

MÁS SOBRE EL ALGORITMO DE EUCLIDES

ALAN REYES-FIGUEROA
TEORÍA DE NÚMEROS

(AULA 05) 18.JULIO.2025

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.

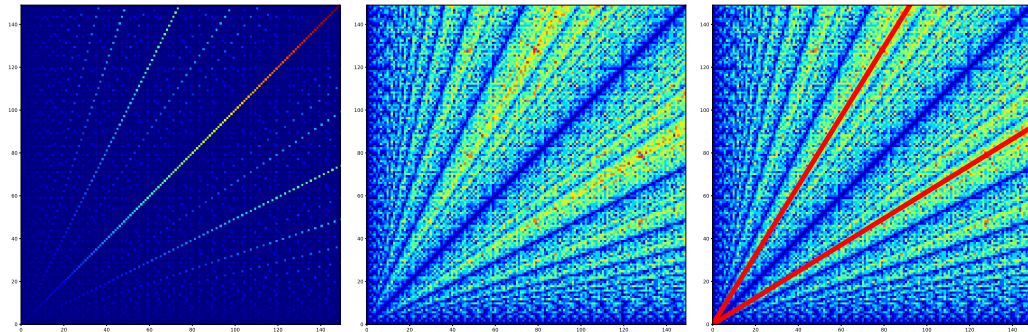
Algoritmo de Euclides

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.

Algoritmo de Euclides

Recordemos el algoritmo de Euclides. Si el proceso tiene exactamente $k + 1$ divisiones:

Se obtiene como resultado el siguiente sistema de ecuaciones:

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

donde $r_{k+1} = 0$, y r_k , el último residuo distinto de cero, es (a, b) .

Estimativa de LAMÉ

Sean $a \geq b \geq 0$. Recordemos que si el Algoritmo de Euclides hace $k + 1$ divisiones para hallar $d = (a, b)$, entonces en cada paso $r_{k+1} = q_k r_{k-1} + r_k$, $q_k \geq 1$, $b > r \geq 0$, se tiene

$$a = qb + r \geq b + r > 2r, \Rightarrow r < \frac{a}{2}.$$

Similarmente, $r_1 < \frac{b}{2} \leq \frac{a}{2}$, $r_2 < \frac{r}{2} < \frac{a}{4}$, $r_3 < \frac{r_1}{2} < \frac{b}{4} \leq \frac{a}{4}$, \dots , y en general

$$r_{2j} < \frac{a}{2^j}, \quad r_{2j+1} < \frac{a}{2^j} \quad \text{para } j = 1, 2, \dots, (k+1)/2.$$

Por otro lado, existe $t \in \mathbb{Z}^+$ tal que $a < 2^t \Rightarrow \log_2 a < t \Rightarrow r_{2t} < \frac{a}{2^t} < 1 \Rightarrow r_{2t} = 0$. (i.e., el algoritmo acaba a lo sumo en $2t$ pasos)

Si a tiene N dígitos en su representación decimal, entonces $a < 10^N$. Luego, $\log_2 a < N \log_2 10$.

Estimativa de LAMÉ

Así

$$k + 1 = 2t \leq 2(\lfloor \log_2 a \rfloor + 1) \leq 2(N \lfloor \log_2 10 \rfloor + 1) \approx 6.6N.$$

(LAMÉ, 1844).

Se puede mostrar que para que el Algoritmo de Euclides efectúe n pasos ($n = k + 1$), se debe tomar al menos $a = F_{n+2}$, $b = F_{n+1}$.

En particular $n < 2 \log_2 a \Rightarrow \frac{n}{2} < \log_2 a \Rightarrow a > 2^{n/2}$.

Recordemos la **Fórmula de BINET** (1843)

$$F_n = \frac{1}{\sqrt{5}} \left[\left(\frac{1 + \sqrt{5}}{2} \right)^n - \left(\frac{1 - \sqrt{5}}{2} \right)^n \right]$$

Como $\left(\frac{1 - \sqrt{5}}{2} \right)^n \rightarrow 0$, cuando $n \rightarrow \infty$, podemos simplificar

Estimativa de LAMÉ

$$F_n \approx \frac{1}{\sqrt{5}} \left(\frac{1 + \sqrt{5}}{2} \right)^n = \frac{1}{\sqrt{5}} \varphi^n,$$

donde $\varphi = \frac{1+\sqrt{5}}{2}$ es la razón áurea. (i.e., los F_n se parecen a los φ^n)

Recordemos que φ satisface $\varphi^2 - \varphi - 1 = 0$, de modo que $\varphi^2 = \varphi + 1$.
Afirmamos que $F_n \geq \varphi^{n-1}$, para todo $n \geq 1$.

$F_1 = 1 \geq \varphi^0$, $F_2 = 2 \geq \varphi$. Asumiendo la hipótesis inductiva que $F_k \geq \varphi^{k-1}$ siempre que $k \leq n$, entonces $F_{n+1} = F_n + F_{n-1} \geq \varphi^{n-1} + \varphi^{n-2} = \varphi^{n-2}(\varphi + 1) = \varphi^{n-2}\varphi^2 = \varphi^n$, lo que completa la afirmación.

Luego, $a = F_{n+2} \geq \varphi^{n+1}$ y vale que $n \leq n+1 = \log_{\varphi} \varphi^{n+1} \leq \log_{\varphi} a$.

Estimativa de LAMÉ

De esta última desigualdad, obtenemos

$$n \leq \log_{\varphi} a = \frac{\log_{10} a}{\log_{10} \varphi} \approx 4.7851..(\log_{10} a) < 5 \log_{10} a \leq 5N.$$

(Teorema de LAMÉ, 1844).