Construcción de Algoritmos para trabajar con polinomios

Alberto Marileo Benjamín Jiménez
Benjamín Junemann

Departamento de Ingeniería Matemática
Universidad de Concepción

Junio 2025

Índice

1 Motivación

2 Resultados en $\mathbb{Z}$

3 Extensión a $\mathbb{R}[x]$

4 Teorema de las Raíces Racionales

5 Funciones racionales

6 Conclusión

Motivación

- Los **Polinomios** son un elemento muy importante en diversas areas de la **Matematica, Fisica, Biologia o Ingeneria**.
- Sin embargo algunas veces trabajar con ellos nos lleva a calculos complejos o tediosos.

Definiciones previas para $(\mathbb{Z})$

1. Sean a, b enteros diremos que a **divide a** b si existe un entero k tal que $ak = b$.
2. Sean a, b enteros diremos que $a|b$ si y solo si a **divide a** b.
3. Diremos que el **Maximo comun divisor** de a y b es **d** $(mcd(a, b) = d)$ si se cumple que:
   - $d|a$ y $d|b$
   - Si $\hat{d}$ es otro entero tal que $\hat{d}|a$ y $\hat{d}|b$ entonces $\hat{d}|d$.

División Euclidiana ($\mathbb{Z}$)

Division Euclideana

$\forall (a, d) \in \mathbb{Z} \times \mathbb{Z}^* : \exists! (q, r) \in \mathbb{Z} \times \mathbb{Z} : a = dq + r, 0 \leq r < |d|.$

Donde $\mathbb{Z}^* = \mathbb{Z} \backslash \{0\}$

Proposicion

Sean $a, b \in \mathbb{Z}$, con $b \neq 0$. Sean q y r el cociente y el resto obtenidos al aplicar el **Algoritmo de la Division** a **a** y **b** es decir $a = bq + r$. Entonces se cumple que:

$$mcd(a, b) = mcd(b, r) \ .$$

Algoritmo de Euclides ($\mathbb{Z}$)

Algoritmo de Euclides

Dados $a, b \in \mathbb{Z}^+$, con $a > b$ y **b no es factor de a**.
Sean

$$\begin{gathered}
(q_1, r_1) \in \mathbb{Z} \times \mathbb{Z}_0^+ : a = bq_1 + r_1, \quad 0 < r_1 < b \\
(q_2, r_2) \in \mathbb{Z} \times \mathbb{Z}_0^+ : b = r_1 q_2 + r_2, \quad 0 < r_2 < r_1 \\
\vdots \\
(q_m, r_m) \in \mathbb{Z} \times \mathbb{Z}_0^+ : r_{m-2} = r_{m-1} q_m + r_m, \quad 0 < r_m < r_{m-1} \\
(q_{m+1}, r_{m+1}) \in \mathbb{Z} \times \mathbb{Z}_0^+ : r_{m-1} = r_m q_{m+1}, \quad r_{m+1} = 0
\end{gathered}$$

Entonces $r_m = mcd(a, b)$

Notemos además que $r_m = mcd(a, b)$ se obtiene luego de una cantidad finita de pasos, ya que

$$r_m < r_{m-1} < \cdots < r_1 \text{ y } r_m = mcd(a, b) \geq 1.$$

Identidad de Bézout ($\mathbb{Z}$)

Identidad de Bezout

Sean $a, b \in \mathbb{Z} \setminus \{0\}$, y sea $d := \text{mcd}(a, b)$. Entonces

$$\exists (x, y) \in \mathbb{Z}^2 : ax + by = d$$

Extension a $\mathbb{R}[x]$

- Buscaremos extender los resultados y herramientas anteriores a $\mathbb{R}[x]$, es decir, al espacio de los **Polinomios**.

- Para ello, necesitaremos las siguientes definiciones

Definiciones previas para $(\mathbb{R}[x])$

División Euclidiana Polinomios

$$\forall (A, B) \in \mathbb{R}[X] \times \mathbb{R}[X]^* : \exists! Q, R \in \mathbb{R}[X] :$$

$$A = BQ + R \quad , grad(R) < grad(B)$$

Definiciones previas para ($\mathbb{R}[x]$)

Divisibilidad en Polinomios

Diremos que $Q(x) \in \mathbb{R}[X]^*$ divide a $P(x) \in \mathbb{R}[X]$ y escribiremos $Q(x) \mid P(x)$ si al realizar la **Division Euclideana** entre $P(x)$ y $Q(x)$ su resto $R(x)$ es 0, es decir:

$$\exists B(x) \in \mathbb{R}[X]^* : P(x) = Q(x)B(x) + 0$$

Definiciones previas para $(\mathbb{R}[x])$

Máximo Común Divisor Polinomios

Sean $P(x), Q(x) \in \mathbb{R}[x]^*$ El *máximo común divisor* de P y Q es el polinomio $D(x) \in \mathbb{R}[x]$ que cumple:

1. $D(x) \mid P(x)$ y $D(x) \mid Q(x)$;
2. Si $E(x) \in \mathbb{R}[x]$ divide simultáneamente a P y Q, entonces $E(x) \mid D(x)$;
3. $D(x)$ es **mónico**, es decir, su coeficiente líder es 1.

En tal caso, escribimos

$$D(x) = mcd(P(x), Q(x)).$$

- Usando todas las definiciones anteriores buscamos generalizar el **Algoritmo de Euclides** y **Lema de Bezout**.

Algoritmo de Euclides ($\mathbb{R}[x]$)

Algoritmo de Euclides

Dados $P_1, P_2 \in \mathbb{R}[X]$, con $grad(P_2) \leq grad(P_1)$

$$\begin{array}{l} (Q_1, R_1) \in \mathbb{R}[X] \times \mathbb{R}[X]^* : P_1 = P_2 Q_1 + R_1, \quad grad(R_1) < grad(P_2) \\ (Q_2, R_2) \in \mathbb{R}[X] \times \mathbb{R}[X]^* : P_2 = Q_2 R_1 + R_2, \quad grad(R_2) < grad(R_1) \\ \vdots \\ (Q_m, R_m) \in \mathbb{R}[X] \times \mathbb{R}[X]^* : R_{m-2} = R_{m-1} Q_m + R_m, grad(R_m) < grad(R_{m-1}) \\ (Q_{m+1}, R_{m+1}) \in \mathbb{R}[X] \times \mathbb{R}[X]^* : R_{m-1} = R_m Q_{m+1} + R_{m+1}, \quad R_{m+1} = 0 \end{array}$$

Sea A el coeficiente principal de R_m, luego se tiene que $\frac{1}{A} R_m = mcd(P_1, P_2)$

Notemos que, similarmente al caso de $\mathbb{Z}$, el algoritmo termina en pasos finitos ya que

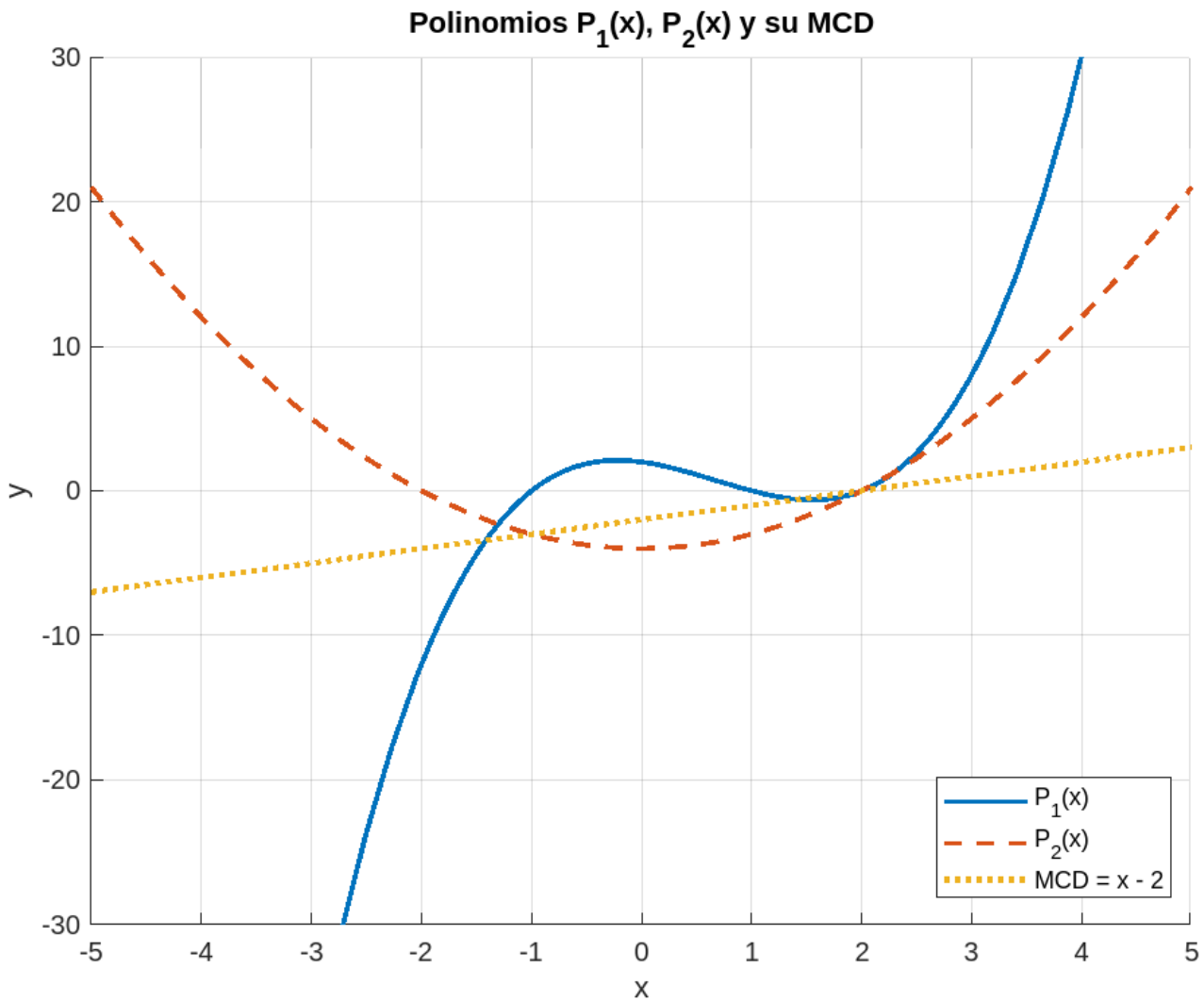
$$grad(R_{m+1}) < grad(R_m) < \cdots < grad(R_1) \text{ y } grad(R_{m+1}) = 0.$$

Ejemplos

Encuentre el **MCD** de los siguientes **polinomios**:

1. $P_1(x) = (x-2)(x^2-1), \quad P_2(x) = (x-2)(x+2).$
2. $P_1(x) = x^6 - 22x^5 + 190x^4 - 820x^3 + 1849x^2 - 2038x + 840$
   $P_2(x) = x^5 - 45x^4 + 805x^3 - 7155x^2 + 31594x - 55440$

Para el segundo ejemplo usaremos el **Algoritmo de Euclides** implementado en **Matlab**.


Polinomios P1(x), P2(x) y su MCD
30
20
10
0
-10
-20
-30
y
-5
-4
-3
-2
-1
0
1
2
3
4
5
x
P1(x)
P2(x)
MCD = x - 2

Identidad de Bézout ($\mathbb{R}[x]$)

Identidad de Bezout en $\mathbb{R}[x]$

Sean $P_1, P_2 \in \mathbb{R}[X]^*$. Entonces $\exists (A, B) \in (\mathbb{R}[X])^2$:

$$A(x)P_1 + B(x)P_2 = mcd(P_1, P_2)$$

Demostración.

Supongamos que hemos aplicado el **Algoritmo de Euclides** a P_1 y P_2 y se tiene que $R_{m+1} = mcd(P_1, P_2)$ es decir el algoritmo ha terminado en $m+1$ pasos. (Notar que $m+1$ es finito ya que $grad(R_{i+1}) < grad(R_i), \quad \forall i \in \{1, \ldots, m\}$)
Buscaremos mostrar que:

$$R_j = A_j(x)P_1 + B_j(x)P_2 \quad , \forall j \in \{1, \ldots, m\}$$

Del **Algoritmo de Euclides** sabemos que:

$$R_j = R_{j-2} - R_{j-1}Q_j \quad , \forall j \in \{1, \ldots, m+1\}$$

.

Usaremos inducción sobre j, notando que para $j = 1, j = 2$ se cumple que:

$$\begin{aligned} R_1 &= P_1 - P_2 Q_1 \\ R_2 &= P_2 - Q_2 R_1 = P_2 - Q_2(P_1 - P_2 Q_1) \\ &= P_2 - Q_2 P_1 + P_2 Q_1 Q_2 = (-Q_2)P_1 + (Q_1 Q_2 + 1)P_2 \end{aligned}$$

Supongamos que $R_j = A_j(x)P_1 + B_j(x)P_2 \quad , \forall j \in \{1, \ldots, m\}$, luego

$$\begin{aligned} R_{m+1} &= R_{m-1} - R_m Q_{m+1} \\ &= A_{m-1}P_1 + B_{m-1}P_2 - Q_{m+1}(A_m P_1 + B_m P_2) \\ &= (A_{m-1} - Q_{m+1}A_m)P_1 + (B_{m-1} - Q_{m+1}B_m)P_2 \end{aligned}$$

Por tanto hemos mostrado que $R_{m+1} = mcd(P_1, P_2) = A(x)P_1 + B(x)P_2$.

□

La demostración anterior nos entrega un algoritmo para encontrar **A(x)** y **B(x)**.

Algoritmo de Bézout

Algoritmo de Bezout

Sean $P_1, P_2 \in \mathbb{R}[X]^*$ luego para encontrar los **Coeficientes de Bezout**:
Sean $R_0 := P_1, \quad A_0 := 1, \quad B_0 := 0, \quad R_1 := P_2, \quad A_1 := 0, \quad B_1 := 1$.
Ademas al inicio, se cumple que $R_k = A_k P_1 + B_k P_2$ para $k = 0, 1$.
Luego mientras $R_i \neq 0$:

1. Realizar la división euclidiana entre R_{i-2} y R_{i-1}, obteniendo:

$$R_{i-2} = Q_i R_{i-1} + R_i, \quad grad(R_i) < grad(R_{i-1}).$$

2. Actualizar los coeficientes de la combinación:

$$A_i := A_{i-2} - Q_i A_{i-1}, \qquad B_i := B_{i-2} - Q_i B_{i-1}.$$

Si $R_i = 0$, detener y fijar $m := i - 1$. Por tanto, el último resto no nulo R_m es:

$$D := R_m = mcd(P_1, P_2), \quad A := A_m, \quad B := B_m,$$

y se cumple que:

$$A\,P_1 + B\,P_2 = mcd(P_1, P_2) = D.$$

Por tanto, hemos obtenido los **Coeficientes de Bezout A** y **B**.

Ejemplos

Calcular el **MCD** y los **Coeficientes de Bezout** de los siguientes **polinomios**:

1. $P_1(x) = x^3 - 1, \quad P_2(x) = x^2 + 1.$
2. $P_1(x) = -5x^4 + 6x^3 - 7x^2 + 3x + 2$ y
   $P_2(x) = 3x^4 + 4x^3 - 5x^2 + 6x - 7$

Para el segundo ejemplo usaremos el **Algoritmo de Bezout** implementado en **Matlab**.

El Teorema de las Raíces Racionales

Teorema de las Raíces Racionales

Sea $p(x) := a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ un polinomio tal que $a_i \in \mathbb{Z}\ \forall i \in \{0, \ldots, n\}$ y $a_0, a_n \neq 0$. Si $x = \frac{p}{q}$ con $mcd(p, q) = 1$ es raíz de p, entonces $p \mid a_0$ y $q \mid a_n$.

- El Teorema anterior induce un algoritmo para encontrar **raices racionales**

Ejemplos

Calcule, si es que existen las **raices racionales de los siguientes polinomios**.

1. $p(x) = 2x^3 - 3x^2 + 1$
2. $\vartheta(x) = 24x^6 - 7x^5 + 7x^4 + 2x^3 - 6x^2 + x + 8$
3. $\varsigma(x) = x^5 - 11x^4 + 2x^3 + 226x^2 - 803x + 585$

Para el segundo y tercer ejemplo usaremos el **Algoritmo** obtenido del teorema anterior implementado en **Matlab**.

Funciones Racionales

Las funciones racionales de la forma $f(x) = \frac{P(x)}{Q(x)}$, donde $P, Q \in \mathbb{R}[X]$, son comunes en diversos problemas matemáticos.

En busca de simplificar estos problemas, hacemos lo siguiente:

Descomposición de funciones racionales

Supongamos que $Q(x)$ no es irreducible en $\mathbb{R}[X]$. Entonces, puede factorizarse como:

$$Q(x) = Q_1(x) \cdot Q_2(x), \quad \text{donde } Q_1, Q_2 \in \mathbb{R}[X] \quad y \quad mcd(Q_1, Q_2) = 1,$$

Además, $grad(Q_1), grad(Q_2) < grad(Q)$.

Por la **Identidad de Bézout**, existen polinomios $A_0(x), A_1(x) \in \mathbb{R}[X]$ tales que:

$$A_0(x)Q_1(x) + A_1(x)Q_2(x) = 1.$$

Descomposición de funciones racionales

Sustituyendo en $f(x)$, se obtiene:

$$f(x) = \frac{P(x) \cdot (A_0(x)Q_1(x) + A_1(x)Q_2(x))}{Q_1(x)Q_2(x)} = \frac{P(x)A_0(x)}{Q_2(x)} + \frac{P(x)A_1(x)}{Q_1(x)}.$$

Ejemplos

Calcular la Serie de Taylor alrededor de $x = 0$ de la función racional:

$$f(x) = \frac{2x^4 - x^3 + 3x^2 + x + 5}{\left(1 - x^2\right)(1 - 2x)}$$

Para ello, usaremos lo anterior y el **Algoritmo de Bezout** implementado en Matlab.

Conclusión

- Extendimos resultados clasicos de $\mathbb{Z}$ a $\mathbb{R}[x]$.
- En base a lo obtenido, generamos **Algoritmos** que nos ayudaran al trabajo con **Polinomios**

Referencias


Wikipedia contributors. *Euclidean division*. Wikipedia, The Free Encyclopedia.
https://en.wikipedia.org/wiki/Euclidean_division


Wikipedia contributors. *Euclidean Algorithm*. Wikipedia, The Free Encyclopedia.
https://en.wikipedia.org/wiki/Euclidean_algorithm


Wikipedia contributors. *Rational Root Theorem*. Wikipedia, The Free Encyclopedia.
https://en.wikipedia.org/wiki/Rational_root_theorem


Wikipedia contributors. *RSA cryptosistem*. Wikipedia, The Free Encyclopedia.
https://en.wikipedia.org/wiki/RSA_cryptosystem


Rommel Bustinza. *Curso TRM-1 2024, Universidad de Concepcion*.
https://shorturl.at/NRhRs