AMPLIACIÓN DE MATEMÁTICAS

EL ALGORITMO DE EUCLIDES.

El cálculo de *m.c.d* y de identidades de Bezout, así como su aplicación en congruencias de polinomios (que veremos en el siguiente tema), requiere de una herramienta efectiva para dicho cálculo: **el Algoritmo de Euclides**.

El algoritmo se basa en el siguiente hecho.

Lema 1. *Sean* $P, Q \in \mathbb{F}[x] \backslash \{0\}$*, de modo que* $P = qQ + r$*,* $r \neq 0$ *y* $0 \leq grad.r < grad.Q$*, entonces*

$$m.c.d.(P, Q) = m.c.d.(Q, r)$$

Demostración: Si $d|P$ y $d|Q$, entonces también $d|r = P - qQ$. Al contrario, si $d|Q$ y $d|r$, entonces también $d|P$. Es decir los divisores comunes de P y Q son los mismos que los de Q y r, por tanto los de mayor grado de estos divisores comunes forman tanto el $m.d.c.$ de P y Q, como él de Q y $r\square$

Teorema 1. *(**Algoritmo de Euclides**). Sean* $P, Q \in \mathbb{F}[x] \backslash \{0\}$*, de modo que* $P = qQ + r$*, y* $0 \leq grad.r < grad.Q$*. Generamos una tabla de cuatro entradas:* r, q, α *y* β*.*

i	*0*	*1*	*2*	*3*
r_i	P	Q	r	
q_i		q		
α_i	*1*	*0*		
β_i	*0*	*1*		

donde se definen

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

siendo

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

y

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

Entonces la sucesión de grados de polinomios

$$grad.P = grad.r_0 \geq grad.Q = grad.r_1 > grad.r_2 > .... > grad.r_n \geq 0$$

con $r_{n+1} = 0$*, que se obtiene es decreciente en el grado y además*

$$m.c.d.(P, Q) = r_n$$

y

$$m.c.d.(P, Q) = \alpha_n P + \beta_n Q.$$

Demostración: Análoga a la que se ve para números enteros.

- Que $m.c.d.(P, Q) = r_n$ es una sencilla aplicación del Lema teniendo en cuenta que
$$m.c.d.(r_n, r_{n+1}) = m.c.d.(r_n, 0) = r_n.$$
- Por otro lado es claro que
$$P = r_0 = \alpha_0 P + \beta_0 Q$$
y
$$r_1 = \alpha_1 P + \beta_1 Q$$
por la elección arbitraria de los primeros α_i y β_i. Ahora procederemos por inducción. Supuesto que $r_j = \alpha_j P + \beta_j Q$ para todo $j \leq i$, entonces usando esta hipótesis de inducción
$$\begin{aligned} r_{i+1} &= r_{i-1} - q_i r_i = \alpha_{i-1} P + \beta_{i-1} Q - q_i(\alpha_i P + \beta_i Q) \\ &= (\alpha_{i-1} - q_i\alpha_i)P + (\beta_{i-1} - q_i\beta_i)Q = \alpha_{i+1} P + \beta_{i+1} Q. \end{aligned}$$
En particular $m.c.d.(P, Q) = r_n = \alpha_n P + \beta_n Q \square$

Ejemplo 1. *Dados* $P(x) = x^4 - x^3 + x^2 + x - 2, Q(x) = x^3 - 1 \in \mathbb{Q}[x]$*, queremos calcular* $m.c.d.(P, Q)$ *y la identidad de Bezout asociada.*

En primer lugar hay que dividir polinomios para calcular la sucesión de restos decrecientes en grado.

$$\begin{array}{rl} x^4 - x^3 + x^2 + x - 2 & \underline{|x^3 - 1} \\ \underline{-x^4 \qquad\qquad + x} & \;\; x - 1 \\ -x^3 + x^2 + 2x - 2 & \\ \underline{x^3 \qquad\qquad\quad - 1} & \\ x^2 + 2x - 3 & \end{array}$$

$$\begin{array}{l|l} x^3 \qquad\qquad -1 & x^2+2x-3 \\ \underline{-x^3-2x^2+3x} & x-2 \\ -2x^2+3x-1 & \\ \underline{2x^2+4x-6} & \\ 7x-7 & \end{array} \qquad \begin{array}{l|l} x^2+2x-3 & 7x-7 \\ \underline{-x^2+x} & \frac{1}{7}x-\frac{3}{7} \\ 3x-3 & \\ \underline{-3x+3} & \\ 0 & \end{array}$$

A continuación escribimos la tabla del algoritmo:

i	0	1	2	3	4
r_i	$x^4-x^3+x^2+x-2$	x^3-1	x^2+2x-3	$7x-7$	0
q_i		$x-1$	$x-2$	$\frac{1}{7}x-\frac{3}{7}$	
α_i	1	0	1	$-x+2$	
β_i	0	1	$-x+1$	x^2-3x+3	

Así

$$m.c.d.(x^4-x^3+x^2+x-2, x^3-1) = 7x-7$$
$$= (2-x)(x^4-x^3+x^2+x-2) + (x^2-3x+3)(x^3-1).$$

Por último el máximo común divisor mónico es $x-1$ $\square$

Ejemplo 2. *Dados $P(x) = x^5+5x^4+3x^3+2x+1, Q(x) = x^4+3 \in \mathbb{Z}_7[x]$, queremos calcular $m.c.d.(P,Q)$ y la identidad de Bezout asociada.*

Antes de empezar a operar necesitamos conocer

$(\mathbb{Z}_7, \times)$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

En primer lugar hay que dividir polinomios para calcular la sucesión de restos decrecientes en grado.

$$\begin{array}{l|l} x^5+5x^4+3x^3+2x+1 & x^4+3 \\ \underline{-x^5 \qquad\qquad -3x} & x+5 \\ 5x^4+3x^3+6x+1 & \\ \underline{-5x^4 \qquad\qquad -1} & \\ 3x^3+6x & \end{array}$$

$$\begin{array}{l|l} x^4 \qquad\qquad +3 & 3x^3+6x \\ \underline{-x^4-2x^2} & 5x \\ -2x^2+3 & \end{array} \qquad \begin{array}{l|l} 3x^3+6x & 5x^2+3 \\ \underline{-3x^3-6x} & 2x \\ 0 & \end{array}$$

A continuación escribimos la tabla del algoritmo:

i	0	1	2	3	4
r_i	$x^5+5x^4+3x^3+2x+1$	x^4+3	$3x^3+6x$	$5x^2+3$	0
q_i		$x+5$	$5x$	$2x$	
α_i	1	0	1	$2x$	
β_i	0	1	$6x+2$	$5x^2+4x+1$	

Así

$$m.c.d.(x^5+5x^4+3x^3+2x+1, x^4+3) = 5x^2+3$$

$$= 2x(x^5+5x^4+3x^3+2x+1) + (5x^2+4x+1)(x^4+3).$$

Por último el máximo común divisor mónico es $3(5x^2+3) = x^2+2$ $\square$

Referencias

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

Email address: Cesar_Ruiz@mat.ucm.es