Divulgaciones Matemáticas Vol. 11 No. 2(2003), pp. 149–152

Sobre la Divisibilidad de Polinomios con Coeficientes Enteros

On the Divisibility of Polynomials with Integer Coefficients

José H. Nieto (jhnieto@luz.ve)
Departamento de Matemática, Facultad de Ciencias
Universidad del Zulia, Maracaibo, Venezuela

Resumen

Sean $f, g \in \mathbb{Z}[x]$. En este trabajo se prueba que $g \mid f$ si y sólo si $c(g) \mid c(f)$ (donde $c(f)$ denota el *contenido* de f, es decir el máximo común divisor de sus coeficientes) y $g(n) \mid f(n)$ para infinitos $n \in \mathbb{Z}$. Como aplicación se prueba que los polinomios mónicos irreducibles y no constantes $f \in \mathbb{Z}[x]$ tales que $f(n)$ divide a $f(n^k)$ para todo entero n (siendo $k \geq 2$ un entero fijo) son los polinomios ciclotómicos Φ_j de orden j coprimo con k.
Palabras y frases clave: polinomios, divisibilidad, ciclotómico.

Abstract

Let $f, g \in \mathbb{Z}[x]$. In this paper it is proved that $g \mid f$ if and only if $c(g) \mid c(f)$ (where $c(f)$ denotes the *content* of f, i.e. the greatest common divisor of its coefficients) and $g(n) \mid f(n)$ for infinitely many $n \in \mathbb{Z}$. As an application it is proved that the monic irreducible non constant polynomials $f \in \mathbb{Z}[x]$ such that $f(n)$ divides $P(n^k)$ for all integers n ($k \geq 2$ being a fixed integer) are the cyclotomic polynomials Φ_j with order j coprime with k.
Key words and phrases: polynomials, divisibility, cyclotomic.

1 Introducción

Denotemos con $\mathbb{Z}[x]$ al anillo de los polinomios con coeficientes enteros en una indeterminada x, y con $\mathbb{Q}[x]$ al anillo de los polinomios con coeficientes

Recibido 2002/12/17. Aceptado 2003/11/27.
MSC (2000): Primary 13F20; Secondary 11C08.

racionales. Si $f, g \in \mathbb{Z}[x]$ se dice que g divide a f en $\mathbb{Z}[x]$ (y se denota $g \mid f$) si existe $h \in \mathbb{Z}[x]$ tal que $f = gh$. Si $g \mid f$ entonces es claro que $g(n) \mid f(n)$ para todo entero n. El propósito de esta nota es establecer algún tipo de recíproco para esta propiedad, en otras palabras deducir la relación de divisibilidad entre dos polinomios a partir de la divisibilidad entre los valores adoptados por ellos. El teorema de identidad de polinomios establece que si dos polinomios toman valores iguales al ser evaluados en un número de valores superior al grado de ambos, entonces son idénticos. Estamos interesados en un resultado similar pero sustituyendo la relación de igualdad por la de divisibilidad. Los siguientes ejemplos muestran las dificultades inherentes a este problema.

Ejemplo 1. Sea N un entero positivo y consideremos los polinomios $f(x) = x + N!$ y $g(x) = x$. Entonces $g(n) \mid f(n)$ para $n = 1, 2, \ldots, N$ pero $g \nmid f$.

Este ejemplo muestra que ningún número finito de valores es suficiente para deducir la divisibilidad de polinomios a partir de los valores adoptados por ellos.

Ejemplo 2. Sean $f(x) = x^2 + x$ y $g(x) = 2$. Entonces $g(n) \mid f(n)$ para todo $n \in \mathbb{Z}$ pero $g \nmid f$ en $\mathbb{Z}[x]$.

¡Este ejemplo muestra que ni siquiera la totalidad de los valores es suficiente! Pero es claro que esta situación es consecuencia de que los coeficientes de g admiten un divisor común (en este caso el 2) que no divide a todos los coeficientes de f.

Definamos el *contenido* $c(f)$ de un polinomio $f \in \mathbb{Z}[x]$ como el máximo común divisor de todos sus coeficientes. Si $c(f) = 1$ entonces se dice que el polinomio f es *primitivo*. Es claro que para cualquier polinomio $f \in \mathbb{Z}[x]$ existe $f_1 \in \mathbb{Z}[x]$ tal que f_1 es primitivo y $f = c(f)f_1$.

A continuación se enuncian un resultado clásico de Gauss y dos corolarios inmediatos:

Lema 1 (Gauss). *Si $f, g \in \mathbb{Z}[x]$ son ambos primitivos entonces su producto fg también es primitivo.*

La demostración puede verse en [3] o [1].

Corolario 1. *Si $f, g \in \mathbb{Z}[x]$ entonces $c(fg) = c(f)c(g)$.*

Corolario 2. *Si $f, g \in \mathbb{Z}[x]$ y $g \mid f$ entonces $c(g) \mid c(f)$.*

2 El resultado principal

Teorema 1. *Si $f, g \in \mathbb{Z}[X]$, $c(g) \mid c(f)$ y $g(n) \mid f(n)$ para infinitos enteros n, entonces $g \mid f$ en $\mathbb{Z}[X]$.*

Demostración. Dividamos f entre g en $\mathbb{Q}[x]$ para obtener $f(x) = g(x)q(x) + r(x)$, con $q, r \in \mathbb{Q}[x]$ y el grado de r es menor que el de g. Sea m el mínimo común múltiplo de los denominadores de todos los coeficientes de q y r, de modo tal que $mq, mr \in \mathbb{Z}[x]$. Sea $n_1, n_2, \ldots$ una sucesión de enteros diferentes tales que $g(n_i) \mid f(n_i)$ y $g(n_i) \neq 0$ para todo $i = 1, 2, \ldots$

Entonces $mf(n_i)/g(n_i) - mq(n_i) = mr(n_i)/g(n_i)$ para $i = 1, 2, \ldots$ y como el miembro izquierdo es entero el miembro derecho también debe serlo. Pero como $\lim_{i\to\infty} |n_i| = \infty$ y el grado de r es menor que el de g se tiene que $\lim_{i\to\infty} mr(n_i)/g(n_i) = 0$. Por lo tanto $r(n_i) = 0$ a partir de un cierto i_0 en adelante. Esto implica que r es idénticamente nulo y por lo tanto $f = gq$ y $mf = g(mq)$. Aplicando ahora el Corolario 2 resulta que $mc(f) = c(mf) = c(g)c(mq)$, y como por hipótesis $c(g) \mid c(f)$ se sigue que $m(c(f)/c(g)) = c(mq)$. Por lo tanto todos los coeficientes de mq son múltiplos de m y $q \in \mathbb{Z}[x]$, con lo cual $g \mid f$ en $\mathbb{Z}[X]$. □

3 Una aplicación

En [2] se plantea el problema siguiente: "Hallar todos los polinomios P con coeficientes enteros, irreducibles, mónicos y de grado 2000, tales que $P(n)$ divide a $P(n^2)$ para todo entero n". Es fácil hallar los polinomios de grado 1 que satisfacen las demás condiciones del problema, a saber x y $x - 1$. De grado 2 hay sólo uno, a saber $x^2 + x + 1$. Pero tratar de hallar los de grado 2000 por métodos directos no parece factible. Una generalización natural de este problema consiste en buscar polinomios de grado arbitrario, irreducibles y mónicos, tales que $P(n)$ divida a $P(n^k)$ para todo entero n (siendo $k \geq 2$ un entero fijo).

Denotemos mediante $\mathbf{\Phi}_n$ al *polinomio ciclotómico* de orden n, es decir

$$\mathbf{\Phi}_n(x) = \prod_{\substack{d=1 \\ (d,n)=1}}^{n-1} (x - e^{\frac{2\pi i d}{n}}).$$

Es bien conocido (ver [3]) que $\mathbf{\Phi}_n$ es un polinomio con coeficientes enteros, mónico e irreducible. Sus raíces son las raíces primitivas de la unidad de orden n, y su grado es por lo tanto igual a $\phi(n)$ (siendo ϕ la función de Euler).

Se tiene entonces el siguiente resultado:

Teorema 2. *Sea $k \geq 2$ un entero. Los polinomios con coeficientes enteros, mónicos e irreducibles tales que $P(n)|P(n^k)$ para infinitos enteros n son 1, x y los polinomios ciclotómicos $\mathbf{\Phi}_j$ para j coprimo con k.*

Demostración. Obviamente el polinomio constante 1 y el polinomio x satisfacen las condiciones del problema, y los consideraremos como soluciones triviales. Si P es otro polinomio solución entonces por el Teorema 1 se tiene que $P(x^k) = P(x)Q(x)$, para algún $Q \in \mathbb{Z}[x]$. Si ζ es una raíz (compleja) de P entonces $P(\zeta^k) = P(\zeta)Q(\zeta) = 0$, es decir que ζ^k también es raíz de P. Aplicando reiteradamente este razonamiento resulta que también ζ^{k^2}, ζ^{k^3}, ζ^{k^4},... son raíces de P. Pero como P sólo puede tener un número finito de raíces, deben existir enteros $r > s > 0$ tales que $\zeta^{k^r} = \zeta^{k^s}$, es decir que $\zeta^{k^s}(\zeta^{k^r-k^s} - 1) = 0$. Pero $\zeta \neq 0$ (pues P no es una de las soluciones triviales), por lo tanto ζ es una raíz de la unidad. Si ζ es primitiva de orden j, entonces las demás raíces primitivas de la unidad de orden j deben ser raíces de P, es decir que P debe ser múltiplo de $\mathbf{\Phi}_j$, y como P es irreducible en realidad se tiene que $P = \mathbf{\Phi}_j$. Ahora bien, para que ζ^k sea también primitiva de orden j, k y j deben ser coprimos. □

Referencias

[1] Herstein, I. N. *Topics in Algebra*, Blaisdell, Waltham, 1964. Hay traducción al castellano: *Álgebra Moderna*, Trillas, México, 1970.

[2] Caragea, D., Ene, V. *Problem 10802*, The American Mathematical Monthly, **107**(5) (2000), p. 462.

[3] Lang, S. *Algebra*, Addison-Wesley, Reading, 1965.