UNIVERSIDAD DE CONCEPCION
FACULTAD DE CIENCIAS FISICAS Y MATEMATICAS
DEPARTAMENTO DE INGENIERIA MATEMATICA

Taller 1 Concepción 2025, Mayo

Division Euclidiana de polinomios, Identidad de bezout y Algoritmo Generalizado de Euclides. Racices de Polinomios de Coeficientes Enteros

Alberto Marileo
Benjamin Jimenez
Benjamin Junemann

1. Introduccion

En este trabajo desarrollaremos herramientas fundamentales para el trabajo con polinomios, centrándonos en:

- **Division de Polinomios**
- **Descomposición en fracciones simples de funciones racionales**
- **Cálculo de raíces para polinomios con coeficientes enteros**

Comenzaremos con un repaso de resultados clásicos sobre divisibilidad en $\mathbb{Z}$, que luego generalizaremos al contexto de polinomios. A continuación, demostraremos el Teorema de las Raíces Racionales, una herramienta poderosa para identificar raíces en polinomios con coeficientes enteros. Finalmente, implementaremos algoritmos que automatizan estos procesos, combinando teoría y aplicaciones prácticas.

1.1. Notacion

- Sean a, b enteros diremos que a **divide a** b si existe un entero k tal que $ak = b$.
- Sean a, b enteros diremos que $a|b$ si y solo si a **divide a** b.
- Diremos que el **Maximo comun divisor** de a y b es **d** ($mcd(a, b) = d$) si se cumple que:
  1. $d|a$ y $d|b$
  2. Si $\hat{d}$ es otro entero tal que $\hat{d}|a$ y $\hat{d}|b$ entonces $\hat{d}|d$.
- Sea $\mathbb{R}[X]$ es el conjunto de todos los polinomios variable de x y coeficientes en $\mathbb{R}$ y $\mathbb{R}[X]^*$ es el conjunto de todos los polinomios con coeficientes en $\mathbb{R}$ menos el polinomio nulo.

2. Division Euclideana

La división euclidiana es un algoritmo que nos muestra el proceso de division de números enteros que produce un cociente y un resto. Es definida de la siguiente forma :

Teorema (Division Euclideana)

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

La siguiente proposicion nos ayudara a construir otra herramienta importante:

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:

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

Demostración. Analoga a la realizada en Subsección 5.1. □

De lo anterior se desprende el **Algoritmo de Euclides** el cual es un metodo eficiente para calcular el maximo comun divisor **(MCD)** de dos numeros enteros.

3. Algoritmo de Euclides

El algoritmo de euclides es un método para calcular el MCD de dos números enteros y su funcionamiento se basa en la proposición demostrada anteriormente.

Algoritmo de Euclides

Dados $a, b \in \mathbb{Z}^+$, con $a > b$ tal que **b no es factor de a** y $b \neq 0$
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 ademas que $r_m = mcd(a,b)$ se obtiene luego de una cantidad finita de pasos ya que

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

4. Lema de Bezout

Una de las consecuencias del algoritmo de Euclides es que el **mcd** entre 2 números enteros puede ser expresado como una combinación lineal de los 2 números originales.

Lema de Bezout

Sean $a, b \in \mathbb{Z} \setminus \{0\}$, y sea $d := \text{mcd}(a,b)$. Entonces $\exists (x,y) \in \mathbb{Z}^2 : ax + by = d$

Demostración. Ver apendice □

5. Generalizaciones a Polinomios

Los resultados presentados anteriormente corresponden a Teoremas y Proposiciones útiles para resolver problemas con números enteros. Sin embargo, este trabajo se enfoca en el estudio de los polinomios. Por ello, buscamos extender dichos resultados al ámbito polinomial y desarrollar algoritmos que faciliten la resolución de problemas relacionados. Estos algoritmos, incluidos en la sección de Algoritmos, se aplicarán en ejemplos ilustrativos de los siguientes resultados:

5.1. Division Euclideana (Polinomios)

Teorema (Division Euclideana Polinomios)

$$\forall (A, B) \in \mathbb{R}[X] \times \mathbb{R}[X]^* : \exists! Q, R \in \mathbb{R}[X] : A = BQ + R \quad , grad(R) < grad(B)$$

Definicion (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:

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

Definición (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

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

Proposicion

Sean $P_1, P_2 \in \mathbb{R}[X]$, con $P_2 \neq 0$. luego sean Q y R el cociente y el resto obtenidos al aplicar el **Algoritmo de la Division (Polinomial)** a P_1 y P_2 tal que $P_1 = P_2Q + R$. Entonces

$$mcd(P_1, P_2) = mcd(P_2, R) \ .$$

Demostracion. Sean $P_1, P_2 \in \mathbb{R}[X]$, con $P_2 \neq 0$, y sean $Q, R \in \mathbb{R}[X]$ tales que:

$$P_1 = P_2Q + R, \quad grad(R) < grad(P_2)$$

Luego sea $D := mcd(P_1, P_2)$ asi se tiene que $D|P_1$ y $D|P_2$ y por tanto D divide a cualquier combinacion lineal de ellos, en particular $D|(P_1 - P_2Q)$ es decir $D|R$ y por tanto $D|mcd(P_2, R)$.

Por otro lado sea $D_0 := mcd(P_2, R)$, sabemos que $D|mcd(P_2, R)$ asi $D|D_0$ y analogamente a lo anterior deducimos que $D_0|P_2Q + R$ por tanto $D_0|P_1$ y como $D_0|P_2$ entonces $D_0|mcd(P_1, P_2)$ asi hemos llegado a que $D_0|D$ y $D|D_0$ asi concluimos que $D = D_0$ es decir:

$$mcd(P_1, P_2) = mcd(P_2, R)$$

□

5.2. Algoritmo de Euclides (Polinomios)

Algoritmo de Euclides (Polinomios)

Dados $P_1, P_2 \in \mathbb{R}[X]$, con $grad(P_2) \leq grad(P_1)$ y $P_2 \neq 0$

$$\begin{gathered}(Q_1, R_1) \in \mathbb{R}[X] \times \mathbb{R}[X]^* : P_1 = P_2Q_1 + R_1, \quad grad(R_1) < grad(P_2) \\ (Q_2, R_2) \in \mathbb{R}[X] \times \mathbb{R}[X]^* : P_2 = Q_2R_1 + R_2, \quad grad(R_2) < grad(R_1) \\ \vdots \\ (Q_m, R_m) \in \mathbb{R}[X] \times \mathbb{R}[X]^* : R_{m-2} = R_{m-1}Q_m + R_m, \quad grad(R_m) < grad(R_{m-1}) \\ (Q_{m+1}, R_{m+1}) \in \mathbb{R}[X] \times \mathbb{R}[X]^* : R_{m-1} = R_mQ_{m+1} + R_{m+1}, \quad R_{m+1} = 0\end{gathered}$$

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

$$grad(R_m) < \ldots < grad(R_1) \text{ y } grad(R_m) = 0.$$

Ademas $R_{m+1} = 0$ ya que como $grad(R_m) = 0$ se tiene que $R_m = c, \quad c \in \mathbb{R}$. y por tanto en el siguiente paso basta tomar $Q_{m+1} = \dfrac{R_{m-1}}{c}$ para obtener $R_{m+1} = 0$.

Ejemplos

Ejemplo 5.2.1. Sean los polinomios

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

Aplicando el algoritmo de Euclides:

$$x^3 - 2x^2 - x + 2 = (x^2 - 4)(x - 2) + (3x - 6), \tag{1}$$

$$x^2 - 4 = (3x - 6)\left(\tfrac{1}{3}x + \tfrac{2}{3}\right) + 0. \tag{2}$$

Por tanto, tomando el último resto no nulo $R_1(x) = 3(x-2)$, asi $A = 3$ concluyendo que:

$$mcd\big(P_1, P_2\big) = \frac{1}{3}(3(x-2)) = (x-2).$$

Ejemplo 5.2.2 Sean los polinomios

$$\begin{aligned}P_1(x) &= x^6 - 22x^5 + 190x^4 - 820x^3 + 1849x^2 - 2038x + 840, \\ P_2(x) &= x^5 - 45x^4 + 805x^3 - 7155x^2 + 31594x - 55440\end{aligned}$$

Podemos preguntarnos ¿Cual sera $mcd(P_1, P_2)$?.

Respuesta: Usando el algoritmo **diveu.m** y como entradas a los coeficientes de cada polinomio en orden descendente de la siguiente forma:

$$\begin{aligned}&\textbf{Entrada 1: } [1, -22, 190, -820, 1849, -2038, 840] \\ &\textbf{Entrada 2: } [1, -45, 805, -7155, 31594, -55440]\end{aligned}$$

Obteniendo como salida $[1, -7]$, es decir $mcd(P_1, P_2) = x - 7$.

5.3. Identidad de Bezout (Polinomios)

Lema de Bezout (Polinomios)

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 $grad(R_{i+1}) < grad(R_i), \quad \forall i \in \{1, \dots, m\}$)
Buscaremos mostrar que:

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

Del **Algoritmo de Euclides** sabemos que:

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

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

$$\begin{aligned} R_1 &= P_1 - P_2Q_1 \\ R_2 &= P_2 - Q_2R_1 = P_2 - Q_2(P_1 - P_2Q_1) \\ &= P_2 - Q_2P_1 + P_2Q_1Q_2 = (-Q_2)P_1 + (Q_1Q_2 + 1)P_2 \end{aligned}$$

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

$$\begin{aligned} R_{m+1} &= R_{m-1} - R_mQ_{m+1} \\ &= A_{m-1}P_1 + B_{m-1}P_2 - Q_{m+1}(A_mP_1 + B_mP_2) \\ &= (A_{m-1} - Q_{m+1}A_m)P_1 + (B_{m-1} - Q_{m+1}B_m)P_2 \end{aligned}$$

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

□

La demostracion anterior nos entrega un algoritmo para encontrar $\boldsymbol{A(x)}$ y $\boldsymbol{B(x)}$.

Algoritmo de Bézout

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 $R_k = A_kP_1 + B_kP_2$ 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** y estos son **A** y **B**.
Observacion: *Notemos que este algoritmo es equivalente al propuesto en la demostracion anterior.*

Ejemplos

Ejemplo 5.3.1 Sean los polinomios

$$P_1(x) = x^3 - 1, \quad P_2(x) = x^2 + 1.$$

Aplicando el algoritmo de Euclides:

$$P_1(x) = x\,P_2(x) + \big(-x - 1\big), \tag{3}$$
$$P_2(x) = (-x)\big(-x - 1\big) + \big(-x + 1\big), \tag{4}$$
$$(-x - 1) = 1 \cdot (-x + 1) + (-2). \tag{5}$$

Como el último resto no nulo es la constante -2, concluimos que

$$mcd\big(P_1, P_2\big) = 1.$$

De (3) y (4) sabemos que:

$$R_1(x) = -x - 1, \quad R_2(x) = -x + 1.$$

Ademas:

$$\begin{aligned} R_1(x) &= P_1(x) - x\,P_2(x), \\ R_2(x) &= P_2(x) + x\,R_1(x) = (1 - x^2)P_2 + xP_1, \\ -2 &= R_1(x) - R_2(x). \end{aligned}$$

Dividiendo por -2 la ultima expresion obtenemos:

$$1 = mcd(P_1, P_2) = -\frac{1}{2}\big(R_1(x) - R_2(x)\big) = -\frac{1}{2}\left((1 - x)P_1 - (1 + x - x^2)P_2)\right)$$

Por tanto, los coeficientes de Bézout encontrados son:

$$\boxed{A(x) = \frac{x - 1}{2}}, \qquad \boxed{B(x) = \frac{1 + x - x^2}{2}},$$

pues

$$A(x)\,P_1(x) + B(x)\,P_2(x) = 1.$$

Ejemplo 5.3.2 Sean $P_1(x) = -5x^4 + 6x^3 - 7x^2 + 3x + 2$ y $P_2(x) = 3x^4 + 4x^3 - 5x^2 + 6x - 7$, asi con los algoritmos obtenidos podemos responder: ¿Cual es $mcd(P_1, P_2)$? y cuales son los polinomios $Q(x), R(x)$ tales que $P_1Q + P_2R = mcd(P_1, P_2)$?

Respuesta: Usando el algoritmo **bezoutpoly.m** con las entradas:

Entrada 1: $[-5, 6, -7, 4, 2]$
Entrada 2: $[3, 4, -5, 6, -7]$

Obtenidas usando un proceso analogo al del **ejemplo 5.2.2**, obtenemos como salida:

$$1, \quad \left[\frac{34458}{154655}, \frac{15742}{30931}, \frac{7070}{30931}, \frac{129271}{154655}\right], \quad \left[\frac{11486}{30931}, -\frac{14306}{154655}, \frac{19338}{30931}, \frac{14841}{154655}\right].$$

Es decir:

$$mcd(P_1, P_2) = 1$$
$$A(x) = \frac{34458}{154655}x^3 + \frac{15742}{30931}x^2 + \frac{7070}{30931}x + \frac{129271}{154655}$$

$$B(x) = \frac{11486}{30931}x^3 - \frac{14306}{154655}x^2 + \frac{19338}{30931}x + \frac{14841}{154655}$$

Asi hemos extendido los resultados anteriores de $\mathbb{Z}$ a $\mathbb{R}[X]$ que es justamente lo que buscabamos.

6. Raices de polinomios con coeficientes enteros

Cuando tratemos con polinomios de coeficientes enteros, existe un Teorema que nos ayudara a encontrar las **Raices Racionales** del polinomio (si esque existen). Este teorema es conocido como el Teorema de las Raices Racionales **(RRT)**.

Teorema de las Raices 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 $q \mid a_n$.

Demostración. Ver apendice □

Asi dado un polinomio con coeficientes enteros basta buscar entre las posibles combinaciones de los divisores de a_0 y a_n y probar con cada una para verificar si existen o no raices racionales.

Ejemplos

Ejemplo 6.1 Sea $q(x) = 2x^3 - 3x^2 + 1$ asi del **Teorema de las raices racionales** sabemos que si existe una solucion racional $\varphi := \dfrac{a}{b} \in \mathbb{Q}$ entonces $a|1$ y $b|2$ asi se tiene que $a = \pm 1$ y $b = \pm 1$ o $b = \pm 2$. Probando todas las combinaciones posibles concluimos que:

$$\varphi_1 = -\frac{1}{2} \text{ y } \varphi_2 = 1 \text{ son } \textbf{raices racionales} \text{ de } q(x).$$

Usando el algoritmo podemos responder preguntas mas complejas como:

Ejemplo 6.2 ¿Tendra $\vartheta(x) = 24x^6 - 7x^5 + 7x^4 + 2x^3 - 6x^2 + x + 8$ **raices racionales**? Si es asi ¿Cuales son?.

Respuesta: Para responder esta pregunta usaremos el algoritmo **rrt.m**, por tanto nuestra entrada seran los coeficientes del polinomio $\vartheta(x)$ ingresados de manera descendiente y en el siguiente formato:

$$\textbf{Entrada:}\quad [24, -7, 7, 2, -6, 1, 8]$$

obtienendo como salida que $\vartheta(x)$ **no** posee raices racionales.

Ejemplo 6.3 ¿Tendra $\varsigma(x) = x^5 - 11x^4 + 2x^3 + 226x^2 - 803x + 585$ **raices racionales**? Si es asi ¿Cuales son?

Respuesta: Analogamente al ejemplo anterior usaremos el programa **rrt.m** con la **entrada:** $[1, -11, 2, 226, -803, 585]$ obteniendo como salida que $\varsigma(x)$ posee raices racionales y que estas son:

$$\varphi_1 = 1, \quad \varphi_2 = -5, \quad \varphi_3 = 9$$

7. Aplicación a la descomposición en elementos simples de una función racional

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. Algunos problemas clásicos son el cálculo de **Integrales definidas/indefinidas** y expansiones por **Series de Taylor**, por ejemplo:

$$\int_a^b \frac{P(x)}{Q(x)}\, dx.$$

Resolver esta integral directamente puede llegar a ser complejo, por lo que buscamos simplificar la función racional, como sigue:

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

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

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

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

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

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

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

Esta descomposición permite simplificar cálculos de la **Integración** o el calculo de la **Serie de Taylor** de $f(x)$.

Ejemplos

Ejemplo 7.1 Supongamos que queremos calcular:

$$I = \int \frac{5x+1}{x^2+x-2}\,dx.$$

Sea $Q = x^2 + x - 2$ notamos que $Q(x) = Q_1(x)Q_2(x) = (x-1)(x+2)$ donde $mcd(Q_1, Q_2) = 1$ por tanto usando el **Algoritmo de Bezout** manualmente identificamos que sus **Coeficientes de Bezout** son:

$$A_0(x) = -\frac{1}{3} \quad , \quad A_1(x) = \frac{1}{3}$$

Por tanto se tiene que :

$$I = -\frac{1}{3}\int \frac{5x+1}{(x+2)}\,dx + \frac{1}{3}\int \frac{5x+1}{(x-1)}\,dx$$

Luego usamos la **Division de polinomios** obteniendo:

$$I = -\frac{1}{3}\left(\int 5\,dx - 9\int \frac{dx}{x+2}\right) + \frac{1}{3}\left(\int 5\,dx + 6\int \frac{dx}{x-1}\right)$$

Notamos asi que todas las integrales obtenidas son facilmente resolubles y todos los pasos anteriores fueron hechos con metodos explicados en este trabajo.

Ejemplo 7.2. Supongamos que queremos calcular la serie de Taylor alrededor de $x = 0$ de la función racional :

$$f(x) \;=\; \frac{x+2}{\left(1-x^2\right)(1-2x)} \;=\; \frac{N(x)}{Q_1(x)\,Q_2(x)},$$

donde

$$N(x) = x + 2, \quad Q_1(x) = 1 - x^2, \quad Q_2(x) = 1 - 2x$$

De forma directa, obtener la expansión en potencia de $f(x)$ resulta muy complejo, pues el denominador factoriza en dos polinomios irreducibles de grados 3 y 4. Para simplificarlo, aplicaremos el **Algoritmo de Bézout**, a los polinomios

$$Q_1(x) = 1 - x^2, \quad Q_2(x) = 1 - 2x.$$

Usaremos el algoritmo `bezoutpoly.m` en el cual ingresamos:

$$\text{Entrada 1: } [-1,\, 0,\, 1], \qquad \text{Entrada 2: } [-2,\, 1].$$

Donde obtenemos como resultado:

$$mcd\big(Q_1, Q_2\big) = 1, \quad A_0(x) = \frac{4}{3}, \quad A_1(x) = -\frac{1}{3}\,(2x+1)\,,$$

Luego reescribimos $f(x)$ utilizando lo obtenido:

$$f(x) = \; N(x)\,\frac{1}{Q_1 Q_2} = \; N(x)\big(A_0 Q_1 + A_1 Q_2\big)\,\frac{1}{Q_1 Q_2} = \frac{N(x)A_0(x)}{Q_2(x)} \; + \; \frac{N(x)A_1(x)}{Q_1(x)},$$

donde

$$N(x)\,A_0(x) = \frac{4}{3}(x+2), \quad N(x)\,A_1(x) = -\frac{1}{3}\,(2x+1)\,(x+2).$$

Recordando la serie geometrica:

$$\frac{1}{1-x} = \sum_{n=0}^{\infty} x^n \quad , |x| < 1$$

Deducimos que:

$$\frac{1}{Q_1(x)} = \frac{1}{1-x^2} = \sum_{n=0}^{\infty} x^{2n}, \quad |x| < 1, \quad \frac{1}{Q_2(x)} = \frac{1}{(1-2x)} = \sum_{n=0}^{\infty} (2x)^n, \quad |x| < \frac{1}{2}$$

Multiplicamos a cada termino por $N(x)\,A_1(x)$ y $N(x)\,A_0(x)$ respectivamente y luego combinamos ambas series, resultando la expansión de $f(x)$:

$$f(x) = \sum_{n=0}^{\infty} N(x)A_1(x)x^{2n} + \sum_{n=0}^{\infty} N(x)A_0(x)2^n x^n, \quad |x| < \frac{1}{2}.$$

$$= \underbrace{\sum_{n=0}^{\infty} -\tfrac{2}{3}\,x^{2n+2} - \tfrac{5}{3}\,x^{2n+1} - \tfrac{2}{3}\,x^{2n}}_{S_1(x)} + \underbrace{\sum_{n=0}^{\infty} \tfrac{4}{3}\,2^n\,x^{n+1} + \tfrac{4}{3}\,2^{n+1}\,x^n}_{S_2(x)}, \quad |x| < \frac{1}{2}$$

Luego para llevar esto a su forma de Taylor usual, notamos lo siguiente:

Sea a_n el coeficiente numerico de la serie S_1, se cumple que:

$$a_n = \begin{cases} -\frac{2}{3} & , n = 0 \\ -\frac{5}{3} & , n \text{ impar} \\ -\frac{4}{3} & , n \geq 2 \text{ par} \end{cases} = \begin{cases} -\frac{2}{3} & , n = 0 \\ -\frac{3}{2} + \frac{(-1)^n}{6} & , n \geq 1 \end{cases}$$

Analogamente el coeficiente de numerico b_n en la serie S_2 es:

$$b_n = \begin{cases} \frac{8}{3} & , n = 0 \\ \frac{10}{3}2^n & , n \geq 1 \end{cases}$$

Deducimos que el coeficiente numerico c_n de la serie $S_1 + S_2$ es:

$$c_n = a_n + b_n = \frac{20 \cdot 2^n - 9 + (-1)^n}{6}, \quad n \geq 0.$$

Por tanto la serie de Taylor de la funcion es:

$$\boxed{f(x) = \sum_{n=0}^{\infty} c_n x^n = \sum_{n=0}^{\infty} \left(\frac{20 \cdot 2^n - 9 + (-1)^n}{6}\right) x^n, \quad |x| < \frac{1}{2}}$$

8. Aplicacion a Problemas de Ingeneria

En general, lo expuesto en este trabajo es útil para cualquier disciplina que requiera el manejo de polinomios o números enteros. Sus aplicaciones se orientan a la simplificación y resolución de problemas relacionados con estos conceptos, en particular en los siguientes casos:

1. Control automatico: colocacion de polos

Dada la planta $G(s) = B(s)/A(s)$ y un polinomio objetivo $C(s)$ que fija los polos deseados, hallar un regulador $R(s) = Y(s)/X(s)$ tal que:

$$A(s)X(s) + B(s)Y(s) = C(s).$$

Para esto podemos usar resultados obtenidos anteriormente:

1. **Bezout (polinomios)**. Obtiene U, V con $U(s)A(s) + V(s)B(s) = 1$.
2. **Identidad de Bezout**. Multiplicando por $C(s)$ se define

   $$X(s) = U(s)C(s), \qquad Y(s) = V(s)C(s),$$

   los cuales satisfacen la ecuacion y colocan los polos en las raíces de $C(s)$

2. Ingeniería Eléctrica y Mecánica

La excitación de un circuito RLC serie o de un sistema masa–resorte–amortiguador con un escalón produce la función de transferencia

$$X(s) = \frac{N(s)}{D(s)}.$$

1. **Factorización de** $D(s)$. Con coeficientes enteros o racionales, el **Teorema de las raices racionales** identifica polos reales antes de recurrir a métodos numéricos de mayor precisión.
2. **Descomposición en Fracciones Simples**. Se escribe $X(s) = \sum_k A_k/(s - p_k)$, empleando la combinación de Bézout si hay raíces múltiples.

3. Ciberseguridad

En RSA (algoritmo de encriptacion) se requiere hallar $d \equiv e^{-1} \pmod{\varphi(n)}$; en curvas elípticas, la operación P/Q implica el inverso de un denominador módulo p.

- **Algoritmo de Euclides extendido**. Opera en $\mathbb{Z}$ (RSA), obteniendo los coeficientes de Bézout los cuales permiten determinar el inverso modular deseado.

9. Conclusion

Tal como vimos en la sección 8, las herramientas desarrolladas en este trabajo, además de ser valiosas por sí mismas para la Matemática, también se aplican a distintos problemas de Ingeniería. Por ello, los resultados y algoritmos obtenidos son fundamentales para la formación y el desempeño de un Ingeniero Matemático.

Referencias

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

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

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

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

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

10. Apendice

10.1. Algoritmos

i) Implementacion **Division Euclideana de Polinomios (diveu.m)**:

```
% Calcula el m ximo com n divisor de los polinomios P1 y P2.
P1 = input('Ingrese coeficientes del primer polinomio [a_n ... a_0]: ');
P2 = input('Ingrese coeficientes del segundo polinomio [b_m ... b_0]: ');
syms x;
P1=poly2sym(P1,x);
P2=poly2sym(P2,x);

% Algoritmo de Euclides para polinomios:
while P2 ~= 0
    [Q,R] = quorem(P1, P2, x);
    R = expand(R);
    P1 = P2;
    P2 = R;
end

%Pasar a MCD monico
D = P1;
coeffsD = coeffs(D, x,'All');
scale = 1/coeffsD(1);
scaled=coeffsD*scale;
disp('MCD:');
disp(scaled);
```

ii) Implementacion **Algoritmo de Bezout (bezoutpoly.m)**

```
P1 = input('Ingrese coeficientes del primer polinomio [a_n ... a_0]: ');
P2 = input('Ingrese coeficientes del segundo polinomio [b_m ... b_0]: ');
syms x;
P1=poly2sym(P1,x);
P2=poly2sym(P2,x);


% Inicializar variables
r0 = P1;
r1 = P2;
s0 = 1; s1 = 0;
t0 = 0; t1 = 1;

% Iterar hasta que r1 sea cero:
while r1 ~= 0
    [q, r2] = quorem(r0, r1, x);  % Divisi n polin mica: r0 = q*r1 + r2
    r2 = expand(r2);

    % Actualizar residuos
    r0 = r1;
    r1 = r2;
    % Actualizar coeficientes de B zout
    s2 = s0 - q*s1;
    t2 = t0 - q*t1;
    s0 = s1;
    s1 = s2;
    t0 = t1;
    t1 = t2;
end

%Resultados
G = r0;      % MCD
A = s0;      % Coeficiente de B zout para P1
B = t0;      % Coeficiente de B zout para P2

% Pasar a MCD m nico:
coeffsG = coeffs(G, x);
lc = coeffsG(1);
G = G / lc;
A = A / lc;
B = B / lc;
%Mostrar resultados
disp(coeffs(G,x,'All'));
disp(coeffs(A,x,'All'));
disp(coeffs(B,x,'All'));
```

iii) Implementacion del **Teorema de las Raices Racionales (rrt.m)**:

```
p1 = input('Ingrese los coeficientes: ');
ooo=roots(p1);
% Divisores
l1 = double(divisors(sym(p1(end))));
l2 = double(divisors(sym(p1(1))));

% Prueba todas las combinaciones
sol = [];
for i = 1:length(l1)
    for j = 1:length(l2)
        p = l1(i);
        q = l2(j);
        if (polyval(p1,p/q)) == 0
            sol = [sol; p,   q];
        elseif polyval(p1,-p/q) == 0
            sol = [sol; -p,  q];
        end
    end
end


% Resultados
if ~isempty(sol)
    sol = unique(sol, 'rows');
    fprintf('Las raices racionales son:\n');
    for k = 1:size(sol,1)
        fprintf('%d/%d\n', sol(k,1), sol(k,2));
    end
else
    fprintf('El polinomio no posee soluciones racionales.\n');

end
```

10.2. Demostraciones

10.2.1. Bezout en $\mathbb{Z}$

Demostración. Definimos el conjunto de las combinaciones lineales enteras de a y b:

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

Este conjunto es no vacío pues $z = |a| \in S$ (tomando $x = (a)$, $y = 0$). Por el **Principio del Buen Orden**, S posee un primer elemento, que denotaremos por d. Como $d \in S$, existen $(x_0, y_0) \in \mathbb{Z}^2$ tales que:

$$d = ax_0 + by_0.$$

falta demostrar que $d = \text{mcd}(a, b)$:

- d **divide a** a**:** Por el Algoritmo de la División de Euclides, existen únicos $(q, r) \in \mathbb{Z}^2$ con $0 \leq r < d$ tales que:

  $$a = qd + r$$

  Observemos que:

  $$r = a - qd = a(1 - qx_0) + b(-qy_0)$$

  Como $1 - qx_0, -qy_0 \in \mathbb{Z}$, se tiene que $r \in S \cup \{0\}$. Pero $r < d$ y d es el mínimo de S, luego necesariamente $r = 0$. Por tanto, $d \mid a$.

- d **divide a** b**:** Análogo al caso anterior.

- d **es el máximo:** Sea $\tilde{d}$ otro divisor común de a y b. Entonces existen $\alpha, \beta \in \mathbb{Z}$ tales que:

  $$a = \alpha\tilde{d}, \quad b = \beta\tilde{d}$$

  Luego:

  $$d = ax_0 + by_0 = \tilde{d}(\alpha x_0 + \beta y_0)$$

  Como $\alpha x_0 + \beta y_0 \in \mathbb{Z}$, se concluye que $\tilde{d} \mid d$.

Por lo tanto, $d = mcd(a, b)$.

□

10.2.2. Teorema de las racies racionales

Demostración. Supongamos que $x = \frac{p}{q}$ es raíz de $p(x)$. Luego multiplicando por q^n :

$$\begin{aligned} p(x) = 0 &\Leftrightarrow a_n\left(\tfrac{p}{q}\right)^n + a_{n-1}\left(\tfrac{p}{q}\right)^{n-1} + \cdots + a_0 = 0 \\ &\Leftrightarrow a_n p^n + a_{n-1}p^{n-1}q + \cdots + a_1 pq^{n-1} + a_0 q^n = 0 \\ &\Leftrightarrow p(a_n p^{n-1} + a_{n-1}p^{n-2}q + \cdots + a_1 q^{n-1}) = -a_0 q^n. \end{aligned}$$

Dado que $mcd(p, q) = 1$, se concluye que $p \mid a_0$. Análogamente, reagrupando los términos:

$$a_n p^n + \cdots + a_0 q^n = 0 \Leftrightarrow q(a_{n-1}p^{n-1} + \cdots + a_0 q^{n-1}) = -a_n p^n.$$

Como $mcd(p, q) = 1$, se deduce que $q \mid a_n$.

□