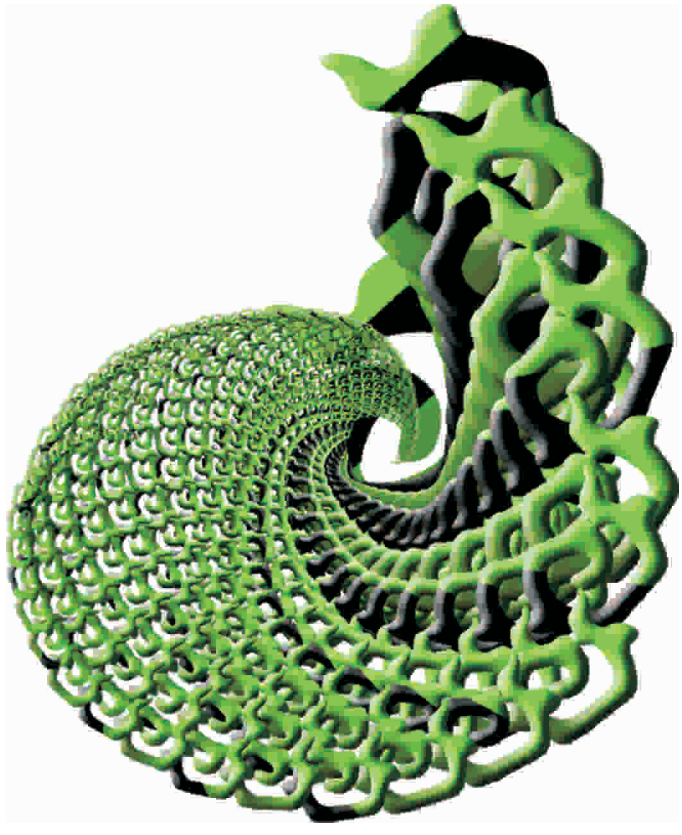
mixba'al

Revista Metropolitana de Matemáticas

2007-7874
ISSN:2007-7874
Versión electrónica



VOL IV, No. 1, JUNIO 2013

Casa abierta al tiempo

Revista del Departamento de Matemáticas de la la

UNIVERSIDAD AUTÓNOMA METROPOLITANA
Unidad Iztapalapa

MIXBA´AL. Vol. IV, No. 1, enero-junio del 2013, es una publicación anual de la Universidad Autónoma Metropolitana a través de la Unidad Iztapalapa, División de Ciencias Básicas e Ingeniería. Departamento deMatemáticas.
Prolongación Canal de Miramontes 3855, Col. Ex Hacienda San Juan de Dios, Delegación Tlalpan, C.P. 14387, México, D. F. y Av. San Rafael Atlixco No. 186, Edificio AT. Tercer piso, Col. Vicentina, Delegación Iztapalapa, C.P. 09340, México, D.F. Tel. 58044658, página electrónica de la revista http://repos.izt.uam.mx, y dirección electrónica: mixbaal2009@gmail.com, mixb@xanum.uam.mx.
Editora Responsable: Laura Hidalgo Solís. Certificado de Reserva de Derechos al Uso Exclusivo de Título No. 04-2010-072017382600-203, ISSN: 2007-7874 ver. Elec., ambos otorgados por el Instituto Nacional del Derecho de Autor. Responsable de la última actualización de este número, Unidad Iztapalapa, División de Ciencias Básicas e Ingeniería, Departamento de Matemáticas, Mat. Daniel Espinosa Pérez.
Fecha de última modificación: 3 de julio de 2013. Tamaño de archivo: 4.8 MB.

Contacto.
Departamento de Matemáticas,
Universidad Autónoma Metropolitana, Iztapalapa
Tel: (01) 55 5804 4600 Ext. 3322.
Fax: (01) 55 5804 4660.
e-mail: mixbaal2009@gmail.com.
e-mail: mixb@xanum.uam.mx.
Web Revista: http://repos.izt.uam.mx/

Emblema de la UAM.
El emblema institucional fue desarrollado por el destacado arquitecto mexicano Pedro Ramírez Vázquez, quien fuera inclusive el primer Rector General de la UAM, en 1974. El arquitecto Ramírez Vázquez diseñó y reglamentó el emblema que, junto con el lema "Casa abierta al tiempo", realizado por el doctor Miguel León-Portilla, conforma el logotipo de la Universidad Autónoma Metropolitana; símbolo de identidad y orgullo de la comunidad universitaria.
La representación gráfica del emblema institucional retoma la figura que identifica a una pirámide, por ser ésta la construcción tradicional y de identidad de las culturas autóctonas.

Una Universidad asentada en la tradición

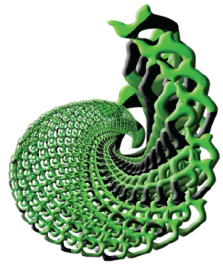
Abierta

Interdisciplinaria y Autónoma

Flexible

Casa abierta al tiempo

Mixba'al
Revista Metropolitana de Matemáticas



In Memoriam

Ernesto Lacomba Zamora

(1945-2012)

Casa abierta al tiempo

A los autores

Mixba'al es una publicación del Departamento de Matemáticas de la Universidad Autónoma Metropolitana, Unidad Iztapalapa. Está dirigida a la comunidad matemática latinoamericana, formada tanto por estudiantes como por profesores.

Los artículos pueden ser artículos de investigación o trabajos que presenten de manera original algún tema de las matemáticas; por ejemplo, demostraciones nuevas de resultados conocidos, artículos panorámicos sobre un área de investigación, la presentación de una visión distinta de algún tema vinculado con la docencia, notas de cursos avanzados, aplicaciones de las matemáticas, historia y filosofía de las matemáticas y aspectos lúdicos de las mismas, entre otros.

La revista Mixba'al está a cargo de un comité editorial. Los trabajos deben ser presentados en español, en casos excepcionales podrán aceptarse artículos en inglés. Todos los trabajos serán sometidos a arbitraje. El comité editorial decidirá sobre la aceptación de los artículos sometidos. Los artículos de investigación podrán ser panorámicos o ser parte de memorias de congresos, simposios, coloquios, talleres u otros.

Cada volumen está a cargo del comité editorial de la revista. Dicho comité tiene la responsabilidad de garantizar su calidad, así como de su presentación de acuerdo con los lineamientos de formato y tipografía de la revista y de la corrección del lenguaje (ortografía, estilo, etcétera).

La versión preliminar de los trabajos sometidos a la revista deberá enviarse en formato pdf. Puesto que la presentación final de los trabajos se hará en Latex2ε, aquellos autores, cuyos trabajos sean aceptados, deberán enviarlos con el formato y macros que proporcionará la revista para su publicación final. Las fotografías o gráficas que acompañen al texto deberán ser enviadas, por separado, en formato pdf y deberán tener la calidad y resolución suficientes para una buena reproducción impresa, y deberán contar con los correspondientes derechos de autor. Se recomienda que la extensión de los trabajos no exceda de 20 páginas.

Laura Hidalgo Solís
Coordinadora

Presentación

Mixba'al es una revista de divulgación en matemáticas en el sentido más amplio, concebida con el propósito de apoyar la comunicación entre la comunidad matemática de habla hispana. Entre los artículos de este número, encontrarán tanto trabajos de investigación original como exposición de resultados importantes conocidos en varias ramas de la matemática básica y aplicada. La intención es continuar con este formato y la revista invita a someter contribuciones de esta índole en el idioma español. Inicialmente se publicará al menos un número al año.

Toda comunicación debe ser dirigida al Comité Editorial, al correo electrónico: `mixbaal2009@gmail.com`

...Antes del inicio de su labor, la investigación en Mecánica Celeste en la UAM era prácticamente inexistente. Los congresos internacionales HAMSYS son un reflejo de que el grupo formado por Ernesto Lacomba cuenta, y de forma destacada, a nivel internacional.

Creo que cualquier universidad debe estar muy satisfecha de tener entre su personal profesores capaces de tener un excelente nivel en investigación y de formar grupos de excelencia.

Carles Simó
Catedrático de Matemática Aplicada
Universitat de Barcelona

Mixba'al
Revista Metropolitana de Matemáticas
No. 1, Vol. IV, junio de 2013, 7–11

UNA NOTA SOBRE LA CONJETURA DE SUMNER

NAHID YELENE JAVIER NOL JOAQUÍN TEY CARRERA

Resumen. En 1971 Sumner conjeturó que todo árbol dirigido de orden n es $(2n-2)$-inevitable. Desde entonces, a pesar de los esfuerzos realizados, esta conjetura sólo ha sido demostrada parcialmente. En este trabajo generalizamos la familia de árboles dirigidos $(2n-2)$-inevitables de orden n propuesta por El Sahili en 2004.

1. Introducción

Los torneos son estructuras combinatorias muy ricas que han sido extensamente estudiadas en teoría de gráficas. Se han hecho muchas preguntas acerca de sus subdigráficas y en particular cuándo estas son árboles (ver [1], [2], [3], [4] y [5]). En este sentido, en 1971 Sumner conjeturó que todo árbol dirigido de orden $n \geq 2$ es $(2n-2)$-inevitable.

En 2004 El Sahili [4] demostró que todo árbol enraizado de orden n cuyas componentes hacia atrás son trayectorias es $(2n-2)$-encajable. El propósito de esta nota es mostrar que este resultado puede ser generalizado, siguiendo las ideas desarrolladas en [4].

Hemos omitido las definiciones básicas que pueden encontrarse en cualquier texto de teoría de gráficas (ver [6] por ejemplo).

Sean $A = (V', E')$ y $D = (V, E)$ digráficas.

- Un *encaje* de A en D es una inyección $f : V' \to V$ tal que $(f(v_i), f(v_j)) \in E$ para todo $(v_i, v_j) \in E'$.
- A es *m-inevitable* si existe un encaje de A en T para todo torneo T de orden m.
- Un *orden promedio* de D es un orden lineal $(v_1, v_2, ..., v_n)$ de V que maximiza $|\{(v_i, v_j) \in E : i < j\}|$.
- Sea $M = (v_1, v_2, ..., v_n)$ un orden promedio de D. Un *M-encaje* de A en D es un encaje f de A en D tal que para toda *sección final* $I = [v_{i+1}, v_n]$ de M se tiene que
$$|f(A) \cap I| < \frac{|I|}{2} + 1.$$
- A es *m-encajable* si A tiene un M-encaje en T para todo torneo T de orden m y todo orden promedio M de T.
- Un vértice de una digráfica es una *hoja* si la suma de su ingrado y exgrado es uno.
- Un *árbol enraizado* es un árbol dirigido con un vértice distinguido al que se le denomina *raíz*.
- Una *inarborescencia (exarborescencia)* es un árbol enraizado donde todo vértice tiene exgrado (ingrado) uno, excepto la raíz que tiene exgrado (ingrado) cero.
- Una *garra* es una inarborescencia donde sólo la raíz puede tener ingrado mayor que 1. El *grado de una garra* es el ingrado de su raíz.

2010 *Mathematics Subject Classification.* 05C20, 05C05.
Palabras clave. árbol, árbol encajable, árbol inevitable, orden promedio, torneo.

Claramente, todo árbol dirigido m-encajable es m-inevitable pero el recíproco no es cierto. Para ver esto, en la Sección 3 mostramos un ejemplo de un árbol de orden 4 que es 6-inevitable pero no 6-encajable.

2. Una familia de árboles $(2n-2)$-encajables

Para construir la familia de árboles $(2n-2)$-encajables, necesitamos dos resultados demostrados en [4].

Proposición 1. *Sea T un torneo de orden $n \geq 3$ y $M = (v_1, v_2, ..., v_n)$ un orden promedio de T. Definamos $T' = T[\{v_1, v_2, ..., v_{n-2}\}]$ y $M' = (v_1, v_2, ..., v_{n-2})$. Sea D una digráfica y x una hoja de exgrado cero en D. Supongamos que $D' = D - x$ tiene un M'-encaje f' en T'. Entonces D tiene un M-encaje f en T que extiende a f'.*

Corolario 2. *Toda exarborescencia de orden $n \geq 2$ es $(2n-2)$-encajable.*

Sea A un árbol enraizado, si la raíz tiene ingrado cero diremos que es una *fuente* y que A es un árbol *bien enraizado*. El *nivel* de un vértice v de A es la distancia de v a la raíz de A, sin tener en cuenta las orientaciones de las flechas en A. Una flecha (x, y) es una *flecha hacia adelante* si el nivel de y es mayor que el de x, en caso contrario diremos que es una *flecha hacia atrás*. A una componente conexa de la subdigráfica inducida por las flechas hacia atrás de A la llamaremos *componente hacia atrás de A*.

Denotaremos por $\mathcal{F}$ al conjunto de inarborescencias m-inevitables de orden $m \geq 2$. Por ejemplo, una garra de grado no mayor que $\frac{3}{8}m$ pertenece a $\mathcal{F}$ (ver [5]). Observe que una trayectoria puede interpretarse como una garra de grado uno.

Ahora veremos cómo generalizar los argumentos utilizados en [4] para obtener una familia más amplia de árboles $(2n-2)$-encajables.

Proposición 3. *Todo árbol bien enraizado de orden $n \geq 2$ cuyas componentes hacia atrás están en $\mathcal{F}$ es $(2n-2)$-encajable.*

Demostración. Por inducción sobre $c(A)$, el número de componentes hacia atrás del árbol A. Si $c(A) = 0$, entonces A es una exarborescencia y por el Corolario 2 es $(2n-2)$-encajable. Sea A un árbol bien enraizado de orden $n \geq 2$ con raíz r, $c(A) \geq 1$, T un torneo de orden $2n-2$ sobre el conjunto de vértices $\{v_1, v_2, ..., v_{2n-2}\}$ y $M = (v_1, v_2, ..., v_{2n-2})$ un orden promedio de T. Veamos que A tiene un M-encaje en T. Consideraremos dos casos.

Caso 1. Toda hoja de A tiene exgrado uno.

Sea B' una componente hacia atrás de A, con al menos una hoja de A. Denotemos a la raíz de B' por y. Como r es fuente de A se tiene que $y \neq r$. Supongamos que B' tiene m vértices, entonces $A' = A - B'$ es un árbol bien enraizado (con raíz r) de orden $n-m$ y con $c(A') = c(A) - 1$ componentes hacia atrás. Sean $T' = T\left[\left\{v_1, v_2, ..., v_{2(n-m)-2}\right\}\right]$ y $M' = \left(v_1, v_2, ..., v_{2(n-m)-2}\right)$, note que M' es un orden promedio de T'. Por hipótesis de inducción, A' tiene un M'-encaje f' en T'.

Sea $x \notin B$ tal que (x, y) es una flecha de A, claramente la flecha (x, y) es hacia adelante. Sea S un conjunto de m nuevos vértices y denotemos por A'' el árbol que se obtiene de A' adhiriendo los vértices de S al vértice x con flechas que inician en x. Aplicando la Proposición 1 m veces, A'' tiene un M-encaje f'' en T que extiende a f'. Por otra parte, $B' \in \mathcal{F}$ es decir B' está contenida en todo torneo de orden m. Luego, el subtorneo de T inducido por $f''(S)$ tiene una copia B'' de la inarborescencia B'.

Sea $g : V(B') \to V(B'')$ un isomorfismo de B' en B'' y $f : A \to T$ definida como

$$f(v) = \begin{cases} f'(v) & \text{si} \quad v \in V(A') \\ g(v) & \text{si} \quad v \in V(B') \end{cases}$$

Sin lugar a dudas, f es un encaje de A en T pero necesitamos probar que es también un M-encaje. Sea $I = [v_{i+1}, v_{2n-2}]$ una sección final de M.

Caso 1.1. $i + 1 \leq 2(n-m) - 2$.

Sea $I = I_1 \cup I_2$ donde

$$I_1 = \left[v_{i+1}, ..., v_{2(n-m)-2}\right]$$

e

$$I_2 = \left[v_{2(n-m)-2+1}, ..., v_{2n-2}\right].$$

Entonces

$$|f(A) \cap I| \quad = \quad |f'(A') \cap I_1| + |g(B') \cap I_2|.$$

Como f' es un M'-encaje de A' en T', tenemos que $|f'(A') \cap I_1| < \dfrac{|I_1|}{2} + 1$. Además $|g(B') \cap I_2| = |g(B')| = m = \dfrac{|I_2|}{2}$. Luego

$$|f(A) \cap I| < \frac{|I_1|}{2} + 1 + \frac{|I_2|}{2} = \frac{|I|}{2} + 1.$$

Caso 1.2. $i + 1 > 2(n-m) - 2$.

Considerando que

$$f(A) \cap I = g(B') \cap I \quad \text{y} \quad g(B') \subseteq f''(S),$$

se tiene que

$$f(A) \cap I \subseteq f''(S) \cap I.$$

Como f'' es un M-encaje de A'' en T, se concluye que $|f(A) \cap I| < \dfrac{|I|}{2} + 1$. Por lo tanto f es un M-encaje de A en T.

Caso 2. A tiene al menos una hoja de exgrado cero.

En tal caso, eliminaremos una a una las hojas de exgrado cero (inclusive las nuevas hojas que aparezcan durante este proceso) hasta que el árbol que resulte A' deje de tenerlas. Supongamos que en este proceso fueron eliminados k vértices. Sean $T' = T\left[\left\{v_1, v_2, ..., v_{2(n-k)-2}\right\}\right]$ y $M' = \left(v_1, v_2, ..., v_{2(n-k)-2}\right)$. Observe que A' satisface la condición del Caso 1, luego es posible encontrar un M'-encaje f' de A' en T'. Finalmente, aplicando k veces la Proposición 1, se puede construir un M-encaje de A en T que extiende a f'. □

Corolario 4 (El Sahili, [4]). *Todo árbol enraizado de orden $n \geq 2$ cuyas componentes hacia atrás son trayectorias es $(2n-2)$-encajable.*

Demostración. Sea A un árbol enraizado de orden $n \geq 2$ cuyas componentes hacia atrás son trayectorias. No es difícil comprobar que si la raíz de A no es fuente, es posible sustituirla por otro vértice de tal manera que el árbol que resulta A' es bien enraizado y donde todas sus componentes hacia atrás siguen siendo trayectorias. Como toda trayectoria está en $\mathcal{F}$, por la Proposición 3 A' es $(2n-2)$-encajable. □

3. Un árbol 6-inevitable que no es 6-encajable

En esta sección hacemos notar el hecho esperado de que m-inevitabilidad no implica m-encajabilidad. Daremos un ejemplo de un árbol de orden 4 que es 6-inevitable pero no 6-encajable.

Considere el árbol A de orden 4 en la Figura 1. Como todo torneo de orden 6 tiene un vértice de ingrado al menos tres, se tiene que A es 6-inevitable.

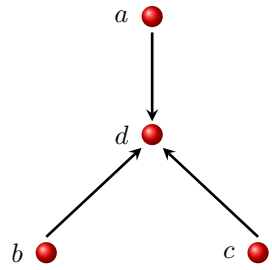


Figura 1. árbol A

Considere el torneo T_0 de orden 6 en la Figura 2. Se puede comprobar que $M_0 = (1, 2, 4, 3, 5, 6)$ es un orden promedio de T_0 (ver Figura 3).

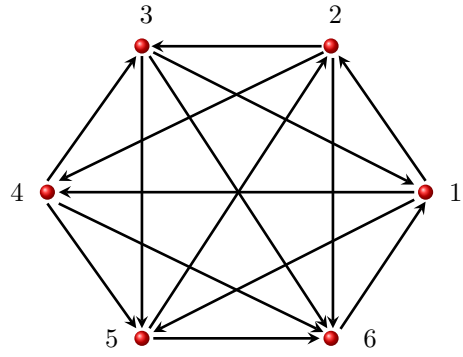


Figura 2. Torneo T_0

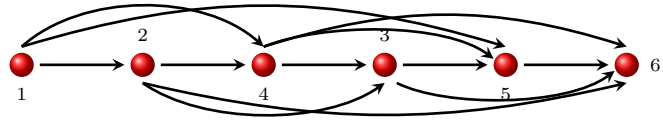


Figura 3. Orden promedio M_0

Recuerde que A es 6-encajable si A tiene un M-encaje en T, para todo torneo T de orden 6 y para todo orden promedio M de T. Para nuestro propósito, basta considerar los cinco encajes siguientes de A en T_0.

A	$f_1(A)$	$f_2(A)$	$f_3(A)$	$f_4(A)$	$f_5(A)$
a	1	2	2	2	3
b	3	3	3	4	4
c	4	4	5	5	5
d	5	6	6	6	6

Claramente para cada f_i y la sección final $I = [4, 6]$, la desigualdad

$$|f_i(A) \cap I| < \frac{|I|}{2} + 1$$

no se cumple por lo tanto A no es M_0-encajable en T_0.

Referencias

[1] B. Grünbaum, *Antidirected Hamiltonian Paths in Tournaments*, J. Combinatorial Theory Ser. B 11 (1971) 249-257.

[2] F. Havet y S. Thomassé, *Median orders of tournaments: a tool for the second neighborhood problem and Sumner's conjecture*, J. Graph Theory 35 (2000) 244-256.

[3] F. Havet, *Trees in tournament*, Discrete Math. 243 (1-3) (2002) 121-134.

[4] A. El Sahili, *Trees in tournaments*, J. Combinatorial Theory Ser. B 92 (2004) 183-187.

[5] X. Lu, *Claws contained in all n-tournaments*, Discrete Math. 119 (1993) 107-111.

[6] D. West, *Introduction to Graph Theory*, Prentice Hall (1996).

Dirección de los autores:

Nahid Yelene Javier Nol
Universidad Autónoma Metropolitana,
Unidad Iztapalapa,
División de Ciencias Básicas e Ingeniería,
Departamento de Matemáticas.
Av. San Rafael Atlixco 186, Col. Vicentina
Del. Iztapalapa, C.P. 09340 México, D.F.
e-mail: nahid@xanum.uam.mx

Joaquín Tey Carrera
Universidad Autónoma Metropolitana,
Unidad Iztapalapa,
División de Ciencias Básicas e Ingeniería,
Departamento de Matemáticas.
Av. San Rafael Atlixco 186, Col. Vicentina
Del. Iztapalapa, C.P. 09340 México, D.F.
e-mail: jtey@xanum.uam.mx

Mixba'al
Revista Metropolitana de Matemáticas
No. 1, Vol. IV, junio de 2013, 13–27

CAMPOS CUADRÁTICOS REALES CON NÚMERO DE CLASE PAR

JANETH A. MAGAÑA-ZAPATA MARIO PINEDA-RUELAS

Resumen. En la clase de un ideal de un anillo de enteros A_F de una extensión cuadrática $\mathbb{Q}(\sqrt{d})$ de $\mathbb{Q}$ mostramos que existe al menos un ideal primitivo y uno reducido. Involucrando las fracciones continuas con los ideales de A_F, para cierta clase de enteros d aseguramos la existencia de un divisor del número de clase de $\mathbb{Q}(\sqrt{d})$. Como una aplicación obtenemos una familia infinita de campos cuadráticos con número de clase par.

1. Introducción

Una célebre conjetura de Gauss afirma que existe una infinidad de campos cuadráticos reales cuyo anillo de enteros es de ideales principales. Sólo se conocen resultados parciales. Por ejemplo, Biró [1], [2] determinó todos los campos cuadráticos reales de la forma $\mathbb{Q}(\sqrt{n^2+1})$ y $\mathbb{Q}(\sqrt{n^2+4})$ con número de clase 1. También, Byeon, Kim y Lee [3] determinaron todos los campos cuadráticos reales de la forma $\mathbb{Q}(\sqrt{n^2-4})$ con número de clase 1, sólo por mencionar algunos de ellos.

El objetivo de este artículo consiste en estudiar la ecuación diofantina

$$d = \sigma^2 a^m + b^2$$

por medio de la teoría de los números algebraicos y la teoría de las fracciones continuas. Mostraremos que, bajo ciertas suposiciones sobre el entero d, el campo cuadrático real $\mathbb{Q}(\sqrt{\sigma^2 a^m + b^2})$ tiene número de clase par.

2. Preliminares

Un subcampo F de los números complejos lo llamaremos *campo de números* si $[F:\mathbb{Q}] < \infty$. Si Ω es el anillo de enteros algebraicos, entonces el conjunto $A_F = F \cap \Omega$ es un anillo el cual llamaremos *el anillo de enteros de* F. Las extensiones que estudiaremos en este trabajo son de la forma $F = \mathbb{Q}(\sqrt{d})$ con $d > 0$ libre de cuadrados. Si $d \equiv 2, 3 \pmod 4$, entonces una base entera de F es $\{1, \sqrt{d}\}$ y el discrimante tiene la forma $\delta_F = 4d$. En el caso $d \equiv 1 \pmod 4$ una base entera es $\left\{1, \dfrac{1+\sqrt{d}}{2}\right\}$ y $\delta_F = d$.

En la familia de ideales $\neq 0$ de A_F definimos la relación: $I \sim J$ si y sólo si existen $\alpha, \beta \in A_F \setminus \{0\}$ tales que $\langle\alpha\rangle I = \langle\beta\rangle J$, donde $\langle\alpha\rangle, \langle\beta\rangle$ representa el ideal principal generado por α y β respectivamente. La relación $\sim$ es de equivalencia. Denotamos por $\mathcal{C}_F = \{\overline{I} : I \text{ es ideal } \neq 0 \text{ de } A_F\}$. Se sabe que $\mathcal{C}_F$ es finito y la operación en $\mathcal{C}_F$ definida por $\overline{I}\,\overline{J} = \overline{IJ}$, impone en $\mathcal{C}_F$ una estructura de grupo abeliano, en donde el neutro es precisamente la clase $\overline{\langle 1\rangle} = \overline{A}_F$ que representa a la familia de ideales principales de A_F. El grupo C_F es conocido como el grupo de clases de ideales del campo F y el orden del grupo $\mathcal{C}_F$, que se denota como h_F, es conocido como el número de clase del campo F. Un resultado conocido en teoría de números algebraicos asegura que la factorización de elementos de A_F en irreducibles es única si y sólo si $\mathcal{C}_F$ es el grupo

2010 *Mathematics Subject Classification.* 11A55, 11R29,11R11.
Palabras clave. anillos de enteros, campos de números cuadráticos, grupo de clases de ideales, número de clases.

trivial, i.e., si y sólo si $h_F = 1$ (Theorem 5.2.1, [11]). Equivalentemente, $h_F > 1$ si y sólo si el anillo A_F no es de factorización única. Justamente el interés de éste trabajo es que, con la ayuda de una ecuación diofantina, construiremos una familia infinita de campos cuadráticos reales tales que el orden del grupo C_F es par. No se sabe si cualquier grupo de clases de ideales con número de clase par se obtiene de esta forma.

3. Fracciones continuas simples

Si $d = \dfrac{a}{b} \in \mathbb{Q}$, entonces calculando el $mcd(a, b)$ a través del algoritmo de Euclides, se puede mostrar fácilmente que:

$$\frac{a}{b} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{\ddots\, q_{k-1} + \cfrac{1}{q_k}}}}}$$

donde $q_0 \in \mathbb{Z}$ y $q_i \in \mathbb{N}$ para $i \geq 1$. Este es un ejemplo de fracción continua finita, de hecho $d \in \mathbb{Q}$ si y sólo si la fracción continua de d es finita. El caso que nos interesa ahora es cuando $d \in \mathbb{R} \setminus \mathbb{Q}$. Las fracciones continuas de números irracionales son las conocidas como fracciones continuas simples y tienen la forma

$$q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{\ddots}}}}$$

donde $q_0 \in \mathbb{Z}$ y $q_i \in \mathbb{N}$ para $i \geq 1$. Denotaremos por $[q_0; q_1, \ldots, q_n, \ldots]$ a la fracción continua simple. Si cortamos en la $(n+1)$-ésima entrada, entonces el número racional

$$[q_0; q_1, \ldots, q_n] = \frac{A_n}{B_n},$$

llamado el n-ésimo convergente, satisface las siguientes relaciones recursivas:

Teorema 1. *Sea $[q_0; q_1, \ldots, q_n]$ el n-ésimo convergente de la fracción continua $[q_0; q_1, \ldots, q_n, \ldots]$. Para $n \in \mathbb{Z}, n \geq -2$ definimos*

$$A_{-2} = 0, \quad A_{-1} = 1, \quad A_n = q_n A_{n-1} + A_{n-2}$$

y

$$B_{-2} = 1, \quad B_{-1} = 0, \quad B_n = q_n B_{n-1} + B_{n-2}.$$

Entonces

$$[q_0; q_1, \ldots, q_n] = \frac{A_n}{B_n} = \frac{q_n A_{n-1} + A_{n-2}}{q_n B_{n-1} + B_{n-2}}.$$

Demostración. La prueba es por inducción sobre n y usando

$$[q_0; q_1, \ldots, q_n, q_{n+1}] = \left[q_0; q_1, \ldots, q_{n-1}, q_n + \frac{1}{q_{n+1}}\right].$$

□

Corolario 2. *Si $\alpha = [q_0; q_1, \ldots, q_n, q_{n+1}, \ldots]$ y $x = [q_{n+1}; q_{n+2}, \ldots]$, entonces*

$$\alpha = \frac{xA_n + A_{n-1}}{xB_n + B_{n-1}}.$$

Demostración. Del Teorema 1, obtenemos el resultado puesto que:

$$\alpha = [q_0; q_1, \ldots, q_n, x] = \frac{A_{n+1}}{B_{n+1}} = \frac{xA_n + A_{n-1}}{xB_n + B_{n-1}}.$$

□

Observamos que:

1. Si $n = -1$, entonces $A_{-1}B_{-2} - A_{-2}B_{-1} = 1$.
2. Si $n = 0$, entonces $A_0B_{-1} - A_{-1}B_0 = -1$ y $A_0B_{-2} - A_{-2}B_0 = q_0$.

En general tenemos:

TEOREMA 3. *Para $n \geq 1$, A_n y B_n satisfacen las siguientes propiedades:*

1. $A_nB_{n-1} - A_{n-1}B_n = (-1)^{n-1}$.
2. $\dfrac{A_n}{B_n} - \dfrac{A_{n-1}}{B_{n-1}} = \dfrac{(-1)^{n-1}}{B_nB_{n-1}}$.
3. $A_nB_{n-2} - A_{n-2}B_n = q_n(-1)^n$.
4. $\dfrac{A_n}{B_n} - \dfrac{A_{n-2}}{B_{n-2}} = \dfrac{(-1)^n q_n}{B_nB_{n-2}}$, *para $n \geq 2$.*

Demostración. La prueba es fácil. Ver por ejemplo el Teorema 2.1.10 de [7], o el Teorema 5.1.2 de [9]. □

Si $C_n = \dfrac{A_n}{B_n}$ denota el n-ésimo convergente de la fracción $[q_0; q_1, \ldots, q_n, \ldots]$, entonces la afirmación 2 del Teorema 3 la podemos escribir como:

$$C_{2m-1} - C_{2m-2} = \frac{(-1)^{2m-2}}{B_{2m-1}B_{2m-2}} > 0.$$

Así las cosas, cualquier convergente impar es mayor que cualquier convergente par.

COROLARIO 4. *Las sucesiones $\{C_{2n}\}$ y $\{C_{2n+1}\}$ convergen.*

Demostración. Esto es consecuencia de que $\{C_{2n}\}$ está acotada superiormente por cualquier convergente impar. Análogamente, la sucesión $\{C_{2n+1}\}$ está acotada inferiormente por cualquier convergente par. □

Como consecuencia de la afirmación 2 del Teorema 3 tenemos:

$$|C_{n+1} - C_n| = \left|\frac{A_{n+1}}{B_{n+1}} - \frac{A_n}{B_n}\right| = \frac{1}{B_{n+1}B_n} < \frac{1}{(n+1)n}.$$

Por lo tanto $\lim_{n\to\infty} C_{2n} = \lim_{n\to\infty} C_{2n+1} = \lim_{n\to\infty} C_n$.

TEOREMA 5. *Cualquier fracción continua simple infinita $[q_0; q_1, \ldots, q_n, \ldots]$ es un número irracional.*

Demostración. Ver [7] Teorema 2.1.15. □

El siguiente resultado es el recíproco del Teorema 5 y describe un algoritmo para calcular la fracción continua simple infinita que representa a un número irracional.

TEOREMA 6. *(**Algoritmo de las fracciones continuas**) Si $\alpha \notin \mathbb{Q}$, entonces α está representada por una fracción continua simple infinita.*

Demostración. Sea $q_0 = \lfloor \alpha \rfloor$, donde $\lfloor \alpha \rfloor$ denota el mayor entero $\leq \alpha$. Como $\alpha \neq \lfloor \alpha \rfloor$, existe un único $\alpha_1 \in \mathbb{R}^+$ tal que

$$\alpha = q_0 + \frac{1}{\alpha_1}.$$

Nótese que $0 < \dfrac{1}{\alpha_1} < 1$. Sea $q_1 = \lfloor \alpha_1 \rfloor$; es claro que $q_1 \neq \alpha_1$ ya que de lo contrario $\alpha \in \mathbb{Q}$. Entonces $\alpha_1 = q_1 + \dfrac{1}{\alpha_2}$, para algún $\alpha_2 > 1$. Hasta aquí se tiene

$$\alpha = q_0 + \frac{1}{\alpha_1} = q_0 + \frac{1}{q_1 + \dfrac{1}{\alpha_2}}.$$

Este proceso es infinito, pues si para alguna i, $q_i = \alpha_i$, entonces α sería un número racional. Sólo falta probar que este proceso infinito produce la fracción continua simple $[q_0; q_1, \ldots, q_n, \ldots]$ que converge a α. Claramente $\alpha = [q_0; q_1, \ldots, q_n, \alpha_{n+1}]$. Puesto que $q_{n+1} = \lfloor \alpha_{n+1} \rfloor < \alpha_{n+1}$, entonces $\alpha > [q_0; q_1, \ldots, q_n, q_{n+1}]$ para cualquier n impar, y $\alpha < [q_0; q_1, \ldots, q_n, q_{n+1}]$ para n par. Si C_i son los i-ésimos convergentes, entonces:

$$C_0 < C_2 < \cdots < C_{2n} < \cdots < \alpha < \cdots < C_{2n-1} < \cdots < C_3 < C_1,$$

lo cual obviamente implica que $\alpha = [q_0; q_1, \ldots, q_n, \ldots]$. □

3.1. **Irracionales Cuadráticos y Fracciones Continuas Periódicas.** Aplicando el Teorema 6 a los números irracionales $\sqrt{7}$ y π, se puede verificar fácilmente que:

$$\sqrt{7} = [2; 1, 1, 1, 4, 1, 1, 1, 4, 1, 1, 1, 4, \ldots]$$

$$\pi = [3; 7, 15, 1, 192, 1, 1, 1, 2, 1, 3, \ldots]$$

Observamos que en la fracción continua de $\sqrt{7}$ se repite el bloque $1, 1, 1, 4$ y en la fracción continua de π no se puede observar el mismo fenómeno. Estudiaremos una clase de números irracionales en cuya representación en fracción continua simple se repite algún bloque de números.

Definición 7. Si $\alpha = [q_0; q_1, \ldots, q_n, \ldots]$ es una fracción continua simple infinita, diremos que es periódica si existen $k \geq 0$ y $l \in \mathbb{N}$ tales que $q_n = q_{n+l}$ para todo $n > k$. Al menor entero l que satisface la condición anterior lo llamaremos la longitud del período de α y lo denotaremos como $l = l(\alpha)$.

La notación que usaremos es la siguiente:

$$\alpha = [q_0; q_1, \ldots, q_k, \overline{q_{k+1}, \ldots, q_{k+l}}].$$

Observemos que si $\alpha = [\overline{q_0; q_1, \ldots, q_n}]$, entonces α es raíz de algún polinomio cuadrático en $\mathbb{Z}[x]$. Esto es así porque si escribimos $\alpha = [q_0; q_1, \ldots, q_n, \alpha]$, entonces tenemos que

$$\alpha = \frac{\alpha A_n + A_{n-1}}{\alpha B_n + B_{n-1}},$$

y por lo tanto $\alpha^2 B_n + \alpha(B_{n-1} - A_n) - A_{n-1} = 0$.

Definición 8. Un irracional cuadrático α es un número irracional que es raíz de algún polinomio cuadrático con coeficientes en $\mathbb{Q}$.

Teorema 9. *(Lagrange) Un número real α es un irracional cuadrático si y sólo si la fracción continua simple que representa a α es periódica.*

Demostración. Ver el Teorema 5.3.1 de [9] página 240. □

En seguida veremos cómo expresar un irracional cuadrático α involucrando los coeficientes del polinomio del cual α es raíz.

Supongamos que α es un irracional cuadrático, es decir, $a\alpha^2 + b\alpha + c = 0$, para ciertos $a, b, c \in \mathbb{Z}$ $(a \neq 0)$. Entonces

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

Así que podemos escribir

$$\alpha = \frac{A \pm \sqrt{B}}{C} = \frac{AC \pm \sqrt{BC^2}}{C^2} = \frac{P \pm \sqrt{d}}{Q},$$

donde $P = AC$, $d = BC^2$ y $Q = C^2$. Entonces un irracional cuadrático α se puede escribir en la forma

$$\alpha = \frac{P + \sqrt{d}}{Q}, \tag{1}$$

para ciertos $P, Q \in \mathbb{Z}$ $(Q \neq 0)$ y tal que $d > 1$ no es un cuadrado perfecto. La otra raíz de $ax^2 + bx + c$ es $\dfrac{P - \sqrt{d}}{Q}$.

Definición 10. Si $\alpha = A + B\sqrt{d}$ con $A, B \in \mathbb{Q}$, definimos el conjugado de α como $\alpha' = A - B\sqrt{d}$.

El siguiente resultado describe un algoritmo para encontrar la representación en fracción continua simple de un irracional cuadrático α.

LEMA 11. *Sean $d > 1$ un entero que no es un cuadrado perfecto y*

$$\alpha = \alpha_0 = \frac{P_0 + \sqrt{d}}{Q_0}$$

un irracional cuadrático, donde $P_0 = P$, $Q_0 = Q$ como en (1)*. Definimos lo siguiente para $k \geq 0$*

$$\alpha_k = \frac{P_k + \sqrt{d}}{Q_k}, \quad q_k = \lfloor \alpha_k \rfloor$$

$$P_{k+1} = q_k Q_k - P_k \quad y \quad Q_{k+1} = \frac{d - P_{k+1}^2}{Q_k}.$$

Entonces $P_k, Q_k \in \mathbb{Z}, Q_k | P_k^2 - d$, $Q_k \neq 0$ y $\alpha_k = [q_k; q_{k+1}, \ldots]$ para $k \geq 0$.

Demostración. Ver el Lema 2.2.8 de [7], o el ejercicio 5.3.6 de [9]. □

3.2. **Fracciones Continuas Puramente Periódicas.** Nuestro propósito ahora es encontrar la forma explícita de la fracción continua del número irracional $\sqrt{d}$, donde d es un entero positivo libre de cuadrados. Para esto, estudiaremos una fracción continua simple cuyo período empieza desde la primera entrada.

Definición 12. Una fracción continua simple infinita α es llamada puramente periódica si $\alpha = [\overline{q_0; q_1, \ldots, q_{l-1}}]$ con longitud del período $l = l(\alpha)$.

Definición 13. Un irracional cuadrático α lo llamaremos reducido si $\alpha > 1$ y $-1 < \alpha' < 0$.

El siguiente teorema relaciona los irracionales cuadráticos reducidos y las fracciones continuas simples puramente periódicas.

TEOREMA 14. *La representación en fracción continua simple de un irracional cuadrático α es puramente periódica si y sólo si α es reducido.*

Demostración. Ver Teorema 2.2.13 [7] o Teorema 5.3.1 [9]. □

El siguiente resultado es un caso especial del Teorema 14.

COROLARIO 15. *Sea $d > 1$ un entero que no es un cuadrado perfecto. Entonces*

$$\sqrt{d} = [q_0; \overline{q_1, \ldots, q_{l-1}, 2q_0}],$$

donde $q_j = q_{l-j}$ para $j = 1, 2, \ldots, l-1$ y $q_0 = \lfloor \sqrt{d} \rfloor$.

Demostración. Consideremos $\alpha = \lfloor\sqrt{d}\rfloor + \sqrt{d}$. Se tiene que α es reducido y por el Teorema 14 su representación en fracción continua simple es puramente periódica, así que

$$\alpha = [\overline{a_0; a_1, a_2, \ldots, a_{l-1}}].$$

Luego $\sqrt{d} = \alpha - \lfloor\sqrt{d}\rfloor = \left[\lfloor\sqrt{d}\rfloor; \overline{a_1, a_2, \ldots, a_{l-1}, 2\lfloor\sqrt{d}\rfloor}\right]$, donde $q_0 = \lfloor\sqrt{d}\rfloor, q_1 = a_1, \ldots, q_{l-1} = a_{l-1}, q_l = 2\lfloor\sqrt{d}\rfloor = 2q_0$. Si definimos $\gamma = [\overline{a_{l-1}; a_{l-2}, \ldots, a_0}]$. Entonces

$$-\alpha' = \frac{1}{\gamma} = \frac{1}{[\overline{a_{l-1}; a_{l-2}, \ldots, a_0}]} = [0; \overline{a_{l-1}, a_{l-2}, \ldots, a_1, a_0}].$$

Por lo anterior

$$-\alpha' = \sqrt{d} - \lfloor\sqrt{d}\rfloor = [0; \overline{a_1, a_2, \ldots, a_{l-1}, 2\lfloor\sqrt{d}\rfloor}].$$

Así concluimos que $q_j = a_j = a_{l-j} = q_{l-j}$ para $j = 1, \ldots, l-1$. □

4. Divisores del número de clase en Campos Cuadráticos Reales

El objetivo de esta sección y de este trabajo es involucrar las fracciones continuas simples con el generador irracional de un ideal de un anillo cuadrático, con la finalidad de estudiar una familia especial de campos cuadráticos reales con número de clase par. Así que estudiaremos dos tipos de ideales: Primitivos y Reducidos. El teorema principal de este trabajo describe todos los ideales reducidos que son equivalentes a un ideal primitivo. Usando este resultado se tiene un criterio de divisibilidad por 2 para el número de clases de una familia de campos cuadráticos reales. Aplicando dichos criterios se obtienen anillos de enteros que no son de factorización única.

4.1. El Orden O_Δ.

A continuación introducimos la noción de discriminante y radicando asociado a un entero libre de cuadrados d_0. Sea

$$\Delta_0 = \begin{cases} d_0 & \text{si } d_0 \equiv 1 \pmod 4 \\ 4d_0 & \text{si } d_0 \equiv 2, 3 \pmod 4 \end{cases}.$$

El entero Δ_0 es llamado discriminante fundamental con radicando fundamental d_0. El irracional fundamental principal asociado a Δ_0 es

$$w_0 = \begin{cases} \dfrac{1+\sqrt{d_0}}{2} & \text{si} \quad d_0 \equiv 1 \pmod 4 \\ \sqrt{d_0} & \text{si} \quad d_0 \equiv 2, 3 \pmod 4 \end{cases}$$

Sea $f_\Delta \in \mathbb{N}$ y escribamos $\Delta = f_\Delta^2 \Delta_0$. Entonces el número

$$\Delta = \begin{cases} d & \text{si } d_0 \equiv 1 \pmod 4 \text{ y } f_\Delta \text{es impar} \\ 4d & \text{de otra forma,} \end{cases}.$$

donde

$$d = \begin{cases} (f_\Delta/2)^2 d_0 & \text{si } d_0 \equiv 1 \pmod 4 \text{ y } f_\Delta \text{es par} \\ f_\Delta^2 d_0 & \text{de otra forma.} \end{cases}.$$

El entero Δ es un discriminante con conductor f_Δ y d es el radicando asociado a dicho discriminante.

Sea Δ un discriminante con radicando d. Entonces el irracional principal asociado a Δ es

$$w_\Delta = \begin{cases} \dfrac{1+\sqrt{d}}{2} & \text{si} \quad \Delta = d \equiv 1 \pmod 4 \\ \sqrt{d} & \text{si} \quad \Delta \equiv 0 \pmod 4 \end{cases}$$

Sea $F = \mathbb{Q}(\sqrt{\Delta}) = \mathbb{Q}(\sqrt{d_0})$ y $\alpha, \beta \in F$. Escribiremos

$$[\alpha, \beta] = \{\alpha x + \beta y : x, y \in \mathbb{Z}\} = \mathbb{Z}\alpha + \mathbb{Z}\beta$$

para denotar al $\mathbb{Z}$-módulo generado por α, β. Observe que $[\alpha, \beta]$ es un anillo.

Definición 16. Si α, β son $\mathbb{Q}$-linealmente independientes, entonces diremos que el $\mathbb{Z}$-módulo $[\alpha, \beta]$ es un orden en $F = \mathbb{Q}(\sqrt{d_0})$.

En particular, si escribimos $O_\Delta = [1, w_\Delta]$, entonces O_Δ es un orden en $F = \mathbb{Q}(\sqrt{d_0})$. Se puede probar que $w_\Delta = f_\Delta w_0 + h$, para cierta $h \in \mathbb{Z}$, de ahí que

$$O_\Delta = [1, w_\Delta] = [1, f_\Delta w_0].$$

El índice $[O_{\Delta_0} : O_\Delta] = f_\Delta$ es precisamente el conductor asociado a Δ, donde O_{Δ_0} es el orden máximal de F que coincide con lo que conocemos como el anillo de enteros de F. Nótese que si $f_\Delta = 1$, entonces O_Δ es el anillo de enteros de F, es decir, $O_\Delta = A_F$.

El siguiente resultado nos ayuda a distinguir $\mathbb{Z}$-submódulos de ideales en O_Δ.

Teorema 17. *(Criterio para ideales) Sea Δ un discriminante y $(0) \neq I$ un $\mathbb{Z}$-submódulo de O_Δ. Entonces I tiene una representación de la forma*

$$I = [a, b + cw_\Delta],$$

para ciertos $a, c \in \mathbb{N}$ y $b \in \mathbb{Z}$. Además I es un ideal de O_Δ si y sólo si esta representación satisface que $c \mid a, c \mid b$ y $ac \mid N(b + cw_\Delta)$.

Demostración. Como $I \subseteq O_\Delta = [1, w_\Delta] = \mathbb{Z} + \mathbb{Z}w_\Delta$, entonces $I = [\alpha_1, \alpha_2]$, donde $\alpha_1, \alpha_2 \in O_\Delta$. Observar que $I \cap \mathbb{Z} \neq (0)$. Sea $a \in I$ el menor entero racional positivo. Es fácil ver que

$$a = (x_1 a_1 + y_1 a_2) + (x_1 b_1 + y_1 b_2) w_\Delta,$$

donde $x_1 b_1 + y_1 b_2 = 0$, $x_1, y_1 \in \mathbb{Z}$ y al menos uno de ellos es distinto de cero. Elegimos x_1, y_1 mínimos en valor absoluto con la propiedad anterior. De todos los elementos en I, elijamos $\beta = b + cw_\Delta \in I$ tales que $b \in \mathbb{Z}$, $c \in \mathbb{N}$ con c mínimo. Luego, se concluye que $[a, \beta] = I$. □

Definición 18. A un ideal en O_Δ que satisface las condiciones del Teorema 17 le llamaremos O_Δ-ideal.

Observemos que si $I = [a, b + cw_\Delta]$ es un O_Δ-ideal, entonces b se puede elegir de tal forma que $0 \leq b < a$.

Ejemplo 1. Sea $O_{17} = A_F = \left[1, \dfrac{1 + \sqrt{17}}{2}\right]$. Entonces por el Teorema 17

$$I = \left[4, 3 + \frac{1 + \sqrt{17}}{2}\right] = \left[4, \frac{7 + \sqrt{17}}{2}\right]$$

es un O_{17}-ideal, donde $a = 4, b = 3, c = 1$ y $N\left(\dfrac{7 + \sqrt{17}}{2}\right) = 8$.

4.2. **Ideales Primitivos.** Si Δ es un discriminante, $I = [a, b + cw_\Delta]$ un O_Δ-ideal, el entero positivo ac tiene la siguiente propiedad importante:

Teorema 19. *Sea $I = [a, b + cw_\Delta]$ un O_Δ-ideal. Entonces $|O_\Delta / I| = ac$.*

Demostración. Sea $(z_1 + z_2 w_\Delta) + I \in O_\Delta / I$. Puesto que $z_2 = cq_1 + r_1$ con $0 \leq r_1 < c$ y $(b + cw_\Delta \in I$, tenemos

$$(z_1 + z_2 w_\Delta) + I = (z_1 + (cq_1 + r_1) w_\Delta) - (b + cw_\Delta) q_1 + I = (z_1 - bq_1) + r_1 w_\Delta + I.$$

Luego $z_1 - bq_1 = aq_2 + r_2$ con $0 \leq r_2 < a$ y ya que $aq_2 \in I$ se tiene que

$$(z_1 + z_2 w_\Delta) + I = (r_2 + r_1 w_\Delta) + I.$$

Por lo tanto, hay a lo más ac elementos en O_Δ / I. El resultado se sigue en virtud de que todos los elementos son distintos. □

Definición 20. Sea $I = [a, b + cw_\Delta]$ un O_Δ-ideal. Definimos la norma de I como $N(I) = ac$. En particular si $c = 1$, entonces $N(I) = a$ y en este caso diremos que I es un O_Δ-ideal primitivo.

Observemos que si $I = [a, b + cw_\Delta]$ un O_Δ-ideal, entonces podemos escribir

$$I = (c)\left[\frac{a}{c}, \frac{b}{c} + w_\Delta\right].$$

Así que el O_Δ-ideal $J = \left[\frac{a}{c}, \frac{b}{c} + w_\Delta\right]$ es primitivo y satisface $J \sim I$. Recordamos este hecho sobresaliente como:

TEOREMA 21. *Si I es un O_Δ-ideal, entonces existe un O_Δ-ideal primitivo J tal que $J \sim I$.*

4.3. **Fracciones Continuas Aplicadas a Campos Cuadráticos Reales.** Ahora relacionaremos las fracciones continuas simples con el generador irracional de un O_Δ-ideal Primitivo. Para esto, veremos que uno de sus generadores es un irracional cuadrático de los cuales ya sabemos exactamente como es su fracción continua simple. De aquí en adelante $\Delta = \Delta_0$, es decir, $O_\Delta = O_{\Delta_0} = A_F$ es el anillo de enteros de $F = \mathbb{Q}(\sqrt{d_0})$. Sea $I = [a, b + w_\Delta]$ un O_Δ-ideal primitivo y

$$\sigma = \begin{cases} 2 & \text{si} \quad d \equiv 1 \pmod 4 \\ 1 & \text{si} \quad d \equiv 2 \text{ ó } 3 \pmod 4 \end{cases}$$

Escribimos $\sigma a = Q$ y $b = \begin{cases} \dfrac{P-1}{2} & \text{si} \quad \sigma = 2 \\ P & \text{si} \quad \sigma = 1, \end{cases}$
donde $P \in \mathbb{Z}$ y $Q \in \mathbb{N}$. Luego,

$$I = \left[\frac{Q}{\sigma}, \frac{P + \sqrt{d}}{\sigma}\right]. \tag{2}$$

Ejemplo 2. Sea $A_F = O_\Delta = \left[1, \dfrac{1 + \sqrt{33}}{2}\right]$ y consideremos el O_Δ-ideal $I = \left[4, 3 + \dfrac{1 + \sqrt{33}}{2}\right]$. Puesto que $33 \equiv 1 \pmod 4$, tenemos que $\sigma = 2$, $Q = \sigma a = 2 \cdot 4 = 8$ y $P = 2b + 1 = 7$. Por lo tanto $I = \left[\dfrac{8}{2}, \dfrac{7 + \sqrt{33}}{2}\right]$.

Con las definiciones de σ, P y Q que hemos establecido y el ejemplo anterior, tenemos una pregunta inmediata: si escribimos un $\mathbb{Z}$-módulo I como en (2) ¿podemos identificar si es un O_Δ-ideal primitivo?.

TEOREMA 22. *El O_Δ-ideal $I = \left[\dfrac{Q}{\sigma}, \dfrac{P + \sqrt{d}}{\sigma}\right]$ es primitivo si y sólo si $P^2 \equiv d \pmod{\sigma Q}$.*

Demostración. El resultado se sigue del Teorema 17. □

Observemos que $\dfrac{P + \sqrt{d}}{\sigma Q}$ es un irracional cuadrático si y sólo si $\dfrac{P + \sqrt{d}}{Q}$ es un irracional cuadrático. Así que por (1) de la Sección 3.1, el Teorema 22 y la observación

anterior tenemos que $I = \left[\frac{Q}{\sigma}, \frac{P+\sqrt{d}}{\sigma}\right]$ es un O_Δ-ideal primitivo si y sólo si $\frac{P+\sqrt{d}}{\sigma Q}$ es un irracional cuadrático si y sólo si $\frac{P+\sqrt{d}}{Q}$ es un irracional cuadrático.

Ejemplo 3. Por el Ejemplo 2 podemos ver que $I = \left[\frac{8}{2}, \frac{7+\sqrt{33}}{2}\right]$ es un O_Δ-ideal primitivo de $O_\Delta = \left[1, \frac{1+\sqrt{33}}{2}\right]$. Entonces $\alpha = \frac{7+\sqrt{33}}{8}$ es un irracional cuadrático que por cierto, es raíz de $x^2 - \frac{7}{4}x + \frac{1}{4}$.

4.4. **Ideales Reducidos.** Hemos visto que cualquier O_Δ-ideal es equivalente a un O_Δ-ideal primitivo. Más adelante veremos que todo O_Δ-ideal primitivo es equivalente a un ideal que llamaremos reducido. Así que a continuación daremos algunos criterios para saber cuándo un O_Δ-ideal es reducido.

Un O_Δ-ideal primitivo I se puede escribir como $I = [N(I), \alpha]$, donde $\alpha = \frac{b+\sqrt{\Delta}}{2}$ para algún $b \in \mathbb{Z}$.

Definición 23. Sea $\Delta > 0$ un discriminante, $I = [N(I), \alpha]$ un O_Δ-ideal primitivo. Diremos que I es reducido si no existe $\gamma \in I$ distinto de cero, tal que

$$|\gamma| < N(I) \qquad \text{y} \qquad |\gamma'| < N(I).$$

Teorema 24. *Sea $\Delta > 0$ un discriminante y sea I un O_Δ-ideal primitivo. Entonces I es reducido si y sólo si existe $\beta \in I$ tal que*

$$I = [N(I), \beta], \quad \beta > N(I) \quad y \quad -N(I) < \beta' < 0.$$

Demostración. Ver [7] o [9], Teorema 3.3.7 o Theorem 5.5.1 respectivamente. □

Ejemplo 4. Sea $O_\Delta = \left[1, \frac{1+\sqrt{145}}{2}\right]$. El O_Δ-ideal

$$I = \left[4, 3 + \frac{1+\sqrt{145}}{2}\right] = \left[4, \frac{7+\sqrt{145}}{2}\right] = [N(I), \beta],$$

es reducido puesto que $\beta > N(I)$ y $-4 < \beta' < 0$.

Corolario 25. *Si $\alpha = \frac{P+\sqrt{d}}{Q}$ es un irracional cuadrático reducido, donde $P \in \mathbb{Z}$, $Q \in \mathbb{N}$ y $d > 1$ es un entero libre de cuadrados, entonces $I = \left[\frac{Q}{\sigma}, \frac{P+\sqrt{d}}{\sigma}\right]$ es reducido.*

Demostración. Es consecuencia inmediata del Teorema 24. □

Los siguientes resultados también son consecuencia del Teorema 24 y nos hacen ver más fácilmente cuándo un O_Δ-ideal es reducido en términos de la norma del ideal.

Corolario 26. *Sean $\Delta > 0$ un discriminante, I un O_Δ-ideal. Si I es reducido, entonces $N(I) < \sqrt{\Delta}$.* □

Corolario 27. *Sean $\Delta > 0$ un discriminante, I un O_Δ-ideal primitivo. Si $N(I) < \frac{\sqrt{\Delta}}{2}$, entonces I es reducido.*

Demostración. Ver el Corolario 3.3.12 de [7] o el Corolario 5.5.2 de [9]. □

Ejemplo 5. En el Ejemplo 4 tenemos $N(I) = 4 < \dfrac{\sqrt{145}}{2} = \dfrac{\sqrt{\Delta}}{2}$. Entonces por el Corolario 27, I es reducido.

4.5. **Ciclos de Ideales Reducidos y Divisores del Número de Clase.** En esta sección presentamos un teorema que muestra que todo O_Δ-ideal primitivo es equivalente a un ideal reducido, dicho teorema es muy importante puesto que lo aplicaremos para estudiar una familia de campos cuadráticos reales a partir de una ecuación diofantina en donde el número de clase es par. Finalmente, daremos ejemplos de anillos cuadráticos que no son de factorización única.

LEMA 28. *Sea* $\Delta > 0$ *un discriminante,* $I = I_1 = \left[\dfrac{Q_0}{\sigma}, \dfrac{P_0 + \sqrt{d}}{\sigma}\right]$ *un* O_Δ*-ideal primitivo. Si* $\alpha = \alpha_0 = \dfrac{P_0 + \sqrt{d}}{Q_0}$ *y* P_k, Q_k, α_k *y* q_k *para* $k \geq 0$ *son definidos como en el* Lema 11, *entonces*

$$I_k = \left[\frac{Q_{k-1}}{\sigma}, \frac{P_{k-1} + \sqrt{d}}{\sigma}\right]$$

es un O_Δ*-ideal primitivo para toda* $k \in \mathbb{N}$.

Demostración. Ver [7], página 73, Lema 3.3.22. □

El siguiente teorema identifica todos los ideales reducidos equivalentes a un O_Δ-ideal primitivo dado.

TEOREMA 29. *Sea* $\Delta > 0$ *un discriminante,* $I = I_1 = \left[\dfrac{Q_0}{\sigma}, \dfrac{P_0 + \sqrt{d}}{\sigma}\right]$ *un* O_Δ*-ideal primitivo. Sea* $\alpha = \alpha_0 = \dfrac{P_0 + \sqrt{d}}{Q_0}$ *y* P_k, Q_k, α_k *y* q_k *para* $k \geq 0$, *definidos como en el* Lema 11. *Si*

$$I_k = \left[\frac{Q_{k-1}}{\sigma}, \frac{P_{k-1} + \sqrt{d}}{\sigma}\right],$$

entonces $I_1 \sim I_k$ *para toda* $k \in \mathbb{N}$. *Además, existe un valor mínimo* $n_0 \in \mathbb{N}$ *tal que* I_{n_0+j} *es reducido para toda* $j \geq 0$. *Estos* I_{n_0+j} *son todos los ideales reducidos equivalentes a* I_1.

Demostración. Ver el Teorema 3.3.23 de [7] o el Teorema 5.5.2 de [9]. □

La siguiente proposición es consecuencia del Teorema 29 y relaciona la longitud del período de la fracción continua simple del generador irracional de un O_Δ-ideal primitivo con el número de ideales reducidos que son equivalentes a dicho ideal.

PROPOSICIÓN 30. *Sea* $\Delta > 0$ *un discriminante. Consideremos* $I = I_1 = \left[\dfrac{Q_0}{\sigma}, \dfrac{P_0 + \sqrt{d}}{\sigma}\right]$ *un ideal primitivo en* O_Δ *y* $\alpha_0 = \dfrac{P_0 + \sqrt{d}}{Q_0}$. *Entonces el número de ideales reducidos equivalentes a* I *es menor o igual que* $l(\alpha_0)$, *donde* $l(\alpha_0)$ *es la longitud del período de la fracción continua de* α_0.

Demostración. Ver [7], página 84, Proposición 3.3.24. □

Ejemplo 6. Si $\Delta = 233$, entonces $A_F = O_\Delta = \left[1, \dfrac{1 + \sqrt{233}}{2}\right]$. Sea

$$I = I_1 = \left[14, 8 + \frac{1 + \sqrt{233}}{2}\right] = \left[14, \frac{17 + \sqrt{233}}{2}\right]$$

un O_Δ-ideal primitivo. Entonces

$$\alpha_0 = \frac{17+\sqrt{233}}{28}.$$

Por el Teorema 29 tenemos que

$$\begin{aligned} I_1 = \left[14, \frac{17+\sqrt{233}}{2}\right] &\sim I_2 = \left[2, \frac{11+\sqrt{233}}{2}\right] \sim I_3 = \left[8, \frac{13+\sqrt{233}}{2}\right] \\ &\sim I_4 = \left[7, \frac{3+\sqrt{233}}{2}\right] \sim I_5 = \left[4, \frac{11+\sqrt{233}}{2}\right] \\ &\sim I_6 = \left[4, \frac{13+\sqrt{233}}{2}\right] \sim I_7 = \left[7, \frac{11+\sqrt{233}}{2}\right] \\ &\sim I_8 = \left[8, \frac{3+\sqrt{233}}{2}\right] \sim I_9 = \left[2, \frac{13+\sqrt{233}}{2}\right] \\ &\sim I_{10} = \left[1, \frac{15+\sqrt{233}}{2}\right] \sim I_{11} = \left[2, \frac{15+\sqrt{233}}{2}\right] = I_2. \end{aligned}$$

Nótese que

$$I_1 = \left[14, \frac{2\cdot 14\cdot n + 17 + \sqrt{233}}{2}\right],$$

para toda $n \in \mathbb{Z}$. Si $n > 0$, siempre se cumple que

$$\frac{2\cdot 14\cdot n + 17 - \sqrt{233}}{2} > 0.$$

Si $n < 0$, siempre se cumple que

$$\frac{2\cdot 14\cdot n + 17 + \sqrt{233}}{2} < N(I_1) = 14.$$

Entonces por la contrapositiva del Teorema 24, I_1 no es un ideal reducido. Es fácil ver que I_r con $r = 2, 3, \ldots, 10$ son ideales reducidos. Por otro lado la fracción continua simple de α_0 es:

$$\alpha_0 = [1; 6, \overline{1, 1, 3, 3, 1, 1, 7, 15, 7}],$$

de donde observamos que $l(\alpha_0) = 9$. En nuestro caso, como afirma la Proposición 30, el número de ideales reducidos equivalentes a I_1 coincide con la longitud del período de α_0.

El siguiente resultado es una aplicación de todo lo antes visto que nos asegura la existencia de un divisor para el número de clase de cierta familia de campos cuadráticos reales.

Teorema 31. *Sea $\Delta = \Delta_0 > 0$ un discriminante fundamental con radicando $d = d_0 = \sigma^2 a^m + b^2$, tal que $a > 1$ y $m > 1$. Entonces existe un divisor n de m tal que $n | h_\Delta$ y $n > \dfrac{\log_a(d/\sigma^2)}{l+1}$, donde $l = l(w_\Delta)$ es el período de la fracción continua de w_Δ y h_Δ es el número de clase de $\mathbb{Q}(\sqrt{d_0})$.*

Demostración. Sea $I = \left[a, \frac{b+\sqrt{d}}{\sigma}\right]$ un ideal en O_Δ. Entonces $I^m = \left[a^m, \frac{b+\sqrt{d}}{\sigma}\right]$. Luego

$$I^m = \left[a^m, \frac{b+\sqrt{d}}{\sigma}\right] = \left[\frac{d-b^2}{\sigma^2}, \frac{b+\sqrt{d}}{\sigma}\right] = \left(\frac{b+\sqrt{d}}{\sigma}\right)\left[\frac{\sqrt{d}-b}{\sigma}, 1\right]$$
$$= \left(\frac{b+\sqrt{d}}{\sigma}\right)\left[1, \frac{\sqrt{d}-b}{\sigma}\right].$$

Si $\sigma = 2$, entonces b es impar. Así que $\frac{b+1}{2} \in \mathbb{Z}$. Por lo que

$$I^m = \left(\frac{b+\sqrt{d}}{2}\right)\left[1, \frac{\sqrt{d}-b}{2}\right] = \left(\frac{b+\sqrt{d}}{2}\right)\left[1, \frac{b+1}{2} + \frac{\sqrt{d}-b}{2}\right]$$
$$= \left(\frac{b+\sqrt{d}}{2}\right)[1, w_\Delta].$$

Si $\sigma = 1$, entonces

$$I^m = \left(b+\sqrt{d}\right)[1, \sqrt{d}-b] = \left(b+\sqrt{d}\right)[1, b+\sqrt{d}-b] = \left(b+\sqrt{d}\right)[1, w_\Delta].$$

Por lo tanto $I^m \sim O_\Delta = A_F$. Así que I^m es un ideal principal.

Si n es el orden de la clase de I en el grupo de clases de ideales de O_Δ, entonces $n|h_\Delta$. Como $I^m \sim O_\Delta$, tenemos que $n|m$. Si $I' = \left[a, \frac{b-\sqrt{d}}{\sigma}\right]$, entonces $I'^m = \left[a^m, \frac{b-\sqrt{d}}{\sigma}\right] \sim O_\Delta$. Sea $r = \left\lfloor \frac{\log_a(d/\sigma^2)}{2n} \right\rfloor$. Entonces $\{I^{jn}, I'^{jn}\}_{j=0}^{r}$ son $2r+1$ ideales principales distintos, tales que

$$N(I^{jn}) \leq a^{rn} < \frac{\sqrt{d}}{\sigma} = \frac{\sqrt{\Delta}}{2} \quad \text{y} \quad N(I'^{jn}) < \frac{\sqrt{\Delta}}{2}.$$

Por el Corolario 27, tenemos que I^{jn} y I'^{jn} son reducidos para $0 \leq j \leq r$. Así que por la Proposición 30 se tiene que $l = l(w_\Delta) \geq 2r+1$, de donde $n > \frac{\log_a(d/\sigma^2)}{l+1}$. □

Ejemplo 7. Sea $d = 65 \equiv 1 \pmod 4$. Entonces $A_F = O_\Delta = \left[1, \frac{1+\sqrt{65}}{2}\right]$. Observemos que $\sigma = 2$ y $65 = 2^2 \cdot 2^2 + 7^2$. Siguiendo el Teorema 31, tenemos que $a = 2, b = 7$ y $m = 2$. Entonces los divisores de m son 1 ó 2. Por otro lado $w_\Delta = \frac{1+\sqrt{65}}{2} = [4; \overline{1, 1, 7}]$, por lo que $l = l(w_\Delta) = 3$ y así $\frac{\log_a(d/\sigma^2)}{l+1} = 1.0056$. Por el Teorema 31 se sigue que $n = 2$ y que $2|h_\Delta$, es decir, h_Δ es par. Entonces $h_\Delta > 1$ y por tanto $A_F = O_\Delta = \left[1, \frac{1+\sqrt{65}}{2}\right]$ no es de factorización única.

Corolario 32. *Si $d = \sigma^2 a^p + b^2$ es un radicando fundamental donde p es primo y $l < p$, entonces $p|h_\Delta$.*

Demostración. Puesto que $l < p$, se tiene $l \leq p-1 < \log_a\left(\frac{d}{\sigma^2}\right) - 1$. Por lo que $1 < \frac{\log_a\left(\frac{d}{\sigma^2}\right)}{l+1}$. Por el Teorema 31, $p|h_\Delta$. □

Por último daremos algunos ejemplos del Corolario 32, que muestran familias de anillos de enteros en campos cuadráticos reales que no son de factorización única.

El siguiente lema clasifica a los números irracionales con representación en fracción continua periódica con longitud 1.

LEMA 33. *Sea $n \in \mathbb{N}$ libre de cuadrados. Entonces $l(\sqrt{n}) = 1$ si y slo si $n = a^2 + 1$ para algún $a \in \mathbb{N}$.*

Demostración. Ver [7], página 91, Lema 3.3.29. □

Ejemplo 8. Sea $d = a^2 + 1$ libre de cuadrados y $a > 1$. Siguiendo el Corolario 32, vemos que $\sigma = 1$, $p = 2$ y $b = 1$. Puesto que $\sigma = 1$, se tiene que $d \equiv 2$ o $3 \pmod 4$. Si a fuera par, se tendría que $d \equiv 1 \pmod 4$ y ese no es el caso para d. Así que a tiene que ser impar y por tanto $d \equiv 2 \pmod 4$. Por el Lema 33, tenemos que $l(\sqrt{d}) = 1$. Entonces por el Corolario 32, se tiene que $2|h_\Delta$. Luego, $h_\Delta > 1$ y por tanto

$$A_F = O_\Delta = [1, \sqrt{a^2 + 1}]$$

no es de factorización única.

Sean $d = a^2 + 1$ con a impar $(a > 1)$ y d libre de cuadrados, h_Δ el número de clase de $\mathbb{Q}(\sqrt{a^2 + 1})$. A continuación presentamos algunos ejemplos que fueron calculados utilizando el programa Mathematica V. 5.2.

Ejemplos de campos cuadráticos con h_Δ par

♯	a	$d = a^2 + 1$	h_Δ
1	3	10	2
2	5	26	2
3	9	82	4
4	11	122	2
5	13	170	4
6	15	226	8
7	17	290	4
8	19	362	2
9	21	442	8
10	23	530	4
11	25	626	4
12	27	730	12
13	29	842	6
14	31	962	4
15	33	1090	12
16	35	1226	10
17	37	1370	4
18	39	1522	12
19	45	2026	14
20	47	2210	8
21	49	2402	8
22	51	2602	10
23	53	2810	8
24	55	3026	16
25	59	3482	6

♯	a	$d = a^2 + 1$	h_Δ
26	61	3722	10
27	63	3970	20
28	65	4226	8
29	67	4490	8
30	69	4762	22
31	71	5042	12
32	73	5330	8
33	75	5626	28
34	77	5930	12
35	79	6242	8
36	81	6562	16
37	83	6890	16
38	85	7226	18
39	87	7570	20
40	89	7922	8
41	91	8282	12
42	95	9026	16
43	97	9410	20
44	101	10202	14
45	103	10610	12
46	105	11026	44
47	109	11882	12
48	111	12322	20
49	113	12770	12
50	115	13226	16

Ejemplo 9. Sean $d = t^6+1 = (t^2)^3+1$ libre de cuadrados y $t > 1$. Por el Corolario 32, $\sigma = 1$, $p = 3$ y $b = 1$. Análogamente al Ejemplo 8, tenemos que t debe ser impar y por tanto $d \equiv 2 \pmod 4$. También $\sqrt{d} = \sqrt{(t^3)^2+1}$ y por el Lema 33 se tiene $\sqrt{d} = [t^3, \overline{2t^3}]$, es decir, $l = 1$. Entonces por el Corolario 32, $3|h_\Delta$. Luego, $h_\Delta > 1$ y por tanto

$$A_F = O_\Delta = [1, \sqrt{(t^2)^3+1}]$$

no es de factorización única.

Observemos que si ahora escribimos $d = (t^3)^2 + 1$, análogamente a lo anterior se tiene que $2 \mid h_\Delta$ y por tanto $6 \mid h_\Delta$.

Nótemos que $d = t^6 + 1$ con las condiciones del Ejemplo 9, está incluida en el Ejemplo 8.

Sean $d = (t^2)^3 + 1$ con t impar ($t > 1$) y d libre de cuadrados, h_Δ el número de clase de $\mathbb{Q}(\sqrt{(t^2)^3+1})$. A continuación presentamos algunos ejemplos que fueron calculados utilizando el programa Mathematica V. 5.2.

Caso particular de la tabla anterior

♯	t^2	$d = (t^2)^3 + 1$	h_Δ
1	9	730	12
2	25	15626	24
3	81	531442	120
4	121	1771562	120
5	169	4826810	216
6	225	11390626	792
7	289	24137570	432
8	441	85766122	1008
9	529	148035890	1008
10	625	244140626	1248

♯	t^2	$(t^2)^3 + 1$	h_Δ
11	729	387420490	2520
12	841	594823322	1632
13	961	887503682	1968
14	1089	1291467970	5664
15	1225	1838265626	4200
16	1369	2565726410	3984
17	1521	3518743762	6216
18	2025	8303765626	15552
19	2209	10779215330	7104
20	2401	13841287202	5184

Agradecemos las valiosas sugerencias del árbitro las cuales mejoraron la presentación de este trabajo.

Referencias

[1] Biró, A., *Chowla's conjecture*. Acta Arith. **107**, 179-194, (2003).
[2] Biró, A., *Yokoi's conjecture*. Acta Arith. **106**, 85-104, (2003).
[3] Byeon, D., Kim M., Lee J., *Mollin's conjecture*. Acta Arith. **126**, 99-114, (2007).
[4] Hardy, G. H., Wright, E. M., *An introduction to the theory of numbers. Fifth edition*, Oxford, at the Clarendon Press, (1979).
[5] Ireland K., Rosen, M., *A classical introduction to modern number theory*. GTM **84** Springer Verlag (1982).
[6] Louboutin, S., Mollin, R. A., Williams, H. C., *Class Numbers of Real Quadratic Fields, Continued Fractions, Reduced Ideals, Prime-Producing Quadratic Polynomials and Quadratic Residue Covers*. Can. J. Math. **44**, 824-842, (1992).
[7] Magaña-Zapata J. A. *Fracciones continuas y divisores del número de clases en campos cuadráticos reales*. Tesis de Maestría del Posgrado en Matemáticas de la Universidad Autónoma Metropolitana-Iztapalapa, 2010.
[8] Mollin, R. A., *Quadratics*. CRC Press, Boca Raton (1996).
[9] Mollin, R.A., *Fundamental Number Theory with Applications*. CRC Press, serie Discrete Mathematics and its Applications, Boca Raton (1998).
[10] Mollin, R. A., *Simple Continued Fraction Solutions for Diophantine Equations*. Expo. Math. **19**, 55-73, (2001).

[11] Stewart, I., Tall, D., *Algebraic Number Theory and Fermat's Last Theorem*. 3rd edition. A. K. Peters 2002, New York. (1979)

Dirección de los autores:
Janeth A. Magaña-Zapata
Universidad Autónoma Metropolitana,
Unidad Iztapalapa,
División de Ciencias Básicas e Ingeniería,
Departamento de Matemáticas.
Av. San Rafael Atlixco 186, Col. Vicentina
Del. Iztapalapa, C.P. 09340 México, D.F.
e-mail: janys23@yahoo.com.mx

Mario Pineda-Ruelas
Universidad Autónoma Metropolitana,
Unidad Iztapalapa,
División de Ciencias Básicas e Ingeniería,
Departamento de Matemáticas.
Av. San Rafael Atlixco 186, Col. Vicentina
Del. Iztapalapa, C.P. 09340 México, D.F.
e-mail: mpr@xanum.uam.mx

Mixba'al
Revista Metropolitana de Matemáticas
No. 1, Vol. IV, junio de 2013, 29–38

SOLUCIÓN DE ECUACIONES DIOFANTINAS A TRAVÉS DE LA FACTORIZACIÓN ÚNICA

ALEJANDRO AGUILAR-ZAVOZNIK

Resumen. Estudiaremos algunas diferencias entre anillos de factorización única y anillos que no lo son. Veremos qué podemos hacer cuando no se tiene factorización única para recuperar algunas de las propiedades que perdemos cuando no se tiene esta propiedad. Usaremos estos resultados para decidir si algunas ecuaciones diofantinas no son solubles y, en el caso contrario, para encontrar todas sus soluciones.

1. Introducción

Un problema que frecuentemente encontramos en las matemáticas es expresar un elemento en términos de otros más sencillos, por ejemplo, si $a \in \mathbb{Z}$ podemos factorizar a como producto de números primos; si V es un espacio vectorial de dimensión finita, podemos expresar $v \in V$ en términos de los elementos de una base; si $A \subseteq \mathbb{R}$ es un conjunto abierto, es posible expresarlo como unión de intervalos abiertos, etc.

Usando la factorización en $\mathbb{Z}$ como modelo, han surgido muchas teorías similares en una gran variedad de anillos, por ejemplo, es común hablar de la factorización en conjuntos de polinomios o matrices. En la actualidad, los principales problemas de factorización se plantean en términos de los anillos de enteros de campos de números, campos de funciones o campos p-ádicos. Incluso hay casos en los que se ha prescindido de la suma, estudiando la factorización de los elementos de algunos monoides [2].

A continuación veremos algunos ejemplos de anillos o monoides donde tenemos factorización única y otros en los que no se tiene esta propiedad. Estudiaremos cómo los ideales se pueden usar para recuperar la factorización única y daremos una aplicación de esta idea para resolver algunas ecuaciones diofantinas.

2. Factorización única

Existen dos dominios de factorización única (DFU) ampliamente estudiados: los enteros y los anillos de polinomios con coeficientes de un campo $\mathbb{K}$. El Teorema Fundamental de la Aritmética afirma que todo número $a \in \mathbb{Z}\setminus\{0, \pm 1\}$ se puede escribir de forma única como producto de primos $a = p_1 \cdot p_2 \cdots p_t$. Es necesario aclarar lo que significa que dos factorizaciones sean iguales. En primer lugar, el orden de los factores no es relevante, por ejemplo, $6 = (2)(3) = (3)(2)$ son la misma factorización. Segundo, dos factorizaciones que difieren por asociados son la misma, por ejemplo $(2)(3)$ y $(-2)(-3)$ son la misma factorización. En esta sección vamos a aclarar lo que significan estos conceptos. A lo largo de este trabajo, la palabra anillo significa anillo conmutativo con unidad 1. Si $\mathbb{A} \subseteq \mathbb{B}$ son anillos y $b_1, \ldots, b_t \in \mathbb{B}$, entonces $\mathbb{A}[b_1, \ldots, b_t]$ es el subanillo más pequeño de $\mathbb{B}$ que contiene a $\mathbb{A}$ y a todos los elementos $b_1, \ldots, b_t$. Si $\mathbb{F} \subseteq \mathbb{K}$ son campos y $b_1, \ldots, b_t \in \mathbb{K}$, entonces $\mathbb{F}(b_1, \ldots, b_t)$ es el menor subcampo de $\mathbb{K}$ que contiene tanto a $\mathbb{F}$ como a los elementos $b_1, \ldots, b_t$. Denotaremos $U(\mathbb{A})$ al grupo de unidades de $\mathbb{A}$. Por ejemplo, $U(\mathbb{Z}) = \{1, -1\}$; si $\mathbb{F}$ es un campo entonces $U(\mathbb{F}[x]) = U(\mathbb{F}) = \mathbb{F} \setminus \{0\}$.

El Teorema Fundamental del Álgebra es el análogo al Teorema Fundamental de la Aritmética en el anillo $\mathbb{C}[x]$. Éste afirma que todo polinomio no constante en $\mathbb{C}[x]$ se

2010 *Mathematics Subject Classification.* 11A51, 11D45,11R04,11R11,11R29.
Palabras clave. Ecuaciones diofantinas, campos de números, factorización única.

factoriza de forma única como producto de polinomios irreducibles de la forma $ax+b$, salvo por el orden y los asociados.

En $\mathbb{Z}$ es común utilizar las palabras "primo" e "irreducible" como si fueran sinónimos. Aunque en este caso son conceptos equivalentes, veremos que no siempre es así.

Definición 1. Un elemento $a \in \mathbb{A}$ es irreducible si, siempre que $a = b_1\, b_2$, entonces $b_1 \in U(\mathbb{A})$ ó $b_2 \in U(\mathbb{A})$.

En un curso elemental de álgebra se demuestra la siguiente propiedad:

Proposición 2. *Si $p \in \mathbb{Z}$ es primo y $p \mid a_1\, a_2$, entones $p \mid a_1$ ó $p \mid a_2$.* □

A partir del resultado anterior surge la definición de primo:

Definición 3. Un elemento $p \in \mathbb{Z}$ es primo si $p \mid a_1\, a_2$ implica $p \mid a_1$ ó $p \mid a_2$.

En la siguiente tabla proporcionamos definiciones equivalentes de primo e irreducible para poder compararlas:

Primo	Irreducible
Para todo $d \in \mathbb{Z}$, $p\, d = a_1 a_2$ implica $p \mid a_1$ ó $p \mid a_2$.	$p = a_1 a_2$ implica $p \mid a_1$ ó $p \mid a_2$.

Podemos observar que, si un elemento es primo, también tiene que ser irreducible pues la definición de irreducible es la de primo con $d = 1$. Más adelante veremos ejemplos en los que estas definiciones no son equivalentes.

Ahora veamos un ejemplo de monoide de factorización única con una operación no conmutativa. Sea A un conjunto finito al que llamaremos alfabeto. Una sucesión finita de elementos de A la llamaremos una palabra de A y al conjunto de palabras de A lo denotaremos A^*. Este conjunto es un monoide con la operación concatenación, es decir,

$$(a_1, \ldots, a_t) * (b_1, \ldots, b_r) = (a_1, \ldots, a_t, b_1, \ldots, b_r).$$

Cuando no hay confusión, es común denotar la palabra $(a_1, a_2, \ldots, a_t)$ como $a_1\, a_2 \cdots a_t$. Claramente A^* es asociativo y el elemento neutro es la sucesión vacía, a la que llamaremos 1. Este monoide es de factorización única donde los elementos irreducibles son las letras del alfabeto A y $U(A^*) = \{1\}$. El conjunto de las palabras no vacías de A^* la denotaremos $A^+ = A^* - \{1\}$.

Si adicionalmente A es totalmente ordenado, podemos usar esta propiedad para ordenar A^+ por medio del orden lexicográfico, que es el que usa el diccionario. Formalmente esto se escribe como sigue: sean $p_1 = (a_1, a_2, \ldots, a_t)$, $p_2 = (b_1, b_2, \ldots, b_r) \in A^+$. Diremos que $p_1 > p_2$ si existe $i < min(t, r)$ tal que $a_j = b_j$ para $j < i$ y $a_i > b_i$ o bien si $t > r$ y $a_j = b_j$ para todo $j \leq r$. Si $A = \{a, b, c, \ldots, z\}$ es el alfabeto con veintisiete letras (incluyendo la ñ) donde $a < b < c < \cdots < z$, entonces: *campo* $>$ *anillo*, *campo* $>$ *cambio* y *cartagena* $>$ *carta*. En particular, una palabra $p \in A^+$ es de Lyndon si $p = p_1 * p_2$, con $p_1, p_2 \in A^+$ implica que $p < p_2 * p_1$. Si $A = \{a, b\}$, las primeras palabras de Lyndon son:

$$\{a, b, ab, aab, abb, aaab, aabb, abbb, aaaab, aaabb, aabab, \ldots\}.$$

Teorema 4. *Toda palabra en A^+ se puede escribir de forma única como producto de una cadena no creciente de palabras de Lyndon.*

Demostración. Ver [4], p.p. 64. □

Por ejemplo, la palabra *aababaaaabaab* se factoriza como producto no creciente de palabras de Lyndon como:

$$aababaaaabaab = aabab * aaaabaab.$$

Notemos que $aabab * aaaab * aab$ también es una factorización, pero $aaaab < aab$.

Los anillos de enteros son una de las familias de anillos donde más se ha estudiado la factorización. Trataremos el caso de los campos cuadráticos. Sugerimos al lector interesado consultar [1], [3], [8] y [10] para profundizar en el tema.

Sea d un entero libre de cuadrados. El campo cuadrático con radicando d es el campo $\mathbb{F} = \mathbb{Q}(\sqrt{d})$. Definimos el anillo de enteros de $\mathbb{F}$ como:

$$\mathbb{O}_d = \{a_1 + a_2\sqrt{d} : a_1, a_2 \in \mathbb{Z}\} \qquad \text{si } d \equiv 2, 3 \pmod 4,$$
$$\mathbb{O}_d = \{a_1 + a_2\frac{1+\sqrt{d}}{2} : a_1, a_2 \in \mathbb{Z}\} \quad \text{si } d \equiv 1 \pmod 4.$$

Para algunos valores de d, $\mathbb{O}_d$ es un DFU. Carl Friedrich Gauss conjeturó que solamente hay un número finito de valores negativos d para los que $\mathbb{O}_d$ es de factorización única. En 1967 Harlold Stark [9] probó que estos valores son $d = -1, -2, -3, -7, -11, -19, -43, -67, -163$. Una observación interesante es el hecho de que únicamente los primeros cinco anillos son dominios euclideanos, los últimos cuatro son ejemplos de anillos que son DFU pero no euclideanos. En el caso $d > 0$, también fue Gauss quien conjeturó que existe una infinidad de $\mathbb{O}_d$'s que son DFU. Esta célebre conjetura aún no ha sido probada.

Antes de continuar vamos a definir algunas herramientas que nos ayudarán a estudiar la factorización en los anillos de enteros. La función norma $N : \mathbb{Q}(\sqrt{d}) \to \mathbb{Z}$ se define como $N(a_1 + a_2\sqrt{d}) = a_1^2 - d\,a_2^2$. Algunas propiedades importantes de la norma son las siguientes:

(1) Un elemento $\alpha \in \mathbb{O}_d$ es unidad si y sólo si $|N(\alpha)| = 1$.
(2) Si $\alpha, \beta \in \mathbb{O}_d$ son asociados, entonces $|N(\alpha)| = |N(\beta)|$.
(3) Si $\gamma = \alpha\,\beta$, entonces $N(\gamma) = N(\alpha)N(\beta)$.

Usando la afirmación 1, es fácil verificar que:

(1) Si $d = -1$, $U(\mathbb{O}_{-1}) = \{\pm 1, \pm i\}$.
(2) Si $d = -3$, $U(\mathbb{O}_{-3}) = \left\{\pm 1, \pm\frac{1+\sqrt{-3}}{2}, \pm\frac{1-\sqrt{-3}}{2}\right\}$.
(3) Si $d < 0, d \neq -1, -3$, entonces $U(\mathbb{O}_d) = \{\pm 1\}$.
(4) Si $d > 0$, existe una unidad μ tal que $U(\mathbb{O}_d) = \{\pm\mu^k : k \in \mathbb{Z}\}$.

Lo anterior nos indica que si $d < 0$, entonces $U(\mathbb{O}_d)$ es finito y en el caso $d > 0$ hay una infinidad de unidades en $\mathbb{O}_d$.

Al igual que en el caso de $\mathbb{Z}$, si $\mathbb{O}_d$ es DFU, entonces primo e irreducible son conceptos equivalentes. En la siguiente sección vamos a ver ejemplos de irreducibles que no son primos.

3. Anillos de enteros sin factorización única

Consideremos el anillo $\mathbb{O}_{10}$. El elemento $10 \in \mathbb{O}_{10}$ tiene dos factorizaciones distintas:

$$10 = (2)(5) = (\sqrt{10})^2.$$

Usando la propiedad 2 de la norma podemos ver que estas dos factorizaciones son esencialmente distintas, es decir, que no podemos ir de una factorización a la otra cambiando el orden de los factores o cambiando algunos de ellos por elementos asociados. Notemos que $N(2) = 2^2 - 10(0)^2 = 4$, $N(5) = 5^2 - 10(0)^2 = 25$ y $N(\sqrt{10}) = 0^2 - 10(1)^2 = -10$. Como $|N(2)| \neq |N(\sqrt{10})|$ y $|N(5)| \neq |N(\sqrt{10})|$, entonces 2 y 5 no son asociados de $\sqrt{10}$ en $\mathbb{O}_d$. Falta demostrar que 2, 5 y $\sqrt{10}$ son elementos irreducibles. Para esto utilizamos la propiedad 3 de la norma. Por ejemplo, si 2 no es irreducible, entonces $2 = \alpha_1\,\alpha_2$ para algunos $\alpha_1, \alpha_2 \in \mathbb{O}_{10}$ no unidades. Por la propiedad 3, $|N(\alpha_1)| = |N(\alpha_2)| = 2$, ya que la norma es un entero y es ± 1 si y sólo si el elemento es una unidad. Vamos a demostrar que no hay ningún elemento con norma ± 2 en $\mathbb{O}_{10}$. Con cálculos sencillos se puede observar que los cuadrados módulo 10 son $0, 1, 4, 5, 6, 9$. Como

$$N(a_1 + a_2\sqrt{10}) = a_1^2 - 10a_2^2 \equiv a_1^2 \pmod{10},$$

entonces la norma de cualquier elemento tiene que ser congruente con alguno de los valores $0, 1, 4, 5, 6, 9$, así que 2 y -2 no son norma de ningún elemento, por lo tanto, no pueden existir $\alpha_1, \alpha_2 \in \mathbb{O}_{10}$ no unidades tales que $2 = \alpha_1\,\alpha_2$. Por lo tanto 2 es irreducible. De forma análoga se puede demostrar que $\sqrt{10}$ es irreducible. Para probar que 5 es irreducible hay que usar un procedimiento similar módulo 40. Por tanto, $\mathbb{O}_{10}$ no es DFU.

Ya vimos que para algunos $d \in \mathbb{Z}$ se tiene que $\mathbb{O}_d$ no es un DFU, ¿esto es algo grave? La respuesta es sí, pues perdemos algunas propiedades. Por ejemplo, consideremos la siguiente proposición:

Proposición 5. *Sea $a, b, c \in \mathbb{Z}$ tales que $a^n = b\,c$ y $\text{m.c.d.}\,(b, c) = 1$. Entonces existen $b_1, c_1 \in \mathbb{Z}$ tales que $b = b_1^n$ y $c = c_1^n$.*

Si revisamos la demostración de la proposición anterior, se usa el hecho de que $\mathbb{Z}$ es un dominio de factorización única. Si esta propiedad no se tiene el resultado puede no ser cierto. Observemos que en $\mathbb{O}_{10}$, $(\sqrt{10})^2 = (2)(5)$, donde 2 y 5 son primos relativos, sin embargo, 2 y 5 no son cuadrados, pues de hecho son irreducibles. En este ejemplo no se cumple la proposición anterior.

¿Entonces qué hacemos para resolver el problema de no tener la factorización única? Kummer propuso el uso de los números ideales. Lo que debemos de hacer es agrandar el campo de tal forma que ahora sí se tenga la factorización única. Por ejemplo, si agregamos los elementos $\sqrt{2}$ y $\sqrt{5}$, entonces

$$(2)(5) = (\sqrt{2})^2(\sqrt{5})^2 = (\sqrt{2}\,\sqrt{5})^2 = (\sqrt{10})^2.$$

Podemos ver que en este caso las dos factorizaciones son la misma. Los números ideales tienen la desventaja de que hay varias opciones para recuperar la factorización única.

Basándose en esta idea, Dedekind propuso sustituir los números ideales por los ideales. En el caso de los anillos de enteros usaremos la notación

$$\langle \alpha_1, \ldots, \alpha_t \rangle = \{\alpha_1\beta_1 + \cdots + \alpha_t\beta_t : \beta_1, \ldots, \beta_t \in \mathbb{O}_d\}$$

para denotar al ideal generado por los elementos $\alpha_1, \ldots, \alpha_t$. En particular, todo ideal de $\mathbb{O}_d$ se puede describir con a lo más dos elementos ([10], Theorem 5.20). Por ejemplo, en $\mathbb{Z}$, $\langle a_1, a_2, \ldots, a_k \rangle = \langle \text{m.c.d.}\,(a_1, a_2, \ldots, a_k) \rangle$. En el anillo $\mathbb{O}_{10}$, $\left\langle 44 + 7\sqrt{10}, 17 + \sqrt{10}, 11 + 4\sqrt{10} \right\rangle = \left\langle 3, 2 + \sqrt{10} \right\rangle$ y los ideales $\left\langle 2, \sqrt{10} \right\rangle$ y $\left\langle 5, \sqrt{10} \right\rangle$ no se pueden expresar usando un solo elemento. Cuando un ideal I se puede escribir usando sólo un generador diremos que $I = \langle \alpha \rangle$ es el ideal principal generado por α. Si no es posible escribir al ideal usando solamente un elemento, diremos que I es un ideal no principal.

La idea de Dedekind era usar los ideales principales como los elementos del anillo y los ideales no principales como los números ideales de Kummer. De esta forma, el ejemplo $\sqrt{10}$ se puede escribir en términos de ideales como:

$$\left\langle \sqrt{10} \right\rangle = \left\langle 2, \sqrt{10} \right\rangle^2 \left\langle 5, \sqrt{10} \right\rangle^2,$$

donde el ideal $\left\langle 2, \sqrt{10} \right\rangle$ juega el papel de $\sqrt{2}$ en el ejemplo con números ideales y $\left\langle 5, \sqrt{10} \right\rangle$ juega el papel de $\sqrt{5}$. Sin importar si $\mathbb{O}_d$ es un DFU o no, el monoide de los ideales no cero de $\mathbb{O}_d$ siempre es de factorización única.

Como ya vimos, $(\sqrt{10})^2 = (2)(5)$ donde $2, 5$ no son cuadrados en $\mathbb{O}_{10}$. Si ahora consideramos la factorización en ideales tenemos:

$$\langle 2 \rangle = \left\langle 2, \sqrt{10} \right\rangle^2 \quad \text{y} \quad \langle 5 \rangle = \left\langle 5, \sqrt{10} \right\rangle^2,$$

por lo que ahora sí $\langle 2 \rangle$ es un cuadrado y $\langle 5 \rangle$ es un cuadrado. De esta forma, si usamos ideales, podemos dar un resultado análogo a la Proposición 5.

Proposición 6. *Sean $\alpha, \beta, \gamma \in \mathbb{O}_d$ tales que $\alpha^n = \beta\,\gamma$ y $\langle \alpha \rangle + \langle \beta \rangle = \mathbb{O}_d$. Entonces existen ideales $I, J \subseteq \mathbb{O}_d$ tales que $\langle \beta \rangle = I^n$ y $\langle \gamma \rangle = J^n$.*

Demostración. Es similar a la de la Proposición 5. □

Si $\mathbb{O}_d$ es de factorización única, entonces el análogo a la Proposición 5 sería:

COROLARIO 7. *Sean $\alpha, \beta, \gamma \in \mathbb{O}_d$ tales que $\alpha^n = \beta\,\gamma$ y $\langle\alpha\rangle + \langle\beta\rangle = \mathbb{O}_d$. Entonces existen $\beta_1, \gamma_1 \in \mathbb{O}_d$ y $\mu_1, \mu_2 \in U(\mathbb{O}_d)$ tales que $\beta = \beta_1^n\,\mu_1$ y $\gamma = \gamma_1^n\,\mu_2$.* □

Existen otros ejemplos de anillos o monoides sin factorización única, algunos ejemplos de esto se pueden consultar en [7].

En cualquier anillo donde sea posible la factorización en irreducibles (por ejemplo $\mathbb{O}_d$), cualquier elemento primo es irreducible pero no necesariamente irreducible implica primo. Así tenemos:

TEOREMA 8. *En un dominio entero en donde la factorización en irreducibles es posible, la factorización es única si y sólo si los elementos irreducibles son primos.*

Demostración. Ver Teorema 4.13 [10]. □

Más adelante estudiaremos esto con más detalle

4. Solución de ecuaciones diofantinas

4.1. **Ecuación de Catalan.** En 1844 el matemático belga Eugene Catalan, en una carta enviada al editor de la revista alemana *Journal für die reine und angewandte Mathematik*, se preguntaba sobre la posibilidad de que dos números consecutivos pudieran ser potencias perfectas. En otras palabras, el afirmaba que las únicas soluciones enteras de la ecuación:

$$x^u - y^w = \pm 1$$

son $x = 3, y = 2, u = 2, w = 3$. Este problema quedó sin resolver durante muchos años. Ahora sabemos que el matemático rumano Prida Mihăilescu ha resuelto esta importante conjetura ([5] y [6]). Si suponemos que los exponentes son $u = 2$ y $w = 3$, tenemos una versión débil de la ecuación de Catalan.

Usando argumentos de divisibilidad se puede mostrar que la ecuación $x^2 - y^3 = 1$ tiene una única solución en los enteros positivos: $x = 3,\ y = 2$. En efecto, pues si x es par, entonces m.c.d. $(x - 1, x + 1) = 1$ y podemos escribir $(x - 1)(x + 1) = y^3$. Por tanto

$$x - 1 = a^3 \quad \text{y} \quad x + 1 = b^3.$$

De lo anterior se sigue que $b^3 - a^3 = (b - a)(b^2 + ab + b^2) = 2$ y así $b^2 + ab + b^2 \mid 2$, lo cual es imposible. Por lo tanto, si existiera solución, $x = 2t + 1$ y $y = 2q$ con $t, q \geq 1$. Es claro que $t = 1$ implica $x = 3$ y $y = 2$. Si $t > 1$, tendríamos $t(t + 1) = (2q)^3$, un número triangular que es un cubo, lo cual no es posible.

Ahora consideremos la ecuación $x^2 - y^3 = -1$, la cual afirmamos, tiene como única solución entera $y = 1$ y $x = 0$. En efecto, tenemos la factorización:

$$y^3 = (x + i)(x - i)$$

lo que nos sugiere trabajar en el anillo de los enteros gaussianos $\mathbb{Z}[i] = \mathbb{O}_{-1}$, el cual es de factorización única y como ya mencionamos, $U(\mathbb{Z}[i]) = \{\pm 1, \pm i\}$. Primero notemos que m.c.d. $(x + i, x - i) = 1$. Así que $x + i = (a + bi)^3$ y $x - i = (a - bi)^3$, salvo unidades. Se observa que $x + i = (a^3 - 3ab^2) + (3a^2b - b^3)i$ y por tanto $x - i = (a^3 - 3ab^2) - (3a^2b - b^3)i$. Igualando parte real e imaginaria tenemos $3a^2b - b^3 = b(3a^2 - b^2) = 1$, de donde $b \mid 1$ y así $b = \pm 1$. El caso $b = 1$ claramente no es posible. El caso $b = -1$ conduce a $y = 1$ y $x = 0$. En suma, la táctica consistió en ir a otro anillo en dónde la aritmética es más apropiada para encontrar la solución. ¿Cuál es la más apropiada? Es difícil saberlo, simplemente reconocer un anillo con factorización única es un problema que ocupa parte de las investigaciones en teoría de números.

4.2. **Ecuación de Bachet.** Antes de Catalan, el matemático francés Claude Gaspar Bachet (1581-1638) se preguntaba cuántas soluciones enteras tiene la ecuación $x^2 - y^3 = k$ con $k \in \mathbb{Z}$. Existen técnicas elementales para dar respuesta a la existencia de soluciones para ciertos valores de k. El caso que sirve para nuestro propósito es $x^2 - y^3 = -19$. Debido a la factorización $x^2 + 19 = (x + \sqrt{-19})(x - \sqrt{-19}) = y^3$, podríamos trabajar en el anillo $\mathbb{Z}[\sqrt{-19}] = \{a + b\sqrt{-19} : a, b \in \mathbb{Z}\}$, el cuál es un subanillo de índice 2 en el anillo $\mathbb{O}_{-19}$. Es conocido que el anillo $\mathbb{O}_{-19}$ tiene la propiedad de la factorización única por la clasificación de H. Stark que ya comentamos. Tenemos las siguientes consideraciones:

1. $U(\mathbb{Z}[\sqrt{-19}]) = \{\pm 1\}$ pues $N(a + b\sqrt{-19}) = a^2 + 19b^2 = 1$ si y sólo si $b = 0$ y $a = \pm 1$. Notemos que cualquier unidad es un cubo.
2. Si $19 \mid y$, entonces $19 \mid y^3$ y $19 \mid x$. Así $x^2 - y^3 = 19^2 q = -19$. Por tanto $19 \nmid y$.
3. Si $2 \mid y$, entonces x es impar y $8 \mid y^3$. Por tanto $x^2 \equiv y^3 - 19 \equiv -1 \pmod 8$, lo cual es imposible.
4. Sea $\pi \in \mathbb{Z}[\sqrt{-19}]$ un divisor irreducible común de $x + \sqrt{-19}$ y $x - \sqrt{-19}$. Entonces $\pi \mid 2\sqrt{-19}$ y por tanto $\pi \mid 2\sqrt{-19}\sqrt{-19}$. Así, $\pi \mid (2)(19)$ y $\pi \mid y^3$. Como $1 = ry^3 + (2)(19)s$ en $\mathbb{Z}$, entonces $\pi \mid 1$ y por tanto m.c.d. $\big(x + \sqrt{-19}, x - \sqrt{-19}\big) = 1$ en $\mathbb{Z}[\sqrt{-19}]$.
5. De la factorización $y^3 = (x + \sqrt{-19})(x - \sqrt{-19})$ y usando el Corolario 7 podemos suponer que $x + \sqrt{-19}$ y $x - \sqrt{-19}$ son cubos, salvo por una unidad.

Supongamos que $x + \sqrt{-19} = (a + b\sqrt{-19})^3$ para ciertos $a, b \in \mathbb{Z}$. Igualando parte real e imaginaria tenemos el sistema

$$x = a^3 - 57\, a\, b^2$$
$$1 = 3\, a^2\, b - 19\, b^3$$

La primera ecuación no aporta mucho; sin embargo la segunda ecuación nos indica que $b \mid 1$ y así $b = \pm 1$. Cualquiera que sea el valor de b implica que $a \notin \mathbb{Z}$. Con todo lo anterior podemos concluir que la ecuación $x^2 - y^3 = -19$ no es soluble en $\mathbb{Z}$. Pero observemos que $18^2 - 7^3 = -19$. ¿ Qué hicimos mal? ¿cómo explicamos esto? Bueno, parte de la respuesta es que es falso que si el anillo $\mathbb{O}_d$ es de factorización única, entonces cualquier subanillo debe tener la misma propiedad. Así, el subanillo $\mathbb{Z}[\sqrt{-19}]$ no es de factorización única. Por ejemplo

$$35 = 5 \cdot 7 = (4 + \sqrt{-19})(4 - \sqrt{-19}).$$

Se puede probar sin mucha dificultad y con la ayuda de la función norma que los números $5, 7, 4 + \sqrt{-19}, 4 - \sqrt{-19}$ son irreducibles en $\mathbb{Z}[\sqrt{-19}]$ y no son primos ni asociados dos a dos. Por ejemplo, 5 es irreducible y no primo. Si $5 = \alpha\, \beta$, entonces

$$25 = N(\alpha)N(\beta)$$

y por tanto $N(\alpha) = N(\beta) = 5$ ó $N(\alpha) = 25$ y $N(\beta) = 1$. El primer caso no es posible pues obviamente la ecuación $a^2 + 19b^2 = 5$ no tiene solución en $\mathbb{Z}$. En el segundo caso tenemos que $\beta \in U(\mathbb{Z}[\sqrt{-19}])$ y 5 es irreducible. ¿Por qué 5 no es primo en $\mathbb{Z}[\sqrt{-19}]$? Claramente $5 \mid (4 + \sqrt{-19})(4 - \sqrt{-19})$. Si $5 \mid 4 + \sqrt{-19}$, entonces

$$4 + \sqrt{-19} = 5(a + b\sqrt{-19}) = 5a + 5b\sqrt{-19}.$$

Por tanto $5 \mid 4$ en $\mathbb{Z}$ lo cual es imposible. Similarmente $5 \nmid 4 - \sqrt{-19}$ y 5 no es primo. Este ejemplo es testimonio del Teorema 8.

Si escribimos $x + \sqrt{-19} = \Big(\dfrac{a + b\sqrt{-19}}{2}\Big)^3$ y seguimos las mismas ideas se puede concluir que las soluciones de $x^2 - y^3 = -19$ son $x = \pm 8, y = 7$. Notemos que ahora estamos trabajando en el anillo $\mathbb{O}_{-19}$ en lugar de $\mathbb{Z}[\sqrt{-19}]$.

Como dato histórico, Bachet es más conocido por su traducción al latín del texto griego de Diofanto en 1621. Esta versión es la que utilizó Fermat como libro de notas en donde escribió su famosa afirmación.

5. El grupo de clases de ideales y solución de ecuaciones diofantinas

Cuando no se tiene la factorización única se puede recurrir a la factorización única con respecto a ideales. Consideremos el anillo $\mathbb{O}_d$ y el monoide:

$$G = \{I \neq 0 : I \text{ es ideal de } \mathbb{O}_d\}.$$

Definimos la siguiente relación $\sim$ en G: Para $I, J \in G$, $I \sim J$ si existen $\alpha, \beta \in \mathbb{O}_d \setminus \{0\}$ tal que $(\alpha)I = (\beta)J$, donde (α) es el ideal principal generado por α. Se sabe que:

1.- $\sim$ es de equivalencia.
2.- El conjunto de clases de equivalencia es finito.
3.- El conjunto de clases de equivalencia tiene estructura de grupo abeliano, el cual denotamos por $\mathbb{G}$. La operación es la natural: $[I][J] = [IJ]$.
4.- El orden h_d del grupo $\mathbb{G}$ satisface: $h_d = 1$ si y sólo si $\mathbb{O}_d$ es de factorización única.

Obviamente cualquier ideal principal está relacionado con el ideal $\mathbb{O}_d = \langle 1 \rangle$ y en particular, el neutro del grupo $\mathbb{G}$ es la clase $[\langle 1 \rangle]$. Así por ejemplo, el grupo de clases de ideales de $\mathbb{O}_{-5}$ es:

$$\mathbb{G} = \{[\langle 1 \rangle], [\langle 3, 1 + \sqrt{-5} \rangle]\}.$$

El grupo de clases de ideales del anillo $\mathbb{O}_{-14}$ es:

$$\mathbb{G} = \{[\langle 1 \rangle], [\langle 2, -\sqrt{-14} \rangle], [\langle 3, 1 + \sqrt{-14} \rangle], [\langle 3, 1 - \sqrt{-14} \rangle]\},$$

y en los anillos $\mathbb{O}_{-5}$ y $\mathbb{O}_{-14}$ no hay factorización única. La pregunta que nos hacemos ahora es ¿cómo se calcula el orden de éstos grupos? La respuesta es que es muy difícil encontrar h_d y la razón es porque algunas fórmulas que se conocen involucran a la función ζ de Riemann y otras involucran el cálculo de unidades fundamentales (ϵ_d, $d > 0$), como en nuestro caso. Por ejemplo, para calcular la unidad fundamental se debe resolver la ecuación $x^2 - dy^2 = \pm 1$ y esto requiere de las fracciones continuas. Una vez encontrada la unidad fundamental, se puede recurrir por ejemplo, a la fórmula

$$h_d = \frac{\sqrt{d}}{2\epsilon_d} L(1, \chi_d),$$

donde L es una L-serie de Dirichlet.

También existen fórmulas explícitas para el caso cuadrático. Por ejemplo Dirichlet descubrió que si $p \equiv 3 \pmod 4$ es un primo y $\mathbb{F} = \mathbb{Q}(\sqrt{-p})$, entonces

$$h_{-p} = \frac{1}{p}\Big(\sum r_i - \sum s_i\Big),$$

donde $\sum r_i$ es la suma de los residuos cuadráticos y $\sum s_i$ es la suma de los residuos no cuadráticos en $\mathbb{F}_p$.

El producto de dos ideales principales es principal y si I satisface

$$\langle \alpha \rangle I = \langle \beta \rangle$$

para ciertos $\alpha, \beta \in \mathbb{O}_d \setminus \{0\}$, entonces I también es un ideal principal.

Para cualquier anillo cuadrático consideremos el monoide G de ideales $\neq 0$ de $\mathbb{O}_d$. Como sabemos, G tiene la propiedad de la factorización única en términos de ideales primos. Usaremos esta cualidad para decidir si cierta clase de ecuaciones diofantinas es soluble en $\mathbb{Z}$.

Teorema 9. *Sean $d > 1$ un entero que no es un cuadrado, $d \equiv 1, 2 \pmod 4$, $F = \mathbb{Q}(\sqrt{-d})$ con anillo de enteros $\mathbb{O}_{-d}$ y el orden de las clases de ideales de $\mathbb{O}_{-d}$ es igual a h_{-d}. Si $p^{2m} \nmid d$ para todo primo $p \mid d$ y $n \geq 2m$ con $n, m \in \mathbb{Z}$, de tal forma que* m.c.d. $(n, h_{-d}) = 1$ *y* m.c.d. $(d, n) \neq 1$, *entonces*

$$y^n = x^{2m} + d \tag{1}$$

no tiene solución en los enteros x, y.

Demostración. Supongamos que x, y es una solución de la ecuación (1). Si $d = d_1 d_2^2$ con d_1 libre de cuadrados, $\mathbb{O}_{-d} = \mathbb{Z}[\sqrt{-d_1}]$. En este anillo, la ecuación (1) se puede reescribir como

$$y^n = (x^m + \sqrt{-d})(x^m - \sqrt{-d}).$$

La factorización única no se cumple en $\mathbb{O}_{-d}$ a menos que $h_{-d} = 1$, así que la transformaremos en una ecuación de ideales:

$$\langle y \rangle^n = \langle x^m + \sqrt{-d} \rangle \langle x^m - \sqrt{-d} \rangle. \tag{2}$$

Primero demostremos que $\langle x^m + \sqrt{-d} \rangle$ y $\langle x^m - \sqrt{-d} \rangle$ son ideales primos relativos entre sí, esto es, no existe un ideal primo en $\mathbb{O}_{-d}$ que los divida a ambos.

El primer paso para probar la afirmación anterior es ver que x y d son primos relativos en $\mathbb{Z}$. Supongamos que existe un primo p tal que $p \mid x$ y $p \mid d$. Como $y^n = x^{2m} + d$, entonces $p \mid y^n$ y así $p \mid y$. De lo anterior, tenemos que $p^n \mid y^n = x^{2m} + d$. $p^{2m} \mid x^{2m}$ y $p^{2m} \mid x^{2m} + d$ implica que $p^{2m} \mid d$, lo que es una contradicción, pues $p^{2m} \nmid d$. Por lo tanto m.c.d. $(x, d) = 1$.

Ahora demostraremos que $x^{2m} + d$ y $x^{2m} - d$ son primos relativos en $\mathbb{Z}$. Si existiera un primo p tal que $p \mid$ m.c.d. $\left(x^{2m} + d, x^{2m} - d\right)$, entonces

$$p \mid 2x^{2m} = (x^{2m} + d) + (x^{2m} - d) \text{ y}$$

$$p \mid 2d = (x^{2m} + d) - (x^{2m} - d).$$

Como m.c.d. $(x, d) = 1$, entonces $p = 2$. Observemos que x y d deben ser impares, pues $2 \mid x^{2m} + d$ y m.c.d. $(x, d) = 1$, y como $d \equiv 1 \pmod 4$ tendremos que $x^{2m} + d \equiv 2 \pmod 4$. Pero entonces y es par, lo que implica que $y^n \equiv 0 \pmod 4$; y así no existe el primo p. Por lo tanto m.c.d. $\left(x^{2m} + d, x^{2m} - d\right) = 1$.

Finalmente, tenemos que ver que $\langle x^m + \sqrt{-d} \rangle + \langle x^m - \sqrt{-d} \rangle = \mathbb{O}_{-d}$, para concluir que efectivamente son primos relativos.

Sean $a, c \in \mathbb{Z}$ tales que $a(x^{2m} - d) + c(x^{2m} + d) = 1$. Si $b = ax^m + cx^m$, entonces

$$(a\sqrt{-d})(x^m + \sqrt{-d}) + (b + c\sqrt{-d})(x^m - \sqrt{-d}) =$$

$$(a\sqrt{-d})(x^m + \sqrt{-d}) + (ax^m + cx^m + c\sqrt{-d})(x^m - \sqrt{-d}) =$$

$$ax^m\sqrt{-d} - ad + ax^{2m} + cx^{2m} + cx^m\sqrt{-d} - ax^m\sqrt{-d} - cx^m\sqrt{-d} + cd =$$

$$a(x^{2m} - d) + c(x^{2m} + d) = 1.$$

Como

$$(a\sqrt{-d})(x^m + \sqrt{-d}) \in \langle x^m + \sqrt{-d} \rangle \text{ y}$$

$$(b + c\sqrt{-d})(x^m - \sqrt{-d}) \in \langle x^m - \sqrt{-d} \rangle,$$

entonces efectivamente los ideales son primos relativos. Con esto concluimos nuestra primera afirmación.

Como los ideales se factorizan de forma única, el hecho de que $\langle x^m + \sqrt{-d} \rangle$ y $\langle x^m - \sqrt{-d} \rangle$ son primos relativos junto con (2), implica que existen I y J, ideales de $\mathbb{O}_{-d}$, tales que

$$I^n = \langle x^m + \sqrt{-d} \rangle \text{ y}$$

$$J^n = \langle x^m - \sqrt{-d} \rangle.$$

Por hipótesis, m.c.d. $(n, h_{-d}) = 1$, por lo que existe $k \in \mathbb{Z}$ tal que $kn \equiv 1 \pmod{h_{-d}}$. Sea r tal que $kn = h_{-d}r + 1$. Entonces

$$I^{kn} = I^{h_{-d}r+1} = \langle \alpha \rangle I = \langle x^m + \sqrt{-d} \rangle^k = \langle (x^m + \sqrt{-d})^k \rangle.$$

Por esto, I debe de ser un ideal principal, digamos $I = \langle a + b\sqrt{-d} \rangle$. De lo anterior,

$$\langle x^m + \sqrt{-d} \rangle = I^n = \langle (a + b\sqrt{-d})^n \rangle,$$

y entonces $x^m + \sqrt{-d}$ debe de ser un asociado de $(a + b\sqrt{-d})^n$ en $\mathbb{O}_{-d}$. El grupo de unidades es $\{\pm 1\}$, pues $d_1 \neq 1, 3$, así que:

$$x^m + \sqrt{-d} = (a + b\sqrt{-d})^n = \pm \sum_{i=0}^{n} \binom{n}{i} a^{n-i} (b\sqrt{-d})^i = a' + b'\sqrt{d}.$$

Como $1 \neq \text{m.c.d.}\,(d, n) \mid \binom{n}{i}$ para $1 < i < n$ y d divide al último término de la suma (pues $n \geq 2$), entonces $\text{m.c.d.}\,(d, n) \mid b'$. Pero $b' = 1$; por lo que tenemos una contradicción, que significa que la suposición de que existen $x, y \in \mathbb{Z}$ es falsa, así que la ecuación (1) no tiene solución. □

Nota: Si n es par, el n-ésimo término de la suma corresponde a a', por lo que la condición de que $\text{m.c.d.}\,(d, n) \neq 1$ no es necesaria; en este caso, lo único que cambia es que en lugar de afirmar que $d \mid b'$ (en el último párrafo de la demostración) diremos que $n \mid b'$. Por lo tanto, también es cierto que:

TEOREMA 10. *Sean $d > 1$ un entero que no es un cuadrado, $d \equiv 1, 2 \pmod 4$ y $F = \mathbb{Q}(\sqrt{-d})$ con anillo de enteros $\mathbb{O}_{-d}$. Si $p^{2m} \nmid d$ para todo primo $p \mid d$ y $2n \geq 2m$ es un entero que cumple $\text{m.c.d.}\,(2n, h_{-d}) = 1$, con $n, m \in \mathbb{Z}$, entonces*

$$y^{2n} = x^{2m} + d$$

no tiene solución. □

Estas ideas también pueden usarse cuando hay soluciones, por ejemplo, resolvamos la siguiente ecuación:

$$y^3 = x^4 + 44 = (x^2 + \sqrt{-44})(x^2 - \sqrt{-44}) = (x^2 + 2\sqrt{-11})(x^2 - 2\sqrt{-11}).$$

Escribiendo la ecuación como ideales de $\mathbb{O}_{-11}$ tenemos:

$$\langle y \rangle^3 = \left\langle x^2 + 2\sqrt{-11} \right\rangle \left\langle x^2 - 2\sqrt{-11} \right\rangle.$$

Por la factorización única de ideales, existen $I, J \subseteq \mathbb{O}_{-11}$ tales que

$$\left\langle x^2 + 2\sqrt{-11} \right\rangle = I^3 \quad \text{y} \quad \left\langle x^2 - 2\sqrt{-11} \right\rangle = J^3.$$

Como $\mathbb{O}_{-11}$ es uno de los anillos de la lista de H. Stark, entonces I y J son principales. Supongamos $I = \left\langle \dfrac{a + b\sqrt{-11}}{2} \right\rangle$ con $a, b \in \mathbb{Z}$, $a \equiv b \pmod 2$, entonces

$$\left(\frac{a + b\sqrt{-11}}{2} \right)^3 = \frac{(a^3 - 33\,a\,b^2) + \sqrt{-11}(3\,a^2\,b - 11\,b^3)}{8} = \pm(x^2 + 2\sqrt{-11}).$$

Igualando términos, la ecuación anterior nos indica que tenemos que resolver el sistema

$$\begin{aligned} \pm 2 &= \frac{3\,a^2\,b - 11\,b^3}{8} = \frac{b(3\,a^2 - 11\,b^2)}{8}, \\ \pm x^2 &= \frac{a^3 - 33\,a\,b^2}{8}, \end{aligned} \tag{3}$$

de donde la primera ecuación se puede reescribir como $\pm 16 = b(3\,a^2 - 11\,b^2)$. Como en cualquier caso $b \mid 16$, entonces las posibilidades para b son ± 1, ± 2, ± 4, ± 8, ± 16. En cada uno de estos casos se obtiene:

$$\begin{array}{ll} b = 1 & \pm 16 = (1)(3\,a^2 - 11) \\ b = -1 & \pm 16 = (-1)(3\,a^2 - 11) \\ b = 2 & \pm 16 = (2)(3\,a^2 - 44) \\ b = -2 & \pm 16 = (-2)(3\,a^2 - 44) \\ b = 4 & \pm 16 = (4)(3\,a^2 - 176) \\ b = -4 & \pm 16 = (-4)(3\,a^2 - 176) \\ b = 8 & \pm 16 = (8)(3\,a^2 - 704) \\ b = -8 & \pm 16 = (-8)(3\,a^2 - 704) \\ b = 16 & \pm 16 = (16)(3\,a^2 - 2816) \\ b = -16 & \pm 16 = (-16)(3\,a^2 - 2816). \end{array}$$

De esta forma, resolver la ecuación diofantina se convierte en resolver veinte polinomios cuadráticos con una variable, lo que es mucho más sencillo. Además, observemos que los dos polinomios del primer renglón son los negativos de los dos polinomios del segundo renglón y así sucesivamente, de tal forma que únicamente hay que encontrar las soluciones de diez polinomios cuadráticos: $0 = 3\,a^2 - 27$ con soluciones ± 3 y $0 = 3\,a^2 + 5$, $0 = 3\,a^2 - 52$, $0 = 3\,a^2 - 36$, $0 = 3\,a^2 - 180$, $0 = 3\,a^2 - 172$, $0 = 3\,a^2 - 706$, $0 = 3\,a^2 - 702$, $0 = 3\,a^2 - 2817$, $0 = 3\,a^2 - 2815$, cuyas soluciones no son enteras. Como podemos ver, los únicos valores en $\mathbb{Z}$ que puede tomar a son ± 3, y esto solamente sucede si $b = \pm 1$. Regresando a la ecuación (3),

$$\pm x^2 = \pm \frac{27 - 99}{8} = \pm 9,$$

de donde x solamente puede ser ± 3. Sin importar el signo, $y^3 = x^4 + 44 = 81 + 44 = 125$. De esta forma, vemos que la ecuación tiene exactamente dos soluciones: $x = 3, y = 5$ y $x = -3, y = 5$.

Referencias

[1] Alaca, S., Williams, K. S., *Introductory Algebraic Number Theory*, Cambridge University Press, 2004.

[2] Halter-Koch, F., *Ideal systems. An introduction to multiplicative ideal theory*, Monographs and Textbooks in Pure and Applied Mathematics, **211**. Marcel Dekker, Inc., New York, 1998.

[3] Ireland K., Rosen M., *A Classical Introduction to Modern Number Theory*, Springer-Verlag, GTM **84**, 2a edición, (1990).

[4] Lothaire, M., *Combinatorics on words*, Cambridge Mathematical Library. Cambridge University Press, Cambridge, 1997.

[5] Mihăilesku, P., *Primary cyclotomic units and a proof of Catalan's conjeture*. J. Reine Angew. Math. **572** (2004), 167-195.

[6] Mihăilesku, P., *On the class groups of cyclotomic extensions in presence of a solution to Catalan's equation*. J. Number Theory **118** (2006), no.1, 123-144.

[7] Pineda-Ruelas, M., Primo y/o irreducible, *Carta Informativa*, No. 54, México, Octubre, 2007.

[8] Ribenboim, P., *Clasical theory of algebraic numbers*, Springer-Velag, UTX, (2001).

[9] Stark, H., On complex quadratic fields with class number equal to one, *Trans. Amer. Math. Soc.*, **122**, 1966, 112-119.

[10] Stewart I., Tall D., *Algebraic Number Theory and Fermat's Last Theorem*, A K Peters, 3rd edition, (2001).

Dirección del autor:
Alejandro Aguilar-Zavoznik
Universidad Autónoma Metropolitana,
Unidad Azcapotzalco,
División de Ciencias Básicas e Ingeniería,
Departamento de Ciencias Básicas.
Av. San Pablo 180, Col. Reynosa Tamaulipas
Del. Azcapotzalco, C.P. 02200 México, D.F.
e-mail: `aaz@correo.azc.uam.mx`

Mixba'al
Revista Metropolitana de Matemáticas
No. 1, Vol. IV, junio de 2013, 39–51

GENERALIZACIÓN DE ALGUNOS CRITERIOS PARA POLINOMIOS SEMI-ESTABLES

CARLOS ARTURO LOREDO VILLALOBOS EDGAR CRISTIAN DÍAZ GONZÁLEZ
BALTAZAR AGUIRRE HERNÁNDEZ

Resumen. La estabilidad de un sistema lineal $\dot{x} = Ax$ se verifica por medio de su polinomio característico asociado $p_A(t)$. Si el polinomio es semi-estable se puede asegurar la estabilidad del sistema y si es estable se puede asegurar la estabilidad asintótica del sistema. En este trabajo presentamos algunas condiciones necesarias para verificar si un polinomio real es semi-estable, además de algunas generalizaciones del criterio de Hermite-Biehler aplicables a polinomios no necesariamente estables.

1. Introducción

En el estudio de la distribución de las raíces de un polinomio sobre el plano complejo, uno de los primeros problemas fue el de determinar el número de raíces reales de una ecuación; esto es, dada una ecuación de coeficientes reales, determinar (por algún criterio, que dependerá de sus coeficientes, y sin resolver la ecuación) si tiene raíces reales, en caso afirmativo, cuántas; o cuántas raíces positivas y cuántas negativas tiene. Decimos que un polinomio $p \in \mathbb{R}[x]$ es estable si todas sus raíces se encuentran en $\mathbb{C}^-$, donde $\mathbb{C}^-$ es el conjunto de números complejos que tienen parte real negativa. Se conocen los criterios clásicos de Routh-Hurwitz (tal vez, el más conocido), el criterio de Routh y Hermite-Biehler que dan condiciones necesarias y suficientes para que un polinomio sea estable. Se pueden consultar otros criterios para saber si un polinomio es polinomio Hurwitz en [3] o [10], recientemente han aparecido resultados relativos a polinomios semi-estables [5]. Decimos que un polinomio $p \in \mathbb{R}[x]$ es semi-estable si sus raíces están en $\mathbb{C}^- \cup i\mathbb{R}$. Esto implica que los polinomios estables son un subconjunto de los polinomios semi-estables. En las siguientes secciones mostraremos algunas condiciones para que un polinomio sea semi-estable, además de algunos criterios acerca de la distribución de sus raíces en el plano complejo.

2. El enfoque de Routh-Hurwitz para polinomios semi-estables

Consideremos el polinomio real $p \in \mathbb{R}[x]$:

$$p(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n \tag{1}$$

con $a_0 \neq 0$, denotamos por $H(p)$ a la matriz de Hurwitz asociada a p, la cual queda definida como

$$H(p) = \begin{pmatrix} a_1 & a_3 & a_5 & \cdots & 0 \\ a_0 & a_2 & a_4 & \cdots & 0 \\ 0 & a_1 & a_3 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & a_n \end{pmatrix}$$

Denotemos por Δ_i, $1 \leq i \leq n$, los menores principales diagonales de $H(p)$, es decir

$$\Delta_1 = a_1, \Delta_2 = \det \begin{pmatrix} a_1 & a_3 \\ a_0 & a_2 \end{pmatrix}, \ldots, \Delta_n = \det H(p)$$

El criterio de Routh-Hurwitz se puede consultar en [1], [8] y [9].

PROPOSICIÓN 1. *Considérese el polinomio real*

$$p(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n, \quad a_n > 0 \tag{2}$$

Si $p(x)$ es semi-estable entonces

$$\Delta_1 \geq 0,\ \Delta_2 \geq 0,\ \ldots, \Delta_n \geq 0$$

Demostración: Sea $p(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n$ un polinomio real semi-estable con $a_n > 0$. Podemos reescribir a $p(x)$ de la siguiente forma $p(x) = a_0(x - r_1)(x - r_2)\cdots(x - r_n)$, entonces se tiene que $\mathrm{Re}(r_i) \leq 0$ para toda $i = 1, \ldots, n$. Ahora considérese la sucesión de polinomios

$$p_k(x) = a_0(x + \frac{1}{k} - r_1)(x + \frac{1}{k} - r_2)\cdots(x + \frac{1}{k} - r_n)$$

con $k = 1, 2, \ldots$. Nótese que $p_k(x) \to p(x)$ cuando $k \to \infty$. Entonces $p_k(x)$ es estable para todo k pues $\mathrm{Re}\left(-\frac{1}{k} + i\right) < 0$ para todo $i = 1, \ldots, n$.

Denotemos por Δ_i^k, $1 \leq i \leq n$ a los menores diagonales principales de $H(p_k)$. Ya que $p_k(x)$ es estable entonces $\Delta_1^k > 0$, $\Delta_2^k > 0$, $\ldots$, $\Delta_n^k > 0$. Tomando el límite cuando $k \to \infty$ se tiene que $\Delta_1 \geq 0$, $\Delta_2 \geq 0$, $\ldots$, $\Delta_n \geq 0$. □

COROLARIO 2. *Si $H(p)$ es la matriz de Hurwitz asociada al polinomio $p(x)$ y si existe al menos un menor principal $\Delta_i < 0$, para algún $i = 1, \ldots, n$, entonces $p(x)$ no es semi-estable.*

Ejemplo 1. Considérese el polinomio real $p(t) = t^3 + t^2 + t + 3$. La matriz de Hurwitz asociada es:

$$H(p) = \begin{pmatrix} a_1 & a_3 & a_5 \\ a_0 & a_2 & a_4 \\ 0 & a_1 & a_3 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 3 \end{pmatrix}$$

Tenemos que $\Delta_1 > 0$, $\Delta_2 < 0$ y $\Delta_3 < 0$. Por lo tanto, $p(t)$ no es semi-estable.

3. El enfoque de Routh para polinomios semi-estables

En 1875 Edward J. Routh, usando el *Teorema de Sturm* y la teoría de *índices de Cauchy*, elabora un algoritmo para determinar el número k de raíces con parte real positiva de un polinomio real (ver [11]). En el caso particular cuando $k = 0$ este algoritmo proveé un criterio de estabilidad. Una demostración de este criterio se desarrolla en [4]. Consideremos el polinomio real

$$f(z) = a_0z^n + b_0z^{n-1} + a_1z^{n-2} + b_1z^{n-3} + \ldots \qquad (a_0 \neq 0)$$

Entonces

$$f(i\omega) = a_0(i\omega)^n + b_0(i\omega)^{n-1} + a_1(i\omega)^{n-2} + b_1(i\omega)^{n-3} + \ldots$$

Tomemos

$$f_1(\omega) = a_0\omega^n - a_1\omega^{n-2} + \ldots$$

$$f_2(\omega) = b_0\omega^{n-1} - b_1\omega^{n-3} + \ldots$$

y construimos una sucesión generalizada de Sturm

$$f_1(\omega),\ f_2(\omega),\ f_3(\omega),\ \ldots,\ f_m(\omega)$$

por medio del algoritmo de Euclides. Entonces

$$\begin{aligned} f_3(\omega) &= \frac{a_0}{b_0}\omega f_2(\omega) - f_1(\omega) \\ &= c_0\omega^{n-2} - c_1\omega^{n-4} + c_2\omega^{n-6} - \ldots \end{aligned}$$

donde

$$
\begin{aligned}
c_0 &= a_1 - \frac{a_0}{b_0}b_1 = \frac{b_0a_1 - a_0b_1}{b_0}, \\
c_1 &= a_2 - \frac{a_0}{b_0}b_2 = \frac{b_0a_2 - a_0b_2}{b_0}, \\
c_2 &= a_3 - \frac{a_0}{b_0}b_3 = \frac{b_0a_3 - a_0b_3}{b_0}, \\
&\vdots
\end{aligned} \tag{3}
$$

Análogamente

$$
\begin{aligned}
f_4(\omega) &= \frac{b_0}{c_0}\omega f_3(\omega) - f_2(\omega) \\
&= d_0\omega^{n-3} - d_1\omega^{n-5} + d_2\omega^{n-7} - \dots
\end{aligned}
$$

$$
\begin{aligned}
d_0 &= b_1 - \frac{b_0}{c_0}c_1 = \frac{c_0b_1 - b_0c_1}{c_0}, \\
d_1 &= b_2 - \frac{b_0}{c_0}c_2 = \frac{c_0b_2 - b_0c_2}{c_0}, \\
d_2 &= b_3 - \frac{b_0}{c_0}c_3 = \frac{c_0b_3 - b_0c_3}{c_0}, \\
&\vdots
\end{aligned} \tag{4}
$$

Los coeficientes de los polinomios restantes $f_5(\omega), f_6(\omega), \dots, f_{n+1}(\omega)$ se determinan de manera similar. Con dichos coeficientes formamos el llamado *esquema de Routh*:

$$
\left.
\begin{array}{cccc}
a_0, & a_1, & a_3, & \dots \\
b_0, & b_1, & b_3, & \dots \\
c_0, & c_1, & c_3, & \dots \\
d_0, & d_1, & d_3, & \dots \\
\vdots & \vdots & \vdots &
\end{array}
\right\} \tag{5}
$$

Las fórmulas (3) y (4) muestran cómo obtener cada fila de este esquema.

Teorema 3 (Routh). *El número de raíces de un polinomio real $f(z)$ en el semiplano derecho ($\operatorname{Re} z > 0$) es igual al número de variaciones de signo de la primera columna del esquema de Routh.*

Corolario 4 (Criterio de Routh). *Todas las raíces del polinomio real $f(z)$ tienen parte real negativa, si y sólo si, al realizar el algoritmo de Routh todos los elementos de la primera columna del esquema de Routh son diferentes de cero y del mismo signo.*

Cuando $f(z)$ tiene raíces sobre el eje imaginario escribimos

$$f(z) = F_1(z) + F_2(z)$$

donde

$$
\begin{aligned}
F_1(z) &= a_0z^n + a_1z^{n-2} + \cdots \\
F_2(z) &= b_0z^{n-1} + b_1z^{n-3} + \cdots
\end{aligned}
$$

Buscamos el máximo común divisor de $F_1(z)$ y $F_2(z)$, *i.e.* $d(z) = \operatorname{mcd}(F_1(z), F_2(z))$ y escribimos:

$$f(z) = d(z)f^*(z)$$

Si $f(z)$ tiene una raíz z en el eje imaginario, entonces $-z$ también será raíz. A partir de que $f(z) = f(-z) = 0$ se tiene que $F_1(z) = 0$ y $F_2(z) = 0$, es decir z es raíz de $d(z)$. Por lo tanto, $f^*(z)$ no tiene una raíz z para la cual $-z$ sea también raíz. Así, $d(z)$ tiene s raíces sobre el eje imaginario y $f^*(z)$ no tiene raíces imaginarias. En este caso el número k de raíces positivas es $k = k_1 + k_2$, donde k_1 y k_2 son el número de raíces

positivas de $f^*(z)$ y $d(z)$ respectivamente. Luego, k_1 puede determinarse mediante el algoritmo de Routh y

$$k_2 = \frac{q-s}{2}$$

donde $q = \text{grado}\,[d(z)]$ y s es el número de raíces reales de $d(i\omega)$.

PROPOSICIÓN 5. *Si $p(x)$ es semi-Hurwitz entonces se satisface sólo una de las siguientes propiedades:*

(1) Los elementos de primera columna del esquema de Routh son diferentes de cero y del mismo signo.

(2) Si $d(x) = mcd(F_1(x), F_2(x)) \neq 1$ entonces $q = s$, donde $q = grado\,[d(z)]$ y s es el número de raíces reales de $d(i\omega)$

Ejemplo 2. Verifiquemos si el polinomio $q(t) = t^5+t^4+2t^3+t^2+t+1$ es Hurwitz. Evaluamos q en $i\omega$

$$q(i\omega) = \omega^4 - \omega^2 + 1 + i(\omega^5 - 2\omega^3 + \omega)$$

Hacemos:

$$a_0 = 1,\ a_1 = 1,\ a_2 = 1$$
$$b_0 = 1,\ b_1 = 2,\ b_2 = 1$$

luego

$$c_0 = \frac{b_0a_1 - a_0b_1}{b_0} = \frac{1(1)-1(2)}{1} = -1$$
$$c_1 = \frac{b_0a_2 - a_0b_2}{b_0} = \frac{1(1)-1(1)}{1} = 0$$

$$d_0 = \frac{c_0b_1 - b_0c_1}{c_0} = \frac{-1(2)-1(0)}{-1} = 2$$
$$d_1 = \frac{c_0b_2 - b_0c_2}{c_0} = \frac{-1(1)-1(0)}{-1} = 1$$
$$e_0 = \frac{d_0c_1 - c_0d_1}{d_0} = \frac{(2)(0)-(-1)(1)}{2} = \frac{1}{2}$$
$$f_0 = \frac{e_0d_1 - d_0e_1}{e_0} = \frac{\frac{1}{2}(1)-2(0)}{\frac{1}{2}} = 1$$

a_0	a_1	a_3	1	2	0
b_0	b_1	b_3	1	2	0
c_0	c_1		-1	0	
d_0	d_1		2	1	
e_0			$\frac{1}{2}$		
f_0			1		

Obsérvese que los elementos de la primera columna del esquema de Routh no son del mismo signo. Por lo tanto, $q(t)$ no es Hurwitz.
Ahora verifiquemos si es semi-Hurwitz. Construimos

$$F_1(t) = t^5 + 2t^3 + t \qquad F_2(t) = t^4 + 2t^2 + 1$$

Luego, puede verificarse que $d(t) = \text{mcd}\,(F_1, F_2) = t^4 + 2t^2 + 1$, por lo que $q(t)$ es semi-Hurwitz.

4. Criterio de Hermite-Biehler para polinomios semi-estables

En esta sección daremos generalizaciones del criterio de Hermite-Biehler primero para polinomios semi-estables y después para polinomios sin ninguna restricción en la localización en sus raíces. Estas últimas generalizaciones son dadas en términos de una expresión analítica para la diferencia entre el número de raíces del polinomio en el semiplano abierto izquierdo y el semiplano abierto derecho.

4.1. **Criterio de Hermite-Biehler.** Para enunciar el Criterio de Hermite-Biehler utilizaremos las siguientes definiciones.

Considérese el polinomio real

$$p^*(z) = p_0 + p_1 z + p_2 z^2 + \cdots + p_n z^n$$

Podemos escribir a p^* de la siguiente forma

$$p^*(z) = (p_0 + p_2 z^2 + p_4 z^4 + \cdots) + z(p_1 + p_3 z^2 + p_5 z^4 + \cdots) \tag{6}$$

Evaluando en $i\omega$:

$$p^*(i\omega) = (p_0 - p_2\omega^2 + p_4\omega^4 - \cdots) + i\omega(p_1 - p_3\omega^2 + p_5\omega^4 - \cdots)$$

Definimos

$$p_e(z^2) = p_0 + p_2 z^2 + p_4 z^4 + \cdots \tag{7}$$

$$z \cdot p_o(z^2) = p_1 z + p_3 z^3 + p_5 z^5 + \cdots \tag{8}$$

$$p_e(-\omega^2) = p_0 - p_2\omega^2 + p_4\omega^4 - \cdots \tag{9}$$

$$p_o(-\omega^2) = p_1 - p_3\omega^2 + p_5\omega^4 - \cdots \tag{10}$$

Los polinomios (9) y (10) son polinomios reales o se convierten en polinomios reales después de cancelar i.

Definición 6 (Alternancia)**.** Un polinomio real $p^*(z)$ satisface la propiedad de la alternancia si

- **a):** los coeficientes principales de $p_e(z^2)$ y $zp_o(z^2)$ tienen el mismo signo y
- **b):** todas las raíces de $p_e(-\omega^2)$ y $p_o(-\omega^2)$ son reales, distintas y además las m raíces positivas de $p_e(-\omega^2)$ y las $m-1$ raíces positivas de $p_o(-\omega^2)$ se van alternando, es decir:

$$0 < \omega_{e,1} < \omega_{o,1} < \omega_{e,2} < \omega_{o,2} < \cdots$$

Para más detalles ver [2] y [4].

Teorema 7 (Hermite-Biehler). *Un polinomio real $p^*(z)$ es Hurwitz, si y sólo si, satisface la propiedad de la alternancia.*

Una versión en condiciones necesarias del criterio de Hermite-Biehler para polinomios semi-estables se da en la siguiente afirmación.

Proposición 8. *Si un polinomio real $p^*(z)$ es semi-estable entonces*

a) los coeficientes principales de $p_e(z^2)$ y $zp_o(z^2)$ tienen el mismo signo;
b) todas las raíces de $p_e(-\omega^2)$ y $p_o(-\omega^2)$ son reales y las raíces positivas de $p_e(-\omega^2)$ y $p_o(-\omega^2)$ cumplen que

$$0 \leq \omega_{e,1} \leq \omega_{o,1} \leq \omega_{e,2} \leq \omega_{o,2} \leq \ldots$$

Corolario 9. *Sea $p^*(z)$ un polinomio real, si los coeficientes de $p_e(z^2)$ y $zp_o(z^2)$ no tienen el mismo signo o si ocurriera que para algún $i = 1, \ldots, n$ las raíces positivas de $p_e(-\omega^2)$ y $p_o(-\omega^2)$ no se alternaran entonces $p(x)$ no es semi-estable.*

Ejemplo 3. Considérese el polinomio real $p^*(t) = t^4 + 2t^3 + 3t^2 + 7t + 2$.
Tenemos que

$$p_e(t^2) = 2 + 3t^2 + t^4, \quad tp_o(t^2) = 7t + 2t^3$$

Por otra parte

$$p^*(i\omega) = 2 - 3\omega^2 + \omega^4 + i\omega(7 - 2\omega^2)$$
$$p_e(-\omega^2) = 2 - 3\omega^2 + \omega^4, \quad p_o(-\omega^2) = 7 - 2\omega^2$$

Luego

$$p_e(-\omega^2) = 0 \;\Leftrightarrow\; \omega = \pm 1 \text{ ó } \omega = \pm\sqrt{2}$$
$$p_o(-\omega^2) = 0 \;\Leftrightarrow\; \omega = \pm\sqrt{7/2}$$

Hacemos $\omega_{e,1} = 1$, $\omega_{e,2} = \sqrt{2}$, $\omega_{o,1} = \sqrt{7/2}$. Ahora $\omega_{e,1} < \omega_{o,1}$, pero $\omega_{o,1} > \omega_{e,2}$. Por lo tanto no se cumple el inciso b) de la propiedad de la alternancia. Luego $p^*(t)$ no es semi-estable.

Un polinomio $p^* \in \mathbb{R}[x]$, no idénticamente cero, se dice que es estándar cuando su coeficiente principal es positivo. El siguiente resultado se obtiene como consecuencia del Teorema de Hermite-Biehler por un argumento de límite.

TEOREMA 10 ([14]). *Sea $p^*(x) = f(x^2) + xg(x^2) \in \mathbb{R}[x]$ un polinomio estándar. Entonces $p^*(x)$ es semi-estable, si y sólo si, tanto f como g son polinomios estándar, tienen sólo raíces reales no positivas y las raíces de f se alternan con las de g.*

4.2. **Relación entre polinomios estables y semi-estables.** El siguiente resultado, publicado en [5], establece la manera en que están relacionados los polinomios estables y semi-estables.

TEOREMA 11. *Sea $p^*(x) = f(x^2)+xg(x^2) \in \mathbb{R}[x]$ un polinomio estándar. Entonces $p^*(x)$ es estable, si y sólo si, $p^*(x)$ es semi-estable, $f(0) \neq 0$ y $mcd(f, g) = 1$.*

4.3. **Generalizaciones del Criterio de Hermite-Biehler.** Es esta subsección se dan otras generalizaciones del Teorema de Hermite-Biehler para polinomios no necesariamente Hurwitz en términos de una expresión que indica la diferencia entre las raíces que se encuentran en el semiplano complejo izquierdo y las raíces que se encuentran en el semiplano derecho. A continuación presentamos nuevamente el criterio de Hermite-Biehler.

TEOREMA 12. *(**Hermite-Biehler**). Sea $p^*(z) = p_0 + p_1 z + \cdots + p_n z^n$, un polinomio real de grado n. Escribimos, $p^*(z) = p_e(z^2) + zp_o(z^2)$, donde $p_e(z^2)$ y $zp_o(z^2)$ son las componentes de $p^*(z)$, formadas con las potencias pares e impares de z, respectivamente. Sean $\omega_{e_1}, \omega_{e_2}, \ldots$ los distintos ceros reales positivos de $p_e(-\omega^2)$ y sean $\omega_{o_1}, \omega_{o_2}, \ldots$ los distintos ceros reales positivos de $p_o(-\omega^2)$, ordenados en magnitud ascendente. Entonces $p^*(z)$ es Hurwitz estable, si y sólo si, todos los ceros de $p_e(-\omega^2)$, $p_o(-\omega^2)$, son reales y distintos, p_n y p_{n-1} son del mismo signo y los ceros reales positivos, satisfacen la siguiente propiedad de la alternancia:*

$$0 < \omega_{e_1} < \omega_{o_1} < \omega_{e_2} < \omega_{o_2} < \cdots \tag{11}$$

Ver [1], [2] y [9] para una demostración.

Ahora proporcionamos algunas caracterizaciones alternativas e interpretaciones del teorema. Para esto, introducimos primero la función $\operatorname{sgn}[\cdot] : \mathbb{R} \to \{-1, 0, 1\}$, definida por:

$$\operatorname{sgn}[\mathrm{x}] = \begin{cases} -1 & \text{si } x < 0, \\ 0 & \text{si } x = 0, \\ 1 & \text{si } x > 0. \end{cases}$$

LEMA 13. *Sea $p^*(z) = p_0 + p_1 z + \cdots + p_n z^n$, un polinomio real de grado n. Escribimos $p^*(z) = p_e(z^2) + zp_o(z^2)$, donde $p_e(z^2)$ y $zp_o(z^2)$ son las componentes de $p^*(z)$ formadas con las potencias pares e impares de z, respectivamente. Para cada $\omega \in \mathbb{R}$, denotamos $p^*(j\omega) = p(\omega) + jq(\omega)$, donde $p(\omega) = p_e(-\omega^2)$, $q(\omega) = \omega p_o(-\omega^2)$. Sean $\omega_{e_1}, \omega_{e_2}, \ldots$ los distintos ceros reales positivos de $p_e(-\omega^2)$ y sean $\omega_{o_1}, \omega_{o_2}, \ldots$ los distintos ceros reales positivos de $p_o(-\omega^2)$, ordenados en magnitud ascendente. Entonces las siguientes condiciones son equivalentes:*

(i): *$p^*(z)$ es Hurwitz estable.*

(ii): *p_n y p_{n-1} son del mismo signo y*

$$n = \begin{cases} \operatorname{sgn}[p_0] \cdot \{\operatorname{sgn}[p(0)] - 2\operatorname{sgn}[p(\omega_{o_1})] + 2\operatorname{sgn}[p(\omega_{o_2})] + \cdots + (-1)^{m-1} \\ \times 2\operatorname{sgn}[p(\omega_{o_{m-1}})] + (-1)^m \cdot \operatorname{sgn}[p(\infty)]\} \qquad \text{para } n = 2m, \\ \operatorname{sgn}[p_0] \cdot \{\operatorname{sgn}[p(0)] - 2\operatorname{sgn}[p(\omega_{o_1})] + 2\operatorname{sgn}[p(\omega_{o_2})] + \cdots + (-1)^{m-1} \\ \times 2\operatorname{sgn}[p(\omega_{o_{m-1}})] + (-1)^m \cdot 2\operatorname{sgn}[p(\omega_{o_m})]\} \qquad \text{para } n = 2m+1. \end{cases}$$

(12)

(iii): *p_n y p_{n-1} son del mismo signo y*

$$n = \begin{cases} \operatorname{sgn}[p_0] \cdot \{2 \operatorname{sgn}[q(\omega_{e_1})] - 2 \operatorname{sgn}[q(\omega_{e_2})] + 2 \operatorname{sgn}[q(\omega_{e_3})] + \cdots + (-1)^{m-2} \\ \times 2 \operatorname{sgn}[q(\omega_{e_{m-1}})] + (-1)^{m-1} \cdot 2 \operatorname{sgn}[q(\omega_{e_m})]\} \qquad \textit{para } n = 2m, \\ \operatorname{sgn}[p_0] \cdot \{2 \operatorname{sgn}[q(\omega_{e_1})] - 2 \operatorname{sgn}[q(\omega_{e_2})] + 2 \operatorname{sgn}[q(\omega_{e_3})] + \cdots + (-1)^{m-1} \\ \times 2 \operatorname{sgn}[q(\omega_{e_m})] + (-1)^{m} \cdot \operatorname{sgn}[q(\infty)]\} \qquad \textit{para } n = 2m+1. \end{cases}$$

(13)

Ver [2] para una prueba.

Observación 1. La propiedad de la alternancia en el Teorema 12 da una interpretación gráfica del criterio de Hermite-Biehler, mientras que el Lema 13 da una caracterización analítica.

Notemos del lema 13 que si $p^*(z)$ es Hurwitz estable entonces todos los ceros de $p(\omega)$ y $q(\omega)$ son reales y distintos, de lo contrario (12) y (13) fallarán.

Ahora presentamos un ejemplo para ilustrar la aplicación del Criterio 12 y del Lema 13, para verificar la propiedad de la alternancia en un polinomio estable.

Ejemplo 4. Consideremos el polinomio real $p^*(z)$, donde

$$p^*(z) = z^7 + 5z^6 + 14z^5 + 25z^4 + 31z^3 + 26z^2 + 14z + 4.$$

Entonces

$$p^*(j\omega) = p(\omega) + jq(\omega)$$

donde

$$p(\omega) = -5\omega^6 + 25\omega^4 - 26\omega^2 + 4,\ q(\omega) = \omega(-\omega^6 + 14\omega^4 - 31\omega^2 + 14).$$

Las gráficas de $p(\omega)$ y $q(\omega)$ son mostradas en la Figura 1. Por lo tanto, el polinomio $p^*(z)$, satisface la propiedad de la alternancia. Además

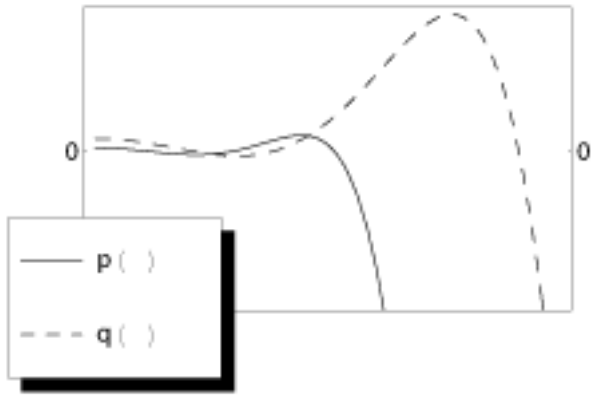


FIGURA 1. Propiedad de la alternancia para un polinomio Hurwitz.

$\omega_{e_1} = 0.43106$, $\omega_{e_2} = 1.08950$, $\omega_{e_3} = 1.90452$
$\omega_{o_1} = 0.78411$, $\omega_{o_2} = 1.41421$, $\omega_{o_3} = 3.37419$.

$\operatorname{sgn}[p(0)] = 1$, $\operatorname{sgn}[p(\omega_{o_1})] = -1$, $\operatorname{sgn}[p(\omega_{o_2})] = 1$, $\operatorname{sgn}[p(\omega_{o_3})] = -1$.
Ahora, $p^*(z)$ es de grado $n = 7$, el cual es impar y $\operatorname{sgn}[p_0] \cdot [\operatorname{sgn}[p(0)] - 2 \operatorname{sgn}[p(\omega_{o_1})] + 2 \operatorname{sgn}[p(\omega_{o_2})] - 2 \operatorname{sgn}[p(\omega_{o_3})]] = 7$; lo cual muestra que (12) se tiene.

También tenemos que
$\operatorname{sgn}[q(\omega_{e_1})] = 1$, $\operatorname{sgn}[q(\omega_{e_2})] = -1$, $\operatorname{sgn}[q(\omega_{e_3})] = 1$, $\operatorname{sgn}[q(\infty)] = -1$.

Así que: $\text{sgn}[p_0] \cdot [2\ \text{sgn}[q(\omega_{e_1})] - 2\ \text{sgn}[q(\omega_{e_2})] + 2\ \text{sgn}[q(\omega_{e_3})] - \text{sgn}[q(\infty)]] = 7$, con lo cual se tiene (13).

Para verificar que $p^*(z)$ es un polinomio Hurwitz, igualamos $p^*(z)$ a cero y encontramos sus raíces:

$$-0.5 \pm 1.3229j \qquad -0.5 \pm 0.8660j \qquad -1 \pm j \qquad -1.$$

Todas las raíces se encuentran en el semiplano izquierdo, así $p^*(z)$ es Hurwitz.

4.4. **Signatura y fase acumulada neta.** En esta subsección desarrollaremos, como paso preliminar para la generalización del criterio de Hermite-Biehler, una relación entre la fase acumulada neta de un polinomio real y la diferencia entre el número de raíces de un polinomio real en el semiplano abierto izquierdo y el semiplano abierto derecho. Sea $\mathbb{C}$ el plano complejo, $\mathbb{C}^-$ el semiplano abierto izquierdo y $\mathbb{C}^+$ el semiplano abierto derecho.

En principio nos enfocaremos en polinomios sin ceros en el eje imaginario. Consideremos un polinomio real $p^*(z)$ de grado n

$$p^*(z) = p_0 + p_1 z + p_2 z^2 + \cdots + p_n z^n,\ p_i \in \mathbb{R},\ i = 0, 1, \ldots, n,\ p_n \neq 0,$$

tal que, $p^*(j\omega) \neq 0,\ \forall \omega \in (-\infty, +\infty)$.

Definición 14. Sean l y r, el número de raíces de $p^*(z)$ en $\mathbb{C}^-$ y $\mathbb{C}^+$ respectivamente. Entonces la *signatura* de $p^*(z)$ denotada por $\sigma(p^*)$ se define como

$$\sigma(p^*) \triangleq l - r.$$

Ya que $n = l + r$, se tiene que $\sigma(p^*)$ y n determinan en forma única l y r, y por lo tanto, la distribución de raíces de $p^*(z)$. Ahora, para cada $\omega \in \mathbb{R}$, $p^*(j\omega)$ es un punto en el plano complejo, sean $p(\omega)$ y $q(\omega)$, dos funciones definidas como $p(\omega) = Re[p^*(j\omega)]$, $q(\omega) = Im[p^*(j\omega)]$.

Con esta definición, tenemos

$$p^*(j\omega) = p(\omega) + jq(\omega),\ \forall \omega.$$

Además, $\theta(\omega) \triangleq \angle p^*(j\omega) = \arctan[q(\omega)/p(\omega)]$. Sea $\Delta_0^\infty(\theta)$ que denota el cambio neto en el argumento $\theta(\omega)$, cuando ω crece de 0 a ∞. Entonces podemos afirmar el siguiente lema [4]:

LEMA 15. *Sea $p^*(z)$ un polinomio real sin raíces imaginarias. Entonces*

$$\Delta_0^\infty(\theta) = \frac{\pi}{2}\sigma(p^*).$$

Ver [2] y [4] para una demostración.

4.5. **Generalizaciones del Criterio de Hermite-Biehler: Ninguna raíz en el eje imaginario.** En esta subsección, nos enfocaremos en polinomios reales sin raíces en el eje imaginario y derivaremos dos generalizaciones del criterio de Hermite-Biehler, desarrollando primero un procedimiento para determinar el cambio de fase acumulada neta de un polinomio. Recordemos primero que para cualquier ω, el ángulo fase de $p^*(j\omega)$, es dado por

$$\theta(\omega) = \arctan \frac{q(\omega)}{p(\omega)}$$

Por lo tanto, la razón de cambio de fase con respecto a la variable dada ω, esta dada por

$$\begin{aligned} \frac{\mathrm{d}\theta(\omega)}{\mathrm{d}\omega} &= \frac{1}{1 + q^2(\omega)/p^2(\omega)} \left[\frac{q'(\omega)p(\omega) - p'(\omega)q(\omega)}{p^2(\omega)} \right] \\ &= \frac{q'(\omega)p(\omega) - p'(\omega)q(\omega)}{p^2(\omega) + q^2(\omega)} \end{aligned} \tag{14}$$

Si $p(\omega)$ y $q(\omega)$ son conocidas para toda ω, podemos integrar (14), para obtener la fase acumulada neta. Sin embargo, para calcular la acumulación neta de la fase, para

todo ω, no es necesario conocer en forma precisa la razón de cambio de fase en cada ω. Esto es porque cada vez que la gráfica polar $p^*(j\omega)$ hace una transición del eje real al eje imaginario o viceversa, puede haber a lo más un cambio de fase neto de $\pm\pi/2$ radianes. El signo real del cambio de fase puede ser determinado examinando (14), en el cruce del eje real ó imaginario de la gráfica de $p^*(j\omega)$. Ya que en el cruce del eje real ó imaginario, uno de los dos términos en el numerador de (14) se anula, y el denominador es siempre positivo, la determinación efectiva del signo cambio de fase es aún más simple.

Ahora, para cualquier polinomio $p^*(z)$ de grado mayor ó igual que uno, la parte real ó imaginaria ó ambas de $p^*(j\omega)$, llega a ser infinitamente grande cuando $\omega \to \pm\infty$. Sin embargo, si deseamos contar la acumulación de fase total en múltiplos enteros del cruzamiento de ejes, es imprescindible que la gráfica se aproxime al eje real o imaginario, cuando $\omega \to \pm\infty$. Para lograr esto, podemos normalizar la gráfica de $p^*(z)$, escalandola con $1/f(\omega)$, donde $f(\omega) = (1+\omega^2)^{n/2}$. Ya que $f(\omega)$ no tiene raíces reales, este escalamiento asegurará que la gráfica normalizada $p_f^*(j\omega) = p_f(\omega)+jq_f(\omega)$, realmente intersecta el eje real o imaginario en $\pm\infty$, mientras que al mismo tiempo, deja sin cambios los valores ω finitos en los cuales $p^*(j\omega)$ intersecta el eje real e imaginario.

$$p_f^*(j\omega) = p_f(\omega) + jq_f(\omega) = \frac{p(\omega)}{f(\omega)} + j\frac{q(\omega)}{f(\omega)}.$$

El siguiente desarrollo en esta sección hace uso de la gráfica normalizada, para la determinación del cambio de fase neto acumulado, cuando ω varía de 0 a ∞.

Como en la subsección 4.4, consideremos un polinomio $p^*(j\omega)$ de grado n

$$p^*(z) = p_0 + p_1 z + p_2 z^2 + \cdots + p_n z^n,\ p_i \in \mathbb{R},\ i = 0, 1, \ldots, n,\ p_n \neq 0,$$

tal que, $p^*(j\omega) \neq 0,\ \forall\omega \in (-\infty, +\infty)$.

Sean $p(\omega), q(\omega), p_f(\omega), q_f(\omega)$, ya definidas y sean

$$0 = \omega_0 < \omega_1 < \omega_2 < \cdots < \omega_{m-1}$$

los ceros finitos, reales, distintos y no negativos de $q_f(\omega)$ con multiplicidad impar.[1]

También definamos $\omega_m = +\infty$.

Entonces podemos hacer las siguientes observaciones:

(1) Si ω_i, ω_{i+1} son ambos ceros de $q_f(\omega)$ entonces:

$$\Delta_{\omega_i}^{\omega_{i+1}}(\theta) = \frac{\pi}{2}\left[\operatorname{sgn}[p_f(\omega_i)] - \operatorname{sgn}[p_f(\omega_{i+1})]\right] \cdot \operatorname{sgn}[q_f(\omega_i^+)]. \tag{15}$$

(2) Si ω_i es un cero de $q_f(\omega)$, mientras que $\omega_{i+1} = +\infty$ no es un cero de $q_f(\omega)$ y ω_{i+1} es un cero de $p_f(\omega)$, además de que n impar, entonces:

$$\Delta_{\omega_i}^{\omega_{i+1}}(\theta) = \frac{\pi}{2}\operatorname{sgn}[p_f(\omega_i)] \cdot \operatorname{sgn}[q_f(\omega_i^+)], \tag{16}$$

(3) Para $i = 0, 1, 2, \ldots, m-2$.

$$\operatorname{sgn}[q_f(\omega_{i+1}^+)] = -\operatorname{sgn}[q_f(\omega_i^+)]. \tag{17}$$

La ecuación (15) es obvia, mientras que la ecuación (17) simplemente establece que $q_f(\omega)$ cambia de signo cuando este pasa a través de un cero de multiplicidad impar. La ecuación (16), por otro lado, puede ser directamente trazada de la ec. (14).

Usando (17) repetidamente, obtenemos:

$$\operatorname{sgn}[q_f(\omega_i^+)] = (-1)^{m-1-i} \cdot \operatorname{sgn}[q_f(\omega_{m-1}^+)], i = 0, 1, \ldots, m-1. \tag{18}$$

Sustituyendo (18) en (15), vemos que si ω_i, ω_{i+1} son ambos ceros de $q_f(\omega)$, entonces

$$\Delta_{\omega_i}^{\omega_{i+1}}(\theta) = \frac{\pi}{2}\left[\operatorname{sgn}[p_f(\omega_i)] - \operatorname{sgn}[p_f(\omega_{i+1})]\right] \cdot (-1)^{m-1-i} \cdot \operatorname{sgn}[q_f(\omega_{m-1}^+)]. \tag{19}$$

Las observaciones anteriores nos permiten formular y demostrar el teorema siguiente acerca de $\sigma(p^*)$.

[1]La función $q_f(\omega)$, no cambia de signo mientras pasa a través de un cero real de multiplicidad par, ya que tales ceros pueden saltarse mientras se cuenta la fase de acumulación neta.

TEOREMA 16. *Sea $p^*(z)$ un polinomio real de grado n, sin raíces en el eje imaginario, i.e., la gráfica normalizada $p_f^*(j\omega)$ no pasa a través del origen. Sean $0 = \omega_0 < \omega_1 < \omega_2 < \cdots < \omega_{m-1}$ los ceros finitos, reales, distintos y no negativos de $q_f(\omega)$ con multiplicidad impar. También definamos $\omega_m = \infty$. Entonces*

$$\sigma(p^*) = \begin{cases} \{\text{sgn}[p_f(\omega_0)] - 2\ \text{sgn}[p_f(\omega_1)] + 2\ \text{sgn}[p_f(\omega_2)] + \cdots + (-1)^{m-1} \\ \times 2\ \text{sgn}[p_f(\omega_{m-1})] + (-1)^m \text{sgn}[p_f(\omega_m)]\} \cdot (-1)^{m-1} \\ \times \text{sgn}[q(\infty)] \quad \textit{si } n \textit{ es par}, \\ \\ \{\text{sgn}[p_f(\omega_0)] - 2\ \text{sgn}[p_f(\omega_1)] + 2\ \text{sgn}[p_f(\omega_2)] + \cdots + (-1)^{m-1} \\ \times 2\ \text{sgn}[p_f(\omega_{m-1})]\} \cdot (-1)^{m-1} \text{sgn}[q(\infty)] \quad \textit{si } n \textit{ es impar}. \end{cases}$$

(20)

Ver [2] para una demostración.

Ahora damos el resultado análogo al Teorema 16, usando los valores de las variables donde $p_f^*(j\omega)$ cruza el eje imaginario, sean

$$0 < \omega_1 < \omega_2 < \cdots < \omega_{m-1}$$

los ceros finitos, reales, distintos y no negativos de $p_f(\omega)$ con multiplicidad impar. También definamos $\omega_m = \infty$ y $\omega_0 = 0$.

TEOREMA 17. *Sea $p^*(z)$ un polinomio real de grado n, sin raíces en el eje imaginario, i.e., la gráfica normalizada $p_f^*(j\omega)$, no pasa a través del origen. Sean $0 < \omega_1 < \omega_2 < \cdots < \omega_{m-1}$ los ceros finitos, reales, distintos y no negativos de $p_f(\omega)$ con multiplicidad impar. También definimos $\omega_m = \infty$. Entonces*

$$\sigma(p^*) = \begin{cases} -\{2\ \text{sgn}[q_f(\omega_1)] - 2\ \text{sgn}[q_f(\omega_2)] + \cdots + (-1)^{m-2} \\ \times 2\ \text{sgn}[q_f(\omega_{m-1})]\} \cdot (-1)^m \text{sgn}[p(\infty)] \quad \textit{si } n \textit{ es par}, \\ \\ -\{2\ \text{sgn}[q_f(\omega_1)] - 2\ \text{sgn}[q_f(\omega_2)] + \cdots + (-1)^{m-2} \\ \times 2\ \text{sgn}[q_f(\omega_{m-1})] + (-1)^{m-1} \text{sgn}[q_f(\omega_m)]\} \cdot (-1)^m \\ \times \text{sgn}[p(\infty)] \quad \textit{si } n \textit{ es impar}. \end{cases}$$

(21)

Ver [2] para una demostración.

Observación 2. Los Teoremas 16 y 17, esencialmente generalizan el Lema 13, partes (ii) y (iii) para polinomios no necesariamente Hurwitz. Es en este sentido que los Teoremas 16 y 17 son generalizaciones del Criterio de Hermite-Biehler.

4.6. **El Criterio de Hermite-Biehler generalizado: Ninguna raíz en el origen.** En esta subsección extenderemos los Teoremas 16 y 17, ahora $p^*(z)$ puede tener raíces imaginarias distintas de cero. Los Teoremas 18 y 19 muestran que las expresiones en las afirmaciones de los Teoremas 16 y 17 son todavía válidas para este caso.

TEOREMA 18. *Sea $p^*(z)$ un polinomio real de grado n, sin raíces en el origen. Sean $0 = \omega_0 < \omega_1 < \omega_2 < \cdots < \omega_{m-1}$ los ceros finitos, reales, distintos y no negativos de $q_f(\omega)$ con multiplicidad impar. También definamos $\omega_m = \infty$. Entonces*

$$\sigma(p^*) = \begin{cases} \{\text{sgn}[p_f(\omega_0)] - 2\ \text{sgn}[p_f(\omega_1)] + 2\ \text{sgn}[p_f(\omega_2)] + \cdots + (-1)^{m-1} \\ \times 2\ \text{sgn}[p_f(\omega_{m-1})] + (-1)^m \text{sgn}[p_f(\omega_m)]\} \cdot (-1)^{m-1} \\ \times \text{sgn}[q(\infty)] \quad \textit{si } n \textit{ es par}, \\ \\ \{\text{sgn}[p_f(\omega_0)] - 2\ \text{sgn}[p_f(\omega_1)] + 2\ \text{sgn}[p_f(\omega_2)] + \cdots + (-1)^{m-1} \\ \times 2\ \text{sgn}[p_f(\omega_{m-1})]\} \cdot (-1)^{m-1} \text{sgn}[q(\infty)] \quad \textit{si } n \textit{ es impar}. \end{cases} \tag{22}$$

Ver [2] para una demostración.

A continuación presentamos el resultado análogo al Teorema 18, concerniente a $p_f(\omega)$.

TEOREMA 19. *Sea $p^*(z)$ un polinomio real de grado n, sin raíces en el origen. Sean $0 < \omega_1 < \omega_2 < \cdots < \omega_{m-1}$ los ceros finitos, reales, distintos y no negativos de $p_f(\omega)$, con multiplicidad impar. También definimos $\omega_m = \infty$. Entonces*

$$\sigma(p^*) = \begin{cases} -\{2\ \mathrm{sgn}[q_f(\omega_1)] - 2\ \mathrm{sgn}[q_f(\omega_2)] + \cdots + (-1)^{m-2} \\ \times 2\,\mathrm{sgn}[q_f(\omega_{m-1})]\}\,(-1)^m \\ \times \mathrm{sgn}[p(\infty)] \quad \textit{si } n \textit{ es par}, \\ \\ -\{2\mathrm{sgn}[q_f(\omega_1)] - 2\ \mathrm{sgn}[q_f(\omega_2)] + \cdots + (-1)^{m-2} \\ \times 2\ \mathrm{sgn}[q_f(\omega_{m-1})] + (-1)^{m-1}\,\mathrm{sgn}[q_f(\omega_m)]\} \cdot (-1)^m \\ \times \mathrm{sgn}[p(\infty)] \quad \textit{si } n \textit{ es impar}. \end{cases}$$

(23)

Ver [2] para una demostración.

4.7. **El Criterio de Hermite-Biehler generalizado: Ninguna restricción en la localización de raíces.** En esta subsección proporcionamos un refinamiento del Teorema 18, donde la presencia de raíces de $p^*(z)$ en el origen se puede admitir.

TEOREMA 20. *Sea $p^*(z)$ un polinomio real de grado n, con una raíz en el origen de multiplicidad k. Sean $0 < \omega_1 < \omega_2 < \cdots < \omega_{m-1}$ los ceros fínitos, reales, distintos, positivos de $q_f(\omega)$ con multiplicidad impar. También definimos $\omega_0 = 0$, $\omega_m = \infty$ y denotamos $p^{(k)}(\omega_0) = \dfrac{\mathrm{d}^k}{\mathrm{d}\omega^k}[p(\omega)]|_{\omega=\omega_0}$. Entonces*

$$\sigma(p^*) = \begin{cases} \{\mathrm{sgn}[p^{(k)}(\omega_0)] - 2\ \mathrm{sgn}[p_f(\omega_1)] + 2\ \mathrm{sgn}[p_f(\omega_2)] + \cdots + (-1)^{m-1} \\ \times 2\ \mathrm{sgn}[p_f(\omega_{m-1})] + (-1)^m\,\mathrm{sgn}[p_f(\omega_m)]\} \cdot (-1)^{m-1} \\ \times \mathrm{sgn}[q(\infty)] \quad \textit{si } n \textit{ es par}, \\ \\ \{\mathrm{sgn}[p^{(k)}(\omega_0)] - 2\ \mathrm{sgn}[p_f(\omega_1)] + 2\ \mathrm{sgn}[p_f(\omega_2)] + \cdots + (-1)^{m-1} \\ \times 2\ \mathrm{sgn}[p_f(\omega_{m-1})]\} \cdot (-1)^{m-1} \\ \times \mathrm{sgn}[q(\infty)] \quad \textit{si } n \textit{ es impar}. \end{cases}$$

(24)

Ver [2] para una demostración.

Utilizaremos el Teorema 20 en el siguiente ejemplo, para obtener información acerca de la distribución de las raíces de un polinomio, en el plano.

Ejemplo 5. Consideremos el polinomio

$$p^*(z) = z^4(z^2+4)(z-1)(z-2)(z-3)(z^2+z+1).$$

Sustituyendo $z = j\omega$, tenemos que $p^*(j\omega) = p(\omega) + jq(\omega)$, donde

$$p(\omega) = 5\omega^{10} - 21\omega^8 + 10\omega^6 - 24\omega^4$$

y

$$q(\omega) = -\omega^{11} + 10\omega^9 - 29\omega^7 + 20\omega^5.$$

Los ceros reales, finitos positivos de $q_f(\omega)$, con multiplicidad impar, son $\omega_1 = 1$, $\omega_2 = 2$ y $\omega_3 = \sqrt{5}$, también definimos $\omega_0 = 0$. Por lo tanto, $\mathrm{sgn}[p^{(4)}(\omega_0)] = -1$, $\mathrm{sgn}[p_f(\omega_1)] = -1$, $\mathrm{sgn}[p_f(\omega_2)] = 0$, $\mathrm{sgn}[p_f(\omega_3)] = 1$, además, $\mathrm{sgn}[q(\infty)] = -1$. Ya que $p^*(z)$ es de grado impar y con una raíz en el origen de multiplicidad 4, de la fórmula (24), se tiene que

$$\begin{aligned} \sigma(p^*) &= \{\mathrm{sgn}[p^{(4)}(\omega_0)] - 2\ \mathrm{sgn}[p_f(\omega_1)] + 2\ \mathrm{sgn}[p_f(\omega_2)] \\ &\quad - 2\ \mathrm{sgn}[p_f(\omega_3)]\} \cdot (-1)^3 \mathrm{sgn}[q(\infty)] \\ &= \{(-1) - 2(-1) + 2(0) - 2(1)\}(-1)^3(-1) = -1. \end{aligned}$$

De la factorización de $p^*(z)$, observamos que el polinomio tiene tres raíces reales y dos raíces con parte real negativa, además, como $\sigma(p^*) = l - r$, el Teorema 20 se cumple.

5. Conclusiones

En este trabajo se presentaron generalizaciones de los teoremas clásicos de estabilidad: el Criterio de Routh-Hurwitz, el Enfoque de Routh y el Teorema de Hermite-Biehler. Estos teoremas clásicos son utilizados para saber si un polinomio tiene todas sus raíces con parte real negativa, es decir, se utilizan para decidir si un polinomio es Hurwitz o no. La justificación de estudiar generalizaciones de tales teoremas es que en algunos problemas se requiere decidir si un polinomio tiene una propiedad diferente, que no es la propiedad de ser polinomio Hurwitz. En particular, muchas veces se requiere saber si un polinomio es semi-estable (esta clase de polinomios también son conocidos como semiHurwitz).

Bibliografía

[1] Bhattacharayya, S.P., Chapellat, H., Keel, L.H. (1995) *Robust Control: The Parametric Approach*, Prentice-Hall.
[2] Díaz, E.C. (2010) *El Teorema de Hermite-Biehler. Tesis de Maestría*, UAM-Iztapalapa, México, D.F.
[3] Ferreyra, V.M. (2011) *Métodos matriciales para el estudio de la estabilidad de polinomios*, UAM-Iztapalapa, México, D.F.
[4] Gantmacher, F.R. (1959) *The Theory of Matrices*, Vol I & Vol II, Chelsea Publishing Company, New York.
[5] Garloff, J., Wagner, D. (1996) *Hadamard products of stable polynomials are stable*, Journal of Mathematical Analysis and Applications, 202, 797-809.
[6] Hinrichsen, D., Pritchard, A.J. (2005) *Mathematical Systems Theory I*, Texts in Applied Mathematics, Vol. 48, Mathematical Systems Theory, Springer-Verlag Berlin Heidelberg.
[7] Hurwitz, A. (1895) *Über die Bedingungen, unter welchen eine Gleichung nur Wurzeln mit negativen reellen Teilen besitzt*, Math. Ann., vol. 46, 273-284.
[8] Lancaster, P. & Tismenetsky, M. (1985) *The Theory of Matrices with applications*, Academic Press.
[9] Loredo, C.A. (2004) *Criterios para determinar si un polinomio es polinomio Hurwitz. Reporte de los seminarios de investigación I y II*, UAM-Iztapalapa, México, D.F.
[10] Rendón, R. (2012) *Métodos de variable compleja en el estudio de polinomios Hurwitz. Reporte de los seminarios de investigación I y II*, UAM-Iztapalapa, México, D.F.
[11] Routh, E.J. (1975) *A Treatise on the Stability of a Given State of Motion*, Taylor and Francis, London, Reprint.
[12] Silva, G.J., Datta, A., Bhattacharayya, S.P. (2005) *PID Controllers for Time-Delay Systems*, Boston, Birkhäuser.
[13] Uspensky, J.V. (1990) *Teoría de ecuaciones,* Limusa.
[14] Wagner, D. (2000) *Zeros of reliability polynomials and f-vectors of matroids*, Combinatorics, probability and computing, vol. 9, 2, 167-190.

Dirección de los autores:
Carlos Arturo Loredo Villalobos
Universidad Autónoma Metropolitana,
Unidad Iztapalapa,
División de Ciencias Básicas e Ingeniería,
Departamento de Matemáticas.
Av. San Rafael Atlixco 186, Col. Vicentina
Del. Iztapalapa, C.P. 09340 México, D.F.
e-mail: r2ro.loredo@gmail.com

Edgar Cristian Díaz González
Universidad Autónoma Metropolitana,
Unidad Iztapalapa,
División de Ciencias Básicas e Ingeniería,
Departamento de Matemáticas.
Av. San Rafael Atlixco 186, Col. Vicentina
Del. Iztapalapa, C.P. 09340 México, D.F.
e-mail: edgardazgonzalez@yahoo.com.mx

Baltazar Aguirre Hernández
Universidad Autónoma Metropolitana,
Unidad Iztapalapa,
División de Ciencias Básicas e Ingeniería,
Departamento de Matemáticas.
Av. San Rafael Atlixco 186, Col. Vicentina
Del. Iztapalapa, C.P. 09340 México, D.F.
e-mail: bahe@xanum.uam.mx

Mixba'al
Revista Metropolitana de Matemáticas
No. 1, Vol. IV, junio de 2013, 53–60

ENTREVISTA REALIZADA AL DR. ERNESTO LACOMBA ZAMORA

ANA IRENE TOVAR EHLERS

FIGURA 1. De derecha a izquierda: Dr. Ernesto Lacomba Zamora, Dr. Gareth Roberts, Dr. Ernesto Pérez Chavela.

Ernesto: ten la seguridad de que cada enseñanza que nos legaste la hemos de seguir compartiendo con nuestros alumnos, fortaleciendo la escuela que tú creaste.

Ernesto Pérez Chavela

Realizar esta entrevista fue difícil, ya que tratar de capturar la esencia del Dr. Ernesto Lacomba en un par de líneas no es tarea fácil. La primera, de muchas clases que tomé con él, fue Ecuaciones Diferenciales Parciales, todos decían que era una clase complicada, sin embargo cuando él llegó al salón sólo vi a una persona sencilla, humilde y cálida que nos presentó de una manera inesperada el temario del curso y más aún lo hizo sumamente ameno. Durante estos y los siguientes cursos que tomé con él, todo el tiempo sólo vi amabilidad, tranquilidad, humildad y sencillez por su parte. Innumerables son los cursos que impartió e innumerables los alumnos que pasamos por sus manos, de todos los niveles, siempre amable y disponible para nuestras dudas.

Lamentablemente el Dr. Ernesto Lacomba falleció el pasado 26 de junio del 2012, pero jamás perdió la energía, la determinación y la entrega con sus alumnos, con sus colegas, con sus amigos y con su institución. Esta sólo es una forma de recordar a un excelente maestro, amigo, y colega; aunque sabemos que la mejor manera de honrar su memoria es predicando sus enseñanzas.

Hasta luego Maestro, buen viaje.

El Dr. Ernesto Lacomba Zamora nació en México, Distrito Federal, el 2 de diciembre de 1945. Desde pequeño mostró interés en las matemáticas. Su formación inicial fue en el Instituto Politécnico Nacional (IPN), ingresando en 1966 a la Carrera de Ingeniería en Comunicaciones y Electrónica, más tarde en 1968, ingresó a la carrera de Física y Matemáticas. ¿Cómo ingresa usted a la licenciatura en Física y Matemáticas?

Al terminar la vocacional, ingresé al IPN, soy totalmente egresado del IPN, excepto por el posgrado, que lo cursé en Estados Unidos. Cuando terminé la vocacional, ingresé a la carrera de Ingeniería en Comunicaciones y Electrónica, porque no estábamos bien informados que existiera la carrera de Físico- Matemáticas, en ese momento tenía 3 años de existencia, era muy nueva. Entré a Zacatenco y después de un año me enteré de esta carrera y decidí inscribirme a matemáticas a partir del segundo año, cada carrera era de 4 años así que cursé de manera simultánea, 3 años las dos carreras.

Sabemos que estudió el Doctorado en Matemáticas en la Universidad de California, Berkeley, siendo alumno de Stephen Smale con el trabajo Relative Equilibria and Bifurcation Sets for Geodesics on Homogeneous Spaces ¿Cómo eligió esta área de investigación?

Mi tesis de licenciatura en matemáticas fue sobre teoría de control y estuve dos años trabajando en el Instituto Mexicano del Petróleo, ahí teníamos un seminario sobre teoría de control. Si hubiese encontrado algo de esto en Berkeley mi trabajo hubiera sido en teoría de control, pero cuando llegué allá, había seminarios, asistí a ellos para ver en qué me interesaba, pero después vino Smale, que había estado de sabático y ofreció un curso que se llamaba "Geometría y Mecánica" relacionado con los artículos que acababa de escribir sobre sistemas mecánicos con simetría e incluye mecánica celeste en cuerpos rígidos. Entonces tomé un curso de tópicos, introductorio, que lleva un poco del material de esos artículos y luego hablé con él para saber si quería dirigir mi tesis, mi interés principal era mecánica celeste. Platicando con Smale me dijo -Muy bien, vamos a ver cuál es el problema para tu trabajo- y yo le pregunté -¿Qué pasa con sistemas mecánicos con simetría cuando la acción es transitiva? (es decir cuando el espacio es un espacio homogéneo en un grupo de Lie)- y le pregunté también -¿Cómo son los conjuntos de bifurcación y los conjuntos singulares?-. Smale me contestó -Ese es un buen problema, me parece que ese va a ser tu problema de tesis-. Y de ahí me seguí por esa línea y me gustó, aunque tuve que investigar mucho más, en cosas de geometría diferencial, grupos de Lie y espacios homogéneos, de lo que yo sabía, pero la idea fue siempre regresar a mecánica celeste. En 1972 terminé mi tesis y dos años después, en 1975, publiqué mi primer artículo sobre mecánica celeste.

¿Cómo es que se decide a trabajar con el Dr. Smale?

Había escuchado sobre él, porque era muy famoso en esa época, yo había ido a Berkeley con otro matemático, egresado de la Facultad de Ciencias de la UNAM, Alejandro López Yáñez, él fue quien me convenció que me fuera más pronto a estudiar el doctorado de lo que yo pensaba, pues en 1968 era el movimiento estudiantil, y había muchos problemas en el ambiente, y nada más estaba uno platicando sobre lo que ocurría, y preocupándose, él me comentó que ya había sido aceptado en Berkeley y me sugirió solicitar ingreso. Como ya no era tan fácil estudiar aquí, e incluso el

curso de maestría que tomé en el CINVESTAV se interrumpió por todos los conflictos estudiantiles. Estaba inscrito en dos cursos y asistí a uno de oyente, presenté trabajos, hice exámenes y todo y nunca me calificaron; entonces decidí irme. A finales de 1968 me fui a Berkeley, al doctorado directo, como el que ahora hay aquí en México, yo entré sólo con la licenciatura, se consideraba, no se si siga siendo así en Berkeley, que sólo si alguien no podía seguir adelante entonces se le daba la ocasión de presentar una maestría con un examen, o presentando una tesis, pero normalmente entraba uno al doctorado, esa era la idea.

¿Inicialmente trató de hacer una maestría en México?

Sí, aquí en el CINVESTAV me inscribí a la maestría en matemáticas. Y también mi compañero, él había pensado, desde hace tiempo, que quería trabajar con Smale. Me convenció y me dijo que seguramente me gustarían sus cursos y efectivamente tuvo razón. Aunque a veces era difícil seguirle, porque él trabajaba a un nivel muy alto, incluso cuando uno le preguntaba cosas, a veces pedía disculpas por no recordar las referencias, eran cosas que él consideraba más bien elementales y uno tenía que buscar por otro lado. Sí era importante su guía porque a veces decía cosas interesantes como cuando me preocupaba por hacer cálculos de algo y yo decía -¡está saliendo muy complicado! no sé qué pasa-, Smale me respondía -precisamente eso hace que las matemáticas sean más interesantes, si fuera algo muy simple entonces no tendría mucho chiste-.

¿Berkeley fue la única universidad a la que solicitó ingreso?

Solicité ingreso en tres universidades distintas, una era la Universidad de Maryland, que tenía gente de control y ecuaciones diferenciales, la segunda fue Berkeley, y otra que no me acuerdo cuál era, entonces yo estaba esperando que me contestaran de las tres, pero decidí ir a Berkeley, era una de mis posibilidades, pero no me había decidido todavía por alguna.

Actualmente es profesor titular C en el Departamento de Matemáticas de la Universidad Autónoma Metropolitana Unidad Iztapalapa, siendo también fundador de esta Institución. ¿Cómo empezó su carrera académica?

Al regresar de Berkeley mi esposa y yo teníamos ganas de ir al cono sur. Así que trate de ver si podía ir a Argentina o a Brasil, fue ahí cuando concursé para un posdoctorado que se llamaba, y creo que ya no existen, Latin American Teaching Fellowship en la Universidad de Tast en Boston; hice mi solicitud, me entrevistaron y finalmente me aprobaron. Me comentaron que iría a Brasilia porque era la universidad que estaba interesada en alguien como yo. Ahí estuve poco menos de un año, de hecho allá me llegó ¡por correo! el diploma del doctorado. Yo había impartido clases en la Escuela Superior de Física y Matemáticas en el IPN. Durante mi estancia en Berkeley impartí 2 años una ayudantía para recibir una ayuda extra. Cuando llegué a Brasilia fui directamente a dar clase, ahí lo interesante fue el idioma, ellos hablan portugués y el primer semestre me tocó un grupo de alumnos de maestría con un curso introductorio de análisis, como eran de maestría, podía yo hablar en español, después de ese semestre vino un curso de verano de dos meses, del verano de allá, que es enero y febrero, y ahí sí di el curso en "portuñol", tratando de hablar una mezcla de ambas cosas.

¿Hablaba un poco de Portugués?

No, un poco, porque había leído libros de Lima, que vienen de Brasil, pero fuera de eso, no sabía mucho. Ese curso era muy grande, tenía 120 estudiantes, aunque tenía dos ayudantes, pero era un curso intensivo, pues era de verano. A veces mientras visitaba el centro de Brasil, veía alumnos por todos lados, pero fue muy interesante y los alumnos

quedaron muy contentos a pesar de que yo estaba iniciándome en "portuñol". Estuve un ciclo escolar y después un semestre impartiendo un curso de licenciatura, aunque este último fue más fácil porque ya llevaba un poco más de práctica en "portuñol".

¿Y después de estar en Brasil regresó a México?

Sí, de hecho, de Brasilia comencé a escribir a un par de instituciones, creo que una de ellas era el Instituto de Matemáticas y otro era el IIMAS. Mi compañero Alejandro López Yáñez había regresado al IIMAS, él se regresó un poco antes de terminar su doctorado, entonces le costó más trabajo, estaba en el IIMAS y me dijo - ¡Vente! tengo un seminario con alumnos sobre mecánica celeste- y finalmente solicité en el IIMAS y ahí fue a donde entré cuando vine a México.

Además de ser profesor titular en el Departamento de Matemáticas es fundador y miembro del área Ecuaciones Diferenciales y Geometría. ¿Cómo se incorporó a la UAM?

Todavía no existía la UAM, eso fue en agosto de 1973, de hecho, se decretó la creación de la UAM hasta enero de 1974 pero yo me enteré hasta poco después. Había varios profesores, sobre todo el Dr. Alberto Luis Moncayo, que en paz descanse, fue el primer jefe de departamento; y trabajaba en el IIMAS, entonces como me conocía junto con otro par de profesores nos dijo -¡tienen que venirse conmigo! pues estoy creando un departamento de matemáticas ahí en la UAM-. Como el ambiente, en el pequeño departamento del IIMAS no era tan propicio, me pareció interesante entrar a la UAM y crear nuevos planes de estudio y decidí aceptar. Fui el primer miembro, oficialmente, del departamento, después del jefe de departamento. De hecho, cuando comenzamos nos reuníamos en unas oficinas de Insurgentes, por San Ángel, no había nada construido, luego nos empezaron a traer aquí para ver cómo comenzaban a construir los edificios y ya unos meses después nos mudamos a un edificio pequeño donde estaba toda la división de Ciencias Básicas e Ingeniería.

¿Cuánto tiempo pasó antes de que en la UAM se iniciaran las clases?

Creo que el Dr. Moncayo comenzó a hablar con nosotros en mayo, yo entré, oficialmente, a partir del 1 de junio de 1974 y la UAM comenzó a impartir clases como el 20 de septiembre de ese año, con algunos pequeños edificios de aulas que ya tenían para ese momento, como eran alumnos de primer ingreso de licenciatura iniciamos con cursos de cálculo. Por cierto algunos de esos primeros cursos no fueron tan agradables de dar, porque como era de nueva creación la UAM había gente de un nivel muy heterogéneo, venían por ejemplo gente de la Normal Superior que los habían admitido y creían que ellos podían, pero la preparación que tenían no era tan buena, o también gente que no había podido con otras carreras y venía con la idea de creo que aquí si puedo, y al principio impartí clases en la tarde que era más complicado, porque era gente que trabajaba, entonces hubo cursos en que los alumnos no respondían mucho, pero más adelante ya comenzó a cambiar la situación.

Además de trabajar en la UAM ha sido Profesor e investigador en la Universidad Federal de Brasilia, Brasil; en el Instituto de Investigación en Matemáticas Aplicadas y Sistemas de la UNAM y en la Escuela Superior de Física y Matemáticas del IPN y ha sido profesor invitado en el Institut des Hautes Études Scientifiques de París y en la Universidad de París, en el Eidgenössische Technische Hochschule (Colegio Técnico Federal) de Zurich, Suiza; en el Centre de Recerca Matemática, en Cataluña; en el Consejo Superior de Investigaciones Científicas, en España y en la Universidad de California, seguramente esto le ha permitido tener un panorama bastante amplio de lo que es el desarrollo matemático, lo que me lleva a preguntarle, ¿cuál es su opinión sobre el desarrollo de la matemática en México?

La veo muy bien, pues considero que actualmente se han consolidado muchos grupos de investigación en distintas instituciones, tanto la UAM, como la UNAM, el CINVESTAV, y otros lugares también en provincia y se cultivan muchas de las áreas de investigación que hay en matemáticas y a un nivel muy bueno, digamos a nivel internacional, considero que en este momento está muy desarrollada.

¿Cómo visualiza el futuro de la matemática en México?

Yo creo que también hay un problema de saturación, yo creo que va a llegar un momento en que más o menos se va a estabilizar. No es una carrera totalmente saturada, pero yo creo que está muy cerca de la saturación, hay otras carreras que ya están saturadas hace tiempo, ingeniería por ejemplo, y sobre todo, ciertas áreas de la ingeniería, pero matemáticas yo creo que en algún momento va a saturarse.

¿Considera que el apoyo que se da a la investigación es suficiente?

Yo creo que no es suficiente, sobre todo en los últimos años, que por razones económicas CONACYT y otros organismos han estado recortando el presupuesto, el mismo presupuesto de las universidades ha disminuido. Yo creo que sí debería darse más énfasis en la educación y la investigación de lo que se está dando, todavía hace falta, porque creo que los políticos aún no reconocen que también la investigación es importante para desarrollar tecnología, como pasa en países desarrollados, ellos sí conocen esa influencia.

Dentro de los trabajos que usted ha realizado confluyen varias áreas de la física y de las matemáticas, entre ellas la de los sistemas hamiltonianos y la de la geometría simpléctica y entre sus líneas de estudio se encuentran la mecánica celeste, contribuyendo en el estudio de singularidades (colisiones y escapes) en los problemas de n cuerpos con simetrías, así como en las propiedades de sistemas mecánicos homogéneos. ¿Son éstos, todavía, problemas que se puedan tratar durante un posgrado?

Por el lado de geometría simpléctica he hecho aplicaciones a circuitos eléctricos y también he hecho aplicaciones a termodinámica de geometría simpléctica y geometría de contacto que está muy relacionada. En principio sí pueden estudiarse durante un posgrado, aunque ya no estoy tan involucrado en eso, aunque a nivel de maestría podría dirigir a alguien, a nivel doctorado tendría que pensarlo porque como estoy más metido con el lado de sistemas mecánicos clásicos y mecánica celeste, movimiento de vórtices y fuentes en fluidos en dos dimensiones y ese tipo de cosas.

¿Cuáles son los proyectos que puede un alumno desarrollar bajo su tutoría?

En mecánica celeste, la posibilidad de caos o tratar de describir globalmente lo más posible las soluciones. Por supuesto ahí estamos suponiendo que la dimensión del espacio fase no es tan alta para que se pueda hacer. Estudiar también colisiones, para lo cual hay que aplicar también un método que se llama explosión de singularidades que esencialmente viene de la geometría algebraica, nada más que aquí lo aplicamos a nivel de energía, tomamos la ecuación de energía y hacemos una explosión, pero luego para que las ecuaciones de movimiento tampoco tengan singularidades hay que hacer un cambio en la escala de tiempo.

Usted ha visto muchas generaciones de alumnos egresar de diferentes instituciones, sin embargo todos hemos requerido de una guía mientras realizamos nuestros estudios. ¿Cuál cree usted que es el mejor momento, y la mejor forma para tomar un alumno y guiarlo académicamente?

La mejor manera es por medio de seminarios, normalmente yo no lo hago, pero hay colegas, incluso en mi área que dan seminarios para interesar a alumnos en mecánica celeste, entonces los van llevando de la mano y encaminando. Yo en el pasado, en la época en que no había gente que estuviera en mi área, promoví seminarios, para profesores, en que también podían entrar alumnos, entonces mucho tiempo tuvimos un seminario de mecánica celeste que después se convirtió en seminario del área de ecuaciones diferenciales y geometría; y que sigue actualmente funcionando, yo creo que la forma más adecuada es mediante seminarios y hacer que los alumnos discutan con uno cuando tienen inquietudes.

Actualmente es miembro del Sistema Nacional de Investigadores de nivel III. Entre sus distinciones, cuenta con Mención Honorífica del Premio de Investigación Noriega Morales (Ciencias Exactas) de la Organización de Estados Americanos en 1985, Premio de Investigación en Ciencias Básicas e Ingeniería 1987 por la Universidad Autónoma Metropolitana. Ha recibido la presea "Lázaro Cárdenas", otorgada por el Instituto Politécnico Nacional a sus egresados distinguidos en 1993, Premio de Investigación al área de Ecuaciones Diferenciales y Geometría, en 1995, por la Universidad Autónoma Metropolitana y el premio Ciudad Capital que lleva el nombre de "Silvia Torres Castilleja" en la categoría de Ciencias Básicas por el Instituto de Ciencia y Tecnología del Distrito Federal, en 2007, sé que estos premios no han sido gratis y que ha trabajado duro para conseguir cada uno de estos galardones. ¿Cuál considera usted que ha sido la cualidad que le ha llevado a ganar estas distinciones?

Posiblemente, trabajar en forma consistente aunque eso no quiere decir ser "workaholic"[1], ahora que estuve enfermo me di cuenta que uno también tiene que descansar y no aceptar muchas comisiones extra y eso que luego te dan. Como cuando CONACYT lo llama a uno para hacer evaluaciones o para pertenecer a algunas comisiones y cosas así, todo esto le resta a uno tiempo y hay que saber aceptar algunas, pero decir que no a otras. En primer lugar, trabajar mucho pero hasta cierto límite, porque la salud lo puede resentir, y ser amistoso con los alumnos y con todos los compañeros, también eso es muy importante, cultivar colaboradores y gente que está en el mismo campo con quien se pueda discutir tanto aquí como en el extranjero. Y tener una visión de que uno quiere formar un grupo o algo similar. Tal vez yo no lo tenía tan claro, pero en algún momento sentía que me gustaría formar un grupo y yo creo que eso también fue importante.

¿Estos premios le significan algún compromiso con la sociedad y no sólo me refiero al ámbito académico?

Bueno, una cosa que es de preocuparse en este momento en México es el nivel de matemáticas entre primaria y preparatoria, está bastante bajo como lo han mostrado estudios que han hecho a alumnos de distintos países, entonces yo creo que ese es un problema que hay que afrontar y con ejemplos como el mío o como la gente que se destaca puede uno tratar de influir en ese aspecto.

Una forma de inculcar a los chicos el interés por la matemática es haciendo difusión de los logros y de los descubrimientos, en términos generales, haciendo divulgación. ¿Ha impartido conferencias de divulgación?

[1]**Nota de la autora:** La palabra es, en sí, una composición de las palabras trabajo y alcohólico. De acuerdo con William Safire, el término fue acuñado por Wayne Oates en 1968. Este término hace referencia a comportamientos de adicción al trabajo y fue ganando popularidad en los años 90's. [Wayne E. Oates, *On Being a "Workaholic" (A Serious Jest)*, Pastoral Psychology 19 (October 1968), pages 16-20.]

Sí, últimamente no, pero cuando me lo han solicitado las he impartido, y de hecho en el programa "Domingos en la Ciencia" y en "Lunes en la Ciencia" he dado charlas, a veces cuando me piden hablar en seminarios para alumnos, en el CINVESTAV y en el ITAM he ido algunas veces, no ocurre tan frecuente, pero en una ocasión mi sobrina me pidió que fuera a dar una charla a una preparatoria, los alumnos querían una orientación, entonces fui a darles una charla de divulgación para que supieran de qué se tratan las matemáticas, últimamente me solicitaron una charla en el UNIVERSUM por parte de la Academia Mexicana de Ciencias, pero la tuve que posponer, primero se pospuso por la influenza, y luego por información cruzada, así que hasta el año próximo que tenga tiempo de prepararles algo más al día y con calma, pero sí he estado siempre interesado en eso, incluso he tenido también alumnos del programa de verano de investigación científica.

Recientemente se realizó el VI INTERNATIONAL SYMPOSIUM HAMSYS-2010, en su honor, por su 65 Aniversario, eso es algo que se suele hacer para demostrar la admiración hacia un Investigador, usted ya sabe que nosotros lo admiramos, sin embargo nos gustaría saber usted, ¿a quién admira?

¿Quién es mi matemático favorito? No sé si haya uno solo, pero puede ser que hayan dos esencialmente, el primero el Dr. Smale, con quien ya no he tenido contacto, sobre todo porque el trabaja en otras cosas, él está tan lleno de ideas y por eso cambia rápidamente de campo. El segundo que considero importante y además es muy bromista es el Dr. Don Saari, estuvo en la celebración de HAMSYS, es alguien muy activo que trabaja en esto y también en otras cosas que tienen que ver con economía y con votaciones.

Para las nuevas generaciones, ¿tiene algún consejo que le gustaría compartir?

Se tienen que esmerar en sus cursos, y posiblemente lo que alguna vez, si tienen problemas, dirigirse hacia la meditación o algo que les permita entrar en contacto con su interior y que puedan resolverlo y no les estorbe para sus estudios. Yo empecé a meditar hace cuarenta años desde 1970. El tipo de meditación que practicamos actualmente es el Siddha Yoga, sin embargo, para los métodos y algunas de las terapias de sanación que estuve siguiendo en los últimos años hay dos que tienen que ver con meditación. En general la medicina alternativa tiene muchas ventajas con respecto a la medicina tradicional, por supuesto que en casos de crisis hay que ir al hospital, a mi me ocurrió hace cuatro años, pero para curar a uno, principalmente de enfermedades graves como cáncer o diabetes o muchas enfermedades la medicina alterna es la que funciona.

Muchas gracias por su tiempo, me gustaría saber si desea agregar algún otro comentario.

Lo que me gustaría agregar es que dentro del grupo de investigación que he formado, los investigadores más importantes son Ernesto Pérez Chavela y Joaquín Delgado Fernández ellos en el SNI son nivel III y II respectivamente. Y sobre la parte académica lo que más me gusta de trabajar aquí en la UAM-I es que en principio uno puede dar clase y dirigir alumnos en investigación a todos los niveles, desde el tronco general, en Ciencias Biológicas y de la Salud, en Ciencias Básicas e Ingeniería, Ciencias Sociales y Humanidades y cursos de licenciatura que pueden ser del tronco común donde pueden entrar también físicos e ingenieros, cursos de licenciatura propiamente para matemáticos, luego cursos de maestría y dirigir alumnos de investigación en el doctorado, es decir, podemos cubrir todos los rangos posibles de enseñanza.

Universidad Autónoma Metropolitana 13 de diciembre 2011.

Agradecimientos: Quiero agradecer a los árbitros por sus valiosos comentarios para mejorar la edición de esta entrevista, al Dr. Ernesto Pérez Chavela por facilitarnos la fotografía y al comité editorial por la oportunidad de publicarla.

Dirección de la autora:
Ana Irene Tovar Ehlers,
Posgrado en Museología,
Escuela Nacional de Conservación,
Restauración y Museografía,
"Manuel Castillo Negrete" (ENCRYM).
e-mail: annyrn.mat@gmail.com

Casa abierta al tiempo

UAM - Iztapalapa

Posgrados:
Maestría y Doctorado en Matemáticas

pmat@xanum.uam.mx
http://pmat.izt.uam.mx/

LÍNEAS DE INVESTIGACIÓN

Teoría de anillos y módulos.
Teoría de conjuntos y lógica.
Geometría algebraica.
Geometría diferencial y Riemanniana.
Teoría de números.
Teoría de códigos y criptografía.
Análisis geométrico.
Física matemática.
Análisis diferencial.
Matemáticas discretas, combinatoria y gráficas.
Dinámica de fluidos computacional.
Resolución numérica de ecuaciones en derivadas parciales.
Métodos matemáticos en finanzas y economía.
Control y sistemas dinámicos.
Mecánica celeste, sistemas hamiltonianos y aplicaciones a la física.
Control, estabilidad y robustez de sistemas estocásticos.
Metodología estadística.
Estadística asintótica.
Topología de conjuntos, grupos topológicos y Cp-teoría.
Métodos geométricos en mecánica. Dinámica de vórtices. Mecánica celeste.

Maestría en Ciencias Matemáticas Aplicadas e Industriales (MACMAI)

mlss@xanum.uam.mx
http://mcmai.izt.uam.mx

LÍNEAS DE INVESTIGACIÓN

Códigos y Criptografía.
Control y Sistemas Dinámicos.
Combinatoria y Optimización.
Estadística.
Métodos Matemáticos en Finanzas.
Modelación y Simulación Computacional.

UNIVERSIDAD AUTÓNOMA METROPOLITANA, UNIDAD IZTAPALAPA
DEPARTAMENTO DE MATEMÁTICAS, EDIFICIO ANEXO DEL T, 3ER PISO, TEL. 58044656 FAX. 5804 4660
AV. SAN RAFAEL ATLIXCO No 186, COL. VICENTINA, IZTAPALAPA, MÉXICO, D.F.

Casa abierta al tiempo

UAM-Iztapalapa

Contenido