Un breve recorrido por los polinomios

Por Carlos Jacob Rubio Barrios

Nivel Intermedio

Definiciones básicas

Un *polinomio* en x es una expresión de la forma

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,$$

donde n es un entero mayor o igual que cero y $a_0, a_1, \ldots, a_n$ son números que pueden ser enteros, racionales, reales o complejos y son llamados los *coeficientes* de $p(x)$. Si $a_n \neq 0$, se dice que $p(x)$ es de *grado* n y se denota $\operatorname{gr} p(x) = n$; en este caso, a_n es llamado *coeficiente principal*. En particular, los polinomios de grado 1, 2 y 3 son llamados *lineal*, *cuadrático* y *cúbico*, respectivamente. Un polinomio constante distinto de cero tiene grado 0, mientras que el polinomio cero se conviene que tiene grado $-\infty$ por razones que pronto quedarán claras.
Por ejemplo, el polinomio $p(x) = x^3(x+1) + (1-x^2)^2 = 2x^4 + x^3 - 2x^2 + 1$ es un polinomio con coeficientes enteros de grado 4.

Los polinomios se pueden sumar, restar o multiplicar y, el resultado, seguirá siendo un polinomio. Si $p(x) = a_0 + a_1 x + \cdots + a_n x^n$ y $q(x) = b_0 + b_1 x + \cdots + b_m x^m$, entonces

$$p(x) \pm q(x) = (a_0 \pm b_0) + (a_1 \pm b_1)x + (a_2 \pm b_2)x^2 + \cdots,$$

$$p(x)q(x) = a_0 b_0 + (a_0 b_1 + a_1 b_0)x + (a_0 b_2 + a_1 b_1 + a_2 b_0)x^2 + \cdots + a_n b_m x^{m+n}.$$

El coeficiente de x^ℓ en el producto $p(x)q(x)$ es

$$\sum_{i=0}^{\ell} a_i b_{\ell - i} = a_0 b_\ell + a_1 b_{\ell-1} + \cdots + a_\ell b_0.$$

Un resultado muy obvio sobre la multiplicación de polinomios es que para cualesquiera polinomios $p(x)$ y $q(x)$,

$$\operatorname{gr} p(x)q(x) = \operatorname{gr} p(x) + \operatorname{gr} q(x).$$

La demostración es sencilla. Si el grado de $p(x)$ es n y el grado de $q(x)$ es m, entonces el producto $p(x)q(x)$ contendrá un término de la forma cx^{m+n} y no contiene términos de grado mayor que $m+n$.
La convención de que el grado del polinomio cero es $-\infty$ surge de esta propiedad, de otra forma tal propiedad no sería siempre cierta. ¿Puedes demostrar que si $\operatorname{gr} p(x) \geq \operatorname{gr} q(x)$, entonces $\operatorname{gr} p(x) + q(x) \leq \operatorname{gr} p(x)$?

Algoritmo de la división y Teorema del residuo

A diferencia de la suma, la resta y el producto, un cociente de dos polinomios no necesariamente es un polinomio. En lugar de esto, como en los números enteros, dos polinomios pueden dividirse dejando un residuo.

Teorema. [Algoritmo de la división] Dados los polinomios $p(x)$ y $q(x)$, con $q(x) \neq 0$, existen únicos polinomios $s(x)$ (polinomio cociente) y $r(x)$ (polinomio residuo), tales que

$$p(x) = q(x)s(x) + r(x) \text{ donde } \operatorname{gr} r(x) < \operatorname{gr} q(x).$$

Demostración. Demostraremos primero la existencia de los polinomios $s(x)$ y $r(x)$. Si $p(x) = 0$, sean $s(x) = r(x) = 0$. Como $q(x) \neq 0$, $\operatorname{gr} q(x)$ es un entero no negativo y $\operatorname{gr} r(x) = -\infty < \operatorname{gr} q(x)$. Supongamos entonces que $p(x) \neq 0$. Sea $m = \operatorname{gr} q(x)$. Si $m > \operatorname{gr} p(x)$, tomamos $s(x) = 0$ y $r(x) = p(x)$. Entonces $p(x) = q(x)s(x) + r(x)$ con $\operatorname{gr} r(x) = \operatorname{gr} p(x) < \operatorname{gr} q(x)$. Supongamos ahora que $\operatorname{gr} p(x) \geq m$. En este caso, la prueba la haremos por inducción en el grado de $p(x)$. Si $\operatorname{gr} p(x) = 0$, entonces $m = 0$ (pues $m \geq 0$ al ser $q(x) \neq 0$). Luego, $p(x), q(x)$ son constantes distintos de cero, de modo que si $s(x) = \frac{p(x)}{q(x)}$ y $r(x) = 0$, entonces $p(x) = q(x)s(x) + r(x)$ con $\operatorname{gr} r(x) < \operatorname{gr} q(x)$. Supongamos que el resultado es cierto para cualquier polinomio de grado menor que n (con $n > 0$) y sea $p(x)$ un polinomio de grado n. Consideremos el polinomio

$$p_1(x) = p(x) - \frac{a_n}{b_m}x^{n-m}q(x),$$

donde a_n y b_m son los coeficientes líderes de $p(x)$ y $q(x)$, respectivamente. Observemos que el grado de $p_1(x)$ es estrictamente menor que el grado de $p(x)$, pues el término principal de $p(x)$ se cancela con el término principal de $\frac{a_n}{b_m}x^{n-m}q(x)$ en la diferencia $p(x) - \frac{a_n}{b_m}x^{n-m}q(x)$. Aplicando la hipótesis de inducción al polinomio $p_1(x)$ se sigue que existen polinomios $s_1(x)$ y $r(x)$ tales que $p_1(x) = s_1(x)q(x) + r(x)$ con $\operatorname{gr} r(x) < \operatorname{gr} q(x)$. Entonces

$$p(x) = \frac{a_n}{b_m}x^{n-m}q(x) + p_1(x) = \frac{a_n}{b_m}x^{n-m}q(x) + s_1(x)q(x) + r(x) = s(x)q(x) + r(x),$$

donde $s(x) = \frac{a_n}{b_m}x^{n-m} + s_1(x)$. Esto completa el paso inductivo.

Para la unicidad, supongamos que $s_1(x)$ y $r_1(x)$ son polinomios que satisfacen las mismas condiciones que $s(x)$ y $r(x)$. Entonces $p(x) = q(x)s(x)+r(x) = q(x)s_1(x)+r_1(x)$ con $\operatorname{gr} r(x) < \operatorname{gr} q(x)$ y $\operatorname{gr} r_1(x) < \operatorname{gr} q(x)$. Tenemos entonces que $q(x)(s(x) - s_1(x)) = r_1(x) - r(x)$. Si $s(x) - s_1(x) \neq 0$, entonces $\operatorname{gr}(s(x) - s_1(x)) \geq 0$. Luego,

$$\begin{aligned}\operatorname{gr} q(x) &\leq \operatorname{gr} q(x) + \operatorname{gr}(s(x) - s_1(x)) = \operatorname{gr}(q(x)(s(x) - s_1(x)) = \operatorname{gr}(r_1(x) - r(x)) \\ &\leq \max\{\operatorname{gr} r_1(x), \operatorname{gr} r(x)\} < \operatorname{gr} q(x),\end{aligned}$$

lo cual es una contradicción. Entonces, $s(x)-s_1(x) = 0$ y, por lo tanto, $r_1(x)-r(x) = 0$. Así, $s(x) = s_1(x)$ y $r(x) = r_1(x)$. □

Por ejemplo, el cociente de la división de $p(x) = x^3 + x^2 - 1$ por $q(x) = x^2 - x - 3$ es $x + 2$ y el residuo es $5x + 5$, esto es,

$$\frac{x^3 + x^2 - 1}{x^2 - x - 3} = x + 2 + \frac{5x + 5}{x^2 - x - 3}.$$

Decimos que el polinomio $p(x)$ es *divisible* por el polinomio $q(x)$ si el residuo $r(x)$ cuando $p(x)$ es dividido por $q(x)$ es igual a 0, esto es, si existe un polinomio $s(x)$ tal que $p(x) = q(x)s(x)$. Como en los números enteros, escribimos $q(x) \mid p(x)$ para indicar que $p(x)$ es divisible por $q(x)$.

Teorema del residuo. El residuo de la división del polinomio $p(x)$ por el binomio $x-a$ es $p(a)$. En particular, el polinomio $p(x)$ es divisible por el binomio $x - a$ si y solo si $p(a) = 0$.

Demostración. Por el teorema anterior, podemos escribir $p(x) = (x - a)s(x) + r(x)$ donde $\operatorname{gr} r(x) < \operatorname{gr}(x-a) = 1$. Luego, necesariamente $r(x)$ es una constante, digamos $r(x) = r$. Sustituyendo $x = a$ en la primera igualdad, obtenemos que $p(a) = r(a) = r$, esto es, el residuo de la división de $p(x)$ por $x - a$ es $p(a)$.
Si $p(x)$ es divisible por $x - a$, entonces existe un polinomio $s(x)$ tal que $p(x) = (x-a)s(x)$ y, por la unicidad del cociente y del residuo en el teorema anterior, se sigue que el residuo de la división de $p(x)$ entre $x-a$ es 0. Luego, $p(a) = 0$. Recíprocamente, si $p(a) = 0$, entonces el residuo de la división de $p(x)$ entre $x - a$ es 0. □

Ejemplo 1. Sea $p(x)$ un polinomio con coeficientes reales. Cuando $p(x)$ es dividido por $x-1$, el residuo es 3. Cuando $p(x)$ es dividido por $x-2$, el residuo es 5. Determinar el residuo cuando $p(x)$ es dividido por el polinomio $x^2 - 3x + 2$.

Solución. Escribamos $p(x) = (x^2 - 3x + 2)s(x) + r(x)$, donde $r(x)$ es el residuo que buscamos. Como $\operatorname{gr} r(x) < \operatorname{gr}(x^2-3x+2) = 2$, podemos escribir $r(x) = ax+b$ para algunos números reales a y b. Por otra parte, por el Teorema del residuo, tenemos que $p(1) = 3$ y $p(2) = 5$. Como $x^2 - 3x + 2 = 0$ para $x = 2$ y $x = 1$, sustituyendo estos valores en la primera igualdad, obtenemos que $p(1) = 0 \cdot s(1) + r(1) = r(1) = a + b$ y $p(2) = 0 \cdot s(2) + r(2) = r(2) = 2a + b$. Como $p(1) = 3$ y $p(2) = 5$, obtenemos que $a + b = 3$ y $2a + b = 5$. Resolviendo este sistema de ecuaciones, encontramos que $a = 2$ y $b = 1$. Por lo tanto, el residuo buscado es $2x + 1$. □

Raíces de polinomios

Un número a es un *cero* o *raíz* de un polinomio $p(x)$ si $p(a) = 0$, de manera equivalente, si $(x - a) \mid p(x)$. Determinar los ceros de un polinomio $p(x)$ significa resolver la ecuación $p(x) = 0$, lo cual no siempre es posible. Por ejemplo, es conocido que determinar los ceros de un polinomio $p(x)$ es imposible en general cuando el grado de $p(x)$ es mayor o igual que 5. Sin embargo, los ceros de un polinomio siempre pueden ser calculados con una precisión arbitraria. Más precisamente, si $p(a) < 0 < p(b)$, entonces $p(x)$ tiene un cero entre a y b.

Polinomios cuadráticos

No todos los polinomios cuadráticos se pueden factorizar fácilmente. Por ejemplo, si tratamos de determinar los ceros del polinomio $x^2 + x - 1$ mediante una factorización, pronto nos daremos cuenta que no podremos. Necesitamos una forma general para determinar los ceros de polinomios cuadráticos, que evite las limitaciones de la factorización.
Consideremos el polinomio $p(x) = ax^2 + bx + c$, con $a \neq 0$. Si α y β son las raíces (reales o complejas) de $p(x)$, tenemos que $a(x - \alpha)(x - \beta) = ax^2 + bx + c$, esto es, $ax^2 - a(\alpha + \beta)x + a\alpha\beta = ax^2 + bx + c$. De aquí, $\alpha + \beta = \frac{-b}{a}$ y $\alpha\beta = \frac{c}{a}$. Estas relaciones son conocidas como fórmulas de Vieta.
Completando el cuadrado, podemos escribir al polinomio $p(x)$ en la forma

$$p(x) = a\left(x + \frac{b}{2a}\right)^2 + c - \frac{b^2}{4a}.$$

Luego, $p(x) = 0$ si y solo si $a\left(x + \frac{b}{2a}\right)^2 + c - \frac{b^2}{4a} = 0$, de donde obtenemos la fórmula general

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

La expresión $D = b^2 - 4ac$ es el *discriminante* de $p(x)$ porque separa las raíces: Si $D > 0$, $p(x)$ tiene dos raíces reales distintas; si $D = 0$, $p(x)$ tiene una raíz real doble; si $D < 0$, $p(x)$ no tiene raíces reales.

Ejemplo 2. Hallar una condición necesaria y suficiente en términos de los coeficientes del polinomio $p(x) = ax^2 + bx + c$, con $a \neq 0$, para que una de sus raíces sea igual al cuadrado de la otra.

Solución. Sean r y r^2 las raíces de $p(x)$. Aplicando las fórmulas de Vieta, tenemos que $r^2 + r = -\frac{b}{a}$ y $r^3 = \frac{c}{a}$. Por otro lado, tenemos que

$$(r^2 + r)^3 = r^3(r + 1)^3 = r^3[r^3 + 3(r^2 + r) + 1],$$

de donde tenemos la condición necesaria $\left(-\frac{b}{a}\right)^3 = \frac{c}{a}\left(\frac{c}{a} - 3\frac{b}{a} + 1\right)$, la cual es equivalente a la relación $b^3 + ca(c + a) = 3abc$.
Esta condición también es suficiente. En efecto, sean r y s las raíces de $p(x)$ y supongamos que $(-\frac{b}{a})^3 = \frac{c}{a}\left(\frac{c}{a} - 3\frac{b}{a} + 1\right)$. Nuevamente, por las fórmulas de Vieta, tenemos

que $r+s=-\frac{b}{a}$ y $rs=\frac{c}{a}$. Sustituyendo en la relación de la hipótesis, obtenemos que $(r+s)^3=rs(rs+3(r+s)+1)$, esto es, $(r^2-s)(r-s^2)=0$, lo que prueba que una de las raíces de $p(x)$ es el cuadrado de la otra. □

Ejemplo 3. Sean a y b enteros. Determinar todas las soluciones de la ecuación

$$(ax-b)^2+(bx-a)^2=x,$$

si se sabe que tiene una solución entera.

Solución. Si $a=b=0$, la ecuación es de primer grado, con única solución $x=0$. Supongamos que $a\neq 0$ o $b\neq 0$. La ecuación se puede reescribir en la forma $(a^2+b^2)x^2-(4ab+1)x+a^2+b^2=0$. Supongamos que c y d son las soluciones de esta ecuación, con c número entero. Como $c=(ac-b)^2+(bc-a)^2$, tenemos que c, además de ser entero, es positivo. Además, como las raíces son reales (¿por qué?), el discriminante de la ecuación es mayor o igual que cero, esto es,

$$(4ab+1)^2-4(a^2+b^2)^2\geq 0.$$

De manera equivalente, tenemos que $(1-2(a-b)^2)(1+2(a-b)^2)\geq 0$ y esto exige que $1-2(a-b)^2\geq 0$. Puesto que $(a-b)^2$ es un entero no negativo (pues a y b son enteros), resulta necesariamente que $(a-b)^2=0$, esto es, $a=b$. Por lo tanto, la ecuación se convierte en $2a^2-(4a^2+1)x+2a^2=0$. De acuerdo con las fórmulas de Vieta, tenemos que $c+d=2+\frac{1}{2a^2}$ y $cd=1$. Como c es un entero, $c=0$ no puede ser raíz (pues $cd=1$), ni tampoco $c=1$ puede serlo (pues $c=1$ y $cd=1$ implican que $d=1$ y $2=c+d=2+\frac{1}{2a^2}$, lo cual es un absurdo). Por lo tanto, $c\geq 2$. Como $d=\frac{1}{c}>0$, se sigue que $c<c+d=2+\frac{1}{2a^2}<3$ y, en consecuencia, $2\leq c<3$. Como c es entero, la única posibilidad es $c=2$ y, de aquí, $d=\frac{1}{2}$. Sustituyendo los valores resulta que $a^2=1$, de donde $a\in\{-1,1\}$. En conclusión, la única posibilidad es $a=b=\pm 1$, en cuyo caso las soluciones son 2 y $\frac{1}{2}$. □

El siguiente resultado es simple pero muy útil. La demostración es fácil y se deja de ejercicio al lector.

Teorema. Si un polinomio $p(x)$ es divisible por un polinomio $q(x)$, entonces cada cero de $q(x)$ también es un cero de $p(x)$.

Ejemplo 4. Determinar todos los enteros positivos n tales que el polinomio x^n+x-1 sea divisible por el polinomio x^2-x+1.

Solución. Usando la fórmula general, encontramos que los ceros de x^2-x+1 son $a=\frac{1+\sqrt{3}i}{2}$ y $b=\frac{1-\sqrt{3}i}{2}$. Si x^n+x-1 es divisible por x^2-x+1, entonces los ceros de x^2-x+1 son ceros de x^n+x-1, esto es, $a^n+a-1=0$ y $b^n+b-1=0$. De manera equivalente, tenemos que $a^n=1-a$ y $b^n=1-b$. Por otra parte, como a y b son raíces de x^2-x+1, tenemos que $1=a-a^2=a(1-a)$ y $1=b-b^2=b(1-b)$, esto es, $1-a=\frac{1}{a}$ y $1-b=\frac{1}{b}$. Luego, $a^n=\frac{1}{a}$ y $b^n=\frac{1}{b}$, de donde $a^{n+1}=1$ y $b^{n+1}=1$. Como $a^k=b^k=1$ si y solo si $6\mid k$ (ejercicio), se sigue que $6\mid(n+1)$, esto es, $n=6m-1$ con m entero positivo. □

El Teorema Fundamental del Álgebra

El Teorema Fundamental del Álgebra afirma que todo polinomio no constante tiene al menos un cero complejo. Desafortunadamente, la prueba es un poco complicada para nuestro texto. Sin embargo, usaremos este teorema para demostrar que todo polinomio de grado $n > 0$ tiene exactamente n raíces. Esto significa que podemos escribir cualquier polinomio $p(x)$ en la forma

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = a_n(x - r_1)(x - r_2)\cdots(x - r_n),$$

donde los números $r_1, \ldots, r_n$ son reales o complejos. Debería ser claro por qué $f(r_i) = 0$ para $i = 1, \ldots, n$.

Para demostrar que todo polinomio no constante se puede escribir de tal forma, usaremos el Teorema Fundamental del Álgebra. La prueba la haremos por inducción en el grado del polinomio. Si el polinomio es de grado 1, el resultado es inmediato. Supongamos que el resultado es cierto para polinomios de grado $n-1$ y consideremos un polinomio $p(x)$ de grado n. De acuerdo con el Teorema Fundamental del Álgebra, $p(x)$ tiene una raíz r_1, esto es, $(x - r_1) \mid p(x)$. Luego, existe un polinomio $q_1(x)$ tal que $p(x) = (x-r_1)q_1(x)$. Como $\text{gr}\, p(x) = n = \text{gr}\,(x-r_1)q_1(x) = \text{gr}\,(x-r_1) + \text{gr}\, q_1(x)$, tenemos que $\text{gr}\, q_1(x) = n-1$. Luego, por la hipótesis de inducción, el polinomio $q_1(x)$ tiene exactamente $n-1$ raíces, esto es, $q_1(x) = c(x-r_2)(x-r_3)\cdots(x-r_n)$. Por lo tanto, $p(x) = c(x-r_1)(x-r_2)\cdots(x-r_n)$.
El resultado que acabamos de demostrar, solo muestra la existencia de las raíces; encontrarlas es otro problema.

Ejemplo 5. Sea $p(x)$ un polinomio cuadrático. Demostrar que existen polinomios cuadráticos $g(x)$ y $h(x)$ tales que $p(x)p(x+1) = g(h(x))$.

Solución. Podríamos comenzar escribiendo $p(x) = ax^2 + bx + c$ y trabajar con los coeficientes de $p(x)p(x+1)$. Es factible, pero muy enmarañado. Mejor trabajemos con las raíces. Escribamos $p(x) = a(x-r)(x-s)$. Entonces,

$$\begin{aligned} p(x)p(x+1) &= a^2 \cdot (x-r)(x-s+1)\cdot(x-s)(x-r+1) \\ &= a^2[(x^2 - (r+s-1)x + rs) - r][(x^2 - (r+s-1)x + rs) - s]. \end{aligned}$$

Por lo tanto, basta poner $g(x) = a^2(x-r)(x-s)$ y $h(x) = x^2 - (r+s-1)x + rs$.□

Polinomios con coeficientes enteros

Consideremos un polinomio $p(x) = a_n x^n + \cdots + a_1 x + a_0$ con coeficientes enteros. La diferencia $p(x) - p(y)$ se puede escribir en la forma

$$a_n(x^n - y^n) + \cdots + a_2(x^2 - y^2) + a_1(x - y),$$

en donde cada sumando $a_i(x^i - y^i)$ es divisible por el polinomio $x - y$. Esto nos lleva a la siguiente importante propiedad aritmética de los polinomios con coeficientes enteros.

Teorema de las raíces enteras. Si $p(x)$ es un polinomio con coeficientes enteros, entonces $p(a) - p(b)$ es divisible por $a - b$ para cualesquiera enteros distintos a y b. En particular, todas las raíces enteras de $p(x)$ dividen a $p(0)$.

Existe un resultado análogo acerca de raíces racionales de polinomios con coeficientes enteros.

Teorema de las raíces racionales. Sea $p(x) = a_n x^n + \cdots + a_1 x + a_0$ un polinomio con coeficientes enteros. Si un número racional $\frac{r}{s}$ (con r, s enteros, $s \neq 0$ y r, s primos relativos) es una raíz de $p(x)$, entonces $r \mid a_0$ y $s \mid a_n$.

Demostración. Tenemos que

$$s^n p\left(\frac{r}{s}\right) = a_n r^n + a_{n-1} r^{n-1} s + \cdots + a_0 s^n.$$

Todos los sumandos, excepto posiblemente el primero, son múltiplos de s y todos, excepto posiblemente el último, son múltiplos de r. Luego, $s \mid a_n r^n$ y $r \mid a_0 s^n$. Como r y s son primos relativos, se sigue que $s \mid a_n$ y $r \mid a_0$. □

Ejemplo 6. Sea $p(x)$ un polinomio con coeficientes enteros que toma los valores ± 1 en tres diferentes enteros. Demostrar que $p(x)$ no tiene raíces enteras.

Solución. Sean a, b, c enteros distintos tales que $p(a), p(b), p(c) \in \{-1, 1\}$. Supongamos, por contradicción, que existe un entero d tal que $p(d) = 0$. Por el Teorema de las raíces enteras, tenemos que $a - d$ divide a $p(a) - p(d) = p(a)$, $b - d$ divide a $p(b) - p(d) = p(b)$ y $c - d$ divide a $p(c) - p(d) = p(c)$. Esto implica que $a - d$, $b - d$ y $c - d$ dividen todos a 1. Luego, $a - d, b - d, c - d \in \{1, -1\}$. Esto implica que al menos dos de las diferencias $a - d$, $b - d$, $c - d$ son iguales a 1 o a -1 y, esto a su vez implica que al menos dos de los números a, b, c son iguales, lo que es una contradicción. □

Ejemplo 7. Sean $a_1, a_2, \ldots, a_n$ números enteros distintos con $n > 1$. Demostrar que el polinomio $p(x) = (x - a_1)(x - a_2) \cdots (x - a_n) - 1$ no puede ser escrito en la forma $g(x)h(x)$ donde $g(x)$ y $h(x)$ son polinomios no constantes con coeficientes enteros.

Solución. Supongamos, por contradicción, que $p(x) = g(x)h(x)$ para ciertos polinomios no constantes $g(x)$ y $h(x)$ con coeficientes enteros. Luego, tenemos que $g(a_i)h(a_i) = p(a_i) = -1$ para $i = 1, \ldots, n$. Como $g(a_i)$ y $h(a_i)$ son enteros (pues $g(x)$ y $h(x)$ son polinomios con coeficientes enteros), uno debe ser 1 y el otro debe ser -1. Por lo tanto, $g(a_i) + h(a_i) = 0$ para $i = 1, \ldots, n$, lo cual implica que el polinomio $q(x) = g(x) + h(x)$ tiene n raíces distintas.
Por otro lado, como $g(x)h(x) = p(x)$, tenemos que $\operatorname{gr} g(x)h(x) = \operatorname{gr} p(x) = n$. Como $g(x)$ y $h(x)$ no son constantes, ni $g(x)$ ni $h(x)$ tiene grado mayor que $n - 1$. Por lo tanto, el grado de $q(x) = g(x) + h(x)$ es menor que n, lo cual implica que $q(x)$ tiene menos de n raíces, lo que es una contradicción. □

Ejemplo 8. [Olimpiada Internacional, 1993] Sea $f(x) = x^n + 5x^{n-1} + 3$, donde $n > 1$ es un entero. Demostrar que $f(x)$ no puede escribirse como el producto de dos polinomios no constantes con coeficientes enteros.

Solución. Supongamos, por contradicción, que $f(x) = p(x)q(x)$ donde $p(x) = a_k x^k + a_{k-1}x^{k-1} + \cdots + a_1 x + a_0$ y $q(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0$ son polinomios no constantes con coeficientes enteros. Luego, $k > 0$ y $m > 0$. Como $\operatorname{gr} f(x) = \operatorname{gr} p(x) + \operatorname{gr} q(x)$, tenemos que $k + m = n$ con $k < n$ y $m < n$. De la igualdad $f(x) = p(x)q(x)$, se sigue que $a_0 b_0 = 3$ y $a_k b_m = 1$. Como los coeficientes de los polinomios $p(x)$ y $q(x)$ son enteros, tenemos que $a_0 = \pm 1$ y $b_0 = \pm 3$ (o al revés) y $a_k = b_m = \pm 1$.
Sea ℓ el menor índice con la propiedad de que $3 \nmid b_\ell$. Como $3 \mid b_0$ y $3 \nmid b_m$, necesariamente $0 < \ell \leq m$. Además, por la definición de ℓ, tenemos que $a_\ell b_0 + a_{\ell-1}b_1 + \cdots + a_1 b_{\ell-1}$ es divisible por 3. Como $a_\ell b_0 + a_{\ell-1}b_1 + \cdots + a_1 b_{\ell-1} + a_0 b_\ell$ es el coeficiente de x^ℓ en el producto $p(x)q(x)$ y $3 \nmid a_0 b_\ell$, se sigue que dicho coeficiente no es divisible por 3. Por lo tanto, el coeficiente de x^ℓ en $f(x)$ no es divisible por 3, lo cual implica que $\ell \geq n - 1$. Así, $n - 1 \leq \ell \leq m < n$, esto es, $\ell = m = n - 1$. En consecuencia, $n = k + m = k + n - 1$ de donde $k = 1$. De esta manera, $p(x) = a_1 x + a_0 = \pm x \pm 1$ (pues $a_0 = \pm 1$ y $a_1 = a_k = \pm 1$). Es fácil ver que las posibles raíces de $p(x)$ son 1 y -1. Como toda raíz de $p(x)$ es raíz de $f(x)$, se sigue que $f(1) = 0$ o $f(-1) = 0$. Sin embargo, tenemos que $f(1) = 1 + 5 + 3 = 9$ y $f(-1) = (-1)^n + 5(-1)^{n-1} + 3 = 4(-1)^{n-1} + 3 = 7$ o -1, lo que es una contradicción. □

Polinomios simétricos elementales y fórmulas de Vieta

¿Hay alguna relación entre las raíces de un polinomio y sus coeficientes? En el caso de los polinomios cuadráticos ya vimos que sí la hay. Consideremos un polinomio de grado $n > 0$ de la forma

$$p(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n = a_0(x - r_1)(x - r_2)\cdots(x - r_n).$$

Comparando los coeficientes de x^{n-1} en cada lado de la igualdad, obtenemos que $r_1 + r_2 + \cdots + r_n = -a_1/a_0$. De manera análoga, si ahora comparamos los términos constantes obtenemos que $r_1 r_2 \cdots r_n = (-1)^n a_n/a_0$. Las relaciones generales entre las raíces de $p(x)$ y sus coeficientes, están dadas por las fórmulas de Vieta, como veremos a continuación. Antes necesitamos una definición.
Sea $k \in \{1, 2, \ldots, n\}$. El k-ésimo *polinomio simétrico elemental* en las variables $x_1, \ldots, x_n$, es el polinomio σ_k definido por

$$\sigma_k = \sigma_k(x_1, x_2, \ldots, x_n) = \sum x_{i_1} x_{i_2} \ldots x_{i_k},$$

donde la suma se realiza sobre los subconjuntos $\{i_1, \ldots, i_k\}$ de tamaño k del conjunto $\{1, 2, \ldots, n\}$. En particular, $\sigma_1 = x_1 + x_2 + \cdots + x_n$ y $\sigma_n = x_1 x_2 \cdots x_n$.

Teorema. [Fórmulas de Vieta] Si $r_1, r_2, \ldots, r_n$ son las raíces del polinomio $p(x) = a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_n$, entonces

$$a_k = (-1)^k \sigma_k(r_1, \ldots, r_n)a_0$$

para $k = 1, 2, \ldots, n$.

Demostración. La prueba la haremos por inducción en n. El caso $n = 1$ es trivial. Supongamos que $n > 1$ y escribamos $p(x) = (x - r_n)q(x)$, donde $q(x) = (x - r_1)\cdots(x - r_{n-1})$. Determinemos el coeficiente a_k de x^k en el polinomio $p(x)$. Como los coeficientes de x^{k-1} y x^k en $q(x)$ son $b_{k-1} = (-1)^{k-1}\sigma_{k-1}(r_1, \ldots, r_{n-1})a_0$ y $b_k = (-1)^k\sigma_k(r_1, \ldots, r_{n-1})a_0$, respectivamente, tenemos que

$$a_k = -r_n b_{k-1} + b_k = (-1)^k \sigma_k(r_1, \ldots, r_n)a_0,$$

lo que completa la inducción. □

Ejemplo 9. Encontrar todos los polinomios con coeficientes racionales

$$p(x) = x^3 + ax^2 + bx + c$$

tales que a, b y c sean raíces de $p(x)$.

Solución. Aplicando las fórmulas de Vieta, tenemos que $a+b+c = -a$, $ab+bc+ca = b$ y $abc = -c$. La tercera ecuación se puede escribir como $(ab+1)c = 0$, lo cual implica que $ab = -1$ o $c = 0$.
Si $c = 0$, sustituyendo en la primera y en la segunda ecuación del sistema anterior obtenemos que $a + b = -a$ y $ab = b$. Resolviendo este sistema de dos ecuaciones, obtenemos las soluciones $(a, b, c) = (0, 0, 0)$, $(1, -2, 0)$.
De la primera ecuación del sistema de tres ecuaciones, tenemos que $c = -2a - b$. Luego, si $ab = -1$, la segunda ecuación del sistema es $-1 + b(-2a - b) + (-2a - b)a = b$, esto es, $2a^2 - 2 + b + b^2 = 0$. Multiplicando por a^2 y usando que $ab = -1$, obtenemos que $2a^4 - 2a^2 - a + 1 = 0$. Así, a es una raíz racional del polinomio $2x^4 - 2x^2 - x + 1$. Aplicando el Teorema de las raíces racionales, los valores posibles de a son ± 1 y $\pm\frac{1}{2}$. Verificando cada posibilidad, es fácil ver que la única solución es $a = 1$, de donde $(a, b, c) = (1, -1, -1)$.
Por lo tanto, los polinomios que satisfacen las condiciones del problema son el polinomio cero, $x^3 + x^2 - 2x$ y $x^3 + x^2 - x - 1$. □

Ejemplo 10. Encontrar todos los polinomios de la forma $x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ con $a_j \in \{-1, 1\}$ para $j = 0, 1, \ldots, n-1$, cuyas raíces sean números reales.

Solución. Observemos que para cualesquiera números reales $r_1, \ldots, r_n$ se satisface que

$$\sum_{i=1}^{n} r_i^2 = \left(\sum_{i=1}^{n} r_i\right)^2 - 2\sum_{i<j} r_i r_j.$$

Luego, si $r_1, \ldots, r_n$ son las raíces del polinomio dado, de las fórmulas de Vieta tenemos que $\sum_{i=1}^{n} r_i = -a_{n-1}$, $\sum_{i<j} r_i r_j = a_{n-2}$ y $r_1 r_2 \cdots r_n = a_0 = \pm 1$. Por lo tanto, $\sum_{i=1}^{n} r_i^2 = a_{n-1}^2 - 2a_{n-2} \leq 3$ y $r_1^2 r_2^2 \cdots r_n^2 = 1$. Por otro lado, por la desigualdad MA-MG aplicada a los números no negativos $r_1^2, \ldots, r_n^2$, tenemos que $(r_1^2 r_2^2 \cdots r_n^2)^{1/n} \leq \frac{r_1^2 + r_2^2 + \cdots + r_n^2}{n}$, esto es, $1 \leq \frac{r_1^2 + r_2^2 + \cdots + r_n^2}{n} \leq \frac{3}{n}$, de donde se sigue que $n \leq 3$.
Si $n = 1$, los polinomios son $x + 1$ y $x - 1$. Si $n = 2$, los polinomios son $x^2 + x - 1$ y $x^2 - x - 1$. Si $n = 3$, tenemos la igualdad en la desigualdad MA-MG anterior, lo que significa que $r_1^2 = r_2^2 = r_3^2$, esto es, $|r_1| = |r_2| = |r_3|$. Como $r_1 r_2 r_3 = \pm 1$, se sigue que $|r_1||r_2||r_3| = 1$. Por lo tanto, $|r_1|^3 = |r_2|^3 = |r_3|^3 = 1$. Así, $|r_1| = |r_2| = |r_3| = 1$ y, en consecuencia, $r_1 = \pm 1$, $r_2 = \pm 1$ y $r_3 = \pm 1$. Ahora es fácil determinar los polinomios de grado 3: $(x^2 - 1)(x - 1) = x^3 - x^2 - x + 1$ y $(x^2 - 1)(x + 1) = x^3 + x^2 - x - 1$.
□

A continuación dejamos unos ejercicios para el lector.

Ejercicios

1) Demuestra que el polinomio $p(x) = x^6 - x^5 + x^4 - x^3 + x^2 - x + \frac{3}{4}$ no tiene raíces reales. (Sugerencia: Demuestra que $p(r) > 0$ para todo número real r).

2) Sea $p(x)$ un polinomio con coeficientes enteros y sean a, b números enteros distintos tales que $p(a)p(b) = -(a - b)^2$. Demuestra que $p(a) + p(b) = 0$.
(Sugerencia: Considera los números $A = \frac{p(a)}{a-b}$ y $B = \frac{-p(b)}{a-b}$).

3) Considera el polinomio $p(x) = x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x + 1$ con coeficientes reales no negativos $a_1, a_2, \ldots, a_{n-1}$. Si $p(x)$ tiene n raíces reales, demuestra que $p(2) \geq 3^n$. (Sugerencia: Usa las fórmulas de Vieta y la desigualdad MA-MG).

4) Determina el residuo de la división del polinomio $x^{2019} + 1$ entre el binomio $x - 1$.

5) Sean a, b y c números reales positivos. ¿Es posible que cada uno de los polinomios $p(x) = ax^2 + bx + c$, $q(x) = cx^2 + ax + b$ y $r(x) = bx^2 + cx + a$ tenga dos raíces reales? (Sugerencia: ¿Qué condiciones debe satisfacer un polinomio cuadrático para tener dos raíces reales?)

6) Sea $p(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_{n-1}x + a_n$ un polinomio con coeficientes enteros distintos de cero. Si $p(x)$ tiene n ceros enteros distintos y son primos relativos dos a dos, demuestra que a_{n-1} y a_n también son primos relativos. (Sugerencia: Procede por contradicción y usa las fórmulas de Vieta).

7) Demuestra que no existe un polinomio $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ con coeficientes enteros y de grado positivo con la propiedad de que cada uno de los números $p(0), p(1), p(2), \ldots$ sea primo. (Sugerencia: Si existiera tal polinomio, entonces a_0 sería primo. Prueba que el polinomio $q(x) = p(a_0 x) - a_0$ tiene una infinidad de raíces).

8) Demuestra que no es posible escribir el polinomio $p(x) = x^{105} - 9$ como el producto de dos polinomios con coeficientes enteros y cada uno de grado menor que 105. (Sugerencia: Supón que $p(x) = q(x)r(x)$ donde $q(x)$ y $r(x)$ son polinomios con coeficientes enteros y de grados menores que 105. Considera el producto de las raíces de $q(x)$).

9) Un polinomio *mónico* es un polinomio cuyo coeficiente líder es igual a 1. Si $p(x)$ es un polinomio mónico de grado 4 tal que $p(1) = 10$, $p(2) = 20$ y $p(3) = 30$, determina el valor de $p(12) + p(-8)$. (Sugerencia: Muestra que el polinomio $p(x) - 10x$ es divisible por el polinomio $(x-1)(x-2)(x-3)$).

10) Sea $p(x) = x^n + a_1x^{n-1} + \cdots + a_n$ un polinomio con coeficientes complejos con raíces $r_1, \ldots, r_n$ y sea $q(x) = x^n + b_1x^{n-1} + \cdots + b_n$ un polinomio con coeficientes complejos con raíces $r_1^2, \ldots, r_n^2$. Demuestra que si $a_1 + a_3 + a_5 + \cdots$ y $a_2 + a_4 + a_6 + \cdots$ son números reales, entonces $b_1 + b_2 + \cdots + b_n$ también es un número real. (Sugerencia: Observa que $q(x^2) = (-1)^n p(x)p(-x)$).

Bibliografía

1) R. Gelca, T. Andreescu. *Putnam and Beyond.* Springer, 2007.

2) T. Andreescu, R. Gelca. *Mathematical Olympiad Challenges*. Birkhäuser, 2009.