ISSN: 2711–1792 (En línea) • Espacio Matemático Vol. 2 No. 2 (2021), pp. 144–151

Comparación de dos algoritmos para resolver el problema de pertenencia a ideales de $\mathbb{Z}[x]$

Luis F. Cáceres Duque, Silvia M. López Gallo

Resumen

En este trabajo, presentamos dos algoritmos para resolver el problema de pertenencia a ideales de $\mathbb{Z}[x]$. El primer algoritmo fue desarrollado por H. Simmons en [5]. El segundo algoritmo se basa en los resultados presentados por G. Szekeres en [6] acerca de bases mínimas para los ideales de un anillo de polinomios sobre un dominio entero.

Palabras y frases clave: problema de pertenencia, ideales, polinomios con coeficientes enteros.

A comparison of two algorithms for solving the ideal membership problem for $\mathbb{Z}[x]$

Abstract

In this work, we present two algorithms for solving the ideal membership problem for $\mathbb{Z}[x]$. The first algorithm was developed by H. Simmons in [5]. The second algorithm is based on the results presented by G. Szekeres in [6] about minimal bases for the ideals of a polynomial ring over an integral domain.

Key words and phrases: membership problem, ideals, polynomials over integers.

1 Introducción

Dado un ideal I de un anillo R, el *problema de pertenencia a un ideal* consiste en determinar si un elemento $r \in R$ pertenece o no a I. En anillos de polinomios, el problema de pertenencia es un problema algorítmico fundamental con importantes aplicaciones en sistemas de álgebra computacional. En general, este problema es notoriamente intratable, incluso cuando se dan explícitamente el polinomio de interés a decidir la pertenencia a un ideal y

un conjunto de polinomios que generen a dicho ideal. Sin embargo, debido a sus aplicaciones, los algoritmos para este problema son ampliamente estudiados, basados principalmente en la teoría de las bases de Gröbner, las cuales están definidas para anillos de polinomios en varias variables sobre un campo.

En particular, dado que $\mathbb{Q}[x]$ es un dominio de ideales principales y, de hecho, un dominio euclídeo, se puede resolver fácilmente el problema de pertenencia a ideales de $\mathbb{Q}[x]$: *Dados* $f(x), f_1(x), \cdots, f_n(x) \in \mathbb{Q}[x]$, *existe un algoritmo para decidir si* $f(x) \in \langle f_1(x), \cdots, f_n(x)\rangle$. El primer paso es encontrar $g(x) := \gcd(f_1(x), \cdots, f_n(x))$. Como $f(x) \in \langle f_1(x), \cdots, f_n(x)\rangle$ es equivalente a $f(x) \in \langle g(x)\rangle$, el siguiente paso es usar el algoritmo de la división para escribir $f(x) = g(x)q(x)+r(x)$, donde $r(x) = 0$ o $\deg(r) < \deg(g)$. Por tanto, $f(x)$ pertenece al ideal si, y solo si, $r(x) = 0$.

A diferencia de $\mathbb{Q}[x]$, $\mathbb{Z}[x]$ no es un dominio de ideales principales, lo cual hace que decidir el problema de pertenencia no sea tan sencillo. Sin embargo, $\mathbb{Z}[x]$ es un anillo noetheriano, por tanto, cada ideal de $\mathbb{Z}[x]$ es finitamente generado. Así, dados $f(x), f_1(x), \cdots, f_n(x) \in \mathbb{Z}[x]$, el problema de pertenencia a ideales de $\mathbb{Z}[x]$ consiste en decidir si $f(x)$ pertenece o no a $I = \langle f_1(x), \cdots, f_n(x)\rangle$. En este trabajo presentamos dos algoritmos que deciden la pertenencia a ideales de $\mathbb{Z}[x]$.

2 Algoritmo de Simmons

En [5], Simmons da un algoritmo que se puede aplicar al problema de pertenencia a ideales de $\mathbb{Z}[x]$ descrito anteriormente. En realidad, da dos procedimientos efectivos: el primero procedimiento termina si, y solo si, $f(x) \in I$, y el segundo procedimiento termina si, y solo si, $f(x) \notin I$.

Primer procedimiento

Se hace una enumeración $\{(g_{i1}(x), \cdots, g_{in}(x)) : i = 1, 2, 3, \ldots\}$ de $(\mathbb{Z}[x])^n$ y para cada n-tupla se calcula $f_1(x)g_{i1}(x) + \cdots + f_n(x)g_{in}(x)$. Este procedimiento se va a detener cuando $f(x) = f_1(x)g_{i1}(x) + \cdots + f_n(x)g_{in}(x)$ para alguna de las n-tuplas.

Aunque el procedimiento anterior es efectivo, realizar una enumeración de

$(\mathbb{Z}[x])^n$ es un problema que requiere mucho tiempo computacional. Para evitar la enumeración de $(\mathbb{Z}[x])^n$, proponemos otro procedimiento efectivo que se va a detener si, y solo si, $f(x) \in I$:

Es claro que $f(x)$ pertenece a I si se puede escribir como una combinación lineal de los generadores de I, es decir,

$$f(x) = g_1(x)f_1(x) + \cdots + g_n(x)f_n(x)$$

para algunos $g_1(x), \cdots, g_n(x) \in \mathbb{Z}[x]$. Usando el método de "comparación de coeficientes", reemplazamos cada $g_i(x)$ por un polinomio arbitrario (es decir, con coeficientes no específicos) de grado $0, 1, 2, \ldots$ hasta que el sistema de ecuaciones obtenido tenga solución en $\mathbb{Z}$. Este procedimiento es efectivo porque existen algoritmos para resolver sistemas de ecuaciones diofánticas lineales.

Ilustramos el procedimiento anterior en el siguiente ejemplo.

Ejemplo 1. Para determinar si el polinomio

$$f(x) = 13x^4 + 23x^3 - 59x^2 + 5x - 21$$

pertenece al ideal generado por $f_1(x) = 6x^2 - x + 3$, $f_2(x) = 19x^2 - 4x - 3$, $f_3(x) = 2x^3 + 8x^2 + 6x - 5$ y $f_4(x) = 5x^4 - x^2 - 4x - 8$, iniciamos resolviendo el sistema de ecuaciones que se obtiene de igualar coeficientes en la ecuación

$$f(x) = a_0f_1(x) + b_0f_2(x) + c_0f_3(x) + d_0f_4(x).$$

Como el sistema anterior no tiene solución, pasamos ahora a resolver el sistema que se obtiene de la ecuación

$$f(x) = (a_1x + a_0)f_1(x) + (b_1x + b_0)f_2(x) + (c_1x + c_0)f_3(x) + (d_1x + d_0)f_4(x).$$

Este sistema tiene infinitas soluciones en $\mathbb{Q}$ y, en particular,

$$a_0 = -1,\ a_1 = 2,\ b_0 = -2,\ b_1 = 1,\ c_0 = 0,\ c_1 = -1,\ d_0 = 3 \text{ y } d_1 = 0$$

es una solución en $\mathbb{Z}$. Por tanto, el procedimiento termina y concluimos que

$$f(x) \in \langle f_1(x), f_2(x), f_3(x), f_4(x) \rangle.$$

La dificultad aquí radica en que no conocemos de antemano si los polinomios buscados existen y tampoco sabemos los grados de dichos polinomios. En [2] se estudian cotas de los grados de los polinomios $g_1(x), \cdots, g_n(x)$.

Segundo procedimiento

El segundo de estos procedimientos utiliza resultados sobre los ideales en anillos de polinomios en varias variables sobre un campo, presentados por Hermann en [4]. Consiste en lo siguiente:

Etapa -1. ¿$f(x) \in I$ sobre $\mathbb{Q}$?
No - entonces $f(x) \notin I$ sobre $\mathbb{Z}$. PARAR.
Sí - ir a la etapa 0.

Etapa 0. Encontrar un entero c tal que $cf(x) \in I$ sobre $\mathbb{Z}$.
Ir a la etapa 1.

Etapa 1. ¿$f(x) \in I + \langle c \rangle$ sobre $\mathbb{Z}$?
No - entonces $f(x) \notin I$ sobre $\mathbb{Z}$. PARAR.
Sí - ir a la etapa 2.

$\vdots$

Etapa s. ¿$f(x) \in I + \langle c^s \rangle$ sobre $\mathbb{Z}$?
No - entonces $f(x) \notin I$ sobre $\mathbb{Z}$. PARAR.
Sí - ir a la etapa $s + 1$.

$\vdots$

Al realizar simultáneamente los dos procedimientos anteriores, uno de ellos va a parar, por tanto, podemos enunciar el siguiente teorema.

Teorema 1. *Existe un procedimiento efectivo para resolver el problema de pertenencia a ideales de* $\mathbb{Z}[x]$.

3 Algoritmo de Szekeres

Dado un conjunto de generadores $f_1(x), \cdots, f_n(x)$ de un ideal I de $\mathbb{Z}[x]$, es deseable pasar a un conjunto diferente de generadores que estén determinados unívocamente y que permitan decidir efectivamente la pertenencia a I.

En [6] se prueba que cada ideal de $\mathbb{Z}[x]$ posee un conjunto de generadores con estas propiedades, al cual llamaremos *base mínima*.

Definimos una *base mínima* para un ideal I de $\mathbb{Z}[x]$ como en [6]. Si I es un ideal principal, $I = \langle f(x) \rangle$, la base mínima de I será $\{f(x)\}$ o $\{-f(x)\}$ si el coeficiente principal de $f(x)$ es positivo o negativo, respectivamente. Si $I = \langle f(x) \rangle J$, donde el coeficiente principal de $f(x)$ es positivo y J tiene la base mínima $\{h_1(x), \cdots, h_n(x)\}$, entonces la base mínima de I estará definida por $\{f(x)h_1(x), \cdots, f(x)h_n(x)\}$. Por tanto, es suficiente encontrar una base mínima para cada ideal no principal primitivo de $\mathbb{Z}[x]$.

En [6] se prueba que si J es un ideal no principal primitivo de $\mathbb{Z}[x]$, este posee una base mínima única $\{g_0(x), g_1(x), \cdots, g_m(x)\}$ con las siguientes propiedades:

$$g_0(x) = q_1 q_2 \cdots q_m$$

$$q_k g_k(x) = x g_{k-1}(x) + \sum_{i=0}^{k-1} b_{ki} g_i(x)$$

$$0 \leq \begin{bmatrix} b_{10} & & & \\ b_{20} & b_{21} & & \\ \vdots & \vdots & \ddots & \\ b_{m0} & b_{m1} & \cdots & b_{m(m-1)} \end{bmatrix} < \begin{bmatrix} q_1 \\ q_2 \\ \vdots \\ q_m \end{bmatrix}$$

Estas propiedades implican que $\deg(g_k) = k$ para $k = 0, 1, \cdots, m$ y que $g_m(x)$ es mónico. El número m se denomina el grado de J.

Una de las propiedades más importantes de la base mínima de un ideal de $\mathbb{Z}[x]$ es que permite caracterizar los elementos del ideal:

Proposición 1. *Sea J un ideal no principal primitivo de $\mathbb{Z}[x]$ con base mínima $\{g_0(x), g_1(x), \cdots, g_{m-1}(x), g_m(x)\}$. Entonces cada elemento de J es de la forma:*

$$c_0 g_0(x) + c_1 g_1(x) + \cdots + c_{m-1} g_{m-1}(x) + h(x) g_m(x)$$

para algunas constantes únicas $c_0, c_1, \cdots, c_{m-1} \in \mathbb{Z}$ y algún polinomio único $h(x) \in \mathbb{Z}[x]$.

Debido a la proposición anterior, toda la dificultad computacional para determinar la pertenencia de un polinomio a un ideal de $\mathbb{Z}[x]$ se completa al encontrar su base mínima. Esto se establece como Lema 4 en [3]:

Lema 1. *Sea J un ideal no principal primitivo de $\mathbb{Z}[x]$ con base mínima $\{g_0(x), g_1(x), \cdots, g_m(x)\}$. Si $f(x)$ es un polinomio de $\mathbb{Z}[x]$, existe un procedimiento efectivo para decidir si $f(x) \in J$ o no.*

Demostración. Usando el algoritmo de la división en $\mathbb{Q}[x]$ podemos escribir $f(x) = g_m(x)q(x) + r(x)$ donde $r(x) = 0$ o $n := \deg(r) < m$. El hecho de que $g_m(x)$ es un polinomio mónico implica que $q(x), r(x) \in \mathbb{Z}[x]$. Por tanto, $f(x) \in J$ si, y solo si, $r(x) \in J$. Usando la Proposición 1, $r(x) \in J$ si, y solo si, existen $a_0, a_1, \cdots, a_n \in \mathbb{Z}$ tal que $r(x) = a_0 g_0(x) + a_1 g_1(x) + \cdots + a_n g_n(x)$. Usando la comparación de coeficientes y los métodos usuales del álgebra lineal, podemos decidir efectivamente si el sistema de $n+1$ ecuaciones con $n+1$ variables tiene solución en $\mathbb{Z}$. □

Para aplicar el algoritmo de la demostración del lema anterior, se debe conocer la base mínima del ideal. En [3], Cáceres-Duque da un procedimiento efectivo para encontrar la base mínima de un ideal que define Szekeres:

Teorema 2. *Dado un conjunto de generadores $f_1(x), \cdots, f_n(x)$ de un ideal I de $\mathbb{Z}[x]$, existe un procedimiento efectivo para encontrar su base mínima.*

El Teorema 2 junto con el Lema 1 permiten enunciar el siguiente teorema. Aunque el enunciado es el mismo del Teorema 1, el procedimiento efectivo al que nos referimos aquí es el algoritmo de Szekeres.

Teorema 3. *Existe un procedimiento efectivo para resolver el problema de pertenencia a ideales de $\mathbb{Z}[x]$.*

Demostración. Sea $I = \langle f_1(x), \cdots, f_n(x)\rangle$ un ideal de $\mathbb{Z}[x]$ y $f(x)$ un polinomio de $\mathbb{Z}[x]$. Supongamos que I no es un ideal principal, de lo contrario la prueba es trivial. Aplicando el Teorema 2, existe un procedimiento efectivo para encontrar la base mínima de I. Si I es primitivo, aplicando el Lema 1 existe un procedimiento efectivo para decidir si $f(x) \in I$ o no. Si I no es primitivo, entonces $I = \langle g(x)\rangle J$, donde $g(x) \in \mathbb{Z}[x]$ y J es un ideal no principal primitivo. Por tanto, $f(x) \in I$ si, y solo si, $f(x) = g(x)q(x)$ y $q(x) \in J$. Se divide $f(x)$ por $g(x)$ en $\mathbb{Q}[x]$, y si no hay residuo, se decide si el cociente obtenido pertenece a J usando el Lema 1. □

Ejemplo 2. El ideal $\langle f_1(x), f_2(x), f_3(x), f_4(x)\rangle$ dado en el Ejemplo 1 es un ideal no principal primitivo, cuya base mínima es $\{x^2 + 4x + 3, 5x, 5\}$. Para decidir si el polinomio

$$f(x) = 13x^4 + 23x^3 - 59x^2 + 5x - 21$$

pertenece o no a este ideal, dividimos $f(x)$ entre x^2+4x+3. El residuo que se obtiene es el polinomio $20x - 75$. Ahora, se resuelve el sistema de ecuaciones que se obtiene al igualar coeficientes en la ecuación

$$20x - 75 = a_1(5x) + a_0(5).$$

Podemos ver fácilmente que $a_0 = -15$ y $a_1 = 4$. Como esta es una solución en $\mathbb{Z}$, concluimos que

$$f(x) \in \langle f_1(x), f_2(x), f_3(x), f_4(x)\rangle.$$

4 Comentarios

- Los pasos del algoritmo de Simmons están explicados detalladamente en [5]. Sin embargo, el primer procedimiento (el que termina si $f(x) \in I$), aunque muy fácil de describir, sería poco práctico de llevar a cabo en un caso particular. Si bien, acá proponemos otro procedimiento efectivo, dicho procedimiento no es necesariamente factible, pues, en general, no es sencillo resolver sistemas de ecuaciones diofánticas lineales (de hecho, los algoritmos para resolver estos sistemas de ecuaciones también son ampliamente estudiados). En ambos casos, debemos concluir que el algoritmo de Simmons es un procedimiento efectivo pero no es en general factible.

- Szekeres demuestra la existencia y unicidad de una base mínima para cada ideal de $\mathbb{Z}[x]$, pero no dice cómo encontrarla. En [3], Cáceres-Duque da un procedimiento efectivo para encontrar la base mínima de un ideal de $\mathbb{Z}[x]$, el cual es el procedimiento efectivo al que nos referimos en el Teorema 2, pero dicho procedimiento no es necesariamente factible. En [1], Arreche hace una modificación del algoritmo de Cáceres-Duque de modo que encontrar la base mínima de un ideal de $\mathbb{Z}[x]$ sea ahora un procedimiento factible. Por tanto, podemos decir que existe un procedimiento factible para el problema de pertenencia a ideales de $\mathbb{Z}[x]$.

Referencias

[1] Arreche, C. E., *The Membership Problem for Ideals in* $\mathbb{Z}[x]$, Rose-Hulman Undergraduate Mathematics Journal, **6**(2) (2005).

[2] Aschenbrenner, M., *Ideal Membership in Polynomial Rings over the Integers*, Journal of the American Mathematical Society, **17**(2) (2004), 407–441.

[3] Cáceres-Duque, L. F., *An Effective Procedure for Minimal Bases of Ideals in* $\mathbb{Z}[x]$, Discussiones Mathematicae General Algebra and Applications, **23**(1) (2003), 5–11.

[4] Hermann, G., *Die Frage der endlich vielen Schritte in der Theorie der Polynomideale*, Mathematische Annalen, **95** (1926), 736–788.

[5] Simmons, H., *The Solution of a Decision Problem for Several Classes of Rings*, Pacific Journal of Mathematics, **34**(2) (1970), 547–557.

[6] Szekeres, G., *A Canonical Basis for the Ideals of a Polynomial Domain*, The American Mathematical Monthly, **59**(6) (1952), 379–386.

Luis F. Cáceres Duque (luis.caceres1@upr.edu)

Universidad de Puerto Rico en Mayagüez.

Silvia M. López Gallo (silvia.lopez4@upr.edu)

Universidad de Puerto Rico en Mayagüez.