

ALGORITMO DE DESCARTE DE RAÍCES ENTERAS DE POLINOMIOS.

¿A quién no le ha ocurrido alguna vez, en su periplo como estudiante, encontrarse con un polinomio hostil, que se resiste a mostrar sus raíces enteras, bien porque no las tenga, bien porque el término independiente posee numerosos divisores y en los ensayos rigen las leyes de Murphy?.

Motivados por esta dificultad, desarrollaremos un procedimiento simplificador de la búsqueda de raíces enteras en ecuaciones polinómicas, estableciendo criterios de eliminación entre los candidatos a raíz entera seleccionados mediante el burdo y usual criterio de los divisores del término independiente.

Obviamente, para que el algoritmo de descartar sea interesante en la práctica, debe ser rigurosamente fiable, sencillo y rápido.

Comenzaremos enunciando y probando las propiedades subyacentes al mismo. Por pragmatismo, la sencillez y eficiencia del mismo se hará patente a través de un ejemplo.

Sea

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

un polinomio de coeficientes enteros.

FUNDAMENTACIÓN.

Propiedades de las raíces enteras de un polinomio con coeficientes enteros:

□ Si x_0 es una raíz entera de $p(x)$, $x_0 \neq 0$, entonces x_0 es un divisor de a_0 :

$$\begin{aligned} p(x_0) = a_n x_0^n + a_{n-1} x_0^{n-1} + \dots + a_1 x_0 + a_0 = 0 &\Rightarrow a_0 = -x_0 (a_n x_0^{n-1} + a_{n-1} x_0^{n-2} + \dots + a_1) \Rightarrow \\ &\Rightarrow \frac{a_0}{x_0} = -(a_n x_0^{n-1} + a_{n-1} x_0^{n-2} + \dots + a_1) \in \mathbb{Z}. \end{aligned}$$

□ Si x_0 es una raíz entera de $p(x)$, $x_0 \notin \{-1, 0, 1\}$, entonces $x_0 - 1$ es un divisor de $p(+1)$:

$$\left. \begin{aligned} a_0 = -a_n x_0^n - a_{n-1} x_0^{n-1} - \dots - a_1 x_0 \\ \frac{p(+1)}{x_0 - 1} = \frac{a_n + a_{n-1} + \dots + a_1 + a_0}{x_0 - 1} \end{aligned} \right\} \Rightarrow \frac{p(+1)}{x_0 - 1} = -\frac{a_n (x_0^n - 1) + a_{n-1} (x_0^{n-1} - 1) + \dots + a_1 (x_0 - 1)}{x_0 - 1}.$$

Por el teorema del resto, es inmediato que los binomios $x_0^k - 1$, considerados como polinomios en x_0 , son divisibles por $x_0 - 1$. En efecto, sea $p_k(x_0) = x_0^k - 1$. Entonces, el resto de la división es $p_k(1) = 0$.

Sea

$$q_k(x_0) = \frac{x_0^k - 1}{x_0 - 1}, \quad k = 1, 2, \dots, n.$$

Se tiene:

$$\frac{p(+1)}{x_0 - 1} = -a_n \frac{x_0^n - 1}{x_0 - 1} - a_{n-1} \frac{x_0^{n-1} - 1}{x_0 - 1} - \dots - a_1 \frac{x_0 - 1}{x_0 - 1} = -\sum_{k=1}^n a_k q_k(x_0),$$

y considerando, de nuevo, la indeterminada x_0 como constante entera, resulta que

$$\frac{p(+1)}{x_0 - 1} = -\sum_{k=1}^n a_k q_k(x_0) \in \mathbb{Z} \sim \{-1, 0, 1\}, -$$

es decir, $x_0 - 1$ divide a $p(+1)$.

Observación: Aunque la propiedad se verifica, trivialmente, para $x_0 = 0$, no se considera esta posibilidad por carecer de interés práctico en la aplicación del algoritmo.

□ Si x_0 es una raíz entera de $p(x)$, $x_0 \in \mathbb{Z} \sim \{-1, 0, 1\}$, entonces $x_0 + 1$ es un divisor de $p(-1)$.

La prueba de esta propiedad es análoga a la de la anterior.

IMPLEMENTACIÓN DEL ALGORITMO.

Seleccionados los candidatos iniciales a raíces enteras por el bien conocido criterio de los divisores del término independiente, si éstos son numerosos puede resultar rentable aplicar el algoritmo de descarte a fin de reducir el número de divisiones necesarias para descubrir las raíces enteras.

Este algoritmo, fundamentado en las tres propiedades probadas en el anterior epígrafe, es un “tamiz” mucho más fino, ya que involucra dos nuevos criterios, determinando un “filtrado” mucho más selectivo; con frecuencia, los enteros que lo atraviesan son únicamente las raíces del polinomio.

Optimizaremos el diseño del algoritmo, de forma que resulte minimizado el volumen de cálculos y escritura, y que su ejecución resulte intuitiva y nemotécnica.

Si el término independiente, a_0 , tiene d divisores positivos, mayores que la unidad, a_0 también tiene d divisores negativos menores que la unidad. Para aplicar las dos últimas propiedades, estos $2d$ divisores deben ser incrementados en ± 1 , lo que produce otros $4d$ números a considerar, y el número de divisores sería $6d$. Así pues, la aplicación directa de las propiedades anteriores tendría el siguiente precio: sería necesario efectuar $4d$ pruebas “extra” de divisibilidad, y escribir el triple de divisores de valor absoluto mayor que uno, a cambio de evitar cierto número de divisiones...

A fin de mejorar la implementación del algoritmo, observemos las siguientes propiedades:

Si x_0 es una raíz entera positiva de $p(x)$, entonces:

- $x_0 - 1$ divide a $p(+1)$, y esto implica que $-(x_0 - 1) = -x_0 + 1$ es un divisor de $p(+1)$.
- $x_0 + 1$ divide a $p(-1)$, y esto implica que $-(x_0 + 1) = -x_0 - 1$ es un divisor de $p(-1)$.

Estas propiedades permiten reducir drásticamente el volumen de escritura, sin más que extender las pruebas de divisibilidad de los divisores positivos:

- Si $x_0 - 1$ no divide a $p(+1)$, se descarta como raíz x_0 .
- Si $x_0 + 1$ no divide a $p(+1)$, se descarta como raíz $-x_0$.
- Si $x_0 + 1$ no divide a $p(-1)$, se descarta como raíz x_0 .
- Si $x_0 - 1$ no divide a $p(-1)$, se descarta como raíz $-x_0$.

En forma más compacta:

$$\frac{p(\pm 1)}{x_0 \mp 1} \notin \mathbb{Z} \Rightarrow p(x_0) \neq 0, \quad \frac{p(\pm 1)}{x_0 \pm 1} \notin \mathbb{Z} \Rightarrow p(-x_0) \neq 0$$

Obviamente, a efectos de divisibilidad, se pueden sustituir $p(+1)$ por $|p(+1)|$ y $p(-1)$ por $|p(-1)|$.

Sea

$$\{d_1, d_2, \dots, d_{p-1}, d_p\}$$

el conjunto de los divisores positivos de a_0 , tales que $1 < d_1 < d_2 < \dots < d_{p-1} < d_p$.

Dispongamos éstos, así como $|p(+1)|$ y $|p(-1)|$, en la forma siguiente:

$ p(+1) $						$ p(+1) $
	d_1	d_2	\dots	d_{p-1}	d_p	
$ p(-1) $						$ p(-1) $

Regla de las diagonales.

Para $k = 1, 2, \dots, p$, se prueba si es divisible $p(+1)$ y $p(-1)$ por $d_k \pm 1$. Cuando se prueba la divisibilidad por $d_k - 1$, se opera con $p(+1)$ y $p(-1)$ a la izquierda; cuando se prueba la divisibilidad por $d_k + 1$, se opera con $p(+1)$ y $p(-1)$ a la derecha.

Cada vez que resulte negativa una de estas pruebas de divisibilidad, se traza en la celda que contiene a d_k la diagonal cuya dirección está determinada por la posición relativa de $p(+1)$ y $p(-1)$ respecto de d_k , de acuerdo con el criterio anteriormente definido para el posicionamiento de $p(+1)$ y $p(-1)$.

Se presentan cuatro casos:

- Si $d_k - 1$ no divide a $p(+1)$, se traza la diagonal principal (ascendente hacia la izquierda), puesto que $p(+1)$ se considera a la izquierda y por encima de d_k . Se descarta d_k .
- Si $d_k - 1$ no divide a $p(-1)$, se traza la diagonal secundaria (descendente hacia la izquierda), puesto que $p(-1)$ se considera a la izquierda y por debajo de d_k . Se descarta $-d_k$.
- Si $d_k + 1$ no divide a $p(+1)$, se traza la diagonal secundaria (descendente hacia la izquierda), puesto que $p(+1)$ se considera a la derecha y por encima de d_k . Se descarta $-d_k$.
- Si $d_k + 1$ no divide a $p(-1)$, se traza la diagonal principal (ascendente hacia la izquierda), puesto que $p(-1)$ se considera a la derecha y por debajo de d_k . Se descarta d_k .

Criterio de descarte:

- La diagonal principal descarta el divisor positivo.
- La diagonal secundaria descarta el divisor negativo.

Obviamente, a los divisores descartados ya no es necesario someterlas a prueba alguna.

ALGORITMO.

- ① Se eliminan de $p(x)$ las raíces 0, 1 y -1 , así como el máximo común divisor de los coeficientes. Designaremos por $q(x)$ el polinomio resultante. El algoritmo se aplica a este polinomio reducido.
- ② Los datos necesarios para poder aplicar el algoritmo son los divisores (mayores que la unidad) del término independiente de $q(x)$, así como los valores de $q(+1)$ y $q(-1)$.
 - $q(-1)$ se obtiene durante el ensayo de la raíz -1 , y es el resto de la división de $q(x)$ entre $x + 1$.
 - Si -1 no es raíz de $p(x)$, es decir, si $p(-1) \neq 0$, entonces $q(+1)$ se obtiene durante el ensayo de la raíz $+1$, y es el resto de la división de $q(x)$ entre $x - 1$. En caso contrario, el cálculo de $q(+1)$ se puede efectuar sin necesidad de realizar la división de $q(x)$ entre $x - 1$, ni aplicar el teorema del resto. En efecto, sea $p_1(x)$ el polinomio resultante de eliminar en $p(x)$ las raíces 0 y 1, así como el máximo común divisor de los coeficientes. Si -1 es una raíz de $p_1(x)$ de orden de multiplicidad m se tiene:

$$p_1(x) = (x + 1)^m q(x) \Rightarrow q(x) = \frac{p_1(x)}{(x + 1)^m} \Rightarrow q(+1) = \frac{p_1(+1)}{2^m}.$$

Así pues, mediante esta **fórmula de corrección**, se deduce de forma inmediata el valor de $q(+1)$ a partir de $p_1(+1)$, cuyo valor se obtiene durante el ensayo de la raíz $+1$.

- ③ Se efectúan las pruebas de divisibilidad según el esquema indicado.

Ejemplo. Consideremos el polinomio $p(x) = 2x^8 + 50x^7 + 48x^6 - 2x^5 - 52x^4 - 96x^3 + 2x^2 + 48x$.

Extrayendo el factor común, resulta: $p(x) = 2x(x^7 + 25x^6 + 24x^5 - x^4 - 26x^3 - 48x^2 + x + 24)$

	1	25	24	-1	-26	-48	1	24	
(+1)		1	26	50	49	23	-25	-24	
	1	26	50	49	23	-25	-24	0	
+1		1	27	77	126	149	124		
	1	27	77	126	149	124	100		$p_1(+1) = 100$
	1	26	50	49	23	-25	-24		
(-1)		-1	-25	-25	-24	1	24		
	1	25	25	24	-1	-24	0		
(-1)		-1	-24	-1	-23	24			
	1	24	1	23	-24	0			$q(x) = x^4 + 24x^3 + x^2 + 23x - 24$
-1		-1	-23	22	-45				
	1	23	-22	45	-69				$q(-1) = -69$

Los cálculos realizados hasta aquí son los habituales para la búsqueda de las raíces ± 1 .

El primer resto no nulo obtenido al iterar en el algoritmo de Ruffini para la raíz -1 es $q(-1)$. Si $p(x)$ no tiene la raíz -1 , el valor de $q(+1)$ coincide con el de $p(+1)$; pero en este ejemplo sí existe la raíz -1 , con orden de multiplicidad $= 2$; por tanto, aplicaremos la corrección expuesta anteriormente:

$$q(+1) = \frac{p_1(+1)}{2^m} = \frac{100}{2^2} = 25 \rightarrow q(+1) = 25$$

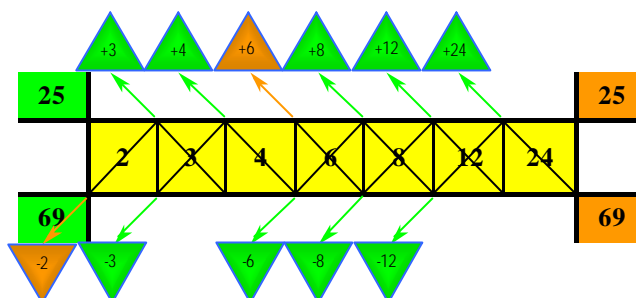
Conocidos $q(+1)$ y $q(-1)$, para poder aplicar el algoritmo de descartar al polinomio $q(x)$ sólo necesitamos determinar el conjunto de los divisores de 24 mayores que 1: $\{2, 3, 4, 6, 8, 12, 24\}$.

25								25
	2	3	4	6	8	12	24	
69								69

Los divisores de 24 disminuidos en una unidad deben dividir a 25 y 69. Esta propiedad, asociada al criterio de las diagonales, permite descartar los siguientes valores:

		+3	+4		+8	+12	+24	
25								25
	2	3	4	6	8	12	24	
69								69
		-3	-4		-8	-12	-24	

Los divisores de **24** aumentados en una unidad deben dividir a **25** y **69**. Esta propiedad, asociada al criterio de las diagonales, permite descartar los siguientes valores:



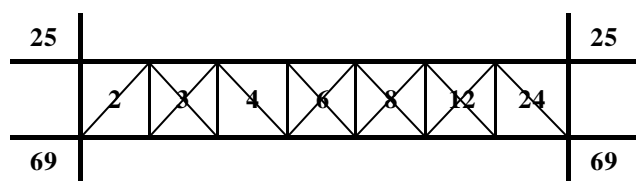
De los 14 candidatos a raíz entera (7 positivos y 7 negativos), con muy poco esfuerzo, han quedado descartados 11. Basta probar ahora por división si $+2$, -4 y -24 son raíces de $q(x)$:

	1	24	1	23	-24
+2		2	52	106	258
	1	26	53	129	234

	1	24	1	23	-24
-4		-4	-80	316	258
	1	20	-79	339	-1380

	1	24	1	23	-24
-24		-24	0	-24	24
	1	0	1	-1	0

La aplicación del algoritmo de descarte ha supuesto en este caso una considerable economía, tanto de cálculo como de volumen de escritura (en la práctica, el procedimiento es muy sencillo, aunque pueda parecer lo contrario en su descripción pormenorizada), ya que se han evitado 11 divisiones por el algoritmo de Ruffini, a cambio del simple esquema



cuya construcción sólo involucra operaciones que se efectúan rápidamente y sin dificultad: restar o sumar la unidad y aplicar criterios de divisibilidad.

Así pues, -24 es la única raíz entera de $q(x)$: $q(x) = x^4 + 24x^3 + x^2 + 23x - 24 = (x + 24)(x^3 + x - 1)$.

Las otras tres raíces de $q(x)$ son la real $\sqrt[3]{\frac{\sqrt{93} + 1}{18} + \frac{1}{2}} - \sqrt[3]{\frac{\sqrt{93} - 1}{18} - \frac{1}{2}}$ y las dos conjugadas complejas

$$\frac{1}{2} \left(\sqrt[3]{\frac{\sqrt{93} - 1}{18} - \frac{1}{2}} - \sqrt[3]{\frac{\sqrt{93} + 1}{18} + \frac{1}{2}} \right) \pm i \left(\frac{1}{2} \left(\sqrt[3]{\frac{\sqrt{31} + 3\sqrt{3}}{2}} + \sqrt[3]{\frac{\sqrt{31} - 3\sqrt{3}}{2}} \right) \right)$$

DETERMINACIÓN DE RAÍCES RACIONALES FRACCIONARIAS.

Afortunadamente, los polinomios con los que se trabaja habitualmente no suelen ser tan hostiles como el $q(x)$ del ejemplo anterior. Sin embargo, las aplicaciones del algoritmo de descartar no se limitan a la búsqueda de raíces enteras. En efecto, puesto que cualquier polinomio puede ser transformado mediante un cambio de variable en otro polinomio cuyas raíces racionales sean todas enteras, el algoritmo de descartar es susceptible de ser aplicado para el descartar de raíces racionales fraccionarias. Además, esta transformada (como veremos en el segundo epígrafe de esta sección), aunque se aplique a polinomios con términos independientes de pocos divisores, suele tener un término independiente con muchos divisores, siendo esta la situación en la que la exclusión rápida de candidatos a raíz racional cobra mayor interés.

Raíces racionales fraccionarias: criterios de existencia.

Sea $p(x)$ una ecuación polinómica de coeficientes enteros y grado n . Si la fracción irreducible $\frac{a}{b}$ es una raíz de $p(x)$, se tiene:

$$p\left(\frac{a}{b}\right) = a_n \left(\frac{a}{b}\right)^n + a_{n-1} \left(\frac{a}{b}\right)^{n-1} + \dots + a_1 \left(\frac{a}{b}\right) + a_0 = 0 \Rightarrow a_n \frac{a^n}{b^n} = -(a_{n-1} a^{n-1} + \dots + a_1 b^{n-1} + a_0 b^{n-1}) \in \mathbb{Z},$$

y siendo b primo relativo con a , también lo será con a^n ; por tanto, b debe dividir al coeficiente a_n .

Por otra parte,

$$\frac{b^n}{a} p\left(\frac{a}{b}\right) = a_n a^{n-1} + a_{n-1} a^{n-2} b + \dots + a_1 b^{n-1} + a_0 \frac{b^n}{a} = 0 \Rightarrow a_0 \frac{b^n}{a} = -(a_n a^{n-1} + a_{n-1} a^{n-2} b + \dots + a_1 b^{n-1}) \in \mathbb{Z},$$

y un razonamiento análogo al anterior, prueba que a , no pudiendo dividir a b^n , ha de dividir a a_0 .

Así pues, podemos enunciar el siguiente **criterio de existencia de raíces racionales fraccionarias**:

“Para que un número fraccionario irreducible pueda ser raíz de una ecuación algebraica de coeficientes enteros, es necesario que el numerador de tal fracción divida al término independiente y el denominador divida al coeficiente del término de mayor grado.”

Transformada de un polinomio genérico a un polinomio cuyas raíces racionales sean enteras.

De acuerdo con el criterio anteriormente establecido, una ecuación algebraica de coeficientes enteros no puede tener raíces racionales fraccionarias si el coeficiente del término de mayor grado es la unidad, es decir, si el polinomio es mónico.

Nos interesa, pues, una transformación que aplicada a un polinomio genérico, lo convierta en otro polinomio de coeficientes enteros, cuyo coeficiente del término de mayor grado sea unitario. Tal transformación es la siguiente:

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \xrightarrow{y=a_n x} q(y) = a_n^{n-1} p\left(\frac{y}{a_n}\right) = y^n + a_{n-1} y^{n-1} + \dots + a_n^{n-2} a_1 x + a_n^{n-1} a_0.$$

Regla para la construcción del transformado mónico y sin raíces racionales fraccionarias.

En la práctica, la transformada de un polinomio $p(x)$ de grado n consiste en sustituirlo por el polinomio mónico $q(y)$, con el mismo coeficiente en el término de grado $n - 1$, y cuyos coeficientes en los términos de grado k , $0 < k < n - 1$, se obtiene multiplicando los correspondientes coeficientes de $p(x)$ por a_n^{n-k-1} , para $k = n - 2, n - 3, \dots, 1, 0$.

Las raíces fraccionarias del polinomio primitivo, $p(x)$, se obtienen dividiendo las raíces enteras del polinomio transformado entre el coeficiente a_n del término de mayor grado de $p(x)$.

Ejemplo.

Consideremos el polinomio

$$p(x) = 3x^5 + x^4 - 2x^3 - 12x + 8.$$

Su transformado mónico y sin raíces racionales fraccionarias es el polinomio $q(x)$, cuya construcción es inmediata aplicando la regla anterior:

$$y = 3x \Rightarrow q(y) = 3^4 p\left(\frac{y}{3}\right) = y^5 + y^4 - 6y^3 - 324y + 648.$$

Aplicando el método tradicional de ir ensayando los divisores de 648 en orden creciente, obtendríamos:

	1	1	-6	0	-324	648
+1		1	2	-4	-4	-328
	1	2	-4	-4	-328	320

	1	1	-6	0	-324	648
-1		-1	0	6	-6	330
	1	0	-6	6	-330	978

	1	1	-6	0	-324	648
+2		2	6	0	0	-648
	1	3	0	0	-324	0

Ciertamente, hemos sido afortunados de hallar una raíz tan pronto, ya que 648 tiene 40 divisores.

Por tanto, $x = \frac{2}{3}$ es una raíz de $p(x)$.

Eliminada la raíz $y = 2$ en $q(y)$, nos queda el polinomio $r(y) = y^4 + 3y^3 - 324$. Si intentásemos buscar una raíz entera en éste, ya no tendríamos tanta suerte, porque sería necesario efectuar ¡28 divisiones! para convencerse de que $r(y)$ no tiene raíces enteras.

Veamos que el algoritmo de descarte sólo filtra un candidato a raíz entera, lo que supone en este caso una economía de 27 divisiones:

- Divisores positivos de 324: {1, 2, 3, 4, 6, 9, 12, 18, 27, 36, 54, 81, 108, 162, 324}.

- Cálculo de $r(+1)$ y $r(-1)$: $r(y) = \frac{q(y)}{x-2} \Rightarrow \begin{cases} r(+1) = \frac{q(+1)}{1-2} = \frac{320}{-1} = -320 \\ r(-1) = \frac{q(-1)}{-1-2} = \frac{978}{-3} = -326 \end{cases}$

- Descarte de divisores:

320																				320	
		2	3	4	6	9	12	18	27	36	54	81	108	162	324						
326																					326

El algoritmo de descartar sólo ha filtrado uno de los 28 divisores: el -3 ; basta, pues, efectuar la división de $r(y)$ entre $x + 3$ para terminar la prueba:

	1	3	0	0	-324
-3		-3	0	0	0
	1	0	0	0	-324

En consecuencia, $p(x)$ sólo tiene una raíz racional: $x = \frac{2}{3}$.

✎

Revista Escolar de la Olimpiada Iberoamericana de Matemática

<http://www.campus-oei.org/oim/revistaoim/>

Edita:

