El algoritmo de Euclides

Ana Ofelia Negrete Fernández

24 de abril de 2022

1. Introducción

El algoritmo de Euclides afirma que podemos aplicar iteradas veces el algoritmo de la división hasta encontrar el máximo común divisor de dos enteros positivos a y b, mediante el siguiente procedimiento:

Sean a, b cualesquiera enteros positivos, con $a \neq b$ y $a > b$. Por el algoritmo de la división, sabemos que siempre existen $q, r \in \mathbb{Z}$ tales que podemos escribir

$$a = bq + r, \text{ con } \qquad 0 \leq r < b.$$

Luego, como b y r son enteros, también existen q_1 y r_1 tales que

$$b = rq_1 + r_1, \text{ con } \qquad 0 \leq r_1 < r.$$

Y como r y r_1 son enteros, existen q_2 y $r_2 \in \mathbb{Z}^+$ tales que

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

Se puede continuar así, de tal forma que en un penúltimo paso tendremos que existen q_i y r_i enteros tales que

$$r_{i-2} = r_{i-1} q_i + r_i, \text{ con } \qquad 0 \leq r_i < r_{i-1}.$$

Y el algoritmo termina cuando el residuo es cero. Es decir, existirán $q_{i+1} \in \mathbb{Z}^+$ y $r = 0$ tales que

$$r_{i-1} = r_i q_{i+1} + 0, \text{ con } \qquad 0 = r_{i+1} < r_i.$$

Luego entonces, el último residuo no cero es el máximo común divisor de a y b.

Este procedimiento lo podemos aplicar cuando a y b sean números muy grandes, de modo que determinar el máximo común divisor no es inmediato. Sin embargo, el algoritmo de Euclides es una receta aún sencilla, que hará fácil encontrar el MCD para cualquier pareja de números enteros.

Ejemplo. Encuentra el máximo común divisor de 3456 y 6524.

Solución. Observamos que $6524 > 3456$. Así,

$$6524 = 3456 \cdot 1 + 3068, \qquad 0 \leq 3068 < 3456.$$

Aplicando nuevamente el algoritmo de la división, obtenemos

$$3456 = 3068 \cdot 1 + 388, \qquad 0 \leq 388 < 3068.$$

Aplicando una vez más el algoritmo de la división, se tiene

$$3068 = 388 \cdot 7 + 352, \qquad 0 \leq 352 < 388.$$

Luego,

$$388 = 352 \cdot 1 + 36, \qquad 0 \leq 36 < 352.$$

$$352 = 36 \cdot 9 + 28, \qquad 0 \leq 28 < 36.$$

$$36 = 28 \cdot 1 + 8, \qquad 0 \leq 8 < 28.$$

$$28 = 8 \cdot 3 + 4, \qquad 0 \leq 4 < 8.$$

$$8 = 4 \cdot 2 + 0.$$

Como el último residuo no cero es 4, entonces 4 es el máximo común divisor de 6524 y 3456.

Observación. Aunque el algoritmo euclidiano requiere que los números a y b sean positivos, cuando ocurriera el caso de que uno de ellos o los dos fueran negativos, no se presentaría mayor obstáculo. Bastaría sacar el valor absoluto de ambos al inicio (ya que los divisores de un número negativo son los mismos que los de sus positivos).

Ejemplo. Obtén el máximo común divisor de -100 y 45.

Solución. Como uno de los números es negativo, antes que nada sacamos valores absolutos: $|-100| = 100$ y $|45| = 45$. Así,

$$100 = 45 \cdot 2 + 10, \qquad 0 \leq 10 < 45.$$

$$45 = 10 \cdot 4 + 5, \qquad 0 \leq 5 < 10.$$

$$10 = 5 \cdot 2 + 0.$$

Por lo tanto, $MCD(-100, 45) = 5$.

2. Demostración del algoritmo de Euclides

La clave por la que el algoritmo de Euclides funciona es el siguiente teorema:

Teorema. *Sean $a, b \in \mathbb{Z}^+$, tales que $a = bq + r$. Entonces $MCD(a, b) = MCD(b, r)$.*

Dem.- Sean $a, b \in \mathbb{Z}^+$ y sea d algún divisor común de a y b elegido arbitrariamente. Como d es divisor de a, entonces $d \mid a$. Asímismo, d es divisor de b, por lo tanto $d \mid b$.

Ya que $d \mid b$, entonces $d \mid bq$.

Ya que $d \mid a$ y $d \mid bq$, también $d \mid a - bq$.

Ya que $a = bq + r$ y $d \mid a - bq$, entonces $d \mid r$. $\quad (*)$

Ahora, fijándonos en los divisores comunes de b y r, sea f un divisor común de b y r tomado arbitrariamente. Se tiene, por lo tanto, que $f \mid b$ y $f \mid r$.

Ya que $f \mid b$, entonces $f \mid bq$.

Ya que $f \mid bq$ y $f \mid r$, también $f \mid bq + r$.

Ya que $a = bq + r$, entonces $f \mid a$. $\quad (**)$

En conclusión, de $(*)$, hemos demostrado que cualquier divisor de a y b es también divisor de r. Y con $(**)$ mostramos que cualquier divisor de b y r es también divisor de a. En otras palabras, "d es divisor de a y b si y sólo si d es divisor de b y r."

Así pues, el conjunto de todos los divisores de a y b es igual al conjunto de todos los divisores de b y r; en particular, el máximo común divisor de a y b debe ser igual al máximo común divisor de b y r.

$\square$

Usando el teorema recién demostrado y regresando al algoritmo de Euclides en el primer paso, si $a = bq + r$, deducimos que $MCD(a, b) = MCD(b, r)$.

En el siguiente paso del algoritmo euclidiano, $b = rq_1 + r_1$. Por lo tanto $MCD(b, r) = MCD(r, r_1)$.

En el tercer paso, $r = r_1 q_2 + r_2$. Así, $MCD(r, r_1) = MCD(r_1, r_2)$.

En el penúltimo paso, $r_{i-2} = r_{i-1} q_i + r_i$. Por lo que $MCD(r_{i+2}, r_{i-1}) = MCD(r_{i-1}, r_i)$.

En el último paso, $r_{i+1} = r_i q_{i+1} + 0$. Por lo que $MCD(r_{i+1}, r_i) = MCD(r_i, 0) = r_i$.

Así pues,

$$MCD(a, b) = MCD(b, r) = MCD(r, r_1) = MCD(r_1, r_2) = \dots$$
$$\dots = MCD(r_{i+2}, r_{i-1}) = MCD(r_{i-1}, r_i) = MCD(r_i, 0) = r_i.$$

Esto demuestra que efectivamente, el último residuo no cero en el algoritmo de Euclides, es igual al máximo común divisor de los números a, b iniciales.

$\square$