AMPLIACIÓN DE MATEMÁTICAS

EL ALGORITMO DE EUCLIDES.

El **algoritmo de Euclides** es un método "rápido" de hallar el **máximo común divisor** de dos números (o de dos polinomios, como veremos más adelante).

Vamos a ver dos algoritmos en uno, de suerte que vamos a calcular el m.c.d. así como la identidad de Bezout asociada al mismo (más adelante veremos que este es el camino para calcular elementos inversos en cuerpos finitos). El método es esencialmente práctico y lo usaremos en buena parte de los problemas referidos a **congruencias** de números (o de polinomios, como más adelante veremos).

Señalar que este método de cálculo del m.c.d. se encuentra al principio del libro séptimo de los Elementos de Euclides.

El algoritmo se basa en el siguiente hecho.

Lema 1. *Sean* $a, b \in \mathbb{N}\backslash\{0\}$, *de modo que* $a = qb + r$, $0 < r < b$, *entonces*

$$m.c.d.(a, b) = m.c.d.(b, r).$$

Demostración: Si $d|a$ y $d|b$, entonces también $d|r$. Al contrario, si $d|b$ y $d|r$, entonces también $d|a$. Es decir los divisores comunes de a y b son los mismos que los de b y r, por tanto el mayor de esos divisores comunes es el m.d.c. tanto de a y b, como de b y $r\square$

Teorema 1. *(**Algoritmo de Euclides.**) Dados dos números naturales* $a, b \in \mathbb{N}\backslash\{0\}$ *se define la sucesión decreciente de números naturales*

$$b = r_1 > r_2 > r_3 > ... > r_n > r_{n+1} = 0$$

dada por la relación

$$r_{i-1} = q_i r_i + r_{i+1} \text{ donde } r_0 = a \ (es \ decir \ a = q_1 b + r_2).$$

Entonces $m.c.d.(a, b) = r_n$.

Demostración: Claramente, por el Teorema del Resto, $0 \leq r_{i+1} < r_i$ para todo i. De ello se deduce que en una cantidad finita de divisiones llegaremos a que algún $r_{n+1} = 0$.

Por otro lado el lema anterior nos dice que

$$m.c.d.(a,b) = m.c.d(b,r_2) = m.c.d(r_2,r_3) = ... = m.c.d(r_{n-1},r_n) = r_n$$

donde la última igualdad se da ya que $r_{n+1} = 0$, por tanto $r_n | r_{n-1} \square$

Ejemplo 1. *¿m.c.d.*(10,672, 4,147)*?*

Primero dividimos

$$\begin{array}{cc|c} 10672 & 4147 & 2 \\ 2387 & & \end{array} \; ; \; \begin{array}{cc|c} 4147 & 2387 & 1 \\ 1769 & & \end{array} \; ; \; \begin{array}{cc|c} 2387 & 1769 & 1 \\ 0609 & & \end{array} \; ; \; \begin{array}{cc|c} 1769 & 609 & 2 \\ 551 & & \end{array} \; ;$$

$$\begin{array}{cc|c} 609 & 551 & 1 \\ 058 & & \end{array} \; ; \; \begin{array}{cc|c} 551 & 58 & 9 \\ 29 & & \end{array} \quad \text{y} \quad \begin{array}{cc|c} 58 & 29 & 2 \\ 0 & & \end{array}$$

Escribimos la tabla

i	0	1	2	3	4	5	6	7	8	9
r_i	10672	4147	2378	1769	609	551	58	29	0	
q_i		2	1	1	2	1	9	2		
α_i	1	0								
β_i	0	1								

De momento las filas α_i y β_i no nos interesan. Lo que vemos es que el resto octavo se anula ($r_8 = 0$), luego el m.c.d. que buscamos es precisamente el resto anterior. Así en nuestro ejemplo, $m.c.d.(10672, 4147) = r_7 = 29$.

Otra forma del Algoritmo de Euclides

Teorema 2. *Sean $a, b \in \mathbb{N}\backslash\{0\}$, de modo que $a = qb + r$, $0 < r < b$. Generamos una tabla de cuatro entradas: r, q, α y β.*

i	*0*	*1*	*2*	*3*
r_i	a	b	r	
q_i		q		
α_i	*1*	*0*		
β_i	*0*	*1*		

donde se definen

$$\begin{array}{rcll} r_i & = & r_{i-2} & - \; q_{i-1} r_{i-1} \\ \alpha_i & = & \alpha_{i-2} & - \; q_{i-1} \alpha_{i-1} \quad \textit{para todo } i \geq 2, \\ \beta_i & = & \beta_{i-2} & - \; q_{i-1} \beta_{i-1} \end{array}$$

siendo

$$r_0 = a, \;\; \alpha_0 = 1 \;\; y \;\; \beta_0 = 0$$

y

$$r_1 = b, \;\; \alpha_1 = 0 \;\; y \;\; \beta_1 = 1.$$

Entonces la sucesión

$$a = r_0 > b = r_1 > r_2 > .... > r_n > r_{n+1} = 0$$

que se obtiene es decreciente y además

$$m.c.d.(a, b) = r_n$$

y

$$m.c.d.(a, b) = \alpha_n a + \beta_n b.$$

Demostración: La relación $r_i = r_{i-2} - q_{i-1} r_{i-1}$ es equivalente a $r_{i-2} = q_{i-1} r_{i-1} + r_i$ que es la recurrencia que aparecía en el Teorema anterior. Por tanto es claro que la sucesión de r_i que genera es la misma; así, decreciente y cuyo término anterior al nulo es el m.c.d. buscado.

Por otro lado es claro que

$$a = r_0 = \alpha_0 a + \beta_0 b$$

y

$$r_1 = \alpha_1 a + \beta_1 b$$

por la elección arbitraria de los primeros α_i y β_i. Ahora procederemos por inducción. Supuesto que $r_j = \alpha_j a + \beta_j b$ para todo $j \leq i$, entonces usando esta hipótesis de inducción

$$r_{i+1} = r_{i-1} - q_i r_i = \alpha_{i-1} a + \beta_{i-1} b - q_i(\alpha_i a + \beta_i b)$$
$$= (\alpha_{i-1} - q_i \alpha_i) a + (\beta_{i-1} - q_i \beta_i) b = \alpha_{i+1} a + \beta_{i+1} b.$$

En particular $m.c.d.(a, b) = r_n = \alpha_n a + \beta_n b \square$

Ejemplo 2. *¿$m.c.d.(10672, 4147)$? Y ¿$m.c.d.(10672, 4147) = \alpha$10,672+ β4,147?*

Lo primero es dividir, pero esa operación ya la hemos realizado arriba. Ahora completando la tabla

i	0	1	2	3	4	5	6	7	8	9
r_i	10672	4147	2378	1769	609	551	58	29	0	
q_i		2	1	1	2	1	9	2		
α_i	1	0	1	-1	2	-5	7	-68		
β_i	0	1	-2	3	-5	13	-18	175		

Deducimos que

$$\begin{aligned} m.c.d.(10672, 4147) = r_7 = 29 = \alpha_7 10{,}672 + \beta_7 4{,}147 \\ = -68 \times 10{,}672 + 175 \times 4{,}147. \end{aligned}$$

Referencias

Departamento de Análisis Matemático, Facultad de Matemáticas, Universidad Complutense, 28040 Madrid, Spain

E-mail address: Cesar_Ruiz@mat.ucm.es