elemento mínimo  $d > 0$ . En particular,  $d = Ma + Nb$  para algunos  $M, N \in \mathbb{Z}$ . Si aplicamos el algoritmo de la división, con  $d$  dividiendo  $a$ , existe  $q \in \mathbb{Z}$  tal que

$$a = qd + r, \quad 0 \leq r < d.$$

Si  $r > 0$ , entonces  $r = a - qd = a - (Ma + Nb) = (1 - M)a - Nb$  sería elemento de  $S$ , lo que contradice la elección minimal de  $r$  en  $S$ . De ahí que  $r = 0$ . Portanto,  $d \mid a$ .

Repitiendo el argumento anterior del algoritmo de la división pero ahora con  $d$  dividiendo  $b$ , se concluye también que  $d \mid b$ .

# Lema de Bézout

Así,  $d$  es un divisor común de  $a$  y  $b$ .

Si  $c$  es otro divisor común de  $a$  y  $b$ , entonces  $c \mid a, c \mid b \Rightarrow c \mid Ma + Nb = d$ . Portanto  $d = (a, b)$ , y hemos establecido que existen  $M, N \in \mathbb{Z}$  tales que

$$d = (a, b) = Ma + Nb. \square$$

## Definición

Dos enteros  $a$  y  $b$  se llaman **primos relativos** o **coprimos** si no tienen factores en común (aparte de 1). Esto es, si  $(a, b) = 1$ .

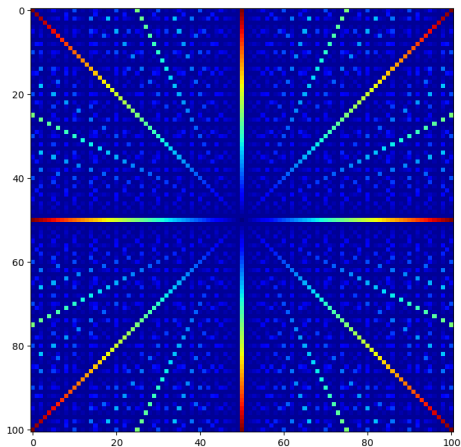
## Corolario

$a$  y  $b$  son primos relativos. si y sólo si, existen  $M, N \in \mathbb{Z}$  tales que  $Ma + Nb = 1$ .  $\square$

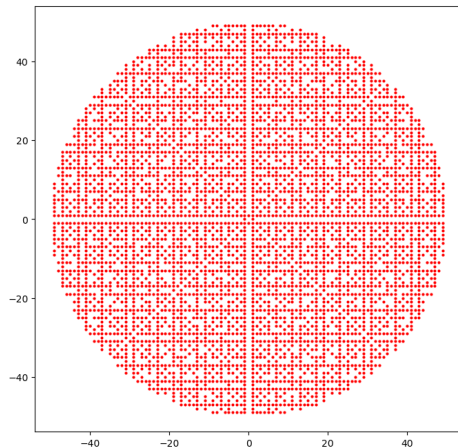
Prueba:  $(\Rightarrow)$   $a, b$  primos relativos,  $\Rightarrow$  existen  $M, N \in \mathbb{Z}$  con  $1 = (a, b) = Ma + Nb$ .

$(\Leftarrow)$  Si  $d \mid a$  y  $d \mid b$ , entonces  $d \mid Ma + Nb = 1$ . Luego,  $|d| = 1$ .

# Consecuencias



Mapa de calor del MDC.



Pares de primos relativos en  $\mathbb{Z}^2$ .

## Corolario

a) Si  $a \mid c$ ,  $b \mid c$  y  $(a, b) = 1$ , entonces  $ab \mid c$ .

b) (Lema de EUCLIDES) Si  $a \mid bc$  y  $(a, b) = 1$ , entonces  $a \mid c$ .

Prueba: (a) Como  $(a, b) = 1$ , por el Teorema de Bézout, existen  $x, y \in \mathbb{Z}$  tales que  $xa + yb = 1$ . Luego  $xac + ybc = c$ .

Ahora  $b \mid c \Rightarrow ab \mid ac \mid xac$  y  $a \mid c \Rightarrow ab \mid bc \mid ybc$ . De ahí que  $ab \mid xac + ybc = c$ .

(b) Como  $(a, b) = 1$ , de nuevo por el Teorema de Bézout, existen  $x, y \in \mathbb{Z}$  tales que  $xa + yb = 1$ . Luego  $xac + ybc = c$ .

Como  $a \mid xab$  y  $a \mid bc \mid ybc$ , entonces  $a \mid xab + ybc = c$ .  $\square$ .

# Consecuencias

## Corolario

Si  $d = (a, b)$ , entonces  $(\frac{a}{d}, \frac{b}{d}) = 1$ .

Prueba: Sea  $d = (a, b)$ . Por el Teorema de Bézout, existen  $x, y \in \mathbb{Z}$  tales que  $xa + yb = d$ . Dividiendo la ecuación anterior entre  $d$ , escribimos

$$x(\frac{a}{d}) + y(\frac{b}{d}) = 1.$$

Como  $x, y \in \mathbb{Z}$ , por el corolario al Teorema de Bézout a esta última ecuación, entonces  $\frac{a}{d}$  y  $\frac{b}{d}$  son primos relativos, y  $(\frac{a}{d}, \frac{b}{d}) = 1$ .  $\square$ .

**Nota Aclaratoria!** El Lema de Bézout **no es** un si y sólo si. De hecho más adelante vamos a probar que los enteros  $n$  que admiten representación en la forma  $n = xa + yb$  son precisamente los múltiplos de  $d = (a, b)$ .

Sin embargo, vale un si y sólo si, cuando se tiene  $xa + yb = 1$ . La única forma que 1 sea combinación lineal de  $a$  y  $b$  es cuando son coprimos.

**Prop:**  $[a, b](a, b) = ab$ , para  $a, b \in \mathbb{N}$ .

Prueba: Sea  $d = (a, b)$ . Por el Teorema de Bézout, existen  $M, N \in \mathbb{Z}$  tales que  $Ma + Nb = d$ .

Por otro lado,  $d \mid ab$ . Sea entonces  $m = \frac{ab}{d} \in \mathbb{N}$ . Como  $m = \left(\frac{a}{d}\right)b = a\left(\frac{b}{d}\right)$ , sabemos que  $m$  es un múltiplo común de  $a$  y de  $b$ .

Suponga que  $n$  es otro múltiplo común de  $a$  y de  $b$ . Mostramos que  $m \mid n$ . En efecto,

$$\frac{n}{m} = \frac{n}{ab/d} = \frac{nd}{ab} = \frac{n(Ma + Nb)}{ab} = n\left(\frac{M}{b} + \frac{N}{a}\right) = \frac{n}{b}M + \frac{n}{a}N \in \mathbb{Z}.$$

Portanto,  $m \mid n$ , y entonces  $m = [a, b]$  es el mínimo múltiplo común. Se concluye que  $ab = md = [a, b](a, b)$ .  $\square$ .

# ¿Cómo calcular $(a, b)$ ?

**Ejemplo:** Calcular el MDC y MMC de 360 y 84.

Solución: Factoramos los números 360 y 84 (en factores primos):

360	2	84	2
180	2	42	2
90	2	21	3
45	3	7	7
15	3	1	
5	5		
1			

Los divisores comunes para 360 y 84 son 2, 2, 3. Entonces  $(360, 84) = 2^2 \cdot 3 = 12$ . Por otro lado,  $[360, 84] = 2^3 \cdot 3^2 \cdot 5 \cdot 7 = 2520$ .



# ¿Cómo calcular $(a, b)$ ?

## Lema

Para  $a, b \in \mathbb{Z}$ ,  $(a, b) = (a - b, b) = (a, b - a)$ .

Prueba: Mostramos  $(a, b) = (a - b, b)$ . La otra igualdad es análoga.

Sean  $d = (a, b)$ ,  $c = (a - b, b)$ . Entonces  $d \mid a$ ,  $d \mid b \Rightarrow d \mid a - b$ . Luego,  $d \mid c$ .

Ahora,  $c \mid a - b$ ,  $c \mid b \Rightarrow c \mid (a - b) + b = a$ . De ahí,  $c \mid d$ . Esto muestra que  $d = c$ .  $\square$

## Lema

Para todo  $a \in \mathbb{Z}$ ,  $(a, 0) = |a|$ .

Prueba:  $a \mid 0$  y  $a \mid a \Rightarrow a \mid (a, 0)$ . Por otro lado,  $(a, 0) \mid a$ . luego, por antisimetría,  $(a, 0) = |a|$ .  $\square$

# ¿Cómo calcular $(a, b)$ ?

Esto ya nos da un primer algoritmo para calcular  $(a, b)$ :

**Algoritmo 1:** (Cálculo del MDC por restas).

```
def mdc(a, b):  
    if (b > a):  
        return mdc(b,a)  
    if (b == 0):  
        return a  
    else:  
        return mdc(a-b,a)
```

# Algoritmo de Euclides

Emplea el algoritmo de la división como base. Conocido por los griegos (publicado por EUCLIDES).

## Lema (Euclides)

Si  $a = qb + r$ , entonces  $(a, b) = (b, r)$ .

Prueba: Sean  $d = (a, b)$  y  $f = (b, r)$ .

Como  $d \mid a$  y  $d \mid b$ , entonces  $d \mid a - qb = r$ . Luego  $d \mid (b, r) = f$ .

Como  $f \mid b$  y  $f \mid r$ , entonces  $f \mid qb - r = a$ . Luego  $f \mid (a, b) = d$ .

Por antisimetría,  $d \mid f$  y  $f \mid d \Rightarrow (a, b) = d = f = (b, r)$ .  $\square$

El Algoritmo de Euclides se basa en el hecho que en la división  $a = qb + r$ , podemos descartar el dividendo y calcular  $(a, b)$  como  $(b, r)$ .

# Algoritmo de Euclides

El algoritmo euclidiano se puede describir de la siguiente manera: sean  $a, b \in \mathbb{Z}$  cuyo máximo común  $(a, b)$  divisor se desea calcular. Como  $(|a|, |b|) = (a, b)$ , podemos suponer que  $a > b > 0$ . El primer paso es aplicar el Algoritmo de la División, para obtener

$$a = q_1 b + r_1, \quad \text{con } 0 \leq r_1 < b.$$

Si  $r_1 = 0$ , entonces  $b \mid a$  y  $(a, b) = b$ . Cuando  $r_1 \neq 0$ , dividimos  $b$  por  $r_1$  para producir enteros  $q_2, r_2$  tales que

$$b = q_2 r_1 + r_2, \quad \text{con } 0 \leq r_2 < r_1.$$

Si  $r_2 = 0$ , entonces  $r_1 \mid b$  y  $(b, r_1) = r_1$ , y nos detenemos. Caso contrario,  $r_2 \neq 0$ , continuamos este proceso y dividimos  $r_1$  por  $r_2$  para producir enteros  $q_3, r_3$  tales que

$$r_1 = q_3 r_2 + r_3, \quad \text{con } 0 \leq r_3 < r_2.$$

# Algoritmo de Euclides

Este proceso de división continúa hasta que aparece un residuo cero, digamos, en el paso  $n + 1$ , donde  $r_{n-1}$  se divide por  $r_n$ .

El resultado es el siguiente sistema de ecuaciones:

$$\begin{aligned}a &= q_1b + r_1, \quad 0 \leq r_1 < b \\b &= q_2r_1 + r_2, \quad 0 \leq r_2 < r_1 \\r_1 &= q_3r_2 + r_3, \quad 0 \leq r_3 < r_2 \\&\dots \\r_{n-2} &= q_nr_{n-1} + r_n, \quad 0 \leq r_n < r_{n-1} \\r_{n-1} &= q_{n+1}r_n + 0.\end{aligned}\tag{1}$$

Argumentamos que  $r_n$ , el último residuo distinto de cero que aparece de esta manera, es igual a  $(a, b)$ .

# Algoritmo de Euclides

## Teorema (Algoritmo de Euclides)

*En el sistema de ecuaciones (1), el máximo divisor común de  $a$  y  $b$  coincide con el último residuo diferente de cero. Esto es,  $(a, b) = r_n$ .*

Prueba:

Por el Lema de Euclides, del sistema de ecuaciones (1), podemos concluir que

$$(a, b) = (b, r_1) = (r_1, r_2) = (r_2, r_3) = \dots = (r_{n-1}, r_n) = (r_n, 0) = r_n.$$

Falta nada más garantizar un detalle. Que el sistema de ecuaciones (1) es posible. La construcción de las relaciones  $r_{i-1} = q_{i+1}r_i + r_{i+1}$ ,  $i = 0, 1, \dots, n$ , (aquí  $r_{-1} = a$ ,  $r_0 = b$ ) está garantizada por el Algoritmo de la División.

Ademas, de la relación de los residuos  $0 \leq r_i < r_{i-1}$ ,  $i = 1, 2, \dots, n$ ,

# Algoritmo de Euclides

se tiene que

$$0 = r_{n+1} < r_n < r_{n-1} < \dots < r_1 < b.$$

Por lo tanto hay a lo sumo  $b$  ecuaciones en el sistema (1). Esto garantiza que el Algoritmo de Euclides consiste a lo sumo de  $b$  pasos. En particular, es finito y termina.  $\square$

# Algoritmo de Euclides

**Ejemplo:** Hallar  $(12378, 3054)$ .

$$12378 = 4 \cdot 3054 + 162$$

$$3054 = 18 \cdot 162 + 138$$

$$162 = 1 \cdot 138 + 24$$

$$138 = 5 \cdot 24 + 18$$

$$24 = 1 \cdot 18 + 6$$

$$18 = 3 \cdot 6 + 0.$$

Luego,  $(12378, 3054) = 6$ .



# Algoritmo de Euclides

**Consecuencias:** A partir del algoritmo de Euclides, podemos calcular los coeficientes en el Teorema de Bézout.

$$12378 = 4 \cdot 3054 + 162$$

$$3054 = 18 \cdot 162 + 138$$

$$162 = 1 \cdot 138 + 24$$

$$138 = 5 \cdot 24 + 18$$

$$24 = 1 \cdot 18 + 6$$

$$18 = 3 \cdot 6 + 0.$$

$$\begin{aligned}(12378, 3054) = 6 &= 24 - 1(18) = 24 - 1(138 - 5 \cdot 24) = 6(24) - 1(138) \\&= 6(162 - 138) - 1(138) = 6(162) - 7(138) \\&= 6(162) - 7(3054 - 18 \cdot 162) = 132(162) - 7(3054) \\&= 132(12378 - 4 \cdot 3054) - 7(3054) = \mathbf{132}(12378) + (-\mathbf{535})(3054).\end{aligned}$$

# Algoritmo de Euclides

El algoritmo de Euclides puede escribirse en forma matricial. Observe que

$$a = q_1 b + r_1 \quad \Rightarrow \quad \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} b \\ r_1 \end{pmatrix}$$

Luego

$$\begin{aligned} \begin{pmatrix} a \\ b \end{pmatrix} &= \begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} b \\ r_1 \end{pmatrix} = \begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} q_2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} r_1 \\ r_2 \end{pmatrix} \\ &= \begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} q_2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} q_3 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} r_2 \\ r_3 \end{pmatrix} \\ &= \begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} q_2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} q_3 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} q_n & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} r_n \\ 0 \end{pmatrix} \\ &= \mathbf{M} \begin{pmatrix} r_n \\ 0 \end{pmatrix} \end{aligned}$$

# Algoritmo de Euclides

Si  $\mathbf{M} = \begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix}$ , y como  $\det \mathbf{M} = (-1)^n$ , entonces  $\mathbf{M}^{-1} = (-1)^n \begin{pmatrix} m_{22} & -m_{12} \\ -m_{21} & m_{11} \end{pmatrix}$ , y tenemos

$$\begin{pmatrix} r_n \\ 0 \end{pmatrix} = (-1)^n \begin{pmatrix} m_{22} & -m_{12} \\ -m_{21} & m_{11} \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}.$$

En particular  $(a, b) = r_n = (-1)^n(m_{22}a - m_{12}b)$ , da los coeficientes en el Teorema de Bézout.

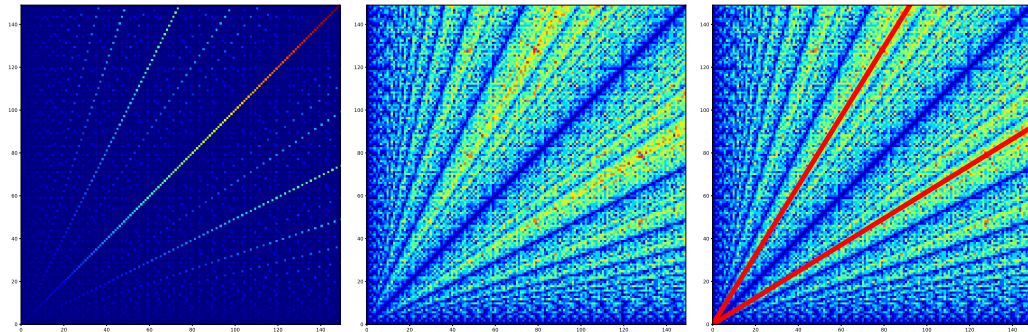
# Algoritmo de Euclides

La eficiencia computacional del algoritmo de Euclides se ha estudiado a fondo.

- A. A. L. REYNAUD (1811), demostró que el número de pasos de división en la entrada  $(a, b)$  está acotado por  $b$ .
- Más tarde mejoró esto a  $\frac{b}{2} + 2$ .
- P. J. E. FINCK (1841), mostró que el número de pasos de división es como máximo  $2 \log_2 b + 1$ .
- ÉMILE LÉGER (1837), estudió el peor caso.
- GABRIEL LAMÉ (1844), refina el análisis de Finck. Mostró que el número de pasos requeridos nunca es más de cinco veces el número  $h$  de dígitos en base 10 del número menor  $b$ .

**Obs!** El peor caso corresponde a cuando todo cociente  $q_i = 1$  en el sistema (1). Esto ocurre exactamente al tomar dos números de Fibonacci consecutivos.

# Algoritmo de Euclides



Comparación de valores en el algoritmo de Euclides. (a)  $d = (a, b)$ . (b) Número requerido de pasos. (c) Observe las diagonales que requieren más pasos coinciden con números  $a$  y  $b$  con una relación cercana al valor  $\varphi = \frac{1+\sqrt{5}}{2}$ , e.g. números de Fibonacci consecutivos.