Los polinomios ciclotómicos binarios son planos: una demostración vía álgebra lineal

Expositor: Javier Pedro García (Ciclo Básico Común. Universidad de Buenos Aires, javgrzgarcia@gmail.com)
Autor/es: Javier Pedro García (Ciclo Básico Común. Universidad de Buenos Aires, javgrzgarcia@gmail.com)

Es un hecho conocido que si p y q son números primos diferentes, los coeficientes del polinomio ciclotómico binario $\Phi_{pq}(x)$ pertenecen al conjunto $\{0, \pm 1\}$. Esta particularidad lleva a decir entonces que los polinomios ciclotómicos binarios son *planos* (*flat* en la terminología inglesa).

La primera demostración de este hecho, en cierto modo asombroso, fue proporcionada en 1883 por un matemático de apellido Migotti ([3], aunque no hemos accedido a la referencia). Posteriormente, otras demostraciones fueron proporcionadas por Lenstra ([2]), Lam y Leung ([1]), entre otros. Los argumentos utilizados para probar la *planitud* de $\Phi_{pq}(x)$ se basan sobre identidades polinomiales que involucran a los polinomios ciclotómicos, como por ejemplo las identidades equivalentes (vía la fórmula de inversión de Moebius):

$$x^n - 1 = \prod_{d|n} \Phi_d(x), \qquad \Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)},$$

siendo μ la función de Moebius.

En esta comunicación presentaremos una nueva demostración de la planitud de los polinomios ciclotómicos binarios $\Phi_{pq}(x)$, apelando al álgebra lineal implícita en la factorización de polinomios; en particular, en la identidad

$$\Phi_{pn}(x) = \frac{\Phi_n(x^p)}{\Phi_n(x)} \quad \text{si } p \text{ no divide a } n.$$

Esta identidad puede deducirse de las anteriores o puede demostrarse de manera independiente. Dado que conocemos $\Phi_q(x)$, la factorización

$$\Phi_q(x)\Phi_{pq}(x) = \Phi_q(x^p)$$

puede expresarse como un sistema lineal $Ax = b$ (siendo A y b una matriz Toeplitz y un vector, respectivamente, cuyas entradas son coeficientes de Φ_q; en particular, 1 es el único valor que toman las entradas no nulas) cuya única solución es el vector de coeficientes de $\Phi_{pq}(x)$. Estos sistemas son casos particulares de sistemas lineales más generales y nuestra tarea consiste, entonces, en demostrar que estos últimos tienen soluciones cuyas entradas pertenecen a $\{0, \pm 1\}$.

Bibliografía

[1] T.Y. Lam and K.H. Leung. On the cyclotomic polynomial $\Phi_{pq}(X)$. *Am. Math. Mon.*, 103(7):562–564, 1999.

[2] H. W. Lenstra, Jr. Vanishing sums of roots of unity. In *Proceedings, Bicentennial Congress Wiskundig Genootschap (Vrije Univ., Amsterdam, 1978), Part II*, volume 101 of *Math. Centre Tracts*, pages 249–268. Math. Centrum, Amsterdam, 1979.

[3] A. Migotti. Zur Theorie der Kreisteilung. *Wien. Ber.*, 87:8–14, 1883.